Math 55: Discrete Mathematics, Fall 2008
Reading and Homework Assignment 10

Reminder: Midterm 2 is this Friday, Nov. 7, covering material on homework assignments 5 through 9. The exam will be held in two rooms:

Last Names A-K in 390 Hearst Mining Building (NOT 50 Birge as initially announced)

Last Names L-Z in the usual lecture room (2060 Valley LSB)

Bring scratch paper. You may use one sheet of notes (written on both sides). No other notes, books, calculators or computers may be used. Please arrive early so we can distribute exams. The exam will start promptly at 12:10.

Reading:

Lectures 28-29: Notes on Error-Correcting Codes, Sections 1 and 2; Rosen 3.8

Homework (due Monday, 11/10):

Odd-numbered self-checking exercises:

3.8: 3, 11

Problems to hand in:

3.8: 2(b), 4(c). Then do each problem assuming that the entries of the matrices represent congruence classes mod 7, expressing the answer as a matrix with entries in the set $\{0, 1, \ldots, 6\}$ of remainders mod 7.

(A) Suppose a binary channel makes errors in each bit independently with probability $p = .05$. Calculate to three decimal places: (a) the probability that at least one error occurs if four bits are transmitted without any encoding (b) the probability that at least two errors occur (thus resulting in incorrect decoding) if the four bits are encoded using the 7-bit 1-error-correcting Hamming code discussed in the lecture and in Exercises 8 and 9 of the notes.

(B) For the binary channel in Problem (A), calculate the maximum data rate for reliable transmission allowed by the Shannon upper bound. How does this compare with the data rate achieved by packaging messages into groups of four bits and encoding them with the 7-bit Hamming code as in Problem (A)?

(C) Show that if a 15-bit binary code can always correct 2 errors, the number of codewords cannot exceed 270. Deduce that if a 2-error correcting 15-bit code encodes m-bit messages, then m is at most 8. [Hint: the sets $D_2(C) = \{R : d(C, R) \leq 2\}$ must be disjoint for all codewords C.] It may interest you to know that 2-error correcting codes of length 15 with 8 data bits do exist. There is a linear *BCH code* over $\mathbb{Z}_2$ with these properties.