Math 350
Spring, 2000

HOMEWORK #4

Do 50 points of the following problems (due 2/10/00).

15 pts. **1** Find the n,M, and d of the binary code whose generator matrix is

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

Since the rows are linearly independent, this code has $M = 8$; the length is $n = 7$. The codewords in this code will have even weight since the sum of any two rows has even weight, and it is not possible to have a word of weight 2, so the minimum weight is $d = 4$.

More answers on next pages!

15 pts. **2** Put the following generator matrix into standard form.

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

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

$$\cong$$

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

$$\cong$$

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

$$\cong$$

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

$$\cong$$

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

20 pts. **3** Let C be a code. Define $C^\perp = \{x \in F_2^n | \sum_{i=1}^n x_i c_i = 0(\text{mod}2)$ for every $c \in C\}$. Find $E_n^\perp$, and argue why you think that you have the correct answer.

$E_n^\perp = \{000\cdots 0, 111\cdots 1\}$. Certainly, these two codewords are contained in $E_n^\perp$. There are two ways to show that this is it: (1) If $E_n^\perp$ contained any word e so that $1 \leq w(e) \leq n-1$, then e has at least one position with a 1 and one position with a 0. We form a codeword in E_n so that the codeword has a 0 in every position except one of the positions with a 1 and one with a 0 (the weight of this new codeword is 2). When we take the dot product of e with this new codeword, we get 1, contradicting the definition. Thus, e could not have been in $E_n^\perp$. (2) The dimension of E_n is $n-1$, so the dimension of its $\perp$ is $n-(n-1)=1$. Since we know that $\{000\cdots 0, 111\cdots 1\}$ is contained in $E_n^\perp$, it must be all of it.

⋆ 30 pts. **4** From the vector space $V(2,q)$, q a prime power, an incidence structure A_q is defined as follows: the 'points' of A_q are the vectors of $V(2,q)$. The 'lines' of A_q are the one-dimensional subspaces of $V(2,q)$ and their cosets. The point P 'belongs to' the line L if and only if P is in L. Prove that A_q is a $(v,k,\lambda,r,b) = (q^2, q, 1, q+1, q^2+q)$ design. List the points and lines of A_2 and A_3. Form the incidence matrix for A_2 and A_3 and compute the dimension and minimum distance for the binary linear codes defined by the rowspaces of these matrices.

Clearly there are q^2 points (there are that many vectors in $V(2,q)$). Each one-dimensional subspace is all the scalar multiples of a single vector, and there are q scalars, so there are that many points on a block. Take any pair of points: if they are scalar multiples, then they will be on the line determined by either of the (nonzero) points. If they are not scalar multiples, then if we subtract them, they are both on the line $p_1 + < p_2 - p_1 >$. In either case, this is the only line they will be a part of. To see that each point is on $q+1$ lines, take any point p and any line l not containing p. There will be a distinct line through p and each of the q points on l, and there will be another line through p that is a coset of l that is parallel to l. That makes $q+1$. To count the number of lines, we need to count the number of one dimensional subspaces (there are $\frac{q^2-1}{q-1} = q+1$ of them) and multiply that number by the number of cosets of each line (there are q) for a total of q^2+q lines.

The points of A_2 are 00,01, 10, and 11. The lines are $\{00, 01\}; \{10, 11\}; \{00, 10\}; \{01, 11\}; \{00, 11\}$; and $\{01, 10\}$. The points of A_3 are 00,01,02, 10,11,12,20,21, and 22. The lines are $\{00, 01, 02\}; \{10, 11, 12\}; \{20, 21, 22\}; \{00, 10, 20\}; \{01, 11, 21\}; \{02, 12, 22\}; \{00, 11, 22\}; \{10, 21, 02\}; \{20, 01, 12\}; \{00, 12, 21\}; \{10, 22, 01\}$; and $\{20, 02, 11\}$.

The incidence matrix for A_2 is (the columns are indexed by the points 00,01,10,and 11, and the rows are indexed by the lines):

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

The rowspace of this incidence matrix is E_4, so the dimension is 3 and the minimum distance is 2.

The incidence matrix for A_3 is (the columns are indexed by the points 00,01,02,10,11,12,20,21, and 22, and the rows are indexed by the lines):

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

The rows 1,2,3,4,5,7,8,10, and 11 are linearly independent, so the dimension is 9. The minimum distance is 1: $r_2 + r_3 + r_4 + r_7 + r_{10} =$ 100000000. (NOTE: you could argue that the minimum distance has to be 1 since the code is as high a dimension as it can be.)