CMSC 442/653 Fall 2007
Instructor: Dr. Lomonaco
Homework 7

- **Optional listening assignment:** Listen to Mozart's ***Eine Kleine Nachtmusik***
- **Optional Reading assignment:** Peterson & Weldon, "Error-Correcting Codes," MIT Press, (Second Edition), Chapters 7 and 8
- **Optional Reading assignment:** MacWilliams & Sloane, "The Theory of Error-Correcting Codes," North-Holland (2nd edition), (1983), Chapter 7.

1U) Let ξ be a primitive element of $GF(2^6)$. Compute the order of ξ^j for $j = 0,1,2,3,\dots,62$.

2U) Let α be the primitive element of $GF\left(2^6\right)$ which is the zero of the primitive polynomial:

$$1 : x + x^6$$

Let $g(x)$ be the polynomial of smallest degree having the following zeros:

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}$$

Let $V = \left(g(x)\right)$ be the corresponding cyclic code of smallest length.

> **a)** Write $g(x)$ as a product of minimal polynomials $m_i(x)$, where $m_i(x)$ is the minimal polynomial of α^i. (Do not explicitly compute the $m_i(x)$'s.)
>
> **b)** What is the degree of $g(x)$?
>
> **c)** What is the length n of V ?
>
> **d)** What is the dimension of V ?

3U) Let ξ be a primitive element of $GF(2^4)$ defined by $\xi = x \bmod p(x)$ for the primitive polynomial

$$p(x) = 1 + x + x^4$$

Let $g(x)$ be the binary polynomial of smallest degree having

$$\xi \text{ and } \xi^5$$

as roots. Let $V = \left(g(x)\right)$ be the cyclic code of smallest length having $g(x)$ as a generator polynomial.

a) What is the length n of V?

b) What is the dimension of $V^{\perp}$?

c) Use ξ and ξ^5 to construct a parity check matrix H of V. (Do not explicitly compute $g(x)$. Be sure that the rows of your parity check matrix are linearly independent. Use the enclosed table for $GF\left(2^4\right)$ to answer this part of the question.)

$$GF\left(2^4\right) = GF(2)[x]/\left(x^4 + x + 1\right)$$

Antilog	Log
$a_0a_1a_2a_3$	
0000	$-\infty$
1000	0
0100	1
0010	2
0001	3
1100	4
0110	5
0011	6
1101	7
1010	8
0101	9
1110	10
0111	11
1111	12
1011	13
1001	14