ENEE626. Midterm examination, 10/25/2007 **Instructor:** A. Barg

All answers should be accompanied with proofs or sufficient explanation. Intermediate calculations should be shown.

10 points for each of the questions marked (a),(b),...,(g).

1. (max 60)

Consider a binary linear code C_1 with the generator matrix

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

(a) What is the distance of C_1?

(b) Do positions 1,2,3 form an information set? What about 1,6,7?

(c) Write the generator matrix of C_1 in the systematic form in which the message positions are 1,6,7.

(d) Write a parity-check matrix of the code C_1 in the systematic form in which the check positions are 2,3,4,5,8.

(e) Use the matrix that you found in step (d) to encode the message 001 (the message positions are still 1,6,7).

(f) Give an example of correctable double error with respect to ML decoding of the code C_1.

2. (max 70)

(a) Let $K = \mathbb{F}_{p^m} (m \geq 3), L = \mathbb{F}_{p^2}, F = \mathbb{F}_p$ be finite fields. Give precise definitions of the following facts:

(i) elements $a_1, a_2, \dots, a_\ell \in K$ are linearly independent over F;

(ii) a given set of elements of K forms a basis of K over F;

(iii) elements $b_1, b_2, \dots, b_k \in K$ are linearly independent over L (assuming that L is a subfield of K).

(b) Let α be a root of $x^4 + x^3 + 1$. Prove directly (without writing out all powers of α) that α is primitive. You may use the fact that β of part (d) below is primitive.

(c) Write out a table of $\mathbb{F}_{16}$ with 2 columns: first represent each element as a polynomial in α of degree 3 or less, then as a power of α.

(d) Let β be a root of $x^4 + x + 1$. Add another column to the table obtained in (c), showing the representation of every element in that table as a positive power of β.

(e) Using the definition you gave in part (a), prove that the elements $\alpha, \alpha^2, \alpha^4, \alpha^8$ form a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

(f) Express α^9 and α^{12} in the basis $\alpha, \alpha^2, \alpha^4, \alpha^8$.

(g) Let $\omega = \beta^5$ be a primitive element of $\mathbb{F}_4$.

(i) Prove that the polynomial $f(x) = x^2 + x + \omega$ is irreducible over $\mathbb{F}_4$.

(ii) Let γ be a root of f. Prove that $\gamma = \alpha^{11}$ or α^{14}.