CMSC 442 Fall 2001
Instructor: Dr. Lomonaco
Homework 8

- READING ASSIGNMENT: Peterson & Weldon, **"Error-Correcting Codes,"** MIT Press, (Second Edition), (1986), Chapter 6 & 7
- OPTIONAL READING ASSIGNMENT: MacWilliams & Sloane, **"The Theory of Error-Correcting Codes,"** North-Holland (Second Edition), (1983), Chapter 7.

Prob. 1. You will find below the Antilog/Log table of $GF(2^6)$ based on the primitive polynomial

$$p(x) = x^6 + x + 1$$

Use this table to compute the minimum polynomial $m_5(x)$ of ξ^5, where ξ is the primitive element defined by $p(x)$.

Antilog $a_0a_1a_2a_3a_4a_5$	Log		Antilog $a_0a_1a_2a_3a_4a_5$	Log
000000	$-\infty$		000101	15
100000	0		110010	16
010000	1		011001	17
001000	2		111100	18
000100	3		011110	19
000010	4		001111	20
000001	5		110111	21
110000	6		101011	22
011000	7		100101	23
001100	8		100010	24
000110	9		010001	25
000011	10		111000	26
110001	11		011100	27
101000	12		001110	28
010100	13		000111	29
001010	14		110011	30

Antilog $a_0a_1a_2a_3a_4a_5$	Log		Antilog $a_0a_1a_2a_3a_4a_5$	Log
101001	31		111001	47
100100	32		101100	48
010010	33		010110	49
001001	34		001011	50
110100	35		110101	51
011010	36		101010	52
001101	37		010101	53
110110	38		111010	54
011011	39		011101	55
111101	40		111110	56
101110	41		011111	57
010111	42		111111	58
111011	43		101111	59
101101	44		100111	60
100110	45		100011	61
010011	46		100001	62

Prob. 2. Consider $GF(3^3)$ defined by the primitive polynomial

$$p(x) = x^3 + 2x + 1,$$

and let $\xi = x \bmod p(x)$. Find the minimum polynomial $m_3(x)$ of ξ^3. You may assume the following theorems:

$$a^p = a \text{ for all } a \in GF(p) \text{ for } p \text{ a prime integer.}$$

$$\left(\sum_{j=1}^{n} a^j\right)^p = \sum_{j=1}^{n} (a^j)^p \text{ in any field of characteristic } p.$$

You may use the following table for you calculations:

$GF(3^3)$ defined by the primitive polynomial $p(x) = x^3 + 2x + 1$

Antilog $a_0a_1a_2$	**Log**	**Antilog** $a_0a_1a_2$	**Log**
000	$-\infty$		
100	0	200	13
010	1	020	14
001	2	002	15
210	3	120	16
021	4	012	17
212	5	121	18
111	6	222	19
221	7	112	20
202	8	101	21
110	9	220	22
011	10	022	23
211	11	122	24
201	12	102	25

Prob. 3. **a)** Draw the linear sequential circuit (LSC) that multiplies by the polynomial

$$h(x) = 1 + x^3 + x^6$$

b) Draw the linear sequential circuit (LSC) that divides by the polynomial

$$g(x) = 1 + x^2 + x^4 + x^6 + x^7$$

c) Draw the linear sequential circuit (LSC) that simultaneously multiplies by $h(x)$ and divides by $g(x)$.

Prob. 4. Draw an LSC which takes as inputs polynomials $a(x)$ and $b(x)$ and then produces the output

$$h(x)a(x) + k(x)b(x),$$

where $h(x)$ and $k(x)$ are the polynomials:

$$h(x) = 1 + x^4 + x^{10} \text{ and } k(x) = x + x^2 + x^4 + x^7 + x^9$$