Sakil Mallick
Roll :- 001510501050
Computer Network Lab
JUCSE

1. Prove that x^n M(x) + C(x) is divisible by P(x)

Given a message to be transmitted: $(b_{k-1}b_{k-2} \ldots b_2b_1b_0)$

View the bits of the message as the coefficients of a polynomial
$M(x) = b_{k-1} x^{k-1} + b_{k-2} x^{k-2} + \ldots b_2 x^2 + b_1 x + b_0$

Multiply the polynomial corresponding to the message by x^n where n is the degree of the generator polynomial and then divide this product by the generator to obtain polynomials Q(x) and C(x) such that:
$x^n M(x) = Q(x) P(x) + C(x)$

Treating all the coefficients not as integers but as integers modulo 2.
Finally, treat the coefficients of the remainder polynomial, C(X) as "parity bits". That is, append them to the message before actually transmitting it.

Since the degree of C(x) is less than n, the bits of the transmitted message will correspond to the polynomial:
$x^n M(x) + C(x)$

Since addition and subtraction are identical in the field of integers mod 2, this is the same as
$x^n M(x) - C(x)$

From the equation that defines division, however, we can conclude that:
x^n M(x) - C(x) = Q(x) P(x)

In other words, if the transmitted message's bits are viewed as the coefficients of a polynomial, then that polynomial will be divisible by P(X).

2. Properties of CRC

Sent F(x), but received F'(x) = F(x)+E(x) Generator polynomial P(x)

a. Errors

- **Single Bit Error E(x) = x^i**
  If P(x) has two or more terms, P(x) will not divide E(x)

- **2 Isolated Single Bit Errors (double errors)**
  E(x) = x^i+x^j, i>j
  E(x) = $x^j(x^{i-j}+1)$
  Provided that P(x) is not divisible by x, a sufficient condition to detect all double errors is that P(x) does not divide (x^t+1) for any t up to i-j (i.e., block length)
- **Odd Number of Bit Errors**
  If x+1 is a factor of P(x), all odd number of bit errors are detected

- **Short Burst Errors**
  E(x) = $x^j(x^{t-1}+\ldots+1)$ (Length t ≤ n, number of redundant bits), starting at bit position j. If P(x) has an x^0 term and t ≤ n, P(x) will not divide E(x). All errors up to length n are detected

- **Long Burst Errors**
  E(x) = $x^j(x^{t-1}+\ldots+1)$ (Length t = n+1) Undetectable only if burst error is the same as P(x). P(x) = x^n+ … + 1 n-1 bits between x^n and x^0 E(x) = 1 + … + 1 must match
  Probability of not detecting the error is $2^{-(n-1)}$

- **Longer Burst Errors**
  E(x) = $x^j(x^{t-1}+\ldots+1)$ (Length t > n+1) Probability of not detecting the error is 2^{-n}

b. They can be easily implemented by hardware and software.

c. They are very fast when implemented in hardware.

3. When no errors are detected

Sent F(x), but received F’(x) = F(x)+E(x) Generator polynomial P(x)

When E(x) completely divides the generator polynomial, we can’t find an error.

This is because the receiver side sees that the remainder as expected is zero, and so no error is detected.