Date:

EXPERIMENT-2

Aim:

Implement the error correcting code Cyclic Redundancy Check (CRC) of data link layer using various polynomials like CRC-CRC 12, CRC 16 and CRC CCIPP.

Description:

The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network. It breaks the datagrams passed down by above layers and convert them into frames ready for transfer. This is called Framing. It provides two main functionalities

- Reliable data transfer service between two peer network layers
- Flow Control mechanism, which regulates the flow of frames such that data congestion is not there at slow receivers due to fast senders.

There are two basic strategies for dealing with errors. One way is to include enough redundant information (extra bits are introduced into the data stream at the transmitter on a regular and logical basis) along with each block of data sent to enable the receiver to deduce what the transmitted character must have been. The other way is to include only enough redundancy to allow the receiver to deduce that error has occurred, but not which error has occurred and the receiver asks for a retransmission. The former strategy uses **Error-Correcting Codes** and latter uses **Error-detecting Codes**.

CRC (Cyclic Redundancy Check)

This Cyclic Redundancy Check is the most powerful and easy to implement technique. Unlike checksum scheme, which is based on addition, CRC is based on binary division. In CRC, a sequence of redundant bits, called **cyclic redundancy check bits**, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. 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 in transit and therefore must be rejected.

- ❖ Bit strings are created as representation of polynomials with coefficients ‘0’ and ‘1’only.

- A k-bit frame is regarded as coefficients list for a polynomial with 'k' terms (x^{k-1} to x^0)

  Eg: $x^5 + x^4 + x^0$ = 110001

- When this method is used, the sender and the receiver should agree upon a generator polynomial, G(x) in advance.
- Both the high and low order bits of G(x) must be '1'
- To compute checksum for some frame with 'm' bits (polynomial = M(x), append 'r' zero bits to the lower end of the frame (r = degree of the generator polynomial) so that this check summed frame is divisible by G(x).
- Divide M(x) by G(x) using modulo-2 division and subtract the remainder from M(x) using modulo-2subtraction. let the resultant be called as T(x)
- T(x) is passed to the receiver and the receiver divides it by G(x).
- If there is a remainder, there has been a transmission error.

Algorithm for computing checksum:

1. Let 'r' be the degree of G(x). append 'r' to the lower end of the frame so that it contains (m + r) bits.
2. Divide M(x) by G(x) using MOD-2 division.
3. Subtract the remainder from M(x) using MOD-2 subtraction.
4. The result is the check summed frame to be transmitted.

Eg: frame = 1101011011

G(x) = $x^4 + x + 1$ = 10011

➔ degree = 4

Therefore, frame = 1101011011 + 0000

➔M(x) = 11010110110000

Commonly used divisor polynomials are:

CRC 12 : $x^{12} + x^{11} + x^3 + x^2 + x + 1$

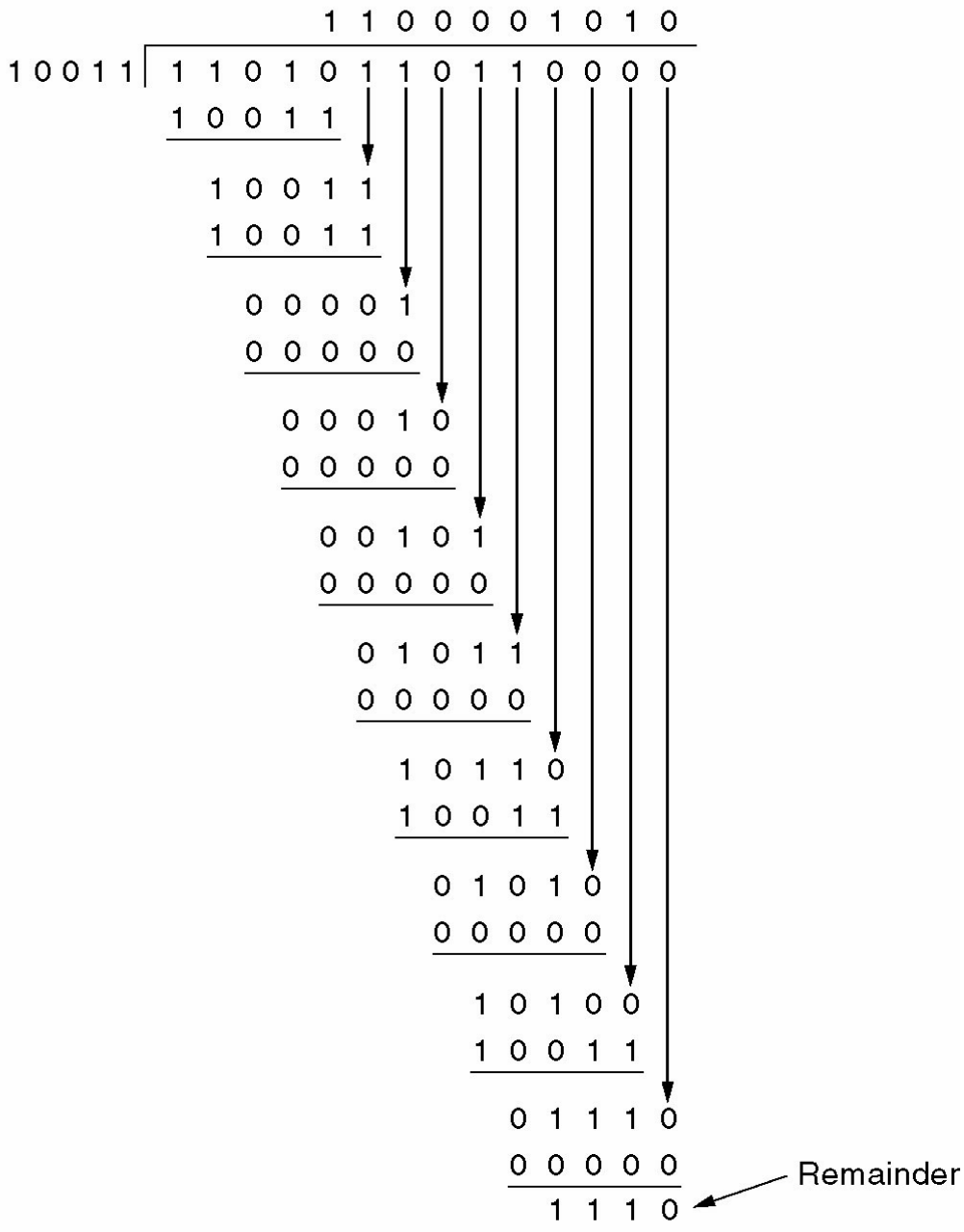
CRC 16 : $x^{16} + x^{15} + x^2 + 1$

CRC CCITT : $x^{16} + x^{12} + x^5 + 1$

Frame : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0

Performance:

CRC is a very effective error detection technique. If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows:

- CRC can detect all single-bit errors
- CRC can detect all double-bit errors (three 1's)
- CRC can detect any odd number of errors (X+1)
- CRC can detect all burst errors of less than the degree of the polynomial.
- CRC detects most of the larger burst errors with a high probability.
- For example CRC-12 detects 99.97% of errors with a length 12 or more.

Program:

```
#include<stdio.h>
#include<conio.h>
#include<string.h>
#include<math.h>
main()
{       int lf,lp,i,j,k,x;
        char f[20],p[20],sf[50]="",a[20];
        printf("Enter the frame:");        //inputting the frame
        scanf("%s",f);
        printf("Enter the polynomial:");   //inputting the polynomial
        scanf("%s",p);
         strcat(sf,f);                     //passing the frame into new string sf
        lf=strlen(f);
        lp=strlen(p);                      //stuffing the sf with 0
        for(i=0;i<lp-1;i++)
                strcat(sf,"0");
        for(i=0;i<lp;i++)                  //passing the first bits to string a
                a[i]=sf[i];
        x=lp;
         for(j=0;j<lf;j++)                 //repeating the loop for lf times
        {       if(a[0]=='1')              //checking and exor operation
                {       for(k=0;k<lp;k++)
                                if(a[k]==p[k])
                                        a[k]='0';
                                else
```

```
                                        a[k]='1';
                }
                for(k=0;k<lp;k++)               //shifting
                        a[k]=a[k+1];
                a[k-1]=sf[x];
                x++;
        }
        printf("the stuffed frame is: %s",f);
        for(k=0;k<lp-1;k++)
                printf("%c",a[k]);
}
```

Output:

Result:

Thus the program for cyclic redundancy check is executed.