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?

not defined for GF(2), result is same as addition

+	0	1
0	0	1
1	1	0

$\equiv$ XOR

not 1

×	0	1
0	0	0
1	0	1

$\equiv$ 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, 2 (1+1)
- no, not closed under addition

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

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

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

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 $GF(2)$?

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

$$\rightarrow \quad x^5 + 2x^3 + x$$

$$GF(2) \rightarrow \quad x^5 + 0x^3 + x = x^5 + x$$

integer arithmetic: $\frac{5}{3} = 1 \text{ rem } 2$

if subtract remainder first, result always has remainder 0

$$\frac{5-2}{3} = 1 \text{ rem } 0.$$

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

$$
\begin{array}{r|l}
 & \qquad\qquad\qquad\qquad\qquad 1 \\
1x^3 + 0x^2 + 1x + 1 & 1x^3 + 1x^2 + 0x + 0x^0 \\
 & 1x^3 + 0x^2 + 1x + 1x^0 \\ \hline
 & 0 \quad 1 \quad 1 \quad 1
\end{array}
\quad = \quad
\begin{array}{r|l}
 & \quad 1 \\
1011 & 1100 \\
 & 1011 \\ \hline
 & \ \ 111
\end{array}
$$

$$
\begin{array}{r|l}
 & \qquad 101 \\
1011 & 100101 \\
 & 1011 \\ \hline
 & 0100 \\
 & 0000 \\ \hline
 & \ \ 1001 \\
 & \ \ 1011 \\ \hline
 & \ \ \ 010
\end{array}
$$

010 ← remainder $R(x)$

$$
\begin{array}{r|l}
 & \quad 1010 \\
1011 & 1001000 \\
 & 1011 \\ \hline
 & 0100 \\
 & 0000 \\ \hline
 & \ 1000 \\
 & \ 1011 \\ \hline
 & \ \ 0110 \\
 & \ \ 0000 \\ \hline
 & \ \ \ 110
\end{array}
\qquad\qquad
\begin{array}{r|l}
 & \quad 1010 \\
1011 & 1001110 \\
 & 1011 \\ \hline
 & 0101 \\ \hline
 & \ 1011 \\
 & \ 1011 \\ \hline
 & \ \ 0000 \\ \hline
 & \ \ \ \ \ 0
\end{array}
$$

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 CRCs

only one is correct

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

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

32-bit CRC $\quad \frac{1}{2^{32}} = 10^{-9}$