Math 422 Winter 2007 - Midterm Exam

March 1, 2007

No books, no notes, no calculators are allowed.

Good Luck!

Problem 1. [12] Let C be the linear $[7, k, d]$-code over $\mathbb{Z}_2$ with generator matrix

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

a) Find k and the number of elements in C. Justify your answer.

b) Find a parity check matrix H for C. If possible, find one in standard form.

c) Is C a Hamming code? Explain.

d) Encode the message vector 1001.

e) Suppose you receive the vector 1110111. Decode it using syndrome decoding with your matrix H from b). Show your work (in particular, compute the syndrome). (*Hint:* You do not have to write down a syndrome table...)

Problem 2. [10] Let C be the linear code of length 5 over $\mathbb{Z}_{11}$ given by the equations

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= 0 \\ x_2 + 2x_3 + 2x_4 + x_5 &= 0 \\ x_1 - 8x_2 + 9x_3 &= 0 \end{aligned}$$

a) Find a generator matrix for C.

b) Find a parity check matrix H for C.

c) Find a basis for the dual code of C.

d) Find the maximum number N such that any collection of N columns of H (cf. b)) is linearly independent. Justify your answer.

e) Find $d(C)$. Is C a perfect code? Justify your answer.

Problem 3. [8] For each of the following statements indicate whether it is true or false. No justification is needed.

a) If G is the generator matrix of a linear code (of dimension k with $1 \leq k < n$), then G is also a parity check matrix for some (possibly different) linear code of dimension $n - k$.

b) There is no linear 3-ary $(7, 16, 3)$-code.

c) An $(n, M, 2t)$-code can be used to correct t errors, using nearest neighbour decoding.

d) An (n, M, d)-code can be used to detect $d - 1$ errors.

e) Two equivalent codes have the same minimum distance.

f) A (nonempty) binary code is linear if and only if the sum of any two (not necessarily distinct) codewords is again a codeword.

g) For every pair of positive integers $n > d$, there is always a perfect (n, M, d)-code (for some M).

h) If C is a linear $[n, k]$-code with generator matrix G, then $\mathbf{x} \in F_q^n$ is a codeword if and only if $G\mathbf{x}^t = \mathbf{0}$.

Problem 4. [8] Let C be a linear $[3, k, 3]$-code over $\mathbb{Z}_3$ with $k \geq 1$. Show that k (i.e. $\dim C$) is equal to 1. How many linear codes with these parameters are there? Justify your answer.

Problem 5. [6] Recall that $A_q(n, d)$ is the largest value for M such that there exists a q-ary (n, M, d)-code.
Let C be a q-ary (n, M, d)-code with $n, d > 0$ and $M \geq 2$. Suppose that M is maximal, i.e. that $M = A_q(n, d)$.
Prove: For every vector $\mathbf{y} \in F_q^n$ there is a codeword $\mathbf{x}$ such that $d(\mathbf{x}, \mathbf{y}) < d$. In other words, every vector is a distance of at most $d - 1$ away from a codeword.
(*Hint:* M is maximal.)