Lecture 9 - 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?

A

+	0	1
0	0	1
1	1	0

B

$\oplus$

(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?

as above, but 1+1=2
this is not a field because addition is not closed
(the results are not values in the field)

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

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

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

				0	0	0
			1	0	1	
		0	0	0		
	1	0	1			
regular addition →	1	0	2	0	1	0
GF(2) addition (XOR) →	1	0	0	0	1	0 ← this can be bits.

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

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.

$n - k = 3$ (1 less than number of bits in $G(x)$)

order of remainder is less than order of $G(x)$

order of CRC is $\underbrace{\_\,x^2 + \_\,x^1 + \_\,x^0}_{CRC}$

$$M(x) = \underbrace{1 \quad 0 \quad 0 \quad 1}_{data} \; \underbrace{\underline{0} \quad \underline{0} \quad \underline{0}}_{CRC}$$

$$\frac{M(x)}{G(x)} = \frac{1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0x^0}{1x^3 + 0x^2 + 1x + 1x^0}$$

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

$1x^3 + 0x^2 + 1x + 1x^0 \,\big)\, 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0x^0$

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

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

0 0 0 0

1 0 0 0

1 0 1 1

0 1 1 0 $R(x) = CRC$

0 0 0 0

$1x^2 + 1x + 0$

check at receiver:

$$\frac{M(x) + k\,G(x) + R(x)}{G(x)}$$

```
              1 0 1 0
       ________________
1011 ) 1 0 0 1 1 1 0
       1 0 1 1
       -------
         0 1 0 1
         -------
           1 0 1 1
           1 0 1 1
           -------
             0 0 0 0
             -------
               0 0 0
```

```
              1 0 1 1
       ________________
1011 ) 1 0 0 0 1 1 0
       1 0 1 1
       -------
         0 1 1 1
         -------
           1 1 1 1
           1 0 1 1
           -------
             1 0 0 0
             1 0 1 1
             -------
               0 1 1
```

error! remainder not zero

Exercise 6: 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?

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

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

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

Exercise 7: How long a CRC is required to guarantee detection of all single-bit errors? Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

a CRC of length n-k can detect n-k errors

for 1 error n-k = 1

yes. will detect up to 32 errors

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