Problem 1. If we restructure the message into a 11×29 matrix, we can see that the ones form the shape of the number 1608.

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

I'm not sure which mathemetician this refers to though.

Problem 2. Suppose that the binary code $\mathcal{C}$ is an (n, M, d) code. Prove that

- If $s \leq d-1$, then C can detect up to s errors in any codeword.

  Let $c \in \mathcal{C}$ be a codeword, and let ϵ have weight $s > 0$. Let $c_2 \in \mathcal{C}, c_2 \neq c$ Then

  $$d(c+\epsilon, c_2) \geq d(c_2, c) - d(c, c+\epsilon) \geq d - s \geq 1$$

  Hence, $c + \epsilon$ is not a codeword in C, and we can detect that an error has occured.

- If $2t \leq d-1$, then C can correct up to t errors in any codeword.

  Let $c \in \mathcal{C}$ be a codeword, and let ϵ have weight $t > 0$. Let $c_2 \in C, c_2 \neq c$. We can can then calculate

  $$d(c_2, c+\epsilon) \geq d(c, c_2) - d(c, c+\epsilon) \geq d - t \geq (2t+1) - t = t + 1 > t = d(c, c+\epsilon)$$

  Hence, if there are t or fewer errors, $c + \epsilon$ is closer to c than any other codeword in $\mathcal{C}$, and therefore, the errors can be corrected.

Problem 3. Let $\mathcal{C}$ be the linear binary code whose parity check matrix is

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

- Find a generator matrix of the code

  We are looking for a basis of the null space of A. We start by putting A into row echelon form

  $$\bar{A} = \begin{pmatrix} 1&0&0&0&0&1&1\\ 0&1&0&0&1&0&1\\ 0&0&1&0&1&1&0\\ 0&0&0&1&1&0&1 \end{pmatrix}$$

  Then $\bar{A}$ is in the form $\left(I|P\right)$. Then a basis for the null space of this matrix is given by $G = \left(P^{\perp}|I\right)$ So

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

- The matrix with its all the codewords as rows is

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

- The code represents 3 bit messages as 7 bit codewords, and the minimum (non-zero) weight is 4 so this is a $[7, 3, 4]$ code.
- The covering radius of the code is 2, since the maximum distance between any two codewords is also 4.
- The minimum weight of the code is 4, so this code can correct 1 error, and can detect up to 3 errors.

Problem 4. Let C be a binary linear code, and H be the parity check matrix for C. Then for a codeword c, we have $Hc = 0$. Let $\bar{c} = c + \epsilon$ for some error ϵ. Then

$$H\bar{c} = H(c + \epsilon) = Hc + H\epsilon = H\epsilon$$

Hence, the syndrome of $\bar{c}$ is the same as the syndrome of the error itself. Furthermore, we can decompose the error ϵ into the sum of vectors of weight 1, where ϵ_n represents the vector of weight one with a 1 in column n. Then

$$H\epsilon = H\sum_{n=1}^{N} \epsilon_n = \sum_{\epsilon_n = 1} H\epsilon_n$$

Problem 5. Let $C + \epsilon$ be a coset of the code $\mathcal{C}$ in the carrier space V. Let $x \in C + \epsilon$, which means that $x = c + \epsilon$ for some $c \in C$. Then the syndrome of x is $Hx = H(c + \epsilon) = Hc + H\epsilon = H\epsilon$. Now let $x \in V$, and Hx be the syndrome of x. Let $y \in V$ such that $Hx = Hy$. Then $Hx = H\epsilon_x = H\epsilon_y = Hy$, and so $C + \epsilon_x = C + \epsilon_y$. Hence, there is a 1-1 correspondence between syndromes and cosets.

Problem 6. In order for a decoder error to occur for the code C in problem 3, at least two single bit errors must be introduced into a codeword.

Hence, the probability of a decoder error is

$$\sum_{n=2}^{7} p^n (1-p)^{7-n} \binom{7}{n} = 1 - \left(p^0 (1-p)^7 \binom{7}{0} + p^1 (1-p)^6 \binom{7}{1} \right) = 1 - 0.999^7 + (0.001)(0.999^6)7 = 0.013937$$

Problem 7. Let C be a t-error correcting binary code of length n, containing M codewords. Let ϵ have weight i. Then there are exactly $\binom{n}{i}$ possible errors ϵ with that weight. And so the total number of words that differ from a codeword c by less than or equal to t errors is

$$M\left(1 + \binom{n}{1} + \cdots + \binom{n}{t}\right)$$

Clearly, if this number is greater than 2^n, then we have more words than there are words in the carrier space, which is a contradiction.

Problem 8. In order for C to be a perfect code, we must have

$$M\left(1 + \binom{n}{1} + \cdots + \binom{n}{t}\right) = 2^n$$

That is, if for all M codewords we have a sphere of radius t, the union of all of the resultiong words is the whole space V.

By brute force, and by filtering out all of the trivial codes where $d < 3$, we have the list of all perfect codes where $n \leq 100$:

[3,2,3] [5,2,5] [7,16,3] [7,16,4] [7,2,7] [9,2,9] [11,2,11] [13,2,13] [15,2048,3] [15,2048,4] [15,2,15] [17,2,17] [19,2,19] [21,2,21] [23,4096,7] [23,4096,8] [23,2,23] [25,2,25] [27,2,27] [29,2,29] [31,67108864,3] [31,67108864,4] [31,2,31] [33,2,33] [35,2,35] [37,2,37] [39,2,39] [41,2,41] [43,2,43] [45,2,45] [47,2,47] [49,2,49] [51,2,51] [53,2,53] [55,2,55] [57,2,57] [59,2,59]