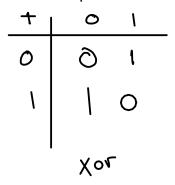
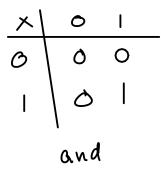
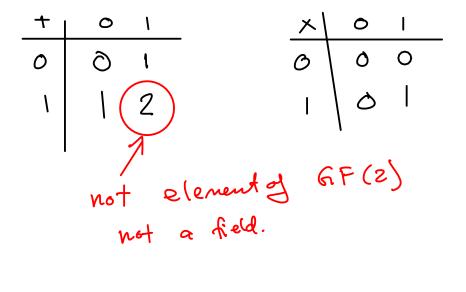
Polynomials in GF(2) and CRCs

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?

$$0 x + 1 x + 1 x + 0 x + 1 x^{\circ}$$

$$= x^{3} + x^{2} + 1$$

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)? Which result can be represented as a bit sequence?

 $x^{2}+1$ $x^{3}+x$ $x^{3}+x$ $x^{3}+x$ $x^{5}+x$ $x^{5}+x$ $x^{5}+2x^{3}+x$ $x^{5}+0x^{3}+x$ $= x^{5}+x$ $= x^{5}+x$

(23+2271) (2211)

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.

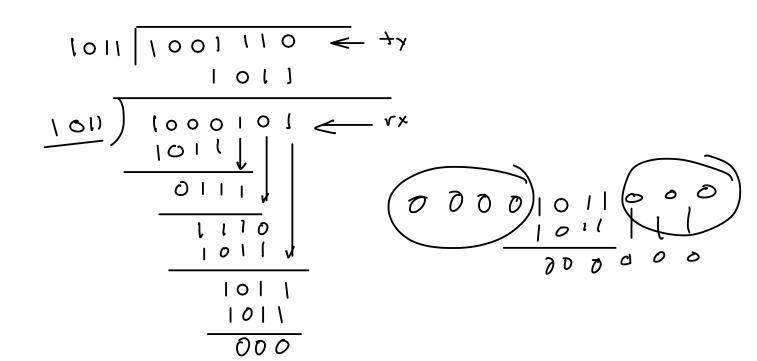
n-k is 3

$$\begin{array}{c|c}
 & 12 \\
\hline
 & 12 \\
\hline
 & 12 \\
\hline
 & 12 \\
\hline
 & 25 \\
\hline
 & 24 \\
\hline
\end{array}$$

$$\frac{145}{12} = 12 \text{ remainder } 1$$

000

0



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

gosnied a 32 bit G(x) sage? no: vandom evrors could be no typle a G(x) hat guarteral. **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?

16-bit CRC? For a 32-bit CRC?

$$32 \text{ bit} \text{ randomy chosen } CPC$$

$$UEP = \frac{1}{2^{32}} \text{ and } 0^{-9}$$