COMMUNICATIONS IN INFORMATION AND SYSTEMS
Vol. 10, No. 3, pp. 183-192, 2010

003

EQUIDISTANT RANK METRIC CODES: CONSTRUCTION AND PROPERTIES

R. S. SELVARAJ* AND JEJAW DEMAMU*

Abstract. This paper introduces a new construction for q-ary equidistant code $\mathfrak{C}$ with rank metric where q is a power of 2. Investigations on structural properties of the proposed code are carried out. The highlight of the paper is that the kernel of the code $\mathfrak{C}$ happens to be an equidistant constant-weight code of same size as $\mathfrak{C}$ and is shown to be $\mathfrak{C} + \mathfrak{C}$. The bounds on number of steps that are required to construct the equidistant code are also given. Moreover, our construction is independent of the choice of metric, though our investigation mainly focuses about rank metric.

Keywords: rank metric codes; equidistant codes; constant-weight codes; kernel

1. Introduction. Recently, codes in rank metric have attracted great attention due to their relevance to wireless communications, cryptography, storage equipments, network coding etc [5, 6, 7, 13, 14]. While a vast amount of knowledge exists for non-linear binary codes with Hamming metric, a relatively little is known about non-linear q-ary codes with rank metric. The majority of previous works on rank metric codes were about rank distance properties, code construction, efficient decoding of rank metric codes. The works in [5, 10, 11, 12, 13, 17], have made significant contribution to these topics. Most of the studies regarding non-linear codes with Hamming metric revolved around perfect codes, equidistant codes and constant-weight codes. Binary equidistant codes have been studied by a number of authors, mainly as examples of designs and other combinatorial objects, for example see [8, 9]. There are no perfect codes [2, 16] with respect to rank metric. Plenty of knowledge exists regarding equidistant codes on binary codes, but as to our knowledge, equidistant rank metric codes have not been investigated. All these inspired us to think of a method of constructing equidistant rank metric codes. Constructing such equidistant codes discloses several properties of the nonlinear behavior of rank metric codes. Moreover, such equidistant codes also led us finding the way to construct constant-weight rank metric codes, applicable to communications, for instance, detecting error signals in ARQ system [4].

Hence this paper is aimed to provide a new technique to construct an equidistant rank metric code, from which we explore various properties possessed by it by investigating its kernel. The kernel of a code C, denoted by $Ker(C)$, is the set of vectors that leave C invariant under translation.

The remainder of this paper is arranged as follows. In section 2, we summarize

*Department of Mathematics, National Institute of Technology Warangal, Warangal - 506 004, India. E-mail: rsselva@nitw.ac.in, jejaw@yahoo.com

definitions and known results that will make this paper a self-contained one. In section 3, we introduce our method of constructing an equidistant rank metric code and determine its cardinality. Section 4 investigates some of the properties of the constructed code and discusses about its kernel. In section 5, we analyze the number of steps our proposed construction method run for. The final section gives the conclusion and suggest some open problems.

2. Preliminaries. Let $\mathbb{F}_{q^m}^n$ denote the n-dimensional vector space over the finite field $\mathbb{F}_{q^m}$ (where m and n are positive integers and q being a power of a prime). A Rank Distance (RD) code is a subset of $\mathbb{F}_{q^m}^n$ wherein the *weight* of each vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ (denoted by $wt(x)$) is defined to be the maximum number of its coordinates x_i that are linearly independent over $\mathbb{F}_q$. This weight is a norm on the rank distance space $\mathbb{F}_{q^m}^n$ called as *rank norm* and denoted as $r(x)$ or simply as $\|x\|$. The rank norm induces a metric called *rank metric* (or rank distance) on $\mathbb{F}_{q^m}^n$ and is denoted by d_R. Thus, the rank distance d_R between two vectors $x, y \in \mathbb{F}_{q^m}^n$ is the rank of their difference: $d_R(x, y) = r(x - y)$. Hereafter, in this paper, we consider $q = 2$, and without loss of generality, we write $d_R(x, y) = r(x+y)$, where "+" means addition modulo 2. Thus, $wt(x) = d_R(\mathbf{0}, x) = \|x\|$. The vector space $\mathbb{F}_{2^m}^n$ over $\mathbb{F}_{2^m}$ equipped with the rank metric d_R is called as a *rank distance space*. For any rank distance code C, the minimum distance d_{min} is defined by: $d_{min} = min\{d_R(x, y) : x, y \in C, x \neq y\}$. A code is said to be *equidistant* if the distance between any two distinct codewords is the same (say d). A code is called a *constant-weight* code if each non-zero codeword is of the same weight. A code is said to be an *additive code* if it is an additive subgroup of the ambient space $\mathbb{F}_{2^m}^n$.

3. Construction of Equidistant Rank Metric Codes. Given any three vectors of length n that are equidistant, we propose a method to construct an equidistant code. To construct an equidistant code, it is reasonable to start with three codewords. Hence our construction starts by picking any three codewords that are equidistant to each other.

The following terminology is used most frequently in our subsequent proofs and discussions. While constructing the code, we have used a sort of give and take technique i.e. if you pick a vector from the entire space, you will in turn be able to produce more codewords. Those vectors you are picking, are termed as **Initial codewords** and those that you will produce in turn, are termed as **Derived codewords**. **Derived codewords** are basically obtained from **Initial codewords** by adding all possible odd sums of the **Initial codewords** by fixing recently chosen or picked initial codeword.

Procedure to Construct the Proposed Equidistant Rank Metric Code:

1. Choose any three distinct initial vectors c_1, c_2, c_3 which are equidistant to

each other and call these as initial codewords.

2. Compute the derived codeword $c_4^d = c_1 + c_2 + c_3$.
3. Pick the fourth initial and call it c_5 which is equidistant to all the previous initials c_1, c_2, c_3 and the derived codeword c_4^d.
4. Compute the derived codewords by taking all possible sums of odd number of initials, with the recent initial c_5 being fixed and name them as indicated below:

$$c_6^d = c_5 + c_1 + c_2$$

$$c_7^d = c_5 + c_1 + c_3$$

$$c_8^d = c_5 + c_2 + c_3$$

5. Pick the fifth initial and call it c_9, which is equidistant from the previous 8 codewords.
6. Compute the derived codewords by forming all possible sums of odd number of initials with the recent initial c_9 being fixed, as follows:

$$c_{10}^d = c_9 + c_1 + c_2$$

$$c_{11}^d = c_9 + c_1 + c_3$$

$$c_{12}^d = c_9 + c_1 + c_5$$

$$c_{13}^d = c_9 + c_2 + c_3$$

$$c_{14}^d = c_9 + c_2 + c_5$$

$$c_{15}^d = c_9 + c_3 + c_5$$

$$c_{16}^d = c_9 + c_1 + c_2 + c_3 + c_5$$

7. Pick the next initial codeword and call it c_{17}. Compute the next derived codewords.

Continuing in this way, one can construct an equidistant code (*Proposition 3.1*). We shall denote the code constructed by the above procedure as $\mathfrak{C}$ throughout this paper.

Convention: During construction, each of the derived codewords is computed by taking all possible sums of odd number of the initial codewords, in which the recent

initial codeword is always fixed. For example, if c_5 is the recent initial codeword, then the subsequent derived codewords are computed from c_1, c_2, c_3 and c_5 by forming the following odd sums:

$$c_5 + c_1 + c_2$$

$$c_5 + c_1 + c_3$$

$$c_5 + c_2 + c_3$$

Each derived codeword is formed by forming a sum of 3 initial codewords, or 5 initial codewords, or 7 initial codewords and so on, by keeping the recently picked initial codeword fixed in each sum. So, from now on, in this paper:

- $\sum_{k}^{soni} c_k$ means the Sum of Odd Number of Initial codewords.
- $\sum_{k}^{seni} c_k$ means the Sum of Even Number of Initial codewords

PROPOSITION 3.1. *The code $\mathfrak{C}$ constructed in this way is an equidistant code.*

Proof. Let $x, y \in \mathfrak{C}$, where $\mathfrak{C}$ is the code constructed by the above method. Then any element of $\mathfrak{C}$ can be expressed as a sum of some odd number of initial codewords. That is x and y can be expressed as $x = \sum_{i}^{soni} c_i$ and $y = \sum_{j}^{soni} c_j$, where c_i, c_j are initial codewords in $\mathfrak{C}$. Now $d_R(x, y) = d_R\left(\sum_{i}^{soni} c_i,\ \sum_{j}^{soni} c_j\right) = r\left(\sum_{i}^{soni} c_i + \sum_{j}^{soni} c_j\right) = r\left(\sum_{k}^{seni} c_k\right)$. Arranging c_k's in their order of suffixes, one of them will have the largest suffix. If we call such initial codeword as c_l, all the other initials have suffixes less than l. As c_l is chosen in such a way that it is equidistant to the initial codewords and derived codewords with lower suffixes, we get the following: $d_R(x, y) = r\left(\sum_{k}^{seni} c_k\right) = d_R\left(\sum_{m}^{soni} c_m,\ c_l\right)$ which is the constant distance d, where $m < l$. Thus $\mathfrak{C}$ is equidistant. □

REMARK 1. *Since our construction is independent of the choice of metric, one can construct an equidistant code for any metric using the above procedure.*

REMARK 2. *During construction if the all-zero codeword is included, then $\mathfrak{C}$ becomes an additive code to the ambient space. Then the elements of $\mathfrak{C}$ can be expressed as a sum of odd or even number of initial codewords. Unless and otherwise stated, we will assume that $\mathfrak{C}$ does not contain the all-zero codeword.*

The above proposition assures, such a construction gives an equidistant rank metric code. Now it should be the duty of this paper to provide how the size of the code looks like. More beautifully, the size of the code constructed by the above method is always a power of 2. The following proposition tells us this fact.

PROPOSITION 3.2. *If t denotes the total number of initial codewords in $\mathfrak{C}$, then the size of the code $\mathfrak{C}$ will be 2^{t-1}.*

Proof. First, let us stay clear of the fact that a codeword y resulting in some step i of the construction procedure is always distinct from codewords x constructed in prior step. There are three possibilities.

(i) If both x and y are initial codewords then by the construction procedure, they are distinct.

(ii) Suppose that both are derived codewords. Then $x = \sum_{i}^{soni} c_i$ and $y = \sum_{j}^{soni} c_j$. If $x = y$ then $\sum_{i}^{soni} c_i - \sum_{j}^{soni} c_j = 0$ which implies $\sum_{k}^{seni} c_k = 0$, after doing necessary simplification. Now, arranging c_k's in their order of suffixes, one of them, say, c_l will have the largest suffix. Thus, $c_l + \sum_{m}^{soni} c_m = 0$, where $m < l$, which means $c_l = \sum_{m}^{soni} c_m$. This shows that c_l is equal to a previously obtained derived codeword $\sum_{m}^{soni} c_m$ which is a contradiction, as the initial codewords are chosen in such a way that they are distinct and equidistant from the previously obtained codewords.

(iii) Suppose that x be an initial codeword, say, c_i and y be a derived codeword found in a later step. Then $y = \sum_{j}^{soni} c_j$. If $y = x$, then $\sum_{j}^{soni} c_j = c_i$ which means that $\sum_{k}^{seni} c_k = 0$. Now, as in the case (ii) above, this cannot happen.

Thus, all codewords that are produced in every step of the construction are distinct.

If $t = 3$, then there is only one derived codeword which will be computed in $\binom{2}{2}$ ways. With the fourth initial, one can produce derived codewords in $\binom{3}{2}$ ways. With the fifth initial, one can compute derived codewords in $\binom{4}{2} + \binom{4}{4}$ ways. Thus with t^{th} initial, one can produce derived codewords in $\binom{t-1}{2} + \binom{t-1}{4} + \cdots + \binom{t-1}{t-2}$ ways, if t is even, or $\binom{t-1}{2} + \binom{t-1}{4} + \cdots + \binom{t-1}{t-1}$ ways, if t is odd. In general, depending on whether t is even or odd, the total size of the code is the totality of all initial codewords and the total number of derived codewords. Note

that the number of initial codewords is t which can be expressed as $\binom{t}{0} + \binom{t-1}{1}$.

If t is odd then,

$$\begin{aligned}|\mathfrak{C}| &= t + \left[\binom{2}{2} + \binom{3}{2}\right] + \left[\binom{4}{2} + \binom{4}{4}\right] + \left[\binom{5}{2} + \binom{5}{4}\right] \\ &\quad + \left[\binom{6}{2} + \binom{6}{4} + \binom{6}{6}\right] + \cdots + \left[\binom{t-2}{2} + \binom{t-2}{4} + \cdots + \binom{t-2}{t-3}\right] \\ &\quad + \left[\binom{t-1}{2} + \binom{t-1}{4} + \cdots + \binom{t-1}{t-1}\right] \\ &= (1+1)^{t-1} = 2^{t-1},\end{aligned}$$

by simplifying and using the recurrence relation $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

If t is even,

$$\begin{aligned}|\mathfrak{C}| &= t + \left[\binom{2}{2} + \binom{3}{2}\right] + \left[\binom{4}{2} + \binom{4}{4}\right] + \left[\binom{5}{2} + \binom{5}{4}\right] \\ &\quad + \left[\binom{6}{2} + \binom{6}{4} + \binom{6}{6}\right] + \cdots + \left[\binom{t-2}{2} + \binom{t-2}{4} + \cdots + \binom{t-2}{t-2}\right] \\ &\quad + \left[\binom{t-1}{2} + \binom{t-1}{4} + \cdots + \binom{t-1}{t-2}\right] \\ &= (1+1)^{t-1} = 2^{t-1}\end{aligned}$$

□

4. Properties of the Equidistant Rank Metric Code. In what follows, we show how an equidistant constant-weight code can be constructed from $\mathfrak{C}$. The results are presented by the following propositions.

Note that $\mathfrak{C}+\mathfrak{C} = \{x = u+v \in \mathbb{F}_{2^m}^n : u, v \in \mathfrak{C}\}$. As $\mathfrak{C}+\mathfrak{C}$ contains many identical elements, clearly $|\mathfrak{C}+\mathfrak{C}| < 2|\mathfrak{C}|$.

PROPOSITION 4.1. *If $\mathfrak{C}$ is an equidistant code with a constant rank distance d, then $\mathfrak{C}+\mathfrak{C}$ is a constant-weight code of same weight d.*

Proof. Let $x \in \mathfrak{C}+\mathfrak{C}$ such that $x \neq \mathbf{0}$. Then $x = c_i + c_j$, for some $c_i \neq c_j$ in $\mathfrak{C}$ and $\|x\| = \|c_i + c_j\| = d_R(c_i, c_j) = d$. □

PROPOSITION 4.2. *Every element of $\mathfrak{C}+\mathfrak{C}$ is expressible as a sum of even number of initial codewords of $\mathfrak{C}$.*

Proof. Let $y \in \mathfrak{C}+\mathfrak{C}$. Then $y = u + v$ for some $u, v \in \mathfrak{C}$. We know that every element of $\mathfrak{C}$ is expressible as a sum of odd number of initials of $\mathfrak{C}$, i.e. $u = \sum_{i}^{soni} c_i$, $v = \sum_{j}^{soni} c_j$ where c_i and c_j are initial codewords of $\mathfrak{C}$. Now $y = u+v = \sum_{i}^{soni} c_i + \sum_{j}^{soni} c_j = \sum_{k}^{seni} c_k$ which implies y is expressible as a sum of even number of initial codewords of $\mathfrak{C}$. Hence, the result follows. □

REMARK 3. *Note that the sum of any even number of initial codewords belongs to* $\mathfrak{C}+\mathfrak{C}$ *which makes* $\mathfrak{C}+\mathfrak{C}$ *an additive subgroup of* $\mathbb{F}_{2^m}^n$.

PROPOSITION 4.3. $\mathfrak{C}+\mathfrak{C}$ *is an equidistant code.*

Proof. Let $x, y \in \mathfrak{C}+\mathfrak{C}$. Then $x = \sum_{k}^{seni} c_k$, $y = \sum_{l}^{seni} c_l$ where c_k's and c_l's are initial codewords. Now $d_R(x,y) = d_R\left(\sum_{k}^{seni} c_k, \sum_{l}^{seni} c_l\right) = r\left(\sum_{k}^{seni} c_k + \sum_{l}^{seni} c_l\right) = r\left(\sum_{i}^{seni} c_i\right) = d$. □

We record the following result which is immediate.

PROPOSITION 4.4. *Any translate of* $\mathfrak{C}$ *is an equidistant code.*

The kernel of a code $\mathfrak{C}$, denoted by $Ker(\mathfrak{C})$, is the set of vectors that leave the code invariant under translation. That is, $Ker(\mathfrak{C}) = \{x \in \mathbb{F}_{2^m}^n : x+\mathfrak{C} = \mathfrak{C}\}$. The following two results establish that $Ker(\mathfrak{C})$ is also an equidistant code. In the sequel, we establish some of the properties of the kernel.

PROPOSITION 4.5. *For all* $y \in \mathfrak{C}+\mathfrak{C}$, $y+\mathfrak{C} = \mathfrak{C}$.

Proof. Let $x \in y+\mathfrak{C}$. Then there exists $c \in \mathfrak{C}$ such that $x = y+c = \sum_{i}^{seni} c_i + \sum_{k}^{soni} c_k$, where $y = \sum_{i}^{seni} c_i$ and $c = \sum_{k}^{soni} c_k$, c_i and c_k being initial codewords. So, $x = \sum_{m}^{soni} c_m \in \mathfrak{C}$, which implies $y+\mathfrak{C} \subseteq \mathfrak{C}$. Conversely, let $z \in \mathfrak{C}$. Then $z = \sum_{i}^{soni} c_i$, where c_i's are initial codewords. Now $z = y+z+y = \sum_{k}^{seni} c_k + \sum_{i}^{soni} c_i + \sum_{k}^{seni} c_k = \sum_{k}^{seni} c_k + \sum_{m}^{soni} c_m \in y+\mathfrak{C}$. Thus, $\mathfrak{C} \subseteq y+\mathfrak{C}$. Hence, the result follows. □

THEOREM 4.6. *If* $Ker(\mathfrak{C})$ *denotes the kernel of the code* $\mathfrak{C}$, *then* $Ker(\mathfrak{C}) = \mathfrak{C}+\mathfrak{C}$.

Proof. By *Proposition 4.5*, $\mathfrak{C}+\mathfrak{C} \subseteq Ker(\mathfrak{C})$. Conversely, let $y \in Ker(\mathfrak{C})$. This means, $y+\mathfrak{C} = \mathfrak{C}$ and so $y+c_j = c_l$ for some $c_j, c_l \in \mathfrak{C}$. This implies $y = c_j+c_l \in \mathfrak{C}+\mathfrak{C}$. Thus, $Ker(\mathfrak{C}) \subseteq \mathfrak{C}+\mathfrak{C}$. Hence, $Ker(\mathfrak{C}) = \mathfrak{C}+\mathfrak{C}$. □

Thus, the above *Theorem 4.6* establishes that $Ker(\mathfrak{C})$ is an equidistant constant-weight additive code.

PROPOSITION 4.7. *For any* $c \in \mathfrak{C}$, $c+\mathfrak{C} = \mathfrak{C}+\mathfrak{C}$.

Proof. Clearly, $c+\mathfrak{C} \subseteq \mathfrak{C}+\mathfrak{C}$ for every $c \in \mathfrak{C}$. Conversely, let $z \in \mathfrak{C}+\mathfrak{C}$ and let $c \in \mathfrak{C}$. Now $z \in Ker(\mathfrak{C})$, which means, $z+c \in \mathfrak{C}$ and thus, $z \in c+\mathfrak{C}$. This implies, $\mathfrak{C}+\mathfrak{C} \subseteq c+\mathfrak{C}$. Hence, $c+\mathfrak{C} = \mathfrak{C}+\mathfrak{C}$ for every $c \in \mathfrak{C}$. □

PROPOSITION 4.8. *For every* $c \in \mathfrak{C}$, $|c + \mathfrak{C}| = |\mathfrak{C}|$.

Proof. Let $x, y \in c + \mathfrak{C}$. So that, $x = c + c_l$ and $y = c + c_k$ for some $c_l, c_k \in \mathfrak{C}$. If $x = y$, then $c + c_l = c + c_k$ which means $c_k = c_l$. Hence all the elements in $c + \mathfrak{C}$ are distinct, which results in $|c + \mathfrak{C}| = |\mathfrak{C}|$, as required. □

Now, the following result follows immediately.

PROPOSITION 4.9. $|Ker(\mathfrak{C})| = 2^{t-1}$.

We have shown that the code $\mathfrak{C}$ and its kernel have the same cardinality 2^{t-1} where t is the total number of initial codewords in $\mathfrak{C}$. As the kernel of $\mathfrak{C}$ is an additive subgroup of $\mathbb{F}_{2^m}^n$, distinct cosets of the kernel partitions $\mathbb{F}_{2^m}^n$.

We illustrate the arrived results by the following example.

EXAMPLE 1. We shall construct an equidistant code with distance $d = 3$. Consider the rank distance code of length $n = 3$ over the Galois field $\mathbb{F}_{2^3}$. Let α be a primitive element of the field $\mathbb{F}_{2^3}$ such that $\alpha^3 = \alpha + 1$. Choose three vectors namely, $c_1 = (\alpha^2,\ 0,\ 0)$, $c_2 = (1,\ \alpha,\ \alpha^2)$, $c_3 = (0,\ 1,\ \alpha)$. Their sum $c_4^d = (1 + \alpha^2,\ 1 + \alpha,\ \alpha + \alpha^2)$ is the derived codeword from the first three initial codewords. Then choose the new initial codeword $c_5 = (\alpha + \alpha^2,\ \alpha + \alpha^2,\ 1)$ such that it is equidistant to all the first four codewords. From this new initial and that of the previous three initial codewords, three more derived codewords are computed: $c_6^d = (1 + \alpha,\ \alpha^2,\ 1 + \alpha^2)$, $c_7^d = (\alpha,\ 1 + \alpha + \alpha^2,\ 1 + \alpha)$, $c_8^d = (1 + \alpha + \alpha^2,\ 1 + \alpha^2,\ 1 + \alpha + \alpha^2)$ using our construction. Computer search shows that no more initial codewords can be found for our choice of initial three codewords. There are $t = 4$ initial codewords and thus the size of the code $\mathfrak{C}$ is 8. Here, $Ker(\mathfrak{C}) = \mathfrak{C} + \mathfrak{C} = \{(0,\ 0,\ 0),\ (1 + \alpha^2,\ \alpha,\ \alpha^2),\ (\alpha^2,\ 1,\ \alpha),\ (1,\ 1 + \alpha,\ \alpha + \alpha^2),\ (\alpha,\ \alpha + \alpha^2,\ 1),\ (1 + \alpha + \alpha^2,\ \alpha^2,\ 1 + \alpha^2),\ (\alpha + \alpha^2,\ 1 + \alpha + \alpha^2,\ 1 + \alpha),\ (1 + \alpha,\ 1 + \alpha^2,\ 1 + \alpha + \alpha^2)\}$. It is easy to observe that the non-zero elements of the kernel of the code $\mathfrak{C}$ form an equidistant constant-weight code.

5. Bounds on t. This section analyzes how many steps our proposed construction method run for. That is, what would be the maximum number of initial codewords one can find from a given ambient space $\mathbb{F}_{2^m}^n$ for constructing an equidistant code of distance d? Clearly, t cannot exceed mn, as that would mean $|\mathfrak{C}| \geq 2^{mn}$ if $t > mn$. For, even if $t = mn + 1$, $|\mathfrak{C}| = 2^{mn} = |\mathbb{F}_{2^m}^n|$ which cannot happen. Thus, we need to find an upper bound for the number of initial codewords t. Now we recall a result from [10] which states that if S_r denote the number of vectors of rank r in $\mathbb{F}_{q^m}^n$ then $q^{(m+n-2)r-r^2} \leq |S_r| \leq q^{(m+n+1)r-r^2}$. Using this, we will give an upper bound for t.

PROPOSITION 5.1. *If* $\mathfrak{C}$ *is the equidistant code of length* n *with constant distance* d *and* t *is the number of initial codewords then* $t \leq 1 + \log_2(1 + 2^{(m+n+1)d-d^2})$.

Proof. Now $\mathfrak{C} + \mathfrak{C}$ is a constant-weight equidistant code with constant weight d.

Thus, $|\mathfrak{C}+\mathfrak{C}|-1 \leq$ number of vectors of rank norm d, which means $2^{t-1}-1 \leq |S_d| \leq 2^{(m+n+1)d-d^2}$. Thus, $t \leq 1+\log_2(1+2^{(m+n+1)d-d^2})$. □

Now, we will try to improve this bound. From the above proof, it is clear that, $t \leq 1+\log_2(1+|S_d|)$. From [5] and [11], the number of vectors of rank r, that is, $|S_r|$ is given by $\begin{bmatrix} n \\ r \end{bmatrix} A(m,r)$ where $A(m,r)$ is defined as follows: $A(m,0)=1$ and $A(m,r)=\prod_{i=0}^{r-1}(q^m-q^i)$ for $r \geq 1$. The $\begin{bmatrix} n \\ r \end{bmatrix}$ term is the Gaussian binomial, defined as $\begin{bmatrix} n \\ r \end{bmatrix} = \frac{A(n,r)}{A(r,r)}$. Note that $\begin{bmatrix} n \\ r \end{bmatrix}$ is the number of r-dimensional linear subspaces of $\mathbb{F}_q^n$.

From [11], we have the following results: For $0 \leq r \leq m$, $A(m,r) \leq q^{mr}$ and $\begin{bmatrix} m \\ r \end{bmatrix} < K_q^{-1} q^{r(m-r)}$, where $K_q = \prod_{j=1}^{\infty}(1-q^{-j})$. Now, $|S_d| \leq K_q^{-1} q^{d(n-d)} q^{md} = K_q^{-1} q^{d(m+n-d)}$. From this follows our new upper bound for t:

PROPOSITION 5.2. *If $\mathfrak{C}$ is the equidistant code of length n with constant distance d and t is the number of initial codewords then $t \leq 1+\log_2(1+K_2^{-1}2^{d(m+n-d)})$.*

Now, the bound from *Proposition 5.1* can be re-written as $t \leq 1+\log_2(1+2^d 2^{d(m+n-d)})$. Comparing these two upper bounds for t, the upper bound in *Proposition 5.2* is tighter, as $K_2^{-1} < 2$.

6. Conclusion. A new method of constructing equidistant codes is introduced. Certain structural properties of the proposed code are investigated. We have shown that the size of the constructed code always turns out to be a power of 2. Our investigation shows that the kernel of the constructed code is $\mathfrak{C}+\mathfrak{C}$ and it is an equidistant constant-weight code. Bounds on the number of initial codewords that can be picked from the ambient space while construction are also discussed. The method proposed is a greedy approach which generates derived codewords from the recently chosen initial codeword. For every t initial codewords chosen, there are $2^{t-1}-t$ codewords that are derived from it by just forming an odd linear combination of the initial codewords. Thus, rather than picking all 2^{t-1} codewords that are equidistant, the proposed method suggests to find just t initial codewords that are equidistant to previously picked/derived codewords. Now, we keep the problem of picking the t initial codewords that is more efficient than the existing approach as open. Finding lowest upper bound for the number of initial codewords for given d and n, is another open problem that is to be answered.

REFERENCES

[1] A.E. BROUWER, J.B. SHEARER, N.J.A. SLOANE, AND W.D. SMITH, *A new table of constant-weight codes*, IEEE Trans. Inform. Theory, 36(1990), pp. 1344 - 1380.

[2] K. Chen, *On the non-existence of perfect codes with rank distance*, Math. Nachr., 182(1996), pp. 89 - 98.

[3] Fang-Wei Fu, Torleiv Klove, Yuan Luo, and Victor K.Wei, *On equidistant constant weight codes*, Discrete Appl. Math., 128(2003), pp. 157 - 164.

[4] Fanxin Zeng, *Construction of Constant Weight Code and Some Upper Bounds*, Proc. IEEE Int. Symp. on Information Theory, Adelaide, Australia, pp. 1073 - 1077, 2005.

[5] E.M. Gabidulin, *Theory of Codes with Maximum Rank Distance*, Problems Inform. Transmission, 21:1(1985), pp. 1 - 12.

[6] E.M. Gabidulin, M. Bossart, and P. Lusina, *Space-time Codes based on Rank Codes*, Proc. IEEE Int. Symp. on Information Theory, Sorrento, Italy, p. 284, 2000.

[7] E.M. Gabidulin, A.V. Paramonov, and O.V. Tretjakov, *Ideals over a non-commutative ring and their application in cryptology*, Proc. EUROCRYPT '91, Brighton, UK, Lecture Notes in Comput. Sci., vol. 547, pp. 482 - 489, 1991.

[8] J.I. Hall, *Bounds for equidistant codes and partial projective planes*, Discrete Math. 17(1977), pp. 85 - 94.

[9] J.I. Hall, A.J.E.M. Jansen, A.W.J. Kolen, and J.H. van Lint, *Equidistant codes with distance 12*, Discrete Math., 17(1977), pp. 71 - 83.

[10] P. Loidreau, *Properties of Codes in Rank Metric*, Proc. Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, pp. 192 - 198, 2008.

[11] Maximilien Gadouleau and Zhiyuan Yan, *On the Decoder Error Probability of Bounded Rank-Distance Decoders for Maximum Rank Distance Codes*, IEEE Trans. Inform. Theory, 54(2008), pp. 3202 - 3206.

[12] Maximilien Gadouleau and Zhiyuan Yan, *Packing and Covering Properties of Rank Metric Codes*, IEEE Trans. Inform. Theory, 54(2008), pp. 3873 - 3883.

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

[14] D. Silva and F.R. Kschischang, *Using rank-metric codes for error correction in random network coding*, in: Proc. IEEE Int. Symp. on Information Theory, Nice, France, pp. 796 - 800, 2007.

[15] D.R. Stinson and G.H.J. van Rees, *The equivalence of certain equidistant binary codes and symmetric BIBDs*, Combinatorica, 4(1984), pp. 357 - 362.

[16] N. Suresh Babu, *Studies on rank distance codes*, Ph.D Dissertation, Indian Institute of Technology Madras, India, 1995.

[17] W.B. Vasantha and R.S. Selvaraj, *Multi-covering Radii of Codes with Rank Metric*, in: Proc. 2002 IEEE Information Theory Workshop, Bangalore, India, p. 215, 2002.