**ECE 697U - Error Control Coding**
**Homework #2**
**Spring, 2008**

**Due: March 26, 2008**

1. Per class: given one code, we can form others by deleting columns of the parity check matrix (these are *shortened* codes).

   (a) Find the longest double-error-correcting code that can be obtained by shortening the (31,26) Hamming code. Prove that your answer is the longest possible code.

   (b) Find the longest code of Hamming distance four (a SEC-DED code) that can be obtained by shortening the (31,26) Hamming code. Prove that your answer is the longest possible code.

2. In decoding the (15,7) DEC code from class, where the elements of the second row are obtained by cubing the elements of the first row, there are five different cases:

   (a) $s_1 = 0, s_3 = 0$ (codeword received)
   (b) $s_3 = s_1^3$ (one error)
   (c) $\theta^2 + s_1\theta + (s_1^3 + s_3)s_1^{-1} = 0$ has two distinct roots (two errors to correct).
   (d) $s_1 = 0, s_3 \neq 0$ (more than two errors).
   (e) $\theta^2 + s_1\theta + (s_1^3 + s_3)s_1^{-1} = 0$ has no roots (more than two errors).

   Find the number of cosets corresponding to each case.

3. Recall again the (15,7) DEC code from class. By building GF(16) as powers of a root of $\alpha^4 + \alpha + 1$, I obtain the parity check matrix explicity in hexadecimal as:

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 1 & 8 & F & C & A & 1 & 1 & A & F & F & C & 8 & A & 8 & C \end{pmatrix}$$

   Decode the following vectors:

   (a) 101011000010000

   (b) 101011000110000

   (c) 110010100101000

   (d) 000000110110010

   (e) 001010000000011

4. Use primitive polynomial $x^6 + x + 1$ to contruct GF(64) and perform the following:

   (a) Find the cyclotomic cosets (denote with powers of $\alpha$ as in class).

   (b) Find the minimal polynomials for each of the 64 elements.

   (c) Factor $x^{64} - x$ into its irreducible factors over GF(2).

5. For the (15,5) triple-error-correcting (narrow-sense) BCH code given in class, decode the following vectors:

   (a) 101011000010000

   (b) 101011000110000

   (c) 110010100101000