Q 1.

(a) The ISBN-10s 0303392611, 0099417561 and 1584885086 can be checked to see whether they are valid or not as follows:

(i)

i	1	2	3	4	5	6	7	8	9
x_i	0	3	0	3	3	9	2	6	1
ix_i	0	6	0	12	15	54	14	48	9

Table 1: $\sum_{i=1}^{9} ix_i = 158$ and $x_{10} \equiv 158 \pmod{11} \equiv 4$.

ISBN-10 0303392611 is invalid as the calculated value of $x_{10} = 4$ is not equal to given value of $x_{10} = 1$.

(ii)

i	1	2	3	4	5	6	7	8	9
x_i	0	0	9	9	4	1	7	5	6
ix_i	0	0	27	36	20	6	49	40	54

Table 2: $\sum_{i=1}^{9} ix_i = 232$ and $x_{10} \equiv 232 \pmod{11} \equiv 1$.

ISBN-10 0099417561 is valid as the calculated value of $x_{10} = 1$ is equal to the given value of $x_{10} = 1$.

(iii)

i	1	2	3	4	5	6	7	8	9
x_i	1	5	8	4	8	8	5	0	8
ix_i	1	10	24	16	40	48	35	0	72

Table 3: $\sum_{i=1}^{9} ix_i = 246$ and $x_{10} \equiv 246 \pmod{11} \equiv 4$.

ISBN-10 1584885086 is invalid as the calculated value of $x_{10} = 4$ is not equal to given value of $x_{10} = 6$.

From the above, two of the three ISBN-10s are invalid; namely: 0303392611 and 1584885086. Assuming a single transposition error has been made in adjacent positions, to determine if it is possible to correct these two ISBN-10s consider the following.

Assume that x_j and x_{j+1}, $j \in \{1, 2, \ldots, 9\}$ are the two adjacent digits that have been transposed. Then,

$$s = \sum_{\substack{i=1 \\ i \neq j \\ i \neq j+1}}^{10} ix_i + (j+1)x_j + jx_{j+1} \equiv 0 \pmod{11}) \tag{1.1}$$

if and only if x_j and x_{j+1} are the two digits that have been transposed. Otherwise,

$$s = \sum_{\substack{i=1 \\ i \neq j \\ i \neq j+1}}^{10} ix_i + (j+1)x_j + jx_{j+1} \not\equiv 0 \pmod{11}$$

and it is know that the chosen pair of digits x_j and x_{j+1} were not the ones that were transposed. Thus, the strategy is to start with $j = 1$ and evaluate (1.1) and test to see if the result is congruent to 0 (mod 11) and if so we have found the pair of digits that were transposed. Otherwise increment j by one and then recalculate (1.1) until the sum $s \equiv 0 \pmod{11}$.

Performing the above strategy on 0303392611 with $j = 1$ (i.e. assume that the first two digits were the ones transposed) gives

i	1	2	3	4	5	6	7	8	9
x_i	3	0	0	3	3	9	2	6	1
ix_i	3	0	0	12	15	54	14	48	9

Table 4: $\sum_{i=1}^{9} ix_i = 155$ and $x_{10} \equiv 155 \pmod{11} \equiv 1$.

ISBN-10 3003392611 is valid as the calculated value of $x_{10} = 1$ is equal to the given value of $x_{10} = 1$.

Similarly, performing the above strategy on 1584885086 with $j = 9$ (i.e. assume that the last two digits were the ones transposed) gives

ISBN-10 1584885068 is valid as the calculated value of $x_{10} = 8$ is equal to the given value of $x_{10} = 8$.

(b) Case 1: If the last digit of the codeword is an erasure then the value of the erasure, e_{10}, is given by:

$$e_{10} = \sum_{i=1}^{9} ix_i \pmod{11}.$$

i	1	2	3	4	5	6	7	8	9
x_i	1	5	8	4	8	8	5	0	6
ix_i	1	10	24	16	40	48	35	0	54

Table 5: $\sum_{i=1}^{9} ix_i = 228$ and $x_{10} \equiv 228 \pmod{11} \equiv 8$.

Otherwise the erasure, e_j, will have occurred at location j, $j \in \{1, 2 \ldots, 9\}$ in which case the value of e_j is given by (1.2):

$$\begin{aligned}
\sum_{i=1}^{j-1} ix_i + je_j + \sum_{i=j+1}^{10} ix_i &\equiv 0 \pmod{11}, \\
\left(\sum_{i=1}^{j-1} ix_i + \sum_{i=j+1}^{10} ix_i \right) &\equiv -je_j \pmod{11}, \\
j^{-1} \left(\sum_{i=1}^{j-1} ix_i + \sum_{i=j+1}^{10} ix_i \right) &\equiv -e_j \pmod{11}, \\
-j^{-1} \left(\sum_{i=1}^{j-1} ix_i + \sum_{i=j+1}^{10} ix_i \right) \pmod{11} &\equiv e_j, \qquad (1.2)
\end{aligned}$$

where j^{-1} is the multiplicative inverse of j in $\mathbb{Z}_{11}$. So ISBN-10 is 1-erasure correcting.

Case 2: Assume two erasures have occurred, e_j and e_k, at locations j and k $(k > j)$ in the codeword. Then, we have:

$$\sum_{i=1}^{j-1} ix_i + je_j + \sum_{i=j+1}^{k-1} ix_i + ke_k + \sum_{i=k+1}^{10} ix_i \equiv 0 \pmod{11}. \qquad (1.3)$$

The congruence modulo 11 (1.3), given j and k, has two unknowns, e_j, e_k, and therefore it is not possible to uniquely determine both erasures from one equation. Thus, ISBN-10 is not 2-erasure correcting.

Given the received vector $04862?263X$, where ? denotes an undecodeable symbol, the correct ISBN-10 can be determined using (1.2) as follows.

The erasure has occurred at location six in the received vector therefore $j = 6$ in this case.

$$-\left[6^{-1} \left(\sum_{i=1}^{5} ix_i + \sum_{i=7}^{10} ix_i \right) \right] \pmod{11} \equiv e_6.$$

The multiplicative inverse of 6 in GF(11) is 2, so we have **H** p.36

$$-2 \left(\sum_{i=1}^{5} ix_i + \sum_{i=7}^{10} ix_i \right) \pmod{11} \equiv e_6.$$

Now,

$$\sum_{i=1}^{5} ix_i = 0 + 2 \cdot 4 + 3 \cdot 8 + 4 \cdot 6 + 5 \cdot 2 = 66,$$

and

$$\sum_{i=7}^{10} ix_i = 7 \cdot 2 + 8 \cdot 6 + 9 \cdot 3 + 10 \cdot 10 = 189.$$

Therefore,

$$\begin{aligned} -2(66 + 189) \pmod{11} &\equiv e_6, \\ -2(255) \pmod{11} &\equiv e_6, \\ -510 \pmod{11} &\equiv e_6, \\ 7 &= e_6. \end{aligned}$$

So, $e_6 = 7$.

Check:

i	1	2	3	4	5	6	7	8	9
x_i	0	4	8	6	2	7	2	6	3
ix_i	0	8	24	24	10	42	14	48	27

Table 6: $\sum_{i=1}^{9} ix_i = 197$ and $x_{10} \equiv 197 \pmod{11} \equiv 10$.

ISBN-10 048627263X is valid as the calculated value of $x_{10} = 10$ is equal to the given value of $x_{10} = X$.

(c) If the ISBN-10 code is modified by appending to each codeword $\mathbf{x} = x_1 x_2 \cdots x_{10}$ an eleventh digit x_{11} given by $x_{11} = \sum_{i=1}^{10} x_i \pmod{11}$ then the minimum distance of the resulting code will be three. This can be justified as follows.

Assume that the digit in the j^{th} $(1 \leq j \leq 9)$ position of the codeword is changed from x_j to y_j where $x_j, y_j \in \mathbb{Z}_{10}$ and $x_j \neq y_j$, then

$$\begin{aligned} x_{10\,(j,x_j)} &\equiv \sum_{\substack{i=1 \\ i \neq j}}^{9} ix_i + jx_j \pmod{11}, \\ x_{10\,(j,y_j)} &\equiv \sum_{\substack{i=1 \\ i \neq j}}^{9} ix_i + jy_j \pmod{11}, \\ x_{10\,(j,y_j)} - x_{10\,(j,x_j)} &\equiv j(y_j - x_j) \pmod{11}. \end{aligned} \tag{1.4}$$

(1.4) Shows that the digit in the tenth position of the codeword x_{10} will change when any one of the digits $x_i, i \in \{1, 2, \ldots, 9\}$ changes.

Now, to see what happens to the eleventh digit when one of the digits $x_i, i \in \{1, 2, \ldots, 9\}$ changes.

$$\begin{aligned}
x_{11\,(j,x_j)} &\equiv \sum_{i=1, i\neq j}^{9} x_i + x_j + x_{10\,(j,x_j)} \pmod{11},\\
x_{11\,(j,y_j)} &\equiv \sum_{i=1, i\neq j}^{9} x_i + y_j + x_{10\,(j,y_j)} \pmod{11},\\
x_{11\,(j,y_j)} - x_{11\,(j,x_j)} &\equiv (y_j - x_j) + x_{10\,(j,y_j)} - x_{10\,(j,x_j)} \pmod{11},\\
x_{11\,(j,y_j)} - x_{11\,(j,x_j)} &\equiv (y_j - x_j) + j(y_j - x_j) \pmod{11},\\
x_{11\,(j,y_j)} - x_{11\,(j,x_j)} &\equiv (y_j - x_j)(1 + j) \pmod{11}. \qquad (1.5)
\end{aligned}$$

(1.5) shows that the digit in the eleventh position of the codeword x_{11} will change when any one of the digits $x_i, i \in \{1, 2, \ldots, 9\}$ changes.

Thus, if one of the digits $x_i, i \in \{1, 2, \ldots, 9\}$ changes, both x_{10} and x_{11} change showing that the minimum distance of this modified ISBN-10 is three.

(i) To find x_4:

$$\begin{aligned}
\sum_{i=1}^{3} ix_i + 4x_4 + \sum_{i=5}^{10} ix_i &\equiv 0 \pmod{11},\\
\sum_{i=1}^{3} x_i + x_4 + \sum_{i=5}^{10} x_i &\equiv 9 \pmod{11},\\
\sum_{i=1}^{3} x_i(i-1) + 3x_4 + \sum_{i=5}^{10} x_i(i-1) &\equiv -9 \pmod{11},\\
\sum_{i=1}^{3} x_i(i-1) + \sum_{i=5}^{10} x_i(i-1) + 9 &\equiv -3x_4 \pmod{11},\\
-3^{-1}\left(\sum_{i=1}^{3} x_i(i-1) + \sum_{i=5}^{10} x_i(i-1) + 9\right) &\equiv x_4 \pmod{11},\\
-4\left(\sum_{i=1}^{3} x_i(i-1) + \sum_{i=5}^{10} x_i(i-1) + 9\right) &\equiv x_4 \pmod{11}. \qquad (1.6)
\end{aligned}$$

Given the received vector 297?2357099 and applying (1.6) to find x_4:

$$\begin{aligned}
-4(23 + 183 + 9) &\equiv x_4 \pmod{11}\\
-860 &\equiv x_4 \pmod{11}\\
9 &\equiv x_4 \pmod{11}
\end{aligned}$$

Therefore, the corrected vector is 297**9**2357099.

(ii) To find x_5:

$$\begin{gathered}
\sum_{i=1,i\neq5,i\neq7}^{10} ix_i + 5x_5 + 7x_7 \equiv 0 \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} x_i + x_5 + x_7 \equiv x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} 7x_i + 7x_5 + 7x_7 \equiv 7x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} (7-i)x_i + 2x_5 \equiv 7x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} (7-i)x_i - 7x_{11} \equiv -2x_5 \pmod{11}, \\
-6\left(\sum_{i=1,i\neq5,i\neq7}^{10} (7-i)x_i - 7x_{11}\right) \equiv x_5 \pmod{11},
\end{gathered} \tag{1.7}$$

Similarly, to find x_7:

$$\begin{gathered}
\sum_{i=1,i\neq5,i\neq7}^{10} ix_i + 5x_5 + 7x_7 \equiv 0 \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} x_i + x_5 + x_7 \equiv x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} 5x_i + 5x_5 + 5x_7 \equiv 5x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} (5-i)x_i - 2x_7 \equiv 5x_{11} \pmod{11}, \\
\sum_{i=1,i\neq5,i\neq7}^{10} (5-i)x_i - 5x_{11} \equiv 2x_7 \pmod{11}, \\
6\left(\sum_{i=1,i\neq5,i\neq7}^{10} (5-i)x_i - 5x_{11}\right) \equiv x_7 \pmod{11}.
\end{gathered} \tag{1.8}$$

Applying (1.7) and (1.8) to the received vector gives

$x_5 \equiv -6(64 + 7 - 6 - 7(1)) \equiv -6(58) \equiv -348 \equiv -7 \equiv 4 \pmod{11}$, and
$x_7 \equiv 6(30 - 7 - 14 - 5(1)) \equiv 6(4) \equiv 24 \equiv 2 \pmod{11}$.

So, $x_5 = 4$ and $x_7 = 2$. Thus, the corrected received vector is 2159**4**7**2**3011.

(iii) From part (ii) we solved for two unknowns using the two equations (1.7) and (1.8) and therefore unique values were found for the two unknowns. In view of this, it is not possible to solve uniquely for three unknowns having access only to these two equations. Three equations would be needed to solve uniquely for three unknowns.

(d) From part (c) above it was shown that we can solve uniquely for one or two erasures but not for three for a modified ISBN-10 code. Therefore, the modified ISBN-10 code is 2-erasure correcting.

Q 2.

(a) To determine which of the following codes are linear over the alphabet indicated use will be made of conditions (1) and (2) of **H** on page 47.

(i)

$$C_1 = \{00000, 11001, 10011, 01010\} \text{ over } \mathbb{Z}_2$$

To check this, we have to show that C_1 is closed under addition and scalar multiplication, so we have for scalar multiplication

$$\mathbf{0}c = 00000, \qquad 1c = c$$

for any codeword c in C_1. For addition we have

$$c + c = 00000 \text{ and } c + 00000 = c$$

for any codeword c in C_1 and

$$\begin{aligned} 11001 + 10011 &= 01010 \in C_1, \\ 11001 + 01010 &= 10011 \in C_1, \\ 10011 + 01010 &= 11001 \in C_1. \end{aligned}$$

In view of the forgoing C_1 is linear as it passes both conditions of **H** on page 47.

(ii)

$$C_2 = \{000, 001, 010, 100\} \text{ over } \mathbb{Z}_2$$

$$001 + 010 = 011 \notin C_2.$$

C_2 is not linear as it fails under condition (1) of **H** on page 47.

(iii)

$$C_3 = 00000, 11001, 10011, 01010 \text{ over } \mathbb{Z}_3$$

$$11001 + 10011 = 21012 \notin C_3.$$

C_3 is not linear as it fails under condition (1) of **H** on page 47.

(b) Using Theorem 5.4 of **H** page 50 G_2 can be obtained from G_1 in the following way:

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \xrightarrow{r_2 \to r_2 + r_1} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \xrightarrow{r_3 \to r_3 + r_2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{r_1 \leftrightarrow r_3} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

. Thus, G_1 and G_2 are equivalent as linear codes.

(c) Listed in Table 7 are the codewords of C.

$\mathbf{0}$	0	0	0	0	0
$\boldsymbol{x_1}$	1	2	0	1	2
$\boldsymbol{x_2}$	1	0	2	0	1
$\boldsymbol{x_3}$	0	1	1	2	0
$\boldsymbol{x_1 + x_2}$	2	2	2	1	0
$\boldsymbol{x_1 + x_3}$	1	0	1	0	2
$\boldsymbol{x_2 + x_3}$	1	1	0	2	1
$\boldsymbol{x_1 + x_2 + x_3}$	2	0	0	0	0

Table 7: List of codewords for C.

(d) Placing generator matrix G of part (c) in standard form gives:

$$
\begin{aligned}
G = \left(\begin{array}{ccc|cc} 1 & 2 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 \end{array}\right) &\xrightarrow{r_1 \to r_1 - 2r_3} \left(\begin{array}{ccc|cc} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 \end{array}\right) \\
&\xrightarrow{r_2 \to r_2 - r_1} \left(\begin{array}{ccc|cc} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 \end{array}\right) \\
&\xrightarrow{r_2 \leftrightarrow r_3} \left(\begin{array}{ccc|cc} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right) \\
&\xrightarrow{r_1 \to r_1 - r_3} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right) \\
&\xrightarrow{r_2 \to r_2 - r_3} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)
\end{aligned}
$$

Now using Theorem 7.6 of **H** page 70: if $G = [I_k|A]$ is the standard form generator matrix of an $[n, k]$-code C, then a parity-check matrix for C is $H = [-A^T|I_{n-k}]$. So, in this case

$$
H = \left(\begin{array}{ccc|cc} 0 & -2 & 0 & 1 & 0 \\ -1 & -2 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|cc} 0 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 1 \end{array}\right).
$$

(e)

(i) Supposing that D is a binary linear code having a generator matrix in which all the rows are of even weight. A 2-ary repetition code of even weight over $GF(2)$ is an $[n, 1]$-code with a generator matrix

H p.62 Example 5.3 (*iii*).

$$[11 \ldots 1]$$

is such a code. The weight of the single row of the generator matrix is of even weight because n is an even number. The codewords obtained from this generator matrix are the all zero vector and the vector comprising the row of the generator matrix. Both vectors have even weight thus showing that all codewords of D obtained from the generator matrix having rows of equal weight also have even weight too.

(ii) Supposing that D is a binary linear code having a generator matrix in which all the rows are of odd weight. A 2-ary repetition code of odd length over $GF(2)$ is an $[n, 1]$-code with a generator matrix

$$[11 \ldots 1]$$

is such a code. The weight of the single row of the generator matrix is of odd weight because n is an odd number. The codewords of D obtained from this generator matrix are the all zero vector and the vector comprising the row of the generator matrix. The former codeword has even weight while the latter has odd weight because n is an odd number. This shows that half the codewords have even weight and half have odd weight when at least one row of the generator matrix has odd weight.

Q 3.

(a) Given that the binary code C has generator matrix

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

the codewords of C are shown in Table 8.

combination	**codewords**						**weight**
$\mathbf{0}$	0	0	0	0	0	0	0
$\boldsymbol{u_1}$	1	0	0	1	1	0	3
$\boldsymbol{u_2}$	0	1	0	1	0	1	3
$\boldsymbol{u_1 + u_3}$	1	0	1	0	0	1	3
$\boldsymbol{u_2 + u_3}$	0	1	1	0	1	0	3
$\boldsymbol{u_3}$	0	0	1	1	1	1	4
$\boldsymbol{u_1 + u_2}$	1	1	0	0	1	1	4
$\boldsymbol{u_1 + u_2 + u_3}$	1	1	1	1	0	0	4

Table 8: Codewords of C ordered by codeword weight.

$$C = 00000\ 100110\ 010101\ 001111\ 110011\ 101001\ 011010\ 111100$$

Show in Table 9 is a Slepian standard array for C

000000	100110	010101	001111	110011	101001	011010	111100
100000	000110	110101	101111	010011	001001	111010	011100
010000	110110	000101	011111	100011	111001	001010	101100
001000	101110	011101	000111	111011	100001	010010	110100
000100	100010	010001	001011	110111	101101	011110	111000
000010	100100	010111	001101	110001	101011	011000	111110
000001	100111	010100	001110	110010	101000	011011	111101
110000	010110	100101	111111	000011	011001	101010	001100

Table 9: A Slepian standard array for C

Table 10 shows the number of coset leaders and their associated weight while Table 11 shows the number of coset leaders of weight i for $i = 0, 1, \ldots, 6$. Thus, from Table 11 we have $\alpha_0 = 1$, $\alpha_1 = 6$, $\alpha_2 = 1$, $\alpha_3 = 0$, $\alpha_4 = 0$, $\alpha_5 = 0$, $\alpha_6 = 0$.

Assuming the codewords are transmitted over a binary symmetric channel that has symbol error probability p, the word error probability is determined as follow.

$$P_{err} = 1 - P_{corr}(C)$$

coset leader	**weight**
000000	0
100000	1
010000	1
001000	1
000100	1
000010	1
000001	1
110000	2

Table 10: Weights of the coset leaders

i	$\boldsymbol{\alpha_i}$
0	1
1	6
2	1
3	0
4	0
5	0
6	0

Table 11: the number of coset leaders of weight i for $i = 0, 1, \ldots, 6$.

where $P_{corr}(C)$ is given by

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}.$$

Here, $n = 6$ with $\alpha_0 = 1, \alpha_1 = 6, \alpha_2 = 1$ and $\alpha_3, \ldots, \alpha_6 = 0$ so that

$$\begin{aligned}
P_{corr}(C) &= \sum_{i=0}^{6} \alpha_i p^i (1-p)^{6-i}, \\
&= \alpha_0 p^0 (1-p)^6 + \alpha_1 p^1 (1-p)^5 + \alpha_2 p^2 (1-p)^4, \\
&= (1-p)^6 + 6p(1-p)^5 + p^2(1-p)^4, \\
&= (1-p)^4 \left[(1-p)^2 + 6p(1-p) + p^2\right], \\
&= (1-p)^4 \left[1 - 2p + p^2 + 6p - 6p^2 + p^2\right], \\
&= (1-p)^4 \left[1 - 2p + p^2 + 6p - 6p^2 + p^2\right], \\
&= (1-p)^4 \left[1 + 4p - 4p^2\right], \\
&= (1-p)^4 \left[1 + 4p(1-p)\right].
\end{aligned}$$

Therefore,

$$P_{err} = 1 - (1-p)^4 \left[1 + 4p(1-p)\right].$$

x_1	x_2	x_3	x_4	x_5	x_6	probability
0	0	0	0	0	0	$(1-r)^6$
1	0	0	0	0	0	$r(1-r)^5$
0	1	0	0	0	0	$r(1-r)^5$
0	0	1	0	0	0	$r(1-r)^5$
0	0	0	1	0	0	$r(1-r)^5$
0	0	0	0	1	0	$r(1-r)^5$
0	0	0	0	0	1	$r(1-r)^5$
1	1	0	0	0	0	$r^2(1-r)^4$

Table 12: Probability of a received vector $\boldsymbol{y}$ being correctly decoded as $\boldsymbol{x} = 000000$ assuming $\boldsymbol{x} = \boldsymbol{y} - \boldsymbol{e}$ where $\boldsymbol{e}$ is a coset leader. In other words the received vector was one of the eight coset leaders.

(b)

From Table 12 is can be seen that the probability of a received vector being correctly decoded is given by the sum of the terms in the probability column of the table. Thus,

$$\begin{aligned} P_{corr} &= (1-r)^6 + 6r(1-r)^5 + r^2(1-r)^4, \\ &= (1-r)^4 \left[(1-r)^2 + 6r(1-r) + r^2, \right], \\ &= (1-r)^4 \left[(1-2r+r^2 + 6r - 6r^2 + r^2, \right], \\ &= (1-r)^4 \left[(1+4r+4r^2, \right], \end{aligned}$$

as required.

Using Table 13 the probability of a received vector being correctly decoded as each of the codewords of weight 3 is given by (3.1).

x_1	x_2	x_3	x_4	x_5	x_6	probability
1	0	0	1	1	0	$(1-r)^3(1-s)^3$
0	0	0	1	1	0	$s(1-r)^3(1-s)^2$
1	1	0	1	1	0	$r(1-r)^2(1-s)^3$
1	0	1	1	1	0	$r(1-r)^2(1-s)^3$
1	0	0	0	1	0	$s(1-r)^3(1-s)^2$
1	0	0	1	0	0	$s(1-r)^3(1-s)^2$
1	0	0	1	1	1	$r(1-r)^2(1-s)^3$
0	1	0	1	1	0	$rs(1-r)^2(1-s)^2$

Table 13: Probability of a received vector being correctly decoded as each of the codewords of weight 3.

$$\begin{aligned} P_{corr} &= (1-r)^3(1-s)^3 + 3s(1-r)^3(1-s)^2 + 3r(1-r)^2(1-s)^3 + rs(1-r)^2(1-s)^2, \\ &= (1-r)^2(1-s)^2\left[(1-r)(1-s) + 3s(1-r) + 3r(1-s) + rs\right], \\ &= (1-r)^2(1-s)^2\left[1 - r - s + rs + 3s - 3rs + 3r - 3rs + rs\right], \\ &= (1-r)^2(1-s)^2\left[1 + 2r + 2s - 4rs\right], \end{aligned} \tag{3.1}$$

as required.

Using Table 14 the probability of a received vector being correctly decoded as each of the codewords of weight 4 is given by (3.2).

$$P_{corr} = (1-r)^2(1-s)^4 + 2r(1-r)(1-s)^4 + 4s(1-r)^2(1-s)^3 + r^2(1-s)^4. \tag{3.2}$$

x_1	x_2	x_3	x_4	x_5	x_6	probability
0	0	1	1	1	1	$(1-r)^2(1-s)^4$
1	0	1	1	1	1	$r(1-r)(1-s)^4$
0	1	1	1	1	1	$r(1-r)(1-s)^4$
0	0	0	1	1	1	$s(1-r)^2(1-s)^3$
0	0	1	0	1	1	$s(1-r)^2(1-s)^3$
0	0	1	1	0	1	$s(1-r)^2(1-s)^3$
0	0	1	1	1	0	$s(1-r)^2(1-s)^3$
1	1	1	1	1	1	$r^2(1-s)^4$

Table 14: Probability of a received vector being correctly decoded as each of the codewords of weight 4.

(c) The Table 15 is used for incomplete decoding and shows a top part and a bottom part. $d(C) = 2t + 1 = 3$ for C in this case and $t = 1$. So, the

000000	100110	010101	001111	110011	101001	011010	111100
100000	000110	110101	101111	010011	001001	111010	011100
010000	110110	000101	011111	100011	111001	001010	101100
001000	101110	011101	000111	111011	100001	010010	110100
000100	100010	010001	001011	110111	101101	011110	111000
000010	100100	010111	001101	110001	101011	011000	111110
000001	100111	010100	001110	110010	101000	011011	111101
110000	010110	100101	111111	000011	011001	101010	001100

Table 15: A partitioned Slepian standard array for C

incomplete decoding scheme guarantees the correction of $\leq t, \leq 1$ errors in any codeword.

(i) Given the received vector $\boldsymbol{y} = 111111$ which appears in the bottom part of Table 15 we conclude that more than one error has occurred during transmission and request the resending of the codeword.

(ii) Given the received vector $\boldsymbol{y} = 110011$ which appears in the top row of the upper part of Table 15 we conclude that no errors have occurred and decode the received vector as the codeword 110011.

(iii) Given the received vector $\boldsymbol{y} = 111101$ which appears in the upper part of Table 15, in a row other than the top row, we conclude that one error has occurred and decode the vector as the codeword 111100.

Q 4.

(a) The code D is a linear $[6,4]$-code over $GF(7) = \{0,1,\ldots,6\}$ and the codewords $\boldsymbol{x} = x_1x_2x_3x_4x_5x_6$ are defined by two parity-check equations

$$\sum_{i=1}^{6} x_i \equiv 0 \pmod 7 \quad \text{and} \quad \sum_{i=1}^{6} ix_i \equiv 0 \pmod 7$$

The algorithm that will correct any single transmission error in a codeword of D is developed as follows.

Assume that a single transmission error has occurred in the j^{th} position of the received codeword. Then the value of $j \in \{1,2,\ldots,6\}$ can be found as follows.

For the codeword as transmitted:

$$\sum_{i=1,i\neq j}^{6} x_i + x_j \equiv 0 \pmod 7, \tag{4.1}$$

$$\sum_{i=1,i\neq j}^{6} ix_i + jx_j \equiv 0 \pmod 7. \tag{4.2}$$

For the codeword as received assuming a single transmission error has occurred at coordinate position j and that x_j has been changed to y_j, then we have:

$$\sum_{i=1,i\neq j}^{6} x_i + y_j \equiv a \pmod 7, \tag{4.3}$$

$$\sum_{i=1,i\neq j}^{6} ix_i + jy_j \equiv b \pmod 7. \tag{4.4}$$

(4.3) − (4.1) gives (4.5)

$$y_j - x_j \equiv a \pmod 7. \tag{4.5}$$

(4.4) − (4.2) gives (4.6)

$$jy_j - jx_j \equiv b \pmod 7. \tag{4.6}$$

(4.5) × j gives (4.7)

$$jy_j - jx_j \equiv ja \pmod 7. \tag{4.7}$$

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 16: $GF\{7\}$ multiplication table to find the multiplicative inverse of j.

(4.7) − (4.6) gives (4.8)

$$\begin{aligned} ja - b &\equiv 0 \pmod 7, \\ ja &\equiv b \pmod 7, \\ j &\equiv a^{-1}b \pmod 7, \end{aligned} \tag{4.8}$$

where a^{-1} is the multiplicative inverse of a in $GF\{7\}$. From (4.2) knowing j then x_j is found as follows

$$\begin{aligned} \sum_{i=1, i\neq j}^{6} ix_i + jx_j &\equiv 0 \pmod 7, \\ \sum_{i=1, i\neq j}^{6} ix_i &\equiv -jx_j \pmod 7, \\ -j^{-1} \sum_{i=1, i\neq j}^{6} ix_i &\equiv x_j \pmod 7. \end{aligned} \tag{4.9}$$

Now assume that two digits of the received codeword have been transposed. Then regardless of which two digits were transposed $\sum_{i=1}^{6} x_i \equiv 0 \pmod 7$ is still true.

Let the two digits that were transposed be the ones at the j^{th} and k^{th} coordinate positions in the received codeword where $k > j$ and $j, k \in \{1, 2, \ldots, 6\}$ and further suppose that $x_i \neq x_j$. Then,

$$\sum_{i=1, i\neq j, i\neq k}^{j-1} ix_i + kx_j + jx_k \not\equiv 0 \pmod 7.$$

Thus, algorithm is as follows.

- If (4.1) and (4.2) are true then no errors have occurred and we therefore accept the received codeword.

- If (4.1) is true but not (4.2) then a transposition error has occurred so request retransmission of the codeword as it cannot be corrected.
- If both (4.1) and (4.2) are not true then assume a single error. Use (4.8) to determine the location, j, of the error in the codeword and then use (4.9) in conjunction with Table 16 to find the multiplicative inverse of j to determine the correct digit.

(i) Given the received vector is $\boldsymbol{x} = 113235$ then using (4.1) we have

$$a = \sum_{i=1}^{6} x_i \equiv 15 \pmod 7 \equiv 1 \pmod 7,$$

and

$$b = \sum_{i=1}^{6} i x_i \equiv 65 \pmod 7 \equiv 2 \pmod 7.$$

Using (4.8)

$$j = a^{-1}b \pmod 7 = 1^{-1} \times 2 \pmod 7 \equiv 2 \pmod 7.$$

So the digit at location 2 is the one that is in error. To determine the correct digit use (4.9).

$$x_2 = -\sum_{i=1, i\neq 2}^{6} i x_i \equiv -63 \pmod 7 \equiv 0.$$

Thus, the correct codeword is 103235.

(ii) Given the received codeword is 625152 then in this case $a = 0$ and $b = 3$ so by the above algorithm a transposition error has occurred and so a request for retransmission of the codeword should be sent.

(b) The linear code D is a [6,4]-code over $GF(7)$ which has a generator matrix G. D contains $q^k = 7^4$ codewords so can be used to transmit any one of 7^4 distinct messages. Each of these codeword can be generated from a message vector $\boldsymbol{u} = u_1u_2u_3u_4$, where each $u_i \in GF(7)$, as follows

$$\begin{aligned}\boldsymbol{x} = \boldsymbol{u}G &= \begin{bmatrix} u_1 & u_2 & u_3 & u_4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & a_{11} & a_{12} \\ 0 & 1 & 0 & 0 & a_{21} & a_{22} \\ 0 & 0 & 1 & 0 & a_{31} & a_{32} \\ 0 & 0 & 0 & 1 & a_{41} & a_{42} \end{bmatrix} \\ &= u_1u_2u_3u_4 \sum_i a_{i1}u_i \sum_i a_{i2}u_i.\end{aligned}$$

Assume now that we choose *one* coordinate position to be the symbol "6". Then we are free to choose any symbol from $GF(7)$ for any other

three coordinate positions. We have no choice of the symbols for the remaining two coordinate positions because the two parity check equations have to be satisfied. Thus, if we fix one coordinate position we have $7 \times 7 \times 7 = 7^3$ choices for three other symbols at three other coordinate positions. Therefore, the number of codewords of D that have the symbol "6" in any one specified coordinate position is 7^3.

Assume now that we choose *two* coordinate positions to be the symbol "6". Then we are free to choose any symbol from $GF(7)$ for any other two coordinate positions. We have no choice of the symbols for the remaining two coordinate positions because the two parity check equations have to be satisfied. Thus, if we fix two coordinate position we have $7 \times 7 = 7^2$ choices for two other symbols at two other coordinate positions. Therefore, the number of codewords of D that have the symbol "6" in any two specified coordinate positions is 7^2.

Assume now that we choose *three* coordinate positions to be the symbol "6". Then we are free to choose any symbol from $GF(7)$ for any other one coordinate position. We have no choice of the symbols for the remaining two coordinate positions because the two parity check equations having to be satisfied. Thus, if we fix three coordinate position we have 7 choices for one other symbol at one other coordinate position. Therefore, the number of codewords of D that have the symbol "6" in any three specified coordinate positions is 7.

Assume now that we choose *four* coordinate position to be the symbol "6". Then we are *not* free to choose any symbol from $GF(7)$ for any other coordinate position because the two parity check equations have to be satisfied. Thus, if we fix four coordinate positions this is the only (one) choice we can make. Therefore, the number of codewords of D that have the symbol "6" in any four specified coordinate positions is $7^0 = 1$.

(c) Using the two parity-check equations it can be proved that no codeword of D contains five or six "6"s as follows. Assume that there can be six sixes in a codeword of D in which case both parity check equation should be zero. It can be easily shown that

$$A = \sum_{i=1}^{6} i6 \equiv 126 \equiv 0 \pmod 7, \tag{4.10}$$

and

$$B = \sum_{i=1}^{6} 6 \equiv 36 \equiv 1 \pmod 7. \tag{4.11}$$

So according to **H** page 78 if $A = 0$ or $B = 0$ but not both, then at least two errors have been detected. If two errors have occurred then that means there cannot be five or six sixes in any codeword of D. Note that the transposition of two digits does not affect the outcome and therefore can be discounted.

(d) By the inclusion-exclusion principle, in which the sets A, B to F are the sets of codewords in D that have the symbol "6" in the first, second, to the sixth coordinate positions respectively, we have

$$
\begin{aligned}
|A \cup B \cup C \cup D \cup E \cup F| = {} & |A| + |B| + |C| + |D| + |E| + |F| \\
& - |A \cap B| - |A \cap C| - |A \cap D| - |A \cap E| - |A \cap F| \\
& - |B \cap C| - |B \cap D| - |B \cap E| - |B \cap F| \\
& - |C \cap D| - |C \cap E| - |C \cap F| \\
& - |D \cap E| - |D \cap F| \\
& - |E \cap F| \\
& + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap B \cap E| + |A \cap B \cap F| \\
& + |A \cap C \cap D| + |A \cap C \cap E| + |A \cap C \cap F| \\
& + |A \cap D \cap E| + |A \cap D \cap F| \\
& + |B \cap C \cap D| + |B \cap C \cap E| + |B \cap C \cap F| \\
& + |B \cap D \cap E| + |B \cap D \cap F| \\
& + |B \cap E \cap F| \\
& + |C \cap D \cap E| + |C \cap D \cap F| \\
& + |C \cap E \cap F| \\
& - |A \cap B \cap C \cap D| - |A \cap B \cap C \cap E| - |A \cap B \cap C \cap F| \\
& - |A \cap B \cap D \cap E| - |A \cap B \cap D \cap F| - |A \cap B \cap E \cap F| \\
& - |A \cap C \cap D \cap E| - |A \cap C \cap D \cap F| - |A \cap C \cap E \cap F| \\
& - |A \cap D \cap E \cap F| \\
& - |B \cap C \cap D \cap E| - |B \cap C \cap D \cap F| - |B \cap C \cap E \cap F| \\
& - |B \cap D \cap E \cap F| \\
& - |C \cap D \cap E \cap F| \\
& + |A \cap B \cap C \cap D \cap E| + |A \cap B \cap C \cap D \cap F| \\
& + |A \cap B \cap C \cap E \cap F| + |A \cap B \cap D \cap E \cap F| \\
& + |A \cap C \cap D \cap E \cap F| \\
& + |B \cap C \cap D \cap E \cap F| \\
& - |A \cap B \cap C \cap D \cap E \cap F|.
\end{aligned}
$$

In the above we have six sets of order 1, $\binom{6}{1} = 6$; fifteen sets of order 2, $\binom{6}{2} = 15$; twenty sets of order 3, $\binom{6}{3} = 20$; fifteen set of order 4, $\binom{6}{4} = 15$. There are six sets of order 5; and one set of order 6. It is not possible to have codewords with five or more sixes in them and therefore the sets of order 5 and order 6 can be discounted. Now, the number of codewords that have the symbol "6" in any specified position is 7^3; the number of codewords that have the symbol "6" in any specified pair of coordinates is 7^2. The number of codewords that have the symbol "6" in any specified triple of coordinate positions is 7^1 and the number of codewords with the

symbol "6" in any specified quadruple of coordinate positions is 7^0. Thus, the number of codewords of D that contain the symbol "6" is

$$6 \cdot 7^3 - 15 \cdot 7^2 + 20 \cdot 7^1 - 15 \cdot 7^0.$$

As there are q^k codewords in a $[n, k]$-code over $GF\{q\}$ then we have in the case of D, which is a $[6, 4]$-code over $GF(7)$, 7^4 codewords. Thus, the number of codewords of D that do not contain the symbol "6" is

$$7^4 - (6 \cdot 7^3 - 15 \cdot 7^2 + 20 \cdot 7^1 - 15) = 953,$$

as required.

(e) Assume that there can be ten sixes in a codeword of C in which case both parity check equation should be zero and the codeword is valid. It can be easily shown that

$$A = \sum_{i=1}^{10} i6 \equiv 330 \equiv 0 \pmod{11}, \tag{4.12}$$

and

$$B = \sum_{i=1}^{10} 6 \equiv 60 \equiv 5 \pmod{11}. \tag{4.13}$$

So according to **H** page 78 if $A = 0$ or $B = 0$ but not both, then at least two errors have been detected. If two errors have occurred then that means there cannot be nine or ten sixes in any codeword of C. Note that the transposition of two digits does not affect the outcome and therefore can be discounted.

Using a similar argument to that of part (d) above but this time for the $[10, 8]$-code defined over $GF\{11\}$ we can summarise the previous argument in Table 17 proving that there are 82644629 codewords in C.

Thus, from the summary Table 17 it is proved that there are 82644629 codewords in C as stated by **H** page 76.

n	k	$a = \binom{n}{k}$	$b = 11^{8-k}$	sign	sign $\times\, a \times b$
10	1	10	19487171	1	194871710
10	2	45	1771561	-1	-79720245
10	3	120	161051	1	19326120
10	4	210	14641	-1	-3074610
10	5	252	1331	1	335412
10	6	210	121	-1	-25410
10	7	120	11	1	1320
10	8	45	1	-1	-45
					131714252
					$11^7 - 131714252 = 82644629$

Table 17: Summary of derivation of the number of codewords in C using a similiar derivation to that in part (d).