Math 422 Winter 2007 - Final Exam

April 24, 2007

No books, no notes, no calculators are allowed.

Good Luck!

Remark: The equation to find the error locator polynomial for a BCH code is of the form

$$\begin{bmatrix} S_1 & S_2 & \dots & S_t \\ S_2 & S_3 & \dots & S_{t+1} \\ \vdots & \vdots & \dots & \vdots \\ S_t & S_{t+1} & \dots & S_{2t-1} \end{bmatrix} \begin{bmatrix} b_t \\ b_{t-1} \\ \vdots \\ b_1 \end{bmatrix} = - \begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix}$$

Problem 1. [14] Let $n > 0$ and let C be the binary *even-weight code* of length n: that is, C consists of all length n vectors that have even weight.

$$C = \{\mathbf{x} \in \mathbb{Z}_2^n \mid w(\mathbf{x}) \text{ is even}\}$$

a) Find a parity check check matrix H for C. (*Hint:* $w(\mathbf{x}) \equiv x_1 + x_2 + \cdots + x_n \mod 2$)

b) Find a generator matrix for C.

c) Compute the minimum distance of both, C and its dual code $C^\perp$. Justify your answers.

d) How many elements does C contain? How many elements does $C^\perp$ contain? Justify your answer.

e) Suppose n is odd. Is $C^\perp$ perfect? Why or why not?

f) Again let $n > 2$ be odd. Is $C \subseteq C^\perp$? Is $C^\perp \subseteq C$?

g) Prove or disprove: C is a cyclic code.

Problem 2. [16] Let $F_9 = \mathbb{Z}_3[x]/\langle x^2+1\rangle$. We denote $\bar{x} \in F_9$ by a. Then $\alpha = 1 + a$ is primitive.
Let C be the BCH code of design-distance 3 over $\mathbb{Z}_3$ corresponding to α, α^2.

a) What is the length of C? Justify your answer.

b) Find the generator polynomial g for C.

c) Find the check polynomial h for C.

d) What are the dimensions of C and $C^\perp$? Justify your answer.

e) How many errors can C at least correct?

f) Suppose you receive the vector 00101100. Translate this into a polynomial and compute the syndromes S_1 and S_2.

g) Decode the received vector in f) to a codeword if possible, using the decoding scheme for BCH codes. How many errors did occur?

h) Is the BCH code corresponding to $\alpha, \alpha^2, \alpha^3$ (design-distance 4) the same code as C? Why or why not?

(You may freely refer to Table 1.)

Element	Minimal polynomial	Power of α
1	$x - 1 = x + 2$	α^8
2	$x - 2 = x + 1$	α^4
a	$x^2 + 1$	α^6
$2a$	$x^2 + 1$	α^2
$1 + a$	$x^2 + x + 2$	α^1
$1 + 2a$	$x^2 + x + 2$	α^3
$2 + a$	$x^2 + 2x + 2$	α^7
$2 + 2a$	$x^2 + 2x + 2$	α^5

Table 1. Elements of F_9, their minimal polynomials over $\mathbb{Z}_3$, and their expression as powers of the primitive element.

Problem 3. [6] For each nonzero element in F_9 (defined as in Problem 2), find its order. Justify your answer.

Problem 4. [4] Prove the singleton bound:
If C is a linear $[n, k, d]$-code over F_q, then $k \leq n - d + 1$ or, equivalently, $d \leq n - k + 1$.
(*Hint:* You need to show only one of the two inequalities. For the second one, you could use the criterion involving a parity check matrix for C.)

Problem 5. [10] For each of the following statements, indicate whether it is true or false. No justification is needed.

a) For a linear code C with a parity check matrix H, its minimum distance is the smallest positive number d such that there are d linearly dependent columns of H.

b) The minimum distance of a Hamming code is always 5.

c) There is a perfect ternary code of length 11 and dimension 6.

d) A binary Hamming code is equivalent to a cyclic code.

e) The degree of the generator polynomial of a cyclic code is equal to the dimension of the code.

Problem 6. [4] Let $q = p^l$ for some prime p and some integer $l > 0$, and let F_q be a finite field with q elements. Show that for each $a \in F_q$, the polynomial $f = x^p - a$ has a unique root in F_q.
(*Hint:* Powers of a?)