Computer Networks

Cyclic Redundancy Check

Fall 24-25, CS 3204, Section A

Dr. Nazib Abdun Nasir

Assistant Professor, CS, AIUB

nazib.nasir@aiub.edu

January 07, 2025

Outline

- Cyclic Redundancy Check
- Frame Check Sequence
  - → FCS – Sequence Types
  - → FCS – Generation by Sender
  - → FCS – Error Detection by Receiver
- How CRC Works
  - → Steps in CRC Calculation
- CRC – FCS – Example
  - → CRC – FCS – Task

Cyclic Redundancy Check

- Cyclic Redundancy Check (CRC) is an error-detecting code used extensively in digital networks and storage devices to identify accidental alterations to data.
- It operates by attaching a short check value, **derived from polynomial division**, to blocks of data.
- This check value, or **checksum**, allows the receiver to verify the **integrity** of the transmitted data.
- The redundant bits are also called **Frame Check Sequence** (FCS).
  - → Strength of the CRC depends on the number of redundant bits (FCS length).
  - → Longer FCS length results in better accuracy in detecting error.

FCS – Sequence Types

- FCS requires 2 types of sequences.
- **Message Sequence (M)**
  - → The desired data to be sent; Can be of any length.
- **Pattern Sequence (P)**
  - → Known to both sender and receiver.
  - → If we want to use *K* bits FCS, we need a pattern bit sequence, *P*, of length *K+1* bits.

FCS – Generation by Sender

- Decide how many FCS bits, *K*, we are going to use.
- Append *K* zeros at the end of the message bits to generate *M+K* bits long sequence *S*.
- Select a *K+1* bits long pattern sequence, *P*.
- Divide the sequence *S* by the pattern *P* to find the *K* bits of the remainder, *R*.
- Remove the appended zeros from sequence *S* and append the calculated remainder *R*.
- Thus, the *M* bits message and *K* bits remainder constitutes the **transmitting sequence, *T***.

FCS – Error Detection by Receiver

- At the destination, the **received sequence, T,** is divided by the same pattern sequence, *P*.

- If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

- A remainder indicates that the data unit has been damaged on the way and therefore must be rejected.

How CRC Works

- **Data Representation:** The data to be transmitted is treated as a **binary polynomial**. Each bit in the data corresponds to a **coefficient** in this polynomial.

- **Generator Polynomial:** A predefined polynomial, known as the **generator polynomial**, is agreed upon by both **sender and receiver**. This polynomial is crucial for the **division** process.

- **Polynomial Division:** The original message polynomial is divided by the generator polynomial using **modulo-2 division (binary division).** The remainder of this division becomes the **CRC checksum**.

Steps in CRC Calculation

- **Augmenting Data:** Append *n* zeros (where *n* is the degree of the generator polynomial) to the original data to create a new polynomial.

- **Division:** Perform binary division of this augmented data by the generator polynomial using XOR operations instead of traditional subtraction.

- **Calculating Remainder:** The remainder from this division is the CRC checksum, which is appended to the original data before transmission.

- **Verification Process:** Upon receiving the data, the receiver performs the same division operation on the received data (including the checksum). If the remainder is zero, it indicates that no errors were detected; otherwise, an error has occurred.

CRC – FCS – Example

- Generate FCS if the message polynomial and generator polynomial are $X^3 + X^2 + 1$ and $X^3 + X + 1$, respectively.
  - → Let M(x) be the message polynomial
  - → Then, M(x) = $X^3 + X^2 + 1$= 1101
  - → Let P(x) be the generator polynomial/pattern sequence
  - → Then, P(x) = $X^3 + X + 1$ = 1011
  - → K + 1 = P (bits); K = 3; Append (000) zeros
  - → Then, S(x) = 1101000
  - → Divide S(x) by P(x)

CRC – FCS – Example

→ Then, Remainder, R(x) = 001

→ Then, Transmit Sequence T(x) = M(x) + R(x) = 1101001

› Verification at Receiver

→ Perform Division Again. Divide T(x) by P(x)

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

At Receiver

Example from the Provided Materials

```
                1 1 1 1
              ---------
P → 1 0 1 1 | 1 1 0 1 0 0 0 ← S
              1 0 1 1
              -------
                1 1 0 0
                1 0 1 1
                -------
                  1 1 1 0
                  1 0 1 1
                  -------
                    1 0 1 0
                    1 0 1 1
                    -------
                      0 0 1 ← R
```

At sender

Transmit sequence or codeword

T = 1 1 0 1 0 0 1

CRC – FCS – Task

- Generate FCS if the message polynomial and generator polynomial are $X^4 + X^2 + X + 1$ and $X^3 + X^2 + 1$, respectively. Will the receiver accept or reject the message, if it receives 1101011? Explain in detail and show all the steps.

- Generate the transmitted sequence/codeword if the message sequence is 11001 and the pattern sequence is 1001. Explain how the receiver will detect an error if it receives 10101001. Explain in detail and show all the steps.

References

- Online Website Research
- 3. Cyclic Redundancy Check - Provided Materials