Mathematics 392 – Seminar in Coding Theory
Problem Set 2
February 1, 2002

A linear code C is a vector subspace of K^n for some n (as in our text, K is the binary field $\{0, 1\}$ with addition and multiplication modulo 2). One of the first advantages of linear codes is that they let us bring most of the familiar tools of linear algebra – vectors, matrices, linear independence, bases for subspaces and the notion of dimension – to bear to study questions about codes. We will always use the following notation for linear codes:

$$\begin{cases} n & \text{is the block length} \\ k & \text{is the dimension (information bits per codeword)} \\ d & \text{is the minimum distance} \end{cases}$$

Problems – due: in class Friday, February 8

A) From the text: 2.1.1 (and say how you know in each case)

B) From the text: 2.1.4

C) From the text: 2.3.17

D) For each of the following sets, list the elements of the linear code $C = \langle S \rangle$, give the parameters (n, k, d) of C, give a basis of C, and find a basis of the dual linear code $C^{\perp}$.
  1) $S = \{0101, 1010, 1100, 0011, 1111\}$
  2) $S = \{11000, 01111, 11110, 01001\}$
  3) $S = \{10001101, 01001000, 11001111, 01100101\}$

E) From the text: 2.3.22

F) Prove Theorem 2.3.19 from the text. (Hint: Follow what you probably did for problem E: construct the basis one vector at a time, and count how many choices you have at each step. Then think about how many of your bases are equal as sets – recall the order of the elements of a set does not matter: $\{a, b, c\} = \{c, b, a\}$, etc.)

G) From the text: 2.4.6