CS & IT ENGINEERING

Computer Network

Error Control

Lecture No. - 04

By - Abhishek Sir

Recap of Previous Lecture

Topic CRC

Topics to be Covered

Topic CRC

#Q. Consider the message $\boxed{M = 1010001101.}$ 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

$\boxed{\text{Ans: A}}$

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

@ABHISHEKSIRCS_PW

$$G(x) = x^5 + x^4 + x^2 + 1$$

$$\text{Divisor} = \underbrace{110101}$$

CRC = (5 bit)

110101) 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0

110101

11101110100000

110101

111010100000

110101

1111100000

110101

10110000

110101

1100100

110101

$$\underbrace{01110}_{CRC}$$

#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

4bit CRC

$\boxed{\text{Ans : B}}$

```
1001 | 110010010000
       1001
       ------------
        10110010000
        1001
        -----------
          10001000
          1001
          --------
              11000
              1001
              -----
               1010
               1001
               ----
                011
```

$\underbrace{011}_{\text{CRC}}$

CRC = (3 bit)

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

Divisor = 1001

Topic : CRC

CASE II : Error Included

Transmitter transmit : $\boxed{[\, M(X) * X^n \,] + [\, R(X) \,]}$

Receiver received : $\boxed{[\, M(X) * X^n \,] + [\, R(X) \,] + [\, E(X) \,]}$

Received Data = Transmitted Data + Error

Topic : Error Polynomial

$E(x) \neq 0$

$E(X)$: Error Polynomial Function

→ Coefficient are either Zero or One

Data : m bits CRC : n bits

Codeword : $(m + n)$ bits

$\text{Degree}(E(X)) < (m + n)$

Topic : Error Polynomial

For single bit error :

$$E(X) = \boxed{X^i}$$

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

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

Topic : Error Polynomial

Transmitter transmited :

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

$$\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ \overset{x^3}{\overset{\downarrow}{1}}\ 0\ 1\ 1}$$

Receiver received :

$$\boxed{X^{10} + X^7 + X^6 + X^5 + X + 1}$$

$$\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ \overset{x^3}{\overset{\downarrow}{0}}\ 0\ 1\ 1}$$

$$\boxed{E(X) = X^3}$$

Topic : Error Polynomial

Transmitter transmited :

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

X^4

$$\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1}$$

Receiver received :

$$\boxed{X^{10} + X^{7} + X^{6} + X^{5} + X^{4} + X^{3} + X + 1}$$

X^4

$$\boxed{1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1}$$

$$\boxed{E(X) = X^{4}}$$

Topic : Error Polynomial

For two bit error :

$$\underline{E(X)} = (X^i + X^j)$$

Where $\underbrace{i \ \& \ j \text{ are } 0 \text{ to } (m + n - 1)}_{}$ and $\boxed{i > j}$

Topic : Error Polynomial

Transmitter transmited :

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

x^9 x^1

$$\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1}$$

Receiver received :

$$\boxed{X^{10} + \underline{X^9} + X^7 + X^6 + X^5 + X^3 + 1}$$

x^9 x^1

$$\boxed{1\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1}$$

$$\boxed{E(X) = X^9 + X}$$

$$BL = (9 - 1 + 1) = 9$$

Topic : Error Polynomial

For two bit error :

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

Where i & j are 0 to $(m + n - 1)$ and $\underbrace{i > j}$

$$\boxed{\text{Burst length} = (i - j + 1)}$$

CASE II : Error Included

Transmitter transmit : $\boxed{[M(X) * X^n] + [R(X)]}$

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

Receiver protocol :

$$\boxed{\boxed{[M(X) * X^n + R(X) + E(X)]}\ \text{[Modulo-2 Division]}\ \boxed{[G(X)]}}$$

Topic : CRC

$$\frac{A+B+C}{G} = \frac{A+B}{G} + \frac{C}{G}$$

CASE II : Error Included

Receiver protocol :

$[\, M(X) * X^n + R(X) + E(X) \,]$ [Modulo-2 Division] $[\, G(X) \,]$ $\longrightarrow R'(x)$

$[\, M(X) * X^n + R(X) \,]$ [Modulo-2 Division] $[\, G(X) \,]$ $\longrightarrow \boxed{R_1(x)}$

$+$ $[\, E(X) \,]$ [Modulo-2 Division] $[\, G(X) \,]$ $\longrightarrow R_2(x)$

$$R'(x) = R_1(x) + R_2(x)$$

Topic : CRC

CASE II : Error Included

$[\,M(X) * X^n + R(X)\,]$ [Modulo-2 Division] $[\,G(X)\,] \rightarrow R_1(x)$

$+ \; [\,E(X)\,]$ [Modulo-2 Division] $[\,G(X)\,] \rightarrow R_2(x)$

$$\boxed{\frac{E(x)}{G(x)}}$$

First equation definitely lead "zero remainder"

For successful error detection, second equation should lead "non-zero remainder"

Topic : CRC

Example 4 :

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

$$\text{Data} = \underbrace{1\,0\,0\,1\,1\,1\,0\,1}_{0}$$

$$\text{Transmitted Data} = \boxed{1\,0\,0\,1\,1\,1\,0\,1\,\underline{1}\,\underline{0}\,\underline{0}}$$

Topic : CRC

degree(G(x)) = 3

Example 4 :

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

$x^6 \quad x^3$

Transmitted Data = $\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0}$

$E(X) = \boxed{X^6 + X^3}$

Received Data = $\boxed{1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0}$

$$\frac{E(x)}{G(x)} = \frac{x^6 + x^3}{x^3 + 1}$$

$$= \frac{x^3(x^3+1)}{(x^3+1)}$$

* complete division

$BL = (6-3+1) = 4$

Topic : CRC

Example 4 :

$G(X) = \boxed{X^3 + 1}$

Received Data = $\boxed{1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0}$

Receiver Conclusion : No any Error detected, Accept the data

AT Recv :-

$$
\begin{array}{r|l}
1001 & 10010100100 \\
 & \underline{1001} \\
 & \quad\quad 100100 \\
 & \quad\quad \underline{1001} \\
 & \quad\quad\quad\quad \underbrace{0}_{R'(x)}
\end{array}
$$

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

Divisor = 1001

Topic : CRC

$degree[G(x)] = 3$

Example 5 :

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

$x^5 \quad x^3$

Transmitted Data = $\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0}$

$E(X) = \boxed{X^5 + X^3}$

Received Data = $\boxed{1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0}$

$$\frac{E(x)}{G(x)} = \frac{(x^5 + x^3)}{(x^3 + 1)}$$

$$= \frac{x^3 * (x^2 + 1)}{(x^3 + 1)}$$

* Not causes complete division

$BL = (5 - 3 + 1) = 3$

Topic : CRC

Example 5 :

$G(X) = \boxed{X^3 + 1}$

Received Data = $\boxed{1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0}$

Receiver Conclusion : Error Detected
(Reject the data)

AT Recv :-

$$
\begin{array}{r|l}
1001 & 10011000100 \\
 & 1001 \\
\hline
 & \quad\;\; 1000100 \\
 & \quad\;\; 1001 \\
\hline
 & \qquad\quad 1100 \\
 & \qquad\quad 1001 \\
\hline
 & \qquad\quad\;\; \underbrace{101}_{R'(x)}
\end{array}
$$

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

Divisor = 1001

Topic : CRC

CASE II : Error Included

$\frac{E(X)}{G(X)}$

[E(X)] [Modulo-2 Division] [G(X)]

→ G(X) have (n+1) terms (length) $\Longrightarrow$ degree[G(X)] = n

→ If E(X) causes at-most (n length burst error) then above equation always lead non-zero remainder

Topic : CRC Property

** CRC limit

→ CRC can detect any length burst error, up-to the degree of generator polynomial function

Topic : CRC Property

→ if the count of total number of corrupted bits is odd then the E(X) definitely contains odd number of terms

Topic : CRC Property

→ if (X+1) is a factor of G(X)

[G(X) is completely divisible by (X+1)]

then G(X) definitely contains even number of terms

$$G(X) = F_1(X) * F_2(X)$$

$$G(X) = (X+1) * F_2(X)$$

No. of terms, must be even

Topic : CRC Property **

→ if (X+1) is a factor of G(X)

then CRC can detect "**all the errors where count of corrupted bits are odd**"

odd term ← E(X)

even terms ← G(X)

Topic : CRC

Example 6 :

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

Transmitted Data = $\boxed{1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0}$

x^7 x^5 x^4

$E(X) = \boxed{X^7 + X^5 + X^4}$

Received Data = $\boxed{1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0}$

$$\frac{E(x)}{G(x)} = \frac{x^7+x^5+x^4}{x^3+1}$$

* Not causes complete division

Topic : CRC

Example 6 :

$$G(X) = \boxed{X^3 + 1}$$

Received Data = $\boxed{1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0}$

Receiver Conclusion : Error Detected

AT Recv :-

$$
\begin{array}{r|l}
1001 & 10001011100 \\
 & 1001 \\
\hline
 & \quad 11011100 \\
 & \quad 1001 \\
\hline
 & \quad\; 1001100 \\
 & \quad\; 1001 \\
\hline
 & \qquad\quad \underbrace{100}_{0} \\
 & \qquad\quad R'(x)
\end{array}
$$

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

Divisor = 1001

#Q. Let G(X) be the generator polynomial used for CRC checking. What is the condition that should be satisfied by G(X) to detect odd number of bits in error?

[GATE 2009]

IIT-R

(A) G(X) contains more than ~~two~~ one terms

(B) G(X) does not divide $1 + X^k$, for any k not exceeding the frame length

(C) $(1 + X)$ is a factor of G(X)

(D) G(x) has an odd number of terms

$\boxed{\text{Ans: C}}$

Topic : CRC Property

→ For two-bit error,

$E(X)$ must have two terms only

$$\boxed{E(X) = (X^i + X^j)}$$

Where i & j are 0 to $(m + n - 1)$, $i > j$

$$\boxed{E(X) = X^j\,(X^{(i-j)} + 1)}$$

suppose $k = (i - j)$

$$\boxed{E(X) = X^j\,(X^{(k)} + 1)}$$

Topic : CRC Property **

→ To detect any two-bit error,

G(X) does not divide $(X^k + 1)$

[for any k from 1 to $(m + n - 1)$]

$\Rightarrow G(x)$ does not divide $(1+x), (1+x^2), (1+x^3)$

$\ldots\ldots (1+x^{(m+n-1)})$

Topic : CRC

Example 7 :

$G(X) = \boxed{X + 1}$

one-bit parity
with even parity

Message (DATA) $= \underbrace{1\,0\,1\,1\,1\,0\,1}_{\text{7bit data}}$

Transmitted Data $= \underbrace{1\,0\,1\,1\,1\,0\,1}_{\text{DATA}}\;\underline{1}$

one bit CRC

```
11 | 10111010
     11
     --------
      1111010
      11
      -------
        11010
        11
        -----
           10
           11
           --
            1
           CRC
```

$G(X) = X + 1$

Divisor = 11

Example 7 :

$G(X) = X + 1$

Transmitted DATA = 1 0 1 1 1 0 1 1

One-bit CRC [**CRC - 1**] is same as **one-bit party** with "**even parity**".

Topic : CRC

Example 8 :

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

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

CRC = 0 0 0

$$
\begin{array}{r|l}
1001 & 1\,0\,0\,1\,1\,0\,0\,1\,\underline{0\,0\,0} \\
 & 1001 \\
\hline
 & \quad\;\; 1001000 \\
 & \quad\;\; 1001 \\
\hline
 & \qquad\qquad \underbrace{000}_{CRC}
\end{array}
$$

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

Divisor = 1001

Example 9 :

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

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

CRC = 1 1 1

$$
\begin{array}{r}
1111 \\
1111 \overline{)\,11110001\underline{000}} \\
1111 \\
\hline
1000 \\
1111 \\
\hline
\underbrace{111}_{\text{CRC}}
\end{array}
$$

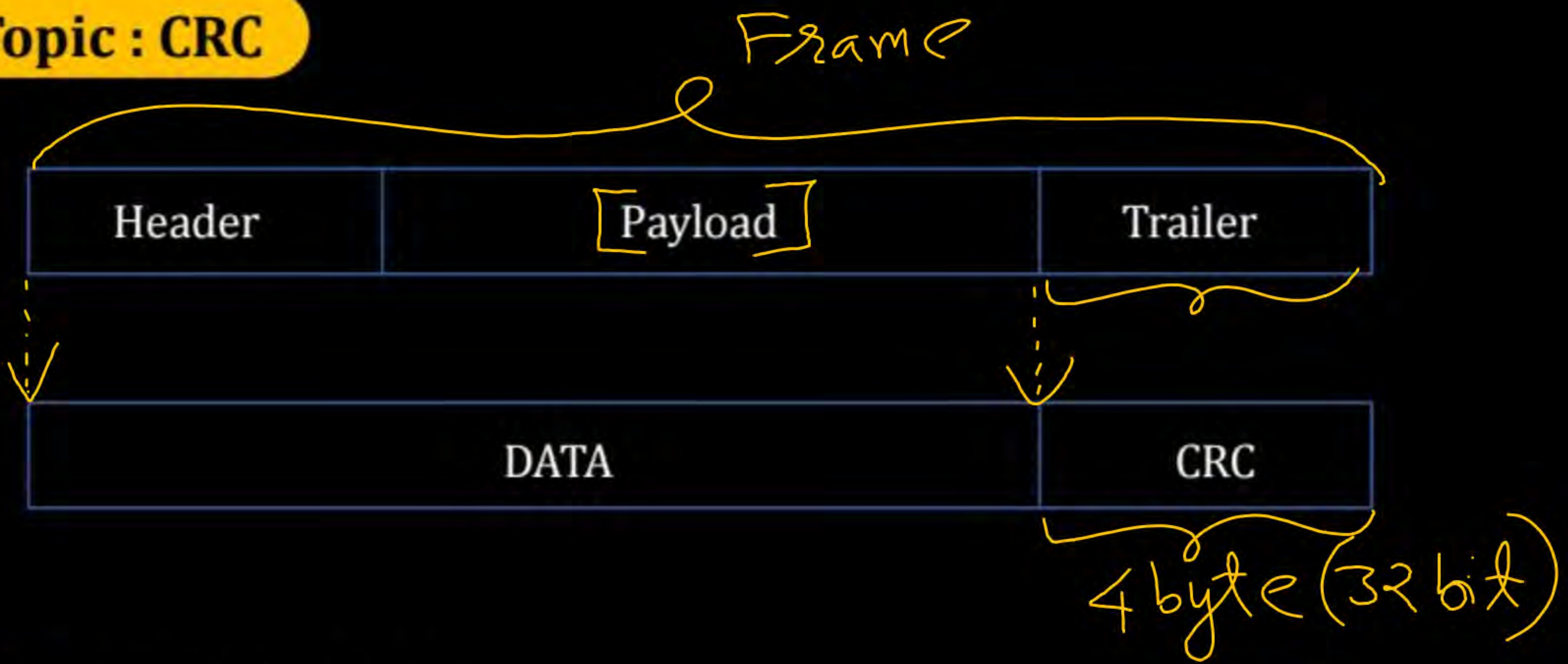
$G(X) = X^3 + x^2 + x + 1$

Divisor = 1111

Topic : CRC Property

→ CRC can be “all zero bits” and can be “all one bits”

Topic : CRC



CRC-32 : [32-bit / 4 byte]

$$G(X) = X^{32} + \ldots\ldots + 1$$

Topic : Cyclic Code

⇒ CRC always produces cyclic code.

CRC [$G(X) = X^3 + 1$] and 3 data bits

Data	-->	Codeword
$d_1d_2d_3$	-->	$d_1d_2d_3C_1C_2C_3$
0 0 0	-->	0 0 0 0 0 0
0 0 1	-->	0 0 1 0 0 1
0 1 0	-->	0 1 0 0 1 0
0 1 1	-->	0 1 1 0 1 1
1 0 0	-->	1 0 0 1 0 0
1 0 1	-->	1 0 1 1 0 1
1 1 0	-->	1 1 0 1 1 0
1 1 1	-->	1 1 1 1 1 1

2^3

2^3 valid codewords of length 6

Topic : Valid Codewords vs Invalid Codewords

m bits input (data) → N bits output (codeword)

→ Number of parity bits = $(N - m)$

→ Number of valid codewords = 2^m

→ Number of invalid codewords = $(2^N - 2^m)$

2 mins Summary

Topic CRC

THANK - YOU

@ABHISHEKSIRCS_PW