Cyclic Redundancy Code (CRC) or Frame Check Sequence (FCS)

Chapter 3

This method uses for long messages and will be used only for the detection of errors.

The formation of the check bits (the bits to be appended to the message) will be done as follows.

3.1 Application

(a) Say the message is M (x)

(b) Choose a polynomial P (x) (assume this has N+1 bits)

(c) Append N zero's to the message M (x)
Now the message will be 2^N M (x)

(d) Divide message 2^N M (x) by the polynomial.

$$\text{i.e. } \frac{2^N M(x)}{P(x)} = Q(N) + \frac{R(x)}{P(x)}$$

(e) Append the remainder of (d) to (c). This will be the transmit message
i.e $F(x) = 2^N M(x) + R(x)$.

At the receiver, the received message is again divided by P(x), and if there is no remainder the message is correctly received.

(f) $$\frac{F_{N+M}(x)}{P_N(x)} = Q(x) + Q_{N-1}$$

If the remainder is not equal to zero the message is having an error hence the receiver will request the transmitter to repeat the message.

3.2 Sensitivity of the error detection code

The receiver will fail to detect an error (E) if and only if received message is divisible by P, i.e. if and only if E is divisible by P. This seems an unlikely occurrence.

It can be shown that all of the following are not divisible by P and hence are detectable.

1. All single – bit error
2. All double – bit errors, as long as P (x) has a factor with at least three terms.
3. Any add number of errors, as long as P (x) contains a factor (X + 1).
4. Any burst error for which the length of the burst is less than the length of the FCS.
5. Most larger burst errors.

3.3 Formation of Check Bits

Procedure

Given an M bit message, assume 11001011101 the transmitter generates an N bit sequence (CRC or FCS) (say) so that resulting frame consists of (M + N) bits.

This is divided by some predetermined (P) number to see no errors.

Assume P = 110101 $X^5 + X^4 + X^2 + X^0 = P(X)$

Example of Module 2 Addition
1111
+ 1010
101 No Carry

In order to formulate the CRC the message of 11 bits (assume) has been shifted by 5 bits and the total modified message has been divided in modulo 2 division by the polynomial which is shown below

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

You will see the residual is 00100 and the quotient is 100101101

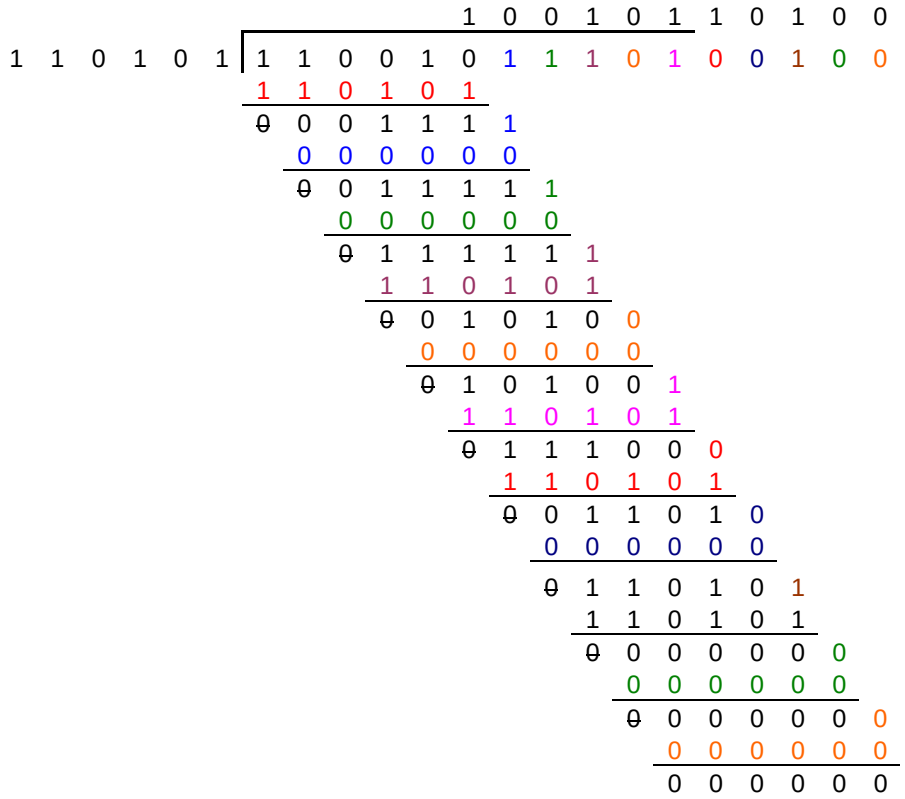
Hence transmit word: 11001011101 : 00100

what will happen at the receiver?

Assume these 15 bits are received at the receiver. Check for correctness.

Received bits are again divided with the same polynomial to see that there is no residual.

Assuming the same bits of message and the CRC – 1100101110 : 00100 is received at the receiver.



When the received bits are divided by modulo 2 with the same polynomial the residual of zero and the quotient of 10010110100 is obtained. The residual zero means the message has been received correctly (there are certain deviations for this and will be analyzed in the section 4.2 below).

3.4 Implementation

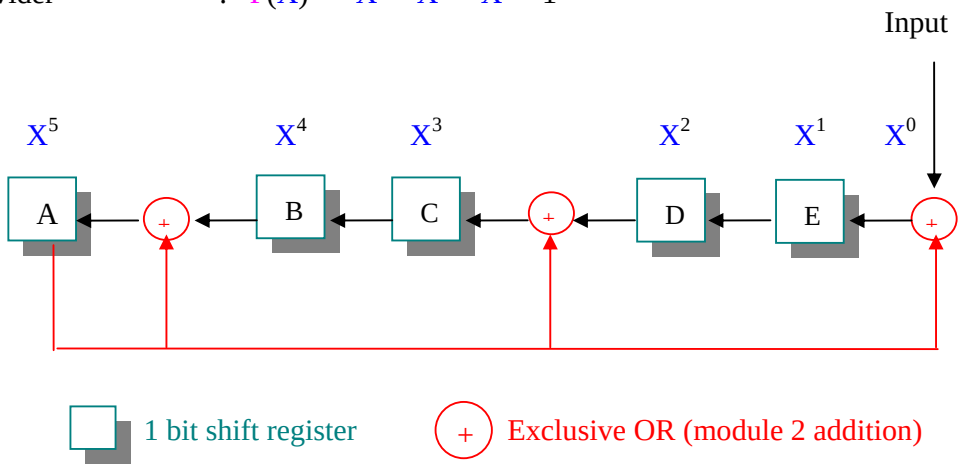
CRC process can easily be implemented as a dividing circuit consisting of exclusive OR gates and one bit shift registers. Implementation is as follows.

1. The input register contains N bit, equal to the length of the FCS.
2. There can be up to n exclusive OR gates.
3. The presence or absence of a gate corresponds to the presence of a term in the divisor polynomial other than to the major significant to the polynomial.
4. Always there is a feedback from the highest corresponding shift register to the input and the same feedback is fed to the other XOR gate, which is given below.

The above example

M = 110010 11101 : $M(X) = X^{10} + X^9 + X^6 + X^4 + X^3 + X^2 + 1$

Divider : $P(X) = X^5 + X^4 + X^2 + 1$



1 bit shift register + Exclusive OR (module 2 addition)

Contents of Shift Registers

	$(A_n \oplus B_n)$ A_{n+1}	(C_n) B_{n+1}	$(A_n \oplus D_n)$ C_{n+1}	(E_n) D_{n+1}	$(I_n \oplus A_n)$ E_{n+1}	I/P
STEP 0	0	0	0	0	0	0
1	0	0	0	0	0	1
2	0	0	0	0	1	1
3	0	0	0	1	1	0
4	0	0	1	1	0	0
5	0	1	1	0	0	1
6	1	1	0	0	1	0
7	0	0	1	1	1	1
8	0	1	1	1	1	1
9	1	1	1	1	1	1
10	0	1	0	1	0	0
11	1	0	1	0	0	1
12	1	1	1	0	0	0
13	0	1	1	0	1	0
14	1	1	0	1	0	0
15	0	0	0	0	1	0
16	0	0	0	1	0	0
17	0	0	1	0	0	

INF

Five Zeros

Frame check sequence

Note:

- Up to step 6 there is no effect from the feedback since the output A is 0.
- With the step 6 the outputs will be affected by the feedback with the following equations

$$E_{n+1} = I_n \oplus A_n$$
$$D_{n+1} = E_n$$
$$C_{n+1} = A_n \oplus D_n$$
$$B_{n+1} = C_n$$
$$A_{n+1} = A_n \oplus B_n$$

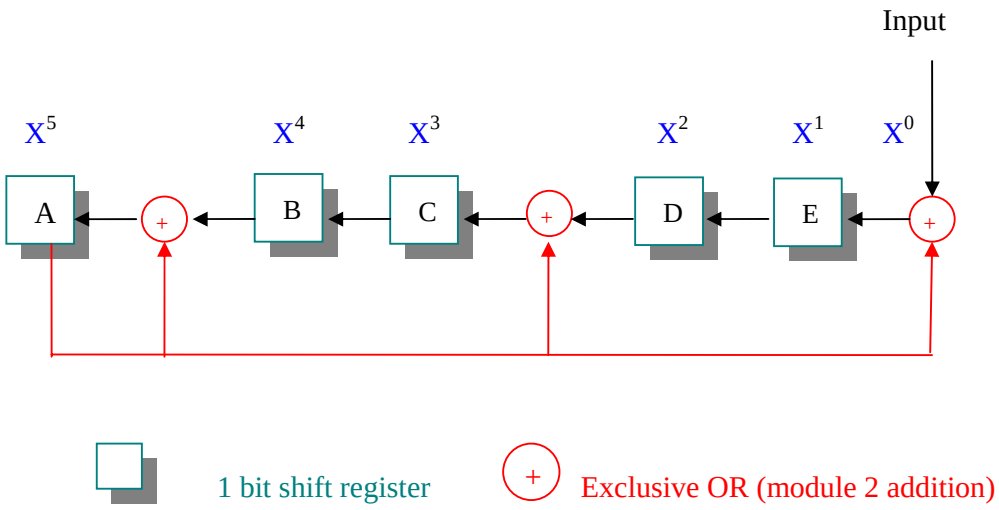
Note: From the above example you will find that only 5 shift registers are employed. Generally the number of shift registers required will be number of bits in the polynomial P less one. Exclusive-or gates should be included at the places where x terms occur, and always there should be a feedback from the highest term to the input exclusive or gate.

Receiver

At the receiver the same circuit deployed in the transmitter to formulate the CRC will be deployed. In this case the information will be the received message which has been transmitted from the transmitter M+R.

Process

1. At the zero clock pulse or step 0, all shift registers reset to zero.
2. From Step 1 the received message will be input, one bit at a time with the most significant bit.



Contents of Shift Registers

	$(A_n \oplus B_n)$		(C_n)	$(A_n \oplus D_n)$	(E_n)	$(I_n \oplus A_n)$	
	A_{n+1}	B_{n+1}	C_{n+1}	D_{n+1}	E_{n+1}	I/P	
STEP 0	0	0	0	0	0	0	
1	0	0	0	0	0	1	
2	0	0	0	0	1	1	
3	0	0	0	1	1	0	INF
4	0	0	1	1	0	0	
5	0	1	1	0	0	1	
6	1	1	0	0	1	0	
7	0	0	1	1	1	1	
8	0	1	1	1	1	1	
9	1	1	1	1	1	1	
10	0	1	0	1	0	0	
11	1	0	1	0	0	1	
12	1	1	1	0	0	0	CRC Bits
13	0	1	1	0	0	0	
14	1	1	0	1	0	1	
15	0	0	0	0	0	0	
16	0	0	0	0	0	0	
17	0	0	0	0	0		