Multi-covering Radius for Rank Metric Codes

W. B. Vasantha
Department of Mathematics
Indian Institute of Technology Madras
Chennai - 600 036, India
vasantha@iitm.ac.in

R. S. Selvaraj*
Department of Mathematics
National Institute of Technology Warangal
Warangal - 506 004, India
rsselva@nitw.ac.in

Submitted: Dec 10, 2008; Accepted: Nov 29, 2009; Published: Dec 8, 2009
Mathematics Subject Classifications: 94B65, 94B75, 05B40, 11H31, 15A03

Abstract

The results of this paper are concerned with the multi-covering radius, a generalization of covering radius, of Rank Distance (RD) codes. This leads to greater understanding of RD codes and their distance properties. Results on multi-covering radii of RD codes under various constructions are given by varying the parameters. Some bounds are established. A relationship between multi-covering radii of an RD code and that of its ambient space is also found. The classical sphere bound is generalized.

1 Introduction

The concept of covering radius has been the subject of hundreds of papers. [2, 3] can be referred for a comprehensive survey and thorough bibliography on the subject. In this paper, simultaneous coverings of m-tuples of vectors, rather than single vector, are investigated for codes over the Galois field $\mathbb{F}_{2^N}$ defined with rank metric. The notion of multi-covering radius, a generalization of the covering radius, was introduced by Andrew Klapper [8] for binary codes with Hamming metric to study the existence of stream ciphers secured against a large class of attacks.

Here, for the first time study of multi-covering radius for codes with a non-Hamming metric, namely rank metric is carried out. Recall that an RD code [5] of length n is a subset of $\mathbb{F}^n_{q^N}$ (where $n \leqslant N$ and $N > 1$, q being a power of a prime) wherein the weight(rank norm) of each vector is defined to be the maximum number of its coordinates that are linearly independent, and the corresponding metric induced by this norm is called

*Thanks to Council of Scientific and Industrial Research(CSIR), India, for its financial support in carrying out this work

the rank metric. If m is a positive integer, then the multi-covering radius or m-covering radius $t_m(C)$ of a block code C of length n is the smallest integer t such that every set of m vectors in the ambient space is contained in, at least one ball of radius t around a codeword in C. Thus multi-covering radius is a natural generalization of the classical notion of covering radius, which is exactly the case when $m = 1$. The notion of multi-covering radius makes sense over any alphabet; however, here attention is restricted to codes over $\mathbb{F}_{2^N}$.

The notion of multi-covering radius arose from investigations concerning the crypt-analysis of stream ciphers [6]. This paper is in search of RD codes with least cardinality for a given length n and multi-covering radius t. Beyond that, multi-covering radii are interesting in their own right as natural generalizations of the covering radius. Understanding it is likely to lead to a greater understanding of codes in general.

In this section, some basic notations and terminology needed for further discussions are given. In the next section, some basic properties and relations are discussed by varying the parameters for multi-covering radii. Section III establishes various bounds for m-covering radius including a relationship between m-covering radius of an RD code and that of its ambient space. The generalization of classical sphere bound is given in section IV. Final section gives the conclusions and future directions.

Let $\mathbb{F}_{2^N}$ denote a finite field of 2^N elements, $N > 1$ and V^n be an n-dimensional vector space over $\mathbb{F}_{2^N}$, $n \leqslant N$. That is, $V^n = \mathbb{F}_{2^N}^n$. Rank weight of any vector $x = (x_1, x_2, \dots, x_n) \in V^n$ is defined as the maximum number of its coordinates that are linearly independent, and is denoted as $r(x)$. For $x, y \in V^n$, $d_R(x, y) = r(x - y)$, the rank distance between x and y. This is the maximum number of coordinates of $x - y$ that are linearly independent over $\mathbb{F}_2$. Any subset C of $\mathbb{F}_{2^N}^n$ equipped with the above rank metric is called as a Rank Distance (RD) code.

The weight of a set $S \subseteq V^n$, is defined as $max\{r(x) : x \in S\}$ and is denoted by $wt(S)$. If $S \subseteq V^n$, then $d_R(x, S) = \ min\ \{d_R(x, y) : y \in S\}$. The covering radius of x for S is $cov(x, S) = max\{d_R(x, y) : y \in S\}$. The covering radius of a code C for S is $cov(C, S) = min\{cov(c, S) : c \in C\}$. Thus, the m-covering radius of C is $max\{cov(C, S) : S \subseteq V^n, |S| = m\}$.

As an example, consider a linear RD code $C = \big\{(0, 0), (1, \alpha^2), (\alpha, 1), (\alpha^2, \alpha)\big\}$ over $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 = \alpha + 1$. Clearly, covering radius of C is 1 i.e., $t_1(C) = 1$ as each vector in the ambient space V^2 can be covered within radius 1 by at least one codeword in C. But 2-covering radius of C is not equal to 1; for, if $S = \{(\alpha^2, 0), (1, \alpha^2)\}$, there does not exist a $c \in C$ such that $cov(c, S) = 1$; hence $cov(C, S) = 2$ implying $t_2(C) = 2$.

Here is an alternate definition of m-covering radius: let $S = \{v_1, v_2, \dots, v_m\}$ be a set of m-vectors. Then, for a $c \in C$, $cov(C, S) = cov(C, S + c)$ where $S + c = \{x + c : x \in S\}$. Consider

$$S +_m C = \{S + c : c \in C\},$$

the collection of all translates of S by elements of C. A translate leader is an m-tuple

$T \in S +_m C$ such that $wt(T)$ is minimal. The m-covering radius of C is the weight of the maximal weight translate leader.

Gaussian coefficient (also known as q-binomial coefficient, here q being 2) is given by

$$\begin{bmatrix} n \\ m \end{bmatrix} = \frac{(2^n-1)(2^n-2)\cdots(2^n-2^{m-1})}{(2^m-1)(2^m-2)\cdots(2^m-2^{m-1})},$$

which gives the number of m-dimensional subspaces of an n-dimensional vector space over the field $\mathbb{F}_2$. The number of vectors of length n whose rank norm is i is given by

$$L_i(n) = \begin{bmatrix} n \\ i \end{bmatrix} (2^N-1)(2^N-2)\cdots(2^N-2^{i-1}).$$

For any $x \in V^n$, $B_t(x) = \{y \in V^n : d_R(x,y) \leqslant t\}$ is said to be the *rank sphere* of radius t with center x, and $S_i(x) = \{y \in V^n : d_R(x,y) = i\}$ is called as the i^{th} *surface of the rank sphere* with center at x. Let $V(n,t) = |B_t(x)|$. Clearly, $|S_i(x)| = L_i(n)$ so that $V(n,t) = \sum_{i=0}^{t} L_i(n)$.

Let $[n,k,d]$ stand for a linear RD code of length n, dimension k and minimum distance d. Let $[n,k]$ stand for a linear RD code of length n and dimension k, and (n,K) for an RD code of length n and cardinality K. Let $t_m(C)$ denote m-covering radius of an RD code C, $t_m[n,k]$, the smallest m-covering radius among all $[n,k]$ codes, $t_m(n,K)$, the smallest m-covering radius among all (n,K) codes, $k_m[n,t]$, the smallest dimension of linear RD codes of length n and m-covering radius t and $K_m(n,t)$, the least cardinality of RD codes of length n and m-covering radius t.

2 Basic Properties of m-Covering Radius

Certain basic relations (as in [8]) hold with varying the parameters for m-covering radii. The proofs are straightforward.

Proposition 2.1. If C_1 and C_2 are RD codes with $C_1 \subseteq C_2$, then $t_m(C_1) \geqslant t_m(C_2)$.

Proof: Let $S \subseteq V^n$ with $|S| = m$.

$$\begin{aligned} cov(C_2, S) &= min\{cov(x,S) : x \in C_2\} \\ &\leqslant min\{cov(x,S) : x \in C_1\} \\ &= cov(C_1, S) \\ \text{Thus,}\ \ t_m(C_2) &\leqslant t_m(C_1). \end{aligned}$$

□

Proposition 2.2. For any RD code C and a positive integer m, $t_m(C) \leqslant t_{m+1}(C)$.

Proof:

$$\begin{aligned} t_m(C) &= max\{cov(C,S) : S \subseteq V^n,\ |S| = m\} \\ &\leqslant max\{cov(C,S) : S \subseteq V^n,\ |S| = m+1\} \\ &= t_{m+1}(C). \end{aligned}$$

□

Proposition 2.3. For any set of positive integers n, m, k and K, $t_m[n,k] \leqslant t_{m+1}[n,k]$ and $t_m(n,K) \leqslant t_{m+1}(n,K)$.

Proof:
$$\begin{aligned} t_m[n,k] &= min\{t_m(C) : C \subseteq V^n,\ dim\ C = k\} \\ &\leqslant min\{t_{m+1}(C) : C \subseteq V^n,\ dim\ C = k\} \\ &= t_{m+1}[n,k]. \end{aligned}$$

Similarly, $t_m(n,K) \leqslant t_{m+1}(n,K)$.
That is,

$$\begin{aligned} t_m(n,K) &= min\{t_m(C) : C \subseteq V^n,\ |C| = K\} \\ &\leqslant min\{t_{m+1}(C) : C \subseteq V^n,\ |C| = K\} \\ &= t_{m+1}(n,K). \end{aligned}$$ □

Proposition 2.4. For any set of positive integers n, m, k and K, $t_m[n,k] \geqslant t_m[n,k+1]$ and $t_m(n,K) \geqslant t_m(n,K+1)$.

Proof:
$$\begin{aligned} t_m[n,k+1] &= min\{t_m(C) : C \subseteq V^n,\ dim\ C = k+1\} \\ &\leqslant min\{t_m(C) : C \subseteq V^n,\ dim\ C = k\} \\ &\quad (\because \text{for each } C_1 \subseteq C_2, t_m(C_2) \leqslant t_m(C_1)) \\ &= t_m[n,k]. \end{aligned}$$

Similarly, $t_m(n,K+1) \leqslant t_m(n,K)$. □

Using these results and the definition of $k_m[n,t]$ and $K_m(n,t)$, the following results are immediate.

Proposition 2.5. For any set of positive integers n, m and t, $k_m[n,t] \leqslant k_{m+1}[n,t]$ and $K_m(n,t) \leqslant K_{m+1}(n,t)$. □

Proposition 2.6. For any set of positive integers n, m and t, $k_m[n,t] \geqslant k_m[n,t+1]$ and $K_m(n,t) \geqslant K_m(n,t+1)$. □

Thus, the m-covering radius of a fixed RD code C, $t_m[n,k]$, $t_m(n,K)$, $k_m[n,t]$ and $K_m(n,t)$ are non-decreasing functions of m, and hold for any arbitrary metric as evident from the proofs.

The relationship between the multi-covering radii of two RD codes and codes that are built from them are given. For $i = 1, 2$, let C_i be an $[n_i, k_i, d_i]$ RD code over $\mathbb{F}_{2^N}$ with $n_1, n_2, n_1 + n_2 \leqslant N$.

Proposition 2.7. Let $C = C_1 \times C_2 = \{(x|y) : x \in C_1, y \in C_2\}$. Then C is a $[n_1+n_2, k_1+k_2, min\{d_1,d_2\}]$ Rank Distance code over $\mathbb{F}_{2^N}$ and $t_m(C) \leqslant t_m(C_1) + t_m(C_2)$.

Proof: Let $S \subseteq V^{n_1+n_2}$ and $S = \{s_1, s_2, \ldots, s_m\}$ with $s_i = (x_i|y_i)$, $x_i \in V^{n_1}$, $y_i \in V^{n_2}$. Let $S_1 = \{x_1, x_2, \ldots, x_m\}$ and $S_2 = \{y_1, y_2, \ldots, y_m\}$. Now, $t_m(C_1)$ being the m-covering radius of C_1, there exists a $c_1 \in C_1$ such that $S_1 \subseteq B_{t_m(C_1)}(c_1)$. This implies $r(x_i + c_1) \leqslant t_m(C_1)$, $\forall\ x_i \in S_1$. Similarly, there exists a $c_2 \in C_2$ such that $S_2 \subseteq B_{t_m(C_2)}(c_2)$. This implies $r(y_i + c_2) \leqslant t_m(C_2)$, $\forall\ y_i \in S_2$. Now, $c = (c_1|c_2) \in C$. Hence,

$$\begin{aligned} r(s_i + c) &= r((x_i|y_i) + (c_1|c_2)) \\ &= r(x_i + c_1 \mid y_i + c_2) \\ &\leqslant r(x_i + c_1) + r(y_i + c_2) \\ &\leqslant t_m(C_1) + t_m(C_2), \quad \text{for all } s_i \in S. \end{aligned}$$

Thus, $t_m(C) \leqslant t_m(C_1) + t_m(C_2)$. □

When $m = 1$, this inequality becomes an equality in the case of Hamming metric (see [2, 3, 8]). As rank distance between any two n-tuples is less than or equal to their Hamming distance, the above inequality does not need to be an equality when $m = 1$, in the case of rank metric codes. For, if $(x|y) \in V^{n_1+n_2}$ such that $x \in V^{n_1}$ and $y \in V^{n_2}$, then there exists $c_1 \in C_1$ and $c_2 \in C_2$ such that $d(x, c_1) = t_1(C_1)$ and $d(y, c_2) = t_1(C_2)$. So, in line with the above proof, Hamming weight of $(x + c_1|y + c_2)$ equals the sum of the Hamming weights of $x + c_1$ and $y + c_2$. But the rank weight of $(x + c_1|y + c_2)$ is less than or equal to the sum of the rank weights of $x + c_1$ and $y + c_2$.

For any positive integer r, the r-fold repetition of a $[n, k, d]$ RD code C is the code $C_{(r)} = \{(c \mid c \mid \ldots \mid c) : c \in C\}$, where the codeword c is concatenated r times. This is a $[rn, k, d]$ Rank Distance code. Note that, here $n \leqslant N$ is chosen so that $rn \leqslant N$. The following proposition establishes the m-covering radius of this r-fold repetition code.

Proposition 2.8. For an r-fold repetition RD code $C_{(r)}$, $t_m(C_{(r)}) \geqslant t_m(C)$.

Proof: Let $S = \{v_1, v_2, \ldots, v_m\} \subseteq V^n$ such that $cov(C, S) = t_m(C)$. Now, let $v'_i = (v_i|v_i|\ldots|v_i)$. Let $S' = \{v'_1, v'_2, \ldots, v'_m\}$ be a set of m vectors of length rn each. An r-fold repetition of any RD codeword retains the same rank weight. Hence, $cov(C_{(r)}, S')$ $= t_m(C)$. Since $t_m(C_{(r)}) \geqslant cov(C_{(r)}, S')$, the result follows. □

This result is different from that for codes with Hamming metric [8] due to the fact that r-fold repetition of any RD codeword retains the same rank weight and hence the distance.

3 Multi-covering Bounds

The m-covering radius $t_m(C)$ is a non-decreasing function of m due to *Proposition 2.2*. Thus, a lower bound for $t_m(C)$ implies a bound for $t_{m+1}(C)$. The first bound in this section shows that for $m \geqslant 2$, the situation for m-covering radii is quite different from that for ordinary covering radii [14].

Proposition 3.1. If $m \geqslant 2$, then the m-covering radius of an RD code of length n is at least $\left\lceil \frac{n}{2} \right\rceil$.

Proof: Let $m = 2$. Let t be the 2-covering radius of an RD code C. Let $x \in V^n$. Choose $y \in V^n$ such that all the n coordinates of $x - y$ are linearly independent, i.e., $d_R(x, y) = n$. Then, for any $c \in C$, $d_R(x, c) + d_R(c, y) \geqslant d_R(x, y) = n$. This implies that one of $d_R(x, c)$ and $d_R(c, y)$ is at least $n/2$ and hence, $t \geqslant \left\lceil \frac{n}{2} \right\rceil$. Since t is nondecreasing function of m, it follows that $t_m(C) \geqslant \left\lceil \frac{n}{2} \right\rceil$ for $m \geqslant 2$. □

The above result is true for any metric d with respect to which the maximum distance (diameter) of the code equals n. If the diameter of a code is, say Δ, then $t_2(C) \geqslant \left\lceil \frac{\Delta}{2} \right\rceil$; for, if $x, y \in V^n$ be such that $d(x, y) = \Delta$, then for any $c \in C$, $d(x, c) + d(c, y) \geqslant d(x, y) = \Delta$ which implies that one of $d(x, c)$ and $d(c, y)$ is at least $\frac{\Delta}{2}$. Thus, $t_m(C) \geqslant \left\lceil \frac{\Delta}{2} \right\rceil$ for $m \geqslant 2$, where Δ is the maximum distance of the code C.

Bounds on the multi-covering radius of V^n can be used to obtain bounds on the multi-covering radii of arbitrary codes. Thus, a relationship between m-covering radius of an RD code and that of its ambient space V^n is established.

Theorem 3.2. Let C be any RD code of length n over $\mathbb{F}_{2^N}$. Then for any positive integer m, $t_m(C) \leqslant t_1(C) + t_m(V^n)$.

Proof: Let $S \subseteq V^n$ with $|S| = m$. Then, there exists $u \in V^n$ such that $cov(u, S) \leqslant t_m(V^n)$. Also, there is a $c \in C$ such that $d_R(c, u) \leqslant t_1(C)$. Now,

$$\begin{aligned} cov(c, S) &= max\{d_R(c, y) : y \in S\} \\ &\leqslant max\{d_R(c, u) + d_R(u, y) : y \in S\} \\ &= d_R(c, u) + cov(u, S) \\ &\leqslant t_1(C) + t_m(V^n). \end{aligned}$$

Thus, for every $S \subseteq V^n$ with $|S| = m$, one can find a $c \in C$ such that $cov(c, S) \leqslant t_1(C) + t_m(V^n)$. Since $cov(C, S) = min\{cov(a, S) : a \in C\} \leqslant t_1(C) + t_m(V^n)$ for any $S \subseteq V^n$ with $|S| = m$, it follows that, $t_m(C) = max\{cov(C, S) : S \subseteq V^n, |S| = m\} \leqslant t_1(C) + t_m(V^n)$. □

Proposition 3.3. For any integer $n \geqslant 2$, $t_2(V^n) \leqslant n - 1$, where $V^n = \mathbb{F}_{2^N}^n$, $n \leqslant N$.

Proof: Let $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in V^n$. Let $u \in V^n$ be such that $u = (x_1, u_2, u_3, \ldots, u_{n-1}, y_n)$. This u covers x and y within radius $n-1$ as $d_R(u, x) \leqslant n-1$ and $d_R(u, y) \leqslant n-1$. Thus, for any pair of vectors $x, y \in V^n$, there always exists a vector namely u, which covers x and y within radius $n-1$. Hence, $t_2(V^n) \leqslant n-1$. □

The above proposition can be improved to $t_2(V^n) \leqslant \lceil \frac{n}{2} \rceil$, by taking for u the vector that agrees with x in the $\lceil \frac{n}{2} \rceil$ leftmost positions, and with y in the $\lfloor \frac{n}{2} \rfloor$ rightmost positions. In the same way, it can be shown that $t_m(V^n) \leqslant n - \lfloor \frac{n}{m} \rfloor$ for any $m \leqslant n$. Hence,

Proposition 3.4.
(1) $t_2(V^n) \leqslant \lceil \frac{n}{2} \rceil$ for $n \geqslant 2$.
(2) $t_m(V^n) \leqslant n - \lfloor \frac{n}{m} \rfloor$ for any $m \leqslant n$. □

The following example illustrates m-covering radius of RD codes.

Example 3.5. Consider the Galois field $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 = \alpha + 1$. Then,

$$\begin{aligned} V^2 &= \mathbb{F}_{2^2}^2 \\ &= \big\{(0,0),(0,1),(0,\alpha),(0,\alpha^2),(1,0),(1,1),(1,\alpha),(1,\alpha^2),(\alpha,0),(\alpha,1),(\alpha,\alpha), \\ &\quad (\alpha,\alpha^2),(\alpha^2,0),(\alpha^2,1),(\alpha^2,\alpha),(\alpha^2,\alpha^2)\big\}. \end{aligned}$$

(a) Clearly, $t_2(V^2) = 1$.

(b) Consider a non-linear RD code (2, 3) of length 2 and cardinality 3: $\big\{(0,0),(1,\alpha),(\alpha,1)\big\}$. It has 1-covering radius 1.

(c) Consider a non-linear RD code (2, 7) of cardinality 7: $\big\{(0,0),(0,1),(1,0),(0,\alpha),(\alpha,0),(\alpha,\alpha),(\alpha^2,\alpha^2)\big\}$. It has 2-covering radius 1.

(d) Consider a $[2,1]$ repetition RD code $C_r = \big\{(0,0),(1,1),(\alpha,\alpha),(\alpha^2,\alpha^2)\big\}$ over $\mathbb{F}_{2^2}$, whose generator matrix is $G = \begin{bmatrix} 1 & 1 \end{bmatrix}$. Clearly, $t_1(C_r) = 1$. But $t_2(C_r) = 2$; for, if $S = \{(0,1),(\alpha,\alpha^2)\}$, $cov(C_r, S) = 2$.

(e) All $[2,1,1]$ RD codes and $[2,1,2]$ RD codes have ordinary covering radius as 1 and 2-covering radius as 2. For $C_2 = [2,2,1]$ RD code, i.e., for the ambient space V^2, $t_1(V^2) = 0$, $t_2(V^2) = 1$, $t_3(V^2) = 1$; but $t_4(V^2) = 2$, as $cov(V^2, S) = 2$ if $S = \{(0,1),(\alpha,\alpha^2),(1,\alpha^2),(\alpha^2,1)\}$. Hence, $k_1[2,1] = 1$, $k_2[2,1] = 2$, $k_3[2,1] = 2$, and $k_4[2,1]$ is *undefined*. Moreover, note that $k_1[2,2] = 0$ and $k_2[2,2] = 0$, by considering the code $C = \big\{(0,0)\big\}$.

(f) Consider $\mathbb{F}_{2^3} = \big\{0, 1, \beta, \beta^2, \ldots, \beta^6\big\}$, where $\beta^3 = \beta + 1$. Now $V^3 = \mathbb{F}_{2^3}^3$. Consider the $C_4 = [3,1,3]$ RD code over $\mathbb{F}_{2^3}$, whose parity check matrix is $H = \begin{bmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta^4 \end{bmatrix}$. Thus, $C_4 = \{(0,0,0),(1,\beta,\beta^4),(\beta,\beta^2,\beta^5),(\beta^2,\beta^3,\beta^6),(\beta^3,\beta^4,1),(\beta^4,\beta^5,\beta),(\beta^5,\beta^6,\beta^2),(\beta^6,1,\beta^3)\}$. C_4 is a maximum Rank Distance code (as $d = n - k + 1 = 3$), and hence $t_1(C_4) = n - k = 2$ (see [14]). Moreover, $t_2(C_4) = 3$; for, if $S = \{(1,\beta,\beta^2),(\beta^3,\beta^4,1)\}$, then $cov(C_4, S) = 3$. Thus, $t_m(C_4) = 3$ for all $m \geqslant 2$.

(g) Consider the $C_5 = [3,2,2]$ RD code over $\mathbb{F}_{2^3}$, whose parity check matrix is $H = \begin{bmatrix} 1 & \beta & \beta^2 \end{bmatrix}$. As C_5 is a maximum Rank Distance code, $t_1(C_5) = 1$. Moreover, one can see that $t_2(C_5) = 2$, $t_3(C_5) = 2$, and $t_4(C_5) = 3$. □

4 Generalized Sphere Covering Bound

A natural question is, for a given t, m and n, what is the smallest RD code whose m-covering radius is at most t? As it turns out, even for $m \geqslant 2$, it is necessary that t be at least $\frac{n}{2}$. In fact, the minimal t for which such a code exists is the m-covering radius of V^n. Various extremal values associated with this notion are $t_m(V^n)$, the smallest m-covering radius among length n RD codes; $t_m(n, K)$, the smallest m-covering radius among all (n, K) RD codes; $K_m(n, t)$, the smallest cardinality of a length n RD code with m-covering radius t, and so on. It is the latter quantity that is studied in this section.

Now, from *Proposition 3.1*, $K_m(n, t)$ is undefined if $t < \frac{n}{2}$. When this is the case, it is accepted to say $K_m(n, t) = \infty$. There are other circumstances when $K_m(n, t)$ is undefined. For example, $K_{2^{Nn}}(n, n-1) = \infty$. Also, $K_m(n, t) = \infty$, if $m > V(n, t)$, since in this case no ball of radius t covers any set of m distinct vectors. More generally, one has the fundamental issue of whether $K_m(n, t)$ is finite for given n, m and t. This is the case if and only if $t_m(V^n) \leqslant t$, since $t_m(V^n)$ lower bounds the m-covering radii of all other codes of dimension n. When $t = n$, every codeword covers every vector, so a code of size 1 will m-cover V^n for every m. Thus $K_m(n, n) = 1$, for every m.

What happens for $K_m(n, t)$, when t is $n-1$? When $m = 1$, $K_1(n, n-1) \leqslant 1 + L_n(n)$; For, $\overline{0} = (0, 0, \ldots, 0)$ will cover all vectors of rank norm less than or equal to $n-1$ within radius $n-1$. That is, $\overline{0}$ will cover all norm-$(n-1)$ vectors within radius $n-1$. Hence, remaining vectors are rank-n vectors. Thus, $\overline{0}$ and these rank-n vectors can cover the ambient space within radius $n-1$. Therefore, $K_1(n, n-1) \leqslant 1 + L_n(n)$.

Proposition 4.1. For any RD code of length n over $\mathbb{F}_{2^N}$,

$$K_m(n, n-1) \leqslant mL_n(n) + 1,$$

provided m is such that $mL_n(n) + 1 \leqslant |V^n|$.

Proof: Consider an RD code C such that $|C| = mL_n(n) + 1$. Each vector in V^n has $L_n(n)$ rank complements, that is, from each vector $v \in V^n$, there are $L_n(n)$ vectors at rank distance n. This means, for any set $S \subseteq V^n$ of m vectors, there always exists a $c \in C$, which covers S within rank distance $n-1$. Thus, $cov(c, S) \leqslant n-1$, which implies, $cov(C, S) \leqslant n-1$. Hence, $K_m(n, n-1) \leqslant mL_n(n) + 1$. □

By bounding the number of m-sets that can be covered by a given codeword, one obtains a straight forward generalization of the classical sphere bound.

Theorem 4.2. (*Generalized Sphere Bound for RD Codes*)
For any (n, K) RD code C,

$$K \binom{V(n, t_m(C))}{m} \geqslant \binom{2^{Nn}}{m}.$$

Hence, for any n, t and m,

$$K_m(n,t) \geqslant \frac{\begin{pmatrix} 2^{Nn} \\ m \end{pmatrix}}{\begin{pmatrix} V(n,t) \\ m \end{pmatrix}}$$

where $V(n,t) = \sum_{i=0}^{t} L_i(n)$, number of vectors in a sphere of radius t and $L_i(n)$ is the number of vectors in V^n whose rank norm is i.

Proof: Each set of m-vectors in V^n must occur in a sphere of radius $t_m(C)$ around at least one codeword. Total number of such sets is $|V^n|$ *choose* m, where $|V^n| = 2^{Nn}$. The number of sets of m-vectors in a neighborhood of radius $t_m(C)$ is $V(n, t_m(C))$ *choose* m. There are K codewords. Hence

$$K \begin{pmatrix} V(n,t_m(C)) \\ m \end{pmatrix} \geqslant \begin{pmatrix} 2^{Nn} \\ m \end{pmatrix}.$$

Thus, for any n, t and m

$$K_m(n,t) \geqslant \frac{\begin{pmatrix} 2^{Nn} \\ m \end{pmatrix}}{\begin{pmatrix} V(n,t) \\ m \end{pmatrix}}. \qquad \square$$

Corollary 4.3. If $\begin{pmatrix} 2^{Nn} \\ m \end{pmatrix} > 2^{Nn} \begin{pmatrix} V(n,t) \\ m \end{pmatrix}$, then $K_m(n,t) = \infty$.

But, converse of *Corollary 4.3* is not true. That is, if $K_m(n,t) = \infty$, one cannot say

$$\begin{pmatrix} 2^{Nn} \\ m \end{pmatrix} > 2^{Nn} \begin{pmatrix} V(n,t) \\ m \end{pmatrix}.$$

For example, take $N = 2$, $n = 2$, $m = 4$, $t = 1$. Clearly, $K_4(2,1) = \infty$ as it is not possible to get a least set in V^2 such that 4-covering radius is 1 (which is clear from *Example 3.5(e)*). But $\begin{pmatrix} 2^{Nn} \\ m \end{pmatrix} = \begin{pmatrix} 2^4 \\ 4 \end{pmatrix} = 1820$ and $2^4 \begin{pmatrix} V(2,1) \\ 4 \end{pmatrix} = 16 \times \begin{pmatrix} 10 \\ 4 \end{pmatrix} = 16 \times 210 = 3360$. Hence, the converse of *Corollary 4.3* is not true.

The generalized sphere bound is true for any alphabet. For an (n, K) RD code C over $\mathbb{F}_{q^N}$ where q is any prime power,

$$K \begin{pmatrix} V(n,t_m(C)) \\ m \end{pmatrix} \geqslant \begin{pmatrix} q^{Nn} \\ m \end{pmatrix}.$$

For a linear $[n,k]$ RD code C over $\mathbb{F}_{q^N}$, the generalized sphere bound becomes

$$q^{Nk}\binom{V(n,t_m(C))}{m} \geqslant \binom{q^{Nn}}{m}$$

$$\text{i.e.,}\quad k \geqslant \frac{1}{N}\log_q \frac{\binom{q^{Nn}}{m}}{\binom{V(n,t_m(C))}{m}}.$$

$$\text{i.e.,}\quad k_m[n,t] \geqslant \frac{1}{N}\log_q \frac{\binom{q^{Nn}}{m}}{\binom{V(n,t)}{m}}.$$

Now, how the generalized sphere bound works is given. It says

$$K_m(n,t) \geqslant \frac{\binom{2^{Nn}}{m}}{\binom{V(n,t)}{m}}, \text{ where } V(n,t) = \sum_{i=0}^{n} L_i(n).$$

For $N = n = 2$, one has $K_1(2,1) = 3$, $K_2(2,1) = 6$, $K_3(2,1) = 13$, and $K_4(2,1)$ as undefined. By using generalized sphere bound, one can get $K_1(2,1) \geqslant 1.6$, $K_2(2,1) \geqslant 2.67$, $K_3(2,1) \geqslant 4.67$, and $K_4(2,1) \geqslant 8.67$. This clearly shows that the generalized sphere bound is not sharp. By taking into account some of the overlap between spheres of radius t, the improvement over the generalized sphere bound for RD codes can be achieved.

5 Conclusion

A generalization to the covering radius problem, namely, multi-covering radius is defined for RD codes to get greater understanding of RD codes and its distance properties. Results on multi-covering radii of RD codes under various constructions are given by varying the parameters. Various multi-covering bounds are established including the generalization of classical sphere bound for RD codes. The problem of improving the lower bound for $K_m(n,t)$ is open.

Acknowledgements: The authors would like to thank the anonymous referee whose comments and suggestions have improved both the results and the presentation of the paper. Thanks are also due to Prof. Ludo M. G. M. Tolhuizen whose valuable comments and inputs are noteworthy.

References

[1] Cary Huffman W., Vera Pless: Fundamentals of error-correcting codes. Cambridge University Press, UK (2003).

[2] Cohen G. D., Karpovsky M. G., Mattson H. F. Jr., Schatz Y. R.: Covering radius - survey and recent results. IEEE Trans. Inform. Theory, 31, 328 - 343 (1985).

[3] Cohen G. D., Litsyn S. N., Lobstein A. C., Mattson H. F. Jr.: Covering radius 1985 - 1994. Appl. Algebra Engrg. Comm. Comput., 8, 173 - 239 (1997).

[4] Delsarte P.: Four fundamental parameters of a code and their combinatorial significance. Inform. and Control, 23, 407 - 438 (1973).

[5] Gabidulin E. M.: Theory of codes with maximum rank distance. Probl. Inf. Transm., 21, 1 - 12 (1985).

[6] Honkala I., Klapper A.: Bounds for the multicovering radii of Reed-Muller codes with applications to stream ciphers. Des. Codes Cryptogr. 23, 131 - 145 (2001).

[7] Ian F. Blake, Ronald C. Mullin: An Introduction to algebraic and combinatorial coding theory. Academic Press, London (1976).

[8] Klapper A.: The multicovering radii of codes. IEEE Trans. Inform. Theory, 43, 1372 - 1377 (1997).

[9] Klapper A.: Improved lower bounds for multicovering codes. IEEE Trans. Inform. Theory, 45, 2532 - 2534 (1999).

[10] MacWilliams F. J.: A theorem on the distribution of weights in a systematic code. Bell Syst. Tech. J., 42, 79 - 94 (1963).

[11] Raja Durai R. S.: On linear codes with rank metric: Constructions, properties and applications. Ph.D Dissertation, Indian Institute of Technology Madras, India (2003).

[12] Roth R. M.: Maximum-rank array codes and their application to crisscross error correction. IEEE Trans. Inform. Theory, 37, 328 - 336 (1991).

[13] Stephen B. Wicker: Error control systems for digital communication and storage. Prentice-Hall, Inc., New Jersey (1995).

[14] Suresh Babu N.: Studies on rank distance codes. Ph.D Dissertation, Indian Institute of Technology Madras, India (1995).

[15] Tarokh V., Seshadri N., Calderbank A. R.: Space-time codes for high data rate wireless communication: Performance criterion and code construction. IEEE Trans. Inform. Theory, 44, 744 - 765 (1998).

[16] van Lint J. H.: Introduction to coding theory. Springer, New York (1999).

[17] van Wee G. J. M.: Improved sphere bounds on the covering radius of codes. IEEE Trans. Inform. Theory, 34, 237 - 245 (1988).

[18] Vasantha W.B., Selvaraj R.S.: Multi-covering radii of codes with rank metric. Proceedings of the 2002 IEEE Information Theory Workshop, Bangalore, India, p. 215 (2002).