Lecture 10 - Fields in GF(2) and CRCs - Answers to Lecture Exercises

Exercise 1: 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

x	0	1
0	0	0
1	0	1

2 ← not element of GF(2) ∴ not a field

Exercise 2: What logic function can be used to implement modulo-2 addition? Modulo-2 subtraction? Modulo-2 multiplication?

modulo2 addition: mod(a + b, 2)   (a+b) % 2

XOR

⊕	0	1
0	0	1
1	1	0

−	0	1
0	0	1
1	1	0

AND

x	0	1
0	0	0
1	0	1

mod(0 − 1, 2) 1

mod(−1, 2)

$$2\overline{)\,-1\,}\ \text{quotient } 0,\ \text{remainder } 1$$

(−1 % 2) = 1

(−1 & 1) = 1

−1   1 1 1 1 1 1 . .

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 $GF(2)$?

$$(x^2+1)(x^3+x) = x^2 \cdot x^3 + x^2 \cdot x + 1 \cdot x^3 \cdot 1 \cdot x$$

$$= 1x^5 + 1x^3 + 1x^3 + 1x$$

if coefficients are integers:

$$= x^5 + 2x^3 + x$$

if coefficients are in $GF(2)$;

$$\cancel{= x^5 + 2x^3 + x}$$

or ? $\cancel{= x^5 + 1x^3 + x}$

or ? $= x^5 + 0x^3 + x$ ← RIGHT

$\uparrow$ $1 \oplus 1$

$$x^5 + x$$

$$\downarrow$$

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

$$\Rightarrow [1\ 0\ 0\ 0\ 1\ 0]$$

−	0	1
0	0	1
1	1	0

Exercise 6: What is result of dividing $x^3 + x^2$ by $x^3 + x + 1$?

$G(x)$

$$
\begin{array}{r|l}
 & 1 \\
\hline
1x^3 + 0x^2 + 1x^1 + 1x^0 & 1x^3 + 1x^2 + 0x + 0x^0 \quad \leftarrow M(x) \\
 & \oplus \; 1x^3 + 0x^2 + 1x + 1x^0 \\
\hline
 & 0x^3 + \boxed{1x^2 + 1x + 1x^0} \quad \leftarrow R(x)
\end{array}
$$

equivalent in GF2

$\oplus \equiv -$

$+ \equiv$

intermediate result

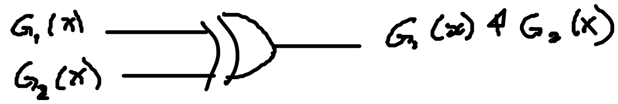
$$
\begin{array}{r|l}
 & \;\;29 \leftarrow \\
\hline
11 & 323 \leftarrow M \\
 & 22 \\
\hline
 & 103 \\
 & \;\;99 \\
\hline
 & \;\;\;4 \leftarrow R
\end{array}
$$

$G \nearrow$

be careful,
there are
many differences
between integer &
GF(2) polynomial
division.

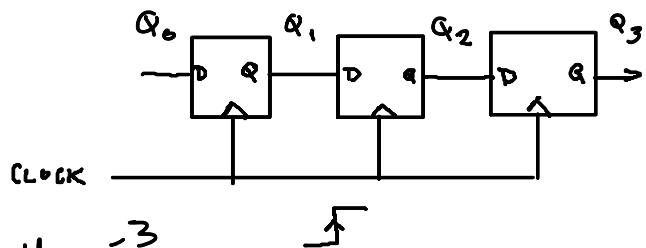
$$
\begin{array}{r|l}
 & \;\;110 \\
\hline
11 & 1011 \\
 & 11 \\
\hline
 & \;\;11
\end{array}
$$

Exercise 5: Draw the schematic of a circuit that sequentially adds two polynomials. A circuit that multiplies the input by x^3. A circuit that multiplies the input by $x^2 + x$.



$G_1(x) = 0, 1, 1, 0 \quad = 1x^2 + 1x$

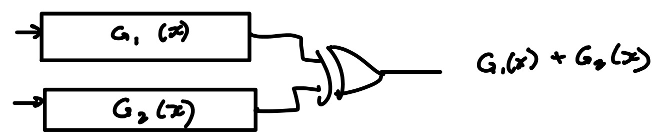
$G_2(x) = 0, 0, 1, 1, \quad = 1x + 1x^0$



Q_3	Q_2	Q_1	Q_0
0	0	0	1
0	0	1	X
0	1	X	Y

a delay of 3 is actually multiplication by x^{-3}

multiplying by



$(x^2 + x)\,x^3 = x^5 + x^4$

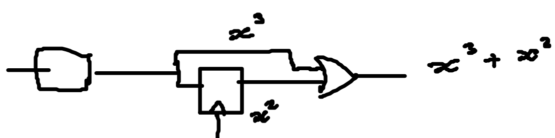
$1x^2 + 1x^1 + 0x^0$

$(1, 1, 0)$

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

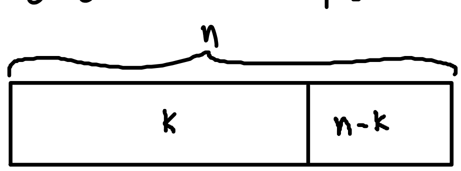
$1x^3 + 0x^2 + 0x^1 + 0x^0$

$(1, 0, 0, 0)$



$x^2 \cdot x^3 = x^5$

1 0 0 $\qquad$ 1 0 0 0 0 0



$\frac{7}{3} = 2 + 1$

$\frac{7-1}{3} = \frac{6}{3} = 2 r 0$

$$\begin{array}{r} 100 \\ +\ 01 \\ \hline 101 \end{array}$$

$\frac{9}{3} = 3 r 0$

Exercise 7: What is the probability that a randomly-chosen 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?

there are 2^{n-k} possible CRCs

$\therefore$ if randomly chosen, probability of matching $= \frac{1}{2^{n-k}}$

for a 16-bit CRC $= \frac{1}{2^{16}} \approx \frac{1}{65000} \approx 15 \times 10^{-6}$

32-bit $= \frac{1}{2^{32}}$ $\frac{1}{4 \times 10^{9}} \approx 0.25 \times 10^{-9}$

~~Exercise 6: What is result of dividing~~ $\underline{x^3+x^2}$ by $\underline{x^3+x+1}$?

Example of Computing CRC:

data: $x^3 + x^2 \equiv 1100$ $\qquad$ $\underline{k=4}$

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

4-bit $G(x)$ $\qquad$ 3-bit CRC (remainder)

$n-k = 3$

$n = n-k+k = 3+4 = 7$

form $M(x)$ by mutiplying by $x^{n-k} = x^3$

$M(x) = (x^3 + x^2)\,x^3 = x^6 + x^5$

or appending $n-k$ zeros:

$\underline{11}\,00\,\underline{000}$ $\qquad (1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 0)$

then compute remainder using modulo-2 operations:

```
          1 1 1 0
1 0 1 1 ) 1 1 0 0 0 0 0
          1 0 1 1
          -------
            1 1 1 0
            1 0 1 1
            -------
              1 0 1 0
              1 0 1 1
              -------
                0 0 1 0
                0 0 0 0
                -------
                  0 1 0  ← remainder is the CRC
```

message transmitted is data + CRC:

$\underbrace{1100}_{\text{DATA}}\underbrace{010}_{\text{CRC}}$

receiver checks for errors by dividing by G(x) & checking remainder:

```
            1110
1011 ) 1100010
       1011
       ----
        1110
        1011
        ----
         1011
         1011
         ----
          0000
          0000
          ----
             0  <- remainder is zero -> no errors
```