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

$a + b \bmod 2$

×	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?

+	0	1
0	0	1
1	1	2

×	0	1
0	0	0
1	0	1

↖ not part of the 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?

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

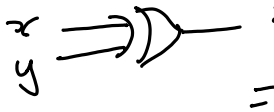
$x^5\ x^4\ x^3\ x^2\ x^1\ x^0$

$1\ 0\ 2\ 0\ 1\ 0$

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

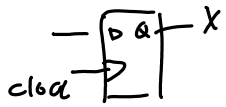
$x^5 + x \leftarrow$

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



= addition in GF(2)

= multiplication in GF(2)



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.

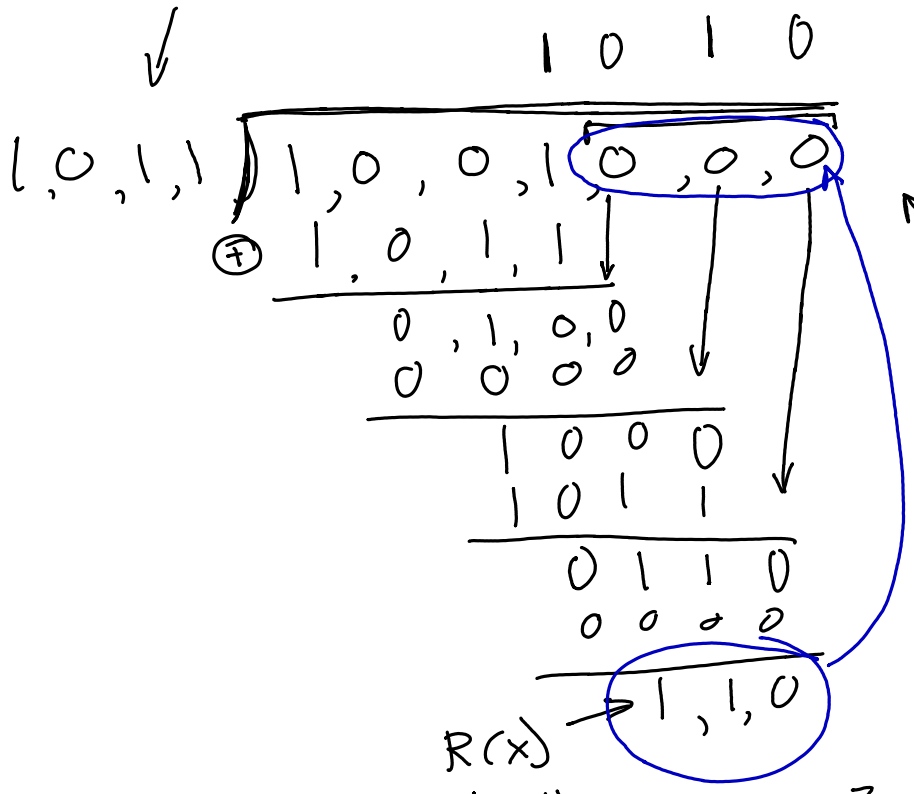
$G(x) = 1x^3 + 0x^2 + 1x + 1x^0$

$n-k = 3$ (one less than number of bits in $G(x)$).
== order of $G(x)$

$M(x) = \underbrace{(1x^3 + 0x^2 + 0x + 1)}_{\text{message}} \underbrace{x^3}_{x^{n-k}}$

$= 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0$

THESE ARE NOT BINARY NUMBERS they are COEFFICIENTS.



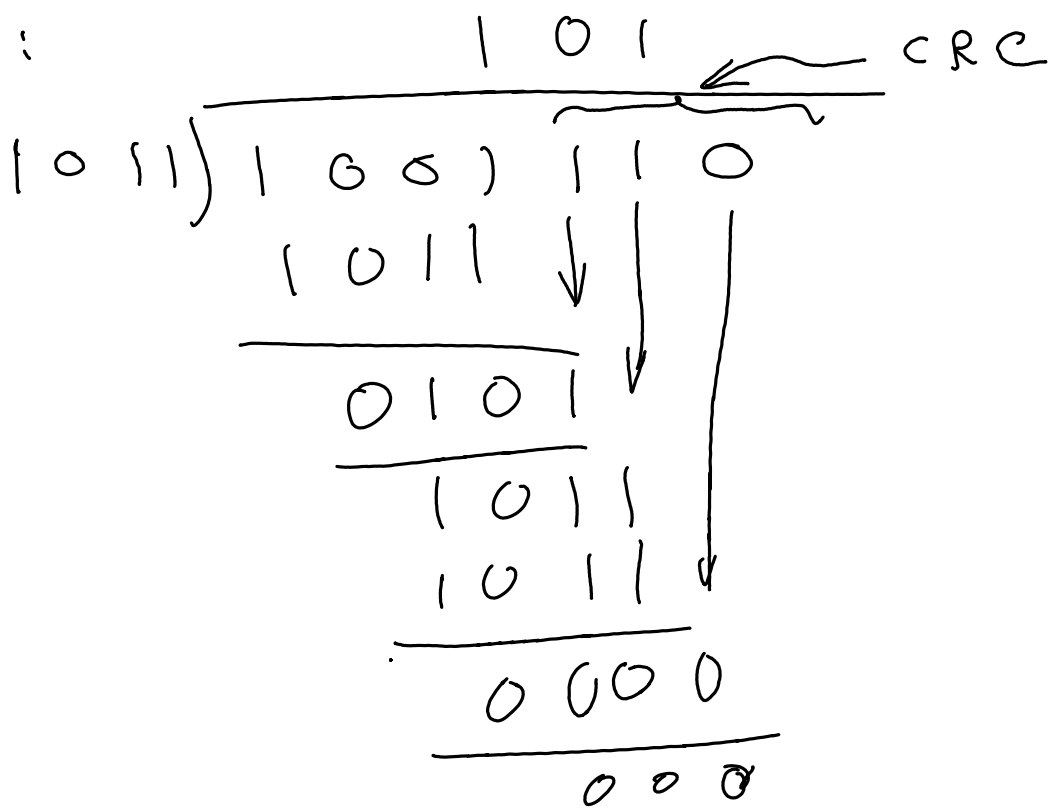
≈ 0.4
31) 635.0
62
15.0
12.4

$k = 4$ $\quad n-k = 3$

we will transmit $\underbrace{1\ 0\ 0\ 1}_{\text{data}}\ \underbrace{1\ 1\ 0}_{\text{CRC}}$

$n = 7$

check:

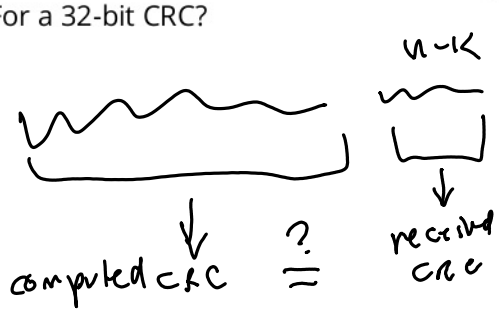


Exercise 6: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

30 < 32 ∴ guaranteed to detect any errors within 30 bits

not guaranteed to detect error burst > 32 bits but very 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?



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

for $n-k=16$ $2^{-16} \approx \frac{1}{65536}$

$n-k=32$ $2^{-32} \approx 0.25 \times 10^{-9}$