This is the peer reviewd version of the followng article:

Non-minimum tensor rank Gabidulin codes / Bartoli, D.; Zini, G.; Zullo, F.. - In: LINEAR ALGEBRA AND ITS APPLICATIONS. - ISSN 0024-3795. - 650:(2022), pp. 248-266. [10.1016/j.laa.2022.06.012]

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

12/10/2024 10:33

(Article begins on next page)

arXiv:2201.08242v1 [cs.IT] 20 Jan 2022

Non-minimum tensor rank Gabidulin codes

Daniele Bartoli* and Giovanni Zini† and Ferdinando Zullo‡

Abstract

The tensor rank of some Gabidulin codes of small dimension is investigated. In particular, we determine the tensor rank of any rank metric code equivalent to an 8-dimensional $\mathbb{F}_q$-linear generalized Gabidulin code in $\mathbb{F}_q^{4\times 4}$. This shows that such a code is never minimum tensor rank. In this way, we detect the first infinite family of Gabidulin codes which are not minimum tensor rank.

1 Introduction

Rank metric codes were introduced by Delsarte [9] in 1978 and have been used in several contexts, such as crisscross error correction [23], cryptography [14], and network coding [25]. Because of their ubiquitous applications, they attracted increasing attention in the last years; see e.g. [15, 22, 24].

Very recently, rank metric codes have been investigated through their tensor rank; see [4–6]. Indeed, a rank metric code $\mathcal{C}$ in $\mathbb{F}_q^{n\times m}$ can be seen as the *slice space* of an associated *generator* 3-*tensor*, similarly to the case of linear codes in the Hamming metric, where a code can be described as the row space of a generator matrix. Therefore, after Byrne, Neri, Ravagnani and Sheekey [6], the **tensor rank** of $\mathcal{C}$ is defined as the tensor rank of a generator tensor of $\mathcal{C}$. Determining the tensor rank of a certain rank metric code is a hard problem in general and the exact value is known only for specific classes of codes; indeed the problem of computing the rank of a 3-tensor is NP-complete [16]. Several lower and upper bounds for the tensor rank of a rank metric code were presented in [6] and [4]. In particular, as a consequence of Kruskal's bound [11], the tensor rank of an h-dimensional $\mathbb{F}_q$-linear rank metric code $\mathcal{C}$ in $\mathbb{F}_q^{n\times m}$ of minimum distance d is lower bounded by $h-d+1$. The code $\mathcal{C}$ is said to be **minimum tensor rank** (**MTR** for short) if its tensor rank is exactly $h-d+1$. The interest for rank metric codes with a low tensor rank is due to the following fact: the smaller the tensor rank of the generating tensors, the more efficient the encoding. Via the

*Department of Mathematics and Informatics, University of Perugia, Perugia, Italy. Email address: daniele.bartoli@unipg.it

†Department of Physics, Informatics and Mathematics, University of Modena and Reggio Emilia, Modena, Italy. Email address: giovanni.zini@unimore.it

‡Department of Mathematics and Physics, University of Campania, Caserta, Italy. Email address: ferdinando.zullo@unicampania.it

correspondence in [8] between full rank codes and semifields, the notion of tensor rank for rank metric codes extends the same notion for semifields, which was used as an invariant by Lavrauw in [17]. Moreover, some criteria by Kruskal [11, Section 4] use the rank of a tensor to assure its identifiability, i.e. the uniqueness of the pure tensors appearing in its decomposition, which is of interest for the numerical applications within statistics; see [7] and [1, Section 2].

A family of particular interest among rank metric codes is the one of square Gabidulin codes $\mathcal{G}_{k,s}$ in $\mathbb{F}_q^{n\times n}$, as they are *maximum rank distance*, and indeed they have been deeply investigated. However, their tensor rank is not known in general; exact results have been provided in [6] and [4] when $k \in \{1, n-1\}$ and in few other cases. Interestingly, when q is large enough, Gabidulin codes with $k \in \{1, n-1\}$ turn out to be MTR codes.

In this paper we are interested in determining the tensor rank of those codes which are equivalent to an $\mathbb{F}_q$-linear 8-dimensional Gabidulin code in $\mathbb{F}_q^{4\times 4}$. The strategy that we apply makes use of [6, Proposition 3.4], which involves rank-one matrices. The framework of our arguments is the one of linearized polynomials, where rank-one matrices correspond to trace functions of the shape $\alpha\mathrm{Tr}(\beta x)$, where $\mathrm{Tr} : \mathbb{F}_{q^4} \to \mathbb{F}_q$ and $\mathrm{Tr}(x) = x + x^q + x^{q^2} + x^{q^3}$. Our main result is the following.

Theorem 1.1. *Let q be a prime power, and $\mathcal{C}$ be a code which is equivalent to an $\mathbb{F}_q$-linear 8-dimensional generalized Gabidulin code in $\mathbb{F}_q^{4\times 4}$. Then the tensor rank of $\mathcal{C}$ is 11 if $q \geq 3$, and 12 if $q = 2$. In particular, $\mathcal{C}$ is not MTR.*

The paper is organized as follows. Section 2 contains preliminary notions on rank metric codes and on the correspondence with linearized polynomials in the case of square codes. Section 3 describes basic definitions and known results about tensors and the tensor rank of square generalized Gabidulin codes. Section 4 is devoted to the proof of Theorem 1.1: Section 4.1 shows that $\mathcal{C}$ is not MTR, while in Section 4.2 we determine the tensor rank of $\mathcal{C}$ for $q \geq 5$. The remaining small values of q, are worked out computationally in Section 5, as well as other Gabidulin codes in $\mathbb{F}_q^{n\times n}$ with small values of q and n. Finally, the Appendix contains two auxiliary results which are needed in Section 4.1, whose proof are quite technical.

2 Rank metric codes and linearized polynomials

The set $\mathbb{F}_q^{n\times m}$ of matrices can be equipped with the **rank metric**, as

$$d(A, B) = \mathrm{rk}\,(A - B), \qquad \text{for } A, B \in \mathbb{F}_q^{n\times m}.$$

A **rank metric code** is a subset $\mathcal{C}$ of $\mathbb{F}_q^{n\times m}$ endowed with the rank metric and its **minimum rank distance** is defined as

$$d := d(\mathcal{C}) = \min\{d(A, B) \colon A, B \in \mathcal{C},\ A \neq B\}.$$

Two $\mathbb{F}_q$-linear rank metric codes $\mathcal{C}$ and $\mathcal{C}'$ in $\mathbb{F}_q^{n\times m}$ are **linearly equivalent** if and only if there exist $X \in \mathrm{GL}(n,q)$ and $Y \in \mathrm{GL}(m,q)$ such that

$$\mathcal{C}' = \{XCY : C \in \mathcal{C}\},$$

or, if $m = n$,

$$\mathcal{C}' = \{XC^\top Y : C \in \mathcal{C}\},$$

where $C^\top$ denote the transpose of C. Since in this paper we will only consider linear equivalence, we will refer to it simply as *equivalence*.

Delsarte showed in [9] that the parameters of a rank metric code $\mathcal{C}$ satisfy a Singleton-like bound, namely

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}.$$

When equality holds, we call $\mathcal{C}$ a **maximum rank distance** (**MRD** for short) code.

In this paper we are interested only in the square case $m = n$, and in this case rank metric codes can be described in terms of linearized polynomials. Indeed, consider the $\mathbb{F}_q$-**linearized** (or simply **linearized**) polynomials of normalized degree over $\mathbb{F}_{q^n}$, i.e. elements of the form

$$f(x) = \sum_{i=0}^{n-1} f_i x^{q^i}, \quad f_i \in \mathbb{F}_{q^n}.$$

The set of linearized polynomials is an $\mathbb{F}_q$-algebra $\mathcal{L}_{n,q}$ with the usual addition, the scalar multiplication by elements of $\mathbb{F}_q$ and the composition modulo $x^{q^n} - x$. It is well-known that the $\mathbb{F}_q$-algebras $\mathcal{L}_{n,q}$ and $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ are isomorphic, via the correspondence between the linearized polynomial $f(x)$ and the $\mathbb{F}_q$-endomorphism

$$\alpha \longmapsto \sum_{i=0}^{n-1} f_i \alpha^{q^i}$$

of $\mathbb{F}_{q^n}$. Hence, $\mathcal{L}_{n,q}$ is also isomorphic to the $\mathbb{F}_q$-algebra $\mathbb{F}_q^{n\times n}$ of $n \times n$ matrices over $\mathbb{F}_q$. In this correspondence, the rank of a matrix in $\mathbb{F}_q^{n\times n}$ equals the rank of the corresponding linearized polynomial in $\mathcal{L}_{n,q}$ as an $\mathbb{F}_q$-endomorphism of $\mathbb{F}_{q^n}$. Therefore, rank metric codes in $\mathbb{F}_q^{n\times n}$ can be seen as sets of linearized polynomials in $\mathcal{L}_{n,q}$, so that we can speak of rank metric codes in $\mathcal{L}_{n,q}$. Notice that the set of matrices of rank 1 in $\mathbb{F}_q^{n\times n}$ corresponds to the set of elements of $\mathcal{L}_{n,q}$ of the shape $\alpha\mathrm{Tr}(\beta x)$ for some $\alpha, \beta \in \mathbb{F}_{q^n}^*$, where $\mathrm{Tr}(z) = z + z^q + \cdots + z^{q^{n-1}}$; see [21, Theorem 2.24]. For a reference on linearized polynomials see [26].

The first class of square MRD codes in the literature was the one of **generalized Gabidulin codes**, namely the $\mathbb{F}_{q^n}$-subspaces

$$\mathcal{G}_{k,s} = \langle x, x^{q^s}, \ldots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^n}}$$

of $\mathcal{L}_{n,q}$, where $1 \leq k \leq n$ and $\gcd(s,n) = 1$; they are MRD codes with $\mathbb{F}_q$-dimension kn and minimum distance $n - k + 1$. Gabidulin codes where first introduced by Delsarte in [9] and later by Gabidulin in [13] in the case $s = 1$, and by Gabidulin and Kshevetskiy in [12] in the general case.

3 Tensor rank of generalized Gabidulin codes

The tensors we will investigate in this paper are 3-**tensors** in $\mathbb{F}_q^h \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m$. If $\{u_1, \dots, u_h\}$, $\{v_1, \dots, v_n\}$, and $\{w_1, \dots, w_n\}$ are bases of $\mathbb{F}_q^h$, $\mathbb{F}_q^n$, and $\mathbb{F}_q^m$ respectively, then an $\mathbb{F}_q$-basis of $\mathbb{F}_q^h \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m$ is given by

$$\{u_l \otimes v_i \otimes w_j \colon 1 \le l \le h, 1 \le i \le n, 1 \le j \le m\}.$$

The tensors of the form $u \otimes v \otimes w$, with $u \in \mathbb{F}_q^h$, $v \in \mathbb{F}_q^n$ and $w \in \mathbb{F}_q^m$, are called **simple** (or **pure**) **tensors**. The **tensor rank** of a tensor $X \in \mathbb{F}_q^h \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m$ is defined as

$$\operatorname{trk}(X) = \min \left\{ R \in \mathbb{N}_0 \colon X = \sum_{i=1}^{R} u_i \otimes v_i \otimes w_i,\ u_i \in \mathbb{F}_q^h, v_i \in \mathbb{F}_q^n, w_i \in \mathbb{F}_q^m \right\}.$$

Let $[i] = \{1, \dots, i\}$. A 3-tensor $X \in \mathbb{F}_q^h \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m$ can be represented as a map $X \colon [h] \times [n] \times [m] \to \mathbb{F}_q$ given by $X = (X_{lij} \colon 1 \le l \le h, 1 \le i \le n, 1 \le j \le m)$. Therefore $\mathbb{F}_q^h \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^m$ can be identified with the space $\mathbb{F}_q^{h \times n \times m}$, and the tensor X can be written as $X = (X_1, \dots, X_h)$ with $X_i \in \mathbb{F}_q^{n \times m}$. The **first slice space** of X, denoted by $\operatorname{ss}_1(X)$, is the $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n \times m}$ generated by $X_1, \dots, X_h$. If $\dim_{\mathbb{F}_q}(\operatorname{ss}_1(X)) = h$, we say that X is 1-**nondegenerate**.

The following result will be a key tool in our investigation.

Proposition 3.1. *(see [6, Proposition 3.4] and [3, Proposition 14.45]) Let $X \in \mathbb{F}_q^{h \times n \times m}$ and R be a positive integer. The following are equivalent:*

1. $\operatorname{trk}(X) \le R$;
2. *there exist $A_1, \dots, A_R \in \mathbb{F}_q^{n \times m}$ of rank 1 such that $\operatorname{ss}_1(X) \subseteq \langle A_1, \dots, A_R \rangle_{\mathbb{F}_q}$.*

In particular, $\operatorname{trk}(X) = R$ if and only if R is the minimum integer such that there exist $A_1, \dots, A_R \in \mathbb{F}_q^{n \times m}$ of rank 1 satisfying $\operatorname{ss}_1(X) \subseteq \langle A_1, \dots, A_R \rangle_{\mathbb{F}_q}$.

Kruskal in [11] bounded the tensor rank of a 3-tensor, using the following map:

$$m_1 \colon \mathbb{F}_q^{s \times h} \times \mathbb{F}_q^{h \times n \times m} \to \mathbb{F}_q^{s \times n \times m}, \quad \left(A, \sum_i u_i \otimes v_i \otimes w_i \right) \mapsto \sum_i (Au_i) \otimes v_i \otimes w_i.$$

Theorem 3.2. *(see [11, Corollary 1]) Let $X \in \mathbb{F}_q^{h \times n \times m}$ be 1-nondegenerate, then*

$$\operatorname{trk}(X) \ge h + \min\{\operatorname{trk}(m_1(u, X)) \colon u \in \mathbb{F}_q^h \setminus \{0\}\} - 1.$$

Tensors are related to rank metric codes as follows. Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{n \times m}$ of dimension h and minimum distance d. A **generator tensor** for $\mathcal{C}$ is a 3-tensor $X \in \mathbb{F}_q^{h \times n \times m}$ such that $\operatorname{ss}_1(X) = \mathcal{C}$. As proved in [6, Proposition 4.2], two generator tensors of the same rank metric code $\mathcal{C}$ have the same tensor rank. Therefore, we can define the **tensor rank** $\operatorname{trk}(\mathcal{C})$ of $\mathcal{C}$ as the tensor rank of any generator tensor of $\mathcal{C}$.

Proposition 3.3. *(see [6, Proposition 4.5]) If $\mathcal{C}, \mathcal{C}'$ are equivalent codes, then* $\mathrm{trk}(\mathcal{C}) = \mathrm{trk}(\mathcal{C}')$.

By Theorem 3.2,

$$\mathrm{trk}(\mathcal{C}) \geq h + d - 1. \tag{1}$$

If $\mathcal{C}$ attains equality in (1), it is called a **minimum tensor rank** (**MTR** for short) code.

Although Gabidulin codes form the most studied family of rank metric codes, the complete determination of their tensor rank is still missing. We now describe the known results on the tensor rank of square Gabidulin codes $\mathcal{G}_{k,s} \subset \mathcal{L}_{n,q}$. Bound (1) reads as follows.

Theorem 3.4. *For every $k \leq n$, we have* $\mathrm{trk}(\mathcal{G}_{k,s}) \geq (k+1)n - k$.

The tensor rank of $\mathcal{G}_{1,s}$ coincides with the tensor rank of the field $\mathbb{F}_{q^n}$ (see [10] and [20] where semifields were described for the first time in terms of tensors). By [3, Propositions 14.47 and 14.48] and a link with a well-studied tensor pointed out in [6, Lemma 5.13], it follows that $\mathrm{trk}(\mathcal{G}_{1,s}) = 2n-1$ if $q \geq 2n-1$, and $\mathrm{trk}(\mathcal{G}_{1,s}) > 2n-1$ if $q \leq 2n-2$. For $n = 3$, $\mathrm{trk}(\mathcal{G}_{1,s}) = 6$ if $q \in \{2, 3\}$ (see [19, Lemma 15] and also [18]). For $n = 4$, $\mathrm{trk}(\mathcal{G}_{1,s}) = 9$ if $q \in \{2, 3\}$ (see [6, Example 6.4] for $q = 2$ and [19, Theorem 4] for $q = 3$), while $\mathrm{trk}(\mathcal{G}_{1,s})$ is unknown for $q \in \{4, 5\}$. Further bounds and asymptotic results for the tensor rank of $\mathbb{F}_{q^n}$ are known, see e.g. [2].

The following upper bound follows from the tensor rank of $\mathcal{G}_{1,s}$.

Theorem 3.5. *(see [6, Proposition 5.15]) Let $q \geq 2n-2$. For every $k \leq n$, we have* $\mathrm{trk}(\mathcal{G}_{1,s}) \leq \min\{n^2, k(2n-1)\}$.

A partial result is known also in the case of Gabidulin codes $\mathcal{G}_{n-1,s}$.

Theorem 3.6. *(see [4, Theorem 5.15]) Let $q \geq n$. Then* $\mathrm{trk}(\mathcal{G}_{n-1,s}) = n^2 - n + 1$.

The tensor rank of Gabidulin codes $\mathcal{G}_{k,s}$ with $k \notin \{1, n-1\}$ is not known. In this paper we study the first open case, namely $k = 2$ and $n = 4$. In Section 5 we will investigate the remaining open cases when $n \leq 4$.

4 The tensor rank of $\mathcal{G}_{2,1} \subset \mathcal{L}_{4,q}$

The two 8-dimensional generalized Gabidulin codes $\mathcal{G}_{2,1}$ and $\mathcal{G}_{2,3}$ in $\mathcal{L}_{4,q}$ are easily seen to be equivalent. Therefore, by Proposition 3.3, in order to prove Theorem 1.1 it is enough to prove it for the Gabidulin code $\mathcal{G} = \mathcal{G}_{2,1} = \langle x, x^q \rangle_{\mathbb{F}_{q^4}}$. In Section 4.1 we show that the tensor rank of $\mathcal{G}$ is not 10 for any q. In Section 4.2 we prove that the tensor rank of $\mathcal{G}$ is 11 if $q \geq 5$. We complete the proof in Section 5, where we determine the tensor rank of some Gabidulin codes for some values of q.

4.1 The tensor rank of $\mathcal{G}$ is larger than 10

This section is devoted to the proof of the following theorem.

Theorem 4.1. *For any prime power q, we have* $\mathrm{trk}(\mathcal{G}) \geq 11$. *Thus, $\mathcal{G}$ is not an MTR code.*

By Proposition 3.1 and Section 2, $\mathrm{trk}(\mathcal{G}) = 10$ if and only if there exist 10 trace functions $\alpha_i \mathrm{Tr}(\beta_i x)$ such that $\mathcal{G} \subseteq \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \ldots, \alpha_{10} \mathrm{Tr}(\beta_{10} x) \rangle_{\mathbb{F}_q}$. This is equivalent to say that there exist $\alpha_1 \mathrm{Tr}(\beta_1 x), \alpha_2 \mathrm{Tr}(\beta_2 x)$ such that there exists an $\mathbb{F}_q$-basis of $\langle x, x^q \rangle_{\mathbb{F}_{q^4}} \oplus \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \alpha_2 \mathrm{Tr}(\beta_2 x) \rangle_{\mathbb{F}_q}$ only composed by traces. So, consider $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_{q^4}$ such that $H = \langle x, x^q \rangle_{\mathbb{F}_{q^4}} \oplus \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \alpha_2 \mathrm{Tr}(\beta_2 x) \rangle_{\mathbb{F}_q}$ has dimension 10 over $\mathbb{F}_q$.

The proof strategy relies on two steps:

Step 1: To find explicit necessary and sufficient conditions on $\alpha_3, \beta_3 \in \mathbb{F}_{q^4}$ such that $\alpha_3 \mathrm{Tr}(\beta_3 x) \in H$.

Step 2: To prove the non-existence of ten $\mathbb{F}_q$-linearly independent traces in H.

In Steps 1 and 2 we will also need auxiliary results (Theorems 6.1 and 6.2 respectively) which are in Appendix, due to their technicality.

Proof. **Step 1:** Suppose that $\alpha_3 \mathrm{Tr}(\beta_3 x)$ is in H. Then there exist $\gamma, \delta \in \mathbb{F}_{q^4}$, $c_1, c_2 \in \mathbb{F}_q$ such that

$$\alpha_3 \mathrm{Tr}(\beta_3 x) \quad = \quad \gamma x + \delta x^q + c_1 \alpha_1 \mathrm{Tr}(\beta_1 x) + c_2 \alpha_2 \mathrm{Tr}(\beta_2 x).$$

This polynomial identity implies that γ, δ, c_1, and c_2 satisfy the following system:

$$\begin{cases} \gamma + c_1 \alpha_1 \beta_1 + c_2 \alpha_2 \beta_2 & = \alpha_3 \beta_3, \\ \delta + c_1 \alpha_1 \beta_1^q + c_2 \alpha_2 \beta_2^q & = \alpha_3 \beta_3^q, \\ c_1 \alpha_1 \beta_1^{q^2} + c_2 \alpha_2 \beta_2^{q^2} & = \alpha_3 \beta_3^{q^2}, \\ c_1 \alpha_1 \beta_1^{q^3} + c_2 \alpha_2 \beta_2^{q^3} & = \alpha_3 \beta_3^{q^3}. \end{cases} \tag{2}$$

It cannot happen that β_2/β_1 and α_2/α_1 are both in $\mathbb{F}_q$. Indeed, if $\beta_2 = \rho \beta_1$ and $\alpha_2 = \omega \alpha_1$ for some $\rho, \omega \in \mathbb{F}_q$ then

$$\alpha_2 \mathrm{Tr}(\beta_2 x) = \rho \omega \alpha_1 \mathrm{Tr}(\beta_1 x)$$

and hence $\dim_{\mathbb{F}_q}(H) < 10$.

Note that if $c_1 = 0$, then the last two equations of System (2) yield $c_2 \alpha_2 / \alpha_3 = (\beta_3/\beta_2)^{q^2} = (\beta_3/\beta_2)^{q^3}$ which implies $\beta_3/\beta_2 \in \mathbb{F}_q^*$ and $\alpha_3/\alpha_2 \in \mathbb{F}_q^*$. This means that $\alpha_3 \mathrm{Tr}(\beta_3 x) = \lambda \alpha_2 \mathrm{Tr}(\beta_2 x)$ for some $\lambda \in \mathbb{F}_q$. A similar conclusion arises from $c_2 = 0$. So, in these cases $\alpha_3 \mathrm{Tr}(\beta_3 x) \in \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \alpha_2 \mathrm{Tr}(\beta_2 x) \rangle_{\mathbb{F}_q}$.

From now on we always assume $c_1 c_2 \neq 0$. By the last two equations in System (2) one gets

$$\beta_3^{q-1} = \frac{c_1 \alpha_1^{q^2} \beta_1^q + c_2 \alpha_2^{q^2} \beta_2^q}{c_1 \alpha_1^{q^2} \beta_1 + c_2 \alpha_2^{q^2} \beta_2} = \frac{\frac{c_1}{c_2} \alpha_1^{q^2} \beta_1^q + \alpha_2^{q^2} \beta_2^q}{\frac{c_1}{c_2} \alpha_1^{q^2} \beta_1 + \alpha_2^{q^2} \beta_2} =: A(c_1/c_2). \tag{3}$$

Note that, since $\beta_3 \neq 0$, $c_1\alpha_1^{q^2}\beta_1^q + c_2\alpha_2^{q^2}\beta_2^q = 0$ if and only if $c_1\alpha_1^{q^2}\beta_1 + c_2\alpha_2^{q^2}\beta_2 = 0$, that is β_1/β_2 and α_1/α_2 both belong to $\mathbb{F}_q^*$. Indeed, since c_1 and c_2 are both nonzero,

$$\det\begin{pmatrix} \alpha_1^{q^2}\beta_1^q & \alpha_2^{q^2}\beta_2^q \\ \alpha_1^{q^2}\beta_1 & \alpha_2^{q^2}\beta_2 \end{pmatrix} = 0,$$

which implies $\beta_1/\beta_2 \in \mathbb{F}_q^*$. Similarly, one can show that $\alpha_1/\alpha_2 \in \mathbb{F}_q^*$. However, this is a contradiction to our assumptions.

An element $\beta_3 \in \mathbb{F}_{q^4}$ satisfying Equation (3) exists if and only if $A(c_1/c_2)^{1+q+q^2+q^3} = 1$, that is,

$$\begin{aligned}(c_1\alpha_1^{q^2}\beta_1^q + c_2\alpha_2^{q^2}\beta_2^q)(c_1\alpha_1^{q^3}\beta_1^{q^2} + c_2\alpha_2^{q^3}\beta_2^{q^2})(c_1\alpha_1\beta_1^{q^3} + c_2\alpha_2\beta_2^{q^3})(c_1\alpha_1^q\beta_1 + c_2\alpha_2^q\beta_2) = \\ (c_1\alpha_1^{q^2}\beta_1 + c_2\alpha_2^{q^2}\beta_2)(c_1\alpha_1^{q^3}\beta_1^q + c_2\alpha_2^{q^3}\beta_2^q)(c_1\alpha_1\beta_1^{q^2} + c_2\alpha_2\beta_2^{q^2})(c_1\alpha_1^q\beta_1^{q^3} + c_2\alpha_2^q\beta_2^{q^3}). \qquad (4)\end{aligned}$$

We are interested in bounding the number of non-$\mathbb{F}_q$-proportional pairs (c_1, c_2), with $c_1c_2 \neq 0$. The above homogeneous polynomial in c_1 and c_2 is of degree at most three in both c_1 and c_2, and its coefficients are as follows:

i) the coefficient of c_2^4 is zero;

ii) the coefficient of $c_1c_2^3$ is

$$\begin{aligned}&-\alpha_1\alpha_2^{q+q^2+q^3}\beta_1^{q^2}\beta_2^{1+q+q^3} + \alpha_1\alpha_2^{q+q^2+q^3}\beta_1^{q^3}\beta_2^{1+q+q^2} + \alpha_1^q\alpha_2^{1+q^2+q^3}\beta_1\beta_2^{q+q^2+q^3} \\ &-\alpha_1^q\alpha_2^{1+q^2+q^3}\beta_1^{q^3}\beta_2^{1+q+q^2} - \alpha_1^{q^2}\alpha_2^{1+q+q^3}\beta_1\beta_2^{q+q^2+q^3} + \alpha_1^{q^2}\alpha_2^{1+q+q^3}\beta_1^q\beta_2^{1+q^2+q^3} \\ &-\alpha_1^{q^3}\alpha_2^{1+q+q^2}\beta_1^q\beta_2^{1+q^2+q^3} + \alpha_1^{q^3}\alpha_2^{1+q+q^2}\beta_1^{q^2}\beta_2^{1+q+q^3},\end{aligned}$$

iii) the coefficient of $c_1^2c_2^2$ is

$$\begin{aligned}&\alpha_1^{1+q}\alpha_2^{q^2+q^3}\beta_1^{1+q^3}\beta_2^{q+q^2} - \alpha_1^{1+q}\alpha_2^{q^2+q^3}\beta_1^{q^2+q^3}\beta_2^{1+q} - \alpha_1^{1+q^2}\alpha_2^{q+q^3}\beta_1^{1+q^2}\beta_2^{q+q^3} \\ &+\alpha_1^{1+q^2}\alpha_2^{q+q^3}\beta_1^{q+q^3}\beta_2^{1+q^2} - \alpha_1^{1+q^3}\alpha_2^{q+q^2}\beta_1^{q+q^2}\beta_2^{1+q^3} \\ &+\alpha_1^{1+q^3}\alpha_2^{q+q^2}\beta_1^{q^2+q^3}\beta_2^{1+q} + \alpha_1^{q+q^2}\alpha_2^{1+q^3}\beta_1^{1+q}\beta_2^{q^2+q^3} \\ &-\alpha_1^{q+q^2}\alpha_2^{1+q^3}\beta_1^{1+q^3}\beta_2^{q+q^2} + \alpha_1^{q+q^3}\alpha_2^{1+q^2}\beta_1^{1+q^2}\beta_2^{q+q^3} \\ &-\alpha_1^{q+q^3}\alpha_2^{1+q^2}\beta_1^{q+q^3}\beta_2^{1+q^2} - \alpha_1^{q^2+q^3}\alpha_2^{1+q}\beta_1^{1+q}\beta_2^{q^2+q^3} + \alpha_1^{q^2}\alpha_1^{q^3}\alpha_2^{1+q}\beta_1^{q+q^2}\beta_2^{1+q^3},\end{aligned}$$

iv) the coefficient of $c_1^3c_2$ is

$$\begin{aligned}&\alpha_1^{1+q+q^2}\alpha_2^{q^3}\beta_1^{1+q+q^3}\beta_2^{q^2} - \alpha_1^{1+q+q^2}\alpha_2^{q^3}\beta_1^{1+q^2+q^3}\beta_2^q + \alpha_1^{1+q+q^3}\alpha_2^{q^2}\beta_1^{1+q^2+q^3}\beta_2^q \\ &-\alpha_1^{1+q+q^3}\alpha_2^{q^2}\beta_1^{q+q^2+q^3}\beta_2 - \alpha_1^{1+q^2+q^3}\alpha_2^q\beta_1^{1+q+q^2}\beta_2^{q^3} + \alpha_1^{1+q^2+q^3}\alpha_2^q\beta_1^{q+q^2+q^3}\beta_2 \\ &+\alpha_1^{q+q^2+q^3}\alpha_2\beta_1^{1+q+q^2}\beta_2^{q^3} - \alpha_1^{q+q^2+q^3}\alpha_2\beta_1^{1+q+q^3}\beta_2^{q^2},\end{aligned}$$

v) the coefficient of c_1^4 is zero.

Therefore the number of non-$\mathbb{F}_q$-proportional solutions (c_1, c_2) with $c_1c_2 \neq 0$ is at most 2, if the polynomial is non-vanishing. Moreover, this polynomial vanishes if and only if

$$\begin{cases} YZ^q - YZ^{q^2} + Y^qZ^{q^2} - Y^qZ^{q^3} - Y^{q^2}Z + Y^{q^2}Z^{q^3} + Y^{q^3}Z - Y^{q^3}Z^q = 0 \\ \\ Y^{q+1}Z^{q^2+q} - Y^{q+1}Z^{q^3+q^2} - Y^{q^2+1}Z^{q^2+1} + Y^{q^2+1}Z^{q^3+q} \\ +Y^{q^3+1}Z^{q+1} - Y^{q^3+1}Z^{q^2+q} - Y^{q^2+q}Z^{q^3+1} + Y^{q^2+q}Z^{q^3+q^2} + Y^{q^3+q}Z^{q^2+1} \\ -Y^{q^3+q}Z^{q^3+q} - Y^{q^3+q^2}Z^{q+1} + Y^{q^3+q^2}Z^{q^3+1} = 0 \\ \\ Y^{q^2+q+1}Z^{q^3+q^2+1} - Y^{q^2+q+1}Z^{q^3+q^2+q} - Y^{q^3+q+1}Z^{q^2+q+1} + Y^{q^3+q+1}Z^{q^3+q^2+q} \\ +Y^{q^3+q^2+1}Z^{q^2+q+1} - Y^{q^3+q^2+1}Z^{q^3+q+1} + Y^{q^3+q^2+q}Z^{q^3+q+1} - Y^{q^3+q^2+q}Z^{q^3+q^2+1} = 0, \end{cases} \tag{5}$$

where $Y = \beta_1/\beta_2$ and $Z = \alpha_1/\alpha_2$. The solutions $(Y, Z) \in \mathbb{F}_{q^4}$ of System (5) are given in Theorem 6.1. From now on we will suppose that $Y = \beta_1/\beta_2$ and $Z = \alpha_1/\alpha_2$ are solutions of System (5). In this case, by Equation (3), the maximum number of non-$\mathbb{F}_q$-proportional possible values of $\beta_3 \in \mathbb{F}_{q^4}$ is $q-1$ when $\frac{c_1}{c_2}$ runs in $\mathbb{F}_q^*$. By System (2), to each such value of β_3 there corresponds at most one value of $\alpha_3 \in \mathbb{F}_{q^4}$.

Define $\lambda = c_1/c_2 \in \mathbb{F}_q^*$, so that $\beta_3 = \beta_3(\lambda)$ satisfies

$$\beta_3^{q-1}(\lambda) = \frac{\lambda\alpha_1^{q^2}\beta_1^q + \alpha_2^{q^2}\beta_2^q}{\lambda\alpha_1^{q^2}\beta_1 + \alpha_2^{q^2}\beta_2}. \tag{6}$$

Now, let $N(\lambda) = \lambda Z^{q^2}Y^q + 1$ and $D(\lambda) = \lambda Z^{q^2}Y + 1$, so that $\beta_3^{q-1}(\lambda) = \beta_2^{q-1}N(\lambda)/D(\lambda)$ and, by the third equation of System (2),

$$\alpha_3\beta_3 = c_2\alpha_2\beta_2^{q^2}D^{q^2}(\lambda)/\beta_3^{q^2-1} = c_2\alpha_2\beta_2D^{q^2+q+1}(\lambda)/N^{q+1}(\lambda), \tag{7}$$

and $\alpha_3\mathrm{Tr}(\beta_3x)$ reads

$$\begin{aligned} &\alpha_3\beta_3(x + \beta_3^{q-1}x^q + \beta_3^{q^2-1}x^{q^2} + \beta_3^{q^3-1}x^{q^3}) \\ &= \frac{c_2\alpha_2\beta_2D^{q^2+q+1}(\lambda)}{N^{q+1}(\lambda)}\left(x + \beta_2^{q-1}\frac{N(\lambda)}{D(\lambda)}x^q + \beta_2^{q^2-1}\frac{N^{q+1}(\lambda)}{D^{q+1}(\lambda)}x^{q^2} + \beta_2^{q^3-1}\frac{N^{q^2+q+1}(\lambda)}{D^{q^2+q+1}(\lambda)}x^{q^3}\right) \\ &= c_2\left(\alpha_2\beta_2\frac{D^{q^2+q+1}(\lambda)}{N^{q+1}(\lambda)}x + \alpha_2\beta_2^q\frac{D^{q^2+q}(\lambda)}{N^q(\lambda)}x^q + \alpha_2\beta_2^{q^2}D^{q^2}(\lambda)x^{q^2} + \alpha_2\beta_2^{q^3}N^{q^2}(\lambda)x^{q^3}\right). \end{aligned}$$

Step 2: We prove that there exist no eight distinct values $\lambda_1, \ldots, \lambda_8 \in \mathbb{F}_q^*$ such that the eight rank-one linear functions $F_i(x) = \alpha_2\beta_2\frac{D^{q^2+q+1}(\lambda_i)}{N^{q+1}(\lambda_i)}x + \alpha_2\beta_2^q\frac{D^{q^2+q}(\lambda_i)}{N^q(\lambda_i)}x^q + \alpha_2\beta_2^{q^2}D^{q^2}(\lambda_i)x^{q^2} + \alpha_2\beta_2^{q^3}N^{q^2}(\lambda_i)x^{q^3}$ and $F_9(x) := \alpha_1\mathrm{Tr}(\beta_1x)$, $F_{10}(x) := \alpha_2\mathrm{Tr}(\beta_2x)$ are $\mathbb{F}_q$-linearly independent. By Proposition 3.1, this will yield that $\mathrm{trk}(\mathcal{G}) \geq 11$.

Equivalently, we prove the existence of $\mu_1, \dots, \mu_{10} \in \mathbb{F}_q$ such that $\mu_1 F_1(x) + \cdots + \mu_{10} F_{10}(x) = 0$ and not all the μ_i's are zero, so that the ten traces $F_i(x)$, $i = 1, \dots, 10$, are $\mathbb{F}_q$-linearly dependent. Let $\mu_1, \dots, \mu_{10} \in \mathbb{F}_q$ be such that

$$\mu_1 F_1(x) + \cdots + \mu_{10} F_{10}(x) = 0. \tag{8}$$

In particular, Equation (8) can be seen as a polynomial identity; the coefficients of degree q^3 and q^2 yield to

$$\alpha_2 \beta_2^{q^3} \left(\sum_{i=1}^{8} \mu_i N^{q^2}(\lambda_i) + \mu_{10} \right) + \alpha_1 \beta_1^{q^3} \mu_9 = 0 = \alpha_2 \beta_2^{q^2} \left(\sum_{i=1}^{8} \mu_i D^{q^2}(\lambda_i) + \mu_{10} \right) + \alpha_1 \beta_1^{q^2} \mu_9.$$

Since $N(\lambda_i) = \lambda_i Z^{q^2} Y^q + 1$ and $D(\lambda_i) = \lambda_i Z^{q^2} Y + 1$,

$$\sum_{i=1}^{8} \mu_i + \mu_{10} = -\left(\sum_{i=1}^{8} \mu_i \lambda_i + \mu_9 \right) Y^{q^3} Z \text{ and } \sum_{i=1}^{8} \mu_i + \mu_{10} = -\left(\sum_{i=1}^{8} \mu_i \lambda_i + \mu_9 \right) Y^{q^2} Z.$$

Suppose that $Y^{q^3} Z = Y^{q^2} Z$, which is equivalent to $Y \in \mathbb{F}_q$. Then $N(\lambda) = D(\lambda)$ and $\beta_3(\lambda)^{q-1} = \beta_2^{q-1} = \beta_1^{q-1}$. By System (2), this implies $\alpha_3 \mathrm{Tr}(\beta_3 x) = c_1 \alpha_1 \mathrm{Tr}(\beta_1 x) + c_2 \alpha_2 \mathrm{Tr}(\beta_2 x) \in \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \alpha_2 \mathrm{Tr}(\beta_2 x) \rangle_{\mathbb{F}_q}$ and hence the F_i's, $i = 1, \dots, 10$, are linearly dependent.

We can then assume that $Y^{q^3} Z \neq Y^{q^2} Z$, so that

$$\mu_9 + \sum_{i=1}^{8} \mu_i \lambda_i = \sum_{i=1}^{8} \mu_i + \mu_{10} = 0. \tag{9}$$

Also, by looking at the the coefficients of degree 1 and q in Equation (8),

$$\alpha_2 \beta_2 \sum_{i=1}^{8} \mu_i \frac{D^{q^2+q+1}(\lambda)}{N^{q+1}(\lambda)} + \mu_9 \alpha_1 \beta_1 + \mu_{10} \alpha_2 \beta_2 = 0 = \alpha_2 \beta_2^q \sum_{i=1}^{8} \mu_i \frac{D^{q^2+q}(\lambda)}{N^q(\lambda)} + \mu_9 \alpha_1 \beta_1^q + \mu_{10} \alpha_2 \beta_2^q. \tag{10}$$

Equations (10) and their images under the q-Frobenius map, together with Equations

(9), form a homogeneous linear system of ten equations whose matrix is

$$M = \begin{pmatrix} 1 & 1 & \cdots & 0 & 1 \\ \lambda_1 & \lambda_2 & \cdots & 1 & 0 \\ \frac{D^{q^2+q+1}(\lambda_1)}{N^{q+1}(\lambda_1)} & \frac{D^{q^2+q+1}(\lambda_2)}{N^{q+1}(\lambda_2)} & \cdots & YZ & 1 \\ \frac{D^{q^3+q^2+q}(\lambda_1)}{N^{q^2+q}(\lambda_1)} & \frac{D^{q^3+q^2+q}(\lambda_2)}{N^{q^2+q}(\lambda_2)} & \cdots & Y^qZ^q & 1 \\ \frac{D^{q^3+q^2+1}(\lambda_1)}{N^{q^3+q^2}(\lambda_1)} & \frac{D^{q^3+q^2+1}(\lambda_2)}{N^{q^3+q^2}(\lambda_2)} & \cdots & Y^{q^2}Z^{q^2} & 1 \\ \frac{D^{q^3+q+1}(\lambda_1)}{N^{q^3+1}(\lambda_1)} & \frac{D^{q^3+q+1}(\lambda_2)}{N^{q^3+1}(\lambda_2)} & \cdots & Y^{q^3}Z^{q^3} & 1 \\ \frac{D^{q^2+q}(\lambda_1)}{N^{q}(\lambda_1)} & \frac{D^{q^2+q}(\lambda_2)}{N^{q}(\lambda_2)} & \cdots & Y^qZ & 1 \\ \frac{D^{q^3+q^2}(\lambda_1)}{N^{q^2}(\lambda_1)} & \frac{D^{q^3+q^2}(\lambda_2)}{N^{q^2}(\lambda_2)} & \cdots & Y^{q^2}Z^q & 1 \\ \frac{D^{q^3+1}(\lambda_1)}{N^{q^3}(\lambda_1)} & \frac{D^{q^3+1}(\lambda_2)}{N^{q^3}(\lambda_2)} & \cdots & Y^{q^3}Z^{q^2} & 1 \\ \frac{D^{q+1}(\lambda_1)}{N(\lambda_1)} & \frac{D^{q+1}(\lambda_2)}{N(\lambda_2)} & \cdots & YZ^{q^3} & 1 \end{pmatrix}. \tag{11}$$

Since the rows of M form orbits under the q-Frobenius map, the solutions of the associated system have entries in $\mathbb{F}_q$. By Theorem 6.2, the rank of M is smaller than 10. Therefore, there are non-trivial solutions $(\mu_1, \ldots, \mu_{10}) \in \mathbb{F}_q^{10}$ of $\mu_1 F_1(x) + \cdots + \mu_{10} F_{10}(x) = 0$. Then $\langle F_1(x), \ldots, F_{10}(x) \rangle_{\mathbb{F}_q}$ has dimension smaller than 10. This shows that $\mathrm{trk}(\mathcal{G}) \geq 11$. Thus, Theorem 4.1 is proved. □

4.2 The tensor rank of $\mathcal{G}$ is 11 for $q \geq 5$

In this section we use the notations of Section 4.1, and assume that $q \geq 5$. By Theorem 4.1, $\mathrm{trk}(\mathcal{G}) \geq 11$. We prove the following theorem.

Theorem 4.2. *For any prime power $q \geq 5$, we have* $\mathrm{trk}(\mathcal{G}) = 11$.

By Proposition 3.1, it is enough to show the existence of 11 $\mathbb{F}_q$-linearly independent trace functions whose $\mathbb{F}_q$-span contains $\mathcal{G}$. Our key tool is Step 1 in Section 4.1.

Proof. Let $\alpha_0, \beta_0 \in \mathbb{F}_{q^4}^*$ and $\lambda_1, \lambda_1', \ldots, \lambda_4, \lambda_4' \in \mathbb{F}_q^*$ with $\lambda_i \neq \lambda_j$ and $\lambda_i' \neq \lambda_j'$ for $i \neq j$. Let $\alpha, \beta, \alpha', \beta' \in \mathbb{F}_{q^4}^*$ be such that $Y := \beta/\beta_0$, $Z := \alpha/\alpha_0$, $Y' := \beta'/\beta_0$ and $Z' := \alpha'/\alpha_0$ satisfy $Z, Z' \notin \mathbb{F}_{q^2}$ and $Y = 1/Z^{q^2+q}$, $Y' = 1/(Z')^{q^2+q}$. By Theorem 6.1, (Y, Z) and (Y', Z') are solutions of System (5). As in the proof of Theorem 4.1, by (6) and (7) for any $i \in \{1, \ldots, 4\}$ there exist $\alpha_i, \beta_i, \alpha_i', \beta_i' \in \mathbb{F}_{q^4}^*$ such that

- $\beta_i^{q-1} = \beta_0^{q-1} N(\lambda_i)/D(\lambda_i)$;
- $(\beta_i')^{q-1} = \beta_0^{q-1} N'(\lambda_i')/D'(\lambda_i')$;
- $\alpha_i = c_i \alpha_0 \beta_0 D(\lambda_i)^{q^2+q+1}/N(\lambda_i)^{q+1}$;

- $\alpha'_i = c'_i \alpha_0 \beta_0 D'(\lambda'_i)^{q^2+q+1}/N'(\lambda'_i)^{q+1}$,

where $c_i, c'_i \in \mathbb{F}_q^*$, $N(\lambda_i) = \lambda_i Z^{q^2} Y^q + 1$, $N'(\lambda'_i) = \lambda'_i (Z')^{q^2} (Y')^q + 1$, $D(\lambda_i) = \lambda_i Z^{q^2} Y + 1$ and $D'(\lambda'_i) = \lambda'_i (Z')^{q^2} Y' + 1$.

Define the rank-one functions $F_0(x) = \alpha_0 \mathrm{Tr}(\beta_0 x)$, $F(x) = \alpha \mathrm{Tr}(\beta x)$, $F'(x) = \alpha' \mathrm{Tr}(\beta' x)$ and, for $i \in \{1, \dots, 4\}$, $F_i(x) := \frac{1}{c_i} \alpha_i \mathrm{Tr}(\beta_i x)$, $F'_i(x) := \frac{1}{c'_i} \alpha'_i \mathrm{Tr}(\beta'_i x)$. All such functions are elements of the linear $\mathbb{F}_{q^4}$-space $V = \mathcal{G} + \langle F(x), F'(x), F_0(x) \rangle_{\mathbb{F}_{q^4}}$ because of Step 1 in Section 4.1. We show that, for some suitable choice of the elements $\lambda_i, \lambda'_i, \alpha_0, \beta_0, \alpha, \beta, \alpha', \beta'$, the 11 elements $F(x)$, $F'(x)$, $F_0(x)$, $F_1(x), \dots, F_4(x)$, $F'_1(x), \dots, F'_4(x)$ are $\mathbb{F}_q$-linearly independent, which implies $\mathrm{trk}(\mathcal{G}) = 11$.

Let $\mu, \mu', \mu_0, \mu_1, \mu'_1, \dots, \mu_4, \mu'_4 \in \mathbb{F}_q$ be such that

$$\mu F(x) + \mu' F'(x) + \mu_0 F_0(x) + \mu_1 F_1(x) + \cdots \mu_4 F_4(x) + \mu'_1 F'_1(x) + \cdots \mu'_4 F'_4(x) = 0,$$

which can be seen a polynomial identity and hence implies

$$\begin{cases} \mu\alpha\beta + \mu'\alpha'\beta' + \mu_0\alpha_0\beta_0 + \alpha_0\beta_0 \sum_{i=1}^4 \left(\mu_i \frac{D^{q^2+q+1}(\lambda_i)}{N^{q+1}(\lambda_i)} + \mu'_i \frac{(D')^{q^2+q+1}(\lambda_i)}{(N')^{q+1}(\lambda_i)} \right) & = 0 \\ \mu\alpha\beta^q + \mu'\alpha'(\beta')^q + \mu_0\alpha_0\beta_0^q + \alpha_0\beta_0^q \sum_{i=1}^4 \left(\mu_i \frac{D^{q^2+q}(\lambda_i)}{N^q(\lambda_i)} + \mu'_i \frac{(D')^{q^2+q}(\lambda_i)}{(N')^q(\lambda_i)} \right) & = 0 \\ \mu\alpha\beta^{q^2} + \mu'\alpha'(\beta')^{q^2} + \mu_0\alpha_0\beta_0^{q^2} + \alpha_0\beta_0^{q^2} \sum_{i=1}^4 \left(\mu_i D^{q^2}(\lambda_i) + \mu'_i (D')^{q^2}(\lambda_i) \right) & = 0 \\ \mu\alpha\beta^{q^3} + \mu'\alpha'(\beta')^{q^3} + \mu_0\alpha_0\beta_0^{q^3} + \alpha_0\beta_0^{q^3} \sum_{i=1}^4 \left(\mu_i N^{q^2}(\lambda_i) + \mu'_i (N')^{q^2}(\lambda_i) \right) & = 0. \end{cases} \tag{12}$$

The four equations in (12), together with their images under the q-Frobenius map, provide a homogeneous linear system of twelve equations with solutions in $\mathbb{F}_q^{11}$, of which

$(\mu, \mu', \mu_0, \mu_1, \mu_1', \ldots, \mu_4, \mu_4')$ is a solution. The matrix M of such a system is

$$\begin{pmatrix}
YZ & Y'Z' & 1 & \frac{D^{q^2+q+1}(\lambda_1)}{N^{q+1}(\lambda_1)} & \frac{(D')^{q^2+q+1}(\lambda_1')}{(N')^{q+1}(\lambda_1')} & \cdots & \frac{D^{q^2+q+1}(\lambda_4)}{N^{q+1}(\lambda_4)} & \frac{(D')^{q^2+q+1}(\lambda_4')}{(N')^{q+1}(\lambda_4')} \\
Y^qZ^q & (Y')^q(Z')^q & 1 & \frac{D^{q^3+q^2+q}(\lambda_1)}{N^{q^2+q}(\lambda_1)} & \frac{(D')^{q^3+q^2+q}(\lambda_1')}{(N')^{q^2+q}(\lambda_1')} & \cdots & \frac{D^{q^3+q^2+q}(\lambda_4)}{N^{q^2+q}(\lambda_4)} & \frac{(D')^{q^3+q^2+q}(\lambda_4')}{(N')^{q^2+q}(\lambda_4')} \\
Y^{q^2}Z^{q^2} & (Y')^{q^2}(Z')^{q^2} & 1 & \frac{D^{1+q^3+q^2}(\lambda_1)}{N^{q^3+q^2}(\lambda_1)} & \frac{(D')^{1+q^3+q^2}(\lambda_1')}{(N')^{q^3+q^2}(\lambda_1')} & \cdots & \frac{D^{1+q^3+q^2}(\lambda_4)}{N^{q^3+q^2}(\lambda_4)} & \frac{(D')^{1+q^3+q^2}(\lambda_4')}{(N')^{q^3+q^2}(\lambda_4')} \\
Y^{q^3}Z^{q^3} & (Y')^{q^3}(Z')^{q^3} & 1 & \frac{D^{q+1+q^3}(\lambda_1)}{N^{1+q^3}(\lambda_1)} & \frac{(D')^{q+1+q^3}(\lambda_1')}{(N')^{1+q^3}(\lambda_1')} & \cdots & \frac{D^{q+1+q^3}(\lambda_4)}{N^{1+q^3}(\lambda_4)} & \frac{(D')^{q+1+q^3}(\lambda_4')}{(N')^{1+q^3}(\lambda_4')} \\
Y^qZ & (Y')^qZ' & 1 & \frac{D^{q^2+q}(\lambda_1)}{N^q(\lambda_1)} & \frac{(D')^{q^2+q}(\lambda_1')}{(N')^q(\lambda_1')} & \cdots & \frac{D^{q^2+q}(\lambda_4)}{N^q(\lambda_4)} & \frac{(D')^{q^2+q}(\lambda_4')}{(N')^q(\lambda_4')} \\
Y^{q^2}Z^q & (Y')^{q^2}(Z')^q & 1 & \frac{D^{q^3+q^2}(\lambda_1)}{N^{q^2}(\lambda_1)} & \frac{(D')^{q^3+q^2}(\lambda_1')}{(N')^{q^2}(\lambda_1')} & \cdots & \frac{D^{q^3+q^2}(\lambda_4)}{N^{q^2}(\lambda_4)} & \frac{(D')^{q^3+q^2}(\lambda_4')}{(N')^{q^2}(\lambda_4')} \\
Y^{q^3}Z^{q^2} & (Y')^{q^3}(Z')^{q^2} & 1 & \frac{D^{1+q^3}(\lambda_1)}{N^{q^3}(\lambda_1)} & \frac{(D')^{1+q^3}(\lambda_1')}{(N')^{q^3}(\lambda_1')} & \cdots & \frac{D^{1+q^3}(\lambda_4)}{N^{q^3}(\lambda_4)} & \frac{(D')^{1+q^3}(\lambda_4')}{(N')^{q^3}(\lambda_4')} \\
YZ^{q^3} & Y'(Z')^{q^3} & 1 & \frac{D^{q+1}(\lambda_1)}{N(\lambda_1)} & \frac{(D')^{q+1}(\lambda_1')}{N'(\lambda_1')} & \cdots & \frac{D^{q+1}(\lambda_4)}{N(\lambda_4)} & \frac{(D')^{q+1}(\lambda_4')}{N'(\lambda_4')} \\
Y^{q^2}Z & (Y')^{q^2}Z' & 1 & D^{q^2}(\lambda_1) & (D')^{q^2}(\lambda_1') & \cdots & D^{q^2}(\lambda_4) & (D')^{q^2}(\lambda_4') \\
Y^{q^3}Z^q & (Y')^{q^3}(Z')^q & 1 & D^{q^3}(\lambda_1) & (D')^{q^3}(\lambda_1') & \cdots & D^{q^3}(\lambda_4) & (D')^{q^3}(\lambda_4') \\
YZ^{q^2} & Y'(Z')^{q^2} & 1 & D(\lambda_1) & D'(\lambda_1') & \cdots & D(\lambda_4) & D'(\lambda_4') \\
Y^qZ^{q^3} & (Y')^q(Z')^{q^3} & 1 & D^q(\lambda_1) & (D')^q(\lambda_1') & \cdots & D^q(\lambda_4) & (D')^q(\lambda_4') \\
Y^{q^3}Z & (Y')^{q^3}Z' & 1 & N^{q^2}(\lambda_1) & (N')^{q^2}(\lambda_1') & \cdots & N^{q^2}(\lambda_4) & (N')^{q^2}(\lambda_4') \\
YZ^q & Y'(Z')^q & 1 & N^{q^3}(\lambda_1) & (N')^{q^3}(\lambda_1') & \cdots & N^{q^3}(\lambda_4) & (N')^{q^3}(\lambda_4') \\
Y^qZ^{q^2} & (Y')^q(Z')^{q^2} & 1 & N(\lambda_1) & N'(\lambda_1') & \cdots & N(\lambda_4) & N'(\lambda_4') \\
Y^{q^2}Z^{q^3} & (Y')^{q^2}(Z')^{q^3} & 1 & N^q(\lambda_1) & (N')^q(\lambda_1') & \cdots & N^q(\lambda_4) & (N')^q(\lambda_4')
\end{pmatrix}.$$

Since $|\mathbb{F}_q^*| \geq 4$, we can choose $\lambda_1 \neq 0$, $\lambda_1^2 \neq 1$ and $\lambda_1^3 \neq 1$ and then

- $\lambda_2 = \lambda_1^2$, $\lambda_3 = \lambda_1^3$ and $\lambda_4 = \lambda_1^4$;
- $\lambda_i = \lambda_{i-4}$ for any $i \in \{5, 6, 7, 8\}$.

We also choose $\alpha_0, \beta_0, \alpha, \beta, \alpha', \beta'$ such that $Z^{q^2+1} = 1$ and $Z' = Z^q$. By direct computation with MAGMA,

$$\begin{aligned}
\det(M) \;=\; & \lambda_1^{40}(\lambda_1 - 1)^{12}(\lambda_1 + 1)^4(\lambda_1^2 + \lambda_1 + 1)^2(Z^2 - 1)^{6q+6}(Z^q - Z)^4(Z^{q+1} - 1)^4 \\
& \cdot(Z^{3q+2} - Z^{2q+1} - 2Z^{q+2} + Z^q + Z^3)(Z^{3q+1} - Z^{2q+2} + Z^{q+3} - 2Z^{q+1} + 1) \\
& \cdot(Z^{3q} + Z^{2q+3} - 2Z^{2q+1} - Z^{q+2} + Z)(Z^{3q+3} - 2Z^{2q+2} + Z^{2q} - Z^{q+1} + Z^2)^2.
\end{aligned}$$

For some $Z \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ satisfying $Z^{q^2+1} = 1$, we have $\det(M) \neq 0$; for $q \geq 16$ this follows because $q^2 + 1$ is greater than the sum of the degrees of the polynomials in parentheses, while for $q < 16$ this follows by direct checking. Therefore, for a suitable choice of $\lambda_i, \lambda_i', \alpha_0, \beta_0, \alpha, \beta, \alpha', \beta'$, the matrix M has full rank 11 and hence

$$(\mu, \mu', \mu_0, \mu_1, \mu_1', \ldots, \mu_4, \mu_4') = (0, \ldots, 0).$$

Thus, $F(x)$, $F'(x)$, $F_0(x)$, $F_1(x)$, $F_1'(x)$, …, $F_4(x)$, $F_4'(x)$ are $\mathbb{F}_q$-linearly independent and $\mathcal{G}$ has tensor rank 11. $\square$

5 Tensor rank of $n \times n$ generalized Gabidulin codes for $n \leq 4$

We compute the tensor rank of some generalized Gabidulin code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ of dimension k over $\mathbb{F}_{q^n}$ for $n \leq 4$. Notice that, up to equivalence, $\mathcal{C} = \mathcal{G}_{k,1}$.

By Section 4.2 and [4, Table 1], the open cases are exactly for n, k, q as in the table below. Since the lower bound on the tensor rank of $\mathcal{G}_{k,1}$ is $nk + n - k$, we start with the exhaustive search for $t := n - k$ rank-one functions $\alpha_i \mathrm{Tr}(\beta_i x) \in \mathbb{F}_{q^n}[x]$ such that the rank-one functions in $\mathcal{C} + \langle \alpha_1 \mathrm{Tr}(\beta_1 x), \ldots, \alpha_t \mathrm{Tr}(\beta_t x) \rangle_{\mathbb{F}_q}$ generate an $\mathbb{F}_q$-space U of dimension $nk + t$. If this succeeds, then we compute explicitly a perfect basis of U (i.e. a basis of pure tensors). Otherwise, we increase t by 1 and perform the same search again. In this way we obtain the tensor rank and a perfect basis $B = \{\eta^i \mathrm{Tr}(\eta^j x) \colon (i,j) \in I\}$ for $\mathcal{G}_{k,1}$, where η is a primitive element of $\mathbb{F}_{q^n}$ and $I \subseteq \{0, \ldots, q^n - 2\}^2$. The precise value of the tensor rank is obtained for all but two cases, namely $n = 4$, $k = 1$ and $q \in \{4, 5\}$; in these cases, an upper bound is provided by means of a random search.

Table 1: Tensor rank of some generalized Gabidulin codes $\mathcal{G}_{k,1} \subseteq \mathcal{L}_{n,q}$

n	k	q	$\mathrm{TR}(\mathcal{G}_{k,1})$	MTR	$\mathrm{MinPol}(\xi)$	I
3	2	2	7	yes	$x^3 + x + 1$	(2,0),(3,5),(1,2),(0,4),(6,6),(5,1),(4,3)
4	1	4	$\in \{7, 8\}$	?	$x^8 + x^4 + x^3 + x^2 + 1$	(73,168),(22,202),(0,180),(69,249),(80,90),(1,96),(33,213),(67,162)
4	1	5	$\in \{7, 8\}$	?	$x^4 + 4x^2 + 4x + 2$	(16,432),(135,81),(21,405),(10,132),(56,593),(24,556),(74,569),(54,268)
4	2	2	12	no	$x^4 + x + 1$	(14,12),(9,14),(4,0),(7,5),(1,13),(5,10),(6,3),(2,1),(12,7),(3,2),(0,4),(13,6)
4	2	3	11	no	$x^4 - x^3 - 1$	(23,8),(0,13),(28,14),(32,46),(2,1),(19,26),(1,18),(6,37),(7,12),(36,28),(21,59)
4	2	4	11	no	$x^8 + x^4 + x^3 + x^2 + 1$	(13,133),(56,175),(20,71),(30,31),(81,124),(0,51),(3,88),(76,34),(70,215),(29,132),(9,24)
4	3	2	13	yes	$x^4 + x + 1$	(12,13),(8,6),(4,4),(9,4),(1,5),(3,1),(14,9),(11,0),(10,2),(0,7),(6,10),(7,8),(5,12)
4	3	3	13	yes	$x^4 - x^3 - 1$	(31,3),(29,49),(0,56),(25,61),(7,75),(26,18),(22,30),(20,36),(39,19),(18,2),(13,57),(32,40),(3,47)

Remark 5.1. *The fourth, fifth, and sixth rows of the table completes the proof of Theorem 1.1.*

Remark 5.2. *Notice that, although only one perfect basis is showed in the table, the computations provide a much larger number of perfect bases in each case. Therefore, no generator tensor of such codes is identifiable.*

6 Appendix

Theorem 6.1. *Let $Y, Z \in \mathbb{F}_{q^4}$. Then (Y, Z) is a solution of System (5) if and only if one of the following pairwise mutually exclusive conditions holds:*

(C1) $Y \in \mathbb{F}_q$ or $Z \in \mathbb{F}_q$;

(C2) $Y \notin \mathbb{F}_{q^2}$ and $Z = \rho Y^{q+1}$ for some $\rho \in \mathbb{F}_q^*$;

(C3) $Z \notin \mathbb{F}_{q^2}$ and $Y = \rho / Z^{q^2+q}$ for some $\rho \in \mathbb{F}_q^*$.

Proof. For any $i = 0, 1, 2, 3$, write $y_i = Y^{q^i}$ and $z_i = Z^{q^i}$. Then System (5) reads

$$\begin{cases} f_1(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) = 0 \\ f_2(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) = 0 \\ f_3(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) = 0, \end{cases} \tag{13}$$

where

$$\begin{aligned} f_1(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) &= y_0z_1 - y_0z_2 + y_1z_2 - y_1z_3 - y_2z_0 + y_2z_3 + y_3z_0 - y_3z_1, \\ f_2(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) &= y_0y_1z_1z_2 - y_0y_1z_2z_3 - y_0y_2z_0z_2 + y_0y_2z_1z_3 + y_0y_3z_0z_1 \\ &\quad -y_0y_3z_1z_2 - y_1y_2z_0z_3 + y_1y_2z_2z_3 + y_1y_3z_0z_2 - y_1y_3z_1z_3 \\ &\quad -y_2y_3z_0z_1 + y_2y_3z_0z_3, \\ f_3(y_0, y_1, y_2, y_3, z_0, z_1, z_2, z_3) &= y_0y_1y_2z_0z_2z_3 - y_0y_1y_2z_1z_2z_3 - y_0y_1y_3z_0z_1z_2 + y_0y_1y_3z_1z_2z_3 \\ &\quad +y_0y_2y_3z_0z_1z_2 - y_0y_2y_3z_0z_1z_3 + y_1y_2y_3z_0z_1z_3 - y_1y_2y_3z_0z_2z_3. \end{aligned}$$

We denote by $\mathrm{Res}_x(g_1, g_2)$ the resultant of two (multivariate) polynomials g_1 and g_2 with respect to the indeterminate x. We have

$$\begin{aligned} \mathrm{Res}_{z_1}\left(\mathrm{Res}_{z_0}(f_3, f_1), \mathrm{Res}_{z_0}(f_2, f_1)\right) &= -(z_2 - z_3)^2 y_3 (y_2 - y_3)(y_2z_3 - y_3z_2) \cdot \\ &\quad (y_1 - y_2)^2 (y_0 - y_3)(y_0 - y_1)^2 (y_0z_2 - y_3z_3) \cdot \\ &\quad (y_0z_2 - y_2z_3)^2 (y_0y_2 - y_1y_3)(y_1 - y_3). \end{aligned}$$

Thus, every solution $(Y, Z) \in \mathbb{F}_{q^4}^2$ of System (5) with $YZ \neq 0$ satisfies one of the following conditions.

1. $y_3 = 0$, that is $Y^{q^3} = 0$, a contradiction.
2. $z_2 - z_3 = 0$, that is $Z \in \mathbb{F}_q$. Indeed (Y, Z) is a solution of System (5) whenever $Z \in \mathbb{F}_q$. In the following cases we can then assume $Z \notin \mathbb{F}_q$.
3. $y_2 - y_3 = 0$, or $y_1 - y_2 = 0$, or $y_0 - y_3 = 0$, or $y_0 - y_1 = 0$. This is equivalent to $Y \in \mathbb{F}_q$, and indeed (Y, Z) is a solution of System (5) whenever $Y \in \mathbb{F}_q$. In the following cases we can then assume $Y \notin \mathbb{F}_q$.

4. $y_1 - y_3 = 0$, that is $Y \in \mathbb{F}_{q^2}$. Then System (5) reads

$$\begin{cases} Z^{q^2+q+1} - Z^{q^3+q+1} + Z^{q^3+q^2+1} - Z^{q^3+q^2+q} = 0 \\ Z - Z^q + Z^{q^2} - Z^{q^3} = 0 \\ (Y^q + Y)(Z^{q^2+1} - Z^{q^3+q}) = 0. \end{cases}$$

The first equation yields $Z^{q^3+q^2+1} + Z^{q^2+q+1} \in \mathbb{F}_q$, that is $Z^{q^2+1}(Z^{q^2}+Z)^q \in \mathbb{F}_q$, while the second equation yields $Z^{q^2} + Z \in \mathbb{F}_q$. Therefore $Z^{q^2+1} \in \mathbb{F}_q$, and hence the third equation is also satisfied. Now, the two conditions $Z^{q^2} + Z \in \mathbb{F}_q$ and $Z^{q^2+1} \in \mathbb{F}_q$ yield $Z^{q^3} = Z^{q^2} - Z^q + Z$ and $Z^{q^3} = Z^{q^2-q+1}$. This implies $Z(Z^{q-1} - 1)^{q+1} = 0$, whence $Z \in \mathbb{F}_q$. In the following cases we can then assume $Y \notin \mathbb{F}_{q^2}$.

5. $y_2 z_3 - y_3 z_2 = 0$, that is $Y^{q-1} = Z^{q-1}$, and hence $Y = \rho Z$ for some $\rho \in \mathbb{F}_q^*$. Then $y_i = \rho z_i$ for any $i = 1, \ldots, 3$, and System (13) reads

$$\begin{cases} g_1 := z_0 z_1 - 2z_0 z_2 + z_0 z_3 + z_1 z_2 - 2z_1 z_3 + z_2 z_3 = 0 \\ g_2 := z_0^2 z_1 z_3 - z_0^2 z_2^2 + z_0 z_1^2 z_2 - 2z_0 z_1 z_2 z_3 + z_0 z_2 z_3^2 - z_1^2 z_3^2 + z_1 z_2^2 z_3 = 0. \end{cases}$$

From $\mathrm{Res}_{z_1}(g_1, g_2) = 0$ it follows that $(z_2 - z_3)^2 (z_3 - z_0)^2 (z_2 - z_0)^2 = 0$, which is equivalent to $Z \in \mathbb{F}_{q^2}$. Then $Y = \rho Z \in \mathbb{F}_{q^2}$.

6. $y_0 z_2 - y_3 z_3 = 0$, that is $Y^{q-1} = 1/Z^{(q^2+q+1)(q-1)}$, and hence $Y = \rho / Z^{q^2+q+1}$ for some $\rho \in \mathbb{F}_q^*$. Then $y_i = \rho/(z_i z_{i+1} z_{i+2})$ for any $i = 0, \ldots, 3$ (where the indices are modulo 4) and System (13) reads

$$\begin{cases} h_1 := z_0 z_1 - 2z_0 z_2 + z_0 z_3 + z_1 z_2 - 2z_1 z_3 + z_2 z_3 = 0 \\ h_2 := z_0^2 z_1 z_3 - z_0^2 z_2^2 + z_0 z_1^2 z_2 - 2z_0 z_1 z_2 z_3 + z_0 z_2 z_3^2 - z_1^2 z_3^2 + z_1 z_2^2 z_3 = 0. \end{cases}$$

From $\mathrm{Res}_{z_3}(h_1, h_2) = 0$ it follows that $z_2 = z_0$. Then $Z \in \mathbb{F}_{q^2}$ and hence $Y = \rho/(Z^2 Z^q)$. By System (5), this implies $Z \in \mathbb{F}_q$.

7. $y_0 z_2 - y_2 z_3 = 0$, that is $YZ^{q^2} - Y^{q^2} Z^{q^3} = 0$. This is equivalent to $Z^{q-1} = Y^{q^2-1}$, and hence to $Z = \rho Y^{q+1}$ for some $\rho \in \mathbb{F}_q^*$. By direct checking, this is indeed a solution of System (5) for any $Y \in \mathbb{F}_{q^4}$. If we require $Y \notin \mathbb{F}_{q^2}$, this also implies $Z \notin \mathbb{F}_q$.

8. $y_0 y_2 - y_1 y_3 = 0$, that is $y_3 = y_0 y_2 / y_1$, or equivalently $Y^{q^3} = Y^{1+q^2}/Y^q$. Then System (13) reads

$$\begin{cases} p_1 := y_0 y_1 z_1 - y_0 y_1 z_2 + y_0 y_2 z_0 - y_0 y_2 z_1 + y_1^2 z_2 - y_1^2 z_3 - y_1 y_2 z_0 + y_1 y_2 z_3 = 0 \\ p_2 := y_0 y_1 z_0 z_1 z_2 - y_0 y_1 z_1 z_2 z_3 - y_0 y_2 z_0 z_1 z_2 + y_0 y_2 z_0 z_1 z_3 - y_1^2 z_0 z_2 z_3 \\ \qquad + y_1^2 z_1 z_2 z_3 - y_1 y_2 z_0 z_1 z_3 + y_1 y_2 z_0 z_2 z_3 = 0 \\ p_3 := y_0^2 y_2 z_0 z_1 - y_0^2 y_2 z_1 z_2 + y_0 y_1^2 z_1 z_2 - y_0 y_1^2 z_2 z_3 - y_0 y_2^2 z_0 z_1 \\ \qquad + y_0 y_2^2 z_0 z_3 - y_1^2 y_2 z_0 z_3 + y_1^2 y_2 z_2 z_3 = 0. \end{cases}$$

From $\mathrm{Res}_{y_2}(p_1, p_2) = 0$ it follows that $(z_0 - z_2)(z_0 z_2 - z_1 z_3)(y_0 z_1 - y_1 z_3) = 0$.

8.1 Suppose $z_0 - z_2 = 0$, i.e. $Z \in \mathbb{F}_{q^2}$, whence also $z_3 = z_1$. Then, by System (13), either $Y \in \mathbb{F}_q$ or $Z \in \mathbb{F}_q$.

8.2 Suppose $z_0 z_2 - z_1 z_3 = 0$, so that $z_3 = z_0 z_2 / z_1$. By System (13),

$$\begin{cases} \ell_1 := y_0^2 y_2 z_0 z_1 - y_0^2 y_2 z_1 z_2 + y_0 y_1^2 z_1 z_2 - y_0 y_1^2 z_2^2 - y_0 y_2^2 z_0 z_1 \\ \qquad + y_0 y_2^2 z_0 z_2 - y_1^2 y_2 z_0 z_2 + y_1^2 y_2 z_2^2 = 0 \\ \ell_2 := y_0 z_0 z_1 - y_0 z_1 z_2 - y_1 z_0 z_2 + y_1 z_1 z_2 - y_2 z_0 z_1 + y_2 z_0 z_2 = 0 \\ \ell_3 := y_0 y_1 z_1 - y_0 y_1 z_2 + y_0 y_2 z_0 - y_0 y_2 z_1 - y_1 y_2 z_0 + y_1 y_2 z_2 = 0. \end{cases}$$

From $\mathrm{Res}_{y_2}(\ell_1, \ell_3) = 0$ it follows $y_0 z_1 - y_1 z_2 = 0$, so that $Y^{q-1} = (1/Z^q)^{q-1}$. This implies $Y = \rho / Z^q$ for some $\rho \in \mathbb{F}_q^*$, whence $y_i = \rho / z_{i+1}$ for any $i = 0, \ldots, 3$ (indices modulo 4). Then, by System (13),

$$\begin{cases} m_1 := z_0^2 z_1 - z_0 z_1 z_2 - 2 z_0 z_1 z_3 + z_0 z_2 z_3 + z_1^2 z_3 = 0 \\ m_2 := z_0^2 z_2 + z_0 z_1^2 - 2 z_0 z_1 z_2 - z_0 z_1 z_3 + z_1 z_2 z_3 = 0 \\ m_3 := z_0^2 z_1 + z_0^2 z_2 + z_0 z_1^2 - 3 z_0 z_1 z_2 - 3 z_0 z_1 z_3 + z_0 z_2 z_3 + z_1^2 z_3 + z_1 z_2 z_3 = 0. \end{cases}$$

From $\mathrm{Res}_{z_3}(m_1, m_2) = 0$ it follows that $Z \in \mathbb{F}_q$.

8.3 Suppose $y_0 z_1 - y_1 z_3 = 0$. This implies $Y^{q-1} = (1/Z^{q^2+q})^{q-1}$, whence $Y = \rho / Z^{q^2+q}$ for some $\rho \in \mathbb{F}_q^*$. Then $y_i = \rho / (z_{i+2} z_{i+1})$ for any $i = 0, \ldots, 3$ (indices modulo 4), which is indeed a solution of System (13) and provide a solution (Y, Z) of System (5). Notice that the condition $Y = \rho / Z^{q^2+q}$ with $Z \in \mathbb{F}_{q^4}$ implies $Y^{q^3} = Y^{1+q^2} / Y^q$. For such a solution, the require $Z \notin \mathbb{F}_{q^2}$ is equivalent to $Y \notin \mathbb{F}_q$. Also, if $Y, Z \in \mathbb{F}_{q^4}^*$ are such that $Y = \rho / Z^{q^2+q}$ and $Z = \rho' Y^{q+1}$ with $\rho, \rho' \in \mathbb{F}_q$, then $Y^{q^3+q^2+q+1+q^2} = \rho / \rho' \in \mathbb{F}_q^*$, whence $Y \in \mathbb{F}_q$.

□

Theorem 6.2. *Let $(Y, Z) \in \mathbb{F}_{q^4}^2$ be a solution of System* (5)*, and M be the matrix in* (11)*.*

(R1) If $Y \in \mathbb{F}_q$ or $Z \in \mathbb{F}_q$, then $\mathrm{rank}(M) = 2$.

(R2) If $Y \notin \mathbb{F}_{q^2}$ and $Z = \rho Y^{q+1}$ for some $\rho \in \mathbb{F}_q^*$, then $\mathrm{rank}(M) = 6$.

(R3) If $Z \notin \mathbb{F}_{q^2}$ and $Y = \rho / Z^{q^2+q}$ for some $\rho \in \mathbb{F}_q^*$, then $\mathrm{rank}(M) = 6$.

Proof. For any $i = 1, \ldots, 10$, denote respectively by $M^{(i)}$ and $M_{(i)}$ the i-th row and the i-th column of M. Note that $M_{(9)}$ and $M_{(10)}$ are linearly independent. Note also that, by construction of M, any possible $\mathbb{F}_q$-linear combination of the columns of M needs to be checked only on the first, second, third, and seventh rows of M.

(R1) Suppose $Y \in \mathbb{F}_q$. Then $N(\lambda) = D(\lambda)$, whence $\frac{D^{q^2+q+1}(\lambda)}{N^{q+1}(\lambda)} = \frac{D^{q^2+q}(\lambda)}{N^q(\lambda)} = \lambda ZY + 1$. Therefore $M_{(j)} = \lambda_j M_{(9)} + M_{(10)}$ for any $j = 1, \dots, 8$, and $\mathrm{rank}(M) = 2$.

Suppose $Z \in \mathbb{F}_q$. Similarly, one has $N(\lambda) = D^q(\lambda)$ and $M_{(j)} = \lambda_j M_{(9)} + M_{(10)}$ for any $j = 1, \dots, 8$, so that $\mathrm{rank}(M) = 2$.

For $i = 6, 7$, denote by S_i the $i \times i$ submatrix of M given by the first i rows and the last i columns of M. If for any distinct $\lambda_4, \dots, \lambda_8 \in \mathbb{F}_q^*$ one has $\det(S_6) \neq 0$ and $\det(S_7) = 0$, then this is enough to conclude that $\mathrm{rank}(M) = 6$ for any distinct $\lambda_1, \dots, \lambda_8 \in \mathbb{F}_q^*$. In fact, the use of the column $M_{(j)}$, $j \in \{1, 2, 3\}$, instead of $M_{(4)}$, implies the replacement of λ_4 with λ_j in $\det(S_7)$, and in this way the fourth column becomes any of the remaining columns. If S_7' is obtained from S_7 by replacing $M^{(7)}$ with $M^{(i)}$, $i \in \{8, 9, 10\}$, then the elementwise q^{i-7}-power Φ maps $M^{(7)}$ to $M^{(i)}$, while $M^{(1)}$ and $M^{(2)}$ are fixed by Φ, and $M^{(3)}, M^{(4)}, M^{(5)}, M^{(6)}$ are cyclically permuted by Φ. Therefore Φ maps the rows of S_7 to the rows of S_7', so that $\det(S_7) = 0$ if and only if $\det(S_7') = 0$.

(R2) Suppose $Y \notin \mathbb{F}_{q^2}$ and $Z = \rho Y^{q+1}$ for some $\rho \in \mathbb{F}_q^*$. Then $\det(S_6)$ equals

$$\rho^{10} Y^{4(q^3+q^2+q+1)} \left(\prod_{i=5}^{8} \lambda_i \right) \left(\prod_{5 \le i < j \le 8} (\lambda_i - \lambda_j) \right) \cdot \left(\prod_{i=0}^{3} (Y^{q^i} - Y^{q^{i+1}})^2 \right) \left(\prod_{i=0}^{1} (Y^{q^i} - Y^{q^{i+2}})^3 \right),$$

and hence $\det(S_6) \neq 0$ because $Y \notin \mathbb{F}_{q^2}$ and the λ_i's are nonzero and distinct. Also, $\det(S_7) = 0$. Therefore, $\mathrm{rank}(M) = 6$.

(R3) Suppose $Z \notin \mathbb{F}_{q^2}$ and $Y = \rho / Z^{q^2+q}$ for some $\rho \in \mathbb{F}_q^*$. Then

$$\det(S_6) = \rho^{10} \left(\prod_{i=5}^{8} \lambda_i \right) \left(\prod_{5 \le i < j \le 8} (\lambda_i - \lambda_j) \right) \cdot \left(\prod_{i=0}^{3} (Z^{q^i} - Z^{q^{i+1}})^2 \right) \left(\prod_{i=0}^{1} (Z^{q^i} - Z^{q^{i+2}})^3 \right)$$

is nonzero. Also, $\det(S_7) = 0$. Therefore, $\mathrm{rank}(M) = 6$.

□

Acknowledgments

The authors of this paper would like to thank Alessandro Neri for fruitful discussions. This research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The last two authors were supported by the project "VALERE: VAnviteLli pEr la RicErca" of the University of Campania "Luigi Vanvitelli".

References

[1] E. Allman, C. Matias and J. Rhodes: Identifiability of parameters in latent structure models with many observed variables, *Ann. Statist.* **37** (2009), 3099–3132.

[2] S. Ballet, J. Pieltant, M. Rambaud, H. Randriambololona, R. Rolland, and J. Chaumine: On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry, *Russian Math. Surveys* **76** (1) (2021), 1–29.

[3] P. Bürgisser, M. Clausen, M.A. Shokrollahi: Algebraic Complexity Theory, *Grundlehren Math. Wiss.* 315, Springer, 1997.

[4] E. Byrne and G. Cotardo: Bilinear complexity of 3-tensors linked to coding theory, arXiv:2103.08544.

[5] E. Byrne and G. Cotardo: Tensor Codes and their Invariants, arXiv:2112.08100.

[6] E. Byrne, A. Neri, A. Ravagnani and J. Sheekey: Tensor representation of rank-metric codes, *SIAM J. Appl. Algebra Geom.* **3** (4) (2019), 614–643.

[7] L. Chiantini and G. Ottaviani: On generic identifiability of 3-tensors of small rank, *SIAM J. Matrix Anal. Appl.* **33** (3) (2012), 1018–1037.

[8] J. de la Cruz, M Kiermaier, A Wassermann and W. Willems: Algebraic structures of MRD codes, *Adv. Math. Commun.* **10**(3) (2016), 499.

[9] P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.

[10] D. E. Knuth: Finite semifields and projective planes, *J. Algebra* **2** (1965), 182–217.

[11] J.B. Kruskal: Three-way arrays: rank and uniqueness of trilinear decompositions, with application to arithmetic complexity and statistics, *Linear Algebra Appl.* **18** (1977), 95–138.

[12] A. Kshevetskiy and E. Gabidulin: The new construction of rank codes, *International Symposium on Information Theory* (2005), 2105–2108.

[13] E. Gabidulin: Theory of codes with maximum rank distance, *Probl. Inf. Transm.*, **21** (3) (1985), 3–16.

[14] E. Gabidulin, A.V. Paramonovand O.V. Tretjakov: Ideals over a non-commutative ring and their application in cryptology, In *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg (1991), 482–489.

[15] E. Gorla and A. Ravagnani: Codes endowed with the rank metric, *Network Coding and Subspace Designs*, Springer, Cham (2018), 3–23.

[16] J. Hastad: Tensor rank is NP-complete, *J. Algorithms* **11** (4) (1990), 644–654.

[17] M. Lavrauw: Finite semifields and nonsingular tensors, *Des. Codes Cryptogr.* **68** (2013), 205–227.

[18] M. Lavrauw, A. Pavan and C. Zanella: On the rank of $3 \times 3 \times 3$-tensors, *Linear Multilinear Algebra* **61** (2013) 648–652.

[19] M. Lavrauw and J. Sheekey: The tensor rank of semifields of order 16 and 81, arXiv:2102.01997.

[20] R. Liebler: On nonsingular tensors and related projective planes, *Geom. Dedicata* **11** (1981), 455–464.

[21] R. Liedl and H. Niederreiter: Finite Fields, Second Edition. Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, Cambridge (1997).

[22] O. Polverino and F. Zullo: Connections between scattered linear sets and MRD-codes, *Bull. Inst. Combin. Appl.* **89** (2020), 46-74.

[23] R. Roth: Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory* **37** (2) (1991), 328–336.

[24] J. Sheekey: MRD codes: constructions and connections, *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*, Radon Series on Computational and Applied Mathematics **23**, K.-U. Schmidt and A. Winterhof (eds.), De Gruyter (2019).

[25] D. Silva F.R. Kschischang and R. Koetter: A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory* **54** (9) (2008), 3951–3967.

[26] B. Wu and Z. Liu: Linearized polynomials over finite fields revisited, *Finite Fields Appl.* **22** (2013), 79–100.