Lecture 11 - Fields 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?

+	0	1
0	0	1
1	1	0

XOR

×	0	1
0	0	0
1	0	1

AND

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?

+	0	1
0	0	1
1	1	2

×	0	1
0	0	0
1	0	1

no, with regular definitions 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 $GF(2)$? Which result can be represented as a bit sequence?

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

$x^5 + 2x^3 + x$ ← result w/ regular arith

$x^5 + 0x^3 + x$ ← if coeff in GF(2)

$$\begin{array}{r} 1x^3 + 0x^2 + 1x + 0 \\ 0x^3 + 1x^2 + 0x + 1 \\ \hline \end{array}$$

$$\begin{array}{rrrrrrr} & & & 1x^3 & 0x^2 & 1x^1 & 0x^0 \\ & & 0x^4 & 0 & 0 & 0 & \\ & 1x^5 & 0 & 1 & 0 & & \\ 0x^6 & 0 & 0 & 0 & 0 & & \\ \hline \end{array}$$

$$0x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 0x^0 = x^5 + x$$

$$\begin{array}{r} 123 \\ 25 \\ \hline 615 \\ 246 \\ \hline 3075 \end{array}$$

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.

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

$\times\ x^3$

$= 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x^1 + 0x^0$

$G(x) = 1x^3 + 0x^2 + 1x + 1$

(1011) 4 bits in $G(x)$

$\therefore\ n-k = 3$ bits

$M(x) = 1001\,\underline{000}$

$x^6 \div x^3 = x^3$

$$
\begin{array}{r|l}
 & \;\;1\;0\;1\;0 \\
\hline
1011 & 1\;0\;0\;1\;0\;0\;0 \\
 & 1\;0\;1\;1 \\
\hline
 & \;\;0\;1\;0\;0 \\
 & \;\;0\;0\;0\;0 \\
\hline
 & \;\;\;\;1\;0\;0\;0 \\
 & \;\;\;\;1\;0\;1\;1 \\
\hline
 & \;\;\;\;\;\;0\;1\;1\;0 \\
 & \;\;\;\;\;\;0\;0\;0\;0 \\
\hline
 & \;\;\;\;\;\;\;\;1\;1\;0
\end{array}
$$

$\dfrac{1001000}{1011} = 1010$ remainder 110

1011) 1001110

1011

0101

1011

1011

0000

000 ✓

1011) 10111110

1011

00011

0011

0110

110

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

yes. will detect up to 32 errors

no. may not be detected (but probably will be).

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?

$$\frac{1}{2^{n-K}}$$

$$\frac{1}{2^{16}} \approx \frac{1}{65\,\text{K}} \approx 10^{-5}$$

$$\frac{1}{2^{32}} \approx \frac{1}{4 \times 10^{9}} \approx 10^{-9}$$