Error location technique in RT-spaces*

Sapna Jain
Department of Mathematics
University of Delhi
Delhi 110 007
India
E-mail: sapnajain@gmx.com

Abstract. The paper considers two-dimensional linear codes with sub-block structure in RT-spaces [2-5,7] whose error location techniques are described in terms of various sub-blocks. Upper and lower-bounds are given for the number of check digits required with any error locating code in RT-spaces.

AMS Subject Classification (2000): 94B65, 95B05

Keywords: RT-metric, linear codes, error location

1. Introduction

Wolf and Elspass [9] introduced the concept of error location for codes in Hamming spaces and devised codes that could locate a single corrupted sub-block containing a given number of random errors. Rosenbloom and Tsfassman [7] initiated the concept of RT-metric (or m-metric) array codes which are subset/subspaces of the linear space of all m by s matrices $Mat_{m\times s}(\mathbf{F}_q)$ with entries from a finite field $\mathbf{F}_q$ endowed with a non-Hamming metric known as RT-metric (or m-metric). Also, we know that RT-metric (also known as ρ-metric) is stronger than Hamming metric ([1, 8]). Motivated by the idea to have error location technique in codes equipped with the RT-metric, we formulate the concept of error locating codes in RT-spaces and obtain lower and upper bounds on the parameters of RT-metric array codes for the location of corrupted sub-block.

Here is a model of an information transmission for which error location technique in RT-metric array coding is useful. Suppose that a sender transmits messages each being an s-tuple of m-tuples of q-ary symbols, transmitted over m parallel channels. Here the codeword is of length $n = ms$ con-

*This research is supported by National Board for Higher Mathematics (NBHM), Department of Atomic Energy, Government of India, under a Research Project vide ref. no. NBHM/RP.3/2007.

sisting of m sub-blocks of length "s" each. There is an interfering noise in a channel which creates errors with in a particular sub-block corresponding to that channel. In ordinary decision feedback systems using error detection technique, the receiver tests each block of received digits of length $n = ms$ for the presence of errors. If errors are detected, the receiver requests the retransmission of the entire corrupted block of ms digits and this process is repeated for each incoming block and thereby resulting in a low data rate transmission. This is more so when channel noise is such as to produce a fairly uniform density of errors in each received block confined to a particular sub-block. The use of error locating codes can soften this problem by identifying the corrupted sub-block with in a block and instead of requesting for retransmission of the entire block of ms digits, now the receiver requests for the retransmission of only corrupted "s" digits thereby increasing the rate of transmission and making the transmission more economical. By a corrupted sub-block we shall always mean a sub-block containing errors of RT-weight e or less $(1 \leq e \leq s)$.

2. Definitions and notations

Let $\mathbf{F}_q$ be a finite field of q elements. Let $Mat_{m\times s}(\mathbf{F}_q)$ denote the linear space of all $m \times s$ matrices with entries from $\mathbf{F}_q$. An RT-metric array code is a subset of $Mat_{m\times s}(\mathbf{F}_q)$ and a linear RT-metric array code is an $\mathbf{F}_q$ linear subspace of $Mat_{m\times s}(\mathbf{F}_q)$. We identify the space $Mat_{m\times s}(\mathbf{F}_q)$ with the space F_q^{ms} by writing every matrix in $Mat_{m\times s}(\mathbf{F}_q)$ as an ms-tuple by writing the first row of the matrix followed by second row and so on. Similarly, every vector in F_q^{ms} can be represented as an m by s matrix in $Mat_{m\times s}(\mathbf{F}_q)$ by separating the co-ordinates of the vector into m groups of s-coordinates. The ms-tuple is called a block and each group of s-elements starting from the first element in an ms-tuple is called a sub-block. Thus there are m sub-blocks each of length "s" in a block. Also, columns of the generator matrix G and parity check matrix H of a linear RT-metric array code V are grouped into m sub-blocks of s columns each. Therefore, the generator matrix G and the parity check matrix H of a linear RT-metric array code V are represented as $G = [G_1, G_2, \cdots, G_m], H = [H_1, H_2, \cdots, H_m]$ where G_i and H_i are the i^{th} sub-block $(1 \leq i \leq m)$ of the generator and parity check matrix respectively of the code V and are given by

$$G_i = [G_{i1}, G_{i2}, \cdots, G_{is}],$$

and

$$H_i = [H_{i1}, H_{i2}, \cdots, H_{is}],$$

where each $G_{ij} (1 \leq i \leq m, 1 \leq j \leq s)$ is a $k \times 1$ column vector and each $H_{ij} (1 \leq i \leq m, 1 \leq j \leq s)$ is an $(ms - k) \times 1$ column vector.

The weight and metric defined by Rosenbloom and Tsfassman [7] on the space $Mat_{m\times s}(\mathbf{F}_q)$ are as follows :

Let $X \in Mat_{1\times s}(\mathbf{F}_q)$ with

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_m \end{pmatrix},$$

then column weight (or weight) of X is given by

$$wt_c(X) = \begin{cases} m - \ \max\ \{\ i \mid x_k = 0 \quad \text{for any } k \le i\} & \text{if } X \neq 0 \\ 0 & \text{if } \ X = 0. \end{cases}$$

This definition of wt_c can be extended to $m \times s$ matrices in the space $Mat_{m\times s}(\mathbf{F}_q)$ as

$$wt_c(A) = \sum_{j=1}^{s} wt_c(A_j)$$

where $A = [A_1, A_2, \cdots, A_s] \in Mat_{m\times s}(\mathbf{F}_q)$ and A_j denotes the j^{th} column of A. Then wt_c satisfies $0 \le wt_c(A) \le n(= ms)$ and determines a metric on $Mat_{m\times s}(\mathbf{F}_q)$ if we set $d(A, A') = wt_c(A - A')\ \forall\ A, A' \in Mat_{m\times s}(\mathbf{F}_q)$. We call this metric as column-metric. Note that for $m = 1$, it is just the usual Hamming metric.

There is an alternative equivalent way of defining the weight of an $m \times s$ matrix using the weight of its rows.

Let $Y \in Mat_{1\times s}(\mathbf{F}_q)$ with $Y = (y_1, y_2, \cdots, y_s)$. Define row weight (or weight) of Y as

$$wt_\rho(Y) = \begin{cases} \max\ \{\ i \mid y_i \neq 0\} & \text{if } Y \neq 0 \\ 0 & \text{if } \ Y = 0. \end{cases}$$

Extending the definitions of wt_ρ to the class of $m \times s$ matrices as

$$wt_\rho(A) = \sum_{i=1}^{m} wt_\rho(R_i)$$

where $A = \begin{bmatrix} R_1 \\ R_2 \\ \cdots \\ R_m \end{bmatrix} \in Mat_{m\times s}(\mathbf{F}_q)$ and R_i denotes the i^{th} row of A. Then wt_ρ satisfies $0 \le wt_\rho(A) \le n(= ms)\ \forall\ A \in Mat_{m\times s}(\mathbf{F}_q)$ and determines a metric on $Mat_{m\times s}(\mathbf{F}_q)$ known as row-metric.

It turns out that row weight of a vector is equal to the column weight of transpose of the vector with its component reversed and hence the two metrics viz. row-metric and column-metric give rise to equivalent codes and both the metrics have been known as m-metric or RT-metric.

In this paper, we take distance and weight in the sense of row-metric.

3. Bounds on the number of check digits

An error locating code (EL code) capable of detecting and locating a single sub-block containing errors of RT-weight e or less $(1 \leq e \leq s)$ must satisfy the following conditions:

(i) The syndrome resulting from the occurence of errors of RT-weight e or less within any one sub-block must be distinct from all-zeros syndrome.

(ii) The syndrome resulting from the occurence of errors of RT-weight e or less with in a single sub-block must be distinct from the syndrome resulting from any combination of errors of RT-weight e or less with in any other sub-block.

We note here that since it is not desired to distinguish between (detectable) error combinations occuring within the same sub-block, it is therefore not necessary that their corresponding syndromes be distinct. In fact, in the interests of coding efficiency such syndromes should be identical whenever possible.

In the following, we shall derive two results. The first result gives a lower bound on the number of check digits required for the existence of an RT-metric array code over $GF(q)$ capable of detecting and locating a single sub-block containing errors of RT-weight e or less $(1 \leq e \leq s)$. In the second result, we derive an upper bound on the number of check digits which assures the existence of such a code.

Theorem 3.1. *The number of parity check digits required for an $(m \times s, k)$ linear RT-metric array code that locates a single corrupted sub-block containing errors of RT-weight e or less $(1 \leq e \leq s)$ is bounded from below by*

$$ms - k \geq log_q\left\{1 + m\sum_{i=1}^{e} q^{(i-1)}(q-1)\right\} \tag{1}$$

Proof. The maximum number of distinct syndromes available using $(ms - k)$ parity check digits over $GF(q)$ is q^{ms-k}. The proof proceeds by first counting the number of syndromes that are required to be distinct by conditions (i) and (ii) and then setting this number less than or equal to q^{ms-k}. Any syndrome produced by errors of RT-weight e or less ($1 \leq e \leq s$) in a given sub-block must be distinct from any such syndrome likewise resulting from another set of errors of RT- weight e or less in the same sub-block, or else there would exist a combination of errors of RT-weight e or less in that sub-block resulting in the zero syndrome contradicting condition (i).

Moreover, syndromes produced by combinations of errors of RT-weight e or less in different sub-blocks must be distinct by condition (ii). Thus, the syndromes of errors of RT-weight e or less ($1 \leq e \leq s$) occuring whether in the same or in different sub-blocks must be distinct. Since there are $\sum_{i=1}^{e} q^{(i-1)}(q-1)$ possible errors of RT-weight e or less in any sub-block and there are m sub-blocks in all, therefore there must be $1+m\sum_{i=1}^{e} q^{(i-1)}(q-1)$ distinct syndromes, counting the all zero syndrome. Thus, we must have

$$q^{ms-k} \geq 1+m\sum_{i=1}^{e} q^{(i-1)}(q-1)$$

or

$$ms-k \geq log_q\left\{1+m\sum_{i=1}^{e} q^{(i-1)}(q-1)\right\}.$$

□

An EL code meeting the bound in (1) is called an optimum EL code. An upper bound on the number of parity check digits for error location is given below:

Theorem 3.2. *An $[m \times s, k]$ linear RT-metric array code capable of detecting errors of RT-weight e or less ($1 \leq e \leq s$) occuring within a single sub-block and of locating that sub-block can always be constructed using $(ms-k)$ parity checks satisfying the inequality*

$$ms-k \geq log_q\left(1+q^{(e-1)}+q^{(e-1)}(m-1)\left(\sum_{i=1}^{e} q^{(i-1)}(q-1)\right)\right) \qquad (2)$$

Proof. The existence of such a code will be proved by constructing a suitable $(ms-k) \times ms$ parity check matrix for the desired code. To locate any corrupted sub-block containing errors of RT-weight e or less, it is necessary and sufficient that any (nonzero) linear combination involving e (or fewer) consecutive columns amongst the first e columns in each sub-block should be nonzero and distinct. Supoose that we have been chosen the first $(m-1)$ sub-blocks of H viz. $H_1, H_2, \cdots, H_{m-1}$ suitably. We now choose m^{th} sub-block H_m as follows:

The j^{th} column viz. $H_{mj}(1 \leq j \leq e)$ in the m^{th} sub-block H_m can be added to H provided

(a) H_{mj} is not a linear combination of previously chosen columns i.e.

$$H_{mj} \neq \alpha_{m,i_1} H_{m,i_1} + \alpha_{m,i_2} H_{m,i_2} + \cdots, \alpha_{m,i_r} H_{m,i_r}$$
$$\text{where} \quad \{i_1, i_2, \cdots, i_r\} \subseteq \{1, 2, \cdots, j-1\},$$

and

(b) $H_{mj}(1 \leq j \leq e)$ is not a linear combination combination of previously chosen $j-1$ columns of the m^{th} sub-block H_m together with a linear combination of first e or fewer consecutive columns from amongst any one of the remaining $(m-1)$ sub-blocks viz. $H_1, H_2, \cdots, H_{m-1}$.

Condition (a) gives rise to q^{j-1} linear combinations whereas the number of linear combination arising out of condition (b) equals

$$q^{(j-1)}(m-1)\left(\sum_{i=1}^{e} q^{(i-1)}(q-1).\right.$$

Thus, the total number of linear combinations arising out of conditions (a) and (b) are given by

$$q^{(j-1)} + q^{(j-1)}(m-1)\left(\sum_{i=1}^{e} q^{(i-1)}(q-1)\right).$$

At worst all these linear combinations might yield a distinct sum. Thus, the column $H_{mj}(1 \leq j \leq e)$ can be added to the m^{th} sub-block H_m provided that all the $(ms-k)$-tuples are not exhausted by theses linear combinations i.e. for $j = e$, the e^{th} column H_{me} can be added to the m^{th} sub-block if

$$q^{ms-k} > q^{(e-1)} + q^{(e-1)}(m-1)\left(\sum_{i=1}^{e} q^{(i-1)}(q-1)\right).$$

or

$$q^{ms-k} \geq 1 + q^{(e-1)} + q^{(e-1)}(m-1)\left(\sum_{i=1}^{e} q^{(i-1)}(q-1)\right).$$

which gives (2) on taking logarithm. After the e^{th} column in the m^{th} sub-block, there is no constraint on the columns $H_{m,e+1}, H_{m,e+2}, \cdots, H_{m,s}$ since the desired code is to locate sub-blocks containing errors of RT-weight e or less. Thus, the m^{th} sub-block can be added to H if (2) is satisfied.

Example 3.1. Take $m = 4, s = 3, e = 2, k = 6$ and $q = 2$. Then

$$\begin{aligned} \text{R.H.S. of } (2) &= 1 + 2^1 + 2^1 \times 3\left(\sum_{i=1}^{2} 2^{(i-1)}\right) \\ &= 1 + 2 + 6(2^0 + 2^1) = 21 \end{aligned}$$

Also,

$$\begin{aligned} \text{L.H.S. of } (2) &= 2^{ms-k} \\ &= 2^{4\times3-6} = 2^6 = 64. \end{aligned}$$

Therefore, L.H.S. of (2) =64 $\geq$ 21 =R.H.S. (2) and hence by Theorem 3.2, there exists a $[4 \times 3, 6]$ linear RT-metric array code over $GF(2)$ that locates any corrupted sub-block containing errors of RT-weight 2 or less.

Consider the following $(4 \times 3 - 6) \times (4 \times 3) = 6 \times 12$ parity check matrix of a $[4 \times 3, 6]$ linear RT-metric array code over $GF(2)$ constructed by the procedure discussed in Theorem 3.2.

$$H = \begin{bmatrix} 1 & 0 & 0 & \vdots & 0 & 0 & 0 & \vdots & 1 & 1 & 0 & \vdots & 0 & 1 & 1 \\ 0 & 1 & 0 & \vdots & 0 & 0 & 1 & \vdots & 1 & 0 & 1 & \vdots & 1 & 0 & 1 \\ 0 & 0 & 1 & \vdots & 0 & 0 & 0 & \vdots & 0 & 1 & 1 & \vdots & 1 & 1 & 1 \\ 0 & 0 & 0 & \vdots & 1 & 0 & 0 & \vdots & 1 & 0 & 0 & \vdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 1 & 0 & \vdots & 0 & 1 & 0 & \vdots & 1 & 0 & 1 \\ 0 & 0 & 0 & \vdots & 0 & 0 & 1 & \vdots & 0 & 0 & 0 & \vdots & 1 & 1 & 1 \end{bmatrix}_{6\times12}$$

The code $V \subseteq \text{Mat}_{4\times3}(F_2)$ which is the null space of H locates any corrupted sub-block containg errors of RT-weight 2 or less since syndromes of these error patterns are all distinct as seen from Table 3.1.

Table 3.1

Errors of RT-weight 2 or less confined to a single sub-block	Syndromes
$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (010 000 000 000)	(010000)
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (110 000 000 000)	(110000)
$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (000 010 000 000)	(000010)
$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (000 110 000 000)	(000110)
$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (000 000 010 000)	(101010)
$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ = (000 000 110 000)	(011110)
$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ = (000 000 000 010)	(101101)
$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$ = (000 000 000 110)	(110010)

Note. If we take $e = s = 3$ in Example 3.1 then inequality (2) is not satisfied as R.H.S. of (2) $=1+2^2+2^2\times 3\left(\sum_{i=1}^{3} 2^{(i-1)}\right) = 1+4+12(2^0+2^1+2^2) = 89$ and L.H.S. of (2) $= 2^{ms-k}$=64.

Thus (2) is not satisfied. Also, the code V which is the null space of H is not able to locate all corrupted sub-blocks containing errors of RT-weight 3 or less as the syndromes of two such distinct corrupted sub-blocks viz. $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ are same and are equal to (000110). This justifies the sufficiency of Theorem 3.2.

4. Construction of an EL code from a row-cyclic array code in RT-spaces

In this section, we construct an EL code from a row-cyclic array code [5] in RT-spaces:

Theorem 4.1. *If $g(x) = g_1(x)g_2(x)\cdots g_l(x)$ is a product of distinct irreducible polynomials $g_i(x)(1 \leq i \leq l)$, over $GF(q)$ all belonging to the same period t with deg $g(x) = \rho$. If the row-cyclic $[1 \times t, t-\rho]$ array code generated by $g(x)$ has RT-distance d, then there exists an $[m \times s, k]$ linear RT-metric array code that locates any corrupted sub-block containing errors of RT-weight $(d-1)$ or less where $m = t+2$ (number of sub-blocks), $s = t$ (length of each sub-block) and $k = ms - 2\rho$.*

Proof. Let $\alpha_i(i = 1\text{to } l)$ be any root of $g_i(x)$ for all $1 \leq i \leq l$. The $1 \times t$ cyclic and hence row-cyclic code V' generated by $g(x)$ is the null space of the parity check matrix

$$H' = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{t-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_l & \alpha_l^2 & \cdots & \alpha_l^{t-1} \end{pmatrix}_{\rho \times t} . \quad (3)$$

The RT-distance of the code V' is d implies that every set of $(d-1)$ or fewer columns of H' taken from first $(d-1)$ columns is linearly independent and there exists a linear dependence relation between first d columns of H'.

Now we first discuss the construction for the parity check matrix H of the desired error locating code for the case when $l = 1$.

Let $g(x) = g_1(x)$ with *deg* $g(x) = \rho$.

Let α be any root of $g(x) = g_1(x)$.

$$H' = (1 \quad \alpha \quad \alpha^2 \cdots\cdots \alpha^{t-1})_{\rho \times t}$$

We form the parity check matrix of the desired error locating codes as

$$H = \begin{pmatrix} H' & 0 & H' & H' & H' & \cdots\cdots & H' \\ 0 & H' & H' & \alpha H' & \alpha^2 H' & \cdots\cdots & \alpha^{t-1} H' \end{pmatrix}_{(2\rho) \times t(t+2)}, \quad (4)$$

where the submatrices $0, H, \alpha H, \alpha^2 H, \cdots\cdots, \alpha^{t-1}H$ are $\rho \times t$ matrices and define the sub-block length $s = t$ of the desired error locating code.

Clearly the code V which is the null space of H has the following parameters:

$$\begin{aligned} m &= \text{Number of sub-blocks } = t+2, \\ s &= \text{Length of each sub-block} = t, \\ k &= \text{Dimension of code} = ms - 2\rho, \\ &\quad \text{Number of parity check digits } = 2\rho. \end{aligned}$$

To prove that the code V locates any corrupted sub-block containing errors of RT-weight $(d-1)$ or less, it suffices to show that

(1) The syndrome resulting from the occurrence of errors of RT-weight $(d-1)$ or less with in any one sub-block must be nonzero and

(2) The syndrome resulting from the occurrence of errors of RT-weight $(d-1)$ or less within a single sub-block must be distinct from the syndrome resulting from any combinations of errors of RT-weight $(d-1)$ or less within any other sub-block.

We note that condition (1) is clearly satisfied since any (nonzero) linear combination involving the first $d-1$ (or fewer) columns of H drawn from the same sub-block is nonzero by virtue of the corresponding property of the matrix H'.

Also, for condition (2) , we note that any (nonzero) linear combination involving the first $(d-1)$ or fewer columns drawn from the first sub-block have its lower ρ entries equal to zero. Likewise any (nonzero) linear combination involving the first $(d-1)$ or fewer columns drawn from the second sub-block of H have its upper ρ entries equal to zero. Any (nonzero) linear combination involving the first $(d-1)$ or fewer columns drawn from the i^{th} sub-block $(3 \le i \le t+2)$ must have its lower as well as upper ρ entries to be nonzero because of the column independence property of matrix H'. Now we show that the syndromes of errors of RT-weight $(d-1)$ or less confined to distinct sub-blocks in the last t sub-blocks is different. For this let

$$w, w' \le d-1 \qquad \text{and } 0 \le a, b \le t-1.$$

Suppose that

$$\sum_{i=1}^{w} \lambda_i \begin{pmatrix} \alpha^{(i-1)} \\ \alpha^{a+(i-1)} \end{pmatrix} = \sum_{j=1}^{w'} \mu_j \begin{pmatrix} \alpha^{(j-1)} \\ \alpha^{b+(j-1)} \end{pmatrix}, \lambda_i, \mu_j \in GF(q). \tag{5}$$

The two terms in (5) represent linear combinations of upto first $(d-1)$ columns of H chosen from the two sub-blocks out of the last t-sub-blocks of H. Equating the first ρ-rows in (5), we get

$$\sum_{i=1}^{w}\lambda_i\alpha^{(i-1)} = \sum_{j=1}^{w'}\mu_j\alpha^{(j-1)} \neq 0, \tag{6}$$

because each term is a linear combination of first $(d-1)$ or fewer columns of H' and hence is nonzero.

Equating last ρ rows in (5), we get

$$\sum_{i=1}^{w}\lambda_i\alpha^{a+(i-1)} = \sum_{j=1}^{w'}\mu_j\alpha^{b+(j-1)}$$

or

$$\alpha^a\sum_{i=1}^{w}\lambda_i\alpha^{(i-1)} = \alpha^b\sum_{j=1}^{w'}\mu_j\alpha^{(j-1)} \tag{7}$$

Dividing (7) by (6) yields

$$\alpha^a = \alpha^b \quad \text{where } 0 \leq a, b \leq t-1.$$

Since $1, \alpha, \alpha^2, \cdots, \alpha^{t-1}$ are all distinct so we must have $a = b$ i.e. a and b refer to the same sub-block. Hence condition (2) is satisfied and the linear RT-metric array code defined by H is an error locating code capable of locating any corrupted sub-block of length t containing errors of RT-weight $(d-1)$ or less.

This proves the theorem for the case $l = 1$. For arbitrary l, we can replace the matrices $H', \alpha H', \alpha^2 H', \cdots\cdots$ in (4) by matrices derived from H' by cyclic permutation of columns of H'. With this modification, we get the theorem by the same reasoning as discussed for the case $l = 1$. □

Example 4.1. Let $g(x) = x^3 + x + 1$ be a primitive irreducible polynomial over $GF(2)$. Then t = order of $g(x) = 2^{\deg g(x)} - 1 = 2^3 - 1 = 7$. Here $\rho = deg\ g(x) = 3$. The parity check matrix of the $[1 \times 7, 4]$ row-cyclic code generated by $g(x)$ is given by

$$H' = (1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6)_{3\times 7}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}_{3\times 7},$$

where α satisfies $\alpha^3 + \alpha + 1 = 0$.

The code V' which is the null sapce of H' has minimum RT-distance 4 as the first 3 columns of H are linearly independent over $GF(2)$ and first 4 coumns of H are linearly dependent. Thus $d = 4$.

We construct the $[t(t+2), t(t+2) - 2\rho] = [7 \times 9, 7 \times 9 - 6] = [63, 57]$ linear RT-metric array code with $m=$ 9 (number of sub-blocks), $s = 7$ (length of each sub-block) that is capable of locating any corrupted sub-block containing errors of RT-weight $d - 1 = 3$ or less.

The parity check matrix of such a code is given by

$$H = \begin{pmatrix} H' & 0 & H' & H' & H' & H' & H' & H' & H' \\ 0 & H' & H' & \alpha H' & \alpha^2 H' & \alpha^3 H' & \alpha^4 H' & \alpha^5 H' & \alpha^6 H' \end{pmatrix}_{6\times 63}.$$

Remark. The code constructed in Example 4.1 is an optimal error locating code in RT-spaces as it meets the bound obtained in (1) in Theorem 3.1 viz.

$$q^{ms-k} \geq 1 + m\sum_{i=1}^{e} q^{(i-1)}(q-1).$$

For the $[7 \times 9, 7 \times 9 - 6] = [63, 57]$ linear RT-mtric array code over $GF(2)$ constructed in Example 4.1, we have

$$\begin{aligned} \text{L.H.S. of (1)} &= 2^{63-57} = 2^6 = 64 \\ \text{R.H.S. of (1)} &= 1 + 9\sum_{i=1}^{d-1} 2^{(i-1)} = 1 + 9\sum_{i=1}^{3} 2^{(i-1)} \\ &= 1 + 9(2^0 + 2^1 + 2^2) \\ &= 1 + 9 \times 7 = 64. \end{aligned}$$

Example 4.2. Let $g(x) = x^4 + x^3 + x^2 + x + 1$ be an irreducible polynomial of degree ρ=4 over $GF(2)$. Here t=order of $g(x) = 5$ as $g(x)$ divides $x^5 - 1$ and 5 is the least positive integer such that $g(x)$ divides $x^n - 1$. Thus $g(x)$ generates a $[1 \times 5, 1]$ row-cyclic linear RT-metric array code V over $GF(2)$ characterized by the following parity check matrix:

$$H' = (1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4)_{4\times 5} \qquad \text{where } \alpha \text{ is a root of } g(x).$$

or

$$H' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}_{4\times 5}.$$

Since first four columns of H' are linearly independent over $GF(2)$ and first five coulmns of H' are linearly dependent, therefore minimum RT-distance of code V' having H' as parity check matrix is $d = 5$.

We construct the $[t(t+2), t(t+2) - 2\rho] = [5 \times 7, 5 \times 7 - 8] = [35, 27]$ linear RT-metric array code with $m = 7$ (number of sub-blocks), $s = 5$ (length of each sub-block) that is capable of locating any corrupted sub-block containing errors of RT-weight $d - 1 = 4$ or less.

The parity check matrix of such a code is given by

$$H = \begin{pmatrix} H' & 0 & H' & H' & H' & H' & H' \\ 0 & H' & H' & \alpha H' & \alpha^2 H' & \alpha^3 H' & \alpha^4 H' \end{pmatrix}_{8 \times 35}$$

This code is not optimal error locating code as it does not meet the bound given by (1) in Theorem 3.1 as shown below:

$$\begin{aligned} \text{L.H.S. of (1)} &= 2^{35-27} = 2^8 = 256 \\ \text{R.H.S. of (1)} &= 1 + 7\left(\sum_{i=1}^{4} 2^{(i-1)}\right) \\ &= 1 + 7(2^0 + 2^1 + 2^2 + 2^3) \\ &= 1 + 7(1 + 2 + 4 + 8) = 106 \end{aligned}$$

Thus L.H.S. of (1) > R.H.S. (1).

Note. Apart from $t(t+2)$ length error locating code constructed in Theorem 4.1, we can also construct error locating code of length t^2 by taking

$$H = \begin{pmatrix} H' & H' & \cdots & H' \\ H' & \alpha H' & \cdots & \alpha^{t-1} H' \end{pmatrix}.$$

Acknowledgment. The author would like to thank her husband Dr. Arihant Jain for his constant support and encouragement for pursuing this research work.

References

[1] S.T. Dougherty and M.M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Moscow Mathematical Journal, 2 (2002), 83-99.

[2] S. Jain, *Bursts in m-Metric Array Codes*, Linear Algebra and Its Applications, 418 (2006), 130-141.

[3] S. Jain, *Campopiano-Type Bounds in Non-Hamming Array Coding*, Linear Algebra and Its Applications, 420 (2007), 135-159.

[4] S. Jain, *CT Bursts-From Classical to Array Coding*, Discrete Mathematics, 308-309 (2008), 1489-1499.

[5] S. Jain, *An Algorithmic Approach to Achieve Minimum ρ-Distance at least d in Linear Array Codes*, Kyushu J. Math., 62 (2008), 189-200.

[6] S. Jain, *Row-Cyclic Codes in Array Coding*, Algebras, Groups, Geometries, 25 (2008), 287-310.

[7] M.Yu. Rosenbloom and M.A. Tsfasman, *Codes for m-metric*, Problems of Information Transmission, 33 (1997), 45-52.

[8] M.M. Skriganov, *Coding Theory and uniform distributions*, St. Petersburg Math. J., 13 (2002), 301-337.

[9] J.K. Wolf and B. Elspass, *Eror-locating codes-A new concept in error control*, IEEE Trans. IT-9 (1963), 113-117.

[10] J.K. Wolf, *On an extended class of error-locating codes*, Information and Control, 8 (1965), 163-169.