Mathematics 392 – Seminar in Coding Theory
Midterm Problem Set
February 20, 2002

Ground Rules

The problems below form the midterm problem set announced in the course syllabus. This is an open book, open notes, open Swords 335 assignment. You must work *independently* on these problems, and you may not consult with other faculty members or students. You may consult other sources in the library, on the Internet, etc. but if you find something relevant there, please *footnote it*. When you have finished your solutions, please write out a short statement that you have abided by these ground rules, sign it, and return it with your solutions.

This assignment is due no later than *5:00pm on Wednesday, February 27.*

I.

A) Show that if a binary code of length $n = 8$ can correct any single error then it contains at most 28 different words.

B) Is it possible for a binary code C (not necessarily linear) to contain two words u and v (among others) such that if u is transmitted, then any error of weight at most 2 can be corrected, while if v is transmitted, then there is some error of weight 1 that cannot be corrected? If so give an example; if not say why not.

II. Two additional code constructions. Let C be an (n, k, d) binary linear code.

A) We say the code C' is obtained by *puncturing* C *at location* i if the words of C' are constructed by deleting the ith locations in all the words of C. Show that C' is also linear with parameters (n', k', d') satisfying $n' = n - 1$, $k - 1 \leq k' \leq k$, and $d - 1 \leq d' \leq d$. Show by examples that both of these values for k', d' are possible.

B) We say the code C'' is obtained by *shortening* C *at location* i if the words of C'' are constructed by deleting the ith locations in all words in C *that have a 0 in location* i. Show that C'' is also linear and discuss its possible parameters (n'', k'', d''). Show by example that $d'' > d$ is possible.

III.

A) Let C be the linear code with $n = 8, k = 4$ and the 4×8 generator matrix:

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

Construct the SDA for this code, and use it to decode the received words $y = 11110111$, $y = 00100010$.

IV. The minimum distance of the code in III is $d = 3$. Can you do better with $n = 8$, $k = 4$? For instance, are there $(8, 4, 4)$ binary linear codes? If so construct one; if not say why not. (Hint: You can specify a code by giving a parity check matrix. What has to be true about H to get $d = 4, 5$, etc.)

V. Let C be the linear code with parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The rows of H are all the nonzero words of length 3, listed in a particular order. $n = 7$, and $k = 4$ for this code.

A) What is the minimum distance of C and what does this say about error-correcting capacity of C?

B) We want next to understand a very interesting feature of this example. Show that every coset of this code has a *unique* coset leader of weight 0 or 1, and that that the Hamming ball of radius 1 centered at each codeword of C contains exactly one vector from each of the cosets of C. (Don't work too hard!) Note: what you are proving here shows that *every received word* would be decoded to some codeword by syndrome decoding – there are no cases where the SDA contains more than one possible error vector of smallest weight in a coset.

C) For which combinations of a blocklength n and dimension k is it possible for a binary linear code to have the property from part B (that is: the Hamming ball of radius 1 centered at each codeword contains exactly one vector from each of the cosets of C).