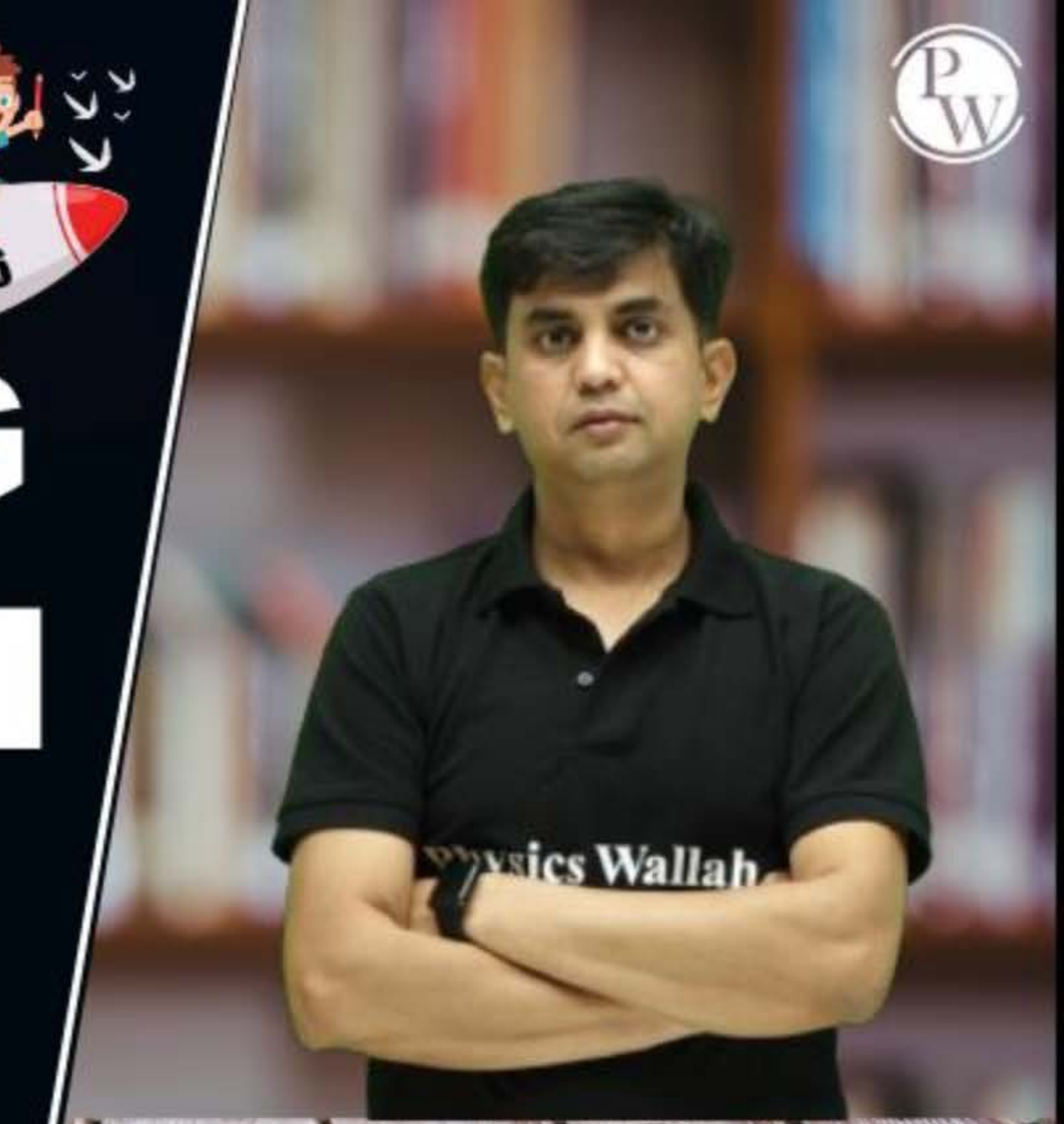
CS & IT ENGINEERING

Computer Network

Error Control

Lecture No. - 03



By - Abhishek Sir

Recap of Previous Lecture

- Topic: One-bit parity
- Topic: Valid & Invalid Codewords
- Topic: CRC

Topics to be Covered

Topic	CRC

Example 2 :-

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

DATA = 1 0 0 1 1 1 0 1

CRC = ? (3-bit) = 011

Solution :

(4 bit)

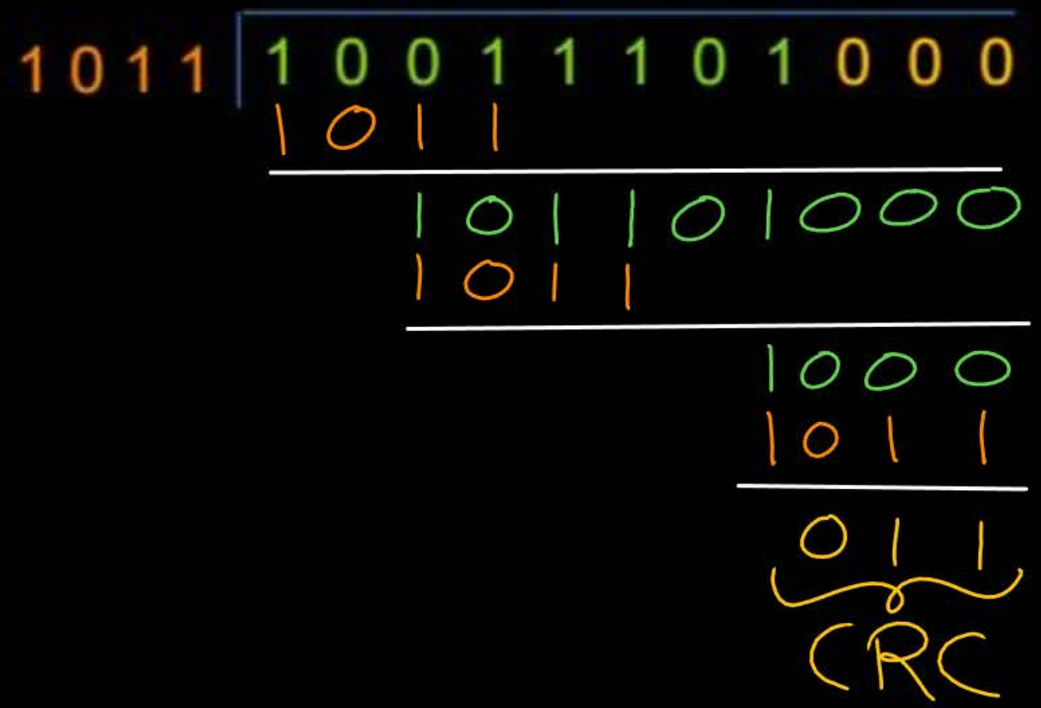
DIVISOR = 1 0 1 1

~~DIVIDEND~~ = 1 0 0 1 1 1 0 1 0 0 0

DIVIDENT

8 bit data 3-zero

Modulo 2 Division
[bit-wise X-OR]



Modulo 2 Division
[bit-wise X-OR]

Example 3 :-

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

degree[G(x)] = 4

DATA = 1 1 0 1 0 1 0 1

CRC = ? = (4 bit) = 0011

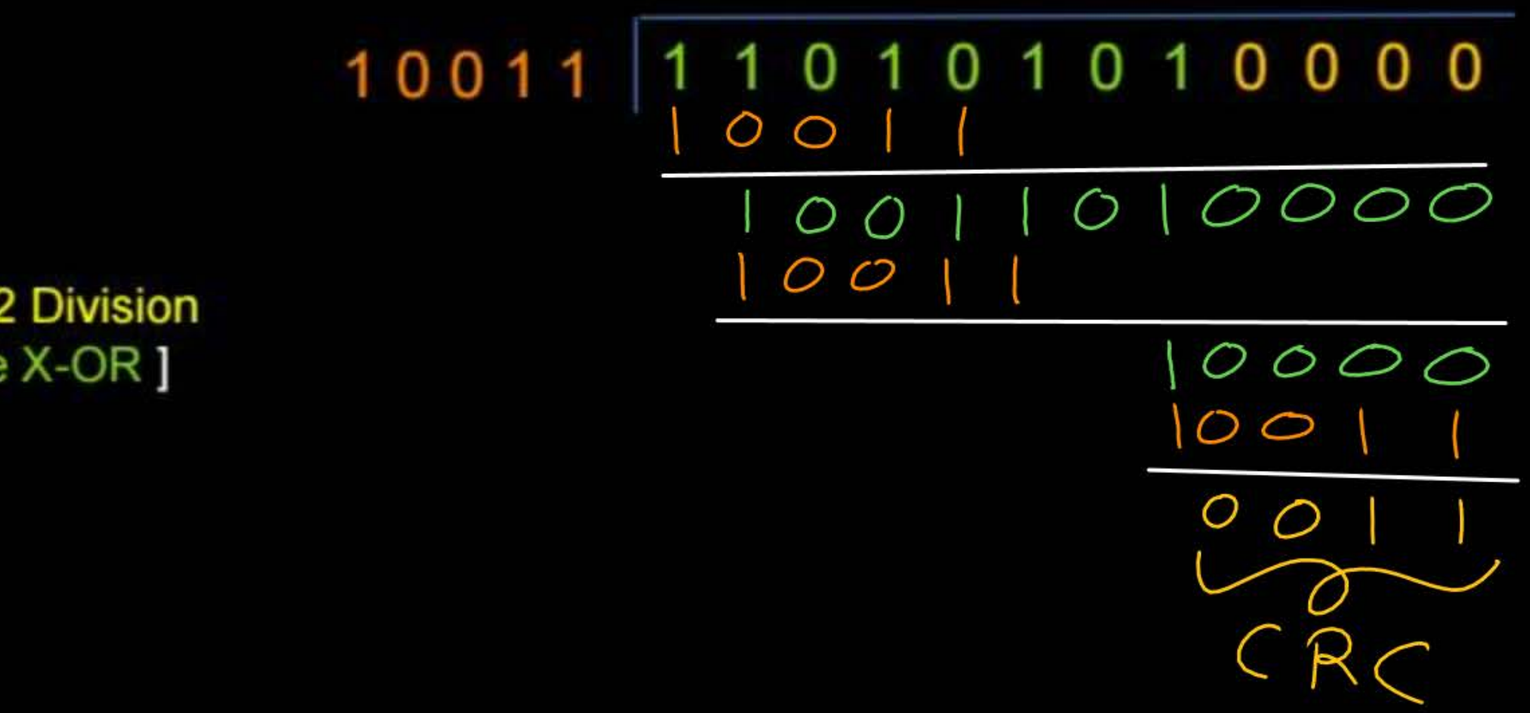
Solution :

DIVISOR = (5 bit) = 10011

DIVIDENT = 1 1 0 1 0 1 0 1 0000

8 bit data 4-zero

Modulo 2 Division
[bit-wise X-OR]



Modulo 2 Division
[bit-wise X-OR]

#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

IIT-B, H.W.

CS-2021

Topic : Generator Polynomial

G(X) : Generator Polynomial function

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

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

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

Topic : Generator Polynomial

G(X) : Generator Polynomial function

→ Degree[G(X)] = **n** [where **n** > **0**]

[G(X) should have atleast two terms]

→ **(n+1)** terms [X^n to X^0]

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

Topic : Divisor

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

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

Example 1 :-

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

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

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 1 :-

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

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

DATA = 1 0 0 1 1 0 1 0

8 bit

Topic : CRC

$degree[G(x)] = n$ $\quad G(x) = x^n + \ldots + 1$

Transmitter protocol :

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

DIVIDENT DIVISOR

Topic : CRC

Example 1 :

$G(X) = X^3 + X^2 + 1$ ← DIVISOR

$M(X) = X^7 + X^4 + X^3 + X$ ← DATA

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

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

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

$M(X) * X^3 = X^{10} + X^7 + X^6 + X^4$ DIVIDEND = 1 0 0 1 1 0 1 0 0 0 0

DATA

Zero (n-bit)

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

Topic : CRC

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

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

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

$x^9 + x^6 + x^4$

$x^9 + x^8 + x^6$

$x^8 + x^4$

$x^8 + x^7 + x^5$

$x^7 + x^5 + x^4$

$x^7 + x^6 + x^4$

$x^6 + x^5$

$x^6 + x^5 + x^3$

x^3

$x^3 + x^2 + 1$

$x^2 + 1$

Modulo 2 arithmetic
[bit-wise X-OR]

Topic : CRC

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

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

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

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

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

$$X^8 + X^4$$

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

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

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

$$X^6 + X^5$$

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

$$X^3$$

$$X^3 + X^2 + 1$$

$$X^2 + 1$$

Modulo 2 arithmetic
[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 :

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

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

CRC = 1 0 1

Topic : CRC

Transmitter protocol :

$$[\ M(X) * X^n\ ] \quad [\text{Modulo-2 Division}] \quad [\ G(X)\ ]$$

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

Transmitter transmit :

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

Topic : CRC

Example 1 :

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

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

Transmitter transmit :

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

Topic : CRC

Example 1 :

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

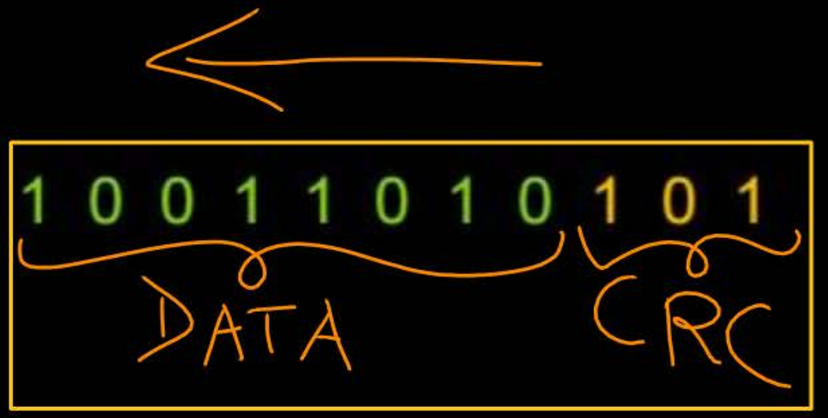
1 0 0 1 1 0 1 0 0 0 0

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

CRC = 1 0 1

Transmitter transmit :

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



#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]

(A) 11001001000

(B) 11001001011

(C) 11001010

(D) 110010010011

IIT-K, H.W.

(GATE 2017)

Topic : CRC

Example 2 :

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

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

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

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

Topic : CRC

Example 2 :

$G(X) = X^3 + X + 1$ ✓

DIVISOR = 1 0 1 1

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

DATA = 1 0 0 1 1 1 0 1

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

DIVIDEND = 1 0 0 1 1 1 0 1 0 0 0

DATA

3-zero

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

Topic : CRC

$X^3 + X + 1$ | $X^{10} + X^7 + X^6 + X^5 + X^3$

$x^7 + x^5 + 1$

$x^{10} + x^8 + x^7$

$x^8 + x^6 + x^5 + x^3$

$x^8 + x^6 + x^5$

x^3

$x^3 + x + 1$

$x + 1$

$R(x)$

Modulo 2 arithmetic
[bit-wise X-OR]

Topic : CRC

$X^7 + X^5 + 1$

$X^3 + X + 1$ | $X^{10} + X^7 + X^6 + X^5 + X^3$

$X^{10} + X^8 + X^7$

$X^8 + X^6 + X^5 + X^3$

$X^8 + X^6 + X^5$

X^3

$X^3 + X + 1$

$X + 1$

Modulo 2 arithmetic
[bit-wise X-OR]

Topic : CRC

Example 2 :

$R(X) = X + 1$

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

CRC = 0 1 1

Topic : CRC

Example 2 :

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

1 0 0 1 1 1 0 1 0 0 0

$R(X) = X + 1$

CRC = 0 1 1

Transmitter transmit :

$X^{10} + X^7 + X^6 + X^5 + X^3 + X + 1$

Topic : CRC

DIVIDENT

DIVISOR

Receiver protocol :

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

R'(X) : Remainder at receiver (of above equation)

if **R'(X) == ZERO** :
    then Receiver concluded "**No any error detected**"
else
    Receiver concluded "**Error detected**"

Topic : CRC

Example 2 :

Transmitter transmited :

$X^{10} + X^7 + X^6 + X^5 + X^3 + X + 1$

1 0 0 1 1 1 0 1 0 1 1

Receiver received :

$X^{10} + X^7 + X^6 + X^5 + X^3 + X + 1$

1 0 0 1 1 1 0 1 0 1 1

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

DIVISOR = 1 0 1 1

Topic : CRC

AT RECV :-

Modulo 2 division
[bit-wise X-OR]

```
1011 | 1 0 0 1 1 1 0 1 0 1 1
       1 0 1 1
       -------
         1 0 1 1 0 1 0 1 1
         1 0 1 1
         -------
           1 0 1 1
           1 0 1 1
           -------
             0 0 0
```

R'(x)

Topic : CRC

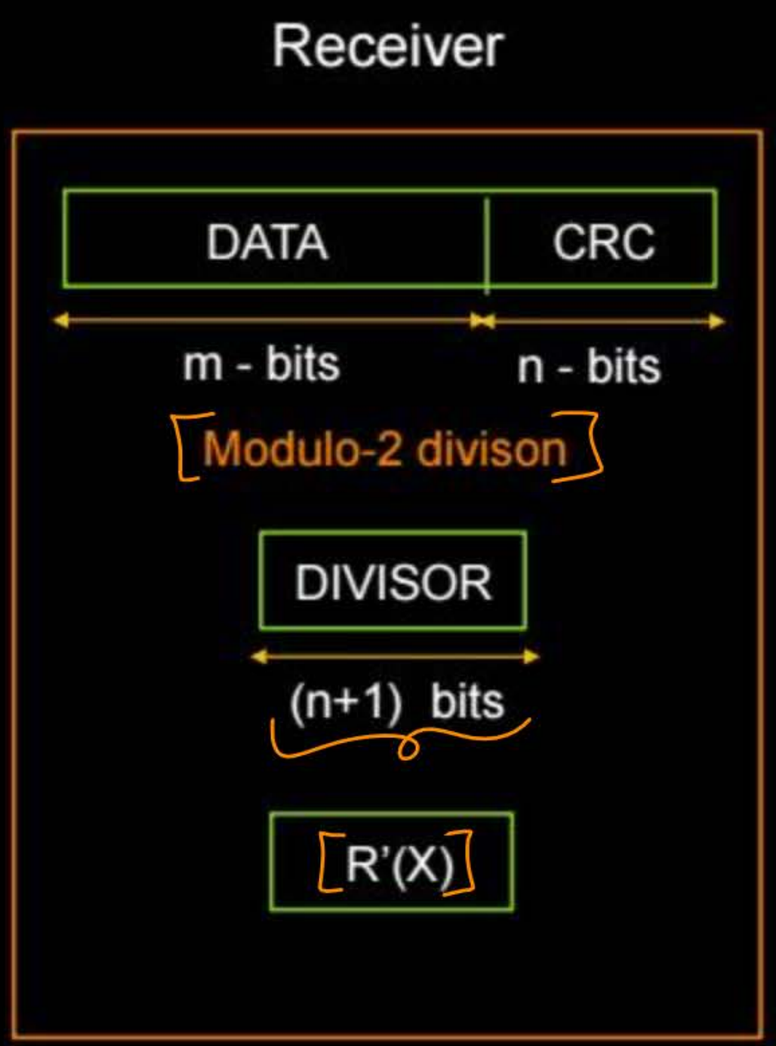
```
1 0 1 1 | 1 0 0 1 1 1 0 1 0 1 1
          1 0 1 1
          -------
            1 0 1 1
            1 0 1 1
            -------
              1 0 1 1
              1 0 1 1
              -------
                0 0 0
```

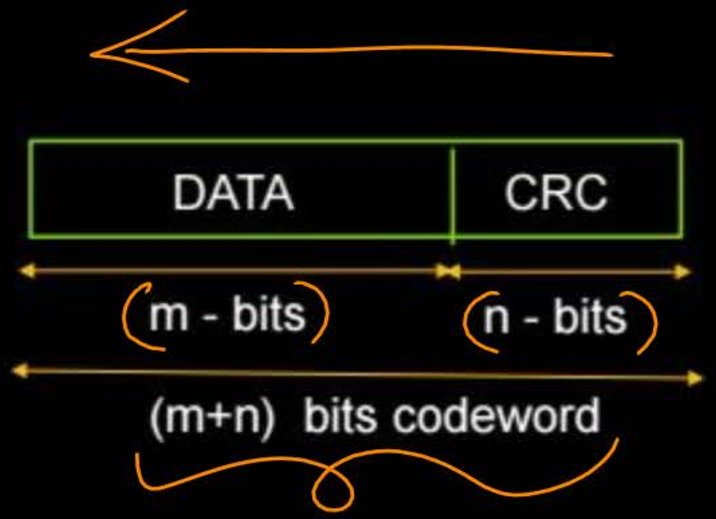
Modulo 2 division
[bit-wise X-OR]

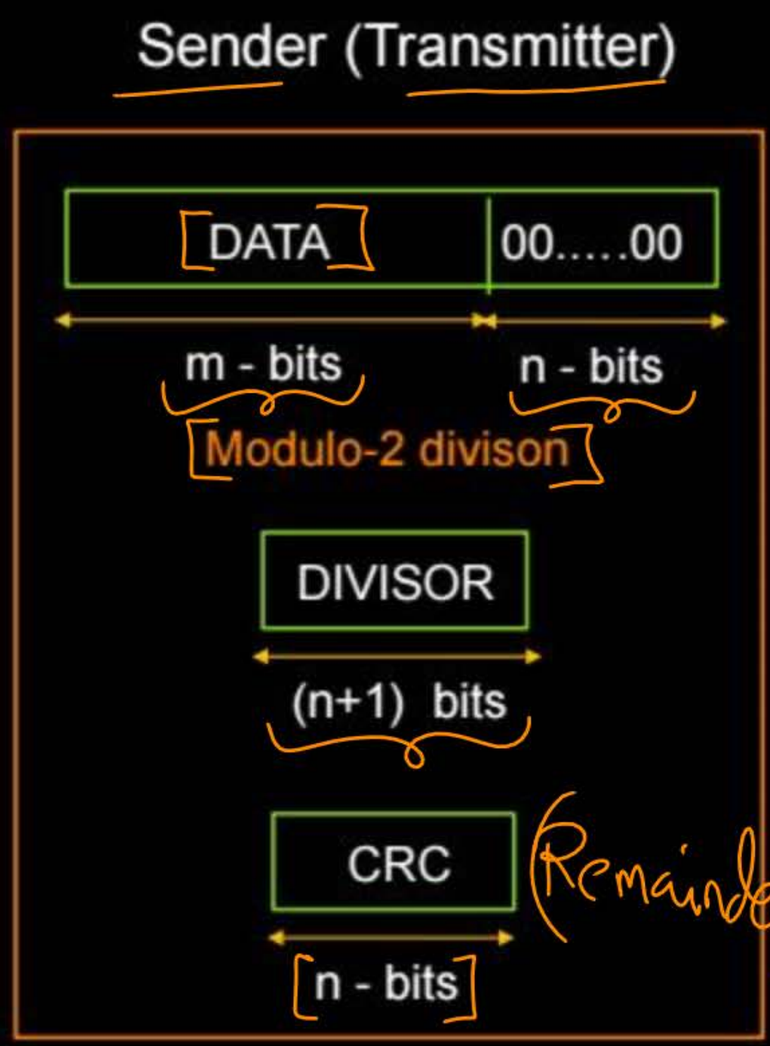
$R'(x)$

Topic : CRC

$G(X) = X^n + ... + 1$ where $n > 0$







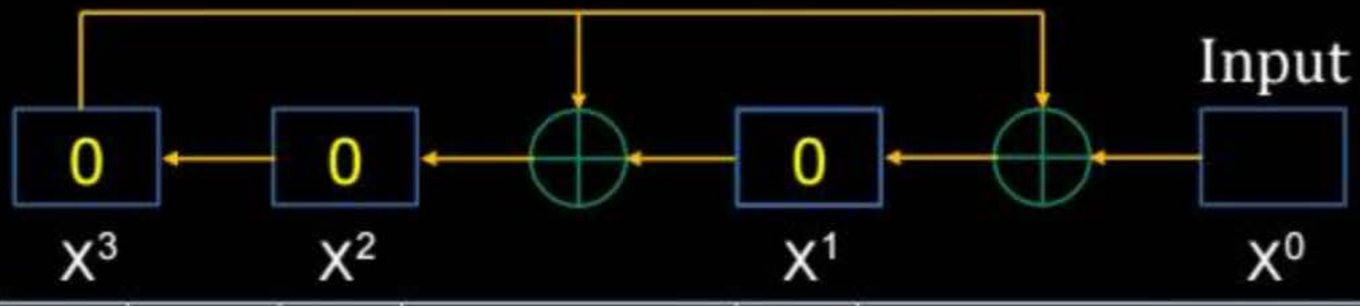
Topic : CRC

Example 2:

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

Message (DATA) = 1 0 0 1 1 1 0 1

CRC = 0 1 1

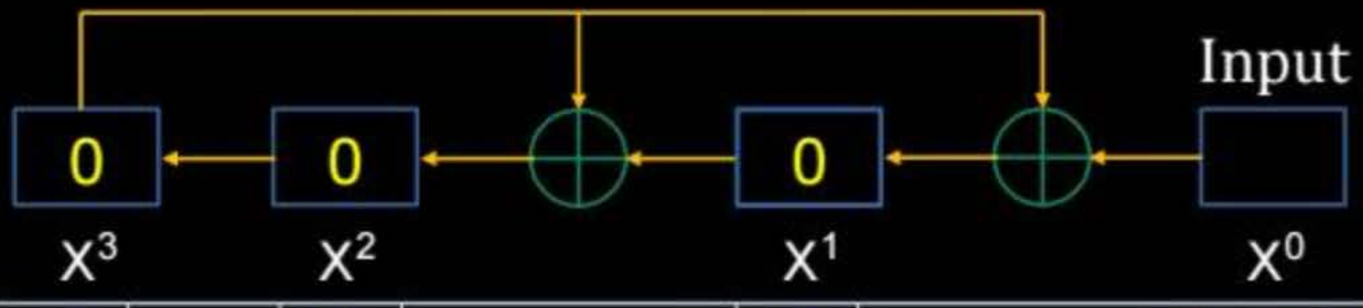


AT Sender (Transmitter)

Input = 1 0 0 1 1 1 0 1 **0 0 0**

$d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8 C_1 C_2 C_3$

0	0	0	$d_1 = 1$
0	0	$d_1=1$	$d_2 = 0$
0	$d_1=1$	$d_2=0$	$d_3 = 0$
$d_1=1$	$d_2=0$	$d_3=0$	$d_4 = 1$
$d_2=0$	1	0	$d_5 = 1$
1	0	1	$d_6 = 1$
0	0	0	$d_7 = 0$
0	0	0	$d_8 = 1$
0	0	1	$C_1 = 0$
0	1	0	$C_2 = 0$
1	0	0	$C_3 = 0$
0	1	1	



0	0	0	$d_1 = 1$
0	0	$d_1=1$	$d_2 = 0$
0	$d_1=1$	$d_2=0$	$d_3 = 0$
$d_1=1$	$d_2=0$	$d_3=0$	$d_4 = 1$
$d_2=0$	1	0	$d_5 = 1$
1	0	1	$d_6 = 1$
0	0	0	$d_7 = 0$
0	0	0	$d_8 = 1$
0	0	1	$C_1 = 0$
0	1	0	$C_2 = 1$
1	0	1	$C_3 = 1$
0	0	0	

AT Receiver

Input = 1 0 0 1 1 1 0 1 **0 1 1**

$d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8 C_1 C_2 C_3$

if **R'(X) == ZERO** :
then Receiver concluded
"**No any error detected**"
else
Receiver concluded
"**Error detected**"

Topic : CRC

CASE I : No any error

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

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

Topic : CRC

CASE I : No any error

Transmitter transmit : [M(X) * X^n] + [R(X)]

Receiver received : [M(X) * X^n] + [R(X)]

Receiver protocol :

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

Topic : CRC

$E(x) = 0$

CASE I : No any error

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

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

Receiver protocol :

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

Above equation definitely lead "zero remainder"

Receiver conclude : "No any error detected"

Topic : CRC

CASE II : Error Included

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

Receiver received : $[M(X) * X^n] + [R(X)] + [E(X)]$

Topic : Error Polynomial

E(X) : Error Polynomial Function

→ Coefficient are either Zero or One

Data : m bits CRC : n bits

Codeword : (m + n) bits

Degree(**E(X)**) < (m + n)

Topic : Error Polynomial

For single bit error :

$$E(X) = X^i$$

Where [0 <= i < (m + n)]

$i \rightarrow 0$ to $(m+n-1)$

2 mins Summary

Topic CRC

THANK - YOU