5-3 Polynomial Modulo Arithmetic

$P(X) = X^n - 1$

This polynomial $[P(X)]$ plays a key role in the theory of cyclic codes. To see this, consider a codeword polynomial

$$C(X) = C_0 + C_1 X + \cdots + C_{n-1} X^{n-1}$$

one cyclic shift $\Rightarrow$ $C'(X) = C_{n-1} + C_0 X + \cdots + C_{n-2} X^{n-1}$

we can write $C'(X)$ as

$$C'(X) = XC(X) - C_{n-1} X^n + C_{n-1}$$

$$= XC(X) - C_{n-1}(X^n - 1)$$

$$\Rightarrow C'(X) = XC(X) \bmod (X^n - 1)$$

The expression $XC(X)$ modulo $(X^n - 1)$

$$\equiv XC(X) \bmod (X^n - 1) \equiv XC(X) / (X^n - 1)$$

- The modulo operation a mod b is the remainder that results from dividing integer a by integer b.

The same thing in polynomials.

we find the remainder by long division.

$$X^n - 1 \;\Big|\; C_{n-1} X^n + C_{n-2} X^{n-1} + \cdots + C_0 X$$

$$C_{n-1} X^n - C_{n-1}$$

remainder when its degree $< n$ $\Rightarrow$ $C_{n-2} X^{n-1} + C_{n-3} X^{n-2} + \cdots + C_0 X + C_{n-1} \equiv C'(X)$

$\therefore$ a cyclic shift of $C(X)$ is equivalent to $XC(X) \bmod (X^n - 1)$

Ring

— The modulo operation creates a mathematical structure called a ring. [See page 165 for more details]

— We denote it as $GF(2)[X]/P(X)$

$\Rightarrow$ (1) scalars are from $GF(2)$
(2) "$[X]$" denotes polynomials
(3) "$/P(X)$" $\Rightarrow$ polynomials are modulo $P(x)$,

note that this is not only division, this is modulo operation [remainder of dividing polynomials by $P(x)$].

— Consider a polynomial ring $GF(2)[X]/(X^n-1)$

Since we are in $GF(2)$,

$\Rightarrow X^n-1 = X^n+1$ $\Rightarrow$ can be factored into lower degree polynomial

For example, $X^7+1 = (X+1)(X^3+X+1)(X^3+X^2+1)$

Irreducible polynomial

A polynomial that can't be factored into lower degree polynomials.

For example, $(X+1)$, (X^3+X+1) and (X^3+X^2+1)

Generator Polynomial

Our cyclic code generator polynomial will be constructed from the factors of X^n+1.

$\Rightarrow g(x)\,h(x) = X^n+1$ $\Rightarrow$ $g(x)$ divides (X^n+1).

- we say that $g(x)$ divides $f(x)$ if $f(x) \bmod g(x) = 0$

In general, $f(x) = Q(x)g(x) + \rho(x)$

, where $\deg[\rho(x)] < \deg[g(x)]$

$Q(x) \Rightarrow$ quotient

$\rho(x) \Rightarrow$ remainder

we use the notation

$\rho(x) = f(x)/g(x)$ = remainder of dividing $f(x)$ by $g(x)$.

Identities

Let $f_1(x) = Q_1(x)g(x) + \rho_1(x)$

$f_2(x) = Q_2(x)g(x) + \rho_2(x)$

$\Rightarrow [f_1(x) + f_2(x)]/g(x) = \rho_1(x) + \rho_2(x)$

Also, $[f_1(x) \cdot f_2(x)]/g(x) = [\rho_1(x) \cdot \rho_2(x)]/g(x)$

Example $f(x) = x^6$ and $g(x) = 1 + x + x^3$

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

$\therefore$

$$f(x) = \underbrace{(x^3 + x + 1)}_{Q(x)}\underbrace{(x^3 + x + 1)}_{g(x)} + \underbrace{x^2 + 1}_{\rho(x)}$$

Example 5.3.2

The ring $GF(2)[X]/(X^7-1)$ contains $2^n = 2^7$ distinct polynomials. In order to find the remainder for any polynomial, we can find the remainder for the terms $\{X^j; j=1,\cdots,n-1\}$ and then add them. For example, For $n=7$, we can construct the following table,

X^j	$\rho(X)$
X^6	$1+X^2$
X^5	$1+X+X^2$
X^4	$X+X^2$
X^3	$1+X$
X^2	X^2
X	X
1	1

for $g(X) = 1+X+X^3$

$\rho(X) = X^j / g(X)$

For any polynomial $f(X)$, we can use the superposition Principle to find the remainder $\rho(X) = f(X)/g(X)$.

for example, $f(X) = 1+X^3+X^5+X^6$

$\Rightarrow \rho(X) = 1+1+X+1+X+X^2+1+X^2$

$= 0$

$\Rightarrow$ $g(X)$ divides $f(X)$.

Lemma $(1+X)$ is always a factor of X^n+1 for any $n>0$ in $GF(2)[X]/(X^n-1)$

Meggitt's Theorem Let $g(X)h(X) = X^n-1$ and $v(X)/g(X) = \rho(X)$. then $[X v(X) \bmod (X^n-1)]/g(X) = [X\rho(X)]/g(X)$

5.4 Generation and Decoding of Cyclic Codes

Generation

The (n,k) cyclic codeword can be generated by

$$c(X) = m(X)\,g(X)$$

where $m(X)$ is the message polynomial
$g(X)$ is the generator polynomial

- Also, $\deg[g(X)] = r = n-k$
  $\deg[m(X)] \leq k-1$

- The code polynomials are elements of the ring
  $GF[2][X]/(X^n-1)$

Also, the generator polynomial $g(X)$ must divide X^n-1,

So, $X^n-1 = X^n+1 = h(X)g(X)$

where $h(X)$ is called the parity check polynomial.

$$\Rightarrow c(X)\,h(X)/(X^n-1) = 0$$

($c(X)$: valid codeword)

Decoding

At the receiver,

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

, where $e(X)$ is the error polynomial.

the syndrome polynomial will be

$$S(X) = v(X)h(X)/(X^n-1) = c(X)h(X)/(X^n-1) + e(X)h(X)/(X^n-1)$$

$$= e(X)h(X)/(X^n-1)$$

§5.4.2 Systematic Cyclic Codes

systematic code

In polynomial form, a systematic code word is

$$\underline{c} = [c_0 c_1 c_2 \cdots c_{r-1} m_0 m_1 \cdots m_{k-1}]$$

$$\Rightarrow c(x) = x^r m(x) - d(x) = x^r m(x) + d(x)$$

Since $c(x) = m(x)g(x) \Rightarrow x^r m(x) = m(x)g(x) + x^r m(x)$

$$\Rightarrow d(x) \equiv \text{remainder} = x^r m(x)/g(x)$$

The syndrom polynomial is defined as

$$S(x) = c(x)/g(x) = x^r m(x)/g(x) + d(x)/g(x)$$
$$= d(x) + d(x) = 0$$

$$d(x)/g(x) = d(x) \text{ since } \deg\{d(x)\} \leq r-1$$

Theorem 5.4.1 A linear (n,k) code defined by a generator polynomial $g(x)$ is a cyclic code if and only if $g(x)h(x) = x^n - 1$.

$\Rightarrow$ "$g(x)$ divides $x^n - 1$"

Also, $g(x)$ must be of degree $r = n-k$

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

These coefficients must be one.

Example 5.4.1

Construct a Systematic (7,4) cyclic Code.
$k=4$, $n=7$ and $r=3$.

- we start by factorizing X^7+1.

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

- The generator polynomial must be of degree $r=3$ and a factor of X^7+1.

Thus, Let $g(X)=X^3+X+1$

- The systematic cycle code is in this Form

$$c(X)=X^r m(X)+d(X)$$
$$c(X)=X^r m(X)+X^r m(X)/g(X)$$

Since $k=4 \Rightarrow m(X)=m_0+m_1X+m_2X^2+m_3X^3$

$$\Rightarrow c(X)=X^3[m_0+m_1X+m_2X^2+m_3X^3]+X^3[m_0+m_1X+m_2X^2+m_3X^3]/g(X)$$

$$\Rightarrow c(X)=[m_0X^3+m_1X^4+m_2X^5+m_3X^6]+[m_0X^3+m_1X^4+m_1X^5+m_3X^6]/g(X)$$

Lets First find the remainders for $g(X)$ for the terms X^3, X^4, X^5 and X^6

$$\begin{array}{r} 1 \\ X^3+X+1 \overline{)\ X^3} \\ X^3+X+1 \\ \hline X+1 \end{array} \Rightarrow X^3/g(X)=X+1$$

$$\begin{array}{r} X \\ X^3+X+1 \overline{)\ X^4} \\ X^4+X^2+X \\ \hline X^2+X \end{array} \Rightarrow X^4/g(X)=X^2+X$$

$$\begin{array}{r} X^2+1 \\ X^3+X+1 \overline{)\ X^5} \\ X^5+X^3+X^2 \\ \hline X^3+X^2 \\ X^3+X+1 \\ \hline X^2+X+1 \end{array} \Rightarrow X^5/g(X)=X^2+X+1$$

$$\begin{array}{r} X^3+X+1 \\ X^3+X+1 \overline{)\ X^6} \\ X^6+X^4+X^3 \\ \hline X^4+X^3 \\ X^4+X^2+X \\ \hline X^3+X^2+X \\ X^3+X+1 \\ \hline X^2+1 \end{array} \Rightarrow X^6/g(X)=X^2+1$$

	$P(X)$
X^6	X^2+1
X^5	X^2+X+1
X^4	X^2+X
X^3	$X+1$

Since $k=4 \Rightarrow$ we have $2^4 = 16$ codewords.
the code table is as follows:

$m(X)$	$C(X)$	$m(X)$	$C(X)$
0	0	X^3	$1+X^2+X^6$
1	$1+X+X^3$	$1+X^3$	$X+X^2+X^3+X^6$
X	$X+X^2+X^4$	$X+X^3$	$1+X+X^4+X^6$
$1+X$	$1+X^2+X^3+X^4$	$1+X+X^3$	$X^3+X^4+X^6$
X^2	$1+X+X^2+X^5$	X^2+X^3	$X+X^5+X^6$
$1+X^2$	$X^2+X^3+X^5$	$1+X^2+X^3$	$1+X^3+X^5+X^6$
$X+X^2$	$1+X^4+X^5$	$X+X^2+X^3$	$X^2+X^4+X^5+X^6$
$1+X+X^2$	$X+X^3+X^4+X^5$	$1+X+X^2+X^3$	$1+X+X^2+X^3+X^4+X^5+X^6$

By inspection, this code is a cyclic code. The minimum hamming distance (d_{min}) is $=3$.
To get the generator matrix G, its rows will be selected by the message words of weight one

$[1000]$, $[0100]$, $[0010]$, and $[0001]$
1, X, X^2, X^3

$$\Rightarrow G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \rightarrow 1+X+X^3 \\ \rightarrow X+X^2+X^4 \\ \rightarrow 1+X+X^2+X^5 \\ \rightarrow 1+X^2+X^6 \end{matrix}$$

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

$\Rightarrow$ This is a Hamming code.

§.4.3 Hardware implementation for systematic cyclic codes.

$$C(X) = X^r m(X) + d(X)$$

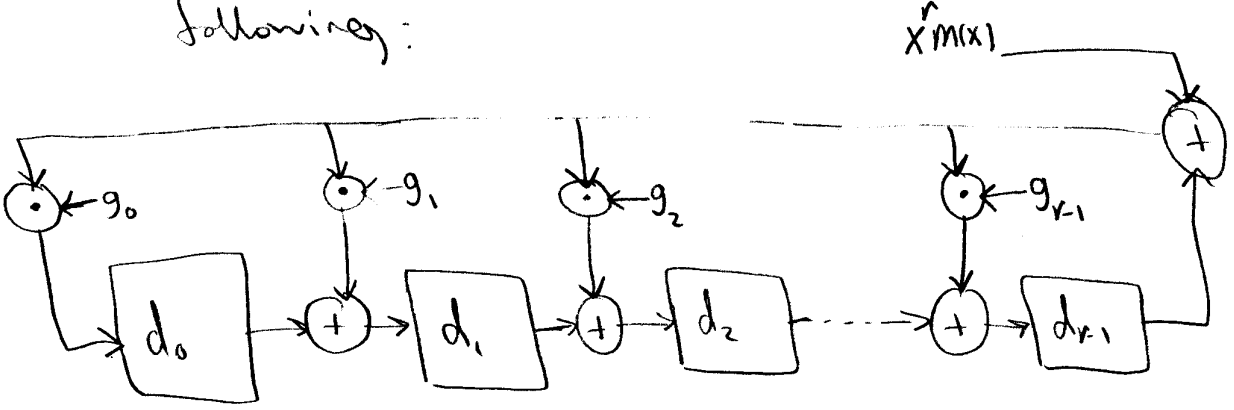
where $m(X) = m_0 + m_1 X + \cdots + m_{k-1} X^{k-1}$

$d(X) = d_0 + d_1 X + \cdots + d_{r-1} X^{r-1}$; where $r = n-k$

recall that $d(X) = X^r m(X) / g(X)$

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

the divide by $g(X)$ circuit consists of the following:

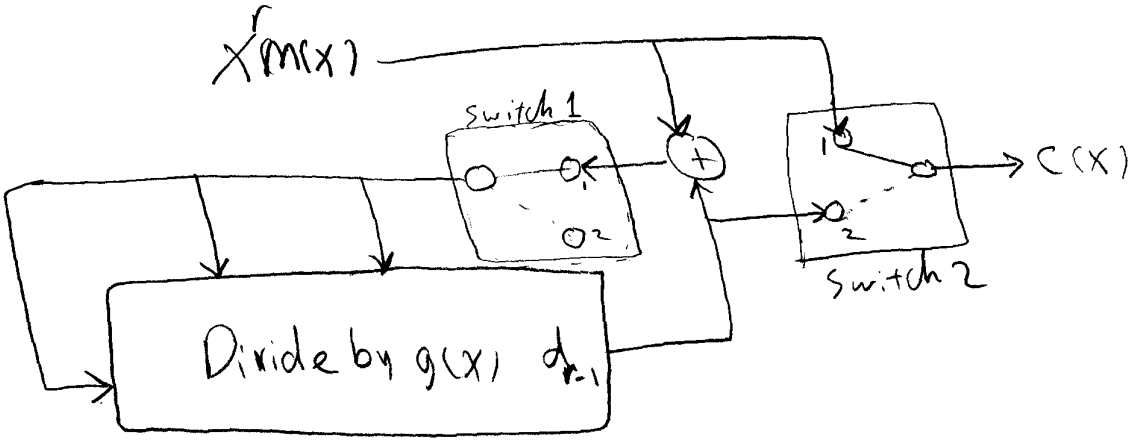


where ⊕ is X-OR addition

⊙ is AND multiplication

After k shifts, the contents of the shift register contain $d(X) = d_0 + d_1 X + \cdots + d_{r-1} X^{r-1}$

The systematic encoder will be in this form



The operation of the above circuit is as follows:
Initially, the switches are set in the above position for the first k cycles of operation, while the message $x^r m(x)$ is shifted in serially.
Then, the switches are set to the second position for the remaining $n-k=r$ cycles. This breaks the feedback action of the divide circuit and shifts the remainder out of the shift register, appending it as $d(x)$ to the transmitted codeword.
The shift register is initialized to zero at the start of each block.

5.4.4 Hardware implementation & Decoders for Cyclic Codes

Similar to block codes, we first find the syndrome, then look it up in a table and find the corresponding error pattern.

The receiver receives

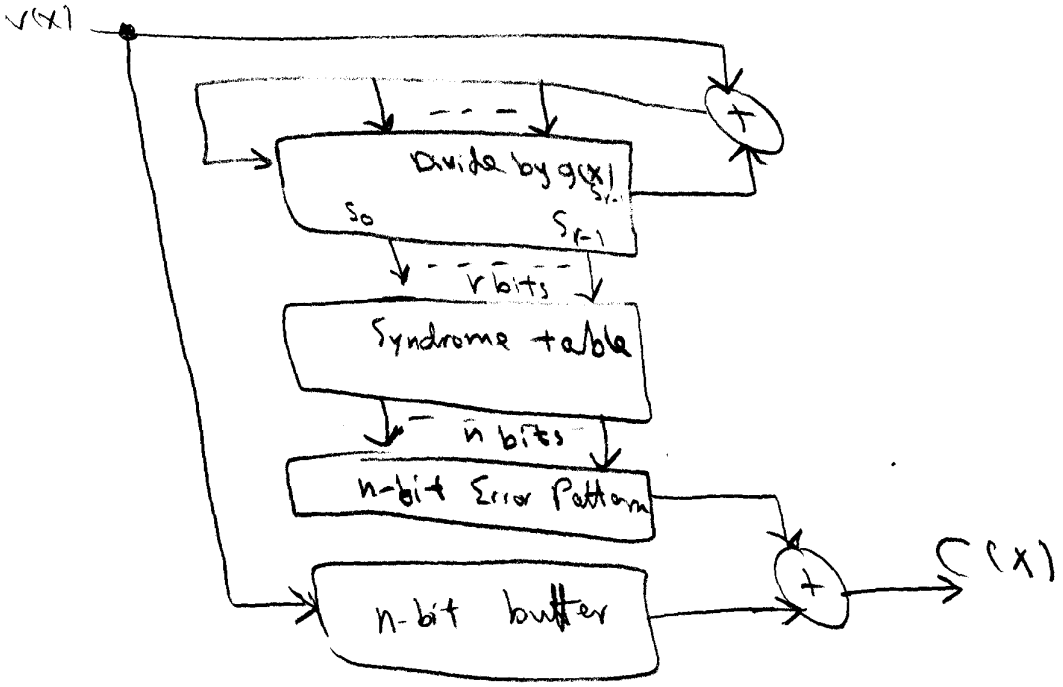
$$v(X) = c(X) + e(X)$$

where $c(X)$ is the codeword
$e(X)$ is the error

The syndrome is given by,

$$S(X) = X^r v(X)/g(X)$$

The decoder can be implemented as follows:



5.6 Some standard Cyclic Block codes.

We specify cyclic codes by means of the generator polynomial $g(X)$ in octal Form.

For example,

$$g(X) = X^4 + X + 1$$

$$\Rightarrow \bar{g} = [\underbrace{1\,0}_{2}\ \underbrace{0\,1\,1}_{3}]$$

$$= (23)_8 \leftarrow \text{base 8 octal Form.}$$

(1) Hamming Codes

- Single error correcting codes
- $d_{min} = 3$

$n = 2^r - 1$, $r \geq 3$

table 5.6.1

n	k	t	$g(X)$ octal
7	4	1	13
15	11	1	23
31	26	1	45
63	57	1	103
⋮			

see the table in Page 185.

(2) BCH codes

- BCH codes can be designed to correct any number of errors.
- Decoding complexity grows with the number of errors t that the code can correct.

- $n = 2^j - 1$, $j \geq 3$

Table 5.6-2 BCH codes

n	k	t	$g(x)$ (octal)
15	7	2	721
15	5	3	2467
31	21	2	3551
31	16	3	10767
⋮			

see the table in page 185

(3) Burst-Correcting Codes

An error is called a burst error if it happens for a group of bits following each other. There is a high correlation in the error between the bits.

Example, A defect on a disk will destroy a string of bits rather than an individual bit.

⇒ A burst of length b ⇒ b consecutive bits are in error.

The minimum possible number of parity-bits required to correct a burst of length b or less is

$$r \geq 2b.$$

Table 5.6-3 Good Burst-Correcting Codes

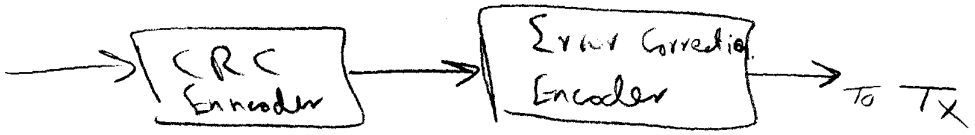
n	k	b	$g(X)$ (octal)
7	3	2	35
15	10	2	65
15	9	3	171

* Another way to design burst correcting codes is by interleaving. "As we will see later".

see the table in page 5.6-3

(4) Cyclic Redundancy Check Codes [CRC]

- CRC are error detecting codes usually used in automatic repeat request (ARQ).
- There is no error correction in CRC.
- The decoder will compute the syndrome.
  - if $\bar{S} = 0 \Rightarrow$ No error and the Packet is correct.
  - if $\bar{S} \neq 0 \Rightarrow$ declare error and ask for Retransmission.
- It could be concatenated with an error correcting code as follows:



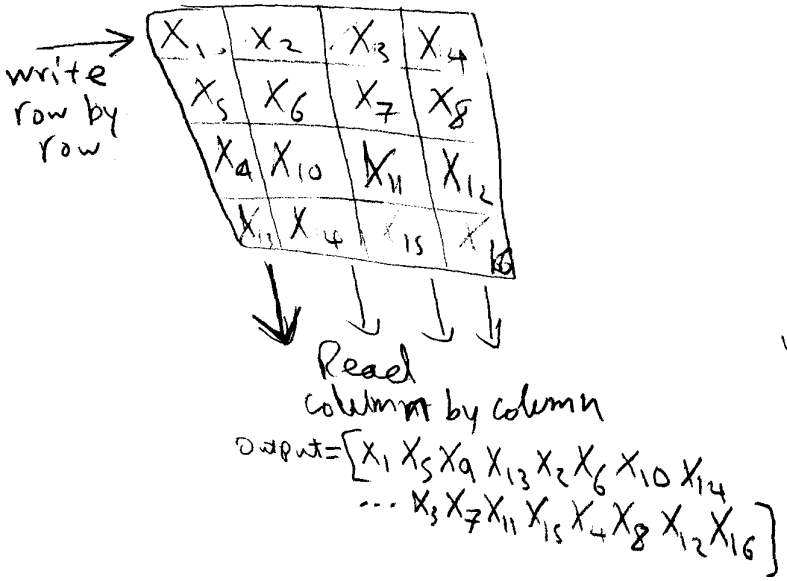
Interleavers

Interleavers can be used to break up a burst of errors. That mean, they can seperate the errors and break up the correlation.

Example Block interleaver

4X4 Bolock interleaver

Interleaver



Deinterleaver