Lecture 10 - GF(2) and CRCs

$\frac{0-1}{2} = \frac{-1}{2}$ 0 remainder -1

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 subtraction? Modulo-2 multiplication?

+	0	1
0	0	1
1	1	0

XOR

−	0	1
0	0	1
1	1	0

XOR ?

X	0	1
0	0	0
1	0	1

AND

fields only define 2 operations + & X this is the same as addition.

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
0	0	1
1	1	2

2 not element of GF(2)

X	0	1
0	0	0
1	0	1

NO, not a field if use conventional operations.

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

$x^0 = 1$

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

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

$$\left(0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0\right) \times x^8$$

$$0x^{12} + 1x^{11} + 1x^{10} + 0x^9 + 1x^8 + \underbrace{0x^7 + \cdots + 0x^0}$$

additional 8 terms generated by multiplying by x^8

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 $GF(2)$?

$$\begin{array}{r} x^2 + 1 \\ x^3 + x \\ \hline x^3 + \quad + x \\ x^5 \quad x^3 \\ \hline x^5 \quad 2x^3 \quad x \end{array} \leftarrow \text{regular addition}$$

$x^6 + 0x^3 + x \leftarrow GF(2)$ addition (modulo-2)

$$\begin{array}{r} 16 \\ \hline 20\overline{)323.} \\ 20\downarrow \\ \hline 123\downarrow \\ 120 \\ \hline 3.0 \end{array}$$

$$\begin{array}{r} 0 \\ 32\overline{)\,23} \\ 23 \end{array}$$

$$\begin{array}{r} 3 \\ 16\overline{)\,52} \\ 48 \\ \hline 4 \end{array}$$

3 remainder 4

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

$$\begin{array}{r} 1 \leftarrow Q(x) \\ \hline x^3+0x^2+1x+1x^0 \;\big)\; 1x^3 + 1x^2 + 0x + 0x^0 \\ \quad 1x^3 + 0x^2 + 1x + 1x^0 \\ \hline 0x^3 + 1x^2 + 1x + 1x^0 \end{array}$$

M(x) — G(x) — R(x)

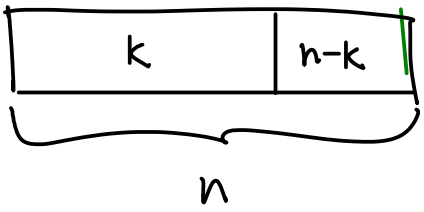
$$\begin{array}{r} 1x^3 + 1x^2 + 1x^1 + 0x^0 \\ \hline x^3+0x^2+1x+1x^0 \;\big)\; 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 0x^1 + 0x^0 \\ \quad 1x^6 + 0x^5 + 1x^4 + 1x^3 \\ \hline \quad 1x^5 + 1x^4 + 1x^3 + 0x^2 \\ \quad 1x^5 + 0x^4 + 1x^3 + 1x^2 \\ \hline \qquad 1 \quad 0 \quad 1 \quad 0 \\ \qquad 1x^4 + 0 \quad 1 \quad 1 \\ \hline +0x^3 + 0x^2 + 1x^1 + 0x^0 \end{array}$$

R(x)

Message: 1 1 0 0

CRC: 0 1 0

Exercise 6: What is the probability that a randomly-chosen (→ noise-like data) 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?



$$P(\text{false correct CRC}) = \frac{1}{2^{n-k}}$$

for 16-bit CRC $\quad n-k = 16 \quad \frac{1}{2^{16}} \approx 10^{-5}$

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