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

draft of November 7, 2000 — 162 Moore

Solutions to Midterm Examination

Problem 1.

(a) $2^r \ge \binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}$. Therefore $r \ge 11$.

(b) $2^r \ge \binom{2^m-1}{0} + \binom{2^m-1}{1} = 2^m$. Therefore $r \ge m$.

(c) $2^r \ge \sum_{j=0}^{m} \binom{2m+1}{j} = 2^{2m}$. Therefore $r \ge 2m$.

(d) Case (b): the family of $(2^m-1, 2^m-m-1, 3)$ Hamming codes. Case (c): The family of $(2m+1, 1, 2m+1)$ repetition codes (see Wicker, p. 78, second bullet). Finally, the case (a) corresponds to the famous $(23, 12, 7)$ Golay code (see Wicker, p. 78 fourth bullet), which we will study in detail later in the class.

Problem 2.

The trick is for the encoder and decoder to use different (but row-equivalent) parity-check matrices. In order that a single error in position i produce a syndrome which gives the binary representation of i, the decoder's parity-check matrix needs to be

$$H_{\text{decoder}} = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

However, for the encoding to be systematic, we need to put H_{decoder} into systematic form. A few row operations puts H_{decoder} into the form

$$H_{\text{encoder}} = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array},$$

which corresponds to the systematic encoding rules

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4 \\ x_6 &= x_1 + x_3 + x_4 \\ x_6 &= x_1 + x_2 + x_4. \end{aligned}$$

Problem 4. If $A(z) = A_0 + A_1 z + A_2 z^2 + A_3 z^3 + A_4 z^4$ is the weight enumerator of the code, then by the MacWilliams identities,

$$\begin{aligned} &4(A_0 + A_1 z + A_2 z^2 + A_3 z^3 + A_4 z^4) \\ &\quad = A_0(1+z)^4 + A_1(1-z)(1+z)^3 + A_2(1-z)^2(1+z)^2 + A_3(1-z)^3(1+z) + A_4(1-z)^4. \end{aligned}$$

Equating coefficients of A_i on both sides, and using the side conditions $A_0 = 1$, $A_0 + A_1 + A_2 + A_3 + A_4 = 4$, we find (after some linear algebra) there are exactly four soultions:

$$\begin{aligned}(A_0, A_1, A_2, A_3, A_4) &= (1, 1, 1, 1, 0)\\ &= (1, 0, 1, 2, 0)\\ &= (1, 2, 1, 0, 0)\\ &= (1, 0, 2, 0, 1)\end{aligned}$$

However, the first three of these solutions cannot correspond to a self-dual code, since no self dual code can contain a word of odd weight (a word of odd weight can't be orthogonal to itself). The only solution is then

$$(A_0, A_1, A_2, A_3, A_4) = (1, 0, 2, 0, 1),$$

which does correspond to a self-dual code, with one possible generator matrix

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Problem 4. (Solution due to Suleyman Gokyigit.)

Suppose the received word has an erasure and an error. A possible decoding strategy is to randomly guess a 0 or a 1 for the erased bit. If the correct guess was made, then the problem becomes that of correcting a single error. If not, the problem becomes that of detecting a double error. (If the decoder detects two errors, it knows it must have guessed wrong and can reverse its guess.) Thus we need a single-error-correcting, double-error-detecting code, which requires $d_{\min} \geq 4$. We know that the minimum redundancy for $d_{\min} = 4$ is $r = 4$, corresponding to the $(8, 4)$ extended Hamming code. One parity-check matrix is therefore

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

Problem 5.

(a) This problem was part of Homework Assignment 1, problem 4 (a). The answer is

$$\begin{bmatrix} 7 \\ 4 \end{bmatrix}_2 = 11,811.$$

(2) A $(7, 4)$ code has $d_{\min} = 3$ if and only if it is described by one of the 7! parity check matrices whose columns are the 7 nonzero three-dimensional vectors. On the other hand, weach such code has exactly $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 168$ such parity-check matrices. Thus there are $7!/168 = 30$ such codes.