

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

\times	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

x	0	1
0	0	0
1	0	1

not element of $GF(2)$
not a field.

Exercise 3: What is the polynomial representation of the code-word 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 $GF(2)$? Which result can be represented as a bit sequence?

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

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

$$\begin{array}{r}
 x^2 + 1 \\
 x^3 + x \\
 \hline
 x^5 + x^3 + x \\
 x^5 + x^3 + x \\
 \hline
 x^5 + 0x^3 + x \\
 = x^5 + x
 \end{array}$$

$$\begin{array}{r}
 1011 \overline{) 1001110} \leftarrow xy \\
 \underline{1011} \\
 0000101 \leftarrow rx \\
 \underline{1011} \downarrow \\
 0111 \downarrow \\
 \underline{1110} \downarrow \\
 1011 \downarrow \\
 \underline{1011} \\
 000
 \end{array}$$

$$\begin{array}{r}
 \textcircled{0000} \mid 0111 \quad \textcircled{000} \\
 \underline{1011} \mid 111 \\
 000 \mid 000
 \end{array}$$

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

randomly
30
11111...111
Yes: 30 errors is not a multiple of
a 32 bit $G(x)$
guaranteed
to
detect

10010011001
no: random errors could be multiple of $G(x)$
& undetectable
not guaranteed.

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?

32 bit randomly chosen CRC

$$\text{UEP} = \frac{1}{2^{32}} \approx 10^{-9}$$