EE/Ma 127a Error-Correcting Codes R. J. McEliece
draft of November 30, 2000 162 Moore

Final Examination

Due: At (or before) 12 noon, Thursday, December 7, 2000: Room 162 Moore

Rules and Regulations: This is a three-hour takehome examination. If possible, use bluebooks. You may consult the class text (Wicker), your own notes and graded homework, and any class handouts, but nothing else. You may also use calculators, computers, and standard math tables. Collaboration is of course not permitted! *Please show all work!* If at the end of three hours, you feel you need more time, you may grant yourself a 90-minute extension to complete the test. Under no circumstances, however, should you spend more than four and one-half consecutive hours on the test. No late examinations will be accepted, except in case of a documented medical crisis.

Note that there are five problems on the exam, weighted unequally,, with a total of 100 points.

Problems to hand in (note that all problems do not count equally) :

Problem 1. (25 points) Suppose you encountered a communications channel that accepted binary words of length n, and the only error patterns ever observed were the $n+1$ patterns 000000, 000001, 000011, 000111, 001111, 011111, 111111 (illustrated for $n = 6$). Design a linear (n, k) code for this channel that will correct *all* such error patterns, and which has as large a rate (i.e., value of k) as possible. Illustrate your construction by exhibiting an explicit parity-check matrix for $n = 7$.

Problem 2. (25 points) Consider the cyclic $(7, 3)$ Abramson code with generator polynomial $g(x) = x^4 + x^3 + x^2 + 1$. It has 16 possible syndromes, but there are only 15 (cyclic) burst error patterns of length 0, 1, and 2. This means there must be one syndrome that does not correspond to any burst of length ≤ 2.

(a) (10 points) Identify this syndrome, where the syndrome of $R(x)$ is $S(x) = R(x) \bmod g(x)$. (Hence the answer to this question will be a polynomial of degree ≤ 3.)

(b) (10 points) What is the minimum weight of an error pattern that produces this syndrome?

(c) (5 points) Characterize all the error patterns that produce this syndrome as completely as you can.

Problem 3. (25 points) Consider the $(15, 7)$ "Hex-BCH" code we discussed in class. It is capable of correcting all error patterns of weight 0, 1, and 2. But if the error pattern has weight 3 or more, one of two bad things will happen:

1. The error pattern will be detected, i.e., the received word will lie at Hamming distance ≥ 3 from evey codeword. This is called *decoder failure.*
2. The error pattern will be miscorrected, i.e., the received word will lie at Hamming distance ≤ 2 from a codeword other than the one transmitted. This is called *decoder error.*

(a) (15 points) Of the $\binom{15}{3} = 455$ error patterns of weight 3, how many will result in decoder error?

(b) (10 points) Of the $\binom{15}{4} = 1365$ error patterns of weight 4, how many will result in decoder error?

[Hint: It may be helpful to know that the code's weight enumerator is

$$A(z) = 1 + 18z^5 + 30z^6 + 15z^7 + 15z^8 + 30z^9 + 18z^{10} + z^{15}.]$$

Problem 4. (15 points) Find a formula for the number of distinct "Hamming" codes of length $2^m - 1$. Here a Hamming code is a $(2^m - 1, 2^m - m - 1)$ binary linear code with minimum distance 3. [Hint: For $m = 3$, the answer is given in Midterm Problem 5b.]

Problem 5. (10 points.) (No computers on this problem.) This problem concerns the "HexField," so you will have to refer to the addition and multiplication tables I handed out. Notice that the "1" row of the addition table and the "F" row of the multiplication table have exactly one entry in common:

$$\begin{array}{cccccccccccccccc} 1 & 0 & 3 & \mathbf{2} & 5 & 4 & 7 & 6 & 9 & 8 & B & A & D & C & F & E \\ 0 & F & D & \mathbf{2} & 9 & 6 & 4 & B & 1 & E & C & 3 & 8 & 7 & 5 & A \end{array}$$

The question is this: if I select the "x" row of the addition table and the "y" row of the multiplication table, how many entries will they have in common? (Just giving the right answer is not enough; I want to know "why.")