Polynomials in GF(2) and CRCs

no subtraction, only + & ×

− ≡ +

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

×	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

not a field if use this definition of addition.

×	0	1
0	0	0
1	0	1

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

4 3 2 1 0

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

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

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

not a coefficient from GF(2)

coefficients are from GF(2)

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

$$x^5 + x$$

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.

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

CRC length $= n - k = 3$ parity bits

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

data bits $\longleftarrow k \longrightarrow$ $\longleftrightarrow_{n-k}$ parity bits

$\longleftarrow n \longrightarrow$

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

writing only the coefficients:

```
1011 ) 1001000
       1011
       --------
        0100
       --------
         1000
         1011
         ------
          0110
          ------
remainder ---> 110
```

check:

```
           1010
       -----------
1011 ) 1001 110   <- CRC
       1011
       ------
        0101
       ------
         1011
         1011
         ------
          0000
         ------
          0000
```

remainder is now zero

if the data (or CRC) changes:

```
         0 0 0 1
      ______________
 1011 ) 0 0 0 1 1 1 0
        _______
          0 0 1 1
        _________
            0 1 1 1
          _________
              1 1 1 0
              1 0 1 1
          _____________
                1 0 1
```

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?

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

a 1-bit CRC - will detect all single-bit errors.

- is a parity bit
- $G(x) = x+1$ for even parity