

Polynomials in GF(2) and CRCs

no subtraction, only + & x
 $- \equiv +$

Exercise 1: Write the addition, subtraction and multiplication tables for GF(2). What logic function can be used to implement modulo-2 addition? Modulo-2 multiplication?

0, 1

+	0	1
0	0	1
1	1	0

XOR

x	0	1
0	0	0
1	0	1

AND

Exercise 2: What are the possible results if we used values 0 and 1 but the regular definitions of addition and multiplication? Would this be a field?

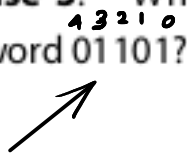
+	0	1
0	0	1
1	1	2

x	0	1
0	0	0
1	0	1

not a field

if use this definition of addition.

Exercise 3: What is the polynomial representation of the codeword 01101?



$$\underline{0}x^4 + \underline{1}x^3 + \underline{1}x^2 + \underline{0}x^1 + \underline{1}x^0 = x^3 + x^2 + 1$$

Exercise 4: What is the result of multiplying $x^2 + 1$ by $x^3 + x$ if the coefficients are regular integers? If the coefficients are values in $GF(2)$?

$GF(2)$
 $GF(64)$
 $GF(256)$
 are com

coefficients are regular integers

$$\begin{array}{r} x^2 + 1 \\ x^3 + x \\ \hline 1x^3 + 1x \\ 1x^5 + 1x^3 \\ \hline x^5 + 2x^3 + x \end{array}$$

not a coefficient from $GF(2)$

coefficients are from $GF(2)$

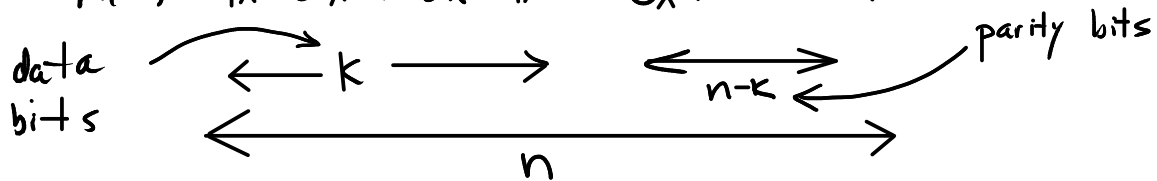
$$\begin{array}{r} x^2 + 1 \\ x^3 + x \\ \hline 1x^3 + x \\ x^5 + 1x^3 \\ \hline x^5 + 0x^3 + x \\ x^5 + x \end{array}$$

Exercise 5: If the generator polynomial is $G(x) = x^3 + x + 1$ and the data to be protected is 1001, what are $n - k$, $M(x)$ and the CRC? Check your result. Invert the last bit of the CRC and compute the remainder again.

$$G(x) = 1x^3 + 0x^2 + 1x + 1x^0$$

$$\text{CRC length} = n - k = 3 \text{ parity bits}$$

$$M(x) = 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x^1 + 0x^0$$



$$x^3 + 0x^2 + x + 1 \overline{) x^6 + 0x^5 + 0x^4 + x^3 + 0x^2 + 0x + 0}$$

writing only the coefficients:

$$\begin{array}{r}
 1011 \overline{) 1001000} \\
 \underline{1011} \\
 0100 \\
 \underline{1000} \\
 1011 \\
 \underline{0110} \\
 \text{remainder} \longrightarrow 110
 \end{array}$$

check:

$$\begin{array}{r}
 1011 \overline{) 1001110} \leftarrow \text{CRC} \\
 \underline{1011} \\
 0101 \\
 \underline{1011} \\
 1011 \\
 \underline{1011} \\
 0000 \\
 \underline{0000} \\
 \text{remainder is now zero}
 \end{array}$$

if the data (or CRC) changes:

$$\begin{array}{r}
 0061 \\
 \hline
 1011 \overline{)0001110} \\
 0011 \\
 \hline
 0111 \\
 1110 \\
 1011 \\
 \hline
 101
 \end{array}$$

changed this bit

remainder not zero.

Exercise 6: What is the probability that a randomly-chosen set of $n - k$ parity bits will match the correct parity bits for a given codeword? Assuming random data, what is the undetected error probability for a 16-bit CRC? For a 32-bit CRC? How long a CRC is required to guarantee detection of all single-bit errors?

$$\frac{1}{2^{n-k}} = \frac{1}{2}$$

- a 1-bit CRC - will detect all single-bit errors.
- is a parity bit
- $G(x) = x+1$ for even parity