EE/Ma 127a Error-Correcting Codes — R. J. McEliece
*draft of November 27, 2000* — 162 Moore

Homework Assignment 7 (**Final Version** )
Due (in class) 9am November 29, 2000

**Reading:** Handout: "Hex Arithmetic"
Handout: "Chapter 9: BCH, Reed-Solomon, and Related Codes," pp. 1-2.

**Problems to Hand In:**

**Problem 1.** Referring to the $(15, 7)$ double-error correcting BCH code with "Hex" parity-check matrix

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

using the decoding algorithm we discussed in class on November 15 and 17, decode the following five vectors:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

That is, find the nearest codeword, if it is within distance 2 or less. If there is no such codeword, report "more than 2 errors."

**Problem 2.** In class on Monday November 20, I reordered the columns of $H$ as follows:

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

Note that the the first row of $H'$ consists of the successive powers of 2, i.e.,

$$1, 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, \ldots, 2^{14} = 9.$$

Note also that $2^{15} = 1$.

(a) Show that the $(15, 7)$ code defined by $H'$ is cyclic.

(b) Find a generator polynomial for the code defined by $H'$. (You may assume that the dimension of the code is 7.)

**Problem 3.** In class on Wednesday Nov. 22, I used the irreduclble polynomial $x^3 + x + 1$ to define a field multiplication on 3-bit vectors and that the corresponding multiplication rule is

$$[a_0, a_1, a_2] \cdot [b_0, b_1, b_2] = [c_0, c_1, c_2],$$

where

$$\begin{aligned} c_0 &= a_0b_0 + a_1b_2 + a_2b_1 \\ c_1 &= a_0b_1 + a_1b_0 + a_1b_2 + a_2b_1 + a_2b_2 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 + a_2b_2. \end{aligned}$$

(a) Using the fact that $x^4 + x + 1$ is irreducible, find a similar rule for multiplying 4-bit vectors that makes a field with 16 elements.

(b) Using the rule you developed in part (a), compute the product of $D$ and 4 in the HexField.

**Problem 4.** In class on November 27, I used the "extended Euclidean algorithm" to compute the inverse of "$D$" in the HexField. Please compute the inverse of "$F$" using the same method.