Polynomials in GF(2) and CRCs

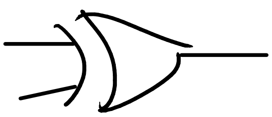
0-1

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?

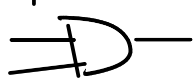
+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

? −	0	1
0	0	1
1	1	0



XOR



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

×	0	1
0	0	0
1	0	1

NOT A FIELD

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

$$0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0$$

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 $GF(2)$?

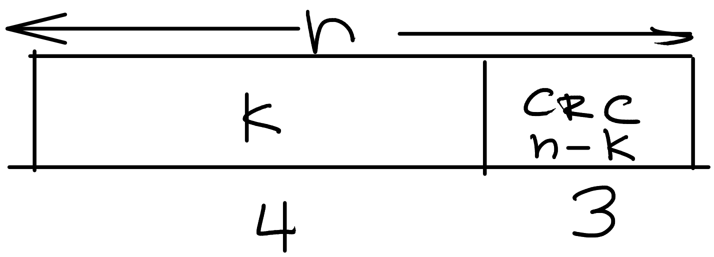
$$(x^2+1)(x^3+x) = x^5 + x^3 + x^3 + x$$

if coeff not $GF(2)$: $x^5 + 2x^3 + x$

if coff from $GF(2)$: $x^5 + x$

$K = 4$

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.



order of remainder $= 2$

$\therefore$ 3 bits in remainder (CRC)

$a x^2 + b x^1 + c x^0$

$n - k = 3$

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

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?