Non-Singular Submatrices of New Array & Triply Extended MDS Codes

B. S. Brar

Abstract

: Roth and Seroussi (1985) showed the construction over the field F = GF(q) of the arrays of the form S_q such that any submatrix of S_q is non-singular and constructed arrays are maximal in the sense that, when q is odd, no field element can be appended to any of the rows without creating singular submatrices. In this paper, new arrays of the form $S_q^{/}$ over the field F = GF(q) have been constructed such that every square submatrix is non-singular; that when q is odd, then a singular submatrix is generated; when q is even, and k = 3, then by appending v = a_1 or v = a_2 to row $S_q(3)$, we will never get a singular submatrix, further we will get two maximal 4 × (q - 2) rectangles and combining these two 4 × (q - 2) rectangles with identity matrix of order 4 × 4, we obtain generator matrices of order 4 × (q + 2) for triply extended (q + 2, 4, q - 1) MDS codes; and by appending v = a_1 or v = a_2 to row $S_q(q - 3)$, we will never get a singular submatrix , further we will get two maximal (q - 2) × 4 rectangles and combining these two (q - 2) × 4 rectangles with identity matrix of order (q - 2) × (q - 2), we obtain generator matrices of order (q - 2) × (q + 2) for triply extended (q + 2, q - 2, 5) MDS codes.

Keywords; Arrays, GC and GEC matrices, generator matrices, primitive element and characteristic of finite field, RS Codes, Triply Extended MDS Codes.

I. Introduction

A primitive element of a finite field F = GF(q) is a generator of the field's multiplicative group [Steven Roman (1995)]. The multiplicative group of a finite field is cyclic, and an element of the field is called a primitive element of that field if and only if it is a generator for the multiplicative group. So, every non-zero element of finite field F = GF(q) is power of a primitive element.

Roth and Seroussi (1985) considered the following triangular array over finite field F = GF(q):

$$S_q : \begin{array}{cccccccccc} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-2} & & \\ . & . & . & . & . & . & . & & & \\ . & . & . & . & . & . & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & & & \\ 1 & a_{q-2} & & & & & & & & \\ 1 & & & & & & & & & \end{array} \qquad (1)$$

`

----

[1]Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab (India) [e-mail: hodas.bfcet@yahoo.in].

where $a_i = \frac{1}{1-\gamma^i}$, 1 ≤ i ≤ (q - 2), for an arbitrary primitive element γ of field F = GF(q).

If the field F = GF(5), i.e. if q = 5, then because a primitive element of field F is a generator of the field as multiplicative group, so for this multiplicative group the binary operation will be "multiplicative modulo 5". Keeping this in view, we find that 3 is a primitive element of field F = GF(q). Now taking γ = 3 for field F = GF(5), (q = 5, so that 1 ≤ i ≤ (q - 2) implies 1 ≤ i ≤ 3), and using $a_i = \frac{1}{1-\gamma^i}$, 1 ≤ i ≤ 3,we shall obtain: a_1 = 2, a_2 = 3, a_3 = 4.

Therefore (1) becomes as:

$$S_5: \begin{array}{lllll} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & \\ 1 & 3 & 4 & & \\ 1 & 4 & & & \\ 1 & & & & \end{array} \qquad (2)$$

If the field F = GF(7), i.e. if q = 7, then because a primitive element of field F = GF(7) is a generator of the field as multiplicative group, so for this multiplicative group the binary operation will be "multiplicative modulo 7". Keeping this in view, we find that 3 is a primitive element of field F = GF(7). Now taking $\gamma = 3$ for field F = GF(7), (q = 7, so that 1 ≤ i ≤ (q - 2) implies 1 ≤ i ≤ 5), and using $a_i = \frac{1}{1-\gamma^i}$,1 ≤ i ≤ 5, we will obtain: $a_1 = 3$, $a_2 = 6$, $a_3 = 4$, $a_4 = 2$, $a_5 = 5$.

Therefore (1) becomes as:

$$S_7: \begin{array}{lllllll} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 6 & 4 & 2 & 5 & \\ 1 & 6 & 4 & 2 & 5 & & \\ 1 & 4 & 2 & 5 & & & \\ 1 & 2 & 5 & & & & \\ 1 & 5 & & & & & \end{array} \qquad (3)$$

Every square submatrices of S_q is non-singular. Such arrays [MacWilliams and Sloane (1977)] were first put forward by Singleton for q = 5 and q = 7 [R.C. Singleton (1964)]. But Singleton gave no generalisation for larger fields. Roth and Seroussi (1985) showed that such arrays are maximal, that is, if q is odd, no field element can be appended to any row, except to first row, without generating singular matrices; and it is true when q is even, except for one element, which can be appended to each of the 3rd and (q - 1)st rows. This leads to Triply Extended Reed- Solomon Codes.

II. Non-Singular Submatrices of New Array

Consider the finite field F = GF(q), and consider the array:

$$S_q^{/}: \begin{array}{lllllllll} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & \\ . & . & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & & \end{array} \qquad (4)$$

where $a_i = \frac{1}{1-\gamma^i}$, 1 ≤ i ≤ (q - 2), for an arbitrary primitive element γ of field F = GF(q).

So, if the field F = GF(11), i.e. if q = 11, then because a primitive element of field F = GF(11) is a generator of the field as multiplicative group, so for this multiplicative group the binary operation will be "multiplicative modulo 11". Keeping this in view, we find that 2 is a primitive element of field F = GF(11). Now taking $\gamma = 2$ for field F = GF(11), (q = 11, so that 1 ≤ i ≤ (q - 2) implies 1 ≤ i ≤ 9), and using $a_i = \frac{1}{1-\gamma^i}$, 1 ≤ i ≤ 9 , we will obtain: $a_1 = 2$, $a_2 = 7$, $a_3 = 3$, $a_4 = 8$, $a_5 = 6$, $a_6 = 4$, $a_7 = 9$, $a_8 = 5$, $a_9 = 2$.

Therefore triangular array (4) corresponding to field F = GF(11) becomes as:

$$S_{11}^{/}: \begin{array}{ccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 10 & 7 & 3 & 8 & 6 & 4 & 9 & 5 \\ 1 & 7 & 3 & 8 & 6 & 4 & 9 & 5 & 2 \\ 1 & 3 & 8 & 6 & 4 & 9 & 5 & 2 & \\ 1 & 8 & 6 & 4 & 9 & 5 & 2 & & \\ 1 & 6 & 4 & 9 & 5 & 2 & & & \\ 1 & 4 & 9 & 5 & 2 & & & & \\ 1 & 9 & 5 & 2 & & & & & \\ 1 & 5 & 2 & & & & & & \end{array} \qquad (5)$$

If the field is F = GF(13), i.e. if q = 13, then because a primitive element of field F = GF(13) is a generator of the field as multiplicative group, so for this multiplicative group the binary operation will be "multiplicative modulo 13". Keeping this in view, we find that 2 is a primitive element of field F = GF(13). Now taking γ = 2 for field F = GF(13), (q = 13, so that 1 ≤ i ≤ (q - 2) implies 1 ≤ i ≤ 11), and using $a_i = \frac{1}{1-\gamma^i}$, 1 ≤ i ≤ 11 , we will obtain: $a_1 = 12$, $a_2 = 4$, $a_3 = 11$, $a_4 = 6$, $a_5 = 5$, $a_6 = 7$, $a_7 = 9$, $a_8 = 8$, $a_9 = 3$, $a_{10} = 10$, $a_{11} = 2$.

Therefore (4) becomes as:

$$S_{13}^{/}: \begin{array}{ccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 12 & 4 & 11 & 6 & 5 & 7 & 9 & 8 & 3 & 10 \\ 1 & 4 & 11 & 6 & 5 & 7 & 9 & 8 & 3 & 10 & 2 \\ 1 & 11 & 6 & 5 & 7 & 9 & 8 & 3 & 10 & 2 & \\ 1 & 6 & 5 & 7 & 9 & 8 & 3 & 10 & 2 & & \\ 1 & 5 & 7 & 9 & 8 & 3 & 10 & 2 & & & \\ 1 & 7 & 9 & 8 & 3 & 10 & 2 & & & & \\ 1 & 9 & 8 & 3 & 10 & 2 & & & & & \\ 1 & 8 & 3 & 10 & 2 & & & & & & \\ 1 & 3 & 10 & 2 & & & & & & & \\ 1 & 10 & 2 & & & & & & & & \end{array} \qquad (6)$$

Theorem 1: Let F = GF(q) be the finite field. Consider the array (4). Then, every square submatrix of $S_q^{/}$ is non-singular.

Proof: Let $S_q^{/*}$ denote the array got from $S_q^{/}$ by deleting its first row.

Therefore, $S_q^{/*}$ will be as:

$$S_q^{/*}: \begin{array}{cccccccc} 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} \quad a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} \quad a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} \\ . & . & . & . & . & . & . & \\ . & . & . & . & . & . & & \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & \end{array} \qquad (7)$$

We take the first column of $S_q^{/*}$ as the zeroth column. Let S_{ij}, 1 ≤ i ≤ (q - 3), 1 ≤ j ≤ (q – i - 1), denote the entries of $S_q^{/*}$, except for the first row for which the value of j will be as 1 ≤ j ≤ (q – i - 2). Now for every row and 0th column of $S_q^{/*}$, each entry is equal to 1. Therefore:

$$S_{i0} = 1, \quad 1 \le i \le (q - 3). \qquad (8)$$

And for every row and other columns, each entry of $S_q^{/*}$ is given by:

$S_{ij} = a_{i+j-1}$, $1 \le i \le (q - 3), 1 \le j \le (q – i - 1)$. (9)

except for first row for which the value of S_{ij} will be:

$S_{ij} = a_{i+j-1}$, $1 \le i \le (q - 3), 1 \le j \le (q – i - 2)$. (10)

For example, consider the entry a_{q-3}, which is present in the 2nd row and (q - 4)th column. Hence, for it, i = 2, j = (q - 4). Therefore, $S_{ij} = a_{i+j-1}$ implies $S_{ij}= a_{2 + (q - 4) – 1} = a_{q - 3}$. Similarly, consider the entry $a_{q - 3}$ in first row, it lies in (q - 3)th column. So, i = 1, j = (q - 3). Therefore, $S_{ij} = a_{i + j – 1} = a_{1 + (q - 3) - 1} = a_{q - 3}$.

Now $a_i = \dfrac{1}{1-\gamma^i}$, $1 \le i \le (q - 3)$, (given) (11)

We discuss the case of all rows, except the first row of $S_q^{/*}$.

Now (10) and (11) implies:

$S_{ij}=\dfrac{1}{1-\gamma^{i+j-1}}$, $1 \le i \le (q - 3), 1 \le j \le (q – i - 1)$. (12)

Now $1 \le i \le (q - 3)$, $1 \le j \le (q – i - 1)$ implies $1 \le i$, $1 \le j$, $j \le (q – i - 1)$ i.e. $1 + 1 \le i + j$, $i + j \le q - 1$ i.e. $1 + 1 - 1 \le i + j - 1$, $i + j - 1 \le q – 1 - 1$ i.e. $1 \le i + j - 1$, $i + j - 1 \le q - 2$ i.e. $1 \le i + j - 1 \le q - 2$.

Therefore in the above ranges, in which S_{ij} is defined, always we have:

$1 \le i + j – 1 \le q - 2$ (13)

Hence $i + j - 1 \ne 0$. So $\gamma^{i+j-1} \ne 1$ for an arbitrary primitive element γ of field F = GF(q). Therefore S_{ij} given by (12) stands.

Now we consider vectors:

x = $(x_1, x_2, \ldots, x_{q-3})$; **y** = $(y_0, y_1, \ldots, y_{q-3})$

defined by: $x_i = - \gamma^{-(i-1)}$, $1 \le i \le (q - 3)$; $y_0 = 0$; $y_j = \gamma^j$, $1 \le j \le (q - 3)$

Therefore $\dfrac{x_i}{x_i+y_j} = \dfrac{-\gamma^{-(i-1)}}{-\gamma^{-(i-1)}+\gamma^j} = \dfrac{-\gamma^{-(i-1)}}{-\gamma^{-(i-1)}.[1-\gamma^{(i-1)+j}]} = \dfrac{1}{1-\gamma^{i+j-1}} = S_{ij}$ (using (12))

Therefore $S_{ij} = \dfrac{x_i}{x_i+y_j}$, $1 \le i \le (q - 3)$, $1 \le j \le (q – i - 1)$. (14)

Now for the first row,

$S_{ij} = a_{i+j-1} = \dfrac{1}{1-\gamma^{i+j-1}}$, $1 \le i \le (q - 3), 1 \le j \le (q – i - 2)$. (15)

Now $1 \le i \le (q - 3)$, $1 \le j \le (q – i - 2)$ implies $1 \le i$, $1 \le j$, $j \le (q – i - 2)$ i.e. $1 + 1 \le i + j$, $i + j \le q - 2$ i.e. $1 + 1 - 1 \le i + j - 1$, $i + j - 1 \le q – 2 - 1$ i.e. $1 \le i + j - 1$, $i + j - 1 \le q - 3$ i.e. $1 \le i + j - 1 \le q - 3$.

Therefore in the above ranges, in which S_{ij} is defined, always we have:

$1 \le i + j - 1 \le q - 3$ (16)

Hence $i + j - 1 \ne 0$. So $\gamma^{i+j-1} \ne 1$ for an arbitrary primitive element γ of field F = GF (q). Therefore S_{ij} given by (15) stands.

Now we consider vectors:

x = $(x_1, x_2, \ldots, x_{q-3})$, **y** = $(y_0, y_1, \ldots, y_{q-3})$

defined by: $x_i = - \gamma^{-(i-1)}$, $1 \le i \le (q - 3)$; $y_0 = 0$; $y_j = \gamma^j$, $1 \le j \le (q - 3)$.

Therefore $\dfrac{x_i}{x_i+y_j} = \dfrac{-\gamma^{-(i-1)}}{-\gamma^{-(i-1)}+\gamma^j} = \dfrac{-\gamma^{-(i-1)}}{-\gamma^{-(i-1)}.[1-\gamma^{(i-1)+j}]} = \dfrac{1}{1-\gamma^{i+j-1}} = S_{ij}$ (using (15))

Therefore $S_{ij} = \frac{x_i}{x_i + y_j}$, $1 \le i \le (q - 3)$, $1 \le j \le (q - i - 2)$. (17)

Hence (14) and (17) implies:

$$S_{ij} = \frac{x_i}{x_i + y_j},\ 1 \le i \le (q - 3),\ 1 \le j \le (q - i - 1);\ \text{OR},\ 1 \le i \le (q - 3),\ 1 \le j \le (q - i - 2) \quad (18)$$

Because all x_i's are different and non-zero, so all y_j's are different, and $x_i + y_j \ne 0$ for i, j in defined ranges. Therefore $S_{ij} = \frac{x_i}{x_i + y_j}$, $1 \le i \le (q - 3)$, $1 \le j \le (q - i - 1)$; OR, $1 \le i \le (q - 3)$, $1 \le j \le (q - i - 2)$ stands, and these represent all the entries of $S_q^{/*}$. Hence if we consider any square-submatrix of $S_q^{/*}$, then that will be nonsingular GC (Generalised Cauchy) matrix.

Now two possibilities can be there. One, every square-submatrix of $S_q^{/}$ may be a square-submatrix of $S_q^{/*}$, in which case it will be nonsingular (by above discussion); OR, may be a rectangular-submatrix of $S_q^{/*}$ having an appended first row of 1s, in which case, such square-submatrices, being GEC (Generalised Extended Cauchy) matrix, are also nonsingular. Therefore we conclude that every square-submatrix of $S_q^{/}$ is non-singular.

From this theorem, it follows that every sub-matrix A of $S_q^{/}$ is either a GC (Generalised Cauchy) or GEC (Generalised Extended Cauchy) matrix, hence non-singular. Therefore, we conclude that MDS code having a generator matrix [I | A] in systematic form, will be either a GRS (Generalised Reed Solomon) or a GDRS (Generalised Doubly-Extended Reed Solomon) code.

III. New Array and (q + 2, 4, q - 1) and (q + 2, q - 2, 5) Triply Extended MDS Codes

Lemma: [Roth and Seroussi (1985)]. (i) Let F = GF(q) be a finite field of the characteristic other than 2. Let a, b, c are distinct elements of F - {1} such that c ≠ 0, and

$$\frac{1}{1-a} + \frac{1}{1-b} = \frac{2}{1-c} \quad (19)$$

Then the matrix: $M = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1-\frac{a}{c}} & \frac{1}{1-\frac{b}{c}} & \frac{1}{1-\frac{1}{c}} \\ \frac{1}{1-a} & \frac{1}{1-b} & \frac{1}{1-c} \end{bmatrix}$ is singular over field.

(ii) Let F = GF(q) be a finite field of the characteristic 2. Let a and b be elements of F - {0, 1} such that

$$ab \ne 1. \quad (20)$$

Then the matrix:

$$N = \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1+ab} & \frac{1}{1+a^2} & \frac{1}{1+a} \\ \frac{1}{1+b} & \frac{1}{1+a} & \frac{1}{1+\frac{1}{b}} \end{bmatrix}$$ is singular over field F = GF(q). (21)

Theorem 2: Let F = GF(q) be the field. Consider the array (6). Let $S_q(0)$, $S_q(1)$, $S_q(2)$, ... , $S_q(q - 3)$ denote the rows of $S_q^{/}$. Then attempt to append an element of field F = GF(q) to first three rows $S_q(0)$, $S_q(1)$, $S_q(2)$ will result to get only 1×1 submatrix [v], and if v is a non-zero element of field, then this submatrix [v] is non-singular, and if v is zero element, then this submatrix [v] is singular. Further appending element v = 0 of field to any row $S_q(k)$, $3 \le k \le q - 3$, results in having a non-singular submatrix. Let $L = \{1\}U\{a_i : k \le i \le (q - 2)\}$. If v (≠ 0) belongs to L, we get a singular submatrix . If v (≠ 0) does not belong to L, and q is odd, then a singular submatrix is generated. If v (≠ 0) does not belong to L, q is even, and k = 3, then by appending $v = a_1$ or $v = a_2$ to row $S_q(3)$, we will never get a singular submatrix, further we will get two maximal 4 × (q - 2) rectangles and combining these two 4 × (q - 2) rectangles with identity matrix of order 4×4, we obtain generator matrices of order 4 × (q + 2) for triply extended (q + 2, 4, q - 1) MDS codes; and by appending $v = a_1$ or $v = a_2$ to row $S_q(q - 3)$, we will never get a singular submatrix, further we will get two maximal (q - 2) × 4 rectangles and combing these two (q - 2) × 4 rectangles with identity matrix of order (q - 2) × (q - 2), we obtain generator matrices of order (q - 2) × (q + 2) for triply extended (q + 2, q - 2, 5) MDS codes. If v (≠ 0) does not belong to L, q is even, $4 \le q \le q/2$, $q \ge 8$ then we will get a singular submatrix.

Proof: Consider v as an arbitrary element of field F = GF(q). It is clear from the form of array $S_q^{/}$ that if we try to append any arbitrary element of field F = GF(q) like v to first three rows $S_q(0)$, $S_q(1)$, $S_q(2)$ of the array $S_q^{/}$ (appending v to any of these first three rows is a similar thing, because all a_i's and 1 are the non-zero elements of the field, say to row $S_q(0)$, then $S_q^{/}$ will become as:

$$S_q^{/}: \begin{array}{cccccccccc} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 & v \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} & \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} & \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & & \\ . & . & . & . & . & . & & & & \\ . & . & . & . & . & . & & & & \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & & & \end{array}$$

Therefore, by utilising this v, we will be able to get only 1 × 1 submatrix [v], and if v is a non-zero element of field, then this submatrix [v] is non-singular, and if v is zero element, then this submatrix [v] is singular.

Now we discuss the situation when we append arbitrary element v of the field F = GF(q) to any one of the rows $S_q(3)$, $S_q(4)$, $S_q(5)$, ... , $S_q(q - 3)$ of array $S_q^{/}$. Generally speaking it means that we append arbitrary element v of the field F = GF(q) to any row $S_q(k)$, $3 \le k \le q - 3$.

If v = 0, then because all a_i's and 1 are distinct and some non-zero elements of the field, then only a trivial 1 × 1 singular submatrix $[v]_{1\times1} = [0]_{1\times1}$ will be formed. It is because the array $S_q^{/}$ will become as (appending v = 0 to 4^{th} row i.e. $S_q(3)$ row (say)):

$$S_q^{/}: \begin{array}{lllllllll}
1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\
1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\
1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\
1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & v = 0 \\
. & . & . & . & . & . & & & \\
. & . & . & . & . & . & & & \\
1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & \\
1 & a_{q-3} & a_{q-2} & & & & & &
\end{array}$$

Or, in general array $S_q^{/}$ will be (by appending v to row $S_q^{/}(k)$, $3 \le k \le q - 3$):

$$S_q^{/}: \begin{array}{lllllllll}
1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\
1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\
1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\
1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & \\
. & . & . & . & . & . & & & \\
. & . & . & . & . & . & & & \\
1 & a_k & a_{k+1} & a_{k+2} & . & v = 0 & & & \\
. & . & . & . & . & & & & \\
1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & \\
1 & a_{q-3} & a_{q-2} & & & & & &
\end{array}$$

Now let $v \ne 0$. Because there is symmetry between rows and columns of $S_q^{/}$, therefore without any loss of generality, we take $k \le (q - 3) / 2$ when q is odd, and $k \le q / 2$ when q is even. Let $L = \{1\} \cup \{a_i : k \le i \le (q - 2)\}$. So clearly L consists of all the elements of row $S_q(k)$.

If v belongs to L, i.e. v can be any one of $a_3, a_4, a_5, \ . \ . \ . \ , a_{q-3}$, and 1, say $v = a_k$ or 1, then array $S_q^{/}$ will become as:

$$S_q^{/}: \begin{array}{lllllllll}
1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\
1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\
1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\
1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & \\
. & . & . & . & . & . & & & \\
. & . & . & . & . & . & & & \\
1 & a_k & a_{k+1} & a_{k+2} & . & v\ (= a_k \text{ or } 1) & & & \\
. & . & . & . & . & & & & \\
1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & \\
1 & a_{q-3} & a_{q-2} & & & & & &
\end{array}$$

Therefore, we shall get a submatrix of the form $\begin{bmatrix} 1 & 1 \\ a_k & a_k \end{bmatrix}$ or $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, which is clearly singular.

Now let v does not belong to L. Because $1, a_1, a_2, \ . \ . \ . \ , a_{q-2}$ exhaust all non-zero elements of the field, therefore $v = a_r$, $1 \le r < k$ (i.e. v can be of any of a_1 and a_2).

Now q can be odd or even.

Case 1 (When q is odd):

We consider all the unordered pairs $\{b_1, b_2\}$ of distinct elements of field F such that $b_1 + b_2 = 2v = 2a_r$ (because $v = a_r$). Now cardinality of $L = 1 + \{(q - 2) - k + 1\} = q - k$. Because the case of q being odd is being discussed, where it has been assumed that $k \le (q - 3) / 2$ i.e $-k \ge -(q - 3) / 2$ i.e. $q - k \ge q - (q - 3) / 2$ i.e. $q - k \ge (2q - q + 3) / 2$ i.e. $q - k \ge (q + 3) / 2$. Therefore cardinality of $L = q - k \ge (q + 3) /$

2. So, at least one such pair of the type $\{b_1, b_2\}$ such that $b_1 + b_2 = 2v = 2a_r$, can be found out among elements of L.

Such a pair is either of the form $\{1, a_j\}$, $k \le j \le (q - 2)$ or is of the form $\{a_i, a_j\}$, $k \le i < j \le (q - 2)$.

When this pair is of the form $\{1, a_j\}$, $k \le j \le (q - 2)$, then $1 + a_j = 2v = 2a_r$. Now condition of Lemma is $\frac{1}{1-a}+\frac{1}{1-b}=\frac{2}{1-c}$, where a, b, c are distinct elements of field F - {1}. Take a = 0, b = γ^j, c = γ^r. Putting these in the above condition of Lemma, we obtain:

$$\frac{1}{1-0}+\frac{1}{1-\gamma^j}=\frac{2}{1-\gamma^r} \quad \text{i.e.} \quad 1/1 + a_j = 2(a_r)$$

[because $a_i = \frac{1}{1-\gamma^i}$, $1 \le i \le (q - 2)$, so for an arbitrary primitive element γ of the field F = GF(q), j satisfies $k \le j \le (q - 2)$, r satisfies $1 < r < k$]. So, we have $1 + a_j = 2a_r$, which is true. Therefore condition of Lemma is satisfied. Hence by Lemma, the matrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1-\frac{a}{c}} & \frac{1}{1-\frac{b}{c}} & \frac{1}{1-\frac{1}{c}} \\ \frac{1}{1-a} & \frac{1}{1-b} & \frac{1}{1-c} \end{bmatrix} \text{ is singular over field F.}$$

$$\text{i.e. } \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1-\frac{0}{\gamma^r}} & \frac{1}{1-\frac{\gamma^j}{\gamma^r}} & \frac{1}{1-\frac{1}{\gamma^r}} \\ \frac{1}{1-0} & \frac{1}{1-\gamma^j} & \frac{1}{1-\gamma^r} \end{bmatrix} \text{ is singular over field F.}$$

$$\text{i.e. } \begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{1}{1-\gamma^{j-r}} & \frac{1}{1-\gamma^{-r}} \\ 1 & \frac{1}{1-\gamma^j} & \frac{1}{1-\gamma^r} \end{bmatrix} \text{ is singular over field F.}$$

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{1}{1-\gamma^{j-r}} & \frac{1}{1-(1)\gamma^{-r}} \\ 1 & \frac{1}{1-\gamma^{j}} & \frac{1}{1-\gamma^{r}} \end{bmatrix}$ is singular over field F.

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{1}{1-\gamma^{j-r}} & \frac{1}{1-(\gamma^{q-1})\gamma^{-r}} \\ 1 & \frac{1}{1-\gamma^{j}} & \frac{1}{1-\gamma^{r}} \end{bmatrix}$ is singular over field F.

[because F = GF(q) is cyclic multiplicative group, therefore if its primitive element (generator) is γ, then γ^{q-1} = e (multiplicative identity element of field F = GF(q)) is 1 (Vasishtha and Vasishtha (2006))].

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & \frac{1}{1-\gamma^{j-r}} & \frac{1}{1-\gamma^{q-1-r}} \\ 1 & \frac{1}{1-\gamma^{j}} & \frac{1}{1-\gamma^{r}} \end{bmatrix}$ is singular over field F.

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & a_{j-r} & a_{q-1-r} \\ 1 & a_j & a_r(=v) \end{bmatrix}$ is singular over field F.

[because $a_i = \frac{1}{1-\gamma^i}$, $1 \le i \le (q - 2)$]

When the pair is of the form $\{a_i, a_j\}$, $k \le i < j \le (q - 2)$, then $a_i + a_j = 2v = a_r$. We take $a = \gamma^i$, $b = \gamma^j$, $c = \gamma^r$. Putting these in the condition of Lemma, we obtain:

$\frac{1}{1-a}+\frac{1}{1-b}=\frac{2}{1-c}$, which implies $\frac{1}{1-\gamma^i}+\frac{1}{1-\gamma^j}=\frac{2}{1-\gamma^r}$ i.e. $a_i + a_j = 2a_r$

[because $a_i = \frac{1}{1-\gamma^i}$, $1 \le i \le (q - 2)$, for an arbitrary primitive element γ of the field F = GF(q), j satisfies $k \le j \le (q - 2)$, r satisfies $1 < r < k$]. So, we have $1 + a_j = 2a_r$, which is true. Therefore condition of Lemma is satisfied. Hence by Lemma, the matrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-\dfrac{a}{c}} & \dfrac{1}{1-\dfrac{b}{c}} & \dfrac{1}{1-\dfrac{1}{c}} \\ \dfrac{1}{1-a} & \dfrac{1}{1-b} & \dfrac{1}{1-c} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-\dfrac{\gamma^i}{\gamma^r}} & \dfrac{1}{1-\dfrac{\gamma^j}{\gamma^r}} & \dfrac{1}{1-\dfrac{1}{\gamma^r}} \\ \dfrac{1}{1-\gamma^i} & \dfrac{1}{1-\gamma^j} & \dfrac{1}{1-\gamma^r} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-\gamma^{i-r}} & \dfrac{1}{1-\gamma^{j-r}} & \dfrac{1}{1-\gamma^{-r}} \\ \dfrac{1}{1-\gamma^i} & \dfrac{1}{1-\gamma^j} & \dfrac{1}{1-\gamma^r} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-\gamma^{i-r}} & \dfrac{1}{1-\gamma^{j-r}} & \dfrac{1}{1-(1)\gamma^{-r}} \\ \dfrac{1}{1-\gamma^i} & \dfrac{1}{1-\gamma^j} & \dfrac{1}{1-\gamma^r} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-\gamma^{i-r}} & \dfrac{1}{1-\gamma^{j-r}} & \dfrac{1}{1-(\gamma^{q-1})\gamma^{-r}} \\ \dfrac{1}{1-\gamma^i} & \dfrac{1}{1-\gamma^j} & \dfrac{1}{1-\gamma^r} \end{bmatrix}$$ is singular over field F.

[because F = GF(q) is cyclic multiplicative group, therefore if its primitive element(generator) is γ, then γ^{q-1} = e (multiplicative identity element of field F = GF(q)) is 1].

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1-\gamma^{i-r}} & \frac{1}{1-\gamma^{j-r}} & \frac{1}{1-\gamma^{q-1-r}} \\ \frac{1}{1-\gamma^{i}} & \frac{1}{1-\gamma^{j}} & \frac{1}{1-\gamma^{r}} \end{bmatrix}$ is singular over field F.

i.e. $\begin{bmatrix} 1 & 1 & 1 \\ a_{i-r} & a_{j-r} & a_{q-1-r} \\ a_i & a_j & a_r(=v) \end{bmatrix}$ is singular over field F.

[because $a_i = \frac{1}{1-\gamma^i}$, $1 \le i \le (q - 2)$, $v = a_r$, $1 < r < k$]

Case 2 (When q is even):

When k = 3: Then L = {1}U{a_i : k ≤ i ≤ (q - 2)} = {1}U{a_i : 3 ≤ i ≤ (q - 2)}

= 1, a_3 , a_4 , . . . , a_{q-1}

Therefore, L contains all the non-zero elements of the field F = GF(q), except a_1, a_2. So, the only non-zero elements of the field F, which are left outside L are a_1, a_2.

Now if we append $v = a_1$ or $v = a_2$ to row $S_q(3)$, we will get:

$$S_q^{/}: \begin{matrix} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & a_1 \text{ or } a_2 (= v) \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} \\ 1 & a_{q-3} & a_{q-2} \end{matrix}$$

Therefore, if we append $v = a_1$ or $v = a_2$ to row $S_q(3)$, we will never get a singular submatrix.

Further we see that by appending $v = a_1$ or $v = a_2$ to row $S_q(3)$, we will get two maximal 4 × (q - 2) rectangles:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & a_1(=v) \end{bmatrix}_{4\times(q-2)} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & a_2(=v) \end{bmatrix}_{4\times(q-2)}.$$

Combining these two 4 × (q - 2) rectangles with this I_4 (identity matrix of order 4 × 4), we obtain:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} & 0 & 1 & 0 & 0 \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} & 0 & 0 & 1 & 0 \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & a_1(=v) & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times(q+2)}$$

[Here k × n = 4 × (q + 2). Therefore k = 4 and n = q + 2, so d = n – k + 1 = (q + 2) – 4 + 1 = q – 1].
and

$$\begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} & 0 & 1 & 0 & 0 \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} & 0 & 0 & 1 & 0 \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & a_2(=v) & 0 & 0 & 0 & 1 \end{bmatrix}_{4\times(q+2)}$$

[Here k × n = 4 × (q + 2). Therefore k = 4 and n = q + 2, so d = n – k + 1 = (q + 2) – 4 + 1 = q – 1].

These two rectangles form generator matrices for triply extended (q + 2, 4, q - 1) MDS codes.

If we append v = a_1 or v = a_2 to row S_q(q - 3), we get:

$$S_q^{/}: \begin{array}{ccccccccc} 1 & 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & . & a_{q-4} & a_{q-3} \\ 1 & a_2 & a_3 & a_4 & . & . & . & a_{q-3} & a_{q-2} \\ 1 & a_3 & a_4 & a_5 & . & . & . & a_{q-2} & \\ . & . & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & & & & & \\ 1 & a_{q-3} & a_{q-2} & a_1 \text{ or } a_2\,(=v) & & & & & \end{array}$$

Therefore, appending v = a_1 or v = a_2 to row S_q(3), we will get two maximal (q - 2) × 4 rectangles:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 \\ 1 & a_2 & a_3 & a_4 \\ 1 & a_3 & a_4 & a_5 \\ . & . & . & . \\ . & . & . & . \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} \\ 1 & a_{q-3} & a_{q-2} & a_1 \end{bmatrix}_{(q-2)\times 4} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 \\ 1 & a_2 & a_3 & a_4 \\ 1 & a_3 & a_4 & a_5 \\ . & . & . & . \\ . & . & . & . \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} \\ 1 & a_{q-3} & a_{q-2} & a_2 \end{bmatrix}_{(q-2)\times 4}.$$

Combining these two 4 × (q - 2) rectangles with this I_{q-2} (identity matrix of order (q – 2) × (q - 2)), we obtain:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & . & . & . & 0 \\ 1 & a_1 & a_2 & a_3 & 0 & 1 & 0 & . & . & . & 0 \\ 1 & a_2 & a_3 & a_4 & 0 & 0 & 1 & . & . & . & 0 \\ 1 & a_3 & a_4 & a_5 & 0 & 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & a_{q-3} & a_{q-2} & a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(q-2)\times(q+2)},$$

[Here k × n = (q - 2) × (q + 2). Therefore k = q - 2 and n = q + 2, so d = n – k + 1 = (q + 2) – (q - 2) + 1 = 5].

and

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & . & . & . & 0 \\ 1 & a_1 & a_2 & a_3 & 0 & 1 & 0 & . & . & . & 0 \\ 1 & a_2 & a_3 & a_4 & 0 & 0 & 1 & . & . & . & 0 \\ 1 & a_3 & a_4 & a_5 & 0 & 0 & 0 & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . \\ 1 & a_{q-4} & a_{q-3} & a_{q-2} & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & a_{q-3} & a_{q-2} & a_2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{(q-2)\times(q+2)},$$

[Here k × n = (q - 2) × (q + 2). Therefore k = q - 2 and n = q + 2, so d = n – k + 1 = (q + 2) – (q - 2) + 1 = 5].

These two rectangles form generator matrices for triply extended (q + 2, q - 2, 5) MDS codes.

When 4 ≤ k ≤ q / 2, q ≥ 8: Let v = a_r, 1 ≤ r < k. Let 1 ≤ s < k and s ≠ r. It should be noted that because 4 ≤ k ≤ q / 2, so k > 3, and 1 ≤ s < k, so such s exists. Now taking a = γ^{-s}, a = γ^{-r}, and utilising Lemma (part 2), where field F = GF(q) is of characteristic 2, we see that:

$$\begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1+ab} & \frac{1}{1+a^2} & \frac{1}{1+a} \\ \frac{1}{1+b} & \frac{1}{1+a} & \frac{1}{1+\frac{1}{b}} \end{bmatrix}$$ is singular over field F.

[Note that because 1 ≤ r < k, 1 ≤ s < k, so 1 + 1 ≤ r + s < k + k, i.e. 2 ≤ (r + s) < 2k, i.e. 2 ≤ (r + s) < 2.q/2 (because 4 ≤ k ≤ q/2), i.e. 2 ≤ (r + s) < q, i.e, (r + s ≠ 0, and hence consequently ab = $\gamma^{-s}.\gamma^{-r}$ =

γ^{-s-r} = $\gamma^{-(s+r)}$ ≠ 1. Therefore, 1 + ab ≠ 1 + 1 ≠ 2(1) ≠ 0 (because 2 is characteristic of field F = GF(q), so 2(a) = a + a = 0 for every a belonging to F = GF(q), hence 2(1) = 1 + 1 = 0, 1 belongs to F = GF(q)).

Therefore, $\dfrac{1}{1+ab}$ stands].

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1+\gamma^{-s}.\gamma^{-r}} & \dfrac{1}{1+(\gamma^{-s})^{2}} & \dfrac{1}{1+\gamma^{-s}} \\ \dfrac{1}{1+\gamma^{-r}} & \dfrac{1}{1+\gamma^{-s}} & \dfrac{1}{1+\dfrac{1}{\gamma^{-r}}} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-(-1).\gamma^{-s}.\gamma^{-r}} & \dfrac{1}{1-(-1).\gamma^{-2s}} & \dfrac{1}{1-(-1).\gamma^{-s}} \\ \dfrac{1}{1-(-1).\gamma^{-r}} & \dfrac{1}{1-(-1).\gamma^{-s}} & \dfrac{1}{1-(-1).\gamma^{r}} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-(1).\gamma^{-s}.\gamma^{-r}} & \dfrac{1}{1-(1).\gamma^{-2s}} & \dfrac{1}{1-(1).\gamma^{-s}} \\ \dfrac{1}{1-(1).\gamma^{-r}} & \dfrac{1}{1-(1).\gamma^{-s}} & \dfrac{1}{1-(1).\gamma^{r}} \end{bmatrix}$$ is singular over field F.

[Because characteristic of field F = GF(q) is smallest positive integar n such that n a = a + a + a + . . . upto n terms = 0 (zero element of field F for every a belonging to F, and because here characteristic of field F = GF(q) is 2, therefore, 2 a = a + a =0 implies a + a = 0, i.e. a = - a. Since 1 belongs to F = GF(q), so 1 = -1 (additive inverse of 1). Also because 1 belongs to F, so -1 belongs to F].

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-(\gamma^{q-1}).\gamma^{-s-r}} & \dfrac{1}{1-(\gamma^{q-1}).\gamma^{-2s}} & \dfrac{1}{1-(\gamma^{q-1}).\gamma^{-s}} \\ \dfrac{1}{1-(\gamma^{q-1}).\gamma^{-r}} & \dfrac{1}{1-(\gamma^{q-1}).\gamma^{-s}} & \dfrac{1}{1-\gamma^{r}} \end{bmatrix}$$ is singular over field F.

[because F = GF(q) is cyclic multiplicative group, so if its generator (primitive element) is γ, then γ^{q-1} = e = 1 (multiplicative identity of field F].

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{1-\gamma^{q-1-s-r}} & \frac{1}{1-\gamma^{q-1-2s}} & \frac{1}{1-\gamma^{q-1-s}} \\ \frac{1}{1-\gamma^{q-1-r}} & \frac{1}{1-\gamma^{q-1-s}} & \frac{1}{1-\gamma^{r}} \end{bmatrix}$$ is singular over field F.

i.e. $$\begin{bmatrix} 1 & 1 & 1 \\ a_{q-1-r-s} & a_{q-1-2s} & a_{q-1-s} \\ a_{q-1-r} & a_{q-1-s} & a_{r} \end{bmatrix}$$ is singular over field F.

[because $a_i = \frac{1}{1-\gamma^{i}}$, $v = a_r$, $1 \le r < k$].

IV. Conclusion

Roth and Seroussi have considered the array S_q over the finite field F = GF(q), and they constructed triply extended (q + 2, 3, q) and (q + 2, q - 1, 4) MDS codes. We have considered New Array $S_q^{/}$ over the finite field F = GF(q), and constructed triply extended (q + 2, 4, q - 1) MDS codes and triply extended (q + 2, q - 2, 5) MDS codes. So, corresponding to triply extended (q + 2, 3, q) MDS code, we have constructed triply extended (q + 2, 4, q - 1) MDS codes. Although block-length of the code does not increase, but we are successful in increasing number of message-symbols, which means that our code will transmit more number of message-symbols, and number of codewords within the code increases thereby enhancing the utility of the code. And corresponding to triply extended (q + 2, q - 1, 4) MDS codes, we have constructed triply extended (q + 2, q - 2, 5) MDS codes. Although block-length of the code does not increase, and number of message-symbols do not increase, but we are successful in increasing minimum distance of the code as a result of which error-correcting-capability of the code is enhanced.

References

1. **MacWilliams, F.J. and Sloane, N.J.A. (1977):** "The Theory of Error-Correcting Codes". Amsterdam: North Holland, 1977.

2. **Roman, Steven (1995):**"Field Theory", New York; Splinger Verlag, ISBN 0-387-94408-7

3. **Roth, Ron M. and Seroussi, Gadiel (1985)**: "On Generator Matrices of MDS Codes, IEEE Transactions on Information Theory, Vol. IT-31, No.6, November, 1985.

4. **Singleton, R.C. (1964):** "Maximum distance q-ary codes", IEEE Trans. Inform.Theory, Vol. IT-10, pp.116-118, 1964.

5. **Vasishtha, A.R., and Vasishtha, A.K., (2006),** *Modern Algebra*, Krishna Prakashan Media (P) Ltd. Meerut, 51st edition.