EE/Ma 127a Error-Correcting Codes — R. J. McEliece

Draft of October 9, 2000 — 162 Moore

Homework Assignment 1, Solutions

Problem 1. The parity-check matrix for the (7,4) Hamming code is:

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

For each codeword $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, we have:

$$x_1h_1+x_2h_2+x_3h_3+x_4h_4+x_5h_5+x_6h_6+x_7h_7=0 \qquad (1)$$

When x_i, x_j, x_k are erased, from equation (1) we get:

$$x_ih_i+x_jh_j+x_kh_k=C \qquad (2)$$

Here C is a constant vector determined by the four known symbols in the codeword.

Equation (2) has a unique solution if and only if h_i, h_j, h_k are linearly independent. Since all the h_i (i=1,2, …,7) are none-zero and distinct, equation (2) has a unique solution if and only if:

$$h_i+h_j+h_k\neq 0 \qquad (3)$$

By equation (3) we found that of all the 35 erasure patterns (i, j, k), the following 7 patterns:

(1,2,4), (1,3,7), (2,3,6), (3,4,5), (1,5,6), (2,5,7), (4,6,7)

cannot be corrected. All the other 35-7=28 erasure patterns can be corrected.

Problem 2. A basis for the nullspace for the (8,4) binary linear code consists of four linearly independent vectors all orthogonal to the four row vectors of generator matrix G. Here the four row vectors of G happen to be such a basis.

Problem 3.

(a) The row-reduced echelon generator matrix for C is:

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

(b) The codeword corresponding to any triple-symbol set (u_1, u_2, u_3) generated by the row-reduced echelon generator matrix in (a) is:

$(u_1, u_2, u_1+u_2, u_3, u_1+u_3, u_1+u_2+u_3)$.

So a parity-check matrix for C is:

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

Problem 4.

(a)

k	1	2	3	4	5	6	7
$\begin{bmatrix} 7 \\ k \end{bmatrix}_2$	127	2667	11811	11811	2667	127	1

(b) Let q=1+δ, then

$$\lim_{q\to 1}\begin{bmatrix} n \\ k \end{bmatrix}_q = \lim_{q\to 1}\prod_{i=0}^{k-1}\frac{q^n - q^i}{q^k - q^i} = \lim_{q\to 1}\prod_{i=0}^{k-1}\frac{q^{n-i} - 1}{q^{k-i} - 1} = \lim_{\delta\to 0}\prod_{i=0}^{k-1}\frac{(1+\delta)^{n-i} - 1}{(1+\delta)^{k-i} - 1} = \lim_{\delta\to 0}\prod_{i=0}^{k-1}\frac{1+(n-i)\delta + o(\delta) - 1}{1+(k-i)\delta + o(\delta) - 1}$$

$$= \prod_{i=0}^{k-1}\frac{n-i}{k-i} = \binom{n}{k}$$

Problem 5.

(a) Parity-check matrix H=(h_1 h_2 h_3 … h_n), here each h_i (i=1,2,3,…,n) is a $r\times 1$ vector. In order to be able to correct all single bit errors, all the h_i should be different and none of them is an all-zero vector. So

$$2^r - 1 \geq n$$

Here n=k+r=32+r. So r≥6.

Now to detect all double bit errors, no h_i+h_j (i,j=1,2,…,n. i≠j) can be the all-zero vector or any of the n column vectors of H. Fix i and it's easy to see that h_i+h_j (j=1,2,…,n. j≠i) can take on n-1 values. So

$$2^r - 1 \geq n + (n-1)$$

From that equation we get r≥7. So n is at least 39. The code can be achieved by first designing a (38,32) code and then extending it to be a (39, 32) code.

(b) A parity-check matrix for the (39, 32) code is:

$$H = (h_1\ h_2\ h_3\ \dots\ h_{39})$$

Here all the h_i (i=1,2,…,39) are distinct 7×1 vectors, and each h_i's last entry is 1.