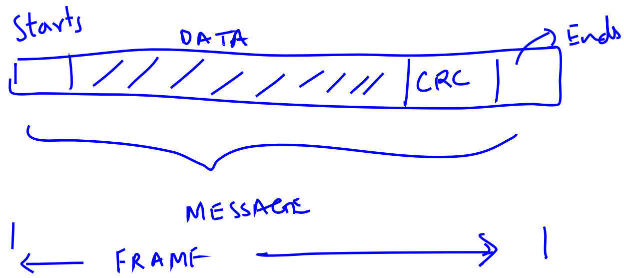
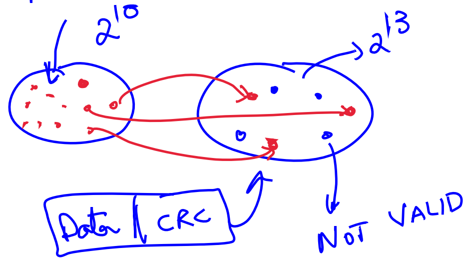


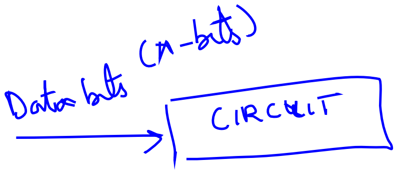
① CRC Easy to generate

② Messages of variable sizes

Support $n=10$ $k=3$



GENERATOR / DIVISOR



1101 Divisor GF(2)

GF(2) ADD / SUBTRACT → XOR

POLYNOMIAL REPRESENTATION

$$1101 \longrightarrow 1.x^3 + 1.x^2 + 0.x^1 + 1.x^0$$

$x^3\ x^2\ x^1\ x^0$

$$= x^3 + x^2 + 1 = C(x)$$

$$C(x)(1+x) = x^3 + x^2 + 1 + x^4 + x^3 + x$$

$$= x^4 + 1.x^3 + 1.x^3 + x^2 + x + 1$$

$$= x^4 + x^2 + x + 1$$

$$\begin{array}{r} 1101 \\ 11 \\ \hline \end{array} \rightarrow x+1$$

$$\begin{array}{rr} & 1101 \\ \oplus & 1101 \\ \hline & 10111 \end{array} \rightarrow x^4 + x^2 + x + 1$$

$x^4\ x^3\ x^2\ x\ x^0$

Codeword : $P(x) \longrightarrow$ 10011 . . . . $\underbrace{1101}_{CRC}$

Error : $E(x)$ 000 100

⇒ 3rd bit in error

RECEIVE = $P(x) + E(x)$

3rd & 5th bits in error ⇒ $E(x) =$ 0000...10100

5th 3rd

Divide received polyn. by $C(x)$ and if resultant is 0 then we say no bit errors

WANT $\dfrac{P(x)+E(x)}{C(x)} \neq 0$ if $E(x) \neq 0$

n+k bits

(i) SINGLE BIT ERRORS:

$E(x) = x^i$ for some 'i' ; $i \in \{0, 1, \ldots, n+k-1\}$

$C(x) = ?$ $\dfrac{P(x) + E(x)}{C(x)} = \cancel{\dfrac{P(x)}{C(x)}}^{\to 0} + \dfrac{E(x)}{C(x)}$

If $C(x) = x^k + \underbrace{\ldots\ldots}_{\text{anything (0s or 1s)}} + 1$

$C(x) \cdot D(x) = E(x)$ if $C(x)$ divides $E(x)$

$(x^k + \ldots + 1)\,(x^m + \ldots + x^q) \overset{?}{=} x^i$

$x^{k+m} + \ldots$ ✓ $+ x^q$ ✓ $\neq x^i$

1101

$x^3 + x^2 + 1$

(ii) Two-bit errors

$E(x) = x^j + x^i$, $(j > i)$

$= \underline{x^i}\,(\underline{x^{j-i} + 1})$

Write each polyn. as a product of irreducible polynomials.

$\dfrac{E(x)}{C(x)} = \dfrac{g_1(x)\, g_2(x) \ldots g_t(x)}{f_1(x)\, f_2(x) \ldots f_m(x)}$

Suppose $C(x)$ is of the form $x^k + \ldots + 1 \neq x^\beta(\ldots)$

then no $f_i(x)$ is of the form x^β for some β.

$$\frac{x^{i}\,(x^{j-i}+1)}{\underbrace{f_1(x)\cdots f_m(x)}_{C(x)}}$$

not going to cancel

$$\underbrace{(x^{k}+\cdots+1)}_{C(x)}(\cdots\cdots) = x^{r}+1 \text{ for large } r$$

$$\cdots 0\,0\,1\,0\,0\,0 \cdots 0\,1\,0\,0$$

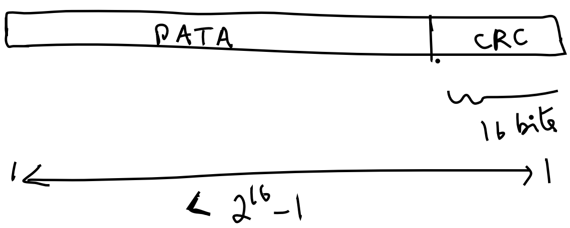
j $\quad$ i

$j-i$ is distance

Definition: The smallest r such that $C(x)$ divides $x^{r}+1$ is called its order (or exponent).

It is known how to find $C(x)$ of form $x^{k}+\cdots+1$ s.t. it has order $2^{k}-1$.

Suppose $k=16$; $C(x)=x^{16}+\cdots+1$; then we can find a $C(x)$ s.t. it will not divide $x^{p}+1$ for $p<2^{16}-1$



(iii) Odd numbers of errors

$$E(x) = \underbrace{x^{j}+x^{i}+\cdots}_{\text{odd \# terms}}$$

Claim: If $C(x)=(1+x)(\cdots\cdots)$ then $C(x)$ cannot divide $E(x)$

$E(x) \neq (1+x)\,G(x)$

$G \longrightarrow$ 0 1 1 1 0 . . . . 0 1 0 . . . . . 0 1 1 0 . . . . 0 1 $\times$ 1

1 1 1 0 $\quad$ 1 0 $\quad$ 0 1 1 0 $\quad$ 1 $\quad$ $\times$ x

1 0 0 1 $\quad$ 1 1 $\quad$ 1 0 1 $\quad$ 1 1 $\rightarrow$ Even # ones

$\rightarrow$ 2 ones

Claim: If $C(x)$ has an even number of terms then it will not divide $E(x)$ if $E(x)$ has an odd number of terms.

HDLC uses CRC-16-IBM

$$C(x) = x^{16} + x^{15} + x^{2} + 1$$

CRC-32 : $C(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$

ARQ