

4/19/07 (1)
Error-Detecting Codes

Cyclic Redundancy Code (CRC)
(Polynomial Code)

K-bit message:

The coefficient list for a polynomial with K terms ranging from x^{K-1} to x^0 .

Generator Polynomial

$G(x)$ agreed by sender and receiver

Example

$$G(x) = x^4 + x + 1$$

Generator (coefficients) 10011

Algorithm for Computing checksum

Message $M(x)$, Generator $G(x)$

≡

1. Append r zero bits to the low-order end of the message
i.e. $x^r M(x)$

r - degree of $G(x)$

2. Divide the bit string of $G(x)$ into the bit string of $x^r M(x)$ using modulo 2 division

3. Subtract (Add) the remainder R to the bit string of $x^r M(x)$.
Using modulo 2

Result $T(x) = x^r M(x) + R$
is the transmitted message.

Example

$$M(x) = x^9 + x^8 + x^6 + x^4 + x^3 + x + 1$$

(BS) Bit string 1101011011

$$G(x) = x^4 + x + 1$$

Bit string 10011

(BS) $xM(x) = 11010110110000$

10011 | 11010110110000

1100001010

10011

10011

10011

00001

00000

00010

00000

00101

00000

01011

00000

10110

10011

01010

00000

10100

10011

01110

01110

00000

R → 1110

$T(x) = 1101011011110$

01010

00000

10100

10011

01110