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?

+	0	1
0	0	1
1	1	0

XOR

x	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
1	(2)	

∴ not a field with conventional definition of +

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

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

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

$$\begin{array}{r} x^2 + 1 \\ \times\ x^3 + x \\ \hline x^3 \quad\quad x \\ x^5 \quad x^3 \\ \hline x^5 + 2x^3 + x \end{array}$$

can't represent as bit

if operations in GF(2): $x^5 + x$

100010

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.

$n-k$ ← $1x^3 + 0x^2 + 1x^1 + 1x^0$

1011

$n-k = 3$ ∴ 3-bit CRC

$M = x^3 + 1 \times x^{3 \leftarrow n-k} = x^6 + x^3 = 1001000$

$$\frac{M}{G} = \frac{x^6 + x^3}{1x^3 + 0x^2 + 1x^1 + 1x^0} = \frac{1001000}{1011}$$

$$\begin{array}{r|l}
x^3 + 0x^2 + x + 1 & 1x^3 + 0x^2 + x \\
\hline
x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0 & \\
x^6 + 0x^5 + 1x^4 + 1x^3 & \\
\hline
0x^5 + 1x^4 + 0x^3 + 0x^2 & \\
x^4 + 0x^3 + 0x^2 + 0x & \\
x^4 + 0x^3 + 1x^2 + x & \\
\hline
0x^3 + 1x^2 + x + 0 & \\
= x^2 + x + 0 &
\end{array}$$

R = 110

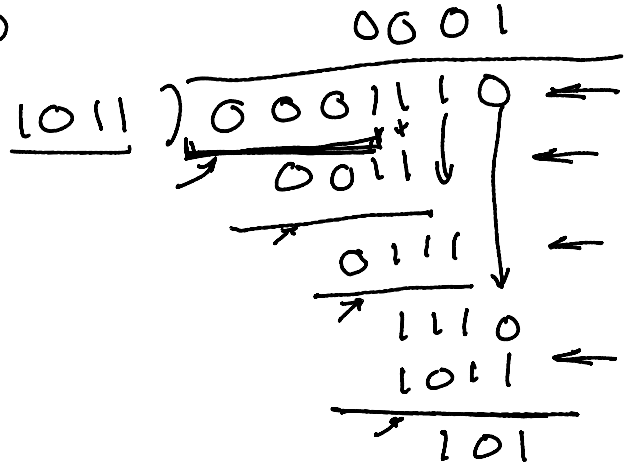
1001000
+ 111
1001110 ← divisible by G

data CRC

$$\begin{array}{r}
101 \\
1011 \overline{)1001110} \\
1011 \\
\hline
0101 \\
1011 \\
\hline
1011 \\
1011 \\
\hline
0000
\end{array}$$

transmit → 1001110

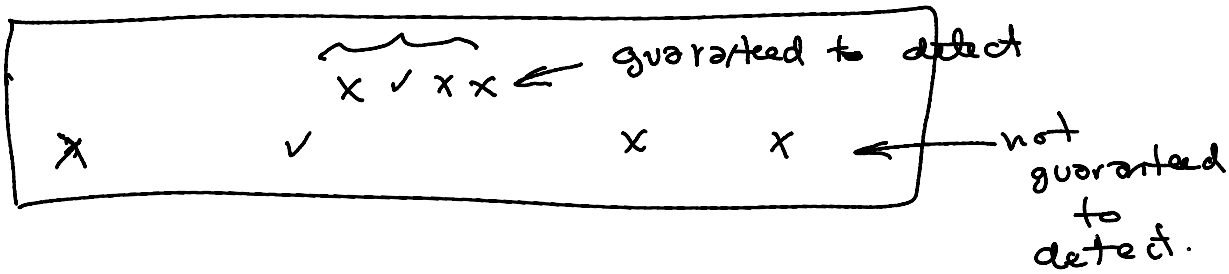
receive 0001110



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

$x^{32} + x^{31} + x^{30} + \dots + x^0$ (32 bits)

- $n-k = 32$ so 32-bit CRC will detect 30 consecutive error. yes $30 < 32$
- 30 error would not be detected if they were a multiple of $G(x)$ (this is unlikely)



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?

$\frac{1 \leftarrow \text{correct CRCs}}{2^{n-k} \leftarrow \text{possible values received for CRC}}$

for $n-k = 16$ $\quad \frac{1}{65536} \approx > 10^{-5}$

$n-k = 32$ $\quad \approx < 1 \times 10^{-9}$