LECTURE 12: GF(2) & CRCs

Ex. 1

modulo 2

+	0	1
0	0	1
1	1	0

regular arithmetic

+	0	1
0	0	1
1	1	2

no, with regular addition don't have closure $\Rightarrow$ not a field

Ex. 2

modulo-2 addition (or subtraction), can be implemented with XOR

modulo 2.

−	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

modulo-2 multiplication can be implemented with AND

Ex3

$$01101 \Rightarrow 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 0\cdot x^1 + 1x^0$$
$$= x^3 + x^2 + 1$$

0101 1010

Ex. 4 $(x^2+1)(x^3+x) = x^2\cdot(x^3+x) + 1\cdot(x^3+x)$

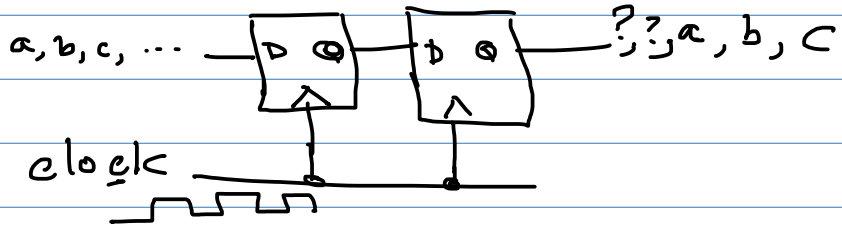
$= x^5 + x^3 + x^3 + x$

with regular arithmetic: $\Rightarrow x^5 + 2x^3 + x$

with coefficients from GF(2): $\Rightarrow x^5 + 0x^3 + x$

$= x^5 + x$

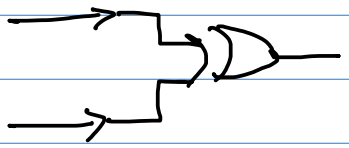
Shift Register:



Ex 5

0, 1, 0, 1

1, 0, 1, 0

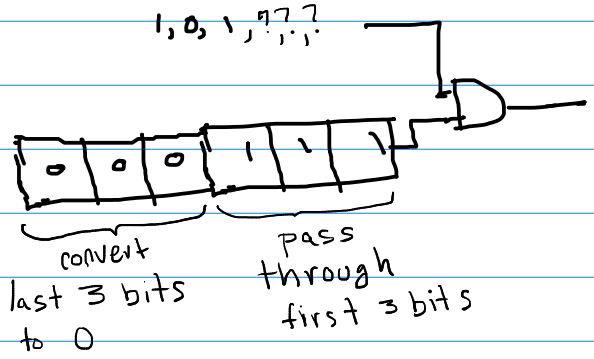
(a) 

(the XOR gate adds two polynomials)

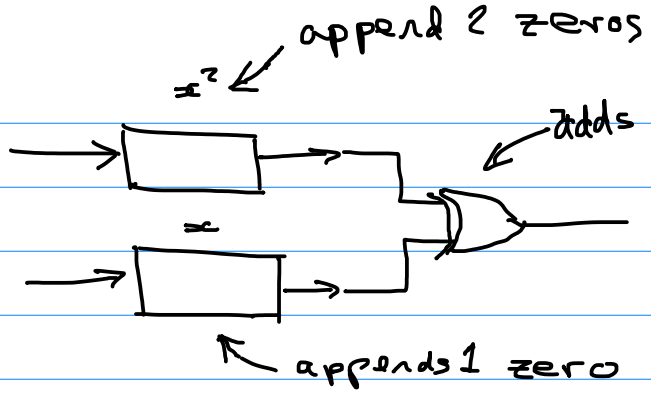
(b) $(x^2+1)x^3 \Rightarrow x^5 + x^3 = 1x^5 + 0x^4 + 1x^3 + 0x^2 + 0x^1 + 0x^0$

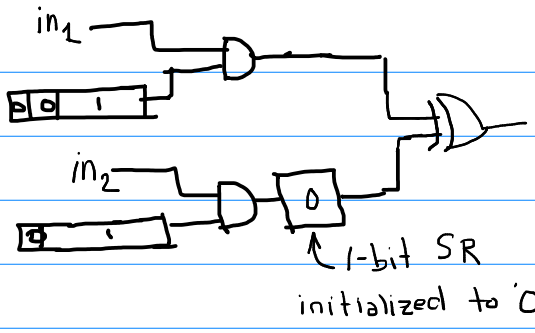
$\downarrow \qquad\qquad \downarrow$

101 $\Rightarrow$ 101000



(c)





Ex. 6

(wrong)

$$x^3 + x + 1 \;\overline{)\; x^3 + x^2}$$

$$G \rightarrow x^3 + 0x^2 + x + 1 \;\overline{)\; x^3 + x^2 + 0x + 0} \leftarrow M$$

$1 \leftarrow Q$

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

$$0x^3 + 1x^2 + 1x + 1 \leftarrow R$$

$M = 1100$

$R = 0111$ transmit $\{M, R\} \Rightarrow \underbrace{1100}_{\text{data}}\ \underbrace{0111}_{\text{CRC}}$

eg. $\frac{7}{3} = \underset{Q}{2}$ remainder $\underset{R}{1}$

(CRCs don't work in base 10 apparently)

Ex. 6

$x^3 + x + 1$) $x^3 + x^2$

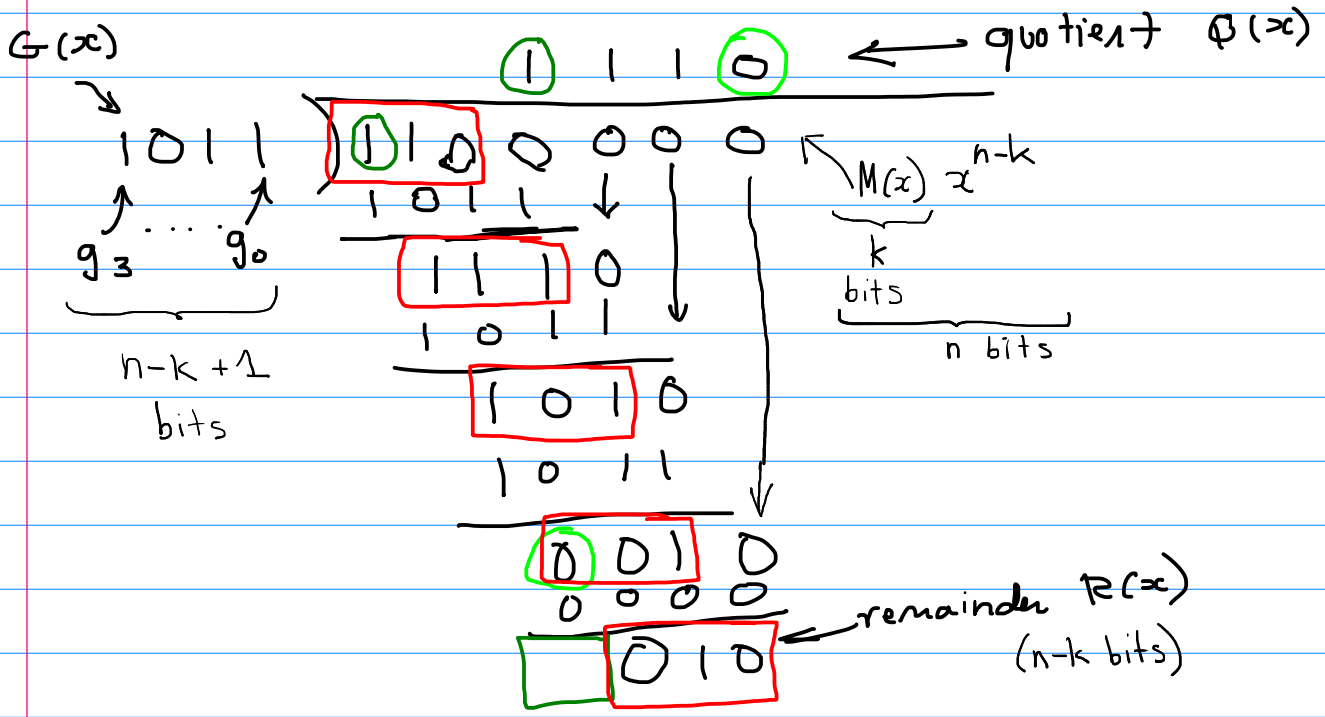
G(x) → $1x^3 + 0x^2 + 1x + 1x^0$) $1x^3 + 1x^2 + 0x^1 + 0x^0$ ← M(x)

step 1 : multiply M(x) by $x^{\text{(order of } G(x))}$ e.g. x^3 ($x^{is\ i+?}_4$ no, x^3)

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

working with the coefficients only:

step 2: divide M(x) by G(x):

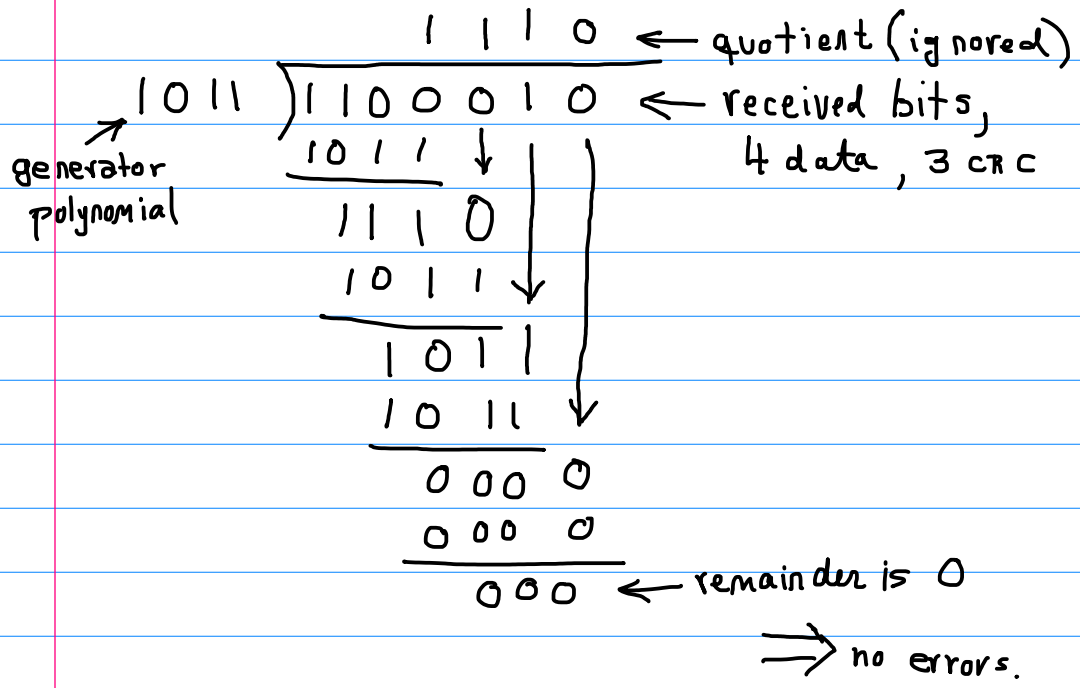


step 3: append remainder to M(x):

1100010

data CRC

At receiver, divide received bits by $G(x)$ & check for zero remainder:



$\Rightarrow$ no errors.

Ex. 7

n-k parity bits chosen at random

probability that they match the correct (required) CRC is

$$\left(\frac{1}{2}\right)^{n-k}$$

for CRC-16 $(n-k=16)$ $\left(\frac{1}{2}\right)^{16} = \frac{1}{65536} \approx \frac{1}{2}\cdot 10^{-3}$

CRC-32 $(n-k=32)$ $\left(\frac{1}{2}\right)^{16} = \frac{1}{2^{32}} \approx \frac{1}{4} \times 10^{-9}$