R. J. McEliece
162 Moore

Solutions to Final Examination

Problem 1.

Each of the $n+1$ error patterns must produce a distinct syndrome, and there are 2^r possible syndromes, so we have $2^r \ge n+1$. Since r must also be an integer, a *necessary* condition for the existence of a code with the desired error-correction capabilities is

$$r \ge \lceil \log_2(n+1) \rceil. \tag{1}$$

The inequality (1) is also sufficient, as we can see as follows. If $2^r \ge n+1$, we can construct an $r \times n$ "Hamming" parity-check matrix of the form

$$H = (\, h_1 \quad h_2 \quad \cdots \quad h_n \,),$$

where the columns $h_1, \ldots, h_n$ of H are n distinct r-vectors. What we want to do is convert H into an $r \times n$ matrix H' of the form

$$H' = (\, h'_1 \quad h'_2 \quad \cdots \quad h'_n \,),$$

such that

$$\begin{aligned} h'_n &= h_n \\ h'_n + h'_{n-1} &= h_{n-1} \\ &\vdots \\ h'_1 + \cdots + h'_n &= h_1, \end{aligned}$$

which will guarantee that the syndromes of the given error patterns are distinct. This is easy to do. Indeed, if we define the columns of H' recursively as follows:

$$\begin{aligned} h'_n &= h_n \\ h'_{n-1} &= h_n + h_{n-1} \\ &\vdots \\ h'_1 &= h_2 + h_1, \end{aligned}$$

the desired relationship will hold. For example with $n = 7$ and $r = 3$, if we choose $h_7 = 001$, $h_6 = 010$, $\ldots$, $h_1 = 111$, the resulting matrix H' is

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

Problem 2.

(a) The syndromes of the 15 correctable bursts are 0 (for no errors), $x^i \bmod g(x)$ for $i = 0, \ldots, 6$ (the single bit errors), and $x^i(x+1) \bmod g(x)$ for $i = 0, \ldots, 6$ (the bursts of length 2). By actual calculation, we find that the only polynomial of degree ≤ 3 which is not of this form is $x^3 + x + 1$. Thus the missing syndrome is $S(x) = x^3 + x + 1$.

(b) The minimum weight is 3—see part (c).

(c) If $R(x) \bmod (x^4 + x^3 + x^2 + 1) = x^3 + x + 1$, then $R(x) \bmod (x^3 + x + 1) = 0$ and $R(x) \bmod (x+1) = 1$. Thus $R(x)$ is an odd weight codeword in the $(7,4)$ cyclic code with generator polynomial $x^3 + x + 1$. This set consists of the seven cyclic shifts of 1101000, plus the vector 1111111.

Problem 3.

(a) If the decoder is given a vector R which is distance 3 from the transmitted codeword A, it will make an error iff it can find a codeword $B \neq A$ with $d(R, B) = 0$, 1, or 2. $d(R, B) = 0$ and 1 are impossible by the triangle inequality, and $d(R, B) = 2$ is possible iff $d(A, B) = 5$. But according to the given weight enumerator, each codeword A has exactly 18 distance-5 neighbors B. For each such B there are $\binom{5}{3} = 10$ possible R's with $d(A, R) = 3$ and $d(R, B) = 2$. Thus the total of "bad" weight 3 error patterns is

$$\binom{5}{3} A_5 = 10 \times 18 = 180.$$

(b) If the decoder starts with a vector R which is distance 4 from a codeword A, it will make an error iff it can find a codeword $B \neq A$ with $d(R, B) = 0$, 1, or 2. $d(R, B) = 0$ is impossible (why?). $d(R, B) = 1$ is only possible if $d(A, B) = 5$, in which case there are $\binom{5}{4} = 5$ R's with $d(A, R) = 4$ and $d(R, B) = 1$. $d(R, B) = 2$ is possible only if $d(A, B) = 6$,, in which case there are $\binom{6}{4} = 15$ R's with $d(A, R) = 4$ and $d(R, B) = 2$. Thus the total number of "bad" error patterns of weight 4 is

$$\binom{5}{4} A_5 + \binom{6}{4} A_6 = 5 \cdot 18 + 15 \cdot 30 = 540.$$

Problem 4. The columns of the parity-check matrix for a Hamming code of length $2^m - 1$ must be the $2^m - 1$ nonzero m-vectors is some order, so there are $(2^m - 1)!$ possible H's. However, each code has $(2^m - 1)(2^m - 2) \cdots (2^m - 2^{m-1})$ parity-check matrices, so there are a total of

$$\frac{(2^m - 1)!}{(2^m - 1)(2^m - 2) \cdots (2^m - 2^{m-1})}$$

such codes.

Problem 5. The z entry in the x row of the addition table is $x + z$. Similarly the z entry of the y row of the multiplication table is yz. The question, therefore, is this: For a fixed

x and y, how many solutions z are there to the equation $x + z = yz$? Rearranging the equation we get

$$z(y + 1) = x.$$

If $y + 1 \neq 0$, i.e., $y \neq 1$, we can divide by $y + 1$ and obtain $z = x/(y + 1)$ as the unique solution. On the other hand, if $y + 1 = 0$, i.e., $y = 1$, then the equation is $z \cdot 0 = x$, which is either true for all z's (when $x = 0$) of no z's, (when $x \neq 0$). In summary:

$$\text{no. of matches} = \begin{cases} 1 & \text{if } y \neq 1 \\ 0 & \text{if } y = 1 \text{ and } x \neq 0 \\ 16 & \text{if } y = 1 \text{ and } x = 0. \end{cases}$$