Q 1.

(a) In order to show that

$$H_{ham} = \begin{pmatrix} 0 & 1 & 2 & 4 & 6 & 4 & 3 & 5 \\ 3 & 2 & 2 & 6 & 1 & 2 & 2 & 0 \end{pmatrix}$$

is a parity check matrix for a Hamming code Ham(2,7) consider the following.

For Ham(2,7) we have $r = 2$ and $q = 7$ so any non-zero vector $\boldsymbol{v}$ in $V(2,7)$ has exactly $7-1=6$ non-zero scalar multiples, forming the set $\{\lambda \boldsymbol{v} | \lambda \in GF(7), \lambda \neq 0\}$. The $(7^2-1)/(7-1) = 8$ such sets or classes are given below.

$$\left\{\begin{pmatrix}0\\3\end{pmatrix}, \begin{pmatrix}0\\6\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}, \begin{pmatrix}0\\5\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\4\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}, \begin{pmatrix}3\\6\end{pmatrix}, \begin{pmatrix}4\\1\end{pmatrix}, \begin{pmatrix}5\\3\end{pmatrix}, \begin{pmatrix}6\\5\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}2\\2\end{pmatrix}, \begin{pmatrix}4\\4\end{pmatrix}, \begin{pmatrix}6\\6\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}3\\3\end{pmatrix}, \begin{pmatrix}5\\5\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}4\\6\end{pmatrix}, \begin{pmatrix}1\\5\end{pmatrix}, \begin{pmatrix}5\\4\end{pmatrix}, \begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}6\\2\end{pmatrix}, \begin{pmatrix}3\\1\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}6\\1\end{pmatrix}, \begin{pmatrix}5\\2\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}, \begin{pmatrix}2\\5\end{pmatrix}, \begin{pmatrix}1\\6\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}4\\2\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix}, \begin{pmatrix}5\\6\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}6\\3\end{pmatrix}, \begin{pmatrix}3\\5\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}6\\4\end{pmatrix}, \begin{pmatrix}2\\6\end{pmatrix}, \begin{pmatrix}5\\1\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}4\\5\end{pmatrix}\right\}$$
$$\left\{\begin{pmatrix}5\\0\end{pmatrix}, \begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}6\\0\end{pmatrix}, \begin{pmatrix}4\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix}\right\}$$

Each class contains exactly one column vector from the parity-check matrix H and as such each column vectors of H is linearly independent of any other. Thus, the given parity-check matrix, H, is that for a Hamming code Ham(2,7).

(b) Using just row operations only the parity check matrix of Ham(2,7) can be transformed into the generator matrix, G, for the simplex code, Sim(2,7), in standard form as shown below.

$$G_{sim} = \begin{pmatrix} 0 & 1 & 2 & 4 & 6 & 4 & 3 & 5 \\ 3 & 2 & 2 & 6 & 1 & 2 & 2 & 0 \end{pmatrix} \xrightarrow[r_2 \to 5r_2]{r_1 \to 3r_1} \begin{pmatrix} 0 & 3 & 6 & 5 & 4 & 5 & 2 & 1 \\ 1 & 3 & 3 & 2 & 5 & 3 & 3 & 0 \end{pmatrix},$$

$$\xrightarrow{r_2 \to r_2 - r_1} \begin{pmatrix} 0 & 3 & 6 & 5 & 4 & 5 & 2 & 1 \\ 1 & 0 & 4 & 4 & 1 & 5 & 1 & 6 \end{pmatrix},$$

$$\xrightarrow{r_1 \to 5r_1} \begin{pmatrix} 0 & 1 & 2 & 4 & 6 & 4 & 3 & 5 \\ 1 & 0 & 4 & 4 & 1 & 5 & 1 & 6 \end{pmatrix},$$

$$\xrightarrow{r_1 \leftrightarrow r_2} \begin{pmatrix} 1 & 0 & 4 & 4 & 1 & 5 & 1 & 6 \\ 0 & 1 & 2 & 4 & 6 & 4 & 3 & 5 \end{pmatrix}.$$

Now using Theorem 7.6 of **H** page 70: if $G_{sim} = [I_2|A]$ then $H_{sim} = [-A^T|I_6]$ and given G_{sim} in standard form above we have,

$$A = \begin{pmatrix} 4 & 4 & 1 & 5 & 1 & 6 \\ 2 & 4 & 6 & 4 & 3 & 5 \end{pmatrix},$$

$$-A = \begin{pmatrix} 3 & 3 & 6 & 2 & 6 & 1 \\ 5 & 3 & 1 & 3 & 4 & 2 \end{pmatrix},$$

$$-A^T = \begin{pmatrix} 3 & 5 \\ 3 & 3 \\ 6 & 1 \\ 2 & 3 \\ 6 & 4 \\ 1 & 2 \end{pmatrix},$$

$$I_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

$$\therefore H_{sim} = \left[-A^T|I_6\right] = \begin{pmatrix} 3 & 5 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 1 & 0 & 0 & 0 & 0 \\ 6 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 6 & 4 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(c) Sim(2,7) has $|V(8,7)| \,/\, |\text{Sim}(2,7)| = 7^8/7^2 = 7^6$ cosets.

Now in our case, $d(C) = 2t + 1 = 7$, so we are guaranteed that $<= t, <= 3$ errors can be corrected in any codeword. Thus, in the top part of the Slepian standard array the coset-leaders will be those that have a weight of three or less. Thus, in the top part of the Slepian standard array we will have one vector of weight zero, namely 00000000. For the case where the weight is one we can choose for a given coordinate position in a vector of length eight any one of the values from $\{1, 2, \ldots, 6\}$. As there are eight coordinate positions in the vector we have

$$8 \times \binom{8}{1} = 8 \times \frac{8!}{(8-1)! \times 1!} = 6 \cdot 8 = 48,$$

coset-leaders of weight one. Continuing with this logic we can build an expression for the number of coset-leaders of weight two and weight three.

Thus, the number of coset-leaders in the top part of the Slepian standard array is given by the following expression:

$$\sum_{k=0}^{t}(q-1)^k\binom{n}{k} = \binom{n}{0} + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} +, \ldots, +(q-1)^t\binom{n}{t}.$$

In our case $q = 7$, $n = 8$ and $t = 3$ as $d(C) = 2t + 1 = 7$ and so we have

$$\begin{aligned}\sum_{k=0}^{3}(7-1)^k\binom{8}{k} &= \binom{8}{0} + (7-1)\binom{8}{1} + (7-1)^2\binom{8}{2} + (7-1)^3\binom{8}{3},\\ &= 1 + 48 + 1008 + 12096 = 13153 \quad \text{coset-leaders.}\end{aligned}$$

Thus, there are 13153 coset leaders in the top part of the Slepian standard array for Sim(2,7).

Shown in Table 1 are the syndromes for the vectors $10000000, 01000000, \ldots .00000001$. To correct the received vector, assuming at most one error, 45632036 which has syndrome 123256 observe that $531342 \times 3 = 123256$. Hence, the received vector 45632036 is in the same coset as that with coset-leader $01000000 \times 3 = 03000000$. So, we decode the received vector as $45632036 - 03000000 = 42632036$.

vector	syndrome
1 0 0 0 0 0 0 0	3 3 6 2 6 1
0 1 0 0 0 0 0 0	5 3 1 3 4 2
0 0 1 0 0 0 0 0	1 0 0 0 0 0
0 0 0 1 0 0 0 0	0 1 0 0 0 0
0 0 0 0 1 0 0 0	0 0 1 0 0 0
0 0 0 0 0 1 0 0	0 0 0 1 0 0
0 0 0 0 0 0 1 0	0 0 0 0 1 0
0 0 0 0 0 0 0 1	0 0 0 0 0 1

Table 1: Syndromes of vectors $10000000, 01000000, \ldots, 00000001$.

(d) The extended binary Hamming code is the code obtained by from $\hat{\text{Ham}}(4, 2)$ by adding an overall parity-check. Thus, parity-check matrix for an extended

Hamming code $\hat{\text{Ham}}(4,2)$ is

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

The incomplete decoding algorithm for this extended binary Hamming code is as follows. Suppose the received vector is $\boldsymbol{y}$. Calculate the syndrome $S(\boldsymbol{y}) = \boldsymbol{y}\hat{H}^T$ such that $S(\boldsymbol{y}) = (s_1, s_2, s_3, s_4, s_5)$. Then

1. If $s_5 = 0$ and $(s_1, s_2, s_3, s_4) = \mathbf{0}$, assume that no errors have occurred,
2. If $s_5 = 0$ and $(s_1, s_2, s_3, s_4) \neq \mathbf{0}$, assume that at least two errors have occurred and request retransmission,
3. If $s_5 = 1$ and $(s_1, s_2, s_3, s_4) = \mathbf{0}$, assume that a single error in the last place of y has occurred,
4. If $s_5 = 1$ and $(s_1, s_2, s_3, s_4) \neq \mathbf{0}$, assume that a single error in the j^{th} place, where j is the number whose binary representation is (s_1, s_2, s_3, s_4).

(e) Applying the algorithm of part (d) to the following received vectors

1. $\boldsymbol{y} = [0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$ so $S(\boldsymbol{y}) = \boldsymbol{y}\hat{H}^T = [0\ 1\ 0\ 1\ 1]$. So $s_5 = 1$ with $(s_1, s_2, s_3, s_4) = (0, 1, 0, 1) \neq \mathbf{0}$. Therefore, assume an error in the $j = 5$ place of $\boldsymbol{y}$.
2. $\boldsymbol{y} = [0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1]$ so $S(\boldsymbol{y}) = \boldsymbol{y}\hat{H}^T = [0\ 0\ 0\ 0\ 1]$. So $s_5 = 1$ with $(s_1, s_2, s_3, s_4) = (0, 0, 0, 0) = \mathbf{0}$. Therefore, assume an error in the last place of $\boldsymbol{y}$.
3. $\boldsymbol{y} = [1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1]$ so $S(\boldsymbol{y}) = \boldsymbol{y}\hat{H}^T = [1\ 1\ 0\ 0\ 0]$. So $s_5 = 0$ with $(s_1, s_2, s_3, s_4) = (1, 1, 0, 0) \neq \mathbf{0}$. Therefore, assume that at least two errors have occurred and request retransmission,

Q 2.

(a) Let C be the code over $GF(q)$ defined to have the parity-check matrix

$$H = \begin{pmatrix} 1^0 & 1^0 & \dots & 1^0 \\ 1^1 & 2^1 & \dots & n^1 \\ 1^2 & 2^2 & \dots & n^2 \\ \vdots & \vdots & \dots & \vdots \\ 1^{d-2} & 2^{d-2} & \dots & n^{d-2} \end{pmatrix},$$

where $d \leq n \leq q-1$. Any $d-1$ columns of H form a Vandermonde matrix and so are linearly independent by Theorems 11.1 and 11.2. Hence, by Theorem 8.4, C has a minimum distance d and so is a q-ary $(n, q^{n-d+1,d})$-code.

We are given

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix}.$$

and as such it is seen that $n = 6$, $3 = d - 2$ and hence $d = 5$. The code is over $GF(7)$ so that $q = 7$. Thus, the code has a minimum distance of 5 and is a 7-ary $(6, 7^{6-5+1}, 5)$-code, that is $(6, 7^2, 5)$-code over $GF(7)$ and as such the dimension of the code $k = 2$. Also, $d = 2t + 1$ and therefore $t = (5-1)/2 = 2$. So we have a 2-error-correcting code of length 6 over $GF(7)$.

(b) The received vector is 324664 and assume that two errors have occurred. Suppose that errors have occurred in positions X_1 and X_2 with respective magnitudes m_1 and m_2. If no errors have occurred then $m_1 = m_2 = 0$ and if only one error has occurred then $m_2 = 0$.

From the received vector $\boldsymbol{y} = 324664$ calculate the syndrome

$$(S_1, S_2, S_3, S_4) = \boldsymbol{y}H^T.$$

That is we calculate

$$S_j = \sum_{i=1}^{6} y_i i^{j-1} = \sum_{i=1}^{2} m_i X_i^{j-1} \text{ for } j = 1, 2, 3, 4, \qquad (2.1)$$ **H** p.132.

which gives the following syndrome for received vector $\boldsymbol{y}$ (see Table 2)

$$(S_1, S_2, S_3, S_4) = (4, 6, 3, 4).$$

$i \rightarrow$	1	2	3	4	5	6	
$j \downarrow$	3	2	4	6	6	4	S_j
1	3	2	4	6	6	4	4
2	3	4	12	24	30	24	6
3	3	8	36	96	150	144	3
4	3	16	108	384	750	864	4

Table 2: Calculation of the syndrome from the received vector $\boldsymbol{y}$.

To find the errors the following systems of equations must be solved for X_i and m_i

$$\begin{aligned} m_1 + m_2 &= S_1 \\ m_1 X_1 + m_2 X_2 &= S_2 \\ m_1 X_1^2 + m_2 X_2^2 &= S_3 \\ m_1 X_1^3 + m_2 X_2^3 &= S_4 \end{aligned}$$

Assuming at most 2 errors in positions X_1, X_2 of respective magnitudes m_1, m_2 we have

$$\phi(\theta) = \frac{m_1}{1 - X_1\theta} + \frac{m_2}{1 - X_2\theta} = \frac{A_1 + A_2\theta}{1 + B_1\theta + B_2\theta^2}$$

where, by 11.6 and 11.7 (**H** page 133), the A_i and B_i satisfy

$$\begin{aligned} A_1 &= 4 \\ A_2 &= 6 + 4B_1 \\ 0 &= 3 + 6B_1 + 4B_2 \\ 0 &= 4 + 3B_1 + 6B_2. \end{aligned}$$

Solving for B_1 and B_2 first

$$\begin{aligned}
-3 &\equiv 6B_1 + 4B_2 \pmod 7 \\
-4 &\equiv 3B_1 + 6B_2 \pmod 7 \\
\\
-3 &\equiv 6B_1 + 4B_2 \pmod 7 \\
-8 &\equiv 6B_1 + 12B_2 \pmod 7 \\
\\
4 &\equiv 6B_1 + 4B_2 \pmod 7 \\
6 &\equiv 6B_1 + 5B_2 \pmod 7 \\
2 &\equiv B_2 \pmod 7 \\
\\
4 &\equiv 6B_1 + 4 \cdot 2 \pmod 7 \\
4 &\equiv 6B_1 + 1 \pmod 7 \\
3 &\equiv 6B_1 \pmod 7 \\
3 \cdot 6^{-1} &\equiv B_1 \pmod 7 \\
3 \cdot 6 &\equiv B_1 \pmod 7 \\
4 &\equiv B_1 \pmod 7.
\end{aligned}$$

Then for A_2

$$\begin{aligned}
A_2 &\equiv 6 + 4 \cdot B_1 \pmod 7 \\
A_2 &\equiv 6 + 4 \cdot 4 \pmod 7 \\
A_2 &\equiv 6 + 16 \pmod 7 \\
A_2 &\equiv 22 \pmod 7 \\
A_2 &\equiv 1 \pmod 7
\end{aligned}$$

Thus, $A_1 = 4$, $A_2 = 1$, $B_1 = 4$, and $B_2 = 2$. Therefore,

$$\begin{aligned}
\phi(\theta) &= \frac{A_1 + A_2\theta}{1 + B_1\theta + B_2\theta^2} \\
&= \frac{4 + \theta}{1 + 4\theta + 2\theta^2} \\
&= \frac{4 + \theta}{2(\theta + 3)(\theta + 6)} \pmod 7.
\end{aligned}$$

The zeros of the quadratic are 1 and 4. The error positions are the inverse of these values, i.e. $X_1 = 1$ and $X_2 = 2$.

To find m_1:

$$\begin{aligned}\frac{4+\theta}{(1-\theta)(1-2\theta)} &= \frac{m_1}{1-\theta} + \frac{m_2}{1-2\theta}\\ \frac{4+\theta}{1-2\theta} &= m_1 + \frac{m_2(1-\theta)}{1-2\theta}\\ \text{Let } \theta = 1 \text{ then,}\\ \frac{4+1}{1-2} &\equiv \frac{5}{6} \equiv 5\cdot 6 \equiv 2 \equiv m_1 \pmod 7\\ m_1 &\equiv 2 \pmod 7.\end{aligned}$$

To find m_2:

$$\begin{aligned}\frac{4+\theta}{(1-\theta)(1-2\theta)} &= \frac{m_1}{1-\theta} + \frac{m_2}{1-2\theta}\\ \frac{4+\theta}{1-\theta} &= \frac{m_1(1-2\theta)}{1-\theta} + m_2\\ \text{Let } \theta = 4 \text{ then,}\\ \frac{4+4}{1-4} &\equiv \frac{1}{4} \equiv 2 \equiv m_2 \pmod 7\\ m_2 &\equiv 2 \pmod 7.\end{aligned}$$

Thus, $m_1 = 2$, $m_2 = 2, X_1 = 1$ and $X_2 = 2$. As a check we can recalculate the syndrome of the received vector as follows.

$$\begin{aligned}S_1 &= m_1 + m_2 = 2 + 2 = 4,\\ S_2 &= m_1X_1 + m_2X_2 = 2\cdot 1 + 2\cdot 2 = 6,\\ S_3 &= m_1X_1^2 + m_2X_2^2 = 2\cdot 1^2 + 2\cdot 2^2 = 10 \equiv 3 \pmod 7,\\ S_3 &= m_1X_1^3 + m_2X_2^3 = 2\cdot 1^3 + 2\cdot 2^3 = 18 \equiv 4 \pmod 7.\end{aligned}$$

These elements of the syndrome are the same as those previously calculated above using (2.1).

Now to obtain the transmitted codeword from the received vector $\boldsymbol{y}$ the error m_i is such that $y_{X_i} = x_{X_i} + m_i$ which enables us to determine transmitted codeword $\boldsymbol{x}$ from the received vector $\boldsymbol{y}$. Thus,

See p.14, **(6.11)** of Block 2 Course Notes.

$$\begin{aligned}y_{X_i} &= x_{X_i} + m_i \text{ where } i = 1, 2.\\ y_{X_1} &= x_{X_1} + m_1,\\ y_1 &= x_1 + m_1,\\ 3 &= x_1 + 2,\\ x_1 &= 1.\end{aligned}$$

$$\begin{aligned}y_{X_2} &= x_{X_2} + m_2,\\ y_2 &= x_2 + m_2,\\ 2 &= x_2 + 2,\\ x_2 &= 0.\end{aligned}$$

Hence, the transmitted codeword was 104664. This can be checked by calculating its syndrome, which if it is a valid codeword, will the **0**. The calculation is summarised in Table 3 where it is seen that the syndrome is indeed **0**.

$i \rightarrow$	1	2	3	4	5	6	
$j \downarrow$	1	0	4	6	6	4	S_j
1	1	0	4	6	6	4	0
2	1	0	12	24	30	24	0
3	1	0	36	96	150	144	0
4	1	0	108	384	750	864	0

Table 3: Calculation of the syndrome from the received vector $\boldsymbol{y} = 104664$.

(c) The values of a, b, c and d for which the vector $11abcd$ is a codeword is calculated as follows noting that the syndrome of a valid codeword is $S = \mathbf{0}$.

$$S_j = \sum_{i=1}^{n} y_i i^{j-1} \text{ for } j = 1, 2, \ldots, 2t.$$

H page 132.

In our case $n = 6$ and $t = 2$, so that

$$S_j = \sum_{i=1}^{6} y_i i^{j-1} \text{ for } j = 1, 2, 3, 4.$$

Hence, we have

$$\begin{aligned}
S_1 &= 1 + 1 + a + b + c + d, \\
S_2 &= 1 \cdot 1 + 2 \cdot 1 + 3a + 4b + 5c + 6d, \\
S_3 &= 1 \cdot 1 + 2 \cdot 1^2 + 3^2 a + 4^2 b + 5^2 c + 6^2 d, \\
S_4 &= 1 \cdot 1 + 2 \cdot 1^3 + 3^3 a + 4^3 b + 5^3 c + 6^3 d.
\end{aligned}$$

$S = \mathbf{0}$, so

$$\begin{aligned}
-2 &= a + b + c + d, \\
-3 &= 3a + 4b + 5c + 6d, \\
-5 &= 3^2 a + 4^2 b + 5^2 c + 6^2 d, \\
-9 &= 3^3 a + 4^3 b + 5^3 c + 6^3 d,
\end{aligned}$$

Solving these simultaneous equations gives $a = 0,\ b = 5,\ c = 2$ and $d = 5$.

Thus, the codeword is $y = 110525$. Check:

$$\begin{aligned}
S_1 &= 1 + 1 + 0 + 5 + 2 + 5 \equiv 0 \pmod 7,\\
S_2 &= 1 + 2 + 3 \cdot 0 + 4 \cdot 5 + 5 \cdot 2 + 6 \cdot 5 \equiv 0 \pmod 7,\\
S_3 &= 1 + 4 + 9 \cdot 0 + 16 \cdot 5 + 25 \cdot 2 + 36 \cdot 5 \equiv 0 \pmod 7,\\
S_4 &= 1 + 8 + 27 \cdot 0 + 64 \cdot 5 + 125 \cdot 0 + 216 \cdot 5 \equiv 0 \pmod 7.
\end{aligned}$$

So, $y = 110525$ is a valid codeword checks out to be $\mathbf{0}$.

(d) v =

4 5

The generator matrix in standard form is of the form $G = [I_t|A_{t\times n-t}]$ where $t = 2$ and $n = 6$, i.e.

$$G = \left(\begin{array}{cc|cccc} 1 & 0 & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ 0 & 1 & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \end{array}\right)$$

We have a valid codeword namely $\boldsymbol{y_1} = 324664$. Thus, to generate this codeword we calculate

$$\begin{aligned}
\boldsymbol{y} &= [3\ 2\ ] \left(\begin{array}{cc|cccc} 1 & 0 & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ 0 & 1 & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \end{array}\right),\\
&= [3\ 2\ \ a_{1,1} + a_{2,1}\ \ a_{1,2} + a_{2,2}\ \ a_{1,3} + a_{2,3}\ \ a_{1,4} + a_{2,4}].
\end{aligned}$$

We also have the valid codeword $\boldsymbol{y_2} = 104664$. Thus, to generate this codeword we calculate

$$\begin{aligned}
\boldsymbol{y} &= [10] \left(\begin{array}{cc|cccc} 1 & 0 & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ 0 & 1 & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \end{array}\right),\\
&= [1\ \ 0\ \ a_{1,1}\ \ a_{1,2}\ \ a_{1,3}\ \ a_{1,4}],
\end{aligned}$$

and it immediately follows that $a_{1,1} = 4,\ a_{1,2} = 6,\ a_{1,3} = 6,\ a_{1,4} = 4,\ a_{2,1} = 3,\ a_{2,2} = 6,\ a_{2,3} = 3,$ and $a_{2,4} = 1$. Thus, the generator matrix in standard form for the code C is

$$G = \begin{pmatrix} 1 & 0 & 4 & 6 & 6 & 4 \\ 0 & 1 & 3 & 6 & 3 & 1 \end{pmatrix}.$$

(e) To find the error in the vector $\boldsymbol{y} = 324130$ calculate

$$c = [3\ \ 2] \begin{pmatrix} 1 & 0 & 4 & 6 & 6 & 4 \\ 0 & 1 & 3 & 6 & 3 & 1 \end{pmatrix} = 324230,$$

and comparing this codeword with the received vector 324130 we see that the single error is in the fourth place of the received vector. Thus, the codeword sent was 324230.

To find the error in the vector $\boldsymbol{y} = 452066$ calculate

$$c = [4 \;\; 5]\begin{pmatrix} 1 & 0 & 4 & 6 & 6 & 4 \\ 0 & 1 & 3 & 6 & 3 & 1 \end{pmatrix} = 453540,$$

and comparing this codeword with the received vector 452066 we see that the error must be in the first or second place of the received vector as there is only a single error in this vector. To find the error calculate in turn $[i \;\; j]G$ for $i \in GF(7)$ and $i \neq 4$ and for $j \in GF(7)$ and $j \neq 5$. After each calculation compare the calculated codeword with received vector. Stop when the comparison yields a difference in only one place between the codeword and the received vector. Implementing this algorithm it is seen that

$$c = [2 \;\; 5]\begin{pmatrix} 1 & 0 & 4 & 6 & 6 & 4 \\ 0 & 1 & 3 & 6 & 3 & 1 \end{pmatrix} = 252066,$$

Thus, the codeword sent was 252066 where the error was in the first place of the received vector.

Q 3.

(a) Given that the code $C = H \ * S$ is formed using Plotkin's $(\boldsymbol{a}|\boldsymbol{a}+\boldsymbol{b})$ construction where $H = \mathrm{Ham}(3,2)$ and $S = \mathrm{Sim}(3,2)$ then length, dimension and minimum distance of C is determined as follows.

From **H** page 82 **Theorem 8.2** a Ham(r,2) has length $n = 2^r - 1 = 8 - 1 = 7$ and dimension $k = 2^r - 1 - r = 8 - 1 - 3 = 4$ and has minimum distance 3. Thus, Ham(3,2) is a $[7, 4, 3]$-code.

From Block 2 Course Notes page 7 **Definition 5.1** Sim(r, 2) is a $[(q^r - 1)/(q-1), r, q^{r-1}]$-code i.e. a $[(2^4 - 1)/(2-1), 3, 2^{3-1}]$-code. Thus, Sim(3,2) is a $[7, 3, 4]$-code.

Now, from Block 2 Course Notes page 22 where it states that the code C, denoted by $A * B$, is formed from Construct 7.1 (Block 2 Course Notes page 21) then as the codes Ham(3,2) and Sim(3,2) are linear codes with dimensions 4 and 3 respectively (so that $M_{\mathrm{Ham}} = 2^4 = 16$ and $M_{\mathrm{Sim}} = 2^3 = 8$) then C is linear and as $M_{\mathrm{Ham}} M_{\mathrm{Sim}} = 2^{4+3}$ has dimension $k_C = k_{\mathrm{Ham}} + k_{\mathrm{Sim}} = 4+3 = 7$. The length of C is $2n = 14$ and the minimum distance is given by $d_C = \min\{2d_{\mathrm{Ham}}, d_{\mathrm{Sim}}\}$ that is $d_C = \min\{2 \cdot 3, 4\} = 4$.

Consequently, C has parameters $(14, 16 \cdot 8, 4) = (14, 128, 4)$ and is a $[14, 7, 4]$-code. That is C has length 14, dimension 7 and minimum distance 4.

************ more to be added ************

(b)

v_1	v_2	v_3	$f(v_.v_2.v_3)$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	1
1	0	1	0
0	1	1	1
1	1	1	1

Table 4: Truth table for function $f : V(3,2) \to V(1,2)$.

We obtain an expression for $f(v_.v_2.v_3)$ as a Boolean multinomial in three Boolean variables as follows.

Making use of: $x \vee y = x + y + xy$; $x + x = 0$; $xx = x$; and $x + x = 0$ in

$GF(2)$, gives

$$\begin{aligned}
f(v_.v_2.v_3) &= \bar{v_1}\bar{v_2}v_3 \ \vee \bar{v_1}v_2\bar{v_3} \ \vee \bar{v_1}v_2v_3 \ \vee v_1\bar{v_2}\bar{v_3} \vee v_1v_2v_3 \\
&= \bar{v_1}v_3(v_2+\bar{v_2}) + \bar{v_1}v_2(v_3+\bar{v_3}) + \bar{v_2}v_3(v_1+\bar{v_1}) + v_1\bar{v_2}\bar{v_3} \\
&= \bar{v_1}v_3 + \bar{v_1}v_2 + \bar{v_2}v_3 + v_1\bar{v_2}\bar{v_3} \\
&= (1+v_1)v_3 + (1+v_1)v_2 + (1+v_2)v_3 + v_1(1+v_2)(1+v_3) \\
&= v_3 + v_1v_3 + v_2 + v_1v_2 + v_3 + v_2v_3 + (v_1+v_1v_2)(1+v_3) \\
&= v_3 + v_1v_3 + v_2 + v_1v_2 + v_3 + v_2v_3 + v_1 + v_1v_2 + v_1v_3 + v_1v_2v_3 \\
&= v_1 + v_2 + v_3 + v_2v_3 + v_1v_2v_3.
\end{aligned}$$

(c) The generator matrix for $RM(1,4)$ is given as follows

See Example 7.7 B2CN's p.36.

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

To obtain the equations needed to apply the Reed decoding algorithm we need to find first the values x_1, x_2, x_3, x_4 and x_5 as follows.

$$\boldsymbol{x} = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \end{pmatrix} \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1
\end{pmatrix}.$$

Thus,

$$\begin{aligned}
x_0 &= a_0 && (3.1)\\
x_1 &= a_0 + a_1 && (3.2)\\
x_2 &= a_0 + a_2 && (3.3)\\
x_3 &= a_0 + a_1 + a_2 && (3.4)\\
x_4 &= a_0 + a_3 && (3.5)\\
x_5 &= a_0 + a_1 + a_3 && (3.6)\\
x_6 &= a_0 + a_2 + a_3 && (3.7)\\
x_7 &= a_0 + a_1 + a_2 + a_3 && (3.8)\\
x_8 &= a_0 + a_4 && (3.9)\\
x_9 &= a_0 + a_1 + a_4 && (3.10)\\
x_{10} &= a_0 + a_2 + a_4 && (3.11)\\
x_{11} &= a_0 + a_1 + a_2 + a_4 && (3.12)\\
x_{12} &= a_0 + a_3 + a_4 && (3.13)\\
x_{13} &= a_0 + a_1 + a_3 + a_4 && (3.14)\\
x_{14} &= a_0 + a_2 + a_3 + a_4 && (3.15)\\
x_{15} &= a_0 + a_1 + a_2 + a_3 + a_4 && (3.16)
\end{aligned}$$

(i) The equations needed to apply the Reed decoding algorithm are as follows.

$$a_1 = x_0 + x_1 \tag{3.17}$$
$$a_1 = x_2 + x_3 \tag{3.18}$$
$$a_1 = x_4 + x_5 \tag{3.19}$$
$$a_1 = x_6 + x_7 \tag{3.20}$$
$$a_1 = x_8 + x_9 \tag{3.21}$$
$$a_1 = x_{10} + x_{11} \tag{3.22}$$
$$a_1 = x_{12} + x_{13} \tag{3.23}$$
$$a_1 = x_{14} + x_{15} \tag{3.24}$$

$$a_2 = x_0 + x_2 \tag{3.25}$$
$$a_2 = x_1 + x_3 \tag{3.26}$$
$$a_2 = x_4 + x_6 \tag{3.27}$$
$$a_2 = x_5 + x_7 \tag{3.28}$$
$$a_2 = x_8 + x_{10} \tag{3.29}$$
$$a_2 = x_9 + x_{11} \tag{3.30}$$
$$a_2 = x_{12} + x_{14} \tag{3.31}$$
$$a_2 = x_{13} + x_{15} \tag{3.32}$$

$$a_3 = x_0 + x_4 \tag{3.33}$$
$$a_3 = x_1 + x_5 \tag{3.34}$$
$$a_3 = x_2 + x_6 \tag{3.35}$$
$$a_3 = x_3 + x_7 \tag{3.36}$$
$$a_3 = x_8 + x_{12} \tag{3.37}$$
$$a_3 = x_9 + x_{13} \tag{3.38}$$
$$a_3 = x_{10} + x_{14} \tag{3.39}$$
$$a_3 = x_{11} + x_{15} \tag{3.40}$$

$$a_4 = x_0 + x_8 \tag{3.41}$$
$$a_4 = x_1 + x_9 \tag{3.42}$$
$$a_4 = x_2 + x_{10} \tag{3.43}$$
$$a_4 = x_3 + x_{11} \tag{3.44}$$
$$a_4 = x_4 + x_{12} \tag{3.45}$$
$$a_4 = x_5 + x_{13} \tag{3.46}$$
$$a_4 = x_6 + x_{14} \tag{3.47}$$
$$a_4 = x_7 + x_{15} \tag{3.48}$$

The first equation for a_0 is simply $a_0 = x_0$. To obtain the remaining fifteen equations for a_0 we make use of the sixteen equations x_0 to x_{15} (3.1) to (3.16), respectively. Explaining how the equations for a_0 are determined is best illustrated by an example of how we find one of them. Consider the expression for x_7 given by (3.7):

$$a_7 = a_0 + a_1 + a_2 + a_3. \tag{3.49}$$

Now, we have eight expressions each for a_1, a_2, a_3 and a_4, and the strategy we take is to maximise the number of terms in the expression for a_0, thus we choose $a_1 = x_0 + x_1$, $a_2 = x_4 + x_6$, and $x_3 = x_8 + x_{12}$, to give

$$x_7 = a_0 + x_0 + x_1 + x_4 + x_6 + x_8 + x_{12}. \tag{3.50}$$

Then, rearranging (3.50) in terms of a_0 we obtain

$$a_0 = x_7 - (x_0 + x_1 + x_4 + x_6 + x_8 + x_{12}). \tag{3.51}$$

As each $x_i \in GF(2)$ and we are using modulo 2 arithmetic we obtain

$$a_0 = x_0 + x_1 + x_4 + x_6 + x_7 + x_8 + x_{12}. \tag{3.52}$$

However, do note that it is possible to generate duplicate equations. In such cases a different choice for one or more of $a_1, a_2, \ldots, a_4$ should be made, while still trying to maximise the number of terms in the expression for a_0, for substitution into the expression for x_i.

The remaining equations for a_0 are found in a similar fashion.

(ii) To determine the original message word from the received vector 1100111100111011 assuming at most three transmission errors, we first determine the majority votes for each of a_1, a_2, a_3 and a_4.

Recall from above that the eight equations for a_1 were as follows.

$$\begin{aligned}
a_1 &= x_0 + x_1\\
a_1 &= x_2 + x_3\\
a_1 &= x_4 + x_5\\
a_1 &= x_6 + x_7\\
a_1 &= x_8 + x_9\\
a_1 &= x_{10} + x_{11}\\
a_1 &= x_{12} + x_{13}\\
a_1 &= x_{14} + x_{15}
\end{aligned}$$

With, $x_1 x_2 \ldots x_{15} = 1100111100111011$, these give eight values to each a_1, namely

$$\begin{aligned}
a_1 &= x_0 + x_1 = 1 + 1 = 0, \\
a_1 &= x_2 + x_3 = 0 + 0 = 0, \\
a_1 &= x_4 + x_5 = 1 + 1 = 0, \\
a_1 &= x_6 + x_7 = 1 + 1 = 0, \\
a_1 &= x_8 + x_9 = 0 + 0 = 0, \\
a_1 &= x_{10} + x_{11} = 1 + 1 = 0, \\
a_1 &= x_{12} + x_{13} = 1 + 0 = 1, \\
a_1 &= x_{14} + x_{15} = 1 + 1 = 0.
\end{aligned}$$

The majority vote is in favour of 0 and therefore $a_1 = 0$.

Repeating the above for a_2, a_3 and a_4 as follows.

With, $x_1x_2 \dots x_{15} = 1100111100111011$, these give eight values to each a_2, namely

$$\begin{aligned}
a_2 &= x_0 + x_2 = 1 + 0 = 1, \\
a_2 &= x_1 + x_3 = 1 + 0 = 1, \\
a_2 &= x_4 + x_6 = 1 + 1 = 0, \\
a_2 &= x_5 + x_7 = 1 + 1 = 0, \\
a_2 &= x_8 + x_{10} = 0 + 1 = 1, \\
a_2 &= x_9 + x_{11} = 0 + 1 = 1, \\
a_2 &= x_{12} + x_{14} = 1 + 1 = 0, \\
a_2 &= x_{13} + x_{15} = 0 + 1 = 1.
\end{aligned}$$

The majority vote is in favour of 1 and therefore $a_2 = 1$.

With, $x_1x_2 \dots x_{15} = 1100111100111011$, these give eight values to each a_3, namely

$$\begin{aligned}
a_3 &= x_0 + x_4 = 1 + 1 = 0, \\
a_3 &= x_1 + x_5 = 1 + 1 = 0, \\
a_3 &= x_2 + x_6 = 0 + 1 = 1, \\
a_3 &= x_3 + x_7 = 0 + 1 = 1, \\
a_3 &= x_8 + x_{12} = 0 + 1 = 1, \\
a_3 &= x_9 + x_{13} = 0 + 0 = 0, \\
a_3 &= x_{10} + x_{14} = 1 + 1 = 0, \\
a_3 &= x_{11} + x_{15} = 1 + 1 = 0.
\end{aligned}$$

The majority vote is in favour of 0 and therefore $a_3 = 0$.

With, $x_1x_2 \dots x_{15} = 1100111100111011$, these give eight values to each a_3, namely

$$\begin{aligned}
a_4 &= x_0 + x_8 = 1 + 0 = 1, \\
a_4 &= x_1 + x_9 = 1 + 0 = 1, \\
a_4 &= x_2 + x_{10} = 0 + 1 = 1, \\
a_4 &= x_3 + x_{11} = 0 + 1 = 1, \\
a_4 &= x_4 + x_{12} = 1 + 1 = 0, \\
a_4 &= x_5 + x_{13} = 1 + 0 = 1, \\
a_4 &= x_6 + x_{14} = 1 + 1 = 0, \\
a_4 &= x_7 + x_{15} = 1 + 1 = 0
\end{aligned}$$

The majority vote is in favour of 1 and therefore $a_4 = 1$.

Now we have $\boldsymbol{a} = a_0 0101$ where $a_0 \in GF(2)$. Therefore, the original message transmitted was either $\boldsymbol{a} = 00101$ or $\boldsymbol{a} = 10101$. To determine which, assuming at most three errors in the received vector, we calculate $\boldsymbol{x} = \boldsymbol{a}G$ for each of the two possibilities for $\boldsymbol{a}$, where G is the generator matrix given previously. We then compare the two generated vectors of $\boldsymbol{x}$ with the received vector and the one that has three or less differences in the coordinate positions is the one transmitted. Thus,

$$\boldsymbol{x} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \end{pmatrix}$$
$$= 0011001111001100.$$

Comparing the vector generated above with the received vector:

$$\begin{gathered} 0011001111001100 \\ 1100111100111011 \end{gathered}$$

shows that they differ in more than three positions and as such the choice of $a_0 = 0$ was incorrect.

$$\boldsymbol{x} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \end{pmatrix}$$
$$= 1100110000110011.$$

Comparing the vector generated above with the received vector:

$$\begin{gathered} 1100110000110011 \\ 1100111100111011 \end{gathered}$$

shows that they differ in three positions and as such the choice of $a_0 = 1$ was correct. Thus, the original message word was $\boldsymbol{a} = 10101$.

Q 4.

(a)

(b)

(c)