

Polynomials in $GF(2)$ and CRCs

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

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

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

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 $GF(2)$? Which result can be represented as a bit sequence?

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.

Exercise 6: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

Exercise 7: What is the probability that a CRC of length $n - k$ bits will be the correct CRC for a randomly-chosen codeword? Assuming random data, what is the undetected error probability for a 16-bit CRC? For a 32-bit CRC?