EVALUATION OF FORMS FOR DISTINGUISHING RANK-METRIC CODES

VALENTINA ASTORE[1,2], MARTINO BORELLO[3,1], MARCO CALDERINI[4], AND FLAVIO SALIZZONI[5]

Abstract. Rank-metric codes have been a central topic in coding theory due to their theoretical and practical significance, with applications in network coding, distributed storage, and post-quantum cryptography. Recent research has focused on constructing new families of rank-metric codes with distinct algebraic structures, emphasizing the importance of invariants for distinguishing these codes from known families and random ones. In this paper, we introduce a novel geometric invariant for linear rank-metric codes, inspired by the Schur product used in the Hamming metric.

Key words: Rank-metric codes, Schur product, generalized Gabidulin codes.

1. Introduction

Rank-metric codes, introduced in 1978 [4,5], have gained attention for both theoretical interest and practical applications, including network coding, distributed storage, crisscross error correction, and cryptography. Gabidulin codes, in particular, were proposed for cryptographic use as early as 1991 [6], but only with the recent focus on post-quantum security have they seen renewed prominence.

This interest has driven the search for new families of optimal codes distinct from Gabidulin codes, especially as most MRD codes are not Gabidulin when large fields are considered [11].

An important step in constructing new codes is proving their inequivalence to known families, and, in this contest, practical invariants are desirable. Moreover, distinguishing a cryptographic code from a random one could threaten security. Few invariants exist: for example, [7,8,12] study invariants based on the dimension of the intersection of the code with itself under some field automorphism.

Similar issues arise in Hamming metric codes, where the Schur product is crucial. The dimension of the Schur product can be used to distinguish generalized Reed-Solomon codes from random ones [13], leading to cryptographic attacks [3].

In this work, we propose a geometric invariant for linear rank-metric codes, based on the Schur powers of the associated extended Hamming code [1]. We show that the dimension sequence of these Schur powers distinguishes Gabidulin codes from random ones. Geometrically, this corresponds to studying the vanishing ideal of the linear set associated with the code. In particular, the behaviour of forms of a certain degree distinguishes (generalized) Gabidulin codes from random ones.

2. Background

Let q be a prime power, $\mathbb{F}_q$ be the finite field with q elements, and m, n be two positive integers. A (linear) *rank-metric code* $\mathcal{C}$ is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank metric $(d_{\mathrm{rk}}((v_1,\dots,v_n),(w_1,\dots,w_n))$ is defined as the $\dim_{\mathbb{F}_q}\langle v_1-w_1,\dots,v_n-w_n\rangle_{\mathbb{F}_q})$. If k is its dimension and d is its minimum rank distance, we say that $\mathcal{C}$ is an $[n,k,d]_{q^m/q}$ code. A *generator matrix* G for $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$. If the $\mathbb{F}_q$-dimension of the columns of G is equal to n,

[1]INRIA, France

[2]LIX, École polytechnique, Institut Polytechnique de Paris, France

[3]Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France.

[4]University of Trento, Italy.

[5]MPI-MiS, Leipzig, Germany.

E-mail addresses: valentina.astore@inria.fr, martino.borello@univ-paris8.fr, marco.calderini@unitn.it, flavio.salizzoni@mis.mpg.de.

then we say that $\mathcal{C}$ is *nondegenerate*. Two rank-metric codes $\mathcal{C}$ and $\mathcal{C}'$ are *equivalent* if there exists an $\mathbb{F}_{q^m}$-linear *isometry*.

2.1. **Maximum rank distance codes.**

Theorem 2.1 ([5, Section 2])**.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an $[n,k,d]_{q^m/q}$ code, with $n \leq m$. Then $k \leq n-d+1$.

Codes attaining the previous bound are called *maximum rank distance* (*MRD*) *codes*. Any linear MRD code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension k has a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ in systematic form, i.e.,

$$G = [\, I_k \,|\, X \,],$$

where all entries of X are elements of $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$ [8, Lemma 5.3]. It was shown in [11, Theorem 4.6] that, when large field extension degrees are considered, a randomly chosen systematic generator matrix defines an MRD code with high probability. In this work, we focus on a specific family of MRD codes:

Definition 2.2. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ be linearly independent elements over $\mathbb{F}_q$ and $s \in \mathbb{N}$ with$\gcd(s,m) = 1$. A *generalized Gabidulin code* $\mathcal{G}_{s,k}(\alpha_1, \ldots, \alpha_n)$ *with parameter* s *and of dimension* k over $\mathbb{F}_{q^m}^n$ is the rank-metric code whose generator matrix is

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^{[s]} & \alpha_2^{[s]} & \cdots & \alpha_n^{[s]} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{[s(k-1)]} & \alpha_2^{[s(k-1)]} & \cdots & \alpha_n^{[s(k-1)]} \end{pmatrix},$$

where, for a nonnegative integer i, we write $[i]$ to mean q^i. If $s = 1$, we will simply say that $\mathcal{G}_k = \mathcal{G}_{1,k}(\alpha_1, \ldots, \alpha_n)$ is a *Gabidulin code of dimension* k.

Hereafter, for a positive integer s and a given matrix (or vector) X, we denote by $X^{[s]}$ the matrix (or vector) obtained by raising all entries of X to the power q^s.
The following result present a useful characterization of generalized Gabidulin codes.

Lemma 2.3 ([11, Lemma 3.3])**.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear MRD code of dimension k with generator matrix $[\, I_k \,|\, X \,]$, and $s \in \{1, \ldots, m-1\}$ with $\gcd(s,m) = 1$. Then, $\mathcal{C}$ is a generalized Gabidulin code with parameter s if and only if $\mathrm{rk}(X^{[s]} - X) = 1$.

2.2. **Schur product in the Hamming metric.**

We denote by $*$ the standard component-wise product in $\mathbb{F}_{q^m}^n$, i.e., for $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathbb{F}_{q^m}^n$,

$$v * w = (v_1 w_1, \ldots, v_n w_n).$$

Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_{q^m}^n$ be two linear codes. The *Schur product* $\star$ of $\mathcal{C}_1$ and $\mathcal{C}_2$ is defined as

$$\mathcal{C}_1 \star \mathcal{C}_2 = \langle c_1 * c_2 \,:\, c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2 \rangle_{\mathbb{F}_{q^m}}.$$

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code and let $\mathcal{C}^{(0)} = \langle (1, \ldots, 1) \rangle_{\mathbb{F}_{q^m}}$. For $i \geq 1$, the *i-th Schur power* of $\mathcal{C}$ is

$$\mathcal{C}^{(i)} = \mathcal{C} \star \mathcal{C}^{(i-1)} = \underbrace{\mathcal{C} \star \cdots \star \mathcal{C}}_{i \text{ times}}.$$

The Schur product between linear codes has been largely studied. In particular, it is well-known that the dimension of the Schur square distinguishes algebraic structured linear codes, such as Reed-Solomon codes, from random ones (see [10, Corollary 27]).
In this context, we are particularly interested in the following definition.

Definition 2.4. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code. The sequence of integers

$$\dim\left(\mathcal{C}^{(i)}\right) \text{ for } i \geq 0$$

is called the *dimension sequence*, or the *Hilbert sequence*, of $\mathcal{C}$. The *Castelnuovo-Mumford regularity* of $\mathcal{C}$ is the smallest integer $r = r(\mathcal{C}) \geq 0$ such that, for every $t \geq r$,

$$\dim\left(\mathcal{C}^{(t)}\right) = \dim\left(\mathcal{C}^{(r)}\right).$$

The terms *Hilbert sequence* and *Castelnuovo-Mumford regularity* are borrowed from commutative algebra, where analogous concepts are defined. The close connection between these objects is clarified in the following proposition.

Proposition 2.5 ([14, Proposition 1.28])**.** Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code with generator matrix $G = [\ g_1 \mid g_2 \mid \cdots \mid g_n\ ]$, where each column g_i is nonzero for all $i \in \{1, \ldots, n\}$. Let

$$\Pi_G = \{\langle g_1\rangle_{q^m}, \ldots, \langle g_n\rangle_{q^m}\} \subseteq \mathrm{PG}(k-1, q^m),$$

where $\langle g_i\rangle_{q^m}$ is the projective point associated to g_i. Then,

(1) the dimension sequence of $\mathcal{C}$ is equal to the Hilbert function of Π_G,
(2) the regularity $r(\mathcal{C})$ of $\mathcal{C}$ is equal to the Castelnuovo-Mumford regularity of Π_G,
(3) $\dim\left(\mathcal{C}^{(t)}\right) = |\Pi_G|$, for all $t \geq r(\mathcal{C})$,

where we define the Hilbert function and the Castelnuovo-Mumford regularity of Π_G as those of its homogeneous coordinate ring.

2.3. **The associated Hamming-metric code.** In the following, we want to generalize the previous concept to rank-metric codes. In order to do that, we need to introduce the notion of Hamming-metric code associated to a rank-metric one, as well as the geometric interpretation of rank-metric codes.
Let $\mathcal{C}$ be a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code. Let G be a generator matrix of $\mathcal{C}$ and $g_1, \ldots, g_n \in \mathbb{F}_{q^m}^k$ be the columns of G. The $\mathbb{F}_q$-vector space

$$\mathcal{U}_G = \langle g_1, \ldots, g_n\rangle_{\mathbb{F}_q}$$

has $\mathbb{F}_q$-dimension n and $\langle \mathcal{U}_G\rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$. Thus, $\mathcal{U}_G$ is naturally called an $[n, k]_{q^m/q}$-*system* associated to the code $\mathcal{C}$. Two $[n, k]_{q^m/q}$-systems $\mathcal{U}$ and $\mathcal{U}'$ are said to be *equivalent* if there is an $\mathbb{F}_{q^m}$-isomorphism $\varphi : \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}^k$ such that $\varphi(\mathcal{U}) = \mathcal{U}'$. Clearly, if G and G' are two generator matrices of the same code, $\mathcal{U}_G$ and $\mathcal{U}_{G'}$ are equivalent. As a consequence, with a little abuse of notation, we may drop the index and simply talk about the $[n, k]_{q^m/q}$-system $\mathcal{U}$ associated to $\mathcal{C}$. It is also straightforward to see that equivalent codes are associated to equivalent systems (see [1]).
Let now $\sim_{\mathbb{F}_q}$ be the proportionality relation over $\mathbb{F}_{q^m}^k$ such that, for $u, v \in \mathbb{F}_{q^m}^k$, $u \sim_{\mathbb{F}_q} v$ if and only if $u = \lambda v$ for some $\lambda \in \mathbb{F}_q^*$.

Definition 2.6. Let $\mathcal{U}$ be the $[n, k]_{q^m/q}$-system associated to the nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code $\mathcal{C}$. Let $G^{\mathrm{H}}(\mathcal{U}) \in \mathbb{F}_{q^m}^{k\times N}$ be a matrix whose columns form a set of representatives for the set of equivalence classes $\left(\mathcal{U} \setminus \{0\}\right)/\sim_{\mathbb{F}_q}$. Let $\mathcal{C}^{\mathrm{H}}$ be the $[N, k]_{q^m}$ code generated by $G^{\mathrm{H}}(\mathcal{U})$, where $N = (q^n - 1)/(q - 1)$. Then, we will denote $\mathcal{C}^{\mathrm{H}}$ as a *Hamming-metric code associated* to $\mathcal{C}$.

Proposition 2.7. Let $\mathcal{C}$ be a nondegenerate $[n, k, d]_{q^m/q}$ rank-metric code. Then, its associated Hamming-metric code $\mathcal{C}^{\mathrm{H}}$ is unique up to columns permutation and right multiplication by a diagonal matrix with entries in $\mathbb{F}_q^*$.

The associated Hamming-metric code is closely related to some geometric objects called *linear sets*, introduced by Lunardon in [9] to construct blocking sets.

Definition 2.8. Let $\mathcal{U}$ be an $[n, k]_{q^m/q}$-system. The $\mathbb{F}_q$-*linear set* of rank n associated with $\mathcal{U}$ is

$$L_{\mathcal{U}} := \left\{\langle u\rangle_{\mathbb{F}_{q^m}} \ :\ u \in \mathcal{U} \setminus \{0\}\right\} \subseteq \mathrm{PG}(k-1, q^m).$$

Two linear sets are said to be *equivalent* if their systems are equivalent.

Then, the *geometric object associated* to a rank-metric code $\mathcal{C}$ with generator matrix G is $L_{\mathcal{U}_G}$. Changing the generator matrix trivially results in equivalent linear sets. Moreover, equivalent rank-metric codes correspond to equivalent associated linear sets. In our context, the following remark is particularly important.

Remark 2.9. Let $\mathcal{C}$ be a $[n,k]_{q^m/q}$ code, G be a generator matrix of $\mathcal{C}$ and $\mathcal{C}^{\mathrm{H}}$ be the Hamming-metric code associated to $\mathcal{C}$, with generator matrix G^{H}. Then, $L_{\mathcal{U}_G} = \Pi_{G^{\mathrm{H}}}$.

3. $\mathbb{F}_q$-dimension sequence of rank-metric codes

The dimension sequence is an important geometric invariant of Hamming-metric codes, which may be used to differentiate between algebraic structured codes and random ones. It might seem natural to define the dimension sequence similarly for rank-metric codes. However, this approach presents two relevant drawbacks:

- the dimension sequence often converges too quickly, so there is not enough "space" to discriminate between families of MRD codes and random ones;
- it is not invariant under rank-metric equivalences, as highlighted in the following example.

Example 3.1. Let $\mathcal{C}_1 = \langle (1,0,1),(1,1,0)\rangle_{\mathbb{F}_{q^m}}$ and $\mathcal{C}_2 = \langle (1,0,0),(0,1,0)\rangle_{\mathbb{F}_{q^m}}$ be two $[3,2,1]_{q^m/q}$ codes. Although the two codes are equivalent, we have $\dim\left(\mathcal{C}_1^{(2)}\right) = 3$ and $\dim\left(\mathcal{C}_2^{(2)}\right) = 2$.

Therefore, we propose the following definition of $\mathbb{F}_q$-dimension sequence for rank-metric codes.

Definition 3.2. The $\mathbb{F}_q$-*dimension sequence*, or $\mathbb{F}_q$-*Hilbert sequence*, $\{h_i(\mathcal{C})\}_{i\geq 0}$ of a nondegenerate rank-metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is the Hilbert sequence of the associate code $\mathcal{C}^{\mathrm{H}}$, that is

$$h_i(\mathcal{C}) = \dim_{\mathbb{F}_{q^m}}\left(\mathcal{C}^{\mathrm{H}(i)}\right).$$

Moreover, the $\mathbb{F}_q$-*Castelnuovo-Mumford regularity* $r(\mathcal{C})$ of $\mathcal{C}$ is the Castelnuovo-Mumford regularity of $\mathcal{C}^{\mathrm{H}}$.

Remark 3.3. The $\mathbb{F}_q$-dimension sequence and the $\mathbb{F}_q$-Castelnuovo-Mumford regularity do not depend on the choice of $\mathcal{C}^{\mathrm{H}}$, hence they are well-defined. Moreover, let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two equivalent codes and G_1^{H} and G_2^{H} be two extended matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. Then, $\Pi_{G_1^{\mathrm{H}}} = \Pi_{G_2^{\mathrm{H}}}$, and therefore $h_i(\mathcal{C}_1) = h_i(\mathcal{C}_2)$, for all $i \geq 0$. Looking at Remark 2.9, we realize that we are merely considering the dimension sequence of the linear set $L_{\mathcal{U}_G}$ associated with the code $\mathcal{C}$ via a generator matrix G.

Theorem 3.4. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code of dimension k and generator matrix G. Let also $\mathcal{I}(L_{\mathcal{U}_G})$ be the vanishing ideal of $L_{\mathcal{U}_G}$ in $\mathbb{F}_{q^m}[x_1,\dots,x_k]$. Then, for every positive integer i,

$$h_i(\mathcal{C}) = \binom{k+i-1}{i} - \dim_{\mathbb{F}_{q^m}}\left(\mathcal{I}(L_{\mathcal{U}_G})_i\right),$$

where $\mathcal{I}(L_{\mathcal{U}_G})_i$ is the set of all homogeneous polynomials in $\mathcal{I}(L_{\mathcal{U}_G})$ of degree i. In particular, for $i \in \{1,\dots,q\}$,

$$h_i(\mathcal{C}) = \binom{k+i-1}{i}.$$

Let $\mathcal{F}_s := \left\langle x_i^{[s]}x_j - x_i x_j^{[s]} \,:\, 1 \leq i < j \leq k\right\rangle_{\mathbb{F}_{q^m}}$. The following result shows that $\mathrm{rk}(X^{[s]} - X)$ is related to the dimension of the subspaces of $\mathcal{F}_s$ vanishing on the points of the linear set associated to the code generated by $[\,I_k \,|\, X\,]$.

Theorem 3.5. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a code of dimension k with generator matrix $G = [\,I_k \,|\, X\,]$, where $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$, and let $s \in \{1,\dots,m-1\}$ with $\gcd(s,m) = 1$. Let also $\mathcal{I}(L_{\mathcal{U}_G})$ be the vanishing ideal of the linear set $L_{\mathcal{U}_G}$ (which contains $\mathrm{PG}(k-1,q)$). Then, for $r \in \{0,\dots,k\}$,

$$\mathrm{rk}(X^{[s]} - X) = r \quad \text{if and only if} \quad \dim \mathcal{F}_s \cap \mathcal{I}(L_{\mathcal{U}_G}) = \binom{k-r}{2},$$

where $\binom{k-r}{2} = 0$ for $r = k-1$ or $r = k$.

Corollary 3.6. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension k with generator matrix $G = [\, I_k \,|\, X \,]$, where $X \in \mathbb{F}_{q^m}^{k\times(n-k)}$, and let $s \in \{1, \ldots, m-1\}$ with $\gcd(s, m) = 1$. Let also $\mathcal{I}(L_{\mathcal{U}_G})$ be the vanishing ideal of the linear set $L_{\mathcal{U}_G}$. Then, $\mathcal{C}$ is a generalized Gabidulin code with parameter s if and only if

$$\dim \mathcal{F}_s \cap \mathcal{I}(L_{\mathcal{U}_G}) = \binom{k-1}{2}.$$

Since, $\dim_{\mathbb{F}_{q^m}}(\mathcal{I}_{q^s+1}(L_{\mathcal{U}_G})) \geq \dim_{\mathbb{F}_{q^m}}(\mathcal{I}(L_{\mathcal{U}_G}) \cap \mathcal{F}_s)$, in general, we have $h_{q^s+1}(\mathcal{C}) \leq \binom{k+q^s}{q^s+1} - \binom{k-r}{2}$. For $s = 1$, the vanishing ideal over $\mathbb{F}_{q^m}$ of $\mathrm{PG}(k-1, q)$ is the ideal generated by $\mathcal{F}_1$ ([2, Theorems 2.5 and 2.8]), implying:

Corollary 3.7. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be an MRD code of dimension $k < n$. Then, $\mathcal{C}$ is a Gabidulin code if and only if

$$h_{q+1}(\mathcal{C}) = \binom{k+q}{q+1} - \binom{k-1}{2}.$$

Computational results show that this cannot be extended directly to generalized Gabidulin codes, for which we have the following conjecture:

Conjecture 3.8. Let $\mathcal{G}_{s,k} \subseteq \mathbb{F}_{q^m}^n$ be a generalized Gabidulin code of dimension k with parameter s such that $sk - 1 \leq n$, and m sufficiently large ($m > n$). Then,

$$h_{q^s+1}(\mathcal{G}_{s,k}) = \binom{k+q^s}{q^s+1} - \binom{k-1}{2}.$$

References

[1] G. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *Journal of Combinatorial Theory, Series A*, 192:105658, 2022.

[2] P. Beelen, M. Datta, and S. R. Ghorpade. Vanishing ideals of projective spaces over finite fields and a projective footprint bound. *Acta Mathematica Sinica, English Series*, 35(1):47–63, 2019.

[3] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. *Designs, Codes and Cryptography*, 73:641–666, 2014.

[4] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226–241, 1978.

[5] E. M. Gabidulin. Theory of codes with maximum rank distance (translation). *Problemy peredachi informatsii*, 21(1):3–16, 1985.

[6] E. M. Gabidulin, A. Paramonov, and O. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8–11, 1991 Proceedings 10*, pages 482–489. Springer, 1991.

[7] L. Giuzzi and F. Zullo. Identifiers for MRD-codes. *Linear Algebra and its Applications*, 575:66–86, 2019.

[8] A.-L. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank-metric code constructions. *Advances in Mathematics of Communications*, 11(3):533–548, 2017.

[9] G. Lunardon. Normal spreads. *Geometriae Dedicata*, 75:245–261, 1999.

[10] D. Mirandola and G. Zémor. Critical pairs for the product singleton bound. *IEEE Transactions on Information Theory*, 61(9):4928–4937, 2015.

[11] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86:341–363, 2018.

[12] A. Neri, S. Puchinger, and A.-L. Horlemann-Trautmann. Equivalence and characterizations of linear rank-metric codes based on invariants. *Linear Algebra and its Applications*, 603:418–469, 2020.

[13] R. Pellikaan and I. Márquez-Corbella. Error-correcting pairs for a public-key cryptosystem. In *Journal of Physics: Conference Series*, volume 855, page 012032. IOP Publishing, 2017.

[14] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. *Algorithmic arithmetic, geometry, and coding theory*, 637:3–78, 2015.