EE/Ma 127a Error-Correcting Codes — R. J. McEliece
draft of October 20, 2000 — 162 Moore

Midterm Examination

Due: At (or before) 12 noon, Friday, October 27, 2000: Either in class, or in 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 equally.

Problems to hand in (all problems count equally) :

Problem 1. Use the "Hamming bound" to estimate the minimum possible redundancy r for binary linear codes with the following values of n and d:

(a) $n = 23$, $d = 7$.

(b) $n = 2^m - 1$, $d = 3$, for $m \geq 2$.

(c) $n = 2m + 1$, $d = 2m + 1$, for $m \geq 1$.

(d) In cases (b) and (c), describe codes that achieve the redundancy predicted by the Hamming bound. Do you have an opinion about case (a)?

Problem 2. Design a systematic encoder for a $(7, 4)$ Hamming code, i.e., a rule for appending to each 4-bit data word (x_1, x_2, x_3, x_4) a three bit "check word" (x_5, x_6, x_7) and a corresponding decoding algorithm based on a parity-check matrix H, so that the syndrome $[s_1, s_2, s_3]$ directly gives the position of the error. For example, a syndrome [011] should correspond to an error in x_3, a syndrome [100] corresponds to an error in x_4, etc.

Problem 3. Use the MacWilliams identities to find the possible weight enumerators for all "self-dual" codes of length 4. [A self-dual code is one for which $C^{\perp} = C$.]

Problem 4. Describe a parity-check matrix for a binary linear code with $k = 4$, which is capable of simultaneously correcting one error and one erasure. (That is: if the transmitted codeword suffers at most and error and/or at most one erasure, the decoder will succeed in repairing the damage.)

Problem 5. This problem concerns $(7, 4)$ binary linear codes.

(a) How many such codes are there?

(b) How may have minimum distance $d \geq 3$?