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?

$\oplus$	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?

if $1+1=2$ $\therefore$ not a field

not one of the allowed values

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?

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

$2x^3$

If coefficients were regular integers

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

or: 1 0 0 0 1 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.

$1001 \equiv 1x^3 + 0x^2 + 0x + 1x^0$

$G(x) = 1x^3 + 0x^2 + 1x + 1x^0 \equiv 1011$

$n-k = 3$ (parity bits, one less than # bits in $G(x)$)

$M(x) = (1x^3 + 0x^2 + 0x^1 + 1x^0)\, x^{\overset{n-k}{3}}$

$= 1x^6 + 0x^5 + 0x^4 + 1x^3 + \underbrace{0x^2 + 0x^1 + 0x^0}$

$G(X)$

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

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

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

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

Using only the coefficients:

1011) 1001000 ← $M(x)$

$G(x)$

1011

0100

0000

1000

1011

0110

0000

110 ← $R(X)$

check:

$$\underbrace{1011}_{G(x)} \,\big)\, 1001\ \underbrace{110}_{CRC}$$

1011

0101

1011

1011

0000

000 ← no error

add an error & check again:

1011) 1001111 ← error

1011

0101

0000

1011

1011

0001

001 ← error

```
1001110    ← original polynomial

1011       ← error polynomial
             = G(x) · x^3

      _______________
1011 ) 0010110        ← received polynomial
       0000
       ----
        0101
        0000
        ----
         1011
         1011
         ----
          0000
          0000
          ----
           000        no remainder: CRC incorrectly
                      indicates no error
```

example where error polynomial is

a multiple of $G(x)$ $= G(x)x^3 + G(x) = G(x)(x^3+1)$

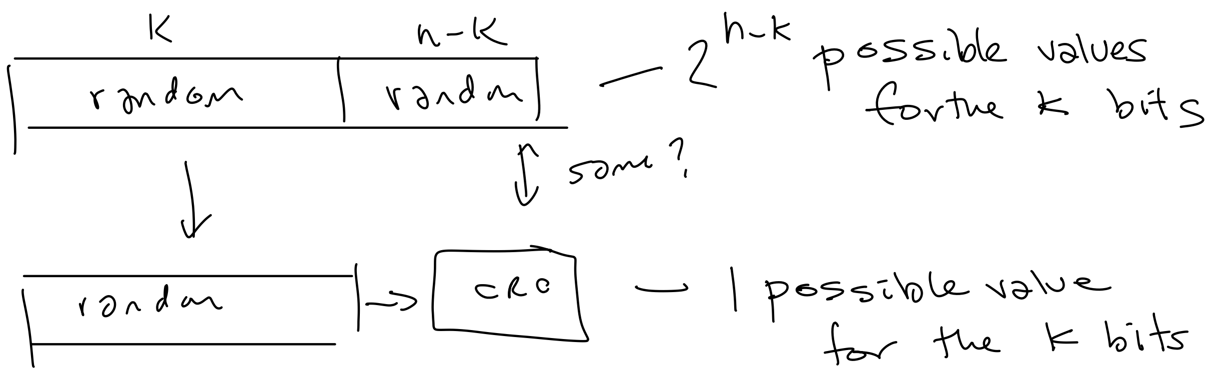
```
   1011
+     1011
  ---------
  1010011   ← error
  1001110   ← original
      ________
  1011 ) 0011101    ← received
         ----
          0111
          ----
           1110
           1011
           ----
            1011
            1011
            ----
             000    ← no remainder
```

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

yes 30 is an error burst length < n-k (32).

No. the errors could be a multiple of the generator polynomial.

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?



$$U.E.P. = \frac{1}{2^{n-k}}$$

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

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