MATH 4383/5383
Exam I
ANSWERS

INSTRUCTIONS

Show your work on all problems.

1. Let $n \geq 3$ and let a, u, and v be binary n-tuples. Suppose that $d(a,u) = d(a,v) = n-1$. Prove that $u \in D_2(v)$.

ANSWER Let $a = (a_1, \ldots, a_n)$; $u = (u_1, \ldots, u_n)$; and $v = (v_1, \ldots, v_n)$. Since $d(a,u) = n-1$, there is some i with $a_i = u_i$, and for $k \neq i$, $a_k \neq u_k$. Since $d(a,v) = n-1$, there is some j with $a_j = v_j$, and for $m \neq j$, $a_m \neq v_m$. This means that for p different from both i and j, both u_p and v_p are different from a_p. In the binary situation, this means $u_p = v_p$ for $p \neq i, j$. So u and v can differ in at most 2 place (i and j), so $d(u,v) \leq 2$ and $u \in D_2(v)$.

2. Let C be the Hamming code Ham(2).

   1. Write the standard check matrix H for C.

   2. List the words in C.

   3. Write the standard generator matrix G for C.

ANSWER

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

If $u = (u_1, u_2, u_3)$ then

$$Hu^T = \begin{bmatrix} u_1 + u_2 \\ u_1 + u_3 \end{bmatrix}$$

so $Hu^T = 0$ implies that $u_1 + u_2 = 0$ (or $u_1 = u_2$) and $u_1 + u_3 = 0$ (or $u_1 = u_3$) so $u_1 = u_2 = u_3$. Thus

$$C = \{(0,0,0), (1,1,1)\}$$

Using the form $H = [AI_n]$ we have $n = 2$ and

$$A = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

So

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

3. The following 3×5 matrix is the check matrix of a $(5, 2)$ binary linear block code C. Find a generator matrix for C.

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

ANSWER Let $u = (u_1, u_2, u_3, u_4, u_5)$. Suppose $u \in C$. Then $Hu^T = 0$ implies the following three equations:

$$u_1 + u_2 + u_4 = 0 \quad (1)$$
$$u_2 + u_3 + u_4 = 0 \quad (2)$$
$$u_3 + u_4 + u_5 = 0 \quad (3)$$

Equation (3) says that $u_3 = u_4 + u_5$. Putting this in Equation (2) says that $u_2 = (u_4 + u_5) + u_4 = u_5$ and putting this in Equation (1) says that $u_1 = u_5 + u_4$. So

$$u = (u_4 + u_5, u_5, u_4 + u_5, u_4, u_5)$$

Taking $u_4 = 1, u_5 = 0$ gives the word $(1, 0, 1, 1, 0)$; taking $u_4 = 0, u_5 = 1$ gives the word $(1, 1, 1, 0, 1)$ and the transpose of these words will be columns of a generator matrix:

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

4. Let $C \subset \mathbb{Z}_2^n$ be an (n, m) linear block code with check matrix H. Suppose that $v_1, \ldots, v_k \in \mathbb{Z}_2^n$ are binary n tuples with the same syndromes (computed with H). Prove that

$$k \leq 2^m.$$

ANSWER The hypothesis is that $Hv_1^T = Hv_2^T = \cdots = Hv_k^T = w$ for some column vector w. So for every i, $H(v_1 + v_i)^T = Hv_1^T + Hv_k^T = w + w = 0$, so each $v_1 + v_i$, $1 \leq i \leq k$ is a codeword. As C is an (n, m) code $\mid C \mid = 2^m$ so there are 2^m codewords. Thus $k \leq 2^m$.

5. Let C be a linear code with generator matrix

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

What is the distance of C?

ANSWER Since C is linear, $d(C) = \min\{\mathrm{wt}(u) \mid u \in C, u \neq 0\}$. The columns of G are the transposes of codewords, so $(1, 0, 0, 1, 1, 1)$ (transpose of column one) and $(0, 1, 0, 1, 1, 1)$ (transpose of column two) are codewords. As C is linear, the sum $(1, 1, 0, 0, 0, 0)$ of these two codewords is a codeword, and this one has weight 2. Note that G is a standard generator matrix, and the corresponding check matrix is then

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

As no column of H is 0, no word of C is of weight 1, so $d(C) = 2$.