Ch. 3 Cyclic Codes

□ Topics in the Chapter

- Definition of Cyclic Codes
- Polynomial Representation
- Generator and Parity Check Polynomials
- Systematic Encoding
- Syndrome Calculation
- Examples: Hamming, Golay, Simplex Codes, etc.

□ Definition of a Cyclic Code

Definition: An $[n,k]$ code is said to be cyclic

if $\underline{c} = (c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C$.

Note: $T =$ cyclic shift operation (to the right)

$$T^i\underline{c} = \underbrace{T \cdots T}_{i \text{ times}}\underline{c} = (c_{n-i}, \cdots, c_{n-1}, c_0, c_1, \cdots, c_{n-i-1})$$

If C is cyclic, then $T^i\underline{c} \in C, \ \forall i = 0,1,2,\cdots, \ \forall \underline{c} \in C$

○ Advantages of cyclic codes

(a) Easy implementation of encoder and syndrome calculator.

(b) Easy to develope implementable decoding algorithm.

(c) Robust against burst errors.

□ Polynomial Representation of Cyclic Codes

○ Polynomial representation

$$\underline{c} = (c_0, c_1, \cdots, c_{n-1}) \longleftrightarrow c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

Cyclic shift of $\underline{c}$ by i positions:

$(c_{n-i}, \cdots, c_{n-1}, c_0, c_1, \cdots, c_{n-i-1})$

$$\longleftrightarrow c_{n-i} + \cdots + c_{n-1} x^{i-1} + c_0 x^i + c_1 x^{i+1} + \cdots + c_{n-i-1} x^{n-1}$$

$$= c_0 x^i + c_1 x^{i+1} + \cdots + c_{n-i-1} x^{n-1} + c_{n-i} x^n + \cdots + c_{n-1} x^{i-1}$$

$$= c_0 x^i + c_1 x^{i+1} + \cdots + c_{n-i-1} x^{n-1} + \underbrace{c_{n-i} x^n + \cdots + c_{n-1} x^{n+i-1}}_{\hookrightarrow \text{ use } x^n = 1}$$

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

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

○ If an $[n, k]$ code C is cyclic, then there is a polynomial $g(x)$ called "generator polynomial", such that $\{g(x), xg(x), \cdots, x^{k-1} g(x)\}$ forms a basis of C.

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

where $g(x) \mid x^n + 1$, $g_{n-k} \neq 0$ (so $\deg g(x) = n - k$)

(In fact, $g_0 = g_{n-k} = 1 \Rightarrow$ the binary case to make $g(x)$ unique.)

○ Code polynomial $c(x) \in C$,

$$c(x) = m_0 g(x) + m_1 x g(x) + m_2 x^2 g(x) + \cdots + m_{k-1} x^{k-1} g(x)$$

$$= (m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}) g(x)$$

i.e. $c(x) = m(x) g(x)$

○ Total # of message polynomials $= 2^k = |C|$

○ $i-$th coefficient in $c(x) = m(x) g(x)$

$$c_i = \sum_{j=0}^{i} m_j g_{i-j}$$

$$= m_i * g_i \qquad \text{"convolution"}$$

Note:

time domain		transform domain
$(c_0, c_1, \cdots, c_{n-1})$	$\longleftrightarrow$	$c(x)$
$m_i * g_i$	$\longleftrightarrow$	$m(x) g(x)$

Example: [7,4] Hamming code (cyclic)

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

$n-k = 3$

$g(x) = x^3+x+1$ (or, x^3+x^2+1 may be chosen).

	polynomial representation	vector representation
$0 \cdot g(x)$	0	(0 0 0 0 0 0 0)
$1 \cdot g(x)$	$1+x+x^3$	(1 1 0 1 0 0 0)ⓞ
$x \cdot g(x)$	$x+x^2+x^4$	(0 1 1 0 1 0 0)①
$(1+x)g(x)$	$1+x^2+x^3+x^4$	(1 0 1 1 1 0 0)
$x^2g(x)$	$x^2+x^3+x^5$	(0 0 1 1 0 1 0)②
$(1+x^2)g(x)$	$1+x+x^2+x^5$	(1 1 1 0 0 1 0)
$(x+x^2)g(x)$	$1+x+x^3+x^4+x^5$	(0 1 1 1 0 0 1)
$(1+x+x^2)g(x)$	$1+x^4+x^5$	(1 0 0 0 1 1 0)④
$x^3g(x)$	$x^3+x^4+x^6$	(0 0 0 1 1 0 1)③
$(1+x^3)g(x)$	$1+x+x^4+x^6$	(1 1 0 0 1 0 1)
$(x+x^3)g(x)$	$x+x^2+x^3+x^6$	(0 1 1 1 0 0 1)
$(1+x+x^3)g(x)$	$1+x^2+x^6$	(1 0 1 0 0 0 1)⑥
$(x^2+x^3)g(x)$	$x^2+x^4+x^5+x^6$	(0 0 1 0 1 1 1)
$(1+x^2+x^3)g(x)$	$1+x+x^2+x^3+x^4+x^5+x^6$	(1 1 1 1 1 1 1)
$(x+x^2+x^3)g(x)$	$x+x^5+x^6$	(0 1 0 0 0 1 1)⑤
$(1+x+x^2+x^3)g(x)$	$1+x^3+x^5+x^6$	(1 0 0 1 0 1 1)

Note:

A nonzero code polynomial of minimum degree is a generator polynomial for the code C.

○ Possible generator polynomials of cyclic code of length 7

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

generator polynomial	parameters	name of codes
1	$[7,7]$	entire space
$x+1$	$[7,6]$	even parity check code
x^3+x+1	$[7,4]$	Hamming code
$(x+1)(x^3+x+1)$	$[7,3]$	expurgated Hamming code
x^3+x^2+1	$[7,4]$	Hamming code
$(x+1)(x^3+x^2+1)$	$[7,3]$	expurgated Hamming code
$(x^3+x+1)(x^3+x^2+1)$	$[7,1]$	repetition code
$(x+1)(x^3+x+1)(x^3+x^2+1)$	$[7,0]$	zero code = {0}

○ Generator polynomial $g(x)$ for an $[n,k]$ cyclic code C

Code polynomial:

$$c(x) = m(x)g(x)$$

$$\Rightarrow \{g(x), xg(x), x^2g(x), \cdots, x^{k-1}g(x)\} \text{ is a basis.}$$

The generator matrix for C is

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots\cdots & g_{n-k} & 0 & 0 & \cdots\cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots\cdots & g_{n-k} & 0 & \cdots\cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & 0 & \cdots\cdots & g_0 & g_1 & g_2 & \cdots\cdots & g_{n-k} \end{bmatrix}.$$

Example: $[7,4]$ Hamming code defined by $g(x) = x^3+x+1$:

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

By elementary row operations, it may be changed to a systematic code.

□ Check Polynomial of an $[n,k]$ Cyclic Code

○ Find $h(x)$ such that $h(x)g(x) = x^n+1$:

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

where $\deg h(x) = k,\ h_0 \neq 0,\ h_k = 1,$ then

$$\begin{aligned} c(x)h(x) &= m(x)g(x)\cdot h(x) \\ &= m(x)(x^n+1) = 0 \qquad (\because x^n=1) \end{aligned}$$

Therefore, the parity check matrix is

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots\cdots & h_1 & h_0 & 0 & 0 & \cdots\cdots\cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & \cdots\cdots\cdots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & 0 & \cdots & & h_k & h_{k-1} & h_{k-2} & \cdots h_1 & h_0 \end{bmatrix}$$

Note: $c(x)h(x) = 0$

$$\updownarrow \qquad \Rightarrow \begin{array}{|cccc|} \hline h_k & h_{k-1} & \cdots & h_0 \\ \hline \end{array}$$

$$\begin{array}{|cccccc|} \hline c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \\ \hline \end{array}$$

$$c_i * h_i = 0$$

Example: $[7,4]$ cyclic code with $g(x) = x^3+x+1$:

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

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \Rightarrow \quad H' = \left[\begin{array}{cccc:ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Note: Dual code:

An $[n,k]$ cyclic code generated by g(x) has the $[n,n-k]$ dual code, which is generated by

$$h^*(x) = h^k + h^{k-1}x + \cdots + h_1 x^{k-1} + h_0 x^k$$
$$= \text{reciprocal of } h(x)$$

□ Systematic Encoding of an $[n,k]$ Cyclic Code

○ Generator polynomial: $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$,

where $g_0 = g_{n-k} = 1$ (in binary case).

○ Message polynomial: $m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$,

$$x^{n-k+i} = g_i(x)g(x) + r_i(x), \quad i = 0, 1, \cdots, k-1$$

where $\deg\ r_i(x) < n-k$.

$$\Rightarrow \quad x^{n-k+i} + r_i(x) = g_i(x)g(x)$$

Therefore, $x^{n-k+i} + r_i(x)$ is a codeword.

$$(r_i(x) = r_{i0} + r_{i1}x + r_{i2}x^2 + \cdots r_{i,n-k-1}x^{n-k-1})$$

○ New basis for $C = \{x^{n-k+i} + r_i(x) \mid i = 0, 1, \cdots, k-1\}$

$$\begin{aligned}
x^{n-k} + r_0(x) &\leftrightarrow (r_{00}\ r_{01}\ r_{02}\ \cdots\ r_{0n-k-1} \ \vdots\ 1\ 0\ 0\ 0\ \cdots\ 0)\\
x^{n-k+1} + r_1(x) &\leftrightarrow (r_{10}\ r_{11}\ r_{12}\ \cdots\ r_{1n-k-1} \ \vdots\ 0\ 1\ 0\ 0\ \cdots\ 0)\\
x^{n-k+2} + r_2(x) &\leftrightarrow (r_{20}\ r_{21}\ r_{22}\ \cdots\ r_{2n-k-1} \ \vdots\ 0\ 0\ 1\ 0\ \cdots\ 0)\\
&\ \ \vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad \vdots\\
x^{n-1} + r_{k-1}(x) &\leftrightarrow (r_{k-1,0}\, r_{k-1,1}\, r_{k-1,2} \cdots r_{k-1,n-k-1} \ \vdots\ 0\ 0\ 0\ 0\ \cdots\ 1)
\end{aligned}$$

Therefore, the generator matrix of an $[n, k]$ systematic cyclic code is

$$G = \left[\begin{array}{cccc|cccc} r_{00} & r_{01} & r_{02} & \cdots & r_{0,n-k-1} & 1 & 0 & \cdots & 0 \\ r_{10} & r_{11} & r_{12} & \cdots & r_{1,n-k-1} & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & & \vdots \\ r_{k-1,0} & r_{k-1,1} & r_{k-1,2} & \cdots & r_{k-1,n-k-1} & 0 & 0 & \cdots & 1 \end{array}\right]$$

P I_k

$$H = [\, I_{n-k} \;\vdots\; P^t \,]$$

○ Generation of systematic cyclic code:

Division by generator polynomial: $x^{n-k} \cdot m(x) = q(x)g(x) + p(x)$

Code polynomial: $c(x) = x^{n-k} \cdot m(x) + p(x) = q(x)g(x)$

where $q(x)$: quotient polynomial, $p(x)$: remainder polynomial.

Example: $[7, 4]$ cyclic code generated by $g(x) = x^3 + x + 1$

$n - k = 3$

$$\left.\begin{array}{l} x^3 = 1g(x) + x + 1 \\ x^4 = xg(x) + x^2 + x \\ x^5 = (x^2 + 1)g(x) + x^2 + x + 1 \\ x^6 = (x^3 + x + 1)g(x) + x^2 + 1 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{New basis} \\ 1 + x + x^3 \\ x + x^2 + x^4 \\ 1 + x + x^2 + x^5 \\ 1 + x^2 + x^6 \end{array}\right.$$

Therefore,

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

□ Syndrome of a Cyclic Code

Received polynomial: $r(x) = c(x) + e(x)$

$$(\underbrace{c_0\ c_1 \cdots c_{n-k-1}}_{\text{Parity check}} \vdots \underbrace{c_{n-k} \cdots c_{n-1}}_{\text{Information}})$$

$p(x)$

$$c_{n-k}x^{n-k} + \cdots + c_{n-1}x^{n-1} = x^{n-k}(c_{n-k} + \cdots + c_{n-1}x^{k-1}) = x^{n-k}m(x)$$

$$r(x) = \underbrace{m(x)x^{n-k} + p(x)}_{c(x)} + \underbrace{e_m(x)x^{n-k}}_{\text{Error pattern in the information bits}} + \underbrace{e_p(x)}_{\text{Errors in the parity bits}}$$

$$= \underbrace{[m(x) + e_m(x)]}_{\text{Received information}}x^{n-k} + \underbrace{p(x) + e_p(x)}_{\text{Received parity bits}}$$

$$r(x) \bmod g(x) = (\underbrace{[m(x) + e_m(x)] \bmod g(x)}_{\text{Parity bits recalculated from the received information}}) + \underbrace{p(x) + e_p(x)}_{\text{Received parity bits}}$$

$$= \text{Syndrome} = s(x)$$

Example: Cyclic code generated by $g(x) = 1 + x + x^3$

Received sequence $\underline{r} = (1\ 0\ 1\ 0\ 1\ 1\ 0)$,

$r(x) = 1 + x^2 + x^4 + x^5$.

$$
\begin{array}{r}
0111 \\
\hline
1011 \;\big|\; 0110101 \\
\quad 1011 \\
\hline
\quad\; 1100 \\
\quad\; 1011 \\
\hline
\quad\;\; 1111 \\
\quad\;\; 1011 \\
\hline
\quad\;\;\; 100
\end{array}
$$

syndrome $s(x) = x^2$

□ Implementation of Encoder

Generator polynomial

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

Message polynomial

$$m(x) = m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}$$

○ Systematic encoding

$$R(x) = \text{Rem}\left\{ \frac{m(x)x^{n-k}}{g(x)} \right\} = p_0 + p_1 x + \cdots + p_{n-k-1} x^{n-k-1}$$

$$m(x)x^{n-k} = g(x)q(x) + p(x)$$

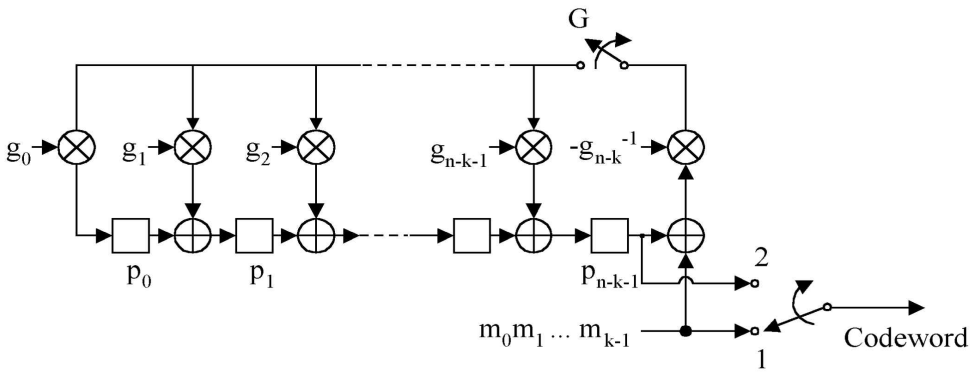
where $p(x)$ is the remainder polynomial or "check polynomial"

Code polynomial

$$c(x) = m(x)x^{n-k} + p(x) \qquad (= q(x) \cdot g(x))$$

$$\leftrightarrow \quad \underline{c} = (p_0, p_1, p_2, \cdots, p_{n-k-1}, m_0, m_1, \cdots, m_{k-1})$$

○ Systematic encoder using division circuit ($g(x)$)



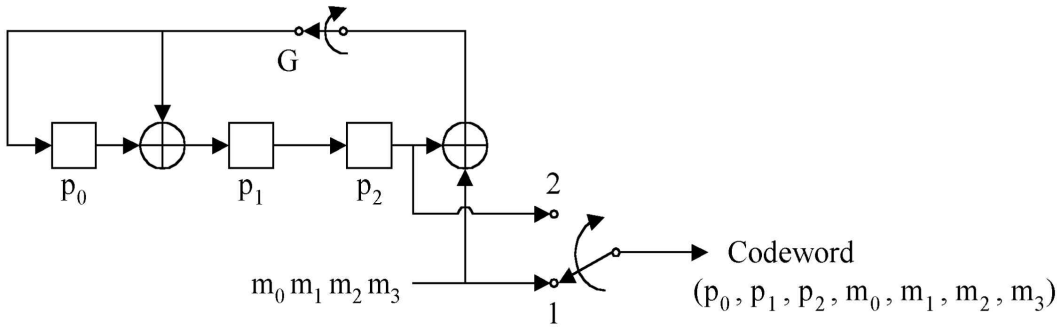
(a) Clock $1 \sim k$:

G: closed, S: position 1 $\Rightarrow$ output: $m_0\, m_1 \cdots m_{k-1}$

(b) Clock $k+1 \sim n$:

G: open, S: position 2 $\Rightarrow$ output: $p_0\, p_1 \cdots p_{n-k-1}$

Example: [7,4] cyclic code generated by $g(x) = x^3 + x + 1$



○ Systematic encoder based on the check polynomial $h(x)$

Check polynomial: $h(x) = h_0 + h_1 x + \cdots + h_k x^k ; \quad (h_k = 1)$

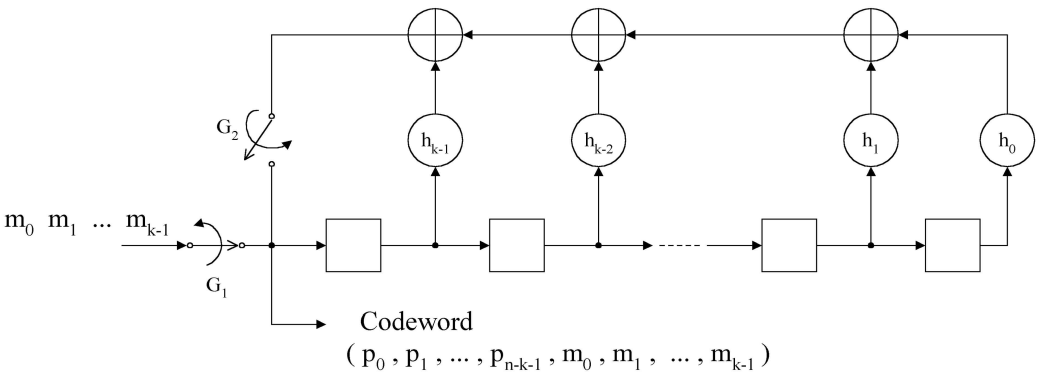
Code polynomial: $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

Relation between $c(x)$ and $h(x)$:

$$c(x)h(x) = 0 \ (\text{mod} \ x^n - 1)$$

$$0 = \sum_{j=0}^{k} h_j c_{n-i-j} \qquad 1 \leqq i \leqq n-k$$

$$\Rightarrow \quad c_{n-k-i} = \sum_{j=0}^{k-1} h_j c_{n-i-j} \qquad 1 \leqq i \leqq n-k$$



(a) Clock $1 \sim k$:

G_1: closed, G_2: open $\Rightarrow$ output: $m_0 \, m_1 \cdots m_{k-1}$

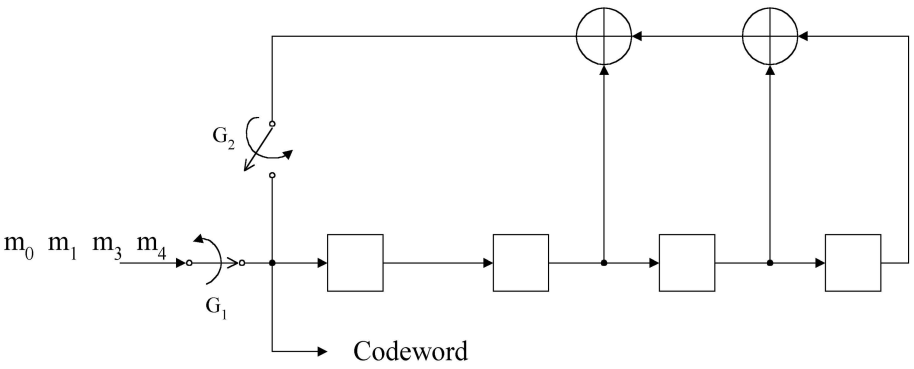
(b) Clock $n-k \sim n$:

G_1: open, G_2: closed $\Rightarrow$ output: $p_0 \, p_1 \cdots p_{n-k-1}$

Example: [7,4] cyclic code generated by $g(x) = x^3 + x + 1$

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

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



□ Implementation of Decoder

○ Decoding procedure

(a) Calculation of syndrome $s(x) = \text{Rem}\left\{\frac{r(x)}{g(x)}\right\}$

(b) Determination of error pattern $e(x)$ from $s(x)$.

It is not possible to use look-up table, when $n-k$ is large.

(c) Error correction:

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

○ Syndrome calculation

(a) Received polynomial

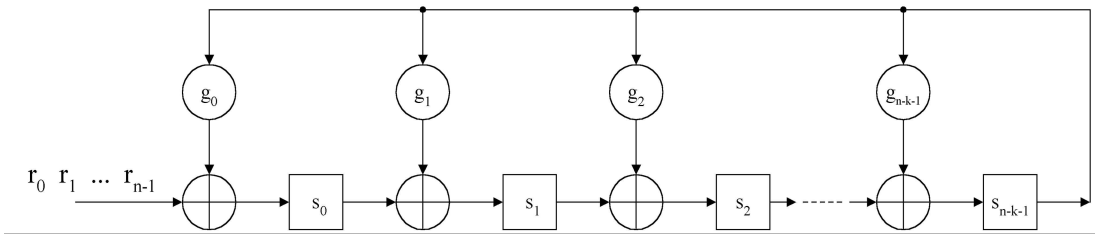
$$r(x) = c(x) + e(x)$$
$$= r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1}$$

(b) Syndrome polynomial

$$s(x) = \text{remainder of } r(x) \text{ divided by } g(x)$$
$$= \text{Rem}\left\{\frac{r(x)}{g(x)}\right\}$$
$$= \text{Rem}\left\{\frac{e(x)}{g(x)}\right\}$$
$$= s_0 + s_1 x + \cdots + s_{n-k-1} x^{n-k-1}$$

If $g(x) | e(x)$, undetectable errors occur.
($\because$ $e(x)$ is a codeword)

○ Syndrome generator using division circuit



Theorem: Let

$r^{(1)}(x)$ = cyclic shift of $r(x)$,

$s^{(1)}(x)$ = syndrome corresponding to $r^{(1)}(x)$.

Then we have $s^{(1)}(x) = x \cdot s(x) \mod g(x)$.

Proof:

$$r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} = q(x)g(x) + s(x)$$

$$r^{(1)}(x) = xr(x) + r_{n-1}(x^n + 1)$$

$$= xq(x)g(x) + r_{n-1}(x^n + 1) + xs(x)$$

$$\Rightarrow \quad s^{(1)}(x) = r^{(1)}(x) \mod g(x) = xs(x) \mod g(x)$$

since $g(x) | x^n + 1$ □□

Note:

Syndrome of $r^{(i)}(x)$ is the remainder of $x^i s(x)$ divided by $g(x)$

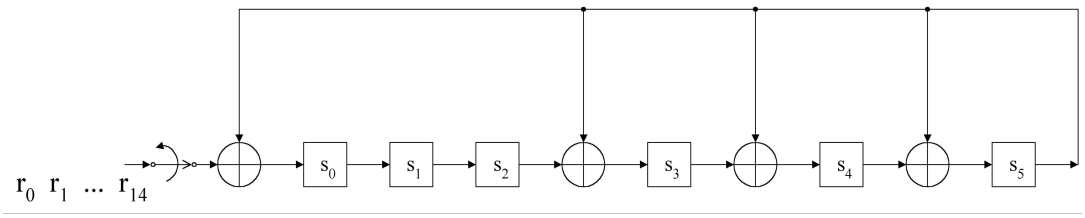
$$s^{(i)}(x) = \text{Rem}\left\{\frac{x^i s(x)}{g(x)}\right\}$$

○ Syndrome calculation of $r^{(i)}(x)$

$g(x) = x^6 + x^5 + x^4 + x^3 + 1$ clock $1 \sim 15$: S is closed

$\Rightarrow [15, 9]$ cyclic code, clock i times : S is open

$\Rightarrow$ Content $= s^{(i)}(x)$



○ Meggit decoder

(a) Choose specific error patterns.

(b) Shift syndromes in the division circuit until we detect the appropriate syndromes.

(c) Use the # of shifts to determine the original location of the errors.

□ Examples of Cyclic Codes

○ Hamming codes

$$n = 2^m - 1 \ , \ k = n - m \ , \ d = 3$$

$$g(x) = \text{primitive polynomial of degree } m$$

$$h(x) = (x^n + 1)/g(x) : \text{check polynomial}$$

$$\deg\ h(x) = 2^m - 1 - m$$

○ Simplex codes

Dual code of Hamming code

$$n = 2^m - 1 \ , \ k^{\perp} = m \ , \ d = 2^{m-1}$$

$$g^{\perp}(x) = h^*(x) = h_k + h_{k-1}x + \cdots + h_1 x^{k-1} + h_0 x^k$$

$$h^{\perp}(x) = g^*(x) = (x^n + 1)/h^*(x)$$

Example: $m = 3$

(a) [7,4] Hamming code

$$g(x) = x^3 + x + 1, \qquad h(x) = x^4 + x^2 + x + 1$$

(b) [7,3] Simplex code

$$g^{\perp}(x) = x^4 + x^3 + x^2 + 1 = h^*(x)$$

$$h^{\perp}(x) = x^3 + x^2 + 1 = g^*(x)$$

$$G^{\perp} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$C = \{(0000000), (1011100), (0101110), (0010111),$$
$$(1001011), (1100101), (1110010), (0111001)\}$$

○ Golay codes

[23,12,7]: $t = 3$ "triple-error-correcting code"

$$x^{23} + 1 = (x + 1) g_1(x) g_2(x)$$

$$g_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

$$g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} = g_1^*(x)$$

$g_1(x)$ or $g_2(x)$ may be used as a generator polynomial of Golay code.

Note: [24,12,8] extended Golay code

$$H_E = \left[\begin{array}{ccc|c} & H & & \begin{matrix}0\\0\\\vdots\\0\end{matrix} \\ \hline 1 & 1 \cdots\cdots & 1 & 1 \end{array}\right] \quad (12 \times 24) \text{ matrix}$$

$$\text{Rate} = \frac{12}{24} = \frac{1}{2}$$

○ Shortened cyclic codes

$$[n, k] \rightarrow [n-i, k-i]$$

$\Rightarrow$ Not cyclic codes

○ Expurgated cyclic codes

$(x+1) \nmid g(x)$

New code: $g_1(x) = (x+1)\, g(x)$

$\Rightarrow$ Every codeword has even weight.

□ Cyclic Redundancy Check (CRC)

○ Data $\underline{D} = (d_0, d_1, d_2, \cdots, d_{k-2}, d_{k-1})$, k: data length

○ Parity bit p is added.

$$\underline{D}' = (p, d_0, d_1, d_2, \cdots, d_{k-2}, d_{k-1})$$

such that $\left(\sum_{i=0}^{k-1} d_i + p \right) \bmod 2 = 0$

$\Downarrow$

Received data $\begin{cases} \text{even parity} \sim \text{no error or undetectable} \\ \text{odd parity} \sim \text{errors} \end{cases}$

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

$$D(x) = d_0 + d_1 x^1 + d_2 x^2 + \cdots + d_{k-2} x^{k-2} + d_{k-1} x^{k-1}$$

$$xD(x) = q(x)g(x) + p(x)$$

$$\deg\ p(x) = 0 \quad \Rightarrow \quad p(x) = p$$

Therefore, $xD(x)+p(x) = q(x)g(x)$

$$p+ d_0x+ d_1x^2+ d_2x^3+\cdots+ d_{k-2}x^{k-1}+ d_{k-1}x^k= q(x)g(x)$$

$$g(x)|(xD(x)+p(x))$$

Therefore, $(xD(x)+p(x))|_{x=1} = 0$: single error detectable

○ Generator polynomial

$$g(x) = g_0+ g_1x+\cdots+ g_{m-1}x^{m-1}+ g_mx^m$$

○ Data polynomial

$$D(x) = d_0+ d_1x+ d_2x^2+\cdots+ d_{k-2}x^{k-2}+ d_{k-1}x^{k-1}$$

$$x^mD(x)=q(x)g(x)+p(x)$$

where $q(x)$: quotient polynomial

$p(x)$: remainder polynomial

$\deg p(x) \le m-1$

Therefore, $p(x) = p_0+ p_1x+ p_2x^2+\cdots+ p_{m-2}x^{m-2}+ p_{m-1}x^{m-1}$

$$x^mD(x)+p(x) = q(x)g(x)$$

$$p_0+ p_1x+\cdots+ p_{m-1}x^{m-1}+ d_0x^m+ d_1x^{m+1}+\cdots+ d_{k-1}x^{m+k-1} = q(x)g(x)$$

Codeword: $\underline{c} = (p_0, p_1, p_2, \cdots, p_{m-1}, d_0, d_1, d_2, \cdots, d_{k-2}, d_{k-1})$

How many errors can we detect ?

$$\begin{cases} k & : \text{data length} \\ k+m & : \text{record length} \end{cases}$$

○ Period of polynomial $g(x)$

The least positive integer e such that x^e+1 is divisible by $g(x)$

○ Recieved polynomial

$$r(x) = c(x) + e(x) = (r_0, r_1, \cdots, r_{k+m-1})$$

Theorem: All single bit error can be detected by any code whose generator polynomial has more than one term. ($g(x) = x^c + 1$)

Theorem: All cases of an odd number of bits in error can be detected by a code whose generator polynomial has $x^c + 1$, $c > 0$.

Theorem: A code will detect all single- and double-bit errors if the record length is no greater than the period of the generator polynomial.

Theorem: A code will detect all single-, double-, and tripple-errors if its generator polynomial is of the form $(x^c+1)\cdot a(x)$ and the record length is no greater than the period of $g(x)$.

Theorem: A code generated by a polynomial of degree m detects all single burst errors of length no greater than m.

(Burst of length b: 1 ····· 1)

error b bits error

Theorem: A code with generator polynomial of the form $(x^c+1)\cdot a(x)$ has a guaranteed double burst detection capability provided the record length is no greater than the period of the generator polynomial. It will detect any combination of double bursts when the length of shorter burst is no greater than the degree of $a(x)$, and the sum of the burst length is no greater than $c+1$.

Example: Generator polynomial of CRC-CCITT code

$$g(x) = x^{16}+x^{12}+x^5+1$$
$$= (x+1)(x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1)$$

Period of $g(x) = 32767$.

○ Guaranteed error detection capability:

(a) All odd number of errors.

(b) All single, double, and tripple-bit errors if record length is ≤ 32767.

(c) All single burst errors of 16 bit, or less.

(d) Detect 99.99695% of all possible bursts of length 17, and 99.99847% of all possible longer burst.

If an error polynomial $e(x)$ is not divisible by $g(x)$, then $e(x)$ can be detected.