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

XOR

AND

0	1
1	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?

+	0	1
0	0	1
1	1	2

x	0	1
0	0	0
1	0	1

Not a field.

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 $GF(2)$? Which result can be represented as a bit sequence?

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

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

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

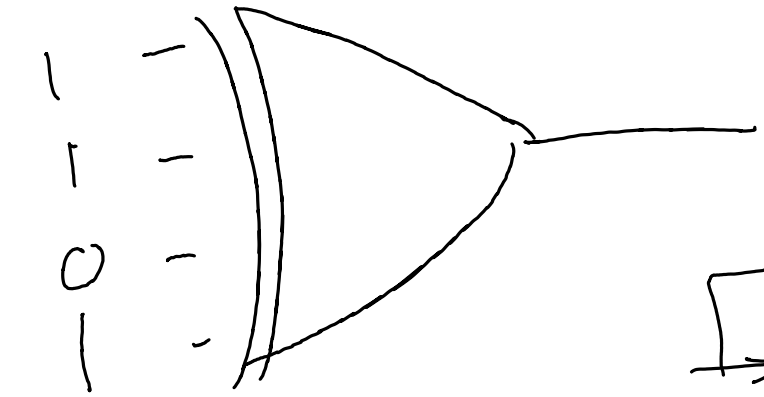
$0x^4$ $1x^3 + 0x^2 + 1x^1 +$

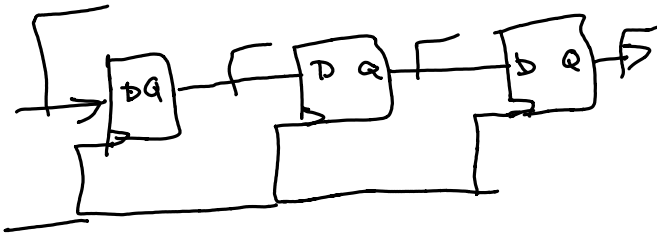
0 0 $0 + 0 + 0$

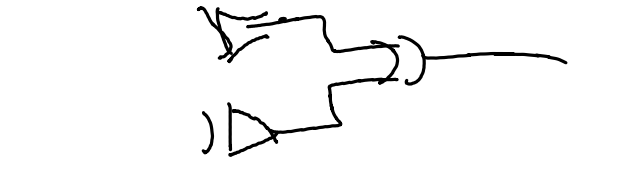
0 1 0 1

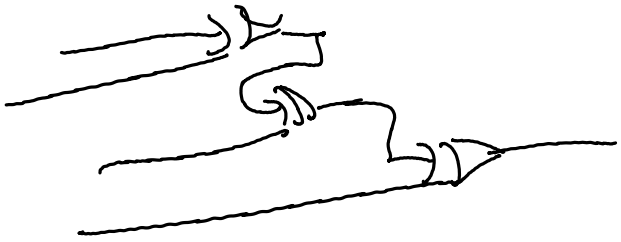
$0x^6 + 1x^5 + 0x^4 + 2x^3 + 0x^2 + 1x^1 + 0x^0$ ← using normal addition

$x^5 + x$ ← GF(2) operations









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.

$1001 \Rightarrow 1x^3 + 0x^2 + 0x + 1x^0 = x^3 + 1$

what is n-k? remainder R(x) has to be

$n-k=3$ of order 2 $(3-1)$ $\_x^2 + \_x + \_x^0$

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

$= x^6 + x^3 + 0x^2 + 0x + 0x^0$

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

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

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

$1x^4 \qquad 1x^2 + x$

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

1001 110

data CRC

k=4 n-k=3

n=7

(1011) 1001 110 (quotient 1010)

1011

0101

1011

1011

000 0 ⇒ remainder 0

(1011) 1000010

1011

0110

1011

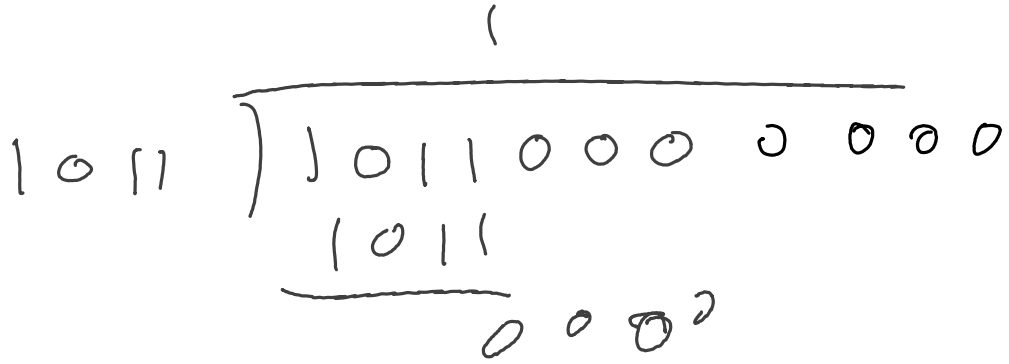
1100

1011

remainder ≠ 0 so there was an error

1001 110 1011

1011

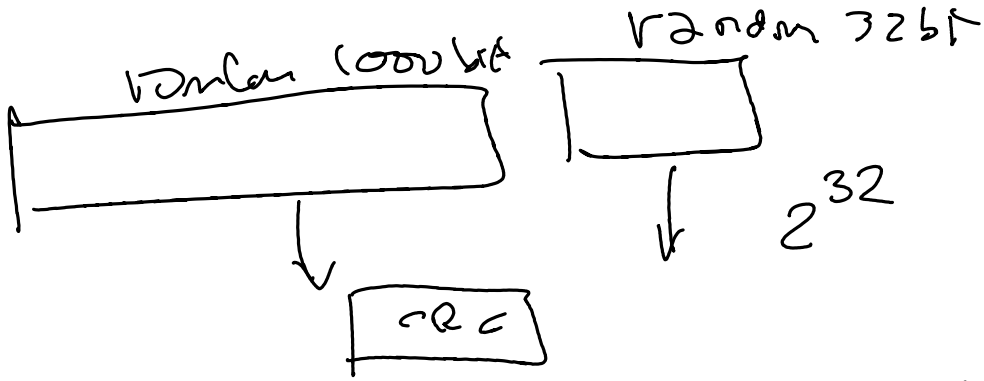


Exercise 6: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

1 - Yes

2 - not guanteed (but likely).

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?



probability of undetected error is $\frac{1}{2^{32}} \approx \frac{1}{4.1 \times 10^9}$