

Normality of Binary Codes in Rosenbloom-Tsfasman Metric

R.S. Selvaraj* and Venkatrajam Marka†

Department of Mathematics

National Institute of Technology Warangal

India

Emails: * rsselva@nitw.ac.in † mvraaz.nitw@gmail.com

Abstract—In this paper, we extend the notion of normality of codes in Hamming metric to the codes in Rosenbloom-Tsfasman metric (RT-metric, in short). Using partition number and l -cell of codes in RT-metric, we establish results on covering radius and normality of codes in this metric. We also investigate the feasibility of applying amalgamated direct sum method for the construction of codes in RT-metric by investigating on the acceptability of various coordinate positions of codes in this metric.

I. INTRODUCTION

Covering radius - a geometric property that characterizes maximal error correcting capability in the case of minimum distance decoding - of codes with the conventional Hamming metric had been extensively studied by many researchers [1], [2]. It has evolved into a subject in its own right mainly because of its practical applicability in areas such as data compression, testing and write-once memories and also because of the mathematical beauty that it possesses. For more on the covering radius one can refer [9]. Various methods for constructing new codes from two or more known codes were given by many researchers over the last few decades in order to improve upon the bounds on covering radius, among which Direct Sum method is a basic yet useful construction method. To improve upon the bounds related to covering radius of binary codes obtained using this method, the notion of normality for binary linear codes and that of the Amalgamated Direct Sum (ADS) of two binary linear normal codes were introduced by Graham and Sloane in [6]. The same were extended to binary nonlinear codes by Cohen et.al. in [3]. Later, Lobstein and Van Wee generalized these results to q -ary codes [10].

Here in this paper, we extend the notion of normality to binary codes in Rosenbloom-Tsfasman metric (RT-metric, in short). This metric was introduced by Rosenbloom and Tsfasman in [7] and independently by Skrikanov in [8]. This metric is more adequate than Hamming metric in dealing with channels in which errors have a tendency to occur with a periodic spike-wise perturbation of period $s \in \mathbb{N}$. As a generalization of the classical Hamming metric with rich mathematical beauty and being advantageous over Hamming metric in dealing with certain channels [7], [8], this metric attracted the attention of many researchers over the last two decades [11]–[13]. The covering problem in RT-metric was first dealt by I. Siap for RT-spaces over Galois Rings [5].

The following is the organization of our paper. Section I-A gives some basic definitions and notations that are used in

this paper. In section II, we have studied the covering radius of binary codes in this metric by introducing two new tools namely, *partition number* and *l-cell* which greatly reduce the difficulty in determining the covering radius. In section III, we investigate the normality of binary codes in RT-metric. In this section, we also discuss the possibilities of extending the direct sum and amalgamated direct sum (ADS) constructions from Hamming metric to RT-metric. And finally, section IV provides the conclusions of this paper.

A. Definitions and Notations

For $x = (x_1, x_2, \dots, x_s) \in \mathbb{F}_2^s$, we define the ρ -weight (RT-weight) of x to be

$$wt_\rho(x) = \max\{i | x_i \neq 0, 1 \leq i \leq s\}$$

The RT-distance or ρ -distance between $x = (x_1, x_2, \dots, x_s)$, $y = (y_1, y_2, \dots, y_s) \in \mathbb{F}_2^s$ can be defined as $d_\rho(x, y) = wt_\rho(x - y)$. The subsets of the space equipped with this metric are called RT-metric codes and the subspaces are called linear RT-metric codes. The maximum distance of any word in the ambient space to an RT-metric code is called the *covering radius* of the code. A code in which each non-zero codeword is of weight w_ρ is said to be a *constant weight code*.

Throughout this paper, unless otherwise specified, by a code we mean a binary RT-metric code and by distance we mean RT-distance. Moreover, $[s, k, d_\rho]R$ denotes a binary linear code of length s , dimension k , minimum distance d_ρ and covering radius R ; and $(s, K, d_\rho)R$ denotes a binary code with cardinality K .

Definition 1: Direct Sum of Two Codes:

Let C_1 and C_2 be codes with parameters (s_1, K_1) and (s_2, K_2) respectively. Then the *direct sum* of C_1 and C_2 is denoted as $C_1 \oplus C_2$ and defined as

$$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1, c_2 \in C_2\}$$

and is a code of length $s_1 + s_2$ and cardinality $K_1 + K_2$.

Definition 2: Normal Codes:

Let C be a binary RT-metric code of length s cardinality K and covering radius R and also let $C_0^{(i)}$ and $C_1^{(i)}$ denote the sets of codewords in which the i^{th} coordinate is 0 and 1 respectively. For any word $\mathbf{x} \in \mathbb{F}_2^s$, we define the *norm* of C with respect to the i^{th} coordinate as

$$N^{(i)} = \max_{x \in \mathbb{F}_2^s} \{d_\rho(x, C_0^{(i)}) + d_\rho(x, C_1^{(i)})\}$$

where

$$d_p(x, C_a^{(i)}) = \begin{cases} \min\{d_p(x, y) | y \in C_a^i\} & \text{if } C_a^i \neq \emptyset \\ s & \text{if } C_a^i = \emptyset \end{cases}$$

Now, $N = \min_i N^{(i)}$, is called the norm of C and the coordinates i for which $N^{(i)} = N$ are said to be *acceptable*. Finally, a code is said to be *normal* if its norm satisfies $N \leq 2R + 1$.

II. COVERING RADIUS OF CODES IN RT-METRIC

Definition 3: Partition Number of an RT-metric Code:

Let C be an (s, K, d_p) binary RT-metric code. The largest non-negative integer l , for which each binary l -tuple can be assigned to at least one codeword whose last l coordinates are actually that l -tuple, is called the *partition number* of the code C . The code with partition number l can be partitioned into 2^l parts, each of which have the property that all its members have the same binary l -tuple as their last l coordinates. A part obtained in the above fashion is called an *l -cell* of the code, if all of its member codewords contain the same $(l+1)$ -tuple as their last $l+1$ coordinates. As the definition of partition number suggests, a code with partition number l contains at least 2^l codewords.

Now, we can observe that covering radius of a code can be determined using the concepts of partition number and l -cell. The definition of partition number serves as a tool in determining the covering radius of an RT-metric code, as shown by the following theorem.

Theorem 1: Let C be an $(s, K, d_p)R$ binary RT-metric code. Then the partition number of C is l iff its covering radius is $s - l$.

Proof: First, let the partition number of the code be l . Let us partition the code into 2^{l+1} parts in the following manner. Take 2^{l+1} boxes each of which is labeled with a unique binary $(l+1)$ -tuple. Arrange all the codewords into these boxes, by putting each codeword into a box whose label is same as the last $l+1$ coordinates of that codeword. But, since the partition number of the code is l , by the definition of partition number, at least one of the 2^{l+1} boxes must be empty. If we pick a word x from the ambient space $\mathbb{F}_2^s$ in such a way that its last $l+1$ coordinates are the $(l+1)$ -tuple which is the label of an empty box, then this word will be at distance $s - l$ from the code, which is the maximum distance of any word from the ambient space. Hence, the covering radius is $s - l$.

Conversely, let $R = s - l$. By the definition of covering radius, any word must be at distance at most $s - l$ from the code, which means that for each word there is at least one codeword which agrees with the word in the last $s - (s - l) = l$ coordinate positions. This implies that the partition number of the code is greater than or equal to l . Let us assume that the partition number of the code is $m > l$. Then, to each m -tuple, we can associate a codeword whose last m coordinates agree with that m -tuple. This means that any word will be at distance at most $s - m$, which is a contradiction to the fact that covering radius of the code C is $R = s - l$. Hence, the partition number of the code C is l . ■

By the definition of l -cell, we can restate the above theorem in terms of l -cell as follows.

Corollary 2: Let C be an RT-metric code of length s over $\mathbb{F}_2$. Then, the covering radius of C is $s - l$ iff $\exists$ an l -cell of the code C .

The covering radius of constant weight codes in RT-metric can be directly determined by its weight as the following proposition suggests.

Proposition 3: Let C be any binary constant weight RT-metric code with constant weight w_p and length s . Then C has covering radius s .

Proof: Now, the last $s - w_p$ coordinates of all the codewords of C will be 0 which implies, the partition number of C will be 0. Hence, covering radius of C will be s (by *theorem 1*). ■

Proposition 4: Let C_1, C_2 be $(s_1, K_1, d_1)R_1$ and $(s_2, K_2, d_2)R_2$ binary RT-metric codes respectively. Then their direct sum $C = C_1 \oplus C_2$ is an $(s_1 + s_2, K_1 + K_2, d)R$ code with minimum distance $d = d_1$ and covering radius $R = s_1 + R_2$, provided $C_2 \neq \mathbb{F}_2^{s_2}$.

Proof: The direct sum of C_1 and C_2 is given by

$$C_1 \oplus C_2 = \{(c_1, c_2) | c_1 \in C_1, c_2 \in C_2\}$$

Clearly this is a code of length $s_1 + s_2$ and cardinality $K_1 + K_2$. Now, since the minimum distance of C_1 is d_1 , there exist two codewords c_1, c'_1 in C_1 such that $d_p(c_1, c'_1) = d_1$. Then the codewords $c = (c_1, c_2)$ and $c' = (c'_1, c_2)$ for some $c_2 \in C_2$, will also be at distance d_1 which is minimum among all the codewords of C . And as the covering radius of a code in RT-metric depends on the partition number of the code and also as the process of partitioning starts with the right most coordinate, unless C_2 is the space $\mathbb{F}_2^{s_2}$, the partition number of C must also be equal to that of C_2 which is $s_2 - R_2$ by *theorem 1*, and hence by the same theorem covering radius of C is $s_1 + s_2 - (s_2 - R_2) = s_1 + R_2$. ■

Remark: If $C_2 = \mathbb{F}_2^{s_2}$, then $R = R_1$

III. NORMALITY OF CODES IN RT-METRIC

Theorem 5: Any RT-metric code of length s and covering radius $R = s$ over $\mathbb{F}_2$ is normal and all the coordinates are acceptable.

Proof: Now, every codeword of C will end with the same field element, say $\alpha \in \mathbb{F}_2$. If an $x \in \mathbb{F}_2^s$ is such that its last coordinate is different from α , then $d_p(x, C_0^{(i)}) = d_p(x, C_1^{(i)}) = s$, $\forall i \in \{1, 2, \dots, s\}$. Thus, $N^{(i)} = s + s = 2s < 2R + 1$, $\forall i$. Hence, C is normal and all the codewords are acceptable as i is arbitrary. ■

Lemma 6: Let C be any RT-metric code with length s and covering radius $R < s$, then

$$N^{(i)} = i + R, \forall R + 1 \leq i \leq s$$

Proof: For a coordinate position $i \in \{R + 1, R + 2, \dots, s\}$, the norm is given by

$$N^{(i)} = \max_{x \in \mathbb{F}_2^s} \{d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)})\}$$

As the covering radius of C is R , it has partition number $s - R$. So the definition of partition number implies that

each codeword can be associated to a unique $(s-R)$ -tuple which actually consists of the last $(s-R)$ coordinates of that codewords and also that there exists at least one $(s-R+1)$ -tuple which is not same as the last $s-R+1$ coordinates of any of the codewords. Now, when we partition the code into two parts namely, $C_0^{(i)}$ and $C_1^{(i)}$, we can also partition the set of all $(s-R)$ -tuples into two parts depending on the corresponding associated codewords. If we choose an $x \in \mathbb{F}_2^s$ whose last $s-R+1$ coordinates does not match with the last $s-R+1$ coordinates of any of the codewords, surely this word will have $d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)}) = i+R$ which is the maximum value that a word can give. Hence, the result. ■

Theorem 7: Let C be any RT-metric code of length s with covering radius $R < s$. Then the coordinates $R+2, R+3, \dots, s$ are not acceptable.

Proof: The minimum norm is

$$N \leq N^{(i)}, \forall i \in \{1, 2, \dots, s\} \quad (1)$$

By Lemma 6, $N^{(i)} = i+R$, $\forall i \geq R+1$ which implies,

$$N^{(R+1)} < N^{(R+2)} < N^{(R+3)} < \dots < N^{(s)} \quad (2)$$

From equations 1 and 2, one can conclude that

$$N < N^{(i)}, \forall i \in \{R+2, R+3, \dots, s\} \quad (3)$$

Hence, the proof. ■

The above theorem is not sufficient to arrive at a decision on the acceptability of the s^{th} coordinate, when the code has covering radius $R = s-1$. This can be overcome by the following theorem which says that no binary RT-metric code with dimension more than or equal to 2 and covering radius $s-1$ has acceptable last coordinate.

Theorem 8: Let C be a linear RT-metric code of length s and dimension greater than or equal to 2 having covering radius $s-1$ over $\mathbb{F}_2$. Then the last coordinate is not acceptable.

Proof: For a coordinate position $i \in \{1, 2, \dots, s\}$, the norm is given by

$$N^{(i)} = \max_{x \in \mathbb{F}_2^s} \{d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)})\}$$

But, by Lemma 6,

$$\begin{aligned} N^{(s)} &= s+R \\ &= s+s-1 = 2(s-1)+1 \quad (\text{since } R = s-1) \\ &= 2R+1 \end{aligned}$$

We prove this theorem by induction on the dimension k of the code C . Let $k=2$. Now, as the covering radius of the code C is $s-1$, by Corollary 2 there exists at least one 1-cell of the code C . But since the code is linear and binary with dimension 2, the code gets partitioned into two 1-cells.

In order for the code C to be normal with last coordinate being acceptable, we must have $N^{(i)} = s+s-1$ for $i \in \{1, 2, \dots, s-1\}$. We will get norm $N^{(i)} = s+s-1$ only when each 1-cell is contained in either of $C_0^{(i)}$, $C_1^{(i)}$. Suppose the codewords belonging to same 1-cell differ in j^{th} coordinate. Then one of these codewords will be sent to $C_0^{(j)}$ and the other to $C_1^{(j)}$. Then for any $x \in \mathbb{F}_2^s$, $d_p(x, C_0^{(j)}) + d_p(x, C_1^{(j)}) \leq (s-1) + (s-1) < s + (s-1)$, which implies $N^{(j)} < s + s - 1$.

Hence, the s^{th} coordinate is not acceptable.

Now, let us suppose the result for a linear code of dimension $k \in \{2, 3, \dots, s-1\}$. Now we have to prove the result for a code D with dimension $k+1$. By induction hypothesis, last coordinate is not acceptable for all the subcodes C of dimension k of the code D . Then there exists some $j \in \{1, 2, \dots, s-1\}$ such that $N^{(j)} < s+s-1$ for such subcode of D . But, we know that if C_1 is a subcode of C_2 , then $d_p(x, C_2) \leq d_p(x, C_1)$, for any x in the ambient space. Thus, $d_p(x, D_0^{(j)}) + d_p(x, D_1^{(j)}) \leq d_p(x, C_0^{(j)}) + d_p(x, C_1^{(j)}) < s+s-1, \forall x$. Hence the last coordinate is not acceptable for the code D of dimension $k+1$. Hence the result. ■

But, when the code is 1-dimensional then all the coordinates are acceptable as the following theorem suggests.

Proposition 9: Let C be a one dimensional binary RT-metric code of length s . Then the code C is normal and all coordinates are acceptable.

Proof: Let C be a one dimensional binary RT-metric code of length s . Then C has covering radius either s or $s-1$. If covering radius of C is s , then C is normal with all its coordinates being normal as shown in theorem 5. We only need to prove the result when the covering radius of C is $s-1$. For such a code C , there exist a 1-cell. Since the dimension of C is one there exist two 1-cells. For each $i \in \{1, 2, \dots, s\}$, the value of $d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)}) \leq s+s-1$ for any $x \in \mathbb{F}_2^s$, which implies $N^{(i)} = 2s-1 = 2R+1$ as $R = s-1$. Thus C is normal and all the coordinates are acceptable. This completes the proof. ■

Proposition 10: The space $\mathbb{F}_2^s$ of all vectors of length s over the field $\mathbb{F}_2$ is normal with the 1^{st} coordinate being the only acceptable coordinate. All other coordinates are not acceptable.

Proof: The partition number of the space $\mathbb{F}_2^s$ is s and so its covering radius R is 0. The norm with respect to the i^{th} coordinate for $2 \leq i \leq s$ is given by,

$$\begin{aligned} N^{(i)} &= \max_{x \in \mathbb{F}_2^s} \{d_p(x, (\mathbb{F}_2^s)_0^{(i)}) + d_p(x, (\mathbb{F}_2^s)_1^{(i)})\} \\ &= i+0 \\ &= i \\ &> 1 = 2R+1 \quad (\because R=0 \text{ and } i \geq 2) \end{aligned}$$

But $N^{(1)} = 1+0 = 1 = 2R+1$ and so the ambient space $\mathbb{F}_2^s$ is normal with the first coordinate being the only acceptable coordinate. ■

Proposition 11: Let C be a binary constant weight code with weight w_p and length s . Then C is normal with norm $2s$ and all the coordinates are acceptable.

Proof: Since code C is constant of RT-weight w_p , by Proposition 3 its covering radius is $R = s$. For a coordinate position $i \in \{1, 2, \dots, s\}$, the norm is given by

$$\begin{aligned} N^{(i)} &= \max_{x \in \mathbb{F}_2^s} \{d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)})\} \\ &= s+s \quad (\because C \text{ has constant RT-weight}) \\ &= 2s < 2R+1 \quad (\because R=s) \end{aligned}$$

Hence the proof. ■

Proposition 12: Let C_1, C_2 be $(s_1, K_1, d_1)R_1$ and $(s_2, K_2, d_2)R_2$ binary RT-metric codes respectively. Then (a) their direct sum $C = C_1 \oplus C_2$ is normal (b) all the coordinates corresponding to C_1 are acceptable for C and (c) the coordinate i for $s_1 + 1 \leq i \leq s_2$ is acceptable for $C_1 \oplus C_2$ only if the norm of C_2 with respect to the coordinate $i - s_1$ is less than or equal to $2R_2$.

Proof: Let C_1, C_2 be $(s_1, K_1, d_1)R_1$ and $(s_2, K_2, d_2)R_2$ binary RT-metric codes respectively. Then by *Proposition 4*, their direct sum $C = C_1 \oplus C_2$ is an $(s_1 + s_2, K_1 + K_2, d_1)R$ code with covering radius $R = s_1 + R_2$. Now for $i \in \{1, 2, \dots, s_1\}$, the norm of C with respect to the i^{th} coordinate is given by

$$\begin{aligned} N^{(i)} &= \max_{x \in \mathbb{F}_2^{s_1+s_2}} \{d_p(x, C_0^{(i)}) + d_p(x, C_1^{(i)})\} \\ &= (s_1 + R_2) + (s_1 + R_2) \\ &= 2(s_1 + R_2) \\ &= 2R < 2R + 1 \end{aligned}$$

That implies C is normal and all the coordinate positions corresponding to C_1 are acceptable. In order for the coordinate position $j \in \{s_1 + 1, s_1 + 2, \dots, s_1 + s_2\}$ corresponding to C_2 to be acceptable for C , it must provide us with norm equal to $2(s_1 + R_2)$ which means C_2 must be normal with the coordinate position $j - s_1$ being acceptable with norm less than or equal to $2R_2$. ■

B. Normality and Amalgamated Direct Sum Construction

The amalgamated direct sum of two codes is defined as follows.

Definition 4: Let C_1 be an $[s_1, k_1]R_1$ normal code with last coordinate acceptable and C_2 be an $[s_2, k_2]R_2$ normal code with first coordinate acceptable. Then their amalgamated direct sum (or shortly ADS), denoted by $C_1 \dot{\oplus} C_2$ is an $[s_1 + s_2 - 1, k_1 + k_2 - 1]s_1 + R_2$ code, and is given by

$$C_1 \dot{\oplus} C_2 = \{(c_1 | u | c_2) : (c_1 | u) \in C_1 \text{ and } (u | c_2) \in C_2\}$$

As we have seen by *Theorem 8*, there is no code of dimension greater than 1 whose last coordinate is acceptable. Hence, we can not use this construction method to combine codes of dimension more than 1. But, since the one-dimensional codes are normal and all the coordinates are acceptable, one can only use this ADS construction method to combine a 1-dimensional code with any other linear code.

Theorem 13: Let C_1 be an $[s_1, 1]$ code with covering radius $t[s_1, 1]$ which is normal with last coordinate acceptable and C_2 be an $[s_2, k_2]$ code with covering radius $t[s_2, k_2]$. Then their amalgamated direct sum $C_1 \dot{\oplus} C_2$ is an $[s_1 + s_2 - 1, k_2]$ code with covering radius $t[s_1 + s_2 - 1, k_2]$

Proof: We know by theorem that $t[s, k] = s - k$. So, $t[s_1, 1] = s_1 - 1$ and $t[s_2, k_2] = s_2 - k_2$. Now, as the dimension of $C_1 \dot{\oplus} C_2$ is k_2 (which is less than or equal to s_2) the covering radius of $C_1 \dot{\oplus} C_2$ depends only on the coordinates pertaining to the code C_2 . But C_2 has covering radius $s_2 - k_2$, hence has partition number k_2 . So, $C_1 \dot{\oplus} C_2$ also will have partition number k_2 and hence has covering radius $s_1 + s_2 - 1 - k_2$ which is equal to $t[s_1 + s_2 - 1, k_2]$. Hence, the proof. ■

We discussed the normality of codes in RT-metric and determined its norm with respect to various coordinate positions. We also established that the last coordinate is not acceptable for any non trivial code in this metric which makes the ADS construction not possible for construction of higher dimensional codes.

REFERENCES

- [1] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and Y. R. Schatz, "Covering radius - survey and recent results", *IEEE Trans. Inform. Theory*, vol. 31, no. 3, pp. 328-343, 1985.
- [2] G. D. Cohen, S. N. Litsyn, A. C. Lobstein, and H. F. Mattson, Jr., "Covering radius 1985 - 1994", *AAECC*, vol. 8, pp. 173-239, 1997.
- [3] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes", *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 680-694, 1986.
- [4] M. Gadouleau and Z. Yan, "Packing and covering properties of rank metric codes", *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3873-3883, 2008.
- [5] B. Yildiz, I. Siap, T. Bilgin, and G. Yesilot, "The covering problem for finite rings with respect to the RT-metric", *Appl. Math. Lett.*, vol. 23, pp. 988-992, 2010.
- [6] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes", *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385-401, 1985.
- [7] M. Yu. Rosenbloom and M. A. Tsfasman, "Codes for the m-metric", *Probl. Inf. Transm.*, vol. 33, pp. 45-52, 1997.
- [8] M. M. Skraganov, "Coding theory and uniform distributions", *Algebra i Analiz*, vol. 13, no. 2, pp. 191-239, 2001(Russian). (English translation in *St. Petersburg Math. J.*, vol. 143, no. 2, pp. 301-337, 2002.)
- [9] G. D. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, Elsevier Science B.V., 1997.
- [10] A. C. Lobstein and G. J. M. van Wee, "On normal and subnormal q-ary codes", *IEEE Trans. Inform. Theory*, vol. 35, no. 6, pp. 1291-1295, 1989.
- [11] S. Jain, "CT bursts - from classical to array coding", *Discrete Math.*, vol. 308, pp. 1489-1499, 2008.
- [12] S. T. Dougherty, "Maximum distance codes in $Mat_{n \times s}(\mathbb{Z}_k)$ with a non-Hamming metric and uniform distributions", *Des. Codes Cryptogr.*, vol. 33, pp. 45-61, 2004.
- [13] I. Siap and M. Ozen, "The complete weight enumerator for codes over $M_{n \times s}(R)$ with respect to the Rosenbloom-Tsfasman metric", *Appl. Math. Lett.*, vol. 17, pp. 65-69, 2004.