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

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?

+	0	1
0	0	1
1	1	2

∴ not a (Galois) field

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?

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

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

1 0 2 0 1 0

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

$= x^5 + x$

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

1 0 0 0 1 0 ✓

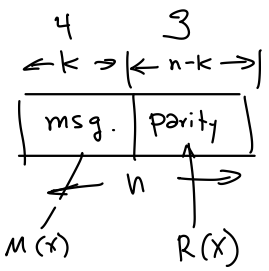
Exercise 5: If the generator polynomial is $G(x) = x^3 + x + 1$ and the data to be protected is 1001, what are $n-k$, $M(x)$ and the CRC? Check your result. Invert the last bit of the CRC and compute the remainder again.

$G(x) = 1\ 0\ 1\ 1$

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

$M(x) = 1001 = x^3 + 1x^0$

$K = 4$



$n = 7$

$$1011 - 1000 = 0011$$

$$M(x)x^{n-k} = x^3 \cdot (x^3 + 1) = x^6 + x^3 + 0x^2 + 0x + 0x^0$$

$M(x)$, x^{n-k}, product

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

$$\begin{array}{r} 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0 \\ 1x^6 + 0x^5 + 1x^4 + 1x^3 \\ \hline 0x^5 + 1x^4 + 0x^3 + 0x^2 \\ 0x^5 + 0x^4 + 0x^3 + 0x^2 \\ \hline 1x^4 + 0x^3 + 0x^2 + 0 \\ 1\ 0\ 1\ 1 \\ \hline 0\ 1\ 1\ 0 \\ 0\ 0\ 0\ 0 \end{array}$$

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

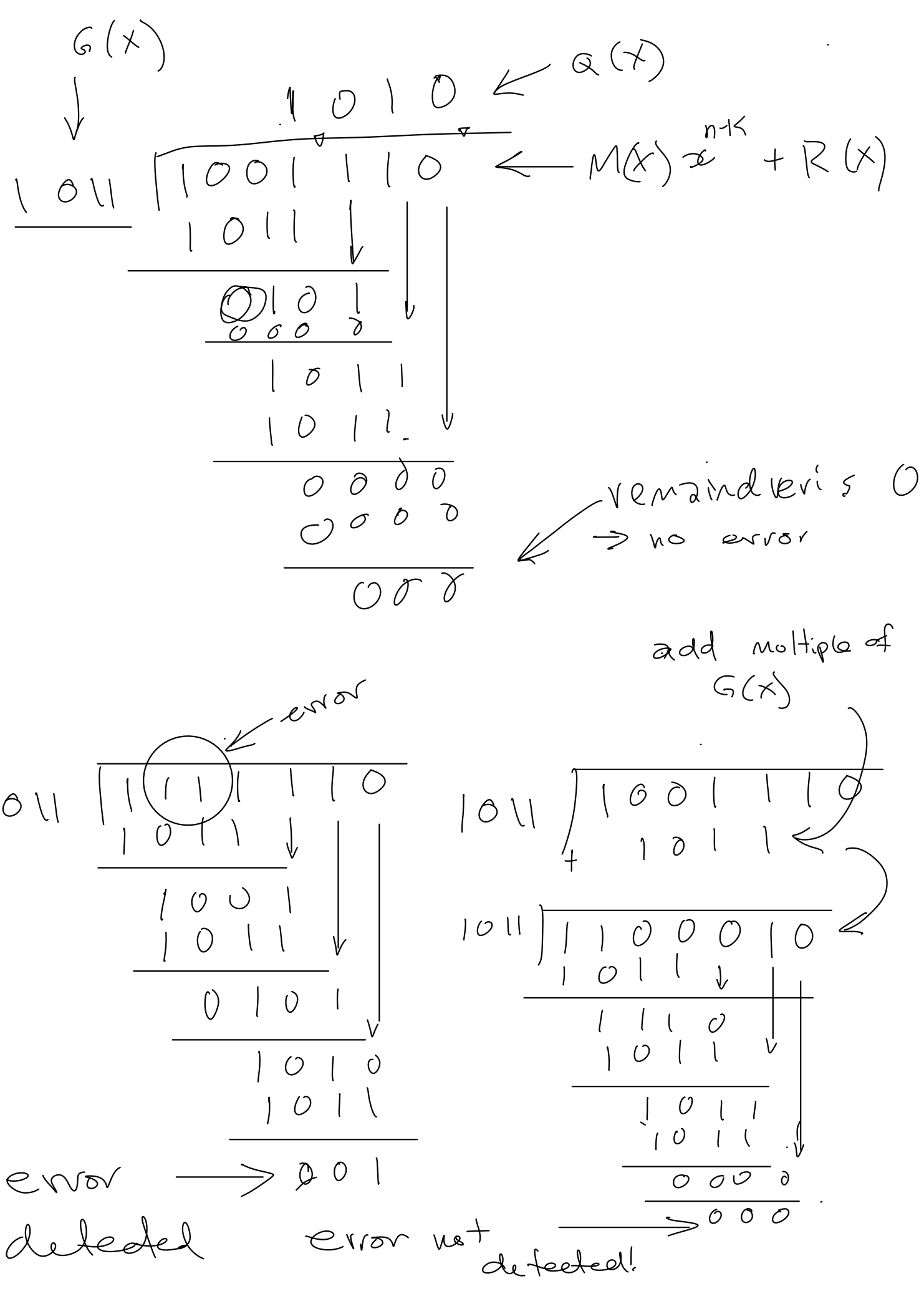
$R(x) = 1x^2 + 1x + 0x^0$

$= x^2 + x$

$M(x)x^{n-k} + R(x)$

$= 1001\ 110$

data | CRC


G(x)
Q(x)
1 0 1 0
1 0 1 1 | 1 0 0 1 1 1 0
M(x) x^{n-k} + R(x)
1 0 1 1
0 0 1 0 1
0 0 0 0
1 0 1 1
1 0 1 1
0 0 0 0
0 0 0 0
0 0 0
remainder is 0
→ no error
add multiple of G(x)
error
1 0 1 1 | 1 1 1 1 1 1 0
1 0 1 1
1 0 0 1 1
1 0 1 1
0 1 0 1 1
1 0 1 1
1 0 1 0
1 0 1 1
0 0 1
error → 001
error detected
1 0 1 1 | 1 0 0 1 1 1 0
1 0 1 1
1 1 0 0 0 1 0
1 0 1 1
1 1 1 0 1
1 0 1 1
1 0 1 1
1 0 1 1
0 0 0 0
→ 000
error not detected!

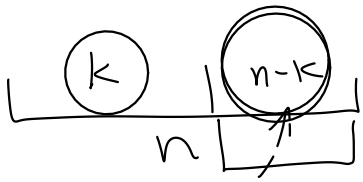
Exercise 6: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

$n-k = 32$.

(a) Yes will detect any error burst (sequence of errors < 32 bits).

(b) no, the 30 errors could 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?



$\frac{1}{2^{n-k}}$ 10 errors.

e.g. $n-k = 16$ $\quad \frac{1}{2^{16}} = \frac{1}{65536} \simeq 1 \times 10^{-4}$

$= 32$ $\quad \frac{1}{2^{32}} = \frac{1}{4 \times 10^9} \simeq 1 \times 10^{-9}$