Self-dual codes in the Rosenbloom-Tsfasman metric

Venkatrajam Marka, R. S. Selvaraj*and Irrinki Gnanasudha

Department of Mathematics, National Institute of Technology Warangal, Warangal, Telangana-506 004, India

Received February 7, 2016; accepted July 13, 2016

Abstract. This paper deals with the study and construction of self-dual codes equipped with the Rosenbloom-Tsfasman metric (RT-metric, in short). An $[s,\ k]$ linear code in the RT-metric over $\mathbb{F}_q$ has codewords with k different non-zero weights. Using the generator matrix in standard form of a code in the RT-metric, the standard information set for the code is defined. Given the standard information set for a code, that for its dual is obtained. Moreover, using the basic parameters of a linear code, the covering radius and the minimum distance of its dual are also obtained. Eventually, necessary and sufficient conditions for a code to be self-dual are established. In addition, some methods for constructing self dual codes are proposed and illustrated with examples.

AMS subject classifications: 94B75, 94B05, 94B60

Key words: linear code, self-dual code, standard information set, covering radius, RT-metric

1. Introduction

Among the most fascinating families of codes, the family of self-dual codes is a very important one. These codes are of utmost interest at least for two reasons. One reason is that self-dual codes include some of the nicest and best known error-correcting codes, and the other is that they have strong and interesting connections with other areas of mathematics such as combinatorics, group theory, lattices and modular forms. Self-dual codes are also of considerable practical importance; for instance, $\mathscr{G}_{24}$, the [24, 12] binary extended Golay code used in the Voyager space probes, that were launched towards Jupiter and Saturn in 1977, is a self-dual code [7].

In the past 50 years, the theory of self-dual codes has inspired many researchers and subsequently has seen a tremendous growth. Over these years, researchers have been busily involved in proposing various techniques for the construction of self-dual codes, investigating the properties of the codes constructed and classifying - eventually, enumerating them [13].

A new metric, known as the Rosenbloom-Tsfasman metric (the RT-metric, in short), was first introduced by Rosenbloom and Tsfasman [14] in the context of coding theory. In the context of the theory of uniform distributions, the same

*Corresponding author. *Email addresses:* mvraaz.nitw@gmail.com (V. Marka), rsselva@nitw.ac.in (R. S. Selvaraj), ignanasudha@nitw.ac.in (I. Gnanasudha)

metric was also introduced by Martin and Stinson [6] and by Skriganov [19]. Being a generalization of the classical Hamming metric, RT-metric immediately received the attention of many coding theorists and subsequently a steady stream of work has been done on codes equipped with this metric. Most of the research carried out on codes in this metric is concerned with various bounds [12], weight distribution and MacWilliam's identities [1, 18, 11, 16], linearity [8, 9, 10], maximum distance separability [19, 2], groups of automorphisms [5], burst error enumeration [3, 4, 17], covering properties [20] and normality [15] over several algebraic structures.

As the inner product considered for RT-metric (see, [19]) is different from the conventional inner product that is used to define duality in Hamming metric, most of the codes which are self-dual in Hamming metric are not so in RT-metric. Hence, there is a great need to thoroughly investigate even the existence of self-dual codes in the different inner product setup for RT metric and subsequently, to explore the properties of those codes if they exist. Here, in this paper we try to address this problem. Our primary interest here is to establish the necessary and sufficient condition for a code in RT-metric to be self-dual and to find their possible weight distribution in terms of, what we shall call as, *type* of the code.

The organization of the paper is as follows. In Section 2, we present the basic definitions and concepts that are useful for the results in the subsequent sections. A linear code over $\mathbb{F}_q$ in RT-metric of dimension k will have k different non-zero weights. Based on this observation, in Section 3, we define the standard information set $\{d_1,\ d_2,\ \ldots,\ d_k\}$ for the code (where d_1 is the minimum RT-weight of the code). Moreover, we define the generator matrix in standard form of a code through which we obtain the standard information set for the dual code. Given the basic parameters of a linear code, we obtain covering radius and minimum distance of its dual. In Section 4, we establish necessary and sufficient conditions for a code in RT-metric to be self-dual. *Formally self-dual* codes and projections of self-dual codes have also been discussed in this section. In Section 5, some constructions for self-dual codes are proposed and illustrated with examples. Finally, Section 6 provides the conclusion.

2. Preliminaries

For $x = (x_1, x_2, \ldots, x_s),\ y = (y_1, y_2, \ldots, y_s) \in \mathbb{F}_q^s$, the ρ-distance between x and y is defined as $d_\rho(x, y) = \max\{i | x_i \neq y_i, 1 \leq i \leq s\}$. The subsets of the space $\mathbb{F}_q^s$ equipped with this metric are called q-ary RT-metric codes (or q-ary codes in the RT metric); in addition, if they are subspaces, then they are called linear RT-metric codes. For any k-dimensional linear code C in $\mathbb{F}_q^s$, any $k \times s$ matrix G whose rows form a basis for C is said to be its generator matrix. For any set of k linearly independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for C. An RT-ball $B_\rho(x; r)$ (also called a ρ-ball) of radius r centered at $x \in \mathbb{F}_q^s$ is the set $\{y \in \mathbb{F}_q^s | d_\rho(x, y) \leq r\}$. The maximum r for which the ρ-balls of radius r centered at codewords do not intersect is called the packing radius of the code and the minimum R for which the ρ-balls of radius R centered at codewords cover the entire ambient space is called the covering radius of the code. A code whose covering radius coincides with its packing radius is said to be perfect.

For an RT-metric code C of length s and minimum ρ-distance d_ρ, the Singleton bound is given by $|C| \leq q^{s-d_\rho+1}$ and, in particular, for linear codes with dimension k, it is $k \leq s - d_\rho + 1$. A code which attains the Singleton bound is said to be a maximum distance separable code (MDS code, in short).

Throughout this paper, unless otherwise specified, a code means an RT-metric code over $\mathbb{F}_q$. Moreover, $[s, k, d_\rho; R]_q$ denotes a q-ary linear code with length s, dimension k, minimum distance d_ρ and covering radius R; and $(s, K, d_\rho; R)_q$ denotes a q-ary code with cardinality K. By $[s]$, we mean the set $\{1, 2, \ldots, s\}$.

2.1. Partition number and covering radius

The notion of partition number of a code, which greatly reduces the difficulty in finding the covering radius of codes in RT-metric was introduced in [15]. The partition number of a code is defined as follows.

Definition 1 (Partition number of a q-ary RT-metric code, see [15])**.** *Let C be an $(s, K, d_\rho)_q$ code in RT-metric. The largest non-negative integer l, for which each q-ary 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 q^l parts, each of which has the property that all its members have the same q-ary l-tuple as their last l coordinates. Now, we state, without proof, the following result from [15] which enables the notion of partition number to act as a tool in determining the covering radius of an RT-metric code.

Theorem 1 (see [15])**.** *Let C be an $(s, K, d_\rho)_q R$ code in RT-metric. Then the partition number of C is l iff its covering radius is $s - l$.* □

3. Generator matrix in standard form of a code in RT-metric

The generator matrix in standard form of an RT-metric code was defined in a different context by Irfan Siap in [8]. We have adapted and modified it to suit to the context of the present paper. We also observe that if d is the minimum ρ-distance, then d will be the greatest minimal element among all the information sets of C.

Definition 2. *Let C be an $[s, k, d]_q$ RT-metric linear code and G the generator matrix of C. Applying certain elementary row operations one can always transform G into the following form:*

$$G' = \begin{bmatrix} g_{1,1} & \cdots & g_{1,d_1-1} & g_{1,d_1} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots\ 0 \\ g_{2,1} & \cdots & g_{2,d_1-1} & 0 & g_{2,d_1+1} & \cdots & g_{2,d_2-1} & g_{2,d_2} & 0 & \cdots & 0 & \cdots\ 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots\ \vdots \\ g_{k,1} & \cdots & g_{k,d_1-1} & 0 & g_{k,d_1+1} & \cdots & g_{k,d_2-1} & 0 & g_{k,d_2+1} & \cdots & g_{k,d_k} & \cdots\ 0 \end{bmatrix}, \quad (1)$$

where $g_{i,d_i} = 1$, $g_{j,d_i} = 0$ for $j \neq i$ and $\{d_1, d_2, \ldots, d_k\}$ is the set of k possible RT-weights so that $d = d_1 < d_2 < \ldots < d_k$. In one way, the set of these d_i's *can be thought of an information set for the code C, which is called the "standard information set" of C.*

Any generator matrix of the linear code C is equivalent to G'. This G' is called the generator matrix in standard form. A linear code having G' as its generator matrix in standard form is said to be of type $(d_1, d_2, \ldots, d_k)$.

Remark 1. *One easily observes that, as far as the codes in RT-metric are concerned, appending additional 0's to the right end of the codewords will achieve nothing except an increase in length. Also, it makes the investigation of vital parameters such as the covering radius of the code a trivial exercise. In order to omit the superfluity, throughout this paper, unless otherwise specified, we assume that the code C always contains a codeword with full RT-weight s, where s is the length of the code. That is, the type of C is $(d_1, d_2, \ldots, d_k)$, such that $d_k = s$.*

Remark 2. *From Definition 1, it is clear that, if a linear code C is of type $(d_1, d_2, \ldots, d_k)$, then its RT-weight distribution will be given by*

$$A_0 = 1, A_i = 0, \forall i \notin \{d_1, d_2, d_3, \ldots, d_k\} \quad \textit{and} \quad A_{d_i} = (q-1)q^{i-1}.$$

3.1. On duality of codes

In order to be able to establish MacWilliam's type relations for codes in RT-metric, a special inner product on $Mat_{m\times s}(\mathbb{F}_q)$ is introduced in [6]. This inner product also plays a significant role in the study of codes in RT-metric, for it influences many interesting results (for example, the dual of an MDS code under this inner product is again an MDS code). For $x = (x_1, x_2, \ldots, x_s)$ and $y = (y_1, y_2, \ldots, y_s) \in \mathbb{F}_q^s$, the inner product of x and y is given by

$$\langle x,\ y\rangle = \langle y,\ x\rangle = \sum_{i=1}^{s} x_i y_{s-i+1} (\text{mod q}) \tag{2}$$

Then, the dual $C^{\perp}$ of the code C can be defined as

$$C^{\perp} = \left\{x \in \mathbb{F}_q^s \mid \langle x,\ y\rangle = 0 \text{ for all } y \in C\right\}. \tag{3}$$

An RT-metric code C is said to be self-orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$. It is obvious that the length s of any self-dual code is even.

Definition 3. *Let $A = (a_{ij})$ be a $p \times r$ matrix. Then, the flip of the matrix A, denoted by $Flip\,(A)$, is defined by*

$$Flip\,(A) = (a_{ik}), \tag{4}$$

where $k = r - j + 1$ for $1 \le i \le p$ and $1 \le j \le r$. We denote the transpose of $Flip\,(A)$ as $A^{\diamond}$.

We obtain this flipping of a matrix as follows.

Example 1. *Let A be any $p \times r$ matrix given by*

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,r-1} & a_{1,r} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,r-1} & a_{2,r} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{p-1,1} & a_{p-1,2} & \cdots & a_{p-1,r-1} & a_{p-1,r} \\ a_{p,1} & a_{p,2} & \cdots & a_{p,r-1} & a_{p,r} \end{pmatrix}. \qquad (5)$$

Then, $Flip(A)$ and $A^{\diamond}$ are given by

$$Flip(A) = \begin{pmatrix} a_{1,r} & a_{1,r-1} & \cdots & a_{1,2} & a_{1,1} \\ a_{2,r} & a_{2,r-1} & \cdots & a_{2,2} & a_{2,1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{p-1,r} & a_{p-1,r-1} & \cdots & a_{p-1,2} & a_{p-1,1} \\ a_{p,r} & a_{p,r-1} & \cdots & a_{p,2} & a_{p,1} \end{pmatrix}, \qquad (6)$$

$$A^{\diamond} = \begin{pmatrix} a_{1,r} & a_{2,r} & \cdots & a_{p-1,r} & a_{p,r} \\ a_{1,r-1} & a_{2,r-1} & \cdots & a_{p-1,r-1} & a_{p,r-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{1,2} & a_{2,2} & \cdots & a_{p-1,2} & a_{p,2} \\ a_{1,1} & a_{2,1} & \cdots & a_{p-1,1} & a_{p,1} \end{pmatrix}. \qquad (7)$$

Theorem 2. *Let C be any $[s,k,d]_q$ linear code of type $(d_1, d_2, \ldots, d_k)$. Then, the dual $C^{\perp}$ of C is an $[s, s-k, d^{\perp}]_q$ linear code of type $\left(d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right)$ such that $\left\{d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right\} = [s] \setminus \{s-d_1+1, s-d_2+1, \ldots, s-d_k+1\}$.*

Proof. The generator matrix of C in standard form is

$$G' = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,d_1-1} & g_{1,d_1} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ g_{2,1} & g_{2,2} & \cdots & g_{2,d_1-1} & 0 & g_{2,d_1+1} & \cdots & g_{2,d_2-1} & g_{2,d_2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,d_1-1} & 0 & g_{k,d_1+1} & \cdots & g_{k,d_2-1} & 0 & g_{k,d_2+1} & \cdots & g_{k,d_k} \end{bmatrix} \qquad (8)$$

such that $g_{i,d_i} = 1$, $g_{j,d_i} = 0$ for $j \neq i$ and $d = d_1 < d_2 < \ldots < d_k = s$. We know that

$$C^{\perp} = \left\{x \in \mathbb{F}_q^s |\, \langle c, x\rangle = 0, \forall c \in C\right\},$$

where

$$\langle c, x\rangle = \sum_{i=1}^{s} c_i x_{s-i+1} (\text{mod } q)$$

for $c = (c_1, c_2, \ldots, c_s)$ and $x = (x_1, x_2, \ldots, x_s)$.
This means that $C^{\perp}$ is the solution space of the system

$$Flip\left(G'\right) x^T = 0. \qquad (9)$$

It is obvious that $dim(C^{\perp}) = s - k$. Let $C^{\perp}$ be of type $\left(d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right)$. From (9), one sees that $\left\{d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right\} = [s] \setminus \{s - d_1 + 1, s - d_2 + 1, \ldots, s - d_k + 1\}$. Otherwise, if $d_i^{\perp} = s - d_j + 1$ for some i and j, then there must exist a codeword of RT-weight $s - d_j + 1$ in $C^{\perp}$ and a codeword of RT-weight d_i in C whose inner product is nonzero, contradicting the definition of $C^{\perp}$. Hence, the proof holds. □

Proposition 1. *Let C be any $[s, k, d; R]_q$ RT-metric linear code. Then the covering radius of $C^{\perp}$ is $s - d + 1$ and the minimum distance of $C^{\perp}$ is $s - R + 1$.*

Proof. From Theorem 2, $C^{\perp}$ is of type $\left(d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right)$ such that $\left\{d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right\} = [s] \setminus \{s - d_1 + 1, s - d_2 + 1, \ldots, s - d_k + 1\}$, where $(d_1, d_2, \ldots, d_k)$ is the type of C. If $d_1 = 1$, then $s \notin \left\{d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right\}$ implying the partition number of $C^{\perp}$ to be 0, and hence its covering radius is s. If $d_1 \neq 1$, then the set $\left\{d_1^{\perp}, d_2^{\perp}, \ldots, d_{s-k}^{\perp}\right\}$ contains, $s,\ s-1,\ s-2, \ldots,\ s-d+2$, but not $s-d+1$. This implies that the partition number of $C^{\perp}$ is $d - 1$, and hence its covering radius is $s - d + 1$. As the covering radius of C is R, its partition number is $s - R$. This implies $R+1,\ R+2,\ \ldots,\ s \in \{d_1, d_2, \ldots, d_k\}$, but $R \notin \{d_1, d_2, \ldots, d_k\}$. Thus, $d_1^{\perp} = s - R + 1$. □

Corollary 1. *Let C be any $[s = 2k, k, d; R]_q$ self-dual RT-metric code. Then covering radius of C is $s - d + 1$.*

Proof. From Proposition 1, the covering radius of $C^{\perp}$ is $s - d + 1$. Since C is self-dual (that is, $C = C^{\perp}$), $R = s - d + 1$. □

4. Existence of self-dual codes

Definition 4. *Let us consider the set $[s] = \{1, 2, \ldots, s\}$. Then $a,\ b \in [s]$ are said to be RT-conjugate (or simply, conjugate) to each other if $a = s - b + 1$ (i.e., if $a + b = s + 1$).*

Proposition 2. *Let C be an $[s = 2k, k, d; R]_q$ self-dual RT-metric code of type $(d_1, d_2, \ldots, d_k)$. Then no pair of d_i's is RT-conjugate.*

Proof. Since C is self-dual, $C = C^{\perp}$. Then by Theorem 2,

$$(d_1, d_2, \ldots, d_k) = [s] \setminus \{s - d_1 + 1, s - d_2 + 1, \ldots, s - d_k + 1\}. \tag{10}$$

Hence, the result follows. □

Remark 3. *The above result also holds for self-orthogonal codes, the proof of which follows similar lines as in the proof above.*

Thus, a code of type $(d_1, d_2, \ldots, d_k)$, in which there exist d_i, d_j such that $s - d_i + 1 = d_j$, can never be self-dual or self orthogonal.

Theorem 3. *Let C be any $[s,k,d]_q$ RT-metric code of type $(d_1, d_2, \ldots, d_k)$ with $s = 2k$ and d_i's are not pair-wise conjugate. Let the generator matrix of C in standard form be*

$$G' = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,d_1-1} & g_{1,d_1} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ g_{2,1} & g_{2,2} & \cdots & g_{2,d_1-1} & 0 & g_{2,d_1+1} & \cdots & g_{2,d_2-1} & g_{2,d_2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,d_1-1} & 0 & g_{k,d_1+1} & \cdots & g_{k,d_2-1} & 0 & g_{k,d_2+1} & \cdots & g_{k,d_k} \end{bmatrix},$$

such that $g_{i,d_i} = 1$, $g_{j,d_i} = 0$ for $j \neq i$ and $d = d_1 < d_2 < d_3 < \ldots < d_k = s$. Then C is self-dual if and only if

$$g_{i,s-d_j+1} + g_{j,s-d_i+1} = 0 \ (mod\ q), \ \forall i \ \&\ j$$

Proof. From the definition of a dual of an RT-metric code, the code C is self-dual if and only if $GG^{\diamond} = \mathbf{0}$, where G is any generator matrix of the code C and $G^{\diamond} = [Flip(G)]^{\top}$. Equivalently, $G'(G')^{\diamond} = \mathbf{0}$. That implies

$$\begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,d_1-1} & g_{1,d_1} & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ g_{2,1} & g_{2,2} & \cdots & g_{2,d_1-1} & 0 & g_{2,d_1+1} & \cdots & g_{2,d_2-1} & g_{2,d_2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,d_1-1} & 0 & g_{k,d_1+1} & \cdots & g_{k,d_2-1} & 0 & g_{k,d_2+1} & \cdots & g_{k,d_k} \end{bmatrix}$$

$$\times \begin{bmatrix} 0 & 0 & \cdots & g_{k,d_k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{k,d_2+1} \\ 0 & g_{2,d_2} & \cdots & 0 \\ 0 & g_{2,d_2-1} & \cdots & g_{k,d_2-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & g_{2,d_1+1} & \cdots & g_{k,d_1+1} \\ g_{1,d_1} & 0 & \cdots & 0 \\ g_{1,d_1-1} & g_{2,d_1-1} & \cdots & g_{k,d_1-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{1,2} & g_{2,2} & \cdots & g_{k,2} \\ g_{1,1} & g_{2,1} & \cdots & g_{k,1} \end{bmatrix} = \mathbf{0}.$$

For any i and j,

$$\begin{aligned} & g_{i,s-d_j+1}g_{j,d_j} + g_{i,s-d_j+2}g_{j,d_j-1} + g_{i,s-d_j+3}g_{j,d_j-2} + \cdots + g_{i,d_i-2}g_{j,s-d_i+3} \\ & \quad + g_{i,d_i-1}g_{j,s-d_i+2} + g_{i,d_i}g_{j,s-d_i+1} = 0 \ (\text{mod } q). \end{aligned}$$

In the above sum, we can observe that, for i and j, the summation runs through the product of elements in rows i and j, which are in columns of the generator matrix having conjugate indices, i.e., $g_{i,k}g_{j,s-k+1}$. Moreover, one can also observe that the summation starts and ends with products whose one of the terms involves g_{j,d_j} and

g_{i,d_i}. Now, in each of the intermediate summands, either of the terms involved in the product must correspond to the columns $d_1, d_2, \ldots,$ or d_k, as suggested by the hypothesis regarding the type of the code C. But, nonzero entries in the columns say, d_l are at g_{l,d_l}; and $g_{s,d_l} = 0$ for $s \neq l$. Hence, all the intermediate summands must be equal to 0. Thus we have,

$$g_{i,s-d_j+1} + g_{j,s-d_i+1} = 0, \quad \text{for each } i,j = 1,2,\ldots,k, (\text{since } g_{i,d_i} = 1 = g_{j,d_j}).$$

Hence, the theorem holds. □

Remark 4. *Let C be any code of type $(d_1, d_2, \ldots, d_k)$. From the definition of the standard information set of C, it is clear that the columns $d_1, d_2, \ldots, d_k$ of G form the identity matrix I_k of order k. Let us denote by G_c, the square sub-matrix of G formed by the columns, in the same order, corresponding to the set complement to $\{d_1, d_2, \ldots, d_k\}$. Let us call this matrix G_c a standard complementary matrix of the code. Now, the above theorem can be restated as follows.*

Theorem 4. *Let C be an $[s,k,d]_q$ RT-metric code of type $(d_1, d_2, \ldots, d_k)$ with $s = 2k$ such that no pair of d_i's is conjugate. C is self-dual if and only if the standard complementary matrix G_c of C is such that the mirror images of elements with respect to the anti-diagonal are additive inverses of each other in $\mathbb{F}_q$.*

Example 2 (For a binary self-dual code)**.** *Consider the binary $[8,4,5]$ RT-metric code C_1 with generator matrix G_1 given by the following matrix.*

$$G_1 = \begin{bmatrix} 0&1&1&1&1&0&0&0 \\ 1&0&1&1&0&1&0&0 \\ 1&1&0&1&0&0&1&0 \\ 1&1&1&0&0&0&0&1 \end{bmatrix}.$$

Here, we observe that this generator matrix is in standard form and the code is of type $(5,6,7,8)$. It is easy to verify that $G_1 G_1^{\diamond} = \mathbf{0}$, where $G_1^{\diamond} = [Flip(G_1)]^{\top}$, and also that this code satisfies all the conditions set by Theorem 3 for an RT-metric code to be self-dual. Thus, C_1 is self-dual. When considered as a code in Hamming metric, the code C_1 is actually equivalent to the $[8,4,4]$ extended binary Hamming code $\hat{\mathrm{H}}_3$, obtained from the $[7,4,3]$ binary Hamming code H_3 by adding an overall parity check coordinate to each codeword of H_3. This code is also a self-dual code as far as the Hamming metric is concerned. Thus, this is a typical example of a binary code which is self-dual in both Hamming and RT metrics.

Example 3 (For a ternary self-dual code)**.** *Consider the ternary $[6,3,3]$ RT-metric code C_2 whose generator matrix in standard form G_2 is given by the following matrix.*

$$G_2 = \begin{bmatrix} 2&0&1&0&0&0 \\ 1&0&0&0&1&0 \\ 0&2&0&1&0&1 \end{bmatrix}.$$

This code is of type $(3,5,6)$ and $G_2 G_2^{\diamond} = \mathbf{0}$. It is easy to observe that this code is self-dual according to Theorem 3 and/or Theorem 4.

4.1. Formally self-dual codes

A code whose weight distribution is the same as that of its dual is said to be a formally self-dual code. In fact, a code is formally self-dual if its weight enumerator is invariant under MacWilliams transformations.

From the above definition, one concludes that a code which satisfies the necessary condition for being self-dual is formally self-dual. That is, a code of type $(d_1, d_2, \ldots, d_k)$ is formally self-dual if no pair of d_i's is conjugate to each other.

Proposition 3. *An $[s, k, d]_q$ RT-metric code of type $(d_1, d_2, \ldots, d_k)$ with $s = 2k$ such that no pair of d_i's is conjugate is always formally self-dual.*

Proof. The proof is obvious from the definition of a formally self-dual code and that of the type of a code and from Remark 2 and Theorem 2. □

Corollary 2. *Every MDS $[s, k, d]_q$ code with $s = 2k$ is formally self-dual.*

Proof. Let C be any $[s, k, d]_q$ MDS code with $s = 2k$. Then, by the Singleton bound and by Defintion 2, we observe that C is of type $(k + 1, k + 2, \ldots, s)$. Hence, the proof follows from Proposition 3. □

4.2. Projections and self-duality

Here, by projection of a code on a subset of coordinates we mean that the projection is on the right hand corner; that is, if a code in $\mathbb{F}_q^s$ is projected to $\mathbb{F}_q^{s'}$ with $s \geq s'$, then it is projected to the coordinates $s - s' + 1, s - s' + 2, \ldots, s$. Let P denote the projection of $\mathbb{F}_q^s$ to $\mathbb{F}_q^{s'}$. Then, we can make the following observations regarding the notion of self-duality of the codes in this metric.

- The standard information set of an $[s, k, d]_q$ MDS code is $\{s - k + 1, s - k + 2, \ldots, s\}$. Hence, the projection of an MDS code is not formally self-dual, as some elements in its standard information set lose their conjugates.

- Projection of a code is formally self-dual only if the code is of type $(d_1, d_2, \ldots, d_k)$ such that $d_1, d_2, \ldots, d_{\frac{(s-s')}{2}} \leq (s - s')$.

- If a code C and its projection $P(C)$ are both self-dual, then the codewords in C with weight less than or equal to $s - s'$ are projected on to the zero codeword in $P(C)$.

5. Self-dual codes: constructions

In this section, we give two methods for constructing self-dual codes from two or more self-dual codes of smaller dimensions and lengths.

5.1. Construction - I:

Let C_i be any $[s_i, k_i, d_i]_q$ RT-metric self-dual codes for $i = 1$ and 2 such that $s_i = 2k_i$. Then, $C = \{c_1|c_2|c_1 : c_1 \in C_1 \text{ and } c_2 \in C_2\}$ is an $[s, k, d]_q$ code with $d = d_1$, $k = 2k_1 + k_2$ and $s = 2s_1 + s_2$, which is also self-dual. If G_1 and G_2 are generator matrices of C_1 and C_2, respectively, then the generator matrix of C is given by

$$G = \begin{bmatrix} G_1 & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & G_2 & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & G_1 \end{bmatrix}.$$

Here, the covering radius of C is $s_1 + s_2 + R_1$ where R_1 is the covering radius of C_1.

Example 4. *The example of a binary self-dual code constructed using this method is as follows. Let us consider a $[4, 2, 3]$ binary RT-metric code C_1 and a $[4, 2, 3]$ binary RT-metric code C_2, whose generator matrices G_1 and G_2, respectively, are given as follows:*

$$G_1 = \begin{bmatrix} 1\,0\,1\,0 \\ 1\,1\,0\,1 \end{bmatrix},$$
$$G_2 = \begin{bmatrix} 0\,1\,1\,0 \\ 1\,0\,0\,1 \end{bmatrix}.$$

It is easy to verify that these two codes C_1 and C_2 are self-dual. Now, consider the code C whose generator matrix is given by

$$G = \begin{bmatrix} 1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1 \end{bmatrix}.$$

From the above generator matrix G, we observe that the code C is a $[12, 6, 3]$ code and it satisfies all the conditions discussed in Theorem 3 for it to be self-dual. Hence, this code is self-dual.

5.2. Construction - II:

Let C_i be any $[s_i, k_i, d_i]_q$ RT-metric self-dual codes for $i = 1$ and 2 such that $s_i = 2k_i$. Then, $C' = \left\{a|c_2|b : a, b \in \mathbb{F}_q^{k_1} \text{ with } (a, b) \in C_1 \text{ and } c_2 \in C_2\right\}$ is an $[s, k, d]_q$ code with $k = k_1 + k_2$ and $s = s_1 + s_2$, which is also self-dual. If G_1 and G_2 are generator matrices of C_1 and C_2, respectively, then the generator matrix of C' is given by

$$G' = \begin{bmatrix} G_1' & \mathbf{O} & G_1'' \\ \mathbf{O} & G_2 & \mathbf{O} \end{bmatrix},$$

where

$$G_1 = \left[G_1' \; G_1'' \right],$$

such that G_1' and G_1'' are square matrices of order k_1. Then, the minimum RT-distance of C' is given by

$$d = \begin{cases} d_1, & \text{if } d_1 \leq k_1 \\ k_1 + d_2, & \text{if } d_1 > k_1 \text{ (i.e. if } d_1 = k_1 + 1). \end{cases}$$

And the covering radius of C' is given by

$$R = \begin{cases} s_2 + R_1, & \text{if } R_1 > k_1 \\ R_1 + R_2, & \text{if } R_1 = k_1 \end{cases},$$

where R_i is the covering radius of C_i.

Example 5. *The example of a binary self-dual code constructed using this method is as follows. Let us consider the same codes C_1 and C_2 which are given in Example 4. Now, consider the code C whose generator matrix is given by*

$$G = \begin{bmatrix} 1&0&0&0&0&0&1&0 \\ 1&1&0&0&0&0&0&1 \\ 0&0&0&1&1&0&0&0 \\ 0&0&1&0&0&1&0&0 \end{bmatrix}.$$

Now, this generator matrix G can be expressed in the standard form as

$$G' = \begin{bmatrix} 0&0&0&1&1&0&0&0 \\ 0&0&1&0&0&1&0&0 \\ 1&0&0&0&0&0&1&0 \\ 1&1&0&0&0&0&0&1 \end{bmatrix}.$$

From the above generator matrix in standard form G', it can be easily seen that C is an $[8,4,5]$ code of type $(5,\ 6,\ 7,\ 8)$. Moreover, from G' we observe that the code C satisfies all the conditions discussed in Theorem 3 for it to be self-dual. Hence, this code is self-dual.

Here, one can observe that even if we take the same combination of codes C_1 and C_2 in both examples, the code constructed using the second method has a greater minimum RT-distance. Furthermore, if we take two MDS self-dual codes as constituent codes, we can not construct an MDS self-dual code using Construction-I whereas Construction-II gives us an MDS self-dual code, which is also evident from Examples 4 and 5. Thus, between these two constructions, the second method is efficient as it provides better codes.

6. Conclusion

As an $[s,k]$ linear code in RT-metric has k different possible non-zero weights, we have adapted and modified the definition of the generator matrix in standard form given in [8] to introduce the standard information set for a code. The standard information set for the dual of a code is determined. Given the basic parameters of a linear code, we have obtained the covering radius and minimum distance of its dual. Further, we have established the necessary and sufficient conditions for a code to be self-dual. Formally self-dual codes are discussed and found to be the ones that satisfy the necessary condition for being self-dual. Finally, some constructions for self-dual codes are proposed.

Acknowledgement

The authors thank the referees for their corrective suggestions.

References

[1] S. T. Dougherty, M. M. Skriganov, *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2**(2002), 81–97.

[2] S. T. Dougherty, M. M. Skriganov, *Maximum distance separable codes in the ρ metric over arbitrary alphabets*, J. Algebraic Combin. **16**(2002), 71–81.

[3] S. Jain, *Bursts in m-metric array codes*, Linear Algebra Appl. **418**(2006), 130–141.

[4] S. Jain, CT *bursts – from classical to array coding*, Discrete Math. **308**(2008), 1489–1499.

[5] K. Lee, *The automorphism group of a linear space with the Rosenbloom-Tsfasman metric*, European J. Combin. **24**(2003), 607–612.

[6] W. J. Martin, D. R. Stinson, *Association schemes for ordered orthogonal arrays and (T, M, S)-nets*, Canad. J. Math. **51**(1999), 326–346.

[7] H. Niederreiter, A. Winterhof, *Coding theory, in: Applied number theory*, Springer, Berlin, 2015.

[8] M. Ozen, I. Siap, *On the structure and decoding of linear codes with respect to the Rosenbloom-Tsfasman metric*, Selçuk J. Appl. Math. **5**(2004), 25–31.

[9] M. Ozen, I. Siap, *Linear codes over $\mathbb{F}_q[u]/(u^s)$ with respect to the Rosenbloom-Tsfasman metric*, Des. Codes Cryptogr. **38**(2006), 17–29.

[10] M. Ozen, I. Siap, *Codes over Galois rings with respect to the Rosenbloom-Tsfasman metric*, J. Franklin Inst. **344**(2007), 790–799.

[11] L. Panek, E. Lazzarotto, F. M. Bando, *Codes satisfying the chain condition over Rosenbloom-Tsfasman spaces*, Int. J. Pure Appl. Math. **48**(2008), 217–222.

[12] J. Quistorff, *On Rosenbloom and Tsfasman's generalization of the Hamming space*, Discrete Math. **307**(2007) 2514–2524.

[13] E. M. Rains, N. J. A. Sloane, *Self-dual codes, in: Handbook of coding theory*, Volumes I, II, North-Holland, Amsterdam, 1998.

[14] M. Yu. Rosenbloom, M. A. Tsfasman, *Codes for the m-metric*, Probl. Inf. Transm. **33**(1997), 45–52.

[15] R. S. Selvaraj, V. Marka, *On normal q-ary codes in Rosenbloom-Tsfasman metric*, ISRN Combinatorics **2014**, Article ID 237915, 5 pp.

[16] A. K. Sharma, A. Sharma, *MacWilliams identities for weight enumerators with respect to the RT metric*, Discrete Math. Algorithms Appl. **6**(2014), Article ID 1450030, 11 pp.

[17] I. Siap, *CT burst error weight enumerator of array codes*, Albanian J. Math. **2**(2008), 171–178.

[18] I. Siap, M. Ozen, *The complete weight enumerator for codes over $M_{n\times s}(R)$*, Appl. Math. Lett. **17**(2004), 65–69.

[19] M. M. Skriganov, *Coding theory and uniform distributions*, Algebra i Analiz **13**(2001), 191–239.

[20] B. Yildiz, I. Siap, T. Bilgin, G. Yesilot, *The covering problem for finite rings with respect to the RT-metric*, Appl. Math. Lett. **23**(2010), 988–992.