Q 1.

(a) To prove that if $1 < m \leq n$, then there cannot exist a set of n mutually orthogonal $m \times n$ Latin rectangles, $(MOLR)_{m\times n}$, consider the following (which follows the argument given in **H Theorem 10.18**, p122.).

Assume we have a set of $(MOLR)_{m\times n}$ where $2 \leq m \leq n$ and with symbols from the alphabet $F_n = \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$. Each of the Latin rectangles in the set of $(MOLR)_{m\times n}$ may have their symbols renamed while still maintaining the orthogonality of the set. For example, assume that we have a set of two $(MOLR)_{2\times 3}$, namely:

Glossary: Alphabet p5.

$$\left\{ \begin{matrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_2 & \lambda_3 & \lambda_1 \end{matrix}, \begin{matrix} \lambda_3 & \lambda_2 & \lambda_1 \\ \lambda_1 & \lambda_3 & \lambda_2 \end{matrix} \right\} \text{ then } \begin{matrix} (\lambda_1, \lambda_3) & (\lambda_2, \lambda_2) & (\lambda_3, \lambda_1) \\ (\lambda_2, \lambda_1) & (\lambda_3, \lambda_3) & (\lambda_1, \lambda_2) \end{matrix} .$$

Now, by renaming the symbols of each of the Latin rectangles in the set so that the symbols in the first row of each rectangle are $0, 1, 2$ in natural order, we obtain

$$\left\{ \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{matrix}, \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{matrix} \right\} \text{ then } \begin{matrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \end{matrix} ,$$

showing that the two mutually orthogonal Latin rectangles in the set still remain mutually orthogonal after renaming the symbols in the way shown. So, in general, a set of $(MOLR)_{m\times n}$ can have the symbols in their first rows renamed so that each of the first rows of each rectangles are $0, 1, \ldots, n-1$ in natural order and still maintain the orthogonality between pairs of rectangles in the set. Having established this, now consider the symbol in the first index position of the second row (i.e. row 1, column 0 using the indexing scheme given in the question) of each of the Latin rectangles. From the definition of a Latin rectangle given in the question this symbol cannot be 0 as the first row of each rectangle is in the natural order of $0, 1, \ldots, n-1$ so it must be one of the symbols in the set $\{1, 2, \ldots, n-1\}$. Also, none of the symbols in the first column of the second row of each rectangle in the set can be the same, for if they were, then when superimposing one rectangle upon another a duplicate of $(0,0), (1,1), \ldots (n-1, n-1)$ would appear in the first row of the superimposed rectangles. This constrains the cardinality of the set of $(MOLR)_{m\times n}$ to a maximum of $n-1$. Consequently, it has been proved that if $1 < m \leq n$, then there cannot exist a set of n mutually orthogonal $m \times n$ Latin rectangles as the maximum value of the cardinality of such a set is $n-1$.

To determine the maximum possible number of mutually orthogonal $1 \times n$ Latin rectangles consider the following cases for $n = 1$, $n = 2$ and $n = 3$.

For the case where $n = 1$ then we have $1! = 1$ Latin rectangle so there is no other rectangle for it to be mutually orthogonal to apart from itself.

For the case where $n = 2$ then we have $2! = 2$ mutually orthogonal Latin rectangles: $[a\ b]$ and $[b\ a]$.

For the case where $n = 3$ then we have $3! = 6$ mutually orthogonal Latin rectangles: $[a\ b\ c]$, $[a\ c\ b]$, $[b\ a\ c]$, $[b\ c\ a]$, $[c\ a\ b]$ and $[c\ b\ c]$.

For the general case where we have a $1 \times n$ Latin rectangles then we have the permutation of n objects taken n at a time:

$$^nP_n = \frac{n!}{(n-n)!} = n!$$

In view of this the maximum possible number of mutually orthogonal $1 \times n$ Latin rectangles is $n!$.

(b)

(i) From the question preamble $p > 1$ is prime and $q > 1$ is an integer such that each of the prime factors of q are greater or equal to p. Let $n = pq$. Then for $\lambda = 1, 2, \ldots, n-1$, define A_λ to be the $p \times n$ array with entries $a_{i,j}^{(\lambda)} \equiv \lambda i + j \pmod{n}$ for $i = 0, 1, \ldots, p-1$, $j = 0, 1, \ldots, n-1$. Now, in order to prove that A_λ is a $p \times n$ Latin rectangle consider the following.

The entries in A_λ, $a_{i,j}^{(\lambda)}$, are those in the $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ as $a_{i,j}^{(\lambda)} \equiv \lambda i + j \pmod{n}$, where λ is non-zero. The rows are indexed by $0, 1, \ldots, n-1$ and columns are indexed by $0, 1, \ldots, p-1$ where i refers to the row index and j to that of the column index in the array element $a_{i,j}^{(\lambda)}$. Therefore, the array A_λ is a $p \times n$ array, i.e. a rectangle with the number of columns greater than the number of rows.

Now, assume that two elements in a given row, row i say, are the same at index locations j and j'. In this case we then have $a_{i,j}^{(\lambda)} = a_{i,j'}^{(\lambda)}$ in which case $\lambda i + j = \lambda i + j'$ with arithmetic in $\mathbb{Z}_n$. As $\lambda \neq 0$ this implies that $j = j'$ and therefore each element of the i-th row appears exactly once.

Similarly assume two elements are the same in two columns, column j say. In this case we then have $a_{i,j}^{(\lambda)} = a_{i',j}^{(\lambda)}$ in which case $\lambda i + j = \lambda i' + j$ with, as before, arithmetic in $\mathbb{Z}_n$. As $\lambda \neq 0$ this implies $i = i'$ and therefore each element of the j-th column are distinct.

Thus, the conditions for the array A_λ to be that of a Latin rectangle have been met.

(ii) To prove that A_λ and A_μ are mutually orthogonal given that $\lambda \neq \mu$, thus forming a set $\{A_\lambda : 1 \leq \lambda \leq n-1\}$ of $n-1$ mutually orthogonal Latin rectangles consider the following.

First we prove that the elements of the first row of each rectangle A_λ and A_μ are equal as follows:

Let the elements of the first rectangle be $a_{i,j} = \lambda i + j$ and those of the second rectangle be $b_{i,j} = \mu i + j$. When $i = 0$, that is the first row of each rectangle, then

$$a_{0,j} = 0 \times i + j = j; \quad \text{and} \quad b_{0,j} = 0 \times i + j = j,$$

and thus, elements of the first rows of each of the rectangles are equal corresponding to the column index, j, for $j = 0, 1, \ldots, n-1$.

Now consider a row, i, which is not the first and as such $i \neq 0$ and assume that the element $a_{i,j} = b_{i,j}$ in which case the rectangles A_λ and A_μ are *not* mutually orthogonal as the pair $(a_{i,j}, b_{i,j})$ will have occurred in the first row of the superposition of A_λ on A_μ. Then,

$$a_{i,j} = \lambda \times i + j \quad \text{and} \quad b_{i,j} = \mu \times i + j, \quad i \neq 0, \quad j = 0, 1, \ldots, n-1,$$

which implies that $\lambda = \mu$ which is a contradiction. As such each of the Latin rectangles in the set $\{A_\lambda : 1 \leq \lambda \leq n-1\}$ are mutually orthogonal.

(c)

(i)

0	0	0	0	0	0	0
0	1	1	1	1	1	1
0	2	2	2	2	2	2
0	3	3	3	3	3	3
0	4	4	4	4	4	4
0	5	5	5	5	5	5
1	0	1	2	3	4	5
1	1	2	3	4	5	0
1	2	3	4	5	0	1
1	3	4	5	0	1	2
1	4	5	0	1	2	3
1	5	0	1	2	3	4

Table 1: The codewords of $C_{2,3}$.

(ii) To determine the minimum distance of $C_{p,q}$ in terms of p and q consider the following.

A code $C_{p,q}$ is formed from Latin rectangles A_λ by taking as codewords all vectors of the form:

$$(i, j, a_{i,j}^{(1)}, a_{i,j}^{(2)}, \ldots, a_{i,j}^{(n-1)})$$

for $i = 0, 1, \ldots, p-1$ and $j = 0, 1, \ldots, n-1$ where $n = pq$. Now, $a_{i,j}^{(\lambda)} = \lambda i + j$ for $\lambda = 1, 2, \ldots, n-1$ and the codewords can be generated using the generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 1 & 2 & \cdots & n-1 \\ 0 & 1 & 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Thus, for example, each of the codewords shown in Table 1 can be generated from the generator matrix, G, as follows.

$$\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$i = 0, 1, \ldots, p-1, \quad j = 0, 1, \ldots, n-1.$$

As an example consider the case for $i = 1$ and $j = 5$; the codeword generated is thus:

$$\begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

In order to determine the minimum distance between codewords for the general case consider what happens when i and j are both zero; i is zero but j is non-zero and visa-versa; and when both are non-zero.

$i = 0, 1, \ldots, p-1,$
$j = 0, 1, \ldots, pq-1.$

1. When $i = 0$ and $j = 0$ then the codeword is the zero vector of length $pq + 1$.

2. When $i = 0$ and $j \neq 0$ then the codewords are of the form:

$$\begin{pmatrix} 0 & j & j & \cdots & j \end{pmatrix}$$

   where the length of the vector is $pq+1$ so that the symbol represented by j appears exactly pq times. That is, the weight of the vector is pq.

3. When $i \neq 0$ and $j = 0$ the the codewords are of the form:

$$\begin{pmatrix} i & 0 & i & 2i & \cdots & (pq-1)i \end{pmatrix} \pmod{pq},$$

   $\lambda = 1, 2, \ldots, pq-1.$

   where the length of the vector is $pq + 1$ and the symbol zero appears precisely once in the codewords generated in this fashion. This can easily been seen by considering the case where $i = p - 1$ and $\lambda = pq - 1$ (giving the maximum value of λi), then the last symbol of the codeword will be $\lambda i = (pq - 1)(p - 1) < pq$ and therefore, $\lambda i \not\equiv 0 \pmod{pq}$. Thus, the weights of these codewords are also pq.

4. Finally, when $i \neq 0$ and $j \neq 0$ the codewords are of the form

$$\begin{pmatrix} i & j & i+j & 2i+j & \cdots & (pq-1)i+j \end{pmatrix} \pmod{pq},$$

   where the length of the vector is $pq + 1$ and the symbol zero appears precisely once in the codewords generated in this fashion. This can be seen by considering how and when the symbol zero is generated in the codeword. It is generated precisely when

$$pq = \lambda i + j, \quad \lambda = 1, 2, \ldots, pq-1,$$

   which can only occur once in a codeword. So, again the weight of the codewords is equal to pq when $i \neq 0$ and $j \neq 0$.

In view of the foregoing and given each codeword is distinct then the minimum distance of $C_{p,q}$ is pq as each codeword differs from another in exactly pq coordinate positions.

Q 2.

(a)

(b)

(c)

(d)

Q 3.

(a)

(b)

(c)

(d)

Q 4.

(a)

(b)

(i)

(ii)

(c)