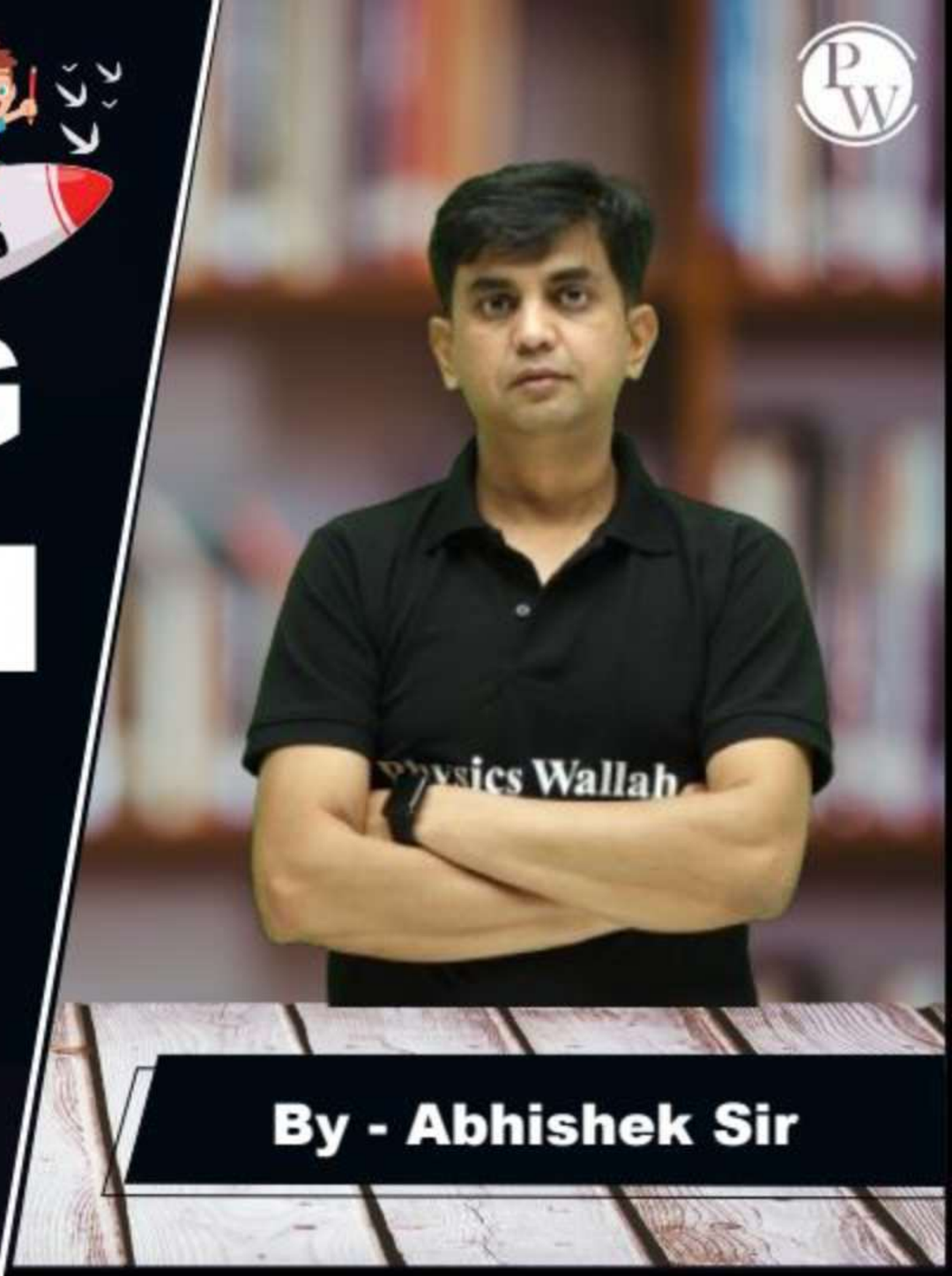
CS & IT ENGINEERING

Computer Network

Error Control

Lecture No. - 03



By - Abhishek Sir

Recap of Previous Lecture

Topic Block Code

Topic CRC

Topics to be Covered

Topic	CRC

ABOUT ME

Hello, I'm Abhishek

- GATE CS AIR - 96
- M.Tech (CS) - IIT Kharagpur
- 12 years of GATE CS teaching experience

Telegram Link : https://t.me/abhisheksirCS_PW

Topic : Generator Polynomial

G(X) : Generator Polynomial function

→ **(n+1)** terms [X^n to X^0]

→ Degree[G(X)] = **n**

→ Coefficient of term X^0 should be **"one"**
[G(X) shuold not be divisible by X]

→ Both transmitter and receiver must agree on same G(X)

$G(X) = X^n + ... + 1$

Topic : Divisor

$G(X) = X^n + ... + 1$

Divisor : binary string, **(n+1) bits** [1 . . . . 1]

Example :

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

$= 1*X^3 + 1*X^2 + 0*X^1 + 1*X^0$

Divisor = 1 1 0 1

Topic : Message Polynomial

M(X) : Message Polynomial function

→ **m** terms, [$X^{(m-1)}$ to X^0]

→ coefficients are either zero or one

DATA (Message) : binary string (**m - bits**)

Topic : Message Polynomial

DATA (Message) : binary string (**m - bits**)

Example :-

$$M(X) = X^7 + X^4 + X^3 + X$$

$$= 1*X^7 + 0*X^6 + 0*X^5 + 1*X^4 + 1*X^3 + 0*X^2 + 1*X^1 + 0*X^0$$

DATA = 1 0 0 1 1 0 1 0

Topic : CRC

Transmitter protocol :

[M(X) * X^n] [Modulo-2 Division] [G(X)]

n : degree of [G(x)]

modulo 2 Arithmatic

Topic : CRC

Example 1 :

Divisor (भाजक)

$G(X) = X^3 + X^2 + 1$ degree[G(x)] = 3

$M(X) = X^7 + X^4 + X^3 + X$

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$ Divident (भाजक)

[$M(X) * X^3$] [Modulo-2 Division] [$G(X)$]

Divident Divisor

Topic : CRC

$X^7 + X^6 + X^5 + X^4 + X^3 + 1$

$X^3 + X^2 + 1$) $X^{10} + X^7 + X^6 + X^4$

$X^{10} + X^9 + X^7$

$X^9 + X^6 + X^4$

$X^9 + X^8 + X^6$

$X^8 + X^4$

$X^8 + X^7 + X^5$

$X^7 + X^5 + X^4$

$X^7 + X^6 + X^4$

$X^6 + X^5$

$X^6 + X^5 + X^3$

X^3

$X^3 + X^2 + 1$

$X^2 + 1$

Modulo 2 division
[bit-wise X-OR]

Topic : Remainder Polynomial

R(X) : Remainder Polynomial function

→ **n** terms, [$X^{(n-1)}$ to X^0]

→ coefficients are either zero or one

CRC (Remainder) : binary string (**n - bits**)

Topic : CRC

Example 1 :

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

$M(X) = X^7 + X^4 + X^3 + X$

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$

[$M(X) * X^3$] [Modulo-2 Division] [$G(X)$]

$R(X) = 1*X^2 + 0*X^1 + 1*X^0$

Topic : CRC

Transmitter protocol :

$[M(X) * X^n]$ [Modulo-2 Division] $[G(X)]$

$R(X)$: Remainder Polynomial function (of above equation)

Transmitter transmit :

$[M(X) * X^n] + [R(X)]$

Topic : CRC

Example 1 :

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$ Divident

$R(X) = X^2 + 1$ Remainder

Transmitter transmit :

$$X^{10} + X^7 + X^6 + X^4 + X^2 + 1$$

Topic : CRC

Example 1 :

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

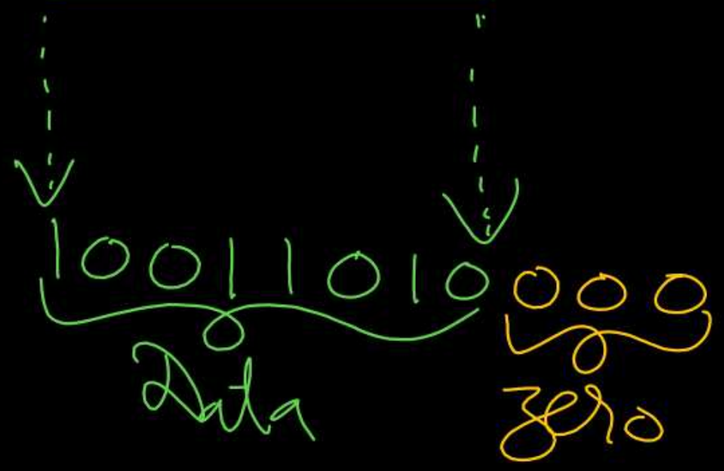
$M(X) = X^7 + X^4 + X^3 + X$

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$

DIVISOR = 1 1 0 1

DATA = 1 0 0 1 1 0 1 0

Divident = 1 0 0 1 1 0 1 0 0 0 0



[M(X) * X^3] [Modulo-2 Division] [G(X)]

Topic : CRC

Modulo 2 division
[bit-wise X-OR]

```
          1 1 1 1 1 0 0 1
      ┌─────────────────────
1 1 0 1 | 1 0 0 1 1 0 1 0 0 0 0
          1 1 0 1
          ---------
            1 0 0 1
            1 1 0 1
            ---------
              1 0 0 0
              1 1 0 1
              ---------
                1 0 1 1
                1 1 0 1
                ---------
                  1 1 0 0
                  1 1 0 1
                  ---------
                    0 0 1 0
                    0 0 0 0
                    ---------
                      0 1 0 0
                      0 0 0 0
                      ---------
                        1 0 0 0
                        1 1 0 1
                        ---------
                          1 0 1
```

Topic : CRC

Modulo 2 division
[bit-wise X-OR]

```
                1 0 0 1 1 0 1 0 0 0 0
          ------------------------------
1 1 0 1 | 1 0 0 1 1 0 1 0 0 0 0
          1 1 0 1
          -------
            1 0 0 1
            1 1 0 1
            -------
              1 0 0 0
              1 1 0 1
              -------
                1 0 1 1
                1 1 0 1
                -------
                  1 1 0 0
                  1 1 0 1
                  -------
                        1 0 0 0
                        1 1 0 1
                        -------
                          1 0 1
```

So CRC

Topic : CRC

Example 1 :

$G(X) = X^3 + X^2 + 1$ DIVISOR = 1 1 0 1

$M(X) = X^7 + X^4 + X^3 + X$ DATA = 1 0 0 1 1 0 1 0

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$

1 0 0 1 1 0 1 0 0 0 0

[M(X) * X^3] [Modulo-2 Division] [G(X)]

R(X) = $1*X^2 + 0*X^1 + 1*X^0$ CRC = 1 0 1

Topic : CRC

Example 1 :

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$

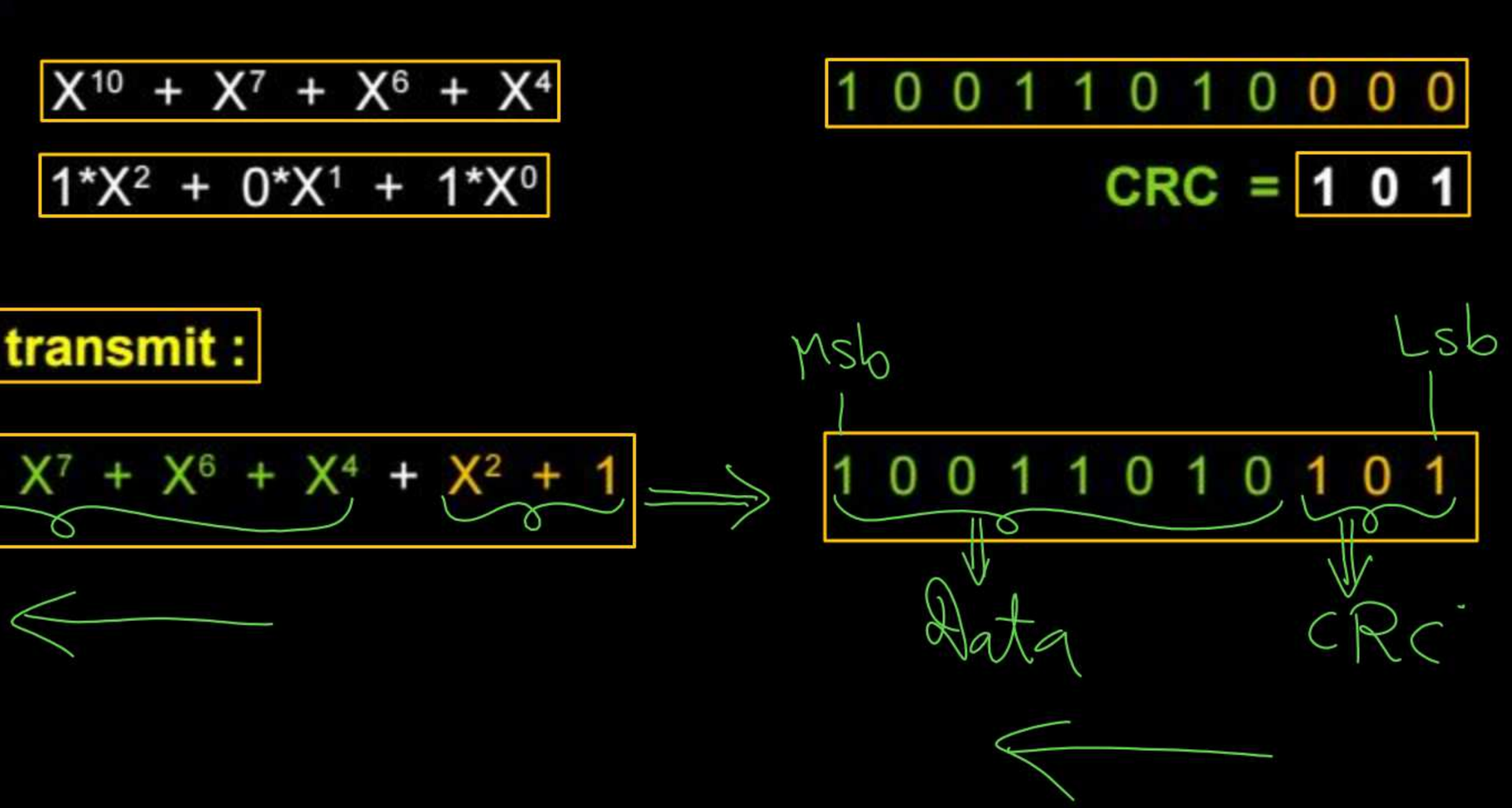
$R(X) = 1*X^2 + 0*X^1 + 1*X^0$

1 0 0 1 1 0 1 0 0 0 0

CRC = 1 0 1

Transmitter transmit :

$X^{10} + X^7 + X^6 + X^4 + X^2 + 1$



#Q. Consider the 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]

(A) 01110

(B) 01011

(C) 10101

(D) 10110

#Q. 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. A computer network uses polynomials 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]

H.W.

(A) 01011011010

(B) 01011011011

(C) 01011011101

(D) 01011011100

#Q. 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 checkbit sequence $c_2c_1c_0$ is :

[GATE 2021, Set-2, 2-Mark]

H.W.

(A) 101

(B) 110

(C) 100

(D) 111

Topic : CRC

Example 2 : H.W.

$G(X) = X^3 + X + 1$ Divisor

$M(X) = X^7 + X^4 + X^3 + X^2 + 1$

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^5 + X^3$ Divident

[$M(X) * X^3$] [Modulo-2 Division] [$G(X)$]

2 mins Summary

Topic CRC

THANK - YOU