



DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

Title: Implementing Cyclic Redundancy Check.

DATA COMMUNICATION LAB
CSE 208



GREEN UNIVERSITY OF BANGLADESH

1 Objective(s)

- To attain knowledge on the cyclic redundancy check (CRC) and how it works.
- To implement parity checker and cyclic redundancy check (CRC) error detection algorithms.

2 Problem Analysis

In digital communication system errors are transferred from one communication system to another, along with the data. If these errors are not detected and corrected, data will be lost. For effective communication, data should be transferred with high accuracy. This can be achieved by first detecting the errors and then correcting them.

Error detection is the process of detecting the errors that are present in the data transmitted from transmitter to receiver, in a communication system. We use some redundancy codes to detect these errors, by adding to the data while it is transmitted from source (transmitter). These codes are called "Error detecting codes".

Types of error detection we will study today:

- Cyclic Redundancy Check (CRC)

2.1 Cyclic Redundancy Check (CRC)

A cyclic code is a linear (n, k) block code with the property that every cyclic shift of a codeword results in another code word. Here k indicates the length of the message at transmitter (the number of information bits). n is the total length of the message after adding check bits. (actual data and the check bits). n, k is the number of check bits. The codes used for cyclic redundancy check there by error detection are known as CRC codes (Cyclic redundancy check codes). Cyclic redundancy-check codes are shortened cyclic codes. These types of codes are used for error detection and encoding. They are easily implemented using shift-registers with feedback connections. That is why they are widely used for error detection on digital communication. CRC codes will provide effective and high level of protection.

2.1.1 CRC Code Generation

Based on the desired number of bit checks, we will add some zeros (0) to the actual data. This new binary data sequence is divided by a new word of length $n + 1$, where n is the number of check bits to be added. The remainder obtained as a result of this modulo 2- division is added to the dividend bit sequence to form the cyclic code. The generated code word is completely divisible by the divisor that is used in generation of code. This is transmitted through the transmitter. If the data stream is "01111010" and the polynomial bit stream is '11011' then we can see in fig 1 the remainder will be "0001".

So the received bit stream will be "011110100001"

At the receiver side, we divide the received code word with the same divisor to get the actual code word. For an error free reception of data, the remainder is 0. If the remainder is a non-zero, that means there is an error in the received code / data sequence. The probability of error detection depends upon the number of check bits (n) used to construct the cyclic code. For single bit and two bit errors, the probability is 100 %.

2.1.2 Algorithm for CRC:

Algorithm for Encoding using CRC:

1. The communicating parties agrees upon the size of message, $M(x)$ and the generator polynomial, $G(x)$.
2. If r is the order of $G(x)$, r bits are appended to the low order end of $M(x)$. This makes the block size bits, the value of which is $x^r M(x)$.
3. The block $x^r M(x)$ is divided by $G(x)$ using modulo 2 division.
4. The remainder after division is added to $x^r M(x)$ using modulo 2 addition. The result is the frame to be transmitted, $T(x)$. The encoding procedure makes exactly divisible by $G(x)$.

Algorithm for Decoding using CRC:

1. The receiver divides the incoming data frame $T(x)$ unit by $G(x)$ using modulo 2 division. Mathematically, if $E(x)$ is the error, then modulo 2 division of $[M(x) + E(x)]$ by $G(x)$ is done.

```

    01011 ← Quotient
-----
11011 | 01111010
- 00000
-----
    1111010
- 11011
-----
    010110
- 00000
-----
    10110
- 11011
-----
    11010
- 11011
-----
    0001 ← Remainder (mod-2)

```

Figure 1: Division of the data bit stream by the polynomial to get the remainder.

2. If there is no remainder, then it implies that $E(x)$. The data frame is accepted.
3. A remainder indicates a non-zero value of $E(x)$, or in other words presence of an error. So the data frame is rejected. The receiver may then send an erroneous acknowledgment back to the sender for re-transmission.

2.1.3 Implementation of CRC:

```

#include<stdio.h>
char data[20],div[20],temp[4],total[100];
int i,j,datalen,divlen,len,flag=1;
void check();
int main()
{
    printf("Enter the total bit of data:");
    scanf("%d",&datalen);
    printf("\nEnter the total bit of divisor");
    scanf("%d",&divlen);
    len=datalen+divlen-1;
    printf("\nEnter the data:");
    scanf("%s",&data);
    printf("\nEnter the divisor");
    scanf("%s",div);

    for(i=0;i<datalen;i++)
    {
        total[i]=data[i];
        temp[i]=data[i];
    }
    for(i=datalen;i<len;i++)
    total[i]='0';
    check();
    for(i=0;i<divlen;i++)
        temp[i+datalen]=data[i];

```

```

        printf("\ntransmitted Code Word:%s",temp);
        printf("\n\nEnter the received code word:");
scanf("%s",total);
check();
for(i=0;i<divlen-1;i++)
    if(data[i]=='1')
    {
        flag=0;
        break;
    }
if(flag==1)
printf("\nsuccessful!!");
else
printf("\nreceived code word contains errors...\n");
}
void check()
{
    for(j=0;j<divlen;j++)
        data[j]=total[j];
    while(j<=len)
    {
        if(data[0]=='1')
            for(i=1;i<divlen;i++)
                data[i] = ((data[i] == div[i])?'0':'1');

        for(i=0;i<divlen-1;i++)
            data[i]=data[i+1];
        data[i]=total[j++];
    }
}

```

2.1.4 Output for the code of CRC:

```

Enter the total bit of data:7
Enter the total bit of divisor:4
Enter the data:1001010
Enter the divisor:1011
transmitted Code Word:1001010111
Enter the received code word:1001010100
received code word contains errors...

```

3 Discussion & Conclusion

Based on the focused objective(s) to understand the cyclic redundancy check, the additional lab exercise made me more confident about the fulfillment of the objectives(s).

4 Lab Task (Please implement yourself and show the output to the instructor)

Implement the CRC code generation from a bitstream/polynomial and CRC error detection given a received bitstream/polynomial when the datastream and divisor can be of variable length.

5 Lab Exercise (Submit as a report)

Implement cyclic redundancy verification where the polynomial bit stream and the data stream received by the receiver will be user input.

6 Policy

Copying from internet, classmate, seniors, or from any other source is strongly prohibited. 100% marks will be *deducted* if any such copying is detected.