1. Suppose that a vector $\mathbf{y}$ corrupted by at most $\tau$ errors and $\sigma$ erasures was observed at the channel output. Delete (puncture) from both $\mathbf{y}$ and $\mathbb{C}$ the $\sigma$ positions where erasures have occurred, to obtain $\mathbf{y}'$ and $\mathbb{C}'$. The minimum distance of $\mathbb{C}'$ is at least $d = \tau + 1$. Hence, we can correct the $\leq \tau$ errors in $\mathbf{y}'$ to recover $\mathbf{x}'$, which stands for the transmitted codeword $\mathbf{x}$ with the $\sigma$ positions erased. Since $d(\mathbf{x}_1, \mathbf{x}_2) \geq d > \sigma$ for any $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{C}$, the unique codeword in $\mathbb{C}$ which agrees with $\mathbf{x}'$ in all the unerased positions is $\mathbf{x}$.

2. There are precisely three binary linear MDS codes: the $(n, 1, n)$ repetition code, the $(n, n-1, 2)$ even-weight code, and the $(n, n, 1)$ code equal to the entire space $\mathbb{F}_2^n$. Let $\mathbb{C}$ be a $(n, k, n-k+1)$ binary linear code with $2 \leq k \leq n-2$, and let $G = [I_k | A]$ be a systematic generator matrix for $\mathbb{C}$. Since $d = n - k + 1$ each row in $G$ has weight $\geq n - k + 1$, and therefore $A$ must be a $k \times (n-k)$ all-1 matrix. Hence, adding any two rows of $G$ produces a codeword of weight 2. Yet, for $k \leq n-2$ we must have $d = n - k + 1 > 2$.

Note: The trivial code consisting of a single codeword is sometimes also considered MDS. However, the minimum distance is not well-defined for this code.

Question: Are there any nonlinear binary MDS codes with $2 \leq k \leq n-2$? (Hint: no, use arguments similar to those employed in the proof of the Singleton bound.)

3. (a) By elementary row operations:

$$ G' = [I_3 | A] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} $$

(b) A parity-check matrix in systematic form is given by:

$$ H = [-A^t | I_4] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} $$

(c) The minimum distance is at most 2, since $G'$ contains a row of weight 2. As all the rows of $A$ are distinct, any linear combination of the rows of $G'$ has weight at least 2. Hence $d = 2$.

4. Clearly $\mathbb{C}'$ is a $(n', k', d')$ code, where $n' = n+1$, $k' = k$, and $d' = d+1$. The last equality follows from:

- $d' \geq d$ — since we are appending an extra coordinate to a code with distance $d$.
- $d' \leq d+1$ — since we are appending only one coordinate.
- $d'$ is even — since the weight of all the codewords in $\mathbb{C}'$ is even.

The parity-check matrix for $\mathbb{C}'$ is given by:

$$ H' = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 0 & & 0 \\ \vdots & & & & \vdots \end{bmatrix} $$
5. Note that for any $x, y \in \mathbb{F}_2^n$ we have $\text{wt}(x + y) = \text{wt}(x) + \text{wt}(y) - 2\text{wt}(x \cdot y)$, where $x \cdot y$ is the vector having $1$'s at those positions where both $x$ and $y$ have $1$'s. Hence the weight of $x + y$ is even if and only if either both $x$ and $y$ have even weight, or both have odd weight. Let $C_x$ and $C_y$ denote the sets of all codewords in a binary linear code $C$ with even and odd weights, respectively. If $C_0$ is empty there is nothing to prove, hence assume $C_0 \neq \emptyset$, and let $x \in C_0$. Then $\forall y \in C : x + y \in C_o$. This shows that $|C_0| \geq |C_x|$. Similarly $\forall z \in C : x + z \in C_x$, which implies $|C_0| \geq |C_x|$. Hence $|C_0| = |C_x|$. Now let $C_0$ and $C_1$ denote the sets of all codewords in $C$ with $0$ and $1$ at the given position, respectively. Proceed as before. Assuming $x \in C_1 \neq \emptyset$, we have $\forall y \in C_0 : x + y \in C_1$ and $\forall z \in C_1 : x + z \in C_0$.

6. Let $d$ be odd, and let $C$ be an $(n, M, d)$ code with $M = A_2(n, d)$. By appending an overall even parity check bit to each codeword of $C$, we obtain an $(n+1, M, d+1)$ code. This shows that $A_2(n+1, d+1) \geq A_2(n, d)$. Now let $C'$ be a $(n+1, M, d+1)$ code with $M = A_2(n+1, d+1)$. Consider the set of positions where two codewords of $C'$, at distance $d+1$ from each other, differ. By deleting (puncturing) any position in this set, we obtain an $(n, M, d)$ code. This implies $A_2(n, d) \geq A_2(n+1, d+1)$.

The optional part (b) of the problem is actually a very old conjecture in coding theory. See, for example, the article by Bernard Elspas, "A conjecture on binary nongroup codes," in the IEEE Transactions on Information Theory, pp. 599–600, October 1965. The extra credit promised is A for the course (at least!).

7. (a) By definition:

$$C^\perp = \{ v \in \mathbb{F}_2^n : \forall x = (x_1, x_2, \ldots, x_n) \in C, \ x \cdot v = x_1v_1 + \cdots + x_nv_n = 0 \}$$

where the summation in (1) is modulo 2. Let $b_1, b_2, \ldots, b_k$ be the rows of a generator matrix $G$ for $C$. Since any $x \in C$ is a linear combination of $b_1, b_2, \ldots, b_k$, we have:

$$C^\perp = \{ v \in \mathbb{F}_2^n : b_i \cdot v = 0 \text{ for } i = 1, 2, \ldots, k \}$$

Yet (2) is just another way of writing:

$$C^\perp = \{ v \in \mathbb{F}_2^n : Gv' = 0 \}$$

This shows that $G$ is a parity-check matrix for $C^\perp$.

(c) Using part (a), we have $\dim C^\perp = n - \text{rank}(G) = n - k$.

(b) Let $a_1, a_2, \ldots, a_{n-k}$ be the rows of $H$. Then by the definition of $C$ we have:

$$\forall x \in C : a_i \cdot x = 0 \text{ for } i = 1, 2, \ldots, n-k$$

Hence the vectors $a_1, a_2, \ldots, a_{n-k}$ belong to $C^\perp$. Since $H$ is full-rank these vectors are linearly independent, and since $\dim C^\perp = n - k$ they form a basis for $C^\perp$.

(d) By (a) and (b), a parity-check matrix for $(C^\perp)^\perp$ is a generator matrix for $C^\perp$ — which is a parity-check matrix for the original code $C$.

8. All the possible error-patterns have syndrome $Hy^t = z$ and it is easy to verify that the syndrome of $e = (a_1^t, e)$ is $H(a_1^t, e)^t = z$, provided $H$ is systematic. Since $\text{wt}(e) \leq t$ and all the vectors of weight $\leq t$ are unique coset leaders, there couldn’t be another "possible" error-pattern of weight $\leq t$ in the same coset with $e$ and $y$.

A conclusion here is that if the code is systematic (i.e. the first $k$ bits of a codeword are equal to the information bits), then $\text{wt}(e) \leq t$ indicates that all the channel errors have occurred in the last $n-k$ bits, which may be simply discarded in this case. This fact is used in decoding techniques known as error trapping.
9. The standard array for the code at hand is given by:

<table>
<thead>
<tr>
<th>message</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
<th>syndrome</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>00000</td>
<td>10011</td>
<td>01110</td>
<td>11101</td>
<td>000</td>
</tr>
<tr>
<td>coset</td>
<td>00001</td>
<td>10010</td>
<td>01111</td>
<td>11100</td>
<td>001</td>
</tr>
<tr>
<td>coset</td>
<td>00010</td>
<td>10001</td>
<td>01100</td>
<td>11111</td>
<td>010</td>
</tr>
<tr>
<td>coset</td>
<td>00100</td>
<td>10111</td>
<td>01010</td>
<td>11001</td>
<td>100</td>
</tr>
<tr>
<td>coset</td>
<td>01000</td>
<td>11011</td>
<td>00110</td>
<td>10101</td>
<td>110</td>
</tr>
<tr>
<td>coset</td>
<td>10000</td>
<td>00011</td>
<td>11110</td>
<td>01101</td>
<td>011</td>
</tr>
<tr>
<td>coset</td>
<td>00101</td>
<td>10110</td>
<td>01011</td>
<td>11000</td>
<td>101</td>
</tr>
<tr>
<td>coset</td>
<td>10100</td>
<td>00111</td>
<td>11010</td>
<td>01001</td>
<td>111</td>
</tr>
</tbody>
</table>

The syndrome of (00111) with respect to $H$ is (111). Note that there are two vectors of the minimum weight 2 in the coset corresponding to (111). Hence, using the MLD strategy, the vector (00111) may be decoded either as (10011) or as (01110).