Theoretical background of Cyclic Redundancy Code

Chapter 4

4.1 Background

Let us define

T = (k + n) bitframe to be transmitted (Transmitted message)
M = k bit message (actual message), the first k bits of T
R = n bit FCS, the last n bits of T
P = pattern of (n + 1) bits (polynomial)

The FCS is found by dividing the message M added with n 0's to the right of M by the polynomial P. Basically adding n 0's to M, shift the message M, n bits to the left. Therefore the new message is 2^nM.

Suppose that we divided 2^nM by P:

$$\frac{2^nM}{P} = Q \oplus \frac{R}{P}$$

Where Q = quotient
R = remainder

This remainder is the FCS. This is added to the message. Hence transmitted message

$$T = 2^nM \oplus R$$

The receiver divides the received message by the same polynomial.

i.e

$$\frac{T}{P} = \frac{2^nM \oplus R}{P}$$

$$= \frac{2^nM}{P} \oplus \frac{R}{P}$$

$$= Q \oplus \frac{R}{P} \oplus \frac{R}{P}$$

However, any binary number added to itself (modulo 2) yields zero. Thus

$$\frac{R}{P} \oplus \frac{R}{P} = 0 \text{ and hence } \frac{T}{P} = Q$$

There is no remainder and therefore T is exactly divisible by P. Thus the FCS is easily generated. Simply divide 2^nM by P and use the remainder as the FCS. On reception, the receiver will divide T by P and will get no remainder if there have been no errors.

4.2 Error Formats

The occurrence of an error can be easily expressed. An error results in the reversal of a bit. Mathematically, this is equivalent to taking the Exclusive-or of the bit and 1

$$\text{i.e} \quad 0 \oplus 1 = 1$$
$$1 \oplus 1 = 0$$

Example :

Let us assume T = 1111010101 and Tr = 1000001111

Therefore received message Tr is in error. The error

E = 0111011010

Hence to find the error, compare the relevant bits in two messages T and Tr. If they are the same there is no error and hence error bit is 0, whereas if they are different there is an error and hence error bit is 1.

Thus the errors in an (n + k) bit frame can be represented by an (n + k) bit field with 1's in each error position. The resulting frame Tr can be expressed as

$$Tr = T + E$$

Where T = transmitted frame
E = error pattern with 1's in positions where errors occur
Tr = received frame

The receiver can identify the errors given in section, but it fails to identify an error if the received signal is divisible by P. i.e and error equal to P itself.

Proof :

Let the received message be Tr = T + E, where $T = 2^nM + R$. At the receiver this is divided by P.

$$\frac{Tr}{P} = \frac{T + E}{P} = \frac{2^nM + R + E}{P}$$

$$= \frac{2^nM}{P} + \frac{R}{P} + \frac{E}{P}$$

$$= Q + \frac{R}{P} + \frac{R}{P} + \frac{E}{P}$$

$$= Q + \frac{E}{P} \qquad \left\{ \text{since } \frac{R}{P} + \frac{R}{P} = 0 \right\}$$

Therefore if E is divisible by P, then the remainder will be zero. Hence no error will be detected by the receiver.

4.2.1 Example:

Let T = 110010111010010, P = 110101 and
Tr = 110010111100111.

Therefore E = 000000000110101 which is same as P.

The method of finding error

(i) Compare the received message with the transmitted message
(ii) If there are no errors make the relevant bits 0, otherwise 1.
(iii) The error message will have the same digit length as T or Tr

To find whether the received message is in error Tr has to be divided by P.

```
                                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 1 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 1
                          1 1 0 1 0 1
                          -----------
                    0 0 0 0 0 0 0
                        0 0 0 0 0 0
                        -----------
                    0 0 0 0 0 0 0
                          0 0 0 0 0 0
                          -----------
Remainder (no error)- 0 0 0 0 0 0
```

Hence if the error is same as the polynomial, then it the error will not be detected at the receiver.

4.3 Summary

In addition to error-detecting codes, there are also error correcting codes. They are rarely used in data transmission, since data transmission generally uses bi-directional transmission. Error-correcting codes are used in some situation where retransmission is impractical for example broadcasting where there are many receiver to one transmitter. Also error-correcting codes find application in real time transmission where retransmission is not warranted. Example of such case is normal voice transmission.

Error correcting codes are referred to as forward error correction to indicate that the receiver, on its own, is correcting the error. Retransmission schemes, in contrast, are referred to as backward error correction, since the receiver controls the transmitter until the receiver receives the message without any error.

Cyclic Redundancy codes are widely applicable in everywhere of data transmission applications.