ENEE626. Midterm examination. Date due Thursday October 28, 2010.

1. *This is a take-home exam.* If you are not coming to class on 10/28, please make sure to submit the paper *before* class. No late papers will be accepted for whatever reason.

2. Any sources, such as books, course notes, and WWW can be consulted. However you must work on your own, not turning to anyone for advice.

3. *Complete* proofs are required. Intermediate calculations should be shown unless they are done by computer. Computers are permitted in problems 1(g), 1(i) and 2 only. All the other problems should be done by hand. If applicable, clearly identify the answer to the problem.

4. Please write *concisely*, restricting your answer to the solution of the problem.

1. (75 pts) Consider a linear code $\mathcal{C}$ defined by its parity check matrix

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

(a) (5pt) Determine the parameters $[n, k, d]$ (length, dimension, distance) of the code $\mathcal{C}$.

(b) (10pt) Show that every vector $\boldsymbol{x} \in \mathbb{F}_2^n$ of weight 3 can be transformed into a vector of the code $\mathcal{C}$ by changing one 0 into 1. Use this fact to find the number A_4 of vectors of weight 4 in $\mathcal{C}$.

(c) (12pt) Use an analogous argument to determine the number of vectors of weight 6 in $\mathcal{C}$. Make sure that your answers match the answers in (g) below.

(d) (8pt) Show that any vector $\boldsymbol{x} \in \mathbb{F}_2^n$ is at the Hamming distance 2 or less from a codeword of the code $\mathcal{C}$.

(e) (6pt) How many vectors in $\mathbb{F}_2^n$ are neither codewords of the code $\mathcal{C}$ nor at distance 1 from a codeword in the code $\mathcal{C}$?

(f) (8pt) Determine (with proof) the weight distribution of the code $\mathcal{C}^{\perp}$.

(g) (6pt) Using the MacWilliams theorem, determine the weight distribution of the code $\mathcal{C}$.

(h) (8pt) Using (a),(d), determine the number of coset leaders of weight $w = 1, 2, \dots$.

(i) (12pt) The code $\mathcal{C}$ is used for transmission over a BSC(p). Based on what you know about $\mathcal{C}$ guess the number of double errors that it corrects (explain your answer; no proof is required).

Use this information to find the value $p_0 \geq 0$ such that for all $0 \leq p \leq p_0$ the error probability of decoding estimated by the Bhattacharyya bound is at most 20 times the true value of this probability.

2. (40 pts) Give an example of a received vector $\boldsymbol{r}$ for an RS code for which Sudan's algorithm outputs more than one codeword. Show all the steps of the decoding algorithm with intermediate results. The choice of the field $\mathbb{F}_q$ and the code's parameters $[n, k]$ are up to you; however you must choose $n \geq 11, n-4 \geq k \geq 4$ (in other words, do not take a code of length $n = 1$ or a code with the parameters $[n, n, 1]$).