Journal of Algebraic Combinatorics (2019) 49:507–534
https://doi.org/10.1007/s10801-018-0833-3

Puncturing maximum rank distance codes

Bence Csajbók[1] · **Alessandro Siciliano**[2]

Received: 1 May 2017 / Accepted: 17 July 2018 / Published online: 14 August 2018

Abstract
We investigate punctured maximum rank distance codes in cyclic models for bilinear forms of finite vector spaces. In each of these models, we consider an infinite family of linear maximum rank distance codes obtained by puncturing generalized twisted Gabidulin codes. We calculate the automorphism group of such codes, and we prove that this family contains many codes which are not equivalent to any generalized Gabidulin code. This solves a problem posed recently by Sheekey (Adv Math Commun 10:475–488, 2016).

Keywords Maximum rank distance code · Circulant matrix · Singer cycle

1 Introduction

Let $M_{m,n}(\mathbb{F}_q)$, $m \leq n$, be the rank metric space of all the $m \times n$ matrices with entries in the finite field $\mathbb{F}_q$ with q elements, $q = p^h$, p a prime. The *distance* between two matrices by definition is the rank of their difference. An $(m, n, q; s)$-*rank distance code* (also *rank metric code*) is any subset $\mathcal{X}$ of $M_{m,n}(\mathbb{F}_q)$ such that the distance between two of its distinct elements is at least s. An $(m, n, q; s)$-rank distance code is said to be *linear* if it is an $\mathbb{F}_q$-linear subspace of $M_{m,n}(\mathbb{F}_q)$.

Bence Csajbók is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. Bence Csajbók acknowledges the support of OTKA Grant No. K 124950.

✉ Bence Csajbók
csajbokb@cs.elte.hu

✉ Alessandro Siciliano
alessandro.siciliano@unibas.it

[1] MTA-ELTE Geometric and Algebraic Combinatorics Research Group, Department of Geometry, ELTE Eötvös Loránd University, Pázmány P. stny. 1/C, Budapest 1117, Hungary

[2] Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Potenza, Italy

It is known [9] that the size of an $(m, n, q; s)$-rank distance code $\mathcal{X}$ is bounded by the *Singleton-like bound*:

$$|\mathcal{X}| \leq q^{n(m-s+1)}.$$

When this bound is achieved, $\mathcal{X}$ is called an $(m, n, q; s)$-*maximum rank distance code*, or $(m, n, q; s)$-*MRD code* for short.

Although MRD codes are very interesting by their own and they caught the attention of many researchers in recent years [1,8,28,29], such codes also have practical applications in error-correction for random network coding [15,20,31], space-time coding [32] and cryptography [14,30].

Obviously, investigations of MRD codes can be carried out in any rank metric space isomorphic to $M_{m,n}(\mathbb{F}_q)$. In his pioneering paper [9], Ph. Delsarte constructed linear MRD codes for all the possible values of the parameters m, n, q and s by using the framework of bilinear forms on two finite-dimensional vector spaces over a finite field. Delsarte called such sets *Singleton systems* instead of maximum rank distance codes. Few years later, Gabidulin [13] independently constructed Delsarte's linear MRD codes as evaluation codes of linearized polynomials over a finite field [21]. Although originally discovered by Delsarte, these codes are now called *Gabidulin codes*. In [19] Gabidulin's construction was generalized to get different MRD codes. These codes are now known as *Generalized Gabidulin codes*. For $m = n$ a different construction of Delsarte's MRD codes was given by Cooperstein [5] in the framework of the tensor product of a vector space over $\mathbb{F}_q$ by itself.

Recently, Sheekey [29] presented a new family of linear MRD codes by using linearized polynomials over $\mathbb{F}_{q^n}$. These codes are now known as *generalized twisted Gabidulin codes*. The equivalence classes of these codes were determined by Lunardon et al. [24]. In [27] a further generalization was considered giving new MRD codes when $m < n$; the authors call these codes generalized twisted Gabidulin codes as well. In this paper the term "generalized twisted Gabidulin code" will be used for codes defined in [29, Remark 8]. For different relations between linear MRD codes and linear sets see [7,23], [29, Section 5], [6, Section 5]. To the extent of our knowledge, these are the only infinite families of linear MRD codes with $m < n$ appearing in the literature.

In [11] infinite families of nonlinear $(n, n, q; n-1)$-MRD codes, for $q \geq 3$ and $n \geq 3$ have been constructed. These families contain the nonlinear MRD codes provided by Cossidente et al. [6]. These codes have been afterward generalized in [10] by using a more geometric approach. A generalization of Sheekey's example which yields additive but not $\mathbb{F}_q$-linear codes can be found in [26].

Let $\mathcal{X}$ be a rank distance code in $M_{n,n}(\mathbb{F}_q)$. For any given $m \times n$ matrix A over $\mathbb{F}_q$ of rank $m < n$, the set $A\mathcal{X} = \{AM : M \in \mathcal{X}\}$ is a rank distance code in $M_{m,n}(\mathbb{F}_q)$. The code $A\mathcal{X}$ is said to be obtained by *puncturing* $\mathcal{X}$ *with* A and $A\mathcal{X}$ is called a *punctured code*. The reason of this definition is that if $A = (\mathrm{I}_m|\mathbf{0}_{n-m})$, where I_m and $\mathbf{0}_{n-m}$ is the $m \times m$ identity and $m \times (n-m)$ null matrix, respectively, then the matrices of $A\mathcal{X}$ are obtained by deleting the last $n-m$ rows from the matrices in $\mathcal{X}$. Punctured rank metric codes have been studied before in [3,25], but the equivalence problem among these codes have not been dealt with in these papers.

In [29, Remark 9] Sheekey posed the following problem:

Are the MRD codes obtained by puncturing generalized twisted Gabidulin codes equivalent to the codes obtained by puncturing generalized Gabidulin codes?

Here we investigate punctured codes and study the above problem in the framework of bilinear forms. We point out that the very recent preprint [34] deals with the same problem by using q-linearized polynomials. In [34] the authors investigate the middle nucleus and the right nucleus of punctured generalized twisted Gabidulin codes, for $m < n$. By exploiting these nuclei, they derive necessary conditions on the automorphisms of these codes which depend on certain restrictions for the parameters.

Let V and V' be two vector spaces over $\mathbb{F}_q$ of dimensions m and n, respectively. Since the rank is invariant under matrix transposition, we may assume $m \leq n$.

A *bilinear form* on V and V' is a function $f : V \times V' \to \mathbb{F}_q$ that satisfies the identity

$$f\left(\sum_i x_i v_i, \sum_j x'_j v'_j\right) = \sum_{i,j} x_i f\left(v_i, v'_j\right) x'_j,$$

for all scalars $x_i, x'_j \in \mathbb{F}_q$ and all vectors $v_i \in V$, $v'_j \in V'$. The set $\Omega_{m,n} = \Omega(V, V')$ of all bilinear forms on V and V' is an mn-dimensional vector space over $\mathbb{F}_q$.

The *left radical* $\mathrm{Rad}(f)$ of any $f \in \Omega_{m,n}$ is by definition the subspace of V consisting of all vectors v satisfying $f(v, v') = 0$ for every $v' \in V'$. The *rank* of f is the codimension of $\mathrm{Rad}(f)$, i.e.,

$$\mathrm{rank}(f) = m - \dim_{\mathbb{F}_q}(\mathrm{Rad}(f)). \tag{1}$$

Then the $\mathbb{F}_q$-vector space $\Omega_{m,n}$ equipped with the above rank function is a rank metric space over $\mathbb{F}_q$.

Let $\{u_0, \ldots, u_{m-1}\}$ and $\{u'_0, \ldots, u'_{n-1}\}$ be a basis for V and V', respectively. For any $f \in \Omega_{m,n}$, the $m \times n$ $\mathbb{F}_q$-matrix $M_f = (f(u_i, u'_j))$, is called the *matrix of f in the bases* $\{u_0, \ldots, u_{m-1}\}$ *and* $\{u'_0, \ldots, u'_{n-1}\}$. It turns out that the map

$$\begin{array}{rccc} \nu_{\{u_0,\ldots,u_{m-1};u'_0,\ldots,u'_{n-1}\}} : & \Omega_{m,n} & \to & M_{m,n}(\mathbb{F}_q) \\ & f & \mapsto & M_f \end{array} \tag{2}$$

is an isomorphism of rank metric spaces with $\mathrm{rank}(f) = \mathrm{rank}(M_f)$.

Let $\Gamma\mathrm{L}(\Omega_{m,n})$ denote the *general semilinear group* of the mn-dimensional $\mathbb{F}_q$-vector space $\Omega_{m,n}$, that is, the group of all invertible semilinear transformations of $\Omega_{m,n}$. Let $\{w_1, \ldots, w_{mn}\}$ be a basis for $\Omega_{m,n}$, and recall that $\mathrm{Aut}(\mathbb{F}_q) = \langle \phi_p \rangle$, where $\phi_p : \mathbb{F}_q \to \mathbb{F}_q$ is the Frobenius map $\lambda \mapsto \lambda^p$. Using ϕ_p, we define the map $\phi : \Omega_{m,n} \to \Omega_{m,n}$ by

$$\phi : \sum_i \lambda_i w_i \mapsto \sum_i \lambda_i^p w_i.$$

Then ϕ is an invertible semilinear transformation of $\Omega_{m,n}$, and for $(a_{ij}) \in \mathrm{GL}(mn, q)$ we have $(a_{ij})^{\phi} = (a_{ij}^{p})$. Therefore ϕ normalizes the general linear group $\mathrm{GL}(mn, q)$ and we have $\Gamma\mathrm{L}(\Omega_{m,n}) = \mathrm{GL}(\Omega_{m,n}) \rtimes \mathrm{Aut}(\mathbb{F}_q)$.

An *automorphism* of the rank metric space $\Omega_{m,n}$ is any transformation $\tau \in \Gamma\mathrm{L}(\Omega_{m,n})$ such that $\mathrm{rank}(f^{\tau}) = \mathrm{rank}(f)$, for all $f \in \Omega_{m,n}$. The *automorphism group* $\mathrm{Aut}(\Omega_{m,n})$ of $\Omega_{m,n}$ is the group of all automorphisms of $\Omega_{m,n}$, i.e.,

$$\mathrm{Aut}(\Omega_{m,n}) = \{\tau \in \Gamma\mathrm{L}(\Omega_{m,n}) : \mathrm{rank}(f^{\tau}) = \mathrm{rank}(f), \quad \text{for all } f \in \Omega_{m,n}\}.$$

By [35, Theorem 3.4],

$$\mathrm{Aut}(\Omega_{m,n}) = (\mathrm{GL}(V) \times \mathrm{GL}(V')) \rtimes \mathrm{Aut}(\mathbb{F}_q) \quad \text{for } m < n,$$

and

$$\mathrm{Aut}(\Omega_{n,n}) = (\mathrm{GL}(V') \times \mathrm{GL}(V')) \rtimes \langle \top \rangle \rtimes \mathrm{Aut}(\mathbb{F}_q) \quad \text{for } m = n,$$

where $\top$ is an involutorial operator. In details, any given $(g, g') \in \mathrm{GL}(V) \times \mathrm{GL}(V')$ defines the linear automorphism of $\Omega_{m,n}$ given by

$$f^{(g,g')}(v, v') = f(gv, g'v'),$$

for any $f \in \Omega_{m,n}$. If A and B are the matrices of $g \in \mathrm{GL}(V)$ and $g' \in \mathrm{GL}(V')$ in the given bases for V and V', then the matrix of $f^{(g,g')}$ is $A^t M_f B$, where t denotes transposition. Additionally, the semilinear transformation ϕ of $\Omega_{m,n}$ is the automorphism given by

$$f^{\phi}(v, v') = \left[f\left(v^{\phi^{-1}}, v'^{\phi^{-1}} \right) \right]^{p}.$$

If $M_f = (a_{ij})$ is the matrix of f in the given bases for V and V', then the matrix of f^{ϕ} is $M_f^{\phi} = (a_{ij}^{p})$. Therefore ϕ normalizes the group $\mathrm{GL}(V) \times \mathrm{GL}(V')$. If $m < n$, the above automorphisms are all the elements in $\mathrm{Aut}(\Omega_{m,n})$.

If $m = n$, one may assume, and we do, $V' = V = \langle u_0, \ldots, u_{m-1} \rangle$. The involutorial operator $\top : \Omega_{n,n} \to \Omega_{n,n}$ is defined by setting

$$f^{\top}(v, v') = f(v', v).$$

If $M_f = (a_{ij})$ is the matrix of f in the given bases for V and V', then the matrix of $f^{\top}$ is the transpose matrix M_f^t of M_f. The operator $\top$ acts on $\mathrm{GL}(V) \times \mathrm{GL}(V)$ by mapping (g, g') to (g', g).

For a given subset $\mathcal{X}$ of $\Omega_{m,n}$, the *automorphism group* of $\mathcal{X}$ is the subgroup of $\mathrm{Aut}(\Omega_{m,n})$ fixing $\mathcal{X}$. Two subsets $\mathcal{X}_1, \mathcal{X}_2$ of $\Omega_{m,n}$ are said to be *equivalent* if there exists $\varphi \in \mathrm{Aut}(\Omega_{m,n})$ such that $\mathcal{X}_2 = \mathcal{X}_1^{\varphi}$.

The main tool we use in this paper is the kth cyclic model in $V(r, q^r)$ for an r-dimensional vector space $V(r, q)$ over $\mathbb{F}_q$, where k is any positive integer such that

$\gcd(r,k)=1$. This model generalizes the cyclic model introduced in [5,12,17], and it is studied in Sect. 2. In particular, the endomorphisms of the kth cyclic model are represented by $r\times r$ q^k-circulant matrices over $\mathbb{F}_{q^r}$.

For any k such that $\gcd(m,k)=1=\gcd(n,k)$, the elements of $\Omega_{m,n}$ acting on the kth cyclic model of V and V' are represented by q^k-circulant $m\times n$ matrices over $\mathbb{F}_{q^d}$, where $d=\operatorname{lcm}(m,n)$. We then have a description of the elements in $\mathrm{Aut}(\Omega_{m,n})$ in terms of q^k-circulant matrices.

In Sect. 3 we prove that the code obtained by puncturing an $(n,n,q;s)$-MRD code is an $(m,n,q;s+m-n)$-MRD code, where $n-s<m\le n$. In particular, the code in $\Omega_{m,n}$ obtained by puncturing a generalized Gabidulin code in $\Omega_{n,n}$ is a generalized Gabidulin code. Conversely, every generalized Gabidulin code in $\Omega_{m,n}$ can be obtained by puncturing a generalized Gabidulin code in $\Omega_{n,n}$.

By using the representation by q^k-circulant matrices of the elements of $\Omega_{m,n}$ acting on the kth cyclic model for V and V', we calculate the automorphism group of some generalized Gabidulin code. In Sect. 3 we also construct an infinite family of MRD codes by puncturing generalized twisted Gabidulin codes [24,29]. We calculate the automorphism group of these codes in Sect. 4. By using a recent result by Liebhold and Nebe [22], we prove in Sect. 5 that the above family contains many MRD codes which are inequivalent to the MRD codes obtained by puncturing generalized Gabidulin codes. This solves the problem posed by Sheekey in [29, Remark 9].

2 Cyclic models for bilinear forms on finite vector spaces

Let $V(r,q)=\langle u_0,\dots,u_{r-1}\rangle_{\mathbb{F}_q}$, $r\ge 2$, be an r-dimensional vector space over the finite field $\mathbb{F}_q$. We denote the set of all linear transformations of $V(r,q)$ by $\mathrm{End}(V(r,q))$.

Embed $V(r,q)$ in $V(r,q^r)$ by extending the scalars. Concretely this can be done by defining $V(r,q^r)=\{\sum_{i=0}^{r-1}\lambda_i u_i:\lambda_i\in\mathbb{F}_{q^r}\}$.

Let $\xi:V(r,q^r)\to V(r,q^r)$ be the $\mathbb{F}_{q^r}$-semilinear transformation with associated automorphism $\delta:x\in\mathbb{F}_{q^r}\to x^q\in\mathbb{F}_{q^r}$ such that $\xi(u_i)=u_i$. Clearly, $V(r,q)$ consists of all the vectors in $V(r,q^r)$ which are fixed by ξ.

In the paper [5], the cyclic model of $V(r,q)$ was introduced by taking the eigenvectors $s_0,\dots,s_{r-1}$ in $V(r,q^r)$ of a Singer cycle σ of $V(r,q)$; here a *Singer cycle* of $V(r,q)$ is an element σ of $\mathrm{GL}(V(r,q))$ of order q^r-1. The cyclic group $S=\langle\sigma\rangle$ is called a *Singer cyclic group of* $\mathrm{GL}(V(r,q))$ [18].

Since $s_0,\dots,s_{r-1}$ have distinct eigenvalues in $\mathbb{F}_{q^r}$, they form a basis of the extension $V(r,q^r)$ of $V(r,q)$.

In this basis the matrix of σ is the diagonal matrix $\mathrm{diag}(w,w^q,\dots,w^{q^{r-1}})$, where w is a primitive element of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ and w^{q^i} is the eigenvalue of s_i. The action of the linear part ℓ_ξ of the $\mathbb{F}_{q^r}$-semilinear transformation ξ is given by $\ell_\xi(s_i)=s_{i+1}$, where the indices are considered modulo r [5]. It follows that

$$V(r,q)=\left\{\sum_{i=0}^{r-1}x^{q^i}s_i:x\in\mathbb{F}_{q^r}\right\}. \tag{3}$$

We call $\{s_0, \ldots, s_{r-1}\}$ a *Singer basis* for $V(r,q)$ and the representation (3) for $V(r,q)$, or equivalently the set $\{(x, x^q, \ldots, x^{q^{r-1}}) : x \in \mathbb{F}_{q^r}\} \subset \mathbb{F}_{q^r}^r$, is the *cyclic model for* $V(r,q)$ [12,17].

We point out that the $\mathbb{F}_{q^r}$-semilinear transformation $\phi : V(r,q^r) \to V(r,q^r)$ with associated automorphism the Frobenius map $\phi_p : x \in \mathbb{F}_{q^r} \to x^p \in \mathbb{F}_{q^r}$ such that $\phi(u_i) = u_i$ acts on the cyclic model (3) by mapping $xs_0 + x^q s_1 + \cdots + x^{q^{r-1}} s_{r-1}$ to $x^{pq^{r-1}} s_0 + x^p s_1 + \cdots + x^{pq^{r-2}} s_{r-1}$.

Let k be a positive integer such that $\gcd(k,r) = 1$. Set $s_i^{(k)} = s_{ki \bmod r}$, for $i = 0, \ldots, r-1$. For brevity, we use $[j] = q^j$ and $a^{[j]} = a^{q^j}$, for any $a \in \mathbb{F}_{q^r}$. It is clear that the exponent j is taken mod r because of the field size. Then we may write

$$V(r,q) = \left\{ \sum_{i=0}^{r-1} x^{[ki]} s_i^{(k)} : x \in \mathbb{F}_{q^r} \right\}. \tag{4}$$

We call the representation (4) for $V(r,q)$, or equivalently the set $\{(x, x^{[k]}, \ldots, x^{[k(r-1)]}) : x \in \mathbb{F}_{q^r}\} \subset \mathbb{F}_{q^r}^r$, the kth *cyclic model for* $V(r,q)$.

It is easily seen that the linear part of the semilinear transformation ξ^k acts on the kth cyclic model for $V(r,q)$ by mapping $s_i^{(k)}$ to $s_{i+1}^{(k)}$, with indices considered modulo r.

An $r \times r$ q^k*-circulant matrix* over $\mathbb{F}_{q^r}$ is a matrix of the form

$$D^{(k)}_{(a_0,a_1,\ldots,a_{r-1})} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{r-1} \\ a_{r-1}^{[k]} & a_0^{[k]} & \cdots & a_{r-2}^{[k]} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{[k(r-1)]} & a_2^{[k(r-1)]} & \cdots & a_0^{[k(r-1)]} \end{pmatrix}$$

with $a_i \in \mathbb{F}_{q^r}$. We say that the above matrix is *generated by the array* $(a_0, \ldots, a_{r-1})$.

Let $\mathcal{D}_r^{(k)}(\mathbb{F}_{q^r})$ denote the matrix algebra formed by all $r \times r$ q^k-circulant matrices over $\mathbb{F}_{q^r}$ and $\mathcal{B}_r^{(k)}(\mathbb{F}_{q^r})$ the set of all invertible q^k-circulant $r \times r$ matrices. When $k = 1$, an $r \times r$ q-circulant matrix over $\mathbb{F}_{q^r}$ is also known as a *Dickson matrix*, $\mathcal{D}_r(\mathbb{F}_{q^r}) = \mathcal{D}_r^{(1)}(\mathbb{F}_{q^r})$ is the *Dickson matrix algebra* and $\mathcal{B}_r(\mathbb{F}_{q^r}) = \mathcal{B}_r^{(1)}(\mathbb{F}_{q^r})$ is the *Betti–Mathieu group* [2,4]. It is known that $\mathrm{End}(V(r,q)) \simeq \mathcal{D}_r(\mathbb{F}_{q^r})$ and $\mathcal{B}_r(\mathbb{F}_{q^r}) \simeq \mathrm{GL}(V(r,q))$ [21,36].

Remark 2.1 In terms of matrix representation, the above isomorphisms are described as follows. Let $V(r,q) = \langle u_0, \ldots, u_{r-1} \rangle_{\mathbb{F}_q}$ and $\{s_0, \ldots, s_{r-1}\}$ a Singer basis for $V(r,q)$ defined by the primitive element w of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Up to a change of the basis $\{u_0, \ldots, u_{r-1}\}$ in $V(r,q)$, we may assume

$$u_i = w^i s_0 + \cdots + w^{iq^{r-1}} s_{r-1}, \quad \text{for } i = 0, \ldots, r-1.$$

Notice that $u_i \in V(r,q)$, for $i = 0, \ldots, r-1$. The non-singular Moore matrix

$$E_r = \begin{pmatrix} 1 & w & \cdots & w^{r-1} \\ 1 & w^q & \cdots & w^{(r-1)q} \\ \vdots & \vdots & & \vdots \\ 1 & w^{q^{r-1}} & \cdots & w^{(r-1)q^{r-1}} \end{pmatrix} \tag{5}$$

is the matrix of the change of basis from $\{u_0, \ldots, u_{r-1}\}$ to $\{s_0, \ldots, s_{r-1}\}$. Therefore, the matrix map $D \in \mathcal{D}_r(\mathbb{F}_{q^r}) \to E_r^{-1} D E_r \in M_{r,r}(\mathbb{F}_q)$ realizes the above isomorphism.

Proposition 2.2 $\mathrm{End}(V(r,q)) \simeq \mathcal{D}_r^{(k)}(\mathbb{F}_{q^r})$ *and* $\mathrm{GL}(V(r,q)) \simeq \mathcal{B}_r^{(k)}(\mathbb{F}_{q^r})$.

Proof For any $\mathbf{a} = (a_0, \ldots, a_{r-1})$ over $\mathbb{F}_{q^r}$, the q^k-circulant matrix $D_{\mathbf{a}}^{(k)}$ acts on the kth cyclic model (4) for $V(r,q)$ by mapping $(x, x^{[k]}, \ldots, x^{[k(r-1)]})$ to $(a_0 x + a_1 x^{[k]} + \cdots + a_{r-1} x^{[k(r-1)]}, a_{r-1}^{[k]} x + a_0^{[k]} x^{[k]} + \cdots + a_{r-2}^{[k]} x^{[k(r-1)]}, \ldots, a_1^{[k(r-1)]} x + a_2^{[k(r-1)]} x^{[k]} + \cdots + a_0^{[k(r-1)]} x^{[k(r-1)]})$, giving $D_{\mathbf{a}}^{(k)}$ is an endomorphism of (4). Let $D_{\mathbf{a}}, D_{\mathbf{a}'} \in \mathcal{D}_r^{(k)}(\mathbb{F}_{q^r})$ such that $D_{\mathbf{a}} \mathbf{x}^t = D_{\mathbf{a}'} \mathbf{x}^t$, for every $\mathbf{x} = (x, x^{[k]}, \ldots, x^{[k(r-1)]})$, $x \in \mathbb{F}_{q^r}$. Hence, $(a_0 - a_0')x + (a_1 - a_1')x^{[k]} + \cdots + (a_{r-1} - a_{r-1}')x^{[k(r-1)]} = 0$, for all $x \in \mathbb{F}_{q^r}$. As the left hand side is a polynomial of degree at most q^{r-1} with q^r roots, we get $\mathbf{a} = \mathbf{a}'$. Therefore, matrices in $\mathcal{D}_r^{(k)}(\mathbb{F}_{q^r})$ represent q^{r^2} distinct endomorphisms of the kth cyclic model for $V(r,q)$. As $q^{r^2} = |\mathrm{End}(V(r,q))|$, we get the result. □

Remark 2.3 Let K_r be the (permutation) matrix of the change of basis from $\{s_0^{(k)}, \ldots, s_{r-1}{}^{(k)}\}$ to $\{s_0, \ldots, s_{r-1}\}$. As $s_i^{(k)} = s_{ik \bmod r}$, for $i = 0, \ldots, r-1$, then the ith column of K_r is the array $(0, \ldots, 0, 1, 0, \ldots, 0)^t$ where 1 is in position $ik \bmod r$, for $i = 0, \ldots, r-1$. If $\tau \in \mathrm{End}(V(r,q))$ has q^k-circulant matrix $D^{(k)}_{(a_0, a_1, \ldots, a_{r-1})}$ in the basis $\{s_0^{(k)}, \ldots, s_{r-1}{}^{(k)}\}$, then the matrix of τ in the Singer basis $\{s_0, \ldots, s_{r-1}\}$ is the q-circulant matrix $D_{(b_0, \ldots, b_{r-1})} = K_r D^{(k)}_{(a_0, a_1, \ldots, a_{r-1})} K_r^{-1}$, for some array $(b_0, \ldots, b_{r-1})$ over $\mathbb{F}_{q^r}$. Since $\gcd(k, r) = 1$, we can write $1 = lr + hk$, for some integers l, h, giving

$$b_i = a_{ih \bmod r}, \quad \text{for } i = 0, \ldots, r-1.$$

Therefore, $\mathcal{D}_r^{(k)}(\mathbb{F}_{q^r}) = K_r^{-1} \mathcal{D}_r(\mathbb{F}_{q^r}) K_r$ and $\mathcal{B}_r^{(k)}(\mathbb{F}_{q^r}) = K_r^{-1} \mathcal{B}_r(\mathbb{F}_{q^r}) K_r$.

Remark 2.4 We explicitly describe the action of $\mathrm{Aut}(\mathbb{F}_q)$ on $V(r, q^r)$ in the Singer basis $\{s_0^{(k)}, \ldots, s_{r-1}^{(k)}\}$. By Remark 2.1 the invertible semilinear transformation ϕ of $V(r, q^r)$ defined by the Frobenius map $\phi_p : x \in \mathbb{F}_{q^r} \to x^p \in \mathbb{F}_{q^r}$ acts in the basis $\{s_0, \ldots, s_{r-1}\}$ via the pair $(E_r (E_r^{-1})^p; \phi_p)$, where E_r is the non-singular Moore matrix (5) and $(E_r^{-1})^p$ is the matrix obtained by E_r^{-1} by applying ϕ_p to every entry. By Remark 2.3 ϕ acts in the basis $\{s_0^{(k)}, \ldots, s_{r-1}^{(k)}\}$ via the pair $(K_r^{-1} E_r (E_r^{-1})^p K_r; \phi_p)$, since $K_r^p = K_r$.

Let $V = \langle u_0, \ldots, u_{m-1}\rangle_{\mathbb{F}_q}$ and $V' = \langle u'_0, \ldots, u'_{n-1}\rangle_{\mathbb{F}_q}$, with $m \leq n$. If $m = n$ we take $V' = V = \langle u_0, \ldots, u_{m-1}\rangle_{\mathbb{F}_q}$. Let σ and σ' be Singer cycles of $\mathrm{GL}(V)$ and $\mathrm{GL}(V')$, respectively, with associated semilinear transformations ξ and ξ'. Let $\{s_0, \ldots, s_{m-1}\}$ and $\{s'_0, \ldots, s'_{n-1}\}$ be a Singer basis for V and V', defined by σ and σ', respectively. For any given positive integer k such that $\gcd(k, n) = \gcd(k, m) = 1$, let $\{s_0^{(k)}, \ldots, s_{m-1}^{(k)}\}$ and $\{s_0^{\prime(k)}, \ldots, s_{n-1}^{\prime(k)}\}$ be the bases of $V(m, q^m)$ and $V(n, q^n)$ defined as above. Therefore, we may consider $\Omega_{m,n}$ as the set of all bilinear forms acting on the kth cyclic model for V and V'. In addition, any element in $\mathrm{GL}(V) \times \mathrm{GL}(V')$ is represented by a pair $(A, B) \in \mathcal{B}_m^{(k)}(\mathbb{F}_{q^m}) \times \mathcal{B}_n^{(k)}(\mathbb{F}_{q^n})$.

Set $e = \gcd(m, n)$ and $d = \mathrm{lcm}(m, n)$, the greatest common divisor and the least common multiple of m and n, respectively.

Let $\mathrm{Tr}_{q^d/q}$ denote the trace function from $\mathbb{F}_{q^d}$ onto $\mathbb{F}_q$:

$$\mathrm{Tr}_{q^d/q} : y \in \mathbb{F}_{q^d} \to \mathrm{Tr}_{q^d/q}(y) = \sum_{i=0}^{d-1} y^{q^i} \in \mathbb{F}_q.$$

Since $\gcd(k, d) = 1$, we may write $\mathrm{Tr}_{q^d/q}$ as

$$T^{(k)} : y \in \mathbb{F}_{q^d} \to T^{(k)}(y) = \sum_{i=0}^{d-1} y^{[k]} \in \mathbb{F}_q.$$

For $0 \leq j \leq e-1$ and a given $a \in \mathbb{F}_{q^d}$ and $v = xs_0^{(k)} + \cdots + x^{[k(m-1)]}s_{m-1}^{(k)} \in V$ and $v' = x's_0^{\prime(k)} + \cdots + x'^{[k(n-1)]}s_{n-1}^{\prime(k)}$, the map

$$f_{a,j}^{(k)}(v, v') = T^{(k)}(axx'^{[kj]}) \tag{6}$$

is a bilinear form on the kth cyclic model for V and V'. We set

$$\Omega_j^{(k)} = \{f_{a,j}^{(k)} : a \in \mathbb{F}_{q^d}\}, \quad \text{for } 0 \leq j \leq e-1. \tag{7}$$

The following result gives the decomposition of $\Omega_{m,n}$ as sum of the subspaces $\Omega_j^{(k)}$.

Theorem 2.5

$$\Omega_{m,n} = \bigoplus_{j=0}^{e-1} \Omega_j^{(k)}. \tag{8}$$

Proof Let first assume $k = 1$. For any e-tuple $\mathbf{a} = (a_0, \ldots, a_{e-1})$ over $\mathbb{F}_{q^d}$ we define an $m \times n$ matrix $D_{\mathbf{a}} = D_{\mathbf{a}}^{(1)} = (d_{i,j})$ over $\mathbb{F}_{q^d}$ as follows. We will use indices from 0 for both rows and columns of $D_{\mathbf{a}}$. Let $d_{0,j} = a_j$, for $0 \leq j \leq e-1$, and let $d_{i,j} = d_{i-1,j-1}$, where the row index is taken modulo m and the column index is taken modulo n. Notice that the above rule determines every entry of $D_{\mathbf{a}}$. In fact, $d_{i,j} = a_l^{q^s}$, where $l \equiv j - iv \pmod{e}$, $0 \leq l \leq e-1$ and $s = \beta m + i$, where β is the unique integer in $\{0, 1, \ldots, n/e - 1\}$ such that $j - i \equiv l + \beta m \pmod{n}$.

Now let $f_{a,j} \in \Omega_j$. Then the matrix of $f_{a,j}$ in the Singer bases $\{s_0, \ldots, s_{m-1}\}$ and $\{s'_0, \ldots, s'_{n-1}\}$ is the matrix obtained by applying the above construction to the array $\mathbf{a} = (0, \ldots, 0, a, 0, \ldots, 0)$, with a in the jth position. It is now easy to see that the $\mathbb{F}_q$-spaces Ω_j, for $j = 0, \ldots, e-1$ intersect trivially. By consideration on dimensions we may write $\Omega_{m,n} = \bigoplus_{j=0}^{e-1} \Omega_j$.

The kth cyclic model for V' and V is obtained from the cyclic model by applying the changing of basis described in Remark 2.3. Therefore the $\mathbb{F}_q$-spaces $\Omega_j^{(k)}$, $k > 1$, are pairwise skew and $\Omega_{m,n} = \bigoplus_{j=0}^{e-1} \Omega_j^{(k)}$. □

Example 1 Let $m = 2$, $n = 6$ and $k = 1$, so that $d = 6$ and $e = 2$. For any array $\mathbf{a} = (a_0, a_1)$ over $\mathbb{F}_{q^6}$, we have

$$D_{\mathbf{a}} = \begin{pmatrix} a_0 & a_1 & a_0^{q^2} & a_1^{q^2} & a_0^{q^4} & a_1^{q^4} \\ a_1^{q^5} & a_0^{q} & a_1^{q} & a_0^{q^3} & a_1^{q^3} & a_0^{q^5} \end{pmatrix}.$$

Example 2 Let $m = 4$, $n = 6$ and $k = 5$, so that $d = 12$ and $e = 2$. For any array $\mathbf{a} = (a_0, a_1)$ over $\mathbb{F}_{q^{12}}$, we have

$$D_{\mathbf{a}}^{(k)} = \begin{pmatrix} a_0 & a_1 & a_0^{[8k]} & a_1^{[8k]} & a_0^{[4k]} & a_1^{[4k]} \\ a_1^{[5k]} & a_0^{[k]} & a_1^{[k]} & a_0^{[9k]} & a_1^{[9k]} & a_0^{[5k]} \\ a_0^{[6k]} & a_1^{[6k]} & a_0^{[2k]} & a_1^{[2k]} & a_0^{[10k]} & a_1^{[10k]} \\ a_1^{[11k]} & a_0^{[7k]} & a_1^{[7k]} & a_0^{[3k]} & a_1^{[3k]} & a_0^{[11k]} \end{pmatrix}$$
$$= \begin{pmatrix} a_0 & a_1 & a_0^{q^4} & a_1^{q^4} & a_0^{q^8} & a_1^{q^8} \\ a_1^{q} & a_0^{q^5} & a_1^{q^5} & a_0^{q^9} & a_1^{q^9} & a_0^{q} \\ a_0^{q^6} & a_1^{q^6} & a_0^{q^{10}} & a_1^{q^{10}} & a_0^{q^2} & a_1^{q^2} \\ a_1^{q^7} & a_0^{q^{11}} & a_1^{q^{11}} & a_0^{q^3} & a_1^{q^3} & a_0^{q^7} \end{pmatrix}.$$

We call a matrix of type $D_{\mathbf{a}}^{(k)}$ an $m \times n$ q^k*-circulant matrix* over $\mathbb{F}_{q^d}$, where $d = \mathrm{lcm}(m, n)$. We say that $D_{\mathbf{a}}^{(k)}$ is *generated by the array* $\mathbf{a} = (a_0, a_1, \ldots, a_{e-1})$, where $e = \gcd(m, n)$. We will denote the set of all $m \times n$ q^k-circulant matrices over $\mathbb{F}_{q^d}$ by $\mathcal{D}_{m,n}^{(k)}(\mathbb{F}_{q^d})$.

The next result gives a description of $\Omega_{m,n}$ and $\mathrm{Aut}(\Omega_{m,n})$ in terms of q^k-circulant matrices.

Proposition 2.6 *Let $m \leq n$. Then $\Omega_{m,n} \simeq \mathcal{D}_{m,n}^{(k)}(\mathbb{F}_{q^d})$.*

If $m < n$, then

$$\mathrm{Aut}(\Omega_{m,n}) \simeq \left(\mathcal{B}_m^{(k)}(\mathbb{F}_{q^m}) \times \mathcal{B}_n^{(k)}(\mathbb{F}_{q^n})\right) \rtimes \mathrm{Aut}(\mathbb{F}_q);$$

if $m = n$, then

$$\mathrm{Aut}(\Omega_{n,n}) \simeq \left(\mathcal{B}_n^{(k)}(\mathbb{F}_{q^m}) \times \mathcal{B}_n^{(k)}(\mathbb{F}_{q^n})\right) \rtimes \langle \top \rangle \rtimes \mathrm{Aut}(\mathbb{F}_q).$$

Proof For any $\mathbf{a} = (a_0, \ldots, a_{e-1})$ over $\mathbb{F}_{q^d}$ we consider the bilinear form $f_{\mathbf{a}}^{(k)} = f_{a_0,0}^{(k)} + \cdots + f_{a_{e-1},e-1}^{(k)}$. Straightforward calculation shows that the matrix of $f_{\mathbf{a}}^{(k)}$ in the bases $\{s_0^{(k)}, \ldots, s_{m-1}^{(k)}\}$ and $\{s_0^{\prime(k)}, \ldots, s_{n-1}^{\prime(k)}\}$ is the $m \times n$ q^k-circulant matrix $D_{\mathbf{a}}^{(k)}$ generated by $\mathbf{a}$. Now assume that $f_{\mathbf{a}}^{(k)}$ is the null bilinear form. Let $V = \langle u_0, \ldots, u_{m-1}\rangle_{\mathbb{F}_q}$ and $V' = \langle u'_0, \ldots, u'_{n-1}\rangle_{\mathbb{F}_q}$. By Remarks 2.1 and 2.3 the matrix of $f_{\mathbf{a}}^{(k)}$ in the bases $\{u_0, \ldots, u_{m-1}\}$ and $\{u'_0, \ldots, u'_{n-1}\}$ is $(K_m^{-1}E_m)^t D_{\mathbf{a}}^{(k)}(K_n^{-1}E_n)$, which is clearly the zero matrix. As $K_m^{-1}E_m$ and $K_n^{-1}E_n$ are both non-singular we get $D_{\mathbf{a}}^{(k)}$ is the zero matrix giving $\mathbf{a}$ is the zero array. Therefore, matrices in $\mathcal{D}_{m,n}^{(k)}(\mathbb{F}_{q^r})$ represent $q^{de} = q^{mn}$ distinct bilinear forms acting on the kth cyclic models for V and V'. As $q^{mn} = |\Omega_{m,n}|$, we get $\Omega_{m,n} \simeq \mathcal{D}_{m,n}^{(k)}(\mathbb{F}_{q^d})$.

To prove the second part of the Proposition we first note that Proposition 2.2 implies that the group of all $\mathbb{F}_q$-linear automorphisms of $\Omega_{m,n}$ is isomorphic to $(\mathcal{B}_m^{(k)}(\mathbb{F}_{q^m}) \times \mathcal{B}_n^{(k)}(\mathbb{F}_{q^n}))$, if $m < n$, and to $(\mathcal{B}_m^{(k)}(\mathbb{F}_{q^m}) \times \mathcal{B}_n^{(k)}(\mathbb{F}_{q^n})) \rtimes \langle \top \rangle$, if $m = n$.

If $D_{(a_0,\ldots,a_{e-1})}^{(k)}$ is the matrix of f in the bases $\{s_0, \ldots, s_{m-1}\}$ and $\{s_0, \ldots, s_{n-1}\}$ for V and V' respectively, then f^{ϕ} is $D_{(a_0^p,\ldots,a_{e-1}^p)}^{(k)}$ by Remark 2.4. This concludes the proof. □

Remark 2.7 The isomorphism $\nu = \nu_{\{s_0^{(k)},\ldots,s_{m-1}^{(k)};s_0^{\prime(k)},\ldots,s_{n-1}^{\prime(k)}\}} : \Omega_{m,n} \to \mathcal{D}_{m,n}^{(k)}(\mathbb{F}_{q^d})$ is described as follows. Let $V = \langle u_0, \ldots, u_{m-1}\rangle_{\mathbb{F}_q}$ and $V' = \langle u'_0, \ldots, u'_{n-1}\rangle_{\mathbb{F}_q}$ and let $f \in \Omega_{m,n}$ with matrix M_f over $\mathbb{F}_q$ in the bases $\{u_0, \ldots, u_{m-1}\}$ and $\{u'_0, \ldots, u'_{n-1}\}$ of V and V'. Since $\{u_0, \ldots, u_{m-1}\}$ is a basis for $V(m, q^d)$ and $\{u'_0, \ldots, u'_{n-1}\}$ is a basis for $V(n, q^d)$, we can extend the action of f on $V \times V'$ to an action on $V(m, q^d) \times V(n, q^d)$ in the natural way. Let $f(s_0^{(k)}, s_j^{\prime(k)}) = a_j \in \mathbb{F}_{q^d}$, $j = 0, \ldots, e-1$. By Remarks 2.1 and 2.3, the matrix of the change of basis from $\{u_0, \ldots, u_{r-1}\}$ to $\{s_0^{(k)}, \ldots, s_0^{(k)}\}$ is $E_r^{-1}K_r$. Therefore, $\nu(f) = D_{\mathbf{a}}^{(k)} = (E_m^{-1}K_m)^t M_f (E_n^{-1}K_n)$, with $\mathbf{a} = (a_0, \ldots, a_{e-1})$. Since change of bases in $V(m, q^d) \times V(n, q^d)$ preserves the rank of bilinear forms, we have $\mathrm{rank}(f) = \mathrm{rank}(M_f) = \mathrm{rank}(D_{\mathbf{a}}^{(k)})$.

3 Puncturing generalized Gabidulin codes

Let $\mathcal{X}$ be a rank distance code in $M_{n,n}(\mathbb{F}_q)$ and A any given $m \times n$ matrix of rank m, $m < n$. It is clear that the set $A\mathcal{X} = \{AM : M \in \mathcal{X}\}$ is a rank distance code in $M_{m,n}(\mathbb{F}_q)$. We say that the code $A\mathcal{X}$, which we will denote by $\mathcal{P}_A(\mathcal{X})$, is obtained by *puncturing* $\mathcal{X}$ *with* A and $\mathcal{P}_A(\mathcal{X})$ is known as a *punctured code*.

Theorem 3.1 (Sylvester's rank inequality) [16, p. 66] *Let A be an $m \times n$ matrix and M an $n \times n'$ matrix. Then*

$$\mathrm{rank}(AM) \geq \mathrm{rank}(A) + \mathrm{rank}(M) - n.$$

Theorem 3.2 (see also [3, Corollary 35]) *Let $\mathcal{X}$ be an $(n, n, q; s)$-MRD code. Let A be any $m \times n$ matrix over $\mathbb{F}_q$ of rank m, with $n - s < m \leq n$. Then the punctured code $\mathcal{P}_A(\mathcal{X})$ is an $(m, n, q; s')$-MRD code, with $s' = s + m - n$.*

Proof We first show that the map $M \mapsto AM$ is injective. Assume $AM_1 = AM_2$ for some distinct matrices $M_1, M_2 \in \mathcal{X}$. Then $A(M_1 - M_2) = 0$, giving $\dim(\ker A) \geq \text{rank}\,(M_1 - M_2) \geq s > 0$, thus $\text{rank}\, A = m - \dim(\ker A) < m$, a contradiction. Therefore, $|A\mathcal{X}| = |\mathcal{X}| = q^{n(n-s+1)} = q^{n(m-s'+1)}$.

By the Sylvester's rank inequality, we have

$$\text{rank}(AM_1 - AM_2) \geq \text{rank}(A) + \text{rank}(M_1 - M_2) - n \geq m + s - n = s' > 0.$$

It follows that $A\mathcal{X}$ is an $(m, n, q; s')$-MRD code. □

Remark 3.3 Let B be matrix in $M_{m,n}(\mathbb{F}_q)$ of rank m. It is known that there exist $S \in \text{GL}(m, q)$ and $T \in \text{GL}(n, q)$ such that $B = SAT$ [16, p. 62]. Therefore

$$\mathcal{P}_B(\mathcal{X}) = \mathcal{P}_{SAT}(\mathcal{X}) = S\mathcal{P}_A(T\mathcal{X}),$$

giving $\mathcal{P}_B(\mathcal{X})$ is equivalent to the punctured code $\mathcal{P}_A(T\mathcal{X})$. Note that $T\mathcal{X}$ is equivalent to $\mathcal{X}$.

We recall the construction of the generalized Gabidulin codes as given in [13]. For any positive integers t, k with $t \leq n$ and $\gcd(k, n) = 1$, set $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$ to be the set of all q^k-polynomials over $\mathbb{F}_{q^n}$ of q^k-degree at most $t - 1$, i.e.,

$$\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n}) = \left\{ a_0 + a_1 x^{[k]} + \cdots + a_{t-1} x^{[k(t-1)]} : a_i \in \mathbb{F}_{q^n} \right\}.$$

We note that by reordering the powers of x in any $f \in \mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$ we actually find a q-polynomial. However, to study the generalized Gabidulin codes in terms of q^k-polynomials we need to keep the original order for the powers in f.

Let $g_0, \ldots, g_{m-1} \in \mathbb{F}_{q^n}$, $m \leq n$, be linearly independent over $\mathbb{F}_q$. Let $G^{[k]}$ be the matrix

$$G^{[k]} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{m-1} \\ g_0^{[k]} & g_1^{[k]} & \cdots & g_{m-1}^{[k]} \\ \cdots & \cdots & \cdots & \cdots \\ g_0^{[(t-1)k]} & g_1^{[(t-1)k]} & \cdots & g_{m-1}^{[(t-1)k]} \end{pmatrix}.$$

We consider the matrix $G^{[k]}$ as a generator matrix of a subset $\tilde{\mathcal{G}}_t^{(k)}$ of arrays over $\mathbb{F}_{q^n}$, i.e., $\tilde{\mathcal{G}}_t^{(k)} = \tilde{\mathcal{G}}_{(g_0,\ldots,g_{m-1});t}^{(k)} = \{(f(g_0), \ldots, f(g_{m-1})) : f \in \mathcal{L}_t^{[k]}(\mathbb{F}_{q^n})\}$.

Let $V' = \mathbb{F}_{q^n} = \langle u'_0, \ldots, u'_{n-1} \rangle_{\mathbb{F}_q}$. The map

$$\begin{array}{rccc} \varepsilon = \varepsilon_{\{u'_0,\ldots,u'_{n-1}\}} : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q^n \\ & \sum x_i u'_i & \mapsto & (x_0, \ldots, x_{n-1})^t \end{array}$$

maps the set $\tilde{\mathcal{G}}_t^{(k)}$ to the matrix set

$$\varepsilon\left(\tilde{\mathcal{G}}_t^{(k)}\right) = \left\{(M^{(0)}\, M^{(1)}\, \ldots\, M^{(m-1)}) : f \in \mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})\right\} \subseteq M_{n,m}(\mathbb{F}_q),$$

where $M^{(i)} = \varepsilon(f(g_i))$. Since the rank is invariant under matrix transposition and in this paper we consider matrix codes in $M_{m,n}(\mathbb{F}_q)$ with $m \leq n$, we may take the matrix code $\mathcal{G}_t^{(k)}$ obtained by taking the transpose of the elements in $\varepsilon(\tilde{\mathcal{G}}_t^{(k)})$. Therefore $\mathcal{G}_t^{(k)}$ is a $(m, n, q; m-t+1)$-MRD code. These MRD codes are called *generalized Gabidulin codes* [19].

By Proposition 2.2, we may identify the elements in $\mathrm{End}(V')$ with elements in $\mathcal{L}_n^{(k)}(\mathbb{F}_{q^n})$ via the map $D_{(a_0,\ldots,a_{n-1})} \mapsto a_0 + a_1 x^{[k]} + \cdots + a_{n-1}x^{[k(n-1)]}$. Therefore, $\mathcal{G}_t^{(k)}$ consists of the matrices of the restriction over the subspace $V = \langle g_0, \ldots, g_{m-1}\rangle_{\mathbb{F}_q}$ of $V' = \mathbb{F}_{q^n}$ of the endomorphisms (of V') in $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$. These matrices act on the set $\mathbb{F}_q^m$ of all row vectors as $v \mapsto vM$. As we are working in the framework of bilinear forms, we consider any matrix in $\mathcal{G}_t^{(k)}$ as a matrix of the restriction on $V \times V'$ of the bilinear form acting on $V' \times V'$ whose $n \times n$ matrix is the matrix in the basis $\{u'_0, \ldots, u'_{n-1}\}$ of an element in $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$. By Proposition 2.6 the elements in $\mathcal{G}_t^{(k)}$ can be represented by q^k-circulant matrices over $\mathbb{F}_{q^d}$, where $d = \gcd(m, n)$.

The following result seems to be known, but we include a proof for the sake of completeness.

Theorem 3.4 *Let $\mathcal{G}$ be any generalized Gabidulin $(n, n, q; n-t+1)$-code and let A be any given $m \times n$ matrix over $\mathbb{F}_q$ of rank m, with $t < m \leq n$. Then the punctured code $\mathcal{P}_A(\mathcal{G})$ is a generalized Gabidulin $(m, n, q; m-t+1)$-code. Conversely, every generalized Gabidulin $(m, n, q; m-t+1)$-code, with $1 \leq t \leq m$, is obtained by puncturing a generalized Gabidulin $(n, n, q; n-t+1)$-code.*

Proof Let $V' = \mathbb{F}_{q^n} = \langle u'_0, \ldots, u'_{n-1}\rangle_{\mathbb{F}_q}$. By the argument above, $\mathcal{G}$ is considered as the set of all bilinear forms acting on $V' \times V'$ whose matrix corresponds to a q^k-polynomial in $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n}) = \{a_0 + a_1 x^{[k]} + \cdots + a_{t-1}x^{[k(t-1)]} : a_i \in \mathbb{F}_{q^n}\}$.

The given matrix $A = (a_{ij})$ corresponds to the linear transformation

$$\tau : u'_i \mapsto \textstyle\sum_{j=0}^{n-1} a_{ij} u'_j, \quad i = 0, \ldots, m-1.$$

As $\mathrm{rank}\, A = m$, the subspace $V = \langle \tau(u'_0), \ldots, \tau(u'_{m-1})\rangle_{\mathbb{F}_q}$ is an m-dimensional subspace of V'. It follows that $\mathcal{P}_A(\mathcal{G})$ consists of the matrices of the bilinear forms on $V \times V'$ in the bases $\{g_i = \tau(u_i) : i = 0, \ldots, m-1\}$ and $\{u'_0, \ldots, u'_{n-1}\}$ of V and V', respectively. Therefore $\mathcal{P}_A(\mathcal{G})$ is the generalized Gabidulin code $\mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1}),t}$. By Theorem 3.2 $\mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1}),t}$ is an $(m, n, q; m-t+1)$-MRD code.

For the converse, let $\mathcal{G}_t^{(k)} = \mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1});t}$ be a generalized Gabidulin code. Set $V = \langle g_0, \ldots, g_{m-1}\rangle_{\mathbb{F}_q}$ and extend $g_0, \ldots, g_{m-1}$ with $g_m, \ldots, g_{n-1}$ to form a basis of $V' = \mathbb{F}_{q^n} = V(n, q)$. Then, elements in $\mathcal{G}_t^{(k)}$ are the restriction on $V \times V'$ of the bilinear forms acting on $V' \times V'$ whose matrix is the matrix of elements in $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$

in the basis $g_0, \ldots, g_{n-1}$. The set $\overline{\mathcal{G}}_t^{(k)} = \mathcal{G}^{(k)}_{(g_0,\ldots,g_{n-1});t}$ of such bilinear forms is a generalized Gabidulin $(n, n, q; n - t + 1)$-code. In addition, matrices in $\mathcal{G}_t^{(k)}$ are obtained from the matrices of $\overline{\mathcal{G}}_t^{(k)}$ by deleting the last $n - m$ rows, i.e., $\mathcal{G}_t^{(k)} = A\overline{\mathcal{G}}_t^{(k)}$ with $A = (I_m | O_{n-m})$. Therefore, the generalized Gabidulin code $\mathcal{G}_t^{(k)}$ is obtained by puncturing the generalized Gabidulin code $\overline{\mathcal{G}}_t^{(k)}$ with A. □

From the proof of the previous result, we get the following description for the generalized Gabidulin codes.

Corollary 3.5 *Let $g_0, \ldots, g_{m-1} \in \mathbb{F}_{q^n}$, $m \leq n$, be linearly independent over $\mathbb{F}_q$, $V = \langle g_0, \ldots, g_{m-1}\rangle_{\mathbb{F}_q}$ and $V' = \mathbb{F}_{q^n}$. Then the generalized Gabidulin code $\mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1});t}$ consists of the restriction on $V \times V'$ of the bilinear forms in $\mathcal{L}_t^{(k)}(\mathbb{F}_{q^n})$.*

Remark 3.6 Let $e = \gcd(m, n)$ and $d = \operatorname{lcm}(m, n)$. From the arguments contained in Sect. 2 there exists a (Singer) basis of $V = \langle g_0, \ldots, g_{m-1}\rangle_{\mathbb{F}_q}$ and a (Singer) basis of $V' = \mathbb{F}_{q^n}$ such that the elements in $\mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1});t}$ may be represented as $m \times n$ q^k-circulant matrices over $\mathbb{F}_{q^d}$.

Remark 3.7 By the isomorphism $\Omega_{m,n} \simeq \mathcal{D}^{(1)}_{m,n}(\mathbb{F}_{q^d})$ stated by Proposition 2.6, the Gabidulin code $\mathcal{G}^{(1)}_{(g_0,\ldots,g_{m-1}),t}$ is actually the Delsarte code defined by (6.1) in [9] with $V = \langle g_0, \ldots, g_{m-1}\rangle_{\mathbb{F}_q}$.

In the rest of the paper, m will be a divisor of n. We set $r = n/m$. Let $V = \langle u_0, \ldots, u_{m-1}\rangle_{\mathbb{F}_q}$ and $V' = \langle u'_0, \ldots, u'_{n-1}\rangle_{\mathbb{F}_q}$ be two vector spaces over $\mathbb{F}_q$ of dimension m and n, respectively. If $m = n$ we take $V' = V = \langle u_0, \ldots, u_{n-1}\rangle_{\mathbb{F}_q}$.

In the light of the isomorphism $\nu_{\{u_0,\ldots,u_{m-1};u'_0,\ldots,u'_{n-1}\}}$ described by (2), every bilinear form acting on $V \times V'$ may be identified with an $m \times n$ matrix over $\mathbb{F}_q$. In other words, if we assume V is an m-dimensional subspace of V' after a vector-space isomorphism, then the bilinear forms in $\Omega_{m,n}$ are the restrictions on $V \times V'$ of the bilinear form in $\Omega_{n,n}$. Thus, $\Omega_{m,n}$ is the puncturing of $\Omega_{n,n}$ by a suitable $m \times n$ matrix of rank m.

In this paper we work with cyclic models for vector spaces over $\mathbb{F}_q$. Let $\{s'_0, \ldots, s'_{n-1}\}$ be a Singer basis for V'. We note that not all m-dimensional subspaces of V' can be represented with a cyclic model over $\mathbb{F}_{q^m}$. Therefore, we need to choose suitable vectors $\{s_0, \ldots, s_{m-1}\}$ in V' such that the projection of the vectors in the cyclic model for V' on the $\mathbb{F}_q^m$-span of $\{s_0, \ldots, s_{m-1}\}$ is an m-dimensional subspace over $\mathbb{F}_q$ represented cyclically. This is what we do in the rest of this section.

Let σ' be a Singer cycle of V' with associated primitive element w'. Let $\{s'_0, \ldots, s'_{n-1}\}$ be the Singer basis for V' defined by σ'. Note that $s'_i \in V(n, q^n)$, for $i = 0 \ldots, n - 1$. Set $s_i = \sum_{j=0}^{r-1} s'_{i+jm}$ for $i = 0, 1, \ldots, m - 1$, $\sigma = \sigma'^{(q^n-1)/(q^m-1)}$ and $w = w'^{(q^n-1)/(q^m-1)}$. Then σ has order $q^m - 1$ and ω is a primitive element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is easily seen that s_i is an eigenvector for σ with eigenvalue w^{q^i}, for $i = 0, \ldots, m - 1$. Since m divides n, the $\mathbb{F}_{q^m}$-span $V(m, q^m)$ of $\{s_0, \ldots, s_{m-1}\}$ is contained in $V(n, q^n)$. Let ξ be the semilinear transformation on $V(m, q^m)$ whose linear part is defined by $\ell_\xi(s_i) = s_{i+1}$, where the indices are considered modulo m,

and whose companion automorphism is $\delta : x \in \mathbb{F}_{q^m} \mapsto x^q \in \mathbb{F}_{q^m}$. Since the subset $\{xs_0 + \cdots + x^{q^{m-1}} s_{m-1} : x \in \mathbb{F}_{q^m}\}$ of $V(m, q^m)$ is fixed pointwise by ξ, it is a cyclic model for an m-dimensional vector space V over $\mathbb{F}_q$. By Proposition 2.6, every bilinear form on $V \times V'$ can be represented by $m \times n$ q-circulant matrices over $\mathbb{F}_{q^n}$.

Lemma 3.8 *Let k be a positive integer such that $\gcd(k, n) = 1$. Then $s_i^{(k)} = \sum_{j=0}^{r-1} s'^{(k)}_{i+jm}$, for $i = 0, 1, \ldots, m-1$.*

Proof For $i = 0, 1, \ldots, m-1$ we have $s_i^{(k)} = s_{ki \bmod m} = \sum_{j=0}^{r-1} s'_{(ki \bmod m)+jm}$. On the other hand, $s'^{(k)}_{i+jm} = s_{k(i+jm) \bmod n}$. Therefore we need to prove

$$\{(ki \bmod m) + jm : j = 0, \ldots, r-1\} = \{k(i + lm) \bmod n : l = 0, \ldots, r-1\}.$$

Let $ki = tm + s$ with $0 \le s \le m-1$. For each $j \in \{0, 1, \ldots, r-1\}$ we need to find $l \in \{0, 1, \ldots, r-1\}$ such that $s + jm \equiv (tm + s + klm) \bmod n$. This is equivalent to

$$j \equiv (t + kl) \bmod r, \tag{9}$$

as $r = n/m$. Since $\gcd(k, n) = 1$, we also have $\gcd(k, r) = 1$. Let k^{-1} denote the inverse of k modulo r. With $l = k^{-1}(j - t) \bmod r$ Eq. (9) is satisfied and

$$\{k^{-1}(j - t) \bmod r : j \in \{0, 1, \ldots, r-1\}\} = \{0, 1, \ldots, r-1\}.$$

Hence the assertion is proved. □

The above lemma implies the following result.

Proposition 3.9 *Let k be a positive integer such that $\gcd(k, n) = 1$ and m a divisor of n. Let $\{s'_0, \ldots, s'_{n-1}\}$ be a Singer basis for V'. Set $s_i^{(k)} = \sum_{j=0}^{r-1} s'^{(k)}_{i+jm}$, for $i = 0, 1, \ldots, m-1$. Then the $\mathbb{F}_q$-subspace $\left\{\sum_{i=0}^{m-1} x^{[ki]} s_i^{(k)} : x \in \mathbb{F}_{q^m}\right\}$ of $V(n, q^n)$ is a kth cyclic model for V.*

Proof By Remark 2.3 the kth cyclic model for V is obtained from the cyclic model $V = \{\sum_{i=0}^{m-1} x^{q^i} s_i : x \in \mathbb{F}_{q^m}\}$ by applying the change of basis, say κ, from $\{s_0, \ldots, s_{m-1}\}$ with $s_i = \sum_{j=0}^{r-1} s'_{i+jm}$ for $i = 0, 1, \ldots, m-1$, to $\{s_0^{(k)}, \ldots, s_{m-1}^{(k)}\}$. We recall that κ is represented by the permutation matrix K_m^{-1}. By Lemma 3.8, $s_i^{(k)} = \sum_{j=0}^{r-1} s'^{(k)}_{i+jm}$, for $i = 0, 1, \ldots, m-1$. This implies that the image under κ of the cyclic model $\{\sum_{i=0}^{m-1} x^{q^i} s_i : x \in \mathbb{F}_{q^m}\}$ is $\left\{\sum_{i=0}^{m-1} x^{[ki]} s_i^{(k)} : x \in \mathbb{F}_{q^m}\right\}$. □

Let f be any given bilinear form acting on the kth cyclic model of V' with q^k-circulant matrix $D_{\mathbf{a}}^{(k)}$ in the basis $\{s_0'^{(k)}, \ldots, s_{n-1}'^{(k)}\}$. As the matrix of the coordinates of the vectors $s_0^{(k)}, \ldots, s_{m-1}^{(k)}$ in this basis is the $1 \times r$ block matrix $A = (I_m \mid I_m \mid \ldots \mid I_m)$, the restriction $f|_{V \times V'}$ of f on $V \times V'$ has matrix $\overline{D} = AD_{\mathbf{a}}^{(k)}$ in the bases $\{s_0^{(k)}, \ldots, s_{m-1}^{(k)}\}$ and $\{s_0'^{(k)}, \ldots, s_{n-1}'^{(k)}\}$.

To make notation easier, we index the rows and columns of an $m \times n$ matrix M by elements in $\{0, \ldots, m-1\}$ and $\{0, \ldots, n-1\}$. Further, $M_{(i)}$ and $M^{(j)}$ will denote the ith row and jth column of M, respectively.

For $i = 0, \ldots, m-1$, we have $A_{(i)} = (0, \ldots, 0, 1, 0, \ldots, 0, 1, 0 \ldots, 0, 1, 0 \ldots)$, with 1 at position $i + km$, for $k = 0, \ldots, r-1$, and 0 elsewhere. Let $D_{\mathbf{a}}^{(k)}$ be generated by the array $\mathbf{a} = (a_0, \ldots, a_{n-1})$. Then, $[D_{\mathbf{a}}^{(k)}]^{(j)} = (a_j, a_{j-1}^{[k]}, \ldots, a_{j+1}^{[k(n-1)]})^t$, for $j = 0, \ldots, n-1$. Therefore, the (i, j)-entry of $\overline{D}$ is

$$a_{j-i}^{[ki]} + a_{j-(i+m)}^{[k(i+m)]} + \cdots + a_{j-(i+(r-1)m)}^{[k(i+(r-1)m)]} = \sum_{h=0}^{r-1} a_{j-(i+hm)}^{[k(i+hm)]},$$

where indices are taken modulo n. It turns out that $\overline{D}$ is the $m \times n$ q^k-circulant matrix over $\mathbb{F}_{q^n}$ generated by the array $(\sum_{h=0}^{r-1} a_{-hm}^{[khm]}, \sum_{h=0}^{r-1} a_{1-hm}^{[khm]}, \ldots, \sum_{h=0}^{r-1} a_{m-1-hm}^{[khm]})$. In particular, if $\mathbf{a} = (a_0, \ldots, a_{t-1}, 0, \ldots, 0)$ for some $t \in \{1, \ldots, m\}$, then $\overline{D}$ is generated by the m-array $(a_0, \ldots, a_{t-1}, 0, \ldots, 0)$ giving $\overline{D}$ to be the matrix of a bilinear form in the rank distance code

$$\Phi_{m,n,t}^{(k)} = \bigoplus_{j=0}^{t-1} \Omega_j^{(k)}, \tag{10}$$

where the $\mathbb{F}_q$-subspaces $\Omega_j^{(k)}$ are given in (7). Note that the dimension of $\Phi_{m,n,t}$ over $\mathbb{F}_q$ is nt. The above arguments together with Theorem 3.4 prove the following result.

Theorem 3.10 *Let $m > 1$ be any divisor of n. For any $t \in \{1, \ldots, m\}$, the subset $\Phi_{m,n,t}^{(k)}$ of $\Omega_{m,n}$ is a generalized Gabidulin $(m, n, q; m - t + 1)$-code.*

We now describe the generalized twisted Gabidulin codes as provided by Sheekey in the recent paper [29] by using the framework of q^k-polynomials over $\mathbb{F}_{q^n}$. In [24] the equivalence between different generalized twisted Gabidulin codes was addressed.

Let $\mathrm{N}_{q^n/q}$ denote the norm map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$:

$$\mathrm{N}_{q^n/q} \colon y \in \mathbb{F}_{q^n} \mapsto \mathrm{N}_{q^n/q}(y) = \prod_{j=0}^{n-1} y^{q^j} \in \mathbb{F}_q.$$

Theorem 3.11 [24,29] *For any $t \in \{1, \ldots, n-1\}$ and $\mu \in \mathbb{F}_{q^n}^{\times}$ with $\mathrm{N}_{q^n/q}(\mu) \neq (-1)^{nt}$, define the subset*

$$\Gamma_{n,n,t,\mu,s}^{(k)} = \left\{ f_{a,0}^{(k)} + f_{\mu a^{q^{sk}},t}^{(k)} : a \in \mathbb{F}_{q^n} \right\}$$

of $\Omega_{n,n}$ and put

$$\mathcal{H}_{n,n,t,\mu,s}^{(k)} = \Gamma_{n,n,t,\mu,s}^{(k)} \oplus \Omega_1^{(k)} \oplus \cdots \oplus \Omega_{t-1}^{(k)}.$$

Then $\mathcal{H}^{(k)}_{n,n,t,\mu,s}$ is an $(n,n,q;n-t+1)$-MRD code which is not equivalent to $\Phi^{(k)}_{n,n,t}$ if $t \neq 1, n-1$.

Let A be the $1 \times r$ block matrix $(I_m \mid I_m \mid \ldots \mid I_m)$. By Theorem 3.2, for any $t \in \{1,\ldots,m-1\}$, the punctured code $\mathcal{P}_A(\mathcal{H}^{(k)}_{n,n,t,\mu,s})$ is an MRD code with the same parameters as the code $\Phi^{(k)}_{m,n,t}$ defined by (10). We denote such $(m,n,q;m-t+1)$-MRD code by $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$. By using the decomposition (8) of $\Omega^{(k)}_{m,n}$ with $e=m$, we get

$$\mathcal{H}^{(k)}_{m,n,t,\mu,s} = \Gamma^{(k)}_{m,n,t,\mu,s} \oplus \Omega^{(k)}_1 \oplus \cdots \oplus \Omega^{(k)}_{t-1} \tag{11}$$

where $\Gamma^{(k)}_{m,n,t,\mu,s} = \{f^{(k)}_{a,0} + f^{(k)}_{\mu a^{q^{sk}},t} : a \in \mathbb{F}_{q^n}\}$ and $f^{(k)}_{a,j} \in \Omega^{(k)}_j$ is defined by (6). It turns out that $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is a linear MRD code of dimension nt.

Remark 3.12 It is easy to see that the MRD code $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ has the same parameters as the $(m, rm/2, q; m-1)$-MRD codes provided in [7] only for $t=2$ and $n=m$.

4 The automorphism group of some punctured generalized Gabidulin codes

Very recently, Liebhold and Nebe calculated the group of all linear automorphisms of any generalized Gabidulin code. Here we give the finite fields version of Theorem 4.9 in [22].

Theorem 4.1 [22] *Let $\mathcal{G}^{(k)}_t = \mathcal{G}^{(k)}_{(g_0,\ldots,g_{m-1}),t}$ be a generalized Gabidulin code. Let $\mathbb{F}_q \leq \mathbb{F}_{q^{m'}} \leq \mathbb{F}_{q^n}$ be the maximal subfield of $\mathbb{F}_{q^n}$ such that $\langle g_0,\ldots,g_{m-1}\rangle_{\mathbb{F}_q}$ is an $\mathbb{F}_{q^{m'}}$-subspace. Let $\mathbb{F}_{q^d}$ be the minimal subfield of $\mathbb{F}_{q^n}$ such that $\langle g_0,\ldots,g_{m-1}\rangle_{\mathbb{F}_q}$ is contained in a one-dimensional $\mathbb{F}_{q^d}$-subspace. Then there is a subgroup G of* $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ *such that the group of all linear automorphisms of $\mathcal{G}^{(k)}_t$ is isomorphic to*

$$\left(\mathbb{F}^{\times}_{q^{m'}} \times \mathrm{GL}(n/d, q^d)\right) \rtimes G.$$

Remark 4.2 The generalized Gabidulin code $\Phi^{(k)}_{m,n,t}$ defined by (10) corresponds to the case $\langle g_0,\ldots,g_{m-1}\rangle_{\mathbb{F}_q} = \mathbb{F}_{q^m}$ in the previous theorem.

In spite of Theorem 4.1, we believe that it is useful to have an explicit description of the full automorphism group of an MRD code to compare MRD codes among each other; see [29,33].

Let $S' = \langle \sigma' \rangle$ be a Singer cyclic group of $\mathrm{GL}(V')$ with associated semilinear transformation ξ' as described in Sect. 2. In the Singer basis $\{s'^{(k)}_0,\ldots,s'^{(k)}_{n-1}\}$, the matrix of σ' is the diagonal matrix $\mathrm{diag}(w, w^{[k]},\ldots,w^{[k(n-1)]})$. Therefore, (σ'^i, σ'^j) acts on $\Omega_{n,n}$ by mapping the bilinear form with q^k-circulant matrix $D^{(k)}_{(a_0,\ldots,a_{n-1})}$ to the bilinear form with matrix $D^{(k)}_{(w^i a_0 w^j,\ldots,w^i a_{n-1} w^{j[k(n-1)]})}$. The matrix of the linear part $\ell_{\xi'}$ of ξ' is the permutation matrix $D^{(k)}_{(0,\ldots,0,1)}$. Then $(\ell_{\xi'}, \ell_{\xi'})$ acts on $\Omega_{n,n}$ by

mapping the bilinear form with q^k-circulant $D^{(k)}_{(a_0,\ldots,a_{n-1})}$ to the bilinear form with matrix $D^{(k)}_{(a_0^{[k]},\ldots,a_{n-1}^{[k]})}$. Set $\bar{\ell} = (\ell_{\xi'}, \ell_{\xi'})$ and $\bar{C}$ be the cyclic subgroup of $\mathrm{Aut}(\Omega_{n,n})$ generated by $\bar{\ell}$. It turns out that any element in $(S' \times S') \rtimes \bar{C} \rtimes \mathrm{Aut}(\mathbb{F}_q)$ fixes every component $\Omega_j^{(k)}$ of $\Omega_{n,n}$.

In the paper [29], Sheekey gave a complete description of the automorphism group of the MRD codes $\Phi^{(k)}_{n,n,t}$ and $\mathcal{H}^{(k)}_{n,n,t,\mu,s}$, for any $t \in \{1,\ldots,n-2\}$.

Theorem 4.3 [29] *Let $q = p^h$, p a prime.*

(i) For any given $t \in \{1,\ldots,n-2\}$, the automorphism group of $\Phi^{(k)}_{n,n,t}$ is the semidirect product $(S' \times S') \rtimes \bar{C} \rtimes \mathrm{Aut}(\mathbb{F}_q)$.

(ii) For any given $t \in \{1,\ldots,n-2\}$, the automorphism group of $\mathcal{H}^{(k)}_{n,n,t,\mu,s}$ is the subgroup of $(S' \times S') \rtimes \bar{C} \rtimes \mathrm{Aut}(\mathbb{F}_q)$ whose elements correspond to the triples $((D_{\mathbf{a}}, D_{\mathbf{b}}); \bar{\ell}^i; p^e)$, with $\mathbf{a} = (a, 0, \ldots, 0)$, $\mathbf{b} = (b, 0, \ldots, 0)$ and $a^{q^s-1}b^{q^s-q^t} = \mu^{p^e q^i - 1}$.

We now give more information on the automorphism group of the MRD code $\mathcal{H}^{(k)}_{n,n,t,\mu,s}$.

Corollary 4.4 $|\mathrm{Aut}(\mathcal{H}^{(k)}_{n,n,t,\mu,s})| = l(q^n-1)(q^{gcd(n,s,t)}-1)$, *for some divisor l of nh. If $\mathbb{F}_{p^d}$ is the smallest subfield of $\mathbb{F}_{q^n}$ which contains μ, then $\frac{nh}{d} \mid l$. In particular, if $\mu \in \mathbb{F}_p^\times$ then $l = nh$.*

Proof Let $G_{n,k} = \{x^{q^k-1} : x \in \mathbb{F}_{q^n}^\times\}$. Note that $G_{n,k}$ is a subgroup of the multiplicative group $\mathbb{F}_{q^n}^\times$. To calculate $|G_{n,k}|$ it is enough to observe that $x^{q^k-1} = y^{q^k-1}$ for some $x, y \in \mathbb{F}_{q^n}^\times$ if and only if $x/y \in \mathbb{F}_{q^k}^\times$, and hence $x/y \in \mathbb{F}_{q^{\gcd(n,k)}}^\times$. It follows that $|G_{n,k}| = \frac{q^n-1}{q^{\gcd(n,k)}-1}$. Also, the size of the subgroup $G_{n,k} \cap G_{n,j}$ is

$$c_{n,k,j} = \gcd\left(\frac{q^n-1}{q^{\gcd(n,k)}-1}, \frac{q^n-1}{q^{\gcd(n,j)}-1}\right).$$

Note that for each $c \in \mathbb{F}_{q^n}^\times$ we have $|G_{n,k} \cap cG_{n,j}| \in \{0, c_{n,k,j}\}$.

Let $d_{n,k,j}$ denote the number of pairs $(x, y) \in \mathbb{F}_{q^n}^\times \times \mathbb{F}_{q^n}^\times$ such that

$$x^{q^k-1}y^{q^j-1} = 1.$$

If $x^{q^k-1}y^{q^j-1} = 1$, then $x^{q^k-1} = (1/y)^{q^j-1}$ and hence $x^{q^k-1} \in G_{n,k} \cap G_{n,j}$. It follows that we can choose $x_0 = x^{q^k-1}$ in $c_{n,k,j}$ different ways, and it uniquely defines $y_0 = y^{q^j-1}$. We have

$$\left|\left\{x : x^{q^k-1} = x_0\right\}\right| = \left|\left\{x : x^{q^k-1} = 1\right\}\right| = q^{\gcd(n,k)} - 1$$

and

$$\left|\left\{y\colon y^{q^j-1}=y_0\right\}\right|=\left|\left\{y\colon y^{q^j-1}=1\right\}\right|=q^{\gcd(n,j)}-1,$$

thus

$$d_{n,k,j}=(q^n-1)(q^{\gcd(n,k,j)}-1).$$

If $x^{q^k-1}y^{q^j-1}=c$, then $x^{q^k-1}=c(1/y)^{q^j-1}$, thus $x^{q^k-1}\in G_{n,k}\cap cG_{n,j}$. By the above arguments, we get that for each $c\in\mathbb{F}_{q^n}^{\times}$, the number of pairs $(x,y)\in\mathbb{F}_{q^n}^{\times}\times\mathbb{F}_{q^n}^{\times}$ such that $x^{q^k-1}y^{q^j-1}=c$ is either 0, or $d_{n,k,j}$.

Now, let μ be a given element in $\mathbb{F}_{q^n}^{\times}$, $q=p^h$ and let $\mathcal{H}$ denote the set of integers r, such that

$$x^{q^k-1}y^{q^j-1}=\mu^{p^r-1}$$

has a solution in $\mathbb{F}_{q^n}^{\times}\times\mathbb{F}_{q^n}^{\times}$. By the above arguments, we have $0\in\mathcal{H}$. If $x_0^{q^k-1}y_0^{q^j-1}=\mu^{p^r-1}$ and $x_1^{q^k-1}y_1^{q^j-1}=\mu^{p^s-1}$, then

$$\left(x_0^{p^s}\right)^{q^k-1}\left(y_0^{p^s}\right)^{q^j-1}=\mu^{p^{r+s}-p^s}$$

and

$$\left(x_0^{p^s}x_1\right)^{q^k-1}\left(y_0^{p^s}y_1\right)^{q^j-1}=\mu^{p^{r+s}-1},$$

thus $r,s\in\mathcal{H}$ yields $r+s\in\mathcal{H}$ giving $\mathcal{H}$ is an additive subgroup in $\mathbb{Z}_{nh}$. Therefore, $l=|\mathcal{H}|$ divides nh.

By the above arguments, the number of triples $(a,b,i)\in\mathbb{F}_{q^n}^{\times}\times\mathbb{F}_{q^n}^{\times}\times\mathbb{Z}_{nh}$ such that $a^{q^s-1}b^{q^s-q^t}=\mu^{p^i-1}$ is $l(q^n-1)(q^{gcd(n,s,t)}-1)$, for some divisor l of nh. If $\mathbb{F}_{p^d}$ is the smallest subfield of $\mathbb{F}_{q^n}$ which contains μ, then $\mathcal{H}$ contains the additive subgroup of $\mathbb{Z}_{nh}$ generated by d, giving $\frac{nh}{d}\mid l$.

If $\mu\in\mathbb{F}_p^{\times}$, then $\mu^{p^i-1}=1$ for all $i\in\mathbb{Z}_{nh}$. □

Let $m>1$ be any divisor of n and k any positive integer such that $\gcd(k,n)=1$. Let $S=\langle\sigma\rangle$ and $S'=\langle\sigma'\rangle$ be Singer cyclic groups of $\mathrm{GL}(V)$ and $\mathrm{GL}(V')$, respectively, and $\{s_0,\ldots,s_{m-1}\}$ and $\{s'_0,\ldots,s'_{n-1}\}$ the Singer bases defined by σ and σ'.

Set $\ell=(\ell_\xi,\ell_{\xi'})$ and let C be the cyclic subgroup of $\mathrm{Aut}(\Omega_{m,n})$ generated by ℓ. Then $C\simeq\mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Remark 4.5 To make notation easier, in all the arguments used in the actual and in the next section we assume $k=1$. We put $\Omega_j=\Omega_j^{(1)}$ and $\Phi_{m,n,t-1}=\Phi_{m,n,t-1}^{(1)}$. By Lemma 3.8, the same arguments work perfectly well for any k with $\gcd(k,n)=1$ if the cyclic model of vector spaces and q-circulant matrices involved are replaced by the kth cyclic model and q^k-circulant matrices. The details are left to the reader.

Both the Singer cyclic groups $S = \langle\sigma\rangle$ and $S' = \langle\sigma'\rangle$, as well as the cyclic group C, fix every component Ω_j of $\Omega_{m,n}$ giving that every element in $(S \times S') \rtimes C$ is an automorphism of $\Phi_{m,n,t}$, for any $t \in \{1, \ldots, m\}$.

Theorem 4.6 *Let $\overline{T}'$ be the subset of* $\mathrm{End}(V')$ *whose elements correspond to q-circulant matrices defined by an array of type*

$$(c_0, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, c_1, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, c_{r-1}, \underbrace{0, \ldots, 0}_{m-1 \text{ times}})$$

over $\mathbb{F}_{q^n}$, and set $T' = \overline{T}' \cap \mathrm{GL}(V')$. Then, for any given $t \in \{1, \ldots, m-1\}$, the automorphism group of $\Phi_{m,n,t}$ is the semidirect product $(S \times T') \rtimes C \rtimes \mathrm{Aut}(\mathbb{F}_q)$.

Proof Straightforward calculations show that the given group is a subgroup of $\mathrm{Aut}(\Phi_{m,n,t})$.

Let $\varphi = (A, B; \theta) \in \mathrm{Aut}(\Phi_{m,n,t})$, with $A \in \mathrm{GL}(V)$, $B \in \mathrm{GL}(V')$ and $\theta \in \mathrm{Aut}(\mathbb{F}_q)$. As $\Phi_{m,n,t}$ is fixed by the semilinear automorphism ϕ defined by the Frobenius map $x \mapsto x^p$, we may assume $\theta = \mathbf{1}$. We identify the elements A and B with their Dickson matrices in $\mathcal{B}_m(\mathbb{F}_{q^m})$ and $\mathcal{B}_n(\mathbb{F}_{q^n})$, respectively. To suit our present needs, we set $A^t = D_{(a_0,a_1,\ldots,a_{m-1})}$ and $B = D^t_{(b_0,b_1,\ldots,b_{n-1})}$.

Let f be any given element in $\Phi_{m,n,t}$ with q-circulant matrix $D_{\mathbf{a}}$. Then, the Dickson matrix of f^φ is defined by the m-tuple formed by the first m entries of $(A^t D_{\mathbf{a}} B)_{(0)}$.

The lth entry, with $0 \le l \le m-1$, in $(A^t D_{\mathbf{a}} B)_{(0)}$ is given by the inner product $(A^t D_{\mathbf{a}})_{(0)} \cdot B^{(l)}$, with $B^{(l)} = (b_{-l}^{q^l}, b_{-l+1}^{q^l}, \ldots, b_{-l+n-1}^{q^l})$ where subscripts are taken modulo n.

We recall that $M^{(i)}$ and $M_{(j)}$ denotes the ith column and the jth row of M, respectively.

Let $f = f_{\alpha,j}$ with $\alpha \in \mathbb{F}_{q^n}$ and $0 \le j \le m-1$. Then $D_{\mathbf{a}}$ has only n nonzero entries, one in each column. More precisely, the nonzero entry of the hth column of $D_{\mathbf{a}}$ is $\alpha^{q^{h-j}}$ at position $(h-j) \bmod m$. It follows that the hth entry of

$$(A^t D_{\mathbf{a}})_{(0)} = \left(A^t_{(0)} D^{(0)}_{\mathbf{a}}, A^t_{(0)} D^{(1)}_{\mathbf{a}}, \ldots, A^t_{(0)} D^{(n-1)}_{\mathbf{a}}\right)$$

is $a_{h-j}\alpha^{q^{h-j}}$, where the subscript $h-j$ is taken modulo m. Hence, the lth entry of $(A^t D_{\mathbf{a}} B)_{(0)}$ is

$$\sum_{h=0}^{n-1} a_{h-j}\alpha^{q^{h-j}} b_{h-l}^{q^l} = \sum_{h=0}^{m-1} a_{h-j} \sum_{k=0}^{r-1} \alpha^{q^{h-j+km}} b_{h-l+km}^{q^l}. \tag{12}$$

Since we are assuming that φ fixes $\Phi_{m,n,t} = \bigoplus_{j=0}^{t-1} \Omega_j$, we must have (by putting $h - j = i$)

$$\sum_{i=0}^{m-1} a_i \sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j-l+km}^{q^l} = 0 \tag{13}$$

for $0 \le j \le t-1$, $t \le l \le m-1$.

Since Eq. (13) holds for all $\alpha \in \mathbb{F}_{q^n}$, we get

$$a_i b_{i+j-l} = a_i b_{i+j-l+m} = \cdots = a_i b_{i+j-l+(r-1)m} = 0,$$

for $0 \le i \le m-1$ and $t \le l \le m-1$.

As $A \in \mathcal{B}_m(\mathbb{F}_{q^m})$, $(a_0, a_1, \ldots, a_{m-1}) \neq (0, \ldots, 0)$. By applying a suitable element in the cyclic subgroup C of $\mathrm{Aut}(\Omega_{m,n})$ generated by ℓ, we may assume $a_0 \neq 0$. Therefore, we get

$$b_{j-l} = b_{j-l+m} = \cdots = b_{j-l+(r-1)m} = 0,$$

for $0 \le j \le t-1$ and $t \le l \le m-1$. By considering subscripts modulo n, we see that the possible nonzero entries in $(b_0, \ldots, b_{n-1})$ are those in position km, with $0 \le k \le r-1$, with at least one of them nonzero.

In $B^{(l)}$, the only nonzero entries are $b_{km}^{q^l}$ in $(l+km)$th positions, for $0 \le k \le r-1$. Then the expression (12) for the lth entry in $(A^t D_{\mathbf{a}} B)_{(0)}$, reduces to $a_{l-j} \sum_{k=0}^{r-1} \alpha^{q^{l-j+km}} b_{km}^{q^l}$, which must be zero for $0 \le j \le t-1$, $t \le l \le m-1$ and all $\alpha \in \mathbb{F}_{q^n}$. In addition, $1 \le l-j \le m-1$ gives $(a_0, a_1, \ldots, a_{m-1}) = (a_0, 0, \ldots, 0)$, $a_0 \neq 0$, and therefore $\mathrm{Aut}(\Phi_{m,n,t})$ has the prescribed form. □

Remark 4.7 Statement (i) in Theorem 4.3 is obtained by taking $m = n$ in the previous Theorem.

Remark 4.8 By Remark 4.5, Theorem 4.6 provides also the description of the automorphism group of the generalized Gabidulin code $\Phi_{m,n,t}^{(k)}$. We notice that the codes $\Phi_{m,n,t}^{(k)}$ are defined in different cyclic models for $\Omega_{m,n}$, for different values of k.

Proposition 4.9 *Let $\overline{T}'$ be defined as in Theorem 4.6. Then $\overline{T}' \simeq \mathrm{End}(V(n/m, q^m))$ and $T' = \overline{T}' \cap \mathrm{GL}(V') \simeq \mathrm{GL}(n/m, q^m)$.*

Proof Set $r = n/m$. By Proposition 2.2 we have $\mathrm{End}(V(r, q^m)) \cong \mathcal{D}_r(\mathbb{F}_{q^n})$, where $\mathcal{D}_r(\mathbb{F}_{q^n})$ is the Dickson matrix algebra of all the q^m-circulant $r \times r$ matrices acting on the cyclic model $W = \{(x, x^{q^m}, \ldots, x^{q^{n-m}}) : x \in \mathbb{F}_{q^n}\}$ for $V(r, q^m)$. Both W and $V' = \{(x, x^q, \ldots, x^{q^{n-1}}) : x \in \mathbb{F}_{q^n}\}$ are n-dimensional vector spaces over $\mathbb{F}_q$ and the map

$$\begin{array}{rccc} \tau : & W & \longrightarrow & V' \\ & (x, x^{q^m}, \ldots, x^{q^{n-m}}) & \mapsto & (x, x^q, \ldots, x^{q^{n-1}}) \end{array}$$

is an isomorphism of vector spaces.

A straightforward computation shows that τ induces the group isomorphism

$$\begin{array}{rccc} \bar{\tau} : & \mathcal{D}_r(\mathbb{F}_{q^n}) & \longrightarrow & T' \\ & D_{(c_0, c_1, \ldots, c_{r-1})} & \mapsto & D_{(c_0, 0, \ldots 0, c_1, 0, \ldots, 0, c_{r-1}, 0, \ldots, 0)} \end{array}.$$

This is enough to get the result. □

Corollary 4.10 *For any given* $t \in \{1, \ldots, m-1\}$,

$$\mathrm{Aut}\left(\Phi_{m,n,t}\right) \simeq \left(\mathbb{F}_{q^m}^{\times} \times \mathrm{GL}(n/m, q^m)\right) \rtimes \mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q) \rtimes \mathrm{Aut}(\mathbb{F}_q).$$

Proof Since the Singer cyclic group S of $\mathrm{GL}(V)$ is isomorphic to the multiplicative group $\mathbb{F}_{q^m}^{\times}$ and the cyclic group C generated by ℓ is isomorphic to $\mathrm{Aut}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, the result follows from Theorem 4.6 and Proposition 4.9. □

5 The automorphism group of some punctured generalized twisted Gabidulin code

The following result gives information on the geometry of the punctured code $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$, and it will be used to calculate the automorphism group of this MRD code. We apply arguments similar to those used by Shekeey [29]. As we did in the previous section, we consider only the case $k = 1$ to make notation easier. The arguments below work perfectly well in the general case. We put $\Omega_j = \Omega^{(1)}_j$, $\Phi_{m,n,t-1} = \Phi^{(1)}_{m,n,t-1}$ and $\mathcal{H}_{m,n,t,\mu,s} = \mathcal{H}^{(1)}_{m,n,t,\mu,s}$.

Theorem 5.1 *Let* $m > 1$ *be any divisor of* n *and* $\mu \in \mathbb{F}_{q^n}^{\times}$ *such that* $\mathrm{N}_{q^n/q}(\mu) \neq (-1)^{nt}$. *For any given* $t \in \{1, \ldots, m-2\}$ *and* $s \not\equiv 0, \pm 1, \pm 2 \pmod m$, $\bigoplus_{j=1}^{t-1} \Omega_j$ *is the unique subspace of* $\mathcal{H}_{m,n,t,\mu,s}$ *which is equivalent to* $\Phi_{m,n,t-1}$.

Proof Let $\varphi = (A, B; \theta) \in \mathrm{Aut}(\Omega_{m,n})$ such that $\Phi^{\varphi}_{m,n,t-1}$ is contained in $\mathcal{H}_{m,n,t,\mu,s}$. Here, $\theta = \phi^e$. As every component Ω_j is fixed by the semilinear automorphism ϕ, we may assume $\theta = \mathbf{1}$. We identify the elements A and B with their Dickson matrices in $\mathcal{B}_m(\mathbb{F}_{q^m})$ and $\mathcal{B}_n(\mathbb{F}_{q^n})$, respectively. To suit our present needs, we set $A^t = D_{(a_0,a_1,\ldots,a_{m-1})}$ and $B = D^t_{(b_0,b_1,\ldots,b_{n-1})}$.

Let $f = f_{\alpha,j}$ with $\alpha \in \mathbb{F}_{q^n}$ and $0 \leq j \leq t-2$. Let $D_{\mathbf{a}}$ be the Dickson matrix of f in the Singer bases $s_0, \ldots, s_{m-1}$ and $s'_0, \ldots, s'_{n-1}$. Set $r = n/m$. By arguing as in the proof of Theorem 4.6, we get that the lth entry in $(A^t D_{\mathbf{a}} B)_{(0)}$ is given by

$$\sum_{h=0}^{m-1} a_{h-j} \sum_{k=0}^{r-1} \alpha^{q^{h-j+km}} b^{q^l}_{h-l+km}, \tag{14}$$

where the indices of the entries of A and B are taken modulo m and n, respectively. Since we are assuming that $\Phi^{\varphi}_{m,n,t-1}$ is contained in $\mathcal{H}_{m,n,t,\mu,s}$, we must have (after substituting $h-j$ with i)

$$\sum_{i=0}^{m-1} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b^{q^l}_{i+j-l+km} \right) = 0,$$

for $0 \leq j \leq t-2$, $t+1 \leq l \leq m-1$ and all $\alpha \in \mathbb{F}_{q^n}$. Therefore,

$$a_i b_{i+j-l+km} = 0, \quad \text{for } 0 \leq i \leq m-1.$$

As $B \in \mathcal{B}_n(\mathbb{F}_{q^n})$, some of the b_i's are nonzero. On the other hand, the cyclic group $C = \langle \ell \rangle$ fixes every component Ω_j. Hence, we can assume $b_0 \neq 0$ and get $a_{l-j} = 0$, for $0 \leq j \leq t-2$ and $t+1 \leq l \leq m-1$, i.e.,

$$a_l = a_{l-1} = \cdots = a_{l-t+2} = 0$$

for $t+1 \leq l \leq m-1$, giving $(a_0, \ldots, a_{m-1}) = (a_0, a_1, a_2, 0 \ldots, 0)$. Whenever $a_i \neq 0$, we get

$$b_{i+j-l+km} = 0,$$

for $0 \leq j \leq t-2$, $0 \leq k \leq r-1$, i.e.,

$$b_{i+km+1} = \cdots = b_{i+(k+1)m-3} = 0 \tag{15}$$

for $i = 0, 1, 2$ and $0 \leq k \leq r-1$ since $j-l$ can take all integers from $\{1-m, 2-m, \ldots, -4, -3\}$. We now compare the 0th and tth entries of $(A^t D_{\mathbf{a}} B)_{(0)}$. From (14) we can see that the 0th entry of $(A D_{\mathbf{a}} B^t)_{(0)}$ is

$$\sum_{i=0,1,2} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j+km} \right)$$

and the tth entry is

$$\sum_{i=0,1,2} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j-t+km}^{q^t} \right).$$

Since we are assuming that $\Phi^{\varphi}_{m,n,t-1}$ is contained in $\mathcal{H}_{m,n,t,\mu,s}$, we must have

$$\mu \left[\sum_{i=0,1,2} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j+km} \right) \right]^{q^s} = \sum_{i=0,1,2} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j-t+km}^{q^t} \right),$$

for all $\alpha \in \mathbb{F}_{q^n}$, i.e.,

$$\sum_{i=0,1,2} a_i \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km}} b_{i+j-t+km}^{q^t} \right) - \mu \sum_{i=0,1,2} a_i^{q^s} \left(\sum_{k=0}^{r-1} \alpha^{q^{i+km+s}} b_{i+j+km}^{q^s} \right) = 0,$$

for all $\alpha \in \mathbb{F}_{q^n}$. Since $s \neq \pm i + km$, for $i = 0, 1, 2$ and $0 \leq k \leq r-1$, we get

$$\{km + i : i = 0, 1, 2,\ 0 \leq k \leq r-1\} \cap \{km + s + i : i = 0, 1, 2,\ 0 \leq k \leq r-1\} = \emptyset$$

and hence

$$\begin{cases} \mu a_i b_{i+j+km} = 0 \\ a_i b_{i+j-t+km} = 0, \end{cases}$$

for $0 \leq j \leq t-2$ and $0 \leq k \leq r-1$. Thus, whenever $a_i \neq 0$, we get

$$\begin{cases} b_{i+j+km} = 0 \\ b_{i+j-t+km} = 0. \end{cases}$$

The first equation with $j = 0$, the second with $j = t-2$ and (15) give

$$b_{i+km} = \cdots = b_{i+(k+1)m-2} = 0,$$

for $i = 0, 1, 2$ and $0 \leq k \leq r-1$.

For $a_0 \neq 0$ we get

$$b_{km} = \cdots = b_{(k+1)m-2} = 0,$$

for $a_1 \neq 0$ we get

$$b_{km+1} = \cdots = b_{(k+1)m-1} = 0$$

and for $a_2 \neq 0$ we get

$$b_{km+2} = \cdots = b_{(k+1)m} = 0,$$

with $0 \leq k \leq r-1$.

Hence, just one of the a_i's is nonzero. By choosing a suitable element in C we can assume $a_0 \neq 0$ so that

$$(b_0, \ldots, b_{n-1}) = (0, \ldots, 0, b_{m-1}, 0, \ldots, 0, b_{2m-1}, 0, \ldots, 0, b_{n-1}).$$

By recalling that $B = D^t_{(b_0,\ldots,b_{n-1})}$, we can see that the action of $\varphi = (A, B; \mathbf{1})$ on $\Omega_j^{(1)}$ is the following:

$$\begin{aligned} f^{\varphi}_{\alpha,j}(v, v') &= f_{\alpha,j}\left(a_0 x, b_{n-1}^q x'^q + b_{(r-1)m-1}^{q^{m+1}} x'^{q^{m+1}} + \cdots + b_{m-1}^{q^{(r-1)m+1}} x'^{q^{(r-1)m+1}}\right) \\ &= \mathrm{Tr}\left(\alpha a_0 x \left(b_{n-1} x' + b_{(r-1)m-1}^{q^m} x'^{q^m} + \cdots + b_{m-1}^{q^{(r-1)m}} x'^{q^{(r-1)m}}\right)^{q^{j+1}}\right) \end{aligned}$$

giving $f^{\varphi}_{\alpha,j} \in \Omega_{j+1}$. By consideration on dimensions we have

$$\Omega_j^{\varphi} = \Omega_{j+1}$$

giving that $\Phi^{\varphi}_{m,n,t-1} = \bigoplus_{j=1}^{t-1} \Omega_j$ is the unique subspace of $\mathcal{H}_{m,n,t,\mu,s}$ which is equivalent to $\Phi_{m,n,t-1}$. □

We are now in position to calculate the automorphism group of the MRD code $\mathcal{H}_{m,n,t,\mu,s}$.

Theorem 5.2 *Let $q = p^h$, p a prime. Let $m > 1$ be any divisor of n and $\mu \in \mathbb{F}_{q^n}^{\times}$ such that $\mathrm{N}_{q^n/q}(\mu) \neq (-1)^{nt}$. Set $r = n/m$. For any given $t \in \{1, \ldots, m-2\}$ and $s \not\equiv 0, \pm 1, \pm 2 \pmod m$, the automorphism group of $\mathcal{H}_{m,n,t,\mu,s}$ is the subgroup of $(S \times T') \rtimes C \rtimes \mathrm{Aut}(\mathbb{F}_q)$ whose elements correspond to triples $((D_{\mathbf{a}}, D_{\mathbf{b}}); \ell^i; \phi^e)$, where $\mathbf{a} = (a, 0, \ldots, 0)$, with $a \in \mathbb{F}_{q^m}$, and $\mathbf{b} = (b_0, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_m, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_{(r-1)m}, \underbrace{0, \ldots, 0}_{m-1 \text{ times}})$, with $b_{lm} \in \mathbb{F}_{q^n}$ such that*

$$\mu a^{q^s-1} b_{lm}^{(q^s-q^t)q^{-lm}} = \mu^{p^e q^{i-lm}},$$

for $0 \leq l \leq r-1$ whenever b_{lm} is nonzero.

Proof From Theorem 5.1 every automorphism of $\mathcal{H}_{m,n,t,\mu,s}$ must fix $\bigoplus_{j=1}^{t-1} \Omega_j$ giving $\mathrm{Aut}(\mathcal{H}_{m,n,t,\mu,s})$ is a subgroup of $\mathrm{Aut}(\bigoplus_{j=1}^{t-1} \Omega_j)$ which in turn is conjugate to $\mathrm{Aut}(\Phi_{m,n,t-1})$. By Theorem 4.6, $\mathrm{Aut}(\Phi_{m,n,t-1}) = (S \times T') \rtimes C \rtimes \mathrm{Aut}(\mathbb{F}_q)$, and it is easy to see that this group fixes every component Ω_j. Let $\varphi = ((A, B), \ell^i; \theta) \in \mathrm{Aut}(\mathcal{H}_{m,n,t,\mu,s})$ with $\theta = \phi^e$. As φ fixes every component Ω_j, then φ must fix $\Gamma_{m,n,t,\mu,s}$. In addition, ℓ^i maps $\Gamma_{m,n,t,\mu,s}$ to $\Gamma_{m,n,t,\mu^{q^i},s}$, thus the above condition holds if and only if $\varphi = ((A, B), \mathbf{1}; \theta)$ maps $\Gamma_{m,n,t,\mu^{q^i},s}$ to $\Gamma_{m,n,t,\mu,s}$.

Let $D_{(a,0,\ldots,0)}$ and $D^t_{(b_0,\ldots,0,b_m,0,\ldots,0,b_{(r-1)m},0,\ldots,0)}$ be the q-circulant matrix of A and B, respectively. Let $f = f_{\alpha,0} + f_{\mu^{q^i}\alpha^{q^s},t}$ be any bilinear form in $\Gamma_{m,n,t,\mu^{q^i},s}$. Then, f^{φ} is the bilinear form defined by

$$\begin{aligned}
f^{\varphi}(v, v') &= f_{\alpha^{p^e},0}\left(ax, b_0x' + b_m x'^{q^m} + \cdots + b_{(r-1)m}x'^{q^{(r-1)m}}\right) \\
&\quad + f_{\mu^{p^e q^i}\alpha^{q^s p^e},t}\left(ax, b_0x' + b_m x'^{q^m} + \cdots + b_{(r-1)m}x'^{q^{(r-1)m}}\right) \\
&= \mathrm{Tr}\left(\alpha^{p^e} ax \left(b_0x' + b_m x'^{q^m} + \cdots + b_{(r-1)m}x'^{q^{(r-1)m}}\right)\right) \\
&\quad + \mathrm{Tr}\left(\mu^{p^e q^i}\alpha^{q^s p^e} ax \left(b_0x' + b_m x'^{q^m} + \cdots + b_{(r-1)m}x'^{q^{(r-1)m}}\right)^{q^t}\right) \\
&= \mathrm{Tr}\left(a\left(\alpha^{p^e} b_0 + \alpha^{p^e q^{(r-1)m}} b_m^{q^{(r-1)m}} + \cdots + \alpha^{p^e q^m} b_{(r-1)m}^{q^m}\right) xx'\right) \\
&\quad + \mathrm{Tr}\left(a\left(\mu^{p^e q^i}\alpha^{p^e q^s} b_0^{q^t} + \mu^{p^e q^{(r-1)m+i}}\alpha^{p^e q^{(r-1)m+s}} b_m^{q^{(r-1)m+t}}\right.\right. \\
&\quad \left.\left. + \cdots + \mu^{p^e q^{m+i}}\alpha^{p^e q^{m+s}} b_{(r-1)m}^{q^{m+t}}\right) xx'^{q^t}\right).
\end{aligned}$$

For f^{φ} to lie in $\Gamma_{m,n,t,\mu,s}$ we must have

$$a^{q^s}\mu\left(\alpha^{p^e q^s} b_0^{q^s} + \alpha^{p^e q^{(r-1)m+s}} b_m^{q^{(r-1)m+s}} + \cdots + \alpha^{p^e q^{m+s}} b_{(r-1)m}^{q^{m+s}}\right)$$
$$= a\left(\mu^{p^e q^i}\alpha^{p^e q^s} b_0^{q^t} + \mu^{p^e q^{(r-1)m+i}}\alpha^{p^e q^{(r-1)m+s}} b_m^{q^{(r-1)m+t}} + \cdots + \mu^{p^e q^{m+i}}\alpha^{p^e q^{m+s}} b_{(r-1)m}^{q^{m+t}}\right)$$

for all $\alpha \in \mathbb{F}_{q^n}$. This yields

$$\mu a^{q^s} b_{lm}^{q^{(r-l)m+s}} = a\mu^{p^e q^{(r-l)m+i}} b_{lm}^{q^{(r-l)m+t}}$$

giving

$$\mu a^{q^s-1} b_{lm}^{(q^s-q^t)q^{-lm}} = \mu^{p^e q^{i-lm}}, \tag{16}$$

for $0 \le l \le r-1$ whenever b_{lm} is nonzero. □

Remark 5.3 Statement ii) in Theorem 4.3 is obtained by taking $m = n$ in the previous Theorem.

Remark 5.4 By Lemma 3.8, the arguments used in the proof of Theorems 5.2 work perfectly well for any k with $\gcd(k, n) = 1$ if the cyclic model of vector spaces and q-circulant matrices involved are replaced by the kth cyclic model and q^k-circulant matrices. This implies that the automorphism group of the punctured code $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is the subgroup of $(S \times T') \rtimes C \rtimes \mathrm{Aut}(\mathbb{F}_q)$ whose elements correspond to triples $((D^{(k)}_{\mathbf{a}}, D^{(k)}_{\mathbf{b}}); \ell^i; \phi^e)$, where $\mathbf{a} = (a, 0, \ldots, 0)$, with $a \in \mathbb{F}_{q^m}$, and $\mathbf{b} = (b_0, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_m, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_{(r-1)m}, \underbrace{0, \ldots, 0}_{m-1 \text{ times}})$ with $b_{lm} \in \mathbb{F}_{q^n}$ such that

$$\mu a^{q^{sk}-1} b_{lm}^{(q^{sk}-q^t)q^{-lm}} = \mu^{p^e q^{i-lm}}, \tag{17}$$

for $0 \le l \le r-1$ whenever b_{lm} is nonzero.

Theorem 5.5 *Let $m > 1$ be any divisor of n and $\mu \in \mathbb{F}^{\times}_{q^n}$, such that $\mathrm{N}_{q^n/q}(\mu) \neq (-1)^{nt}$. For any given $t \in \{1, \ldots, m-2\}$, the punctured code $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$, with $s \not\equiv 0, \pm 1, \pm 2 \pmod m$ and $\gcd(n, sk - t) < m$ is not equivalent to any generalized Gabidulin code.*

Proof In Sect. 3 we have seen that $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is an MRD $(m, n, q; m - t + 1)$-code. Therefore $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ has the same parameters as any generalized Gabidulin code $\mathcal{G}^{(j)}_{(g_0,\ldots,g_{m-1});t}$, with $g_0, \ldots, g_{m-1} \in \mathbb{F}_{q^n}$ linearly independent over $\mathbb{F}_q$.

By Theorem 4.1 the subgroup $L_{\mathcal{G}}$ of all linear automorphisms of $\mathcal{G}^{(j)}_{(g_0,\ldots,g_{m-1});t}$ is isomorphic to

$$\left(\mathbb{F}^{\times}_{q^{m'}} \times \mathrm{GL}(n/d, q^d)\right) \rtimes G,$$

for some divisors m' and d of n and a subgroup G of $\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. Note that m divides d. We represent the elements of $L_{\mathcal{G}}$ by pairs of type $((a, A); \varphi)$, with $a \in \mathbb{F}^{\times}_{q^{m'}}$, $A \in$

$\mathrm{GL}(n/d, q^d)$ and $\varphi \in G$. In particular the subgroup $\{(1, A); id)\}$ of $L_{\mathcal{G}}$ is isomorphic to $\mathrm{GL}(n/d, q^d)$.

By way of contradiction, assume that $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is equivalent to $\mathcal{G}^{(j)}_{(g_0,\ldots,g_{m-1});t}$, for some $g_0, \ldots, g_{m-1} \in \mathbb{F}_{q^n}$ linearly independent over $\mathbb{F}_q$. Then, $\mathrm{Aut}(\mathcal{H}^{(k)}_{m,n,t,\mu,s})$ must be isomorphic to $\mathrm{Aut}(\mathcal{G}^{(j)}_{(g_0,\ldots,g_{m-1});t})$. In particular the subgroup $L_{\mathcal{H}}$ of all linear automorphisms of $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ must be isomorphic to $L_{\mathcal{G}}$.

Set $r = n/m$. By Theorem 5.2 and Remark 5.4, $L_{\mathcal{H}}$ is the subgroup of $(S \times T') \rtimes C$ whose elements correspond to pairs $((D^{(k)}_{\mathbf{a}}, D^{(k)}_{\mathbf{b}}); \ell^i)$, where $\mathbf{a} = (a, 0, \ldots, 0)$, with $a \in \mathbb{F}_{q^m}$, and $\mathbf{b} = (b_0, 0, \ldots, 0, b_m, 0, \ldots, 0, b_{(r-1)m}, 0, \ldots, 0)$, with $b_{lm} \in \mathbb{F}_{q^n}$ satisfying Eq. (17) with $e = 0$.

For $i = 0$ and $\mathbf{a} = (1, 0, \ldots, 0)$, the pairs $((I_m, D^{(k)}_{\mathbf{b}}), id)$, with $b_{lm} \in \mathbb{F}_{q^n}$ such that

$$\mu b_{lm}^{(q^{sk}-q^t)q^{-lm}} = \mu^{q^{-lm}}, \tag{18}$$

for $0 \le l \le r-1$ whenever b_{lm} is nonzero, form a subgroup B of $L_{\mathcal{H}}$ which should be isomorphic to $\mathrm{GL}(n/d, q^d)$. By raising to the q^{lm}th power both sides of Eq. (18), it becomes

$$b_{lm}^{q^t(q^{sk-t}-1)} = \mu^{1-q^{lm}}. \tag{19}$$

It is clear that the elements $b_{lm} \in \mathbb{F}_{q^n}$ that satisfy Eq. (19) corresponds to the solutions of

$$X^{q^{sk-t}-1} = \mu^{1-q^{lm}}. \tag{20}$$

over $\mathbb{F}_{q^n}$. If this equation has no solution in $\mathbb{F}_{q^n}$ then $b_{lm} = 0$.

Let $x, y \in \mathbb{F}^{\times}_{q^n}$ be distinct solutions of Eq. (20). Then $(x/y)^{q^{sk-t}-1} = 1$, or equivalently $x/y \in \mathbb{F}^{\times}_{q^c}$, with $c = \gcd(n, sk-t)$. Thus the solutions of Eq. (20) over $\mathbb{F}_{q^n}$ are exactly the elements in $\{\lambda x : x \in \mathbb{F}^{\times}_{q^c}\}$ where $\lambda \in \mathbb{F}_{q^n}$ is a fixed solution of (20). Therefore the number of solutions of (20) is either 0 or $q^c - 1$. In any case this number is strictly less than q^m. It follows that

$$|B| \le q^{cr} - 1 < q^n - 1 = |\mathrm{GL}(1, q^n)| \le |\mathrm{GL}(n/d, q^d)|.$$

From the above inequality it follows that the subgroup B is not isomorphic to $\mathrm{GL}(n/d, q^d)$. This contradicts the assumption that $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is equivalent to $\mathcal{G}^{(j)}_{(g_0,\ldots,g_{m-1});t}$. The result then follows. □

Corollary 5.6 *Let $m > 1$ be any divisor of n and $\mu, \nu \in \mathbb{F}^{\times}_{q^n}$ such that $\mathrm{N}_{q^n/q}(\mu) \neq (-1)^{nt} \neq \mathrm{N}_{q^n/q}(\nu)$. For any given $t \in \{1, \ldots, m-2\}$ and $s \not\equiv 0, \pm 1, \pm 2 \pmod m$ the punctured code $\mathcal{H}^{(k)}_{m,n,t,\mu,s}$ is equivalent to $\mathcal{H}^{(k)}_{m,n,t,\nu,u}$ if and only if there exist $j \in \{0, \ldots, r-1\}$, an integer i, a nonzero element $a \in \mathbb{F}_{q^m}$ and $b_{hm} \in \mathbb{F}_{q^n}$, $h = 0, \ldots, r-1$, such that $a\mu^{p^e q^{(r-h)m+i}} b_{hm}^{q^{(r-h)m+t}} = a^{q^u} \nu b_{(h-j)m}^{q^{(j-h)m+u}}$, for $0 \le h \le r-1$ (with indices of b considered modulo n) and the q^k-circulant matrix $D_{\mathbf{b}}$ defined by $\mathbf{b} = (b_0, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_m, \underbrace{0, \ldots, 0}_{m-1 \text{ times}}, b_{(r-1)m}, \underbrace{0, \ldots, 0}_{m-1 \text{ times}})$ is non-singular.*

Proof We argue with $k = 1$. By Theorem 5.1, $\mathcal{H}_{m,n,t,\mu,s}$ and $\mathcal{H}_{m,n,t,\nu,u}$ contain a unique subspace equivalent to $\Phi_{m,n,t-1}$. Therefore, any isomorphism from $\mathcal{H}_{m,n,t,\mu,s}$ to $\mathcal{H}_{m,n,t,\nu,u}$ is in $\mathrm{Aut}(\Phi_{m,n,t-1})$. By using similar arguments as in the proof of Theorem 5.2, we may consider isomorphisms of type $((A, B), \mathbf{1}; \theta)$. Let $f = f_{\alpha,0} + f_{\mu^{q^i}\alpha^{q^s},t}$ be any bilinear form in $\Gamma_{m,n,t,\mu^{q^i},s}$. Then, f^{φ} lies in $\Gamma_{m,n,t,\nu,u}$ if and only if

$$\begin{aligned} &a^{q^u}\nu\left(\alpha^{p^e q^u} b_0^{q^u} + \alpha^{p^e q^{(r-1)m+u}} b_m^{q^{(r-1)m+u}} + \cdots + \alpha^{p^e q^{m+u}} b_{(r-1)m}^{q^{m+u}}\right) \\ &= a\left(\mu^{p^e q^i}\alpha^{p^e q^s} b_0^{q^t} + \mu^{p^e q^{(r-1)m+i}}\alpha^{p^e q^{(r-1)m+s}} b_m^{q^{(r-1)m+t}}\right. \\ &\quad \left. + \cdots + \mu^{p^e q^{m+i}}\alpha^{p^e q^{m+s}} b_{(r-1)m}^{q^{m+t}}\right) \end{aligned}$$

for all $\alpha \in \mathbb{F}_{q^n}$. This yields $s = jm + u$ for some $j \in \{0, \ldots, r-1\}$ giving $a\mu^{p^e q^{(r-h)m+i}} b_{hm}^{q^{(r-h)m+t}} = a^{q^u}\nu b_{(h-j)m}^{q^{(j-h)m+u}}$, for $0 \le h \le r-1$. Straightforward calculations show that the latter conditions imply that $\mathcal{H}_{m,n,t,\mu,s}$ is equivalent to $\mathcal{H}_{m,n,t,\nu,u}$. □

Acknowledgements The first author is very grateful for the opportunity and the hospitality of the Department of Mathematics, Computer Science and Economics at the University of Basilicata, where he spent two weeks during the development of this research. The authors would like to thank the referees for their time and useful comments that improved the first version of the paper.

References

1. Augot, D., Loidreau, P., Robert, G.: Rank metric and Gabidulin codes in characteristic zero. In: Proceedings ISIT 2013, pp. 509–513 (2013)
2. Bottema, O.: On the Betti-Mathieu group. Nieuw Arch. Wiskd. **16**, 46–50 (1930)
3. Byrne, E., Ravagnani, A.: Covering radius of matrix codes endowed with the rank metric. SIAM J. Discrete Math. **31**, 927–944 (2017)
4. Carlitz, L.: A note on the Betti–Mathieu group. Port. Math. **22**, 121–125 (1963)
5. Cooperstein, B.N.: External flats to varieties in $\mathrm{PG}(M_{n,n}(\mathrm{GF}(q)))$. Linear Algebra Appl. **267**, 175–186 (1997)
6. Cossidente, A., Marino, G., Pavese, F.: Non-linear maximum rank distance codes. Des. Codes Cryptogr. **79**, 597–609 (2016)
7. Csajbók, B., Marino, G., Polverino, O., Zullo, F.: Maximum scattered linear sets and MRD-codes. J. Algebraic Combin. **46**, 517–531 (2017)
8. de la Cruz, J., Kiermaier, M., Wassermann, A., Willems, W.: Algebraic structures of MRD codes. Adv. Math. Commun. **10**, 499–510 (2016)
9. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. J. Combin. Theory Ser. A **25**, 226–241 (1978)
10. Donati, G., Durante, N.: A generalization of the normal rational curve in $\mathrm{PG}(d, q^n)$ and its associated non-linear MRD codes. Des. Codes Cryptogr. **86**, 1175–1184 (2018)
11. Durante, N., Siciliano, A.: Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries. Electron. J. Combin. **24**, Paper 2.33 (2017)
12. Faina, G., Kiss, G., Marcugini, S., Pambianco, F.: The cyclic model for $\mathrm{PG}(n, q)$ and a construction of arcs. European J. Combin. **23**, 31–35 (2002)
13. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**, 3–16 (1985)

14. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a noncommutative ring and their application in cryptology. In: Advances in Cryptology, EUROCRYPT '91. Lecture Notes in Computer Science, vol. 547, pp. 482–489 (1991)
15. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Rank errors and rank erasures correction. In: Proceedings of the 4th International Colloquium on Coding Theory, Dilijan, Armenia, Yerevan, pp. 11–19 (1992)
16. Gantmacher, F.R.: The Theory of Matrices, vol. 1. AMS Chelsea Publishing, Providence (1998)
17. Hirschfeld, J.W.P.: Projective Geometries Over Finite Fields, 2nd edn. Clarendon Press, Oxford (1998)
18. Huppert, B.: Endliche Gruppen I. Spriger, Berlin (1967)
19. Kshevetskiy, A., Gabidulin, E.M.: The new construction of rank codes. Proceedings of the International Symposium on Information Theory (ISIT) 2005, pp. 2105–2108 (2005)
20. Kötter, R., Kschischang, F.: Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory **54**, 3579–3591 (2008)
21. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
22. Liebhold, D., Nebe, G.: Automorphism groups of Gabidulin-like codes. Arch. Math. **107**, 355–366 (2016)
23. Lunardon, G.: MRD-codes and linear sets. J. Combin. Theory Ser. A **149**, 1–20 (2017)
24. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. J. Combin. Theory Ser. A **159**, 79–106 (2018)
25. Martínez-Peñas, U.: On the similarities between generalized rank and hamming weights and their applications to network coding. IEEE Trans. Inform. Theory **62**, 4081–4095 (2016)
26. Otal, K., Özbudak, F.: Additive rank metric codes. IEEE Trans. Inform. Theory **63**, 164–168 (2017)
27. Puchinger, S., Rosenkilde né Nielsen, J., Sheekey, J.: Further generalisations of twisted Gabidulin codes. arXiv:1703.08093
28. Ravagnani, A.: Rank-metric codes and their duality theory. Des. Codes Cryptogr. **80**, 197–216 (2016)
29. Sheekey, J.: A new family of linear maximum rank distance codes. Adv. Math. Commun. **10**, 475–488 (2016)
30. Silva, D., Kschischang, F.R.: Universal secure network coding via rank-metric codes. IEEE Trans. Inform. Theory **57**, 1124–1135 (2011)
31. Silva, D., Kschischang, F.R., Kötter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inform. Theory **54**, 3951–3967 (2008)
32. Tarokh, V., Seshadri, N., Calderbank, A.R.: Space-time codes for high data rate wireless communication: performance criterion and code construction. IEEE Trans. Inform. Theory **44**, 744–765 (1998)
33. Trautmann, A.-L.: Isometry and automorphisms of constant dimension codes. Adv. Math. Commun. **7**, 147–160 (2013)
34. Trombetti, R., Zhou, Y.: Nuclei and automorphism group of generalized twisted Gabidulin codes. arXiv:1611.04447
35. Wan, Z.-X.: Geometry of Matrices. In memory of Professor L. K. Hua. World Scientific Publishing, Hackensack (1996)
36. Wu, B., Liu, Z.: Linearized polynomials over finite fields revisited. Finite Fields Appl. **22**, 79–100 (2013)