Math 350
Spring, 2000

HOMEWORK #9

Do 50 points of the following problems (due 4/11/00).

25 pts. **1** Suppose we want to construct a Huffman code on the 5 letters A(50), E(100), H(20), R(40), and T(45), where the numbers in parenthesis represent the frequency of these letters in a test text. Construct the Huffman code, and decode the following three words: 11010010100; 1000111101110; 1101001010111110. You can use http://swww.ee.uwa.edu.au/ plsd210/ds/huffman.html to remind yourself of how the code is constructed.

The letters will get the following assignments: A=111; T = 110; R=101; H = 100; E = 0. With this assignment, the words above are THREE; HEART; and THREAT.

⋆ 25 pts. **2** Start with the field with 8 elements in it, the Goppa polynomial $G(x) = x^2+x+1$, and the subset $L = \{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1; \alpha^6 = \alpha^2+1\}$. Construct the Goppa code of length 8 based on this set-up, and describe the properties of this code. You can find copies of Mohammed's slides at http://www.mathcs.richmond.edu/ jad/350s00/Mohammedpresentation.pdf.

The parity check matrix for the Goppa code with the properties listed above is

$$\left(\begin{matrix} G(0)^{-1} & G(1)^{-1} & G(\alpha)^{-1} & G(\alpha^2)^{-1} & G(\alpha^3)^{-1} & G(\alpha^4)^{-1} & G(\alpha^5)^{-1} & G(\alpha \\ 0G(0)^{-1} & 1G(1)^{-1} & \alpha G(\alpha)^{-1} & \alpha^2 G(\alpha^2)^{-1} & \alpha^3 G(\alpha^3)^{-1} & \alpha^4 G(\alpha^4)^{-1} & \alpha^5 G(\alpha^5)^{-1} & \alpha^6 G(\end{matrix}\right.$$

When we translate this into binary, we get the parity check matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

This parity check matrix is associated to a code of length $n = 8, k = 2$, and $d \geq 3$. I think the actual minimum distance is 5: can you show that??

25 pts. **3** Define the four quadratic residue codes of length 17, and explain what properties they have.

The codes are generated by $e_1(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{15} + x^{13} + x^9$; $e_2(x) = x^3 + x^6 + x^{12} + x^7 + x^{14} + x^{11} + x^5 + x^{10}$; $1 + e_1(x)$ and $1 + e_2(x)$. The first two of these have dimension $\frac{17+1}{2} = 9$ (we did not talk about the dimension of the last two). The minimum distance of the codes are at least 5 by the square root bound (extra credit if you found a word of weight 5).