

Name: KEY

1) Perform the following operation in GF(2):  $x + x^4 \text{ mod } (x^2 + 1)$

$x + x^4 \mid_{x^2 = -1} = x + (x^2)^2 = x + 1$

$$\begin{array}{r} x^2 + 1 \\ 1 + x^2 \overline{) x + x^4} \\ \underline{x^2 + x^4} \phantom{0} \\ x \phantom{0} \phantom{0} \phantom{0} \phantom{0} \\ x^2 + x \phantom{0} \phantom{0} \phantom{0} \phantom{0} \\ \underline{x^2 + 1} \phantom{0} \phantom{0} \phantom{0} \phantom{0} \\ x + 1 \phantom{0} \phantom{0} \phantom{0} \phantom{0} \end{array}$$

2) Simplify in GF(2):  $(1+x^n)^2$

$(1+x^n)(1+x^n) = 1 + (1+1)x^n + x^{2n} = 1 + x^{2n}$

3) Is the following valid generator polynomial  $x + x^2$ , why?

No, because  $g_0 \neq 1$

4) Given that  $x^7 + 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$

a. List all the valid code-words for the (7,5) cyclic code

b. List all the valid code-words for the (7,3) systematic cyclic code generated by  $g(x) = (1+x)(1+x+x^3)$

a) (7,5)  $\Rightarrow r = 2$ . It is not possible to find a polynomial of degree 2 which is a factor of  $x^7 + 1$

we can get (7,6), (7,3), (7,3), (7,4), (7,4), (7,1)

b) For systematic codes.  $c(x) = b_0 b_1 b_2 b_3 m_0 m_1 m_2$

$b(x) = \text{rem} \left[ \frac{x^r m(x)}{g(x)} \right] = \text{rem} \left[ \frac{x^4 m(x)}{(1+x)(1+x+x^3)} \right]$

$(1+x)(1+x+x^3) = 1 + x + x^3 + x + x^2 + x^4 = 1 + x^2 + x^3 + x^4$

for 000  $\Rightarrow m(x) = 0 \Rightarrow c(x) = 0000000$

for 100  $\Rightarrow m(x) = 1$

$b(x) = \text{rem} \left[ \frac{x^4}{1+x^2+x^3+x^4} \right] = 1+x^2+x^3 \Rightarrow c(x) =$

with 7 cyclic shifts we generate all the code words.

- 0 0 0 0 0 0 0
- 1 0 1 1 1 0 0
- 0 1 0 1 1 1 0
- 0 0 1 0 1 1 1
- 1 0 0 1 0 1 1
- 1 1 0 0 1 0 1
- 1 1 1 0 0 1 0
- 0 1 1 1 0 0 1

Note that these are all the possible