Bounds on Covering Codes with the Rank Metric

Maximilien Gadouleau, *Student Member, IEEE,* and Zhiyuan Yan, *Senior Member, IEEE*

***Abstract*—In this paper, we investigate geometrical properties of the rank metric space and covering properties of rank metric codes. We first establish an analytical expression for the intersection of two balls with rank radii, and then derive an upper bound on the volume of the union of multiple balls with rank radii. Using these geometrical properties, we derive both upper and lower bounds on the minimum cardinality of a code with a given rank covering radius. The geometrical properties and bounds proposed in this paper are significant to the design, decoding, and performance analysis of rank metric codes.**

***Index Terms*—Error control codes, covering radius, rank metric codes, geometrical properties, intersection number.**

I. Introduction

THERE is a steady stream of works on rank metric codes due to their applications to data storage, public-key cryptosystems, and space-time coding (see [1], [2] and the references therein for a comprehensive literature survey), and interest in rank metric codes is strengthened by their recent applications in error control for random network coding [2], described below. Constant-dimension codes [3] are an important class of codes for error and erasure correction in random linear network coding. Using the lifting operation [2], rank metric codes can be readily turned into constant-dimension codes without modifying their distance properties. It is shown in [3] that liftings of rank metric codes have many advantages compared to general constant-dimension codes. First, their cardinalities are optimal up to a constant; second, the decoding of these codes can be done in either the subspace metric [3] or the rank metric [2], and for both scenarios efficient decoding algorithms were proposed.

Despite their significance, many research problems in rank metric codes remain open. For example, geometrical properties of the rank metric space are not well studied, and covering properties of rank metric codes have received little attention with the exception of our previous work [1]. The geometrical properties, such as the intersection number, characterize fundamental properties of a metric space, and determine the packing and covering properties of codes defined in the metric space. Packing and covering properties are significant to the code design, decoding, and performance analysis of rank metric codes. For instance, the covering radius can be viewed as a measure of performance: if the code is used for error correction, then the covering radius is the maximum weight of a correctable error vector. The covering radius of a code also gives a criterion for code optimality: if the covering radius of a code is no less than its minimum distance, then the code is not optimal since more codewords can be added without changing the minimum distance. Liftings of rank metric codes have been considered for error control in random network coding and some are nearly optimal constant-dimension codes, but the optimality of these codes are unknown. Based on the results in this paper, it can be shown that covering radii of liftings of rank metric codes are no less than their minimum distances [4], further implying that liftings of rank metric codes are not optimal constant-dimension codes. In this example, covering properties provide guidelines for the design of error control codes for random network coding.

In this paper, we focus on the geometrical properties of the rank metric space and covering properties of rank metric codes. We first establish an analytical expression for the intersection of two balls with rank radii, and then derive an upper bound on the volume of the union of multiple balls with rank radii. Both results are novel to the best of our knowledge. Using these geometrical properties, we derive novel lower and upper bounds on the minimum cardinality $K_{\mathrm{R}}(q^m, n, \rho)$ of a code in $\mathrm{GF}(q^m)^n$ with rank covering radius ρ. The bounds presented in this paper are obtained based on different approaches from those in [1], and they are the tightest bounds to the best of our knowledge for many sets of parameter values.

We note that some technical proofs are omitted due to limited space; interested readers are referred to an expanded manuscript posted online [5].

II. Preliminaries

The rank weight of a vector $\mathbf{x} \in \mathrm{GF}(q^m)^n$, denoted as $\mathrm{rk}(\mathbf{x})$, is defined to be the *maximum* number of coordinates in $\mathbf{x}$ that are linearly independent over $\mathrm{GF}(q)$. The number of vectors of rank weight r in $\mathrm{GF}(q^m)^n$ is $N_r = \begin{bmatrix} n \\ r \end{bmatrix} \alpha(m,r)$, where $\alpha(m,0) \overset{\text{def}}{=} 1$, $\alpha(m,r) \overset{\text{def}}{=} \prod_{i=0}^{r-1}(q^m - q^i)$, and $\begin{bmatrix} n \\ r \end{bmatrix} \overset{\text{def}}{=} \alpha(n,r)/\alpha(r,r)$ for $r \geq 1$ [6]. The rank distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as $d_{\mathrm{R}}(\mathbf{x},\mathbf{y}) = \mathrm{rk}(\mathbf{x}-\mathbf{y})$. Also, the rank distance between a vector $\mathbf{x}$ and a code C is the *minimum* rank distance between $\mathbf{x}$ and any codeword in C. If a vector $\mathbf{x}$ is at distance at most ρ from a code C, we say C covers $\mathbf{x}$ with radius ρ. The rank covering radius ρ of a code C is defined as $\max_{\mathbf{x}\in \mathrm{GF}(q^m)^n} d_{\mathrm{R}}(\mathbf{x}, C)$. When $n \leq m$, the minimum rank distance d_{R} of a code of length n and cardinality M over $\mathrm{GF}(q^m)$ satisfies $d_{\mathrm{R}} \leq n - \log_{q^m} M + 1$; we refer to this bound as the Singleton bound for rank metric codes. The equality is

Manuscript received February 26, 2009. The associate editor coordinating the review of this letter and approving it for publication was P. Popovski.

This work was supported in part by Thales Communications Inc., and in part by a grant from the Commonwealth of Pennsylvania, Department of Community and Economic Development, through the Pennsylvania Infrastructure Technology Alliance (PITA).

M. Gadouleau is with Crestic, Université de Reims Champagne-Ardenne, Reims, France (e-mail: maximilien.gadouleau@univ-reims.fr).

Z. Yan is with the Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA, 18015 USA (e-mail: yan@lehigh.edu).

Digital Object Identifier 10.1109/LCOMM.2009.090447

attained by a class of linear rank metric codes called maximum rank distance (MRD) codes.

III. Geometrical Properties of Balls with Rank Radii

We denote the intersection of two spheres (balls, respectively) in $\mathrm{GF}(q^m)^n$ with rank radii u and s and centers with distance w as $J_{\mathrm{R}}(u,s,w)$ ($I(u,s,w)$, respectively).

Lemma 1: We have

$$J_{\mathrm{R}}(u,s,w) = \frac{1}{q^{mn}N_w}\sum_{i=0}^{n} N_i K_u(i) K_s(i) K_w(i), \tag{1}$$

where $K_j(i)$ is a q-Krawtchouk polynomial [7]:

$$K_j(i) = \sum_{l=0}^{j}(-1)^{j-l}q^{lm+\binom{j-l}{2}}\begin{bmatrix} n-l \\ n-j\end{bmatrix}\begin{bmatrix} n-i \\ l\end{bmatrix}. \tag{2}$$

Although (1) is obtained by a direct application of [8, Chapter II, Theorem 3.6], we present it formally since it is a fundamental geometric property of the rank metric space. Since

$$I(u,s,w) = \sum_{i=0}^{u}\sum_{j=0}^{s} J_{\mathrm{R}}(i,j,w), \tag{3}$$

(1) also leads to an analytical expression for $I(u,s,w)$. In order to simplify notations we denote $I(\rho,\rho,d)$ as $I(\rho,d)$. Both (1) and (3) are instrumental in our later derivations.

We denote the volume of a ball with rank radius ρ as $v(\rho)$, and we now derive a bound on the volume of the union of any K balls with radius ρ, which will be instrumental in Section IV.

Lemma 2: The volume of the union of *any* K balls with rank radius ρ is at most

$$\begin{aligned} B(K) =& v(\rho) + \sum_{a=1}^{l}(q^{am} - q^{(a-1)m})[v(\rho) - I(\rho, n-a+1)] \\ &+ (K - q^{lm})[v(\rho) - I(\rho, n-l)], \end{aligned} \tag{4}$$

where $l = \lfloor \log_{q^m} K \rfloor$.

Proof: Let $\{\mathbf{v}_i\}_{i=0}^{K-1}$ denote the centers of K balls with rank radius ρ and let $V_j = \{\mathbf{v}_i\}_{i=0}^{j-1}$ for $1 \leq j \leq K$. The centers are labeled such that $d_{\mathrm{R}}(\mathbf{v}_j, V_j)$ is non-increasing for $j > 0$. For $1 \leq a \leq l$ and $q^{m(a-1)} \leq j < q^{ma}$, we have $d_{\mathrm{R}}(\mathbf{v}_j, V_j) = d_{\mathrm{R}}(V_{j+1}) \leq n - a + 1$ by the Singleton bound. The center $\mathbf{v}_j$ hence covers at most $v(\rho) - I(\rho, n-a+1)$ vectors that are not previously covered by V_j. ■

IV. Bounds on Covering Codes with the Rank Metric

We consider covering codes in $\mathrm{GF}(q^m)^n$, and without loss of generality we assume $n \leq m$ due to transposition [1]. We first derive a lower bound on $K_{\mathrm{R}}(q^m, n, \rho)$ based on the linear inequalities satisfied by the distance distribution $A_i(\delta)$ of a covering code with respect to a vector at distance δ from the code.

Proposition 1: For $0 \leq \delta \leq \rho$, let $T_\delta = \min \sum_{i=0}^{n} A_i(\delta)$, where the minimum is taken over all integer sequences $\{A_i(\delta)\}$ which satisfy $A_i(\delta) = 0$ for $0 \leq i \leq \delta - 1$, $A_\delta(\delta) \geq 1$, $0 \leq A_i(\delta) \leq N_i$ for $\delta + 1 \leq i \leq n$, and $\sum_{i=0}^{n} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{R}}(r,s,i) \geq N_r$ for $0 \leq r \leq n$. Then $K_{\mathrm{R}}(q^m, n, \rho) \geq \max_{0 \leq \delta \leq \rho} T_\delta$.

Proof: Let C be a code in $\mathrm{GF}(q^m)^n$ with covering radius ρ and cardinality $K_{\mathrm{R}}(q^m, n, \rho)$. For any $\mathbf{u} \in \mathrm{GF}(q^m)^n$ at distance $0 \leq \delta \leq \rho$ from C, let $A_i(\delta)$ denote the number of codewords at distance i from $\mathbf{u}$. Then $\sum_{i=0}^{n} A_i(\delta) = |C| = K_{\mathrm{R}}(q^m, n, \rho)$ and we easily obtain $A_i(\delta) = 0$ for $0 \leq i \leq \delta - 1$, $A_\delta(\delta) \geq 1$, and $0 \leq A_i(\delta) \leq N_i$ for $\delta + 1 \leq i \leq n$. Also, for $0 \leq r \leq n$, any codeword at distance i from $\mathbf{u}$ covers exactly $\sum_{s=0}^{\rho} J_{\mathrm{R}}(r,s,i)$ vectors at distance r from $\mathbf{u}$. All the vectors at distance r from $\mathbf{u}$ are covered, hence $\sum_{i=0}^{n} A_i(\delta) \sum_{s=0}^{\rho} J_{\mathrm{R}}(r,s,i) \geq N_r$. ■

We note that the notation $A_i(\delta)$ is used above since the constraints on the sequence depend on δ. Since T_δ is the solution of an integer linear programming, it is computationally infeasible to determine T_δ for very large parameter values.

We now derive an upper bound on $K_{\mathrm{R}}(q^m, n, \rho)$ by providing a nontrivial refinement of the greedy algorithm in [9].

Lemma 3: Let C be a code which covers at least $q^{mn} - u$ vectors in $\mathrm{GF}(q^m)^n$ with radius ρ. Then for any $k \geq |C|$, there exists a code with cardinality k which covers at least $q^{mn} - u_k$ vectors, where $u_{|C|} = u$ and for $k \geq |C|$

$$u_{k+1} = u_k - \left\lceil \frac{u_k v(\rho)}{\min\{q^{mn} - k, B(u_k)\}} \right\rceil. \tag{5}$$

Thus $K_{\mathrm{R}}(q^m, n, \rho) \leq \min\{k : u_k = 0\}$.

The upper bound in Lemma 3 is nontrivial since the sequence $\{u_k\}$ is monotonically decreasing until it reaches 0 for $k \leq q^{mn}$. Since the sequence $\{u_k\}$ depends on C only through the number of vectors covered by C, to obtain a tighter bound on $K_{\mathrm{R}}(q^m, n, \rho)$ based on Lemma 3, it is necessary to find a code C which leaves a smaller number of vectors uncovered. We consider two choices for C below. Since any codeword can cover at most $v(\rho)$ vectors uncovered by the other codewords, we have $u \geq q^{mn} - v(\rho)|C|$. In the first choice, we consider the largest code C_0 that achieves $u = q^{mn} - v(\rho)|C_0|$, which is an $(n, n-a, a+1)$ linear MRD code with $a = \min\{n, 2\rho\}$.

An alternative choice would be to select a supercode of C_0, that is, an MRD code with a larger dimension. Since there may be intersection between balls of radius ρ around codewords, we now derive a lower bound on the number of vectors covered by only one codeword in an MRD code. Let us denote the number of codewords with rank r in an $(n, n-d+1, d)$ linear MRD code as $M(d,r)$.

Lemma 4: Let the vectors $\mathbf{c}_j \in \mathrm{GF}(q^m)^n$ be sorted such that $\{\mathbf{c}_j\}_{j=0}^{q^{m(n-l+1)}-1}$ is an $(n, n-l+1, l)$ MRD code for $1 \leq l \leq n$. For all $1 \leq k \leq q^{mn} - 1$, we denote $\{\mathbf{c}_j\}_{j=0}^{k-1}$ as C_k and its minimum rank distance is given by $d_k = n - \lceil \log_{q^m}(k+1) \rceil + 1$. Then for $d_k \geq 2\rho + 1$, $\mathbf{c}_k$ covers $v(\rho)$ vectors not covered by C_k. For $d_k \leq 2\rho$, $\mathbf{c}_k$ covers at least $v(\rho) - \sum_{l=d_k}^{a} \mu_l I(\rho, l)$ vectors not covered by C_k, where $a = \min\{n, 2\rho\}$, $\mu_{d_k} = \min\{M(d_k, d_k), k\}$, and $\mu_l = \min\left\{M(d_k, l), k - \sum_{j=d_k}^{l-1} \mu_j\right\}$ for $l > d_k$.

Proposition 2: Let $a = \min\{n, 2\rho\}$, $K_0 = q^{m(n-a)}$, and $u_{K_0} = q^{mn} - q^{m(n-a)}v(\rho)$. Consider two sequences $\{h_k\}$ and $\{u'_k\}$, both of which are upper bounds on the number of vectors yet to be covered by a code of cardinality k, given by

TABLE I
BOUNDS ON $K_{\mathrm{R}}(2^m, n, \rho)$, FOR $2 \leq m \leq 7$, $2 \leq n \leq m$, AND $1 \leq \rho \leq 6$.

m	n	$\rho = 1$	$\rho = 2$	$\rho = 3$	$\rho = 4$	$\rho = 5$	$\rho = 6$
2	2	3	1				
3	2	4	1				
	3	11-16	4	1			
4	2	7-8	1				
	3	40-64	4-7	1			
	4	293-722	10-48	3-**5 J**	1		
5	2	12-16	1				
	3	154-256	6-8	1			
	4	2267-4096	33-256	4-8	1		
	5	34894-2^{17}	233-**2773 I**	**h 10**-32	3-**6 J**	1	
6	2	23-32	1				
	3	601-1024	11-16	1			
	4	17822-2^{15}	124-256	6-16	1		
	5	550395-2^{20}	1770-2^{14}	31-256	**i 4**-16	1	
	6	17318410-2^{26}	27065-**401784 I**	214-**4092 I**	9-**154 J**	3-**7 J**	1
7	2	44-64	1				
	3	2372-4096	20-32	1			
	4	141231-2^{18}	484-1024	**i 10**-16	1		
	5	8735289-2^{24}	13835-2^{15}	**i 112**-1024	**i 6**-16	1	
	6	549829402-2^{30}	42229-2^{22}	**i 1585**-2^{15}	29-**708 I**	**i 4**-16	1
	7	34901004402-2^{37}	13205450-**233549482 I**	**i 23979-573590 I**	203-**5686 I**	**h 9-211 J**	3-**8 J**

$h_{K_0} = u'_{K_0} = u_{K_0}$ and for $k \geq K_0$

$$\begin{aligned} h_{k+1} &= h_k - v(\rho) + \sum_{l=d}^{a} \mu_l I(\rho, l), \\ u'_{k+1} &= \min\left\{ h_{k+1}, u'_k - \left\lceil \frac{u'_k v(\rho)}{\min\{q^{mn} - k, B(u'_k)\}} \right\rceil \right\}. \end{aligned}$$

Then, $K_{\mathrm{R}}(q^m, n, \rho) \leq \min\{k : u'_k = 0\}$.

Proof: Let C_0 be an $(n, n-a, a+1)$ MRD code over $\mathrm{GF}(q^m)$. C_0 has cardinality K_0 and covers $q^{m(n-a)}v(\rho) = q^{mn} - u_{K_0}$ vectors in $\mathrm{GF}(q^m)^n$. By Lemma 4, adding $k - K_0$ codewords of an MRD code which properly contains C_0 leads to a code with cardinality k which covers at least $q^{mn} - h_k$ vectors. On the other hand, u'_k is the upper bound on the number of vectors yet to be covered by a code of cardinality k that is obtained recursively either by applying the greedy approach in the proof of Lemma 3 or by adding more codewords based on the MRD codes as described above. The recursion of u'_k follows from this construction. Since this recursion is constructive, there exists a code with cardinality k which leaves at most u'_k vectors uncovered, and hence $K_{\mathrm{R}}(q^m, n, \rho) \leq \min\{k : u'_k = 0\}$. ∎

We now construct a new class of covering codes with the rank metric. We assume all the vectors in $\mathrm{GF}(q^m)^n$ are expanded with respect to a given basis of $\mathrm{GF}(q^m)$ to $m \times n$ matrices over $\mathrm{GF}(q)$. First, for any positive integer k, we denote $S_k \stackrel{\mathrm{def}}{=} \{0, 1, \ldots, k-1\}$. For $\mathbf{V} \in \mathrm{GF}(q)^{m \times n}$, $I \subseteq S_m$, and $J \subseteq S_n$, we denote $\mathbf{V}(I, J) = (v_{i,j})_{i \in I, j \in J}$, where the indexes are all sorted increasingly. Consider the code C which consists of all matrices $\mathbf{C} \in \mathrm{GF}(q)^{m \times n}$ with $\mathbf{C}(S_\rho, S_n) = \mathbf{0}$ and with at most $n - \rho$ nonzero columns.

Proposition 3: C has covering radius ρ and $K_{\mathrm{R}}(q^m, n, \rho) \leq |C| = \sum_{i=0}^{n-\rho} \binom{n}{i} (q^{m-\rho} - 1)^i$.

In order to illustrate the improvement due to the bounds in this paper, similar to [1], we provide the tightest lower and upper bounds on $K_{\mathrm{R}}(2^m, n, \rho)$ for $2 \leq m \leq 7$, $2 \leq n \leq m$, and $1 \leq \rho \leq 6$ in Table I. The improved entries in Table I due to the results in this paper are boldface, and are associated with letters indicating the sources. The lower bound on $K_{\mathrm{R}}(q^m, n, \rho)$ in [1, Proposition 8] is based on $I(\rho, d)$. However, due to the lack of analytical expression for $I(\rho, d)$, in [1] we were able to compute $I(\rho, d)$ only for small values, using exhaustive search. Using (1)-(3), we calculate $I(u, s, w)$ and hence the bound in [1, Proposition 8] for any set of parameter values, and the improved entries for this reason are associated with the lower case letter i. The lower case letter h and the upper case letters I and J correspond to improvements due to Propositions 1, 2, and 3, respectively. The unmarked entries in Table I are the same as those in [1].

REFERENCES

[1] M. Gadouleau and Z. Yan, "Packing and covering properties of rank metric codes," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3873-3883, Sept. 2008.

[2] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3951-3967, Sept. 2008.

[3] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579-3591, Aug. 2008.

[4] M. Gadouleau and Z. Yan, "Construction and covering properties of constant-dimension codes," submitted to *IEEE Trans. Inform. Theory*, 2009. Available at http://arxiv.org/abs/0903.2675.

[5] —— (2009), "Bounds on covering codes with the rank metric." [Online]. Available: http://arxiv.org/abs/0809.2968

[6] G. E. Andrews, *The Theory of Partitions*, ser. Encyclopedia of Mathematics and its Applications, G.-C. Rota, ed. Reading, MA: Addison-Wesley, 1976, vol. 2.

[7] P. Delsarte, "Properties and applications of the recurrence F(i + 1; k + 1; n+1) = qk+1F(i; k+1; n)..qkF(i; k; n)," *SIAM J. Applied Mathematics*, vol. 31, no. 2, pp. 262-270, Sept. 1976.

[8] E. Bannai and T. Ito, *Algebraic Cominatorics I. Association Schemes*. The Benjamin/Cummings Publishing Company, 1983.

[9] W. E. Clark and L. A. Dunning, "Tight upper bounds for the domination numbers of graphs with given order and minimum degree," *Electronic J. Combinatorics*, vol. 4, 1997.