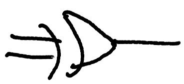
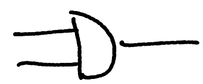
Polynomials in GF(2) and CRCs

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

×	0	1
0	0	0
1	0	1

XOR 

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

NOT A FIELD

NO CLOSURE.

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?

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

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

$$\begin{array}{rrrrrrr} & & & 0 & 1 & 0 & 1 \\ & & & 1 & 0 & 1 & 0 \\ \hline & & & 0 & 0 & 0 & 0 \\ & & 0 & 1 & 0 & 1 & \\ & 0 & 0 & 0 & 0 & & \\ 0 & 1 & 0 & 1 & & & \\ \hline 0 & 1 & 0 & 2 & 0 & 1 & 0 \end{array}$$

x^5+x ← if coefficients from GF2 → 0 1 0 0 0 1 0

How to make remainder zero:

$\frac{7}{3}$ 2 remainder 1

$\frac{7-1}{3} = 2$ remainder $\emptyset$

$\frac{5}{3} = 1$ remainder 2

$\frac{5-2}{3} = 1$ remainder $\emptyset$

$\frac{5-2+1}{3} = 1$ remainder

1011

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.

$k=4 \quad n-k=3$

$$\underbrace{\boxed{1001}\boxed{\_\ \_\ \_}}_{n}$$

$n-k = ?$

$G(x) = 1x^3 + 0x^2 + 1x + 1x^0$ (4 terms).

∴ remainder has 3 terms.

$n-k = 3$

$M(x) = (1x^3 + 0x^2 + 0x + 1x^0)\,x^3$

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

$M(x) = 1001000$

$1x^3 \quad 0x^2 \quad 1x \quad 0x^0$

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

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

$0x^5 \quad 1x^4 \quad 0x^3 \quad 0x^2$

$0 \quad 0 \quad 0 \quad 0$

$1 \quad 0 \quad 0 \quad 0$

$1x^4 \quad 0 \quad 1 \quad 1x$

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

$0 \quad 0 \quad 0 \quad 0$

$1 \quad 1 \quad 0$

$M = \underbrace{1001}_{\text{data}}\ \underbrace{110}_{\text{CRC}}$

check to see if M is divisible by G?

```
          1010
1011 ) 1001110
       1011
        0101
        0000
         1011
         1011
          0000
          0000
           000   ← remainder is zero ∴
```

M is multiple of G

$\frac{7}{3}$

$\frac{6}{3}$

$\frac{9}{3}$ $\frac{12}{3}$ $\frac{3}{3}$

```
1011 ) 0101110
       0000
        1011
        1011
         0001
         0000
          0010
          0000
           010
```

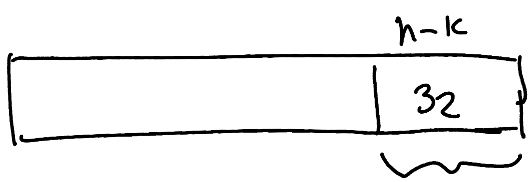
```
1011 ) 0010110
        0101
         1011
         1011
          0000
          0000
           000
```

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

yes. 32-bit CRC will detect up to 32 consecutive errors.

No. 30 errors could span $\geq$ 32 bits & might be a multiple of $G(x)$

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?



$$\underbrace{2 \times 2 \times \cdots \times 2}_{2^{32}}.$$

$$P(\text{undetected error}) = \frac{1}{2^{n-k}}$$

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

16 $\quad \frac{1}{2^{16}} \approx 10^{-4}$