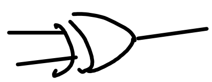
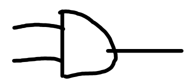
Polynomials in GF(2) and CRCs

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

x	0	1
0	0	0
1	0	1





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?

addition : 0, 1, 2 → not closed → not a field

multiplication: 0, 1

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?

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

$$+0 \cdot 1x^{0+2} + 0 \cdot 0x^{0+1} + (1 \cdot 0)x^{0+0}$$

$$1 \cdot 1 x^{1+2} + 1 \cdot 0 x^{1+1} + 1 \cdot 1 x^{1+0}$$

← ignore

$$1 \cdot 1 x^{3+2} + 1 \cdot 0 x^{3+1} \quad 1 \cdot 1 x^{3+0}$$

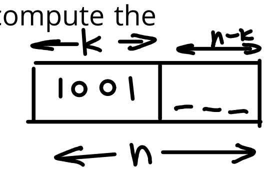
$$x^5 + 2x^3 + x^1$$

If regular addition

$$x^5 + \quad + x$$ ← w/ GF(2) addition

$$\underbrace{1 + 1} + 1 = 1$$

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.



$n-k = 3$

1001

$M(x) = (1x^3 + 0x^2 + 0x + 1) \cdot x^3 = 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0$

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

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

....

```
              1 0 1 0
        -------------------
1 0 1 1 ) 1 0 0 1 0 0 0
          1 0 1 1
          -------
            0 1 0 0
            0 0 0 0
            -------
              1 0 0 0
              1 0 1 1
              -------
                0 1 1 0
                0 0 0 0
                -------
                  1 1 0
```

1011) 1001110

1011

0101

1011

1011

0000

000

1011) 1001 ~~1~~ 10

1011 0

0100

1001

1011

0100

100

1011) 1001110

1011

0010110

1011) 0010110

0101

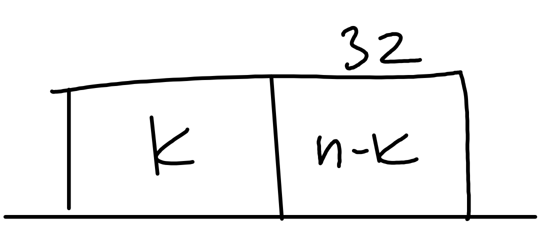
1011

1011

0000 0

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

Yes. $n-k = 32 > 30$ so can detect this error burst.



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?

$$\text{prob.} = \frac{1}{2^{n-k}}$$

$$n-k = 16 \qquad \frac{1}{2^{16}} = \frac{1}{65536} \approx 10^{-4}$$

$$n-k = 32 \qquad \frac{1}{2^{32}} \approx \frac{1}{4\times10^{9}} \approx 1\times10^{-9}$$

Exercise 3: A (5,3) code computes the two parity bits as: $p_0 = d_0 \oplus d_1$ and $p_1 = d_1 \oplus d_2$ where d_i is the i'th data bit. What codeword is transmitted when the data bits are $(d_0, d_1, d_2) = (0, 0, 1)$? How many different codewords are there in the code? What are the first four codewords? In general, how many codewords are there for an (n, k) code?

$$(d_0, d_1, d_2, P_0, P_1) \qquad k = 3 \quad n = 5$$