4/19/07
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) 1 0 0 1 1

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) $x^r M(x)$ = 1101011011 0000