Lecture 10 - Polynomials in GF(2) and CRCs

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?

$$\begin{array}{c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
\hline
1 & 0 & 0
\end{array}$$

$$\begin{array}{c|c}
\times & 0 & 1 \\
\hline
0 & 0 & 0
\end{array}$$

$$\begin{array}{c|c}
\times & 0 & 1 \\
\hline
0 & 0 & 0
\end{array}$$

$$\begin{array}{c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 0
\end{array}$$

$$\begin{array}{c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 0
\end{array}$$

$$\begin{array}{c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 0
\end{array}$$

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?

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)?

$$(\chi^{2}+1)(\chi^{3}+\chi)$$

$$\rightarrow \chi^{5}+2\chi^{3}+\chi$$

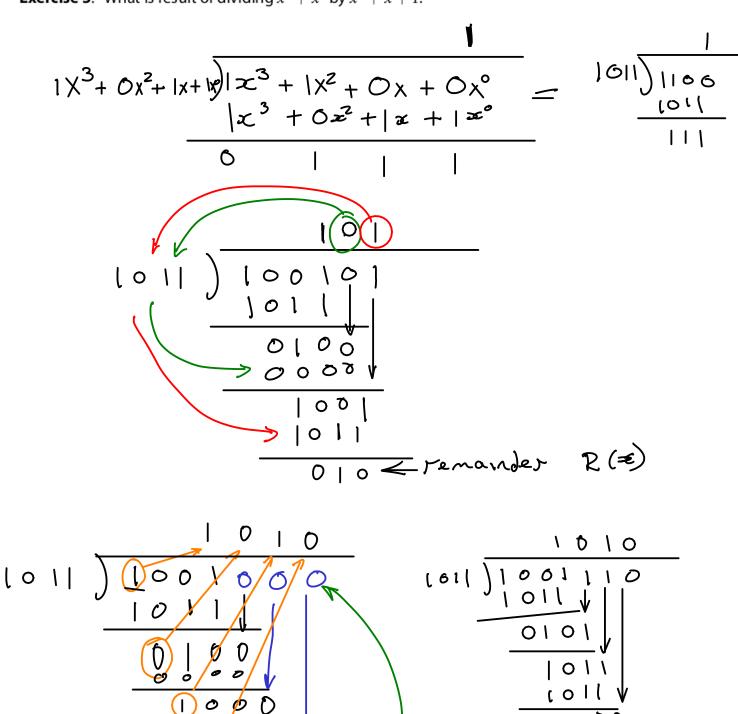
$$GF(2) \rightarrow \chi^{5}+0\chi^{3}+\chi=\chi^{5}+\chi$$

$$Integer animodic: $\frac{5}{3}=1$ ren $2$$$

if subtide remainder first, result always has remained o

$$\frac{5-2}{3} = \frac{5-2}{3}$$

Exercise 5: What is result of dividing $x^3 + x^2$ by $x^3 + x + 1$?



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?

there are
$$2^{n-k}$$
 possible $cecs$
only one is correct

i. prob. of the right cec is $\frac{1}{2^{n-k}}$

e.g. $n-k=16$ bits $\frac{1}{2^{16}}=10^{-4}$
 $32-bit cec$ $\frac{1}{2^{32}}=10^{-4}$