****
NAME : PRAMOD KUMAR
ROLL NO. : 03CS3019
STUDENT NO.:57
****

In CRC process we express all values as ploynomials in a dummy variable X,with binary coefficients. The coefficients correspond to the bits in the binary number.Thus ,for M=110011,we have M(X)=X^5+X^4+X+1, and ,for P=11001,we have P(X)=X^4+X^3+1.

The CRC process can now be described as :

X^n*M(X)/P(X)=Q(X)+R(X)/P(X)

T(X)=X^n*M(X)+R(X)

NOTE : An error E(X) will only be undetectable if it is divisible by P(X).

(1)all single bit errors are detectable ,if P(X) has more than one non-zero terms:

Let T(X) be the correct transmitted pattern, then it is divisible by P(X). Now let us assume that if T1(X) is the recieved pattern which has a single bit error, and it is also divisible by P(X).

Then error E(X)=|T(X)-T1(X)| is also divisible by P(X).

Since there is error in ony one of the recieved bits, so if E(X)=X^n and P(X)=X^m+X^l ,where n,m,l are contstants and n<m,l. Then E(X) is not divisible by P(X) as X^n is not divisible by X^m+X^l , Hence a contradiction, thus all single bit erors are detectable if P(X) has more than one non-zero terms.

Therefore the error E(X) is detectable as it is not divisible by P(X)

(2)All double bit errors are detectable, as long as P(X) has factor with three terms:

Let T(X) be the correct transmitted pattern, then it is divisible by P(X). Now let us assume that if T1(X) is the received pattern which has a double bit error, and it is also divisible by P(X).

Then error E(X)=|T(X)-T1(X)| is also divisible by P(X). since there are errors in two bits then if

E(X)=X^K1+X^k2 and P(X)=X^n1+X^n2+X^n3 ,where k1,k2 ,n1,n2 and n3 are constants and k1,k2 <n1,n2,n3.

Thus E(X) is not divisible by P(X).

Hence a contradiction, thus all double bit errors are detectable if P(X) has atleast three terms. Therefore the error E(X) is detectable as it is not divisible by P(X).

++++++++++++++++++++
BHABEN DEORI
ROLL NO. 03CS3020
Student No. 58
+++++++++++++++++++++

Let D(x) be the transmitted message and k be the degree of the FCS.
So we have:
x^k.D(x)=Q(x).P(x)+R(x) or x^k.D(x)-R(x)=Q(x).P(x)=T(x) is the transmitted bits which is divisible by P(x). During transmission some of the bits are damaged, the actual bits received will correspond to a different polynomial, T'(x).Now we compute:
E(x)=T(x)-T'(x), E(x) is the error pattern.

The coefficients of E(x) will correspond to a bit string with a 1 in each position where T(x) differed from T'(x) and 0's elsewhere. As long as T'(x) is not divisible by P(x),the CRC bits will enable us to detect errors. So we look into cases where T'(x) is divisible by P(x), or infact E(x) is divisible by P(x).

<u>3. Any odd number of errors, as long as P(X) contains a factor of (X+1)</u>
If T'(x) contains an odd number of inverted bits,then E(x) must contain an odd number of 1's. So E(1)=1.
If P(x) is a factor of E(x),then P(1) would also have to be 1.So if we make sure that P(1)=0, we can conclude that P(1) does not divide any E(x) corresponding to an odd number of error bits. In this case, a CRC based on P(x) will detect any odd number of errors. And As long as P(x) has some factor of the form $x^{(i + 1)}$, P(1) will equal 0. So, it isn't hard to find such a polynomial, x+1is such an example.

<u>4. Any burst error for which the length of the burst is less than or equal n-k, that is, less than or equal to the length of the FCS.</u>
Let a bust error affects some j consecutive bits for j less-then k. In this case the error polynomial will look like $E(x)=x^{n1}+x^{n2}+....+x^{nr}$.
We assume n_i greater-then n_i+1 for all i and n_1-n_r less-then j
$E(x)=x^{nr}(x^{(n1-nr)}+x^{(n2-nr)}+......+1)$.
Now $P(x)=x^{(k+1)}$ can't divide E(x) since it can't divide x^{nr} nor $x^{(n1-nr)}+x^{(n2-nr)}+....+1$.
So CRC based on the P(x) detects all burst errors of length less than its degree.

#####################
JOY DEEP NATH
(03CS3021)
Student no. 59
#####################

5. A fraction of error bursts of length n – k + 1; the fraction equals to $1 - 2^{-(n-k-1)}$

Consider now a burst error of length $\boldsymbol{n} - \boldsymbol{k} + 1$ represented by $\boldsymbol{e(x) = x^i (1 + e_1 x + \ldots + e_{n-k-1} x^{n-k-1} + x^{n-k})}$. Of the $\boldsymbol{2^{n-k-1}}$ possible error patterns of this form for each i, $0 <= \boldsymbol{i} <= \boldsymbol{k}-1$, only one error pattern, namely, $\boldsymbol{e(x) = x^i . g(x)}$, is undetectable. (Since $\boldsymbol{g(x)}$ is the generator function of the pattern)
The fraction of undetected burst errors of length $n - \boldsymbol{k} + 1$ is therefore $2^{-(n-k-1)}$. Hence the fraction of detected burst errors is $1 - 2^{-(n-k-1)}$.

6.A fraction of error bursts of length greater than n – k + 1; the fraction equals to $1-2^{-(n-k-1)}$

Similar consideration shows that the fraction of undetected burst errors of length greater than n –k+1 is $2^{-(n-k)}$, It can be proved as the error would be represented by $\boldsymbol{e(x) = x^i (1 + e_1 x + \ldots + e_{n-k-1} x^{n-k-1}} + e_{n-k} \boldsymbol{x^{n-k} + \ldots + e_{n-k+s} x^{n-k+s} + x^{n-k+s+1})}$, where s >0, or $\boldsymbol{e(x)} = \boldsymbol{x^i} (\boldsymbol{S(x)})$, where $\boldsymbol{S(x)} = 1 + \boldsymbol{e_1 x + \ldots + e_{n-k-1} x^{n-k-1}} + e_{n-k} \boldsymbol{x^{n-k} + \ldots + e_{n-k+s} x^{n-k+s} + x^{n-k+s+1}}$

Now breaking S(x) into imporper fractions, S(x) can be written as S(x)=Q(x).g(x) + R(x), where S(x) is in the order of n-k+s+2, Q(x) is of the order s+1 and R(x) is of the order of n-k+1. The only error pattern undetectable is $\boldsymbol{e(x)} = \boldsymbol{x^i} (\boldsymbol{Q(x).g(x)+g(x)})$, ie. $\boldsymbol{R(x)=g(x)}$.
Since $R(x) = 1 + \boldsymbol{f_1 x} + \ldots\ \boldsymbol{f_{n-k} x^{n-k}}$
Hence, there are $2^{(n-k)}$ possible error codes that will decide $\boldsymbol{R(x)}$. Hence the fraction of undetected burst errors of length greater than $n - \boldsymbol{k} + 1$ is therefore $2^{-(n-k-1)}$. Hence the fraction of detected burst errors is $1 - 2^{-(n-k-1)}$.

It is to be noted that fundamental role is played by the number of check bits n –k in the detection of burst errors.