Math 350
Spring, 2003

HOMEWORK #6

Do 50 points of the following problems (due 2/20/03).

10 pts. **1** Prove that all q-ary linear Hamming Codes of a given length are equivalent.

All q-ary linear Hamming codes are defined by giving a parity check matrix. The columns of this parity check matrix include one element from each one dimensional subspace of F_q^r. If we swap columns, we can get the same order of one dimensional subspaces, and we can then use scalar multiplication to make the parity check matrices the same. If the parity check matrices can be made equivalent using the equivalence operations, then we the codes must be equivalent.

20 pts. **2** Construct H(5,3).

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots(27-more-0's)\cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots(27-1's)\cdots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots(alternatingvalues)\cdots \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & \cdots(alternatingvalues)\cdots \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & \cdots(alternatingvalues)\cdots \end{pmatrix}$$

$$\begin{pmatrix} 1 & \cdots(76-more-1's) & 1 & 1 & 1 & 1 \\ 0 & \cdots(alternatingvalues) & 2 & 2 & 2 & 2 \\ 0 & \cdots(alternatingvalues) & 2 & 2 & 2 & 2 \\ 0 & \cdots(alternatingvalues) & 1 & 2 & 2 & 2 \\ 0 & \cdots(alternatingvalues) & 2 & 0 & 1 & 2 \end{pmatrix}$$

10 pts. **3** Use the decoding procedure that we discussed in class to decode 1001001, 0101101, and 1110000 (in Ham(3,2)).

If you multiply 1001001 by the transpose of the parity check matrix we listed in class, you get 010. This indicates that you need to change the second position, so we should decode 1001001 as 1101001. Following the same procedure, the received word 0101101 times the transpose of the parity check matrix is 100, so we change the fourth position to get 0100101. The final received word 1110000 multiplies times the parity check matrix to get 000, so it is a codeword.

20 pts. **4** Use the technique described by theorem 8.4 to find a linear code of length $n = 6$ over Z_3 with $d = 3$ that has the most number of codewords that you can (you should be able to find a code with 27 codewords). Make sure you explain what you are doing.

We will do this by construcing a parity check matrix. We want to use as few rows in the parity check matrix as we can, so we try to use 2 rows. The first column will be 001; the second column must be chosen so that it is not a scalar multiple of the first, so we choose 010; the third column must be chosen so it is not a scalar multiple of either of the first two, so we choose 011; we choose 012 for the fourth; 100 for the fifth; and 101 for the sixth (there are many other ways you can do this). Since the dimension of the Row Space of this matrix is 3, that implies that the dimension of the Null Space (in other words the dimension of the code) is 6-3=3. The minimum distance is at least 3 because no two columns are linearly dependent (they are not scalar multiples), and there are codewords of weight 3 (112000 for example).

20 pts. **5** Use the technique described by theorem 8.4 to find a linear binary code of length $n = 8$ with $d = 5$ that has the most number of codewords that you can (you should be able to find a code with 4 codewords). Make sure you explain what you are doing.

We will want to use 6 rows in the parity check matrix, and we need to find 8 binary vectors of that length so that no 4 of them are linearly independent. One possible choice is 100000; 010000; 001000; 000100; 000010; 000001; 111100; 001111. If those are the columns of the parity check matrix, then 11110010 is a word of weight 5.

30 pts., $\star$ **6** Consider the code generated by the parity check matrix for Ham(4,2) (this is the orthogonal code of the binary Hamming code of length 15): what is the minimum weight of this code? Suppose that we take all of the nonzero codewords of this orthogonal code and use them as the rows of an incidence matrix: show that this forms a block design. What are (v, k, λ, r, b) for this design? This is worth 50 pts if you can state the generalization to the orthogonal code of Ham(r,2) for any r, and you can give reasons why you think that will work.

All of the rows of Ham(4,2) have weight 8, and if you add any two together you get another word of weight 8. In fact, all 15 of the nonzero codewords of this code have weight 8. If we form the incidence matrix as described, then there will be 15 rows and columns (those are the v and b parameters of the design); the row and column sums are 8 (these are the k and r of the design); and any two points will be on $\lambda = 4$ blocks (this can be checked in this case, or you could argue that any pair of rows has exactly 4 points in common because the sum must have weight 8).

The general case can follow by induction. A key observation for the general case is that the weights of the nonzero codewords is always 2^{r-1}, so any two codewords will have exactly 2^{r-2} 1's in common, and this is the λ. The parity check matrices are essentially formed from the previous smaller Hamming parity check matrix, and we can use the inductive step to get the properties of the incidence matrix. I will fill in the details if anyone is interested.