CS & IT ENGINEERING

COMPUTER NETWORKS

Error Control

Lecture No- 04

By- Ankit Doyla Sir

TOPICS TO BE COVERED

- CRC

Cyclic Code

Cyclic Code

Cyclic code :

- Cyclic code are special Linear Block codes with one extra property.
- In Cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

Suppose, C is a Code Word given as

$$C = [C_1, C_2, C_3 \ldots\ldots C_{n-1}]$$

Then after cyclic shifts

Right Shift

$$C = [C_1, C_2, C_3 \ldots\ldots C_{n-1}]$$

$$C^0 = [C_{n-1}, C_1, C_2 \ldots\ldots C_{n-2}]$$

$$C^1 = [C_{n-2}, C_{n-1}, C_1\ C_2, \ldots\ldots C_{n-3}]$$

Or

$C_1\ C_2\ C_3\ C_4$

$C_4\ C_1\ C_2\ C_3$

$C_1 C_2 C_3 C_4$

$C_4\ C_1 C_2 C_3$

Left Shift

$$C = [C_1, C_2, C_3 \ldots\ldots C_{n-1}]$$

$$C^0 = [C_2, C_3 \ldots\ldots C_{n-1,} C_1]$$

Or

$C_1\ C_2\ C_3\ C_4$

$C_2\ C_3\ C_4\ C_1$

OR

$C_1 C_2 C_3 C_4$

$C_2 C_3 C_4 C_1$

Linear Block codes :

- A Linear block code is a code in which the XOR (⊕) of two valid code words create another valid code word.
- Today all most all error detecting codes are linear block codes: Non Liner block codes are difficult to implement.
- It is simple to find the minimum Hamming distance for linear block code the minimum Hamming distance is the number of 1's in a Non zero valid code word with the smallest Number of 1's

Ex1 :

~~Valid~~ code word

(a) 0 0 0

(b) 0 1 1

(c) 1 0 1

(d) 1 1 0

Linear Block code

XOR (a, b) = 011 (valid code word)

XOR (a, c) = 101 (valid code word)

XOR (a, d) = 110 (valid code word)

XOR (b, c) = 110 (valid code word)

XOR (b, d) = 101 (valid code word)

XOR (c, d) = 011 (valid code word)

So above code word is Liner block code.

Min Hamming distance = 2 (min. no. of 1's in the non zero code word)

Cyclic Code

Ex :

Valid code word

(a) 0 0 0

(b) 0 1 1

(c) 1 0 1

(d) 1 1 0

Right shift			Left shift
0 1 1	OR	0 1 1	0 1 1
1 0 1		1 0 1	1 1 0
1 1 0		1 1 0	1 0 1
0 1 1		0 1 1	0 1 1

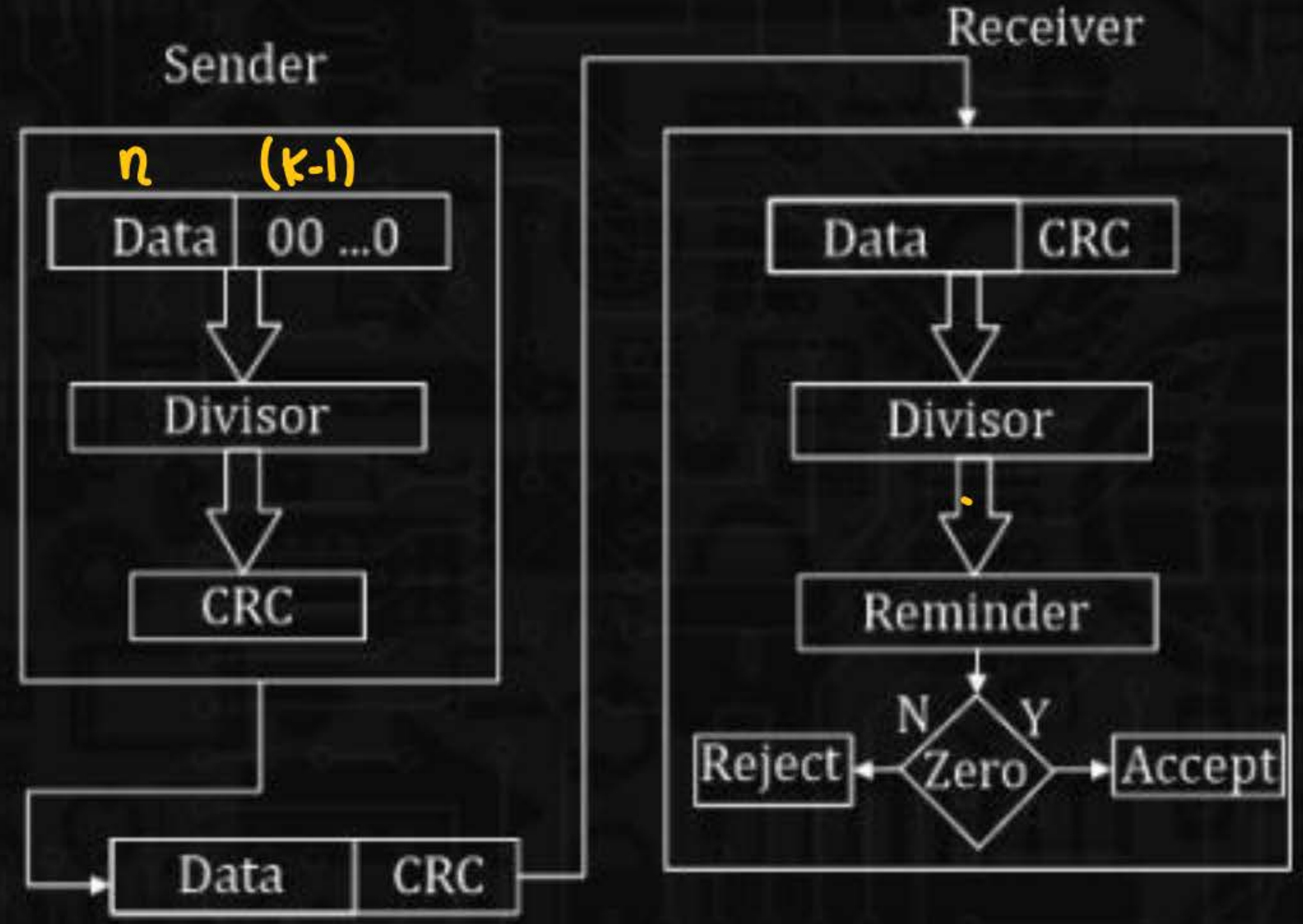
Introduction
To
CRC

Introduction to CRC :

- Length of the dataword=n
- Length of the divisor=k
- Append (k-1) Zero's to the original message
- Perform modulo 2 division
- Remainder of division = CRC
- Code word =n+k-1 (bit)

Note: CRC must be (k-1) bits

- Codeword = dataword with appended (k-1) Zeros+ CRC


Sender
n
(k-1)
Data
00 ...0
Divisor
CRC
Data
CRC
Receiver
Data
CRC
Divisor
Reminder
N
Y
Reject
Zero
Accept

① Data=1001001 (n=7)

msg or

Divisor or CRC generator=1101 (K=4)

Sender

```
1101 ) 1001001000
       1101
       ----------
       0100001000
        1101
        ---------
        010101000
         1101
         --------
         01111000
          1101
          -------
          0010000
            1101
            -----
            01010
             1101
             ----
             0111
```

111 ← CRC OR Remainder

Codeword = 1001001 111

Transmitted data = 1001001 111

Codeword = 1001001000
+111

1001001111

Codeword = n+k-1

7+4-1 = 10 bit

IF Receiver Received uncorrupted data

Receiver

```
1101 ) 1001001111
       1101
       ----------
       0100001111
        1101
        ---------
        010101111
         1101
         --------
         01111111
          1101
          -------
          0010111
            1101
            -----
            1101
            1101
            ----
            0000   syndrom = 0
```

Dataword Accepted = (1001001)

If Receiver Received corrupted data

Receiver

```
1101 ) 1011001111 (
       1101
       ----------
       0110001111
        1101
        ---------
        000101111
            1101
            ------
            011011
             1101
             -----
             00001
```

syndrom $\neq 0$

dataword Rejected

Polynomial Notation In CRC

Polynomial Notation in CRC

- Data word=d(x)
- Codeword=c(x)
- Generator=g(x)
- Syndrome=s(x)
- Error=e(x)

Polynomial Notation in CRC

How to apply the CRC step by step :

1. Determine the degree ‘r’ of g(x) (highest power)

   $g(x) = x^6 + x^3 + 1$, $r = 6$

2. Determine $x^r d(x)$

3. Determine the remainder by dividing $x^r d(x)$ by $g(x)$

4. $\boxed{\text{Codeword} = x^r d(x) + \text{remainder}}$

ex: dataword $d(x) = 1001001$

a_6	a_5	a_4	a_3	a_2	a_1	a_0
1	0	0	1	0	0	1
x^6	x^5	x^4	x^3	x^2	x^1	x^0

$$1\cdot x^6 + 0\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 0\cdot x^2 + 0\cdot x^1 + 1\cdot x^0$$

$$d(x) = x^6 + x^3 + 1$$

Divisor OR generator $g(x) = 1101$

a_3	a_2	a_1	a_0
1	1	0	1
x^3	x^2	x^1	x^0

$$1\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 1\cdot x^0$$

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

(2) Determine $x^r \cdot d(x)$

$x^3(x^6+x^3+1)$

$x^9+x^6+x^3 \xrightarrow{\text{10bit}}$ $3 \to 1's$, $7 \to 0's$

$1\cdot x^9+0\cdot x^8+0\cdot x^7+1\cdot x^6+0\cdot x^5+0\cdot x^4+1\cdot x^3+0\cdot x^2$
$+0\cdot x^1+0\cdot x^0$

$\overbrace{1\,0\,0\,1\,0\,0\,1}^{\text{data}}\overbrace{0\,0\,0}^{(k-1)}$

(3) Determine the remainder by dividing $x^r \cdot d(x)$ by $g(x)$

Sender

$$
\begin{array}{l}
x^3+x^2+1 \,\big)\, \cancel{x^9}+\cancel{x^6}+x^3 \,\big(\, x^6+x^5+x^4+x^3+x+1 \\
\qquad\qquad\quad \cancel{x^9}+x^8+\cancel{x^6} \\
\hline
\qquad\qquad\qquad \cancel{x^8}+x^3 \\
\qquad\qquad\qquad \cancel{x^8}+x^7+x^5 \\
\hline
\qquad\qquad\qquad\quad \cancel{x^7}+x^5+x^3 \\
\qquad\qquad\qquad\quad \cancel{x^7}+x^6+x^4 \\
\hline
\qquad\qquad\qquad\qquad \cancel{x^6}+\cancel{x^5}+x^4+\cancel{x^3} \\
\qquad\qquad\qquad\qquad \cancel{x^6}+\cancel{x^5}+\cancel{x^3} \\
\hline
\qquad\qquad\qquad\qquad\quad \cancel{x^4} \\
\qquad\qquad\qquad\qquad\quad \cancel{x^4}+x^3+x \\
\hline
\qquad\qquad\qquad\qquad\qquad \cancel{x^3}+x \\
\qquad\qquad\qquad\qquad\qquad \cancel{x^3}+x^2+1 \\
\hline
\qquad\qquad\qquad\qquad\qquad\quad x^2+x+1
\end{array}
$$

$x^2+x+1 \rightarrow$ Remainder OR CRC

$CRC = x^2+x+1$

$= 1\cdot x^2+1\cdot x^1+1\cdot x^0$

$\boxed{CRC = 111}$

5. Codeword = $x^r \cdot d(x)$ + Remainder

$$x^9 + x^6 + x^3 + x^2 + x + 1$$

$$\downarrow$$

$$1 \cdot x^9 + 0 \cdot x^8 + 0 \cdot x^7 + 1 \cdot x^6 + 0 \cdot x^5 + 0 \cdot x^4 + 1 x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$$

$\boxed{\text{Codeword} = 1001001111}$

If Receiver Received uncorrupted data

Receiver

$$x^3+x^2+1 \,\big)\, x^9+x^6+x^3+x^2+x+1 \,\big(\, x^6+x^5+x^4+x^3+x+1$$

$$\cancel{x^9}+\cancel{x^6}+x^3+x^2+x+1$$
$$\cancel{x^9}+x^8+\cancel{x^6}$$
$$\overline{\cancel{x^8}+x^3+x^2+x+1}$$
$$\cancel{x^8}+x^7+x^5$$
$$\overline{\cancel{x^7}+x^5+x^3+x^2+x+1}$$
$$\cancel{x^7}+x^6+x^4$$
$$\overline{\cancel{x^6}+\cancel{x^5}+x^4+\cancel{x^3}+x^2+x+1}$$
$$\cancel{x^6}+\cancel{x^5}+\cancel{x^3}$$
$$\overline{\cancel{x^4}+x^2+\cancel{x}+1}$$
$$\cancel{x^4}+x^3+\cancel{x}$$
$$\overline{\cancel{x^3}+\cancel{x^2}+\cancel{1}}$$
$$\cancel{x^3}+\cancel{x^2}+\cancel{1}$$
$$\overline{0}$$

syndrom = 0

Problem solving on CRC

Q.1 Consider the cyclic redundancy check (CRC) based error detecting scheme having the generator polynomial $X^3 + X + 1$. Suppose the message $m_4m_3m_2m_1m_0 = 11000$ is to be transmitted. Check bits $c_2c_1c_0$ are appended at the end of the message by the transmitter using the above CRC scheme. The transmitted bit string is denoted by $m_4m_3m_2m_1m_0c_2c_1c_0$. The value of the check bit sequence $c_2c_1c_0$ is

GATE 2021

A. 111

B. 100

C. 101

D. 110

generator $= x^3 + x + 1$

$= 1\cdot x^3 + 0\cdot x^2 + 1\cdot x^1 + 1\cdot x^0$

1011

Msg = 11000

Sender

```
1011 ) 11000000
       1011
       01110000
        1011
        0101000
         1011
        000100 → CRC
```

Q.2 Given the generator function G(X) and the message function M(X) as follow

$$G(X) = X^4 + X + 1 \quad , r = 4$$

$$\underset{d(x)}{M(X)} = X^7 + X^6 + X^4 + X^2 + X$$

Calculate the transmission function T(X)

A. $X^{11} + X^7 + X^5 + X^4 + X^3 + X$

B. $X^{11} + X^{10} + X^8 + X^6 + X^5 + X^2 + X$

C. $X^{10} + X^7 + X^6 + X^2 + X$

D. $X^{11} + X^{10} + X^8 + X^6 + X^5$

(1) $r = 4$

(2) Determine $x^r \cdot d(x)$

$$= x^4 \cdot (x^7 + x^6 + x^4 + x^2 + x)$$
$$= x^{11} + x^{10} + x^8 + x^6 + x^5$$

(3) Determine the remainder by dividing $x^r d(x)$ by $g(x)$

Sender

$$
\begin{array}{r|l}
x^4+x+1 & \cancel{x^{11}}+x^{10}+\cancel{x^8}+x^6+x^5 \quad \big(x^7+x^6+x \\
 & \cancel{x^{11}}+\cancel{x^8}+x^7 \\
\hline
 & \cancel{x^{10}}+\cancel{x^7}+\cancel{x^6}+x^5 \\
 & \cancel{x^{10}}+\cancel{x^7}+\cancel{x^6} \\
\hline
 & \cancel{x^5} \\
 & \cancel{x^5}+x^2+x \\
\hline
 & x^2+x
\end{array}
$$

x^2+x CRC OR Remainder

Codeword or Transmitted data $= x^r d(x) + \text{Remainder}$

$= x^{11}+x^{10}+x^8+x^6+x^5+x^2+x$

Q.3 The message 11001001 is to be transmitted using the CRC polynomial $x^3 + 1$ to protect it from errors. The message that should be transmitted is

GATE 2007

H.W

A. 11001001000

B. 11001001011

C. 11001010

D. 110010010011

Q.4 A computer network uses polynomial over GF(2) for error checking with 8 bits as information bits and uses $x^3 + x + 1$ as the generator polynomial to generate the check bits.

In this network, the message 01011011 is transmitted as.

GATE 2017 (2m)

A. 01011011010

B. 01011011011

C. 01011011101

D. 01011011100

Generator $= x^3 + x + 1$

$= 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0 = 1011$

Sender

$$
\begin{array}{r}
1011 \,\big)\, 01011011000 \\
1011 \\
\hline
00000011000 \\
1011 \\
\hline
01110 \\
1011 \\
\hline
0101
\end{array}
$$

101 CRC

Transmitted data $= 01011011\,101$

Q.5 Consider the following message M = 1010001101. The cyclic redundancy check (CRC) for this message using the divisor polynomial $x^5 + x^4 + x^2 + 1$ is

GATE 2005

H.W

A. 01110 ✓

B. 01011

C. 10101

D. 10110

Q.6 Consider generator polynomial function G(x) is $X^3 + 1$, the data stream at sender end is 10110101110101, then calculate CRC

H.W

A. 100

B. 110

C. 101

D. 010


THANK YOU
GW
SOLDIERS !