The main aim of this section is to construct codes using some mathematical constructs called **Latin Squares**, and vice-versa. Further, we will solve the *main coding theory problem* for single-error-correcting codes of length 4 i.e. find the values of $A_q(4,3)$ for all values of q.

Definition 0.1. A **Latin square of order** q is a $q \times q$ array whose entries are from a set F_q of q distinct symbols suzh that each row and each column of the array contains each symbol exactly once.

Example: Let $F_3 = \{1, 2, 3\}$. Then an example of a Latin square of order 3 is

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}$$

Theorem 0.2. There exists a Latin square of order q for any positive integer q.

Proof. We can take $1\ 2\ \cdots\ q$ as the first row and cycle this round once for each subsequent row to get

$$\begin{array}{cccccccc} 1 & 2 & 3 & \cdots & & & & q \\ 2 & 3 & 4 & \cdots & & q & & 1 \\ 3 & 4 & 5 & \cdots & q & 1 & & 2 \\ \vdots & \vdots & \vdots & & & & & \vdots \\ q & 1 & 2 & \cdots & & & & q-1 \end{array}$$

Alternatively, the addition table of Z_q is a Latin square of order q. $\square$

Definition 0.3. Let A and B be two Latin squares of order q. Let a_{ij} and b_{ij} denote the i,jth entries of A and B respectively. Then A and B are said to be ***mutually orthogonal*** Latin squares (abbreviated as MOLS) if the q^2 ordered pairs $(a_{ij}, b_{ij}),\ i,j = 1, 2, \ldots, q$ are all distinct.

Example: The Latin squares

$$A = \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array} \quad \text{and } B = \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{array}$$

0.1 Optimal single-error-correcting code of length 4

Theorem 0.4. $A_q(4,3) \leq q^2$, for all q.

Proof. Suppose C is a q-ary $(4, M, 3)$-code and let $\mathbf{x} = x_1x_2x_3x_4$ and $\mathbf{y} = y_1y_2y_3y_4$ be distinct codewords of C. Then $(x_1, x_2) \neq (y_1y_2)$, for otherwise $\mathbf{x}$ and $\mathbf{y}$ could differ only in the last two places, contradicting $d(C) = 3$. Therefore, $M \leq q^2$. $\square$

Theorem 0.5. There exists a q-ary $(4, q^2, 3)$-code if and only if there exists a pair of MOLS of the order q.

Proof. Let

$$C = \{(i, j, a_{ij}, b_{ij}) | (i,j) \in (F_q)^2\}$$

As in the proof of Theorem 0.4, the minimum distance of C is 3 if and only if, for each pair of coordinate positions, the ordered pairs appearing in those positions are distinct. Now the q^2 pairs of (i, a_{ij}) and q^2 pairs of (j, a_{ij}) are distinct if and only if A is a Latin square. Similarly, the q^2 pairs of (i, b_{ij}) and q^2 pairs of (j, b_{ij}) are distinct if and only if B is a Latin square. Lastly, the q^2 pairs (a_{ij}, b_{ij}) are distinct if and only if there exists a MOLS of order q. $\square$

Theorem 0.6. If q is a prime-power and $q \neq 2$, then there exists a pair of MOLS of order q.

Proof. Let F_q be the field $GF(q) = \{\lambda_0, \lambda_1, \ldots, \lambda_{q-1}\}$ where $\lambda_0 = 0$. Let μ and ν be two distinct non-zero elements of $GF(q)$. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $q \times q$ arrays defined by

$$a_{ij} = \lambda_i + \mu\lambda_j \ \ and \ \ b_{ij} = \lambda_i + \nu\lambda_j$$

We now see that A id Latin square and similarly so is B. As if two elements in the same of A are identical, then we have

$$\lambda_i + \mu\lambda_j = \lambda_i + \mu\lambda_j^{'}$$

implying $j = j'$ as μ is non-zero. Now for columns,

$$\lambda_i + \mu\lambda_j = \lambda_i' + \mu\lambda_j$$

implying that $i = i'$. Now, we prove that A and B are orthogonal, suppose on contrary that $(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'})$, then

$$\begin{aligned} \lambda_i + \mu\lambda_j &= \lambda_i' + \mu\lambda_j' \\ \text{and} \quad \lambda_i + \nu\lambda_j &= \lambda_i' + \nu\lambda_j' \end{aligned}$$

which on subtraction gives

$$(\mu - \nu)\lambda_j = (\mu - \nu)\lambda_j'$$

Since $\mu \neq \nu$, we have $j = j'$, and consequently, $i = i'$. □

Theorem 0.7. If there exists a pair of MOLS of order n as well as order m, then there exists a pair of MOLS of order mn.

Proof. Suppose A_1, A_2 is a pair of MOLS of order m and B_1, B_2 is a pair of MOLS of order n. Let C_1 and C_2 be the $mn \times mn$ squares defined by

$$C_k = \begin{matrix} (a_{11}^{(k)}, B_k) & (a_{12}^{(k)}, B_k) & \cdots & (a_{1m}^{(k)}, B_k) \\ (a_{12}^{(k)}, B_k) & (a_{22}^{(k)}, B_k) & \cdots & (a_{2m}^{(k)}, B_k) \\ \vdots & & & \vdots \\ (a_{m1}^{(k)}, B_k) & (a_{m2}^{(k)}, B_k) & \cdots & (a_{mm}^{(k)}, B_k) \end{matrix}$$

where $k \in \{1, 2\}$, $A_k = [a_{ij}^{(k)}]$ and $(a_{ij}^{(k)}, B_k)$ denotes an $n \times n$ array (referred as block in this proof) whose r, sth entry is $(a_{ij}^{(k)}, b_{rs}^{(k)})$ for $r, s \in \{1, 2, \cdots, n\}$.
From this construction it is trivial to see that C_k are Latin squares. Further assuming them to be not a pair of MOLS implies that in both C_1, C_2 either two entries in a block are same or, two entries are same in blocks having different row and column. The first possibility contradicts B_k being a pair of MOLS, and the latter contradicts A_k being a pair of MOLS. □

Theorem 0.8. If $q \equiv 0, 1$ or $3 \pmod 4$. Then there exists a pair of MOLS of order q.

Proof. One can break down each of q satisfying $q \equiv 0, 1$ or $3 \pmod 4$ into their prime factorisation, then each of the prime-power in it will be ≥ 3. Thus, repeated application of Theorem 0.6 and Theorem 0.7 will give us the required pair of MOLS for each of these q. □

Note: Theorem 0.8 leaves cases when $q \equiv 2 \pmod 4$. It has been proved pair of MOLS also exist for these cases except for $q = 2$ and $q = 6$. The proof will not be covered in this report.

Corollary 0.8.1. $A_q(4, 3) = q^2$ for all $q \neq 2, 6$.

Proof. This is immediate from Theorems 0.4, 0.5 and 0.8. □

Remark. For $q = 2$, it is trivial to see that $A_2(4, 3) = 2$, while for $q = 6$, a construction similar to pair of orthogonal Latin squares gives $A_6(4, 3) = 34$.

Some generalization of the above results.

Theorem 0.9 (Singleton bound).

$$A_q(n, d) \leq q^{n-d+1}.$$

Proof. Suppose C is a q-ary (n, M, d)-code.Same as in proof of Theorem 0.4, if now we delete the last $d - 1$ coordinates from each codeword, then the M vectors of length $n - d + 1$ so obtained must be distinct and so $M \leq q^{n-d+1}$. □

Definition 0.10. A set $\{A_1, A_2, \ldots, A_t\}$ of Latin squares of order q is called a set of mutually orthogonal Latin squares (MOLS) if each pair $\{A_i, A_j\}$ is a pair of MOLS, for $1 \leq i < j \leq t$.

Theorem 0.11. There are at most $q-1$ Latin squares in any set of MOLS of order q.

Proof. Let $A_1, A_2, \ldots, A_t$ be the set of MOLS of order q. If we relabel elements of each Latin square such that the first row of A_i is $1\ 2\ \cdots q$ (as relabelling conserves orthogonality). Now considering t entries appearing in the $(2,1)$th positions cannot be 1 as well as no two of them can be same, as for all i, the pair (i,i) has already occured in the first row.
Therefore, we must have $t \leq q-1$. $\square$

Definition 0.12. If a set of $q-1$ MOLS of order q exists, it is called a *complete* set of MOLS of order q.

Theorem 0.13. If q is prime-power, then there exists a complete set of $q-1$ MOLS of order q.

Proof. Similar to what we in Theorem 0.6, if we define $A_k = [a_{ij}^(k)], k \in \{1, 2, \ldots, q-1\}$, with

$$a_{ij}^{(k)} = \lambda_i + \lambda_k \lambda_j.$$

It follows exactly as in the proof of Theorem 0.6, that the set formed by the Latin squares A_k is a set of MOLS of order q. $\square$

Theorem 0.14. A q-ary $(n, q^2, n-1)$-code is equivalent to a set of $n-2$ MOLS of order q.

Proof. As in Theorem 0.5, code C of the form

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

has $d(C) = n-1$ if and only if $A_k = [a_{ij}^{(k)}]$, form a set of MOLS of order q, same outline as in proof of Theorem 0.5. $\square$

Corollary 0.14.1. If q is a prime power and $n \leq q+1$, then

$$A_q(n, n-1) = q^2$$

Proof. This is immediate from above theorems. $\square$