**ELG5372** **Error Control Coding** **Fall 2018**

**Sample Assignment 4**
**Decoding of Linear Block Codes / Performance**

**Question 1**
We want to design a binary linear cyclic code of length n=31 using the minimal polynomials of GF(32) with respect to GF(2) associated to the conjugacy classes of $\alpha^5$ and $\alpha^{15}$.

(a) What is the generator polynomial g(X)?
(b) What is the parity check polynomial h(X)?
(c) What is the rate of the code?
(d) If $m(X) = 1+X^2+X^7$, what is the codeword polynomial assuming that the code is non-systematic?
(e) Repeat (d) assuming that the code is systematic?
(f) What is the encoder structure for non-systematic encoding?
(g) What is the encoder structure for systematic coding?
(h) Based on the BCH bound, what is the lower bound on the minimum distance of this code?

**Question 2**
Is it possible to design a binary linear cyclic code of length n=4? n=6? n=12? What can you conclude about linear binary cyclic codes with even length? Why?

**Question 3**
Find the generator polynomial for a binary linear cyclic code of length 15 with $d_{min} \geq 4$ using $\beta = \alpha^7$ and $b$=1. What is the rate of the code? Draw the non-systematic code generator structure.

**Question 4**
A binary linear cyclic code of length 15 has $g(X) = X^4+X^3+X^2+X+1$. We are using a systematic encoder.
(a) Draw the structure of the systematic encoder.
(b) What is the design distance of this code according to the BCH bound? Explain your answer.
(c) How many errors can this code correct?
(d) If $r(X) = 1+X^3$, what is the most likely transmitted codeword?

Minimal polynomials of $GF(2^m)$ with respect to GF(2) (including conjugacy class)
m=2
1: X+1
$\alpha,\alpha^2$: $X^2+X+1$

m=3
1: X+1
$\alpha,\alpha^2,\alpha^4$: $X^3+X+1$
$\alpha^3,\alpha^6,\alpha^5$: $X^3+X^2+1$

m=4
1: X+1
$\alpha,\alpha^2,\alpha^4,\alpha^8$: $X^4+X+1$
$\alpha^3,\alpha^6,\alpha^{12},\alpha^9$: $X^4+X^3+X^2+X+1$
$\alpha^5,\alpha^{10}$: $X^2+X+1$
$\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}$: $X^4+X^3+1$

m=5

1: X+1

$\alpha,\alpha^{2},\alpha^{4},\alpha^{8}, \alpha^{16}$: $X^{5}+X^{2}+1$

$\alpha^{3},\alpha^{6},\alpha^{12},\alpha^{24}\ \alpha^{17}$: $X^{5}+X^{4}+X^{3}+X^{2}+1$

$\alpha^{5},\alpha^{10}\ \alpha^{20}, \alpha^{9}, \alpha^{18}$: $X^{5}+X^{4}+X^{2}+X+1$

$\alpha^{7},\alpha^{14},\alpha^{28},\alpha^{25}, \alpha^{19}$: $X^{5}+X^{3}+X^{2}+X+1$

$\alpha^{11},\alpha^{22},\alpha^{13},\alpha^{26}, \alpha^{21}$: $X^{5}+X^{3}+X^{2}+X+1$

$\alpha^{15},\alpha^{30},\alpha^{29},\alpha^{27}, \alpha^{23}$: $X^{5}+X^{3}+1$

m=6

1: X+1

$\alpha,\alpha^{2},\alpha^{4},\alpha^{8}, \alpha^{16}, \alpha^{32}$: $X^{6}+X+1$

$\alpha^{3},\alpha^{6},\alpha^{12},\alpha^{24}\ \alpha^{52}, \alpha^{41}$: $X^{6}+X^{4}+X^{2}+X+1$

$\alpha^{5},\alpha^{10}\ \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$: $X^{6}+X^{5}+X^{2}+X+1$

$\alpha^{7},\alpha^{14},\alpha^{28},\alpha^{56}, \alpha^{49}, \alpha^{35}$: $X^{6}+X^{3}+1$

$\alpha^{9},\alpha^{18},\alpha^{36}$: $X^{3}+X^{2}+1$

$\alpha^{11},\alpha^{22},\alpha^{44},\alpha^{25}, \alpha^{50}, \alpha^{37}$: $X^{6}+X^{5}+X^{3}+X^{2}+1$

$\alpha^{13},\alpha^{26},\alpha^{52},\alpha^{41}, \alpha^{19}, \alpha^{38}$: $X^{6}+X^{4}+X^{3}+X+1$

$\alpha^{15},\alpha^{30},\alpha^{60},\alpha^{57}, \alpha^{51}, \alpha^{39}$: $X^{6}+X^{5}+X^{4}+X^{2}+1$

$\alpha^{21},\alpha^{42}$: $X^{2}+X+1$

$\alpha^{23},\alpha^{46},\alpha^{29},\alpha^{58}, \alpha^{53}, \alpha^{43}$: $X^{6}+X^{5}+X^{4}+X+1$

$\alpha^{27},\alpha^{54},\alpha^{45}$: $X^{3}+X+1$

$\alpha^{31},\alpha^{62},\alpha^{61},\alpha^{59}, \alpha^{55}, \alpha^{47}$: $X^{6}+X^{5}+1$