On self-dual MRD codes

Gabriele Nebe[1] and Wolfgang Willems[2]

Abstract. We investigate self-dual MRD codes. In particular we prove that a Gabidulin code in $(\mathbb{F}_q)^{n\times n}$ is equivalent to a self-dual code if and only if its dimension is $n^2/2$, $n \equiv 2 \pmod 4$, and $q \equiv 3 \pmod 4$. On the way we determine the full automorphism group of Gabidulin codes in $(\mathbb{F}_q)^{n\times n}$.

Keywords: self-dual MRD code, automorphism group, Gabidulin code
MSC: 94B05; 20B25

1 Introduction.

Following Delsarte [2] a rank metric code is a set $\mathcal{C} \subseteq k^{m\times n}$ of $m \times n$ matrices over a field k. The distance between two matrices $A, B \in k^{m\times n}$ is defined as $d(A, B) := \mathrm{Rk}(A - B)$, i.e. the rank of the difference of A and B. As usual we denote by

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

the minimum distance of $\mathcal{C}$. The dual code of $\mathcal{C}$ is

$$\mathcal{C}^\perp = \{X \in k^{m\times n} \mid (C, X) := \mathrm{trace}(CX^\mathsf{T}) = 0 \text{ for all } C \in \mathcal{C}\}$$

where X^T is the transpose and $\mathrm{trace}(X)$ the trace of the matrix X. Clearly, $\mathcal{C}^\perp$ is always a k-linear code, i.e. a subspace of the k-vector space $k^{m\times n}$.

Throughout the paper we assume that $m \geq n$, so our matrices have at least as many rows as columns. We will also assume that $\mathcal{C}$ is a linear code. If $\mathcal{C} \leq k^{m\times n}$ has minimum distance d then $d \leq n - \dim(\mathcal{C})/m + 1$ (see [2, Theorem 5.4], [9, Theorem 8]). Codes where equality holds are called MRD codes (maximum rank distance codes). By [2, Theorem 5.4] the dual of an MRD code is again an MRD code (see also [9, Corollary 41]).

In this note we investigate self-dual MRD codes, i.e. MRD codes $\mathcal{C}$ with $\mathcal{C} = \mathcal{C}^\perp$. As $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = \dim(k^{m\times n}) = mn$ a self-dual MRD code $\mathcal{C} \leq k^{m\times n}$ with $m \geq n$ has dimension $\frac{mn}{2}$ and minimum distance $d(\mathcal{C}) = \frac{n}{2} + 1$.

[1]Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany, nebe@math.rwth-aachen.de

[2]Otto-von-Guericke Universität, Magdeburg, Germany and Departamento de Matemáticas, Universidad del Norte, Barranquilla, Colombia, willems@ovgu.de

The inner product $(-,-)$ is the standard inner product if we identify $k^{m\times n}$ with $k^{1\times mn}$. If $\mathrm{char}(k)=2$, then self-dual codes in $k^{1\times mn}$ always contain the all-ones vector. So self-dual rank metric codes contain the all-ones matrix $J\in\{1\}^{m\times n}$ of rank 1. This implies that there are no self-dual MRD codes over fields of characteristic 2 (see Theorem 2.1). In Section 3 we give in odd characteristic a handy criterion to prove if a given rank metric code in $k^{m\times n}$ is equivalent to a self-dual code (see Theorem 3.3).

In the rest of the paper we study MRD codes in $k^{n\times n}$ where k is a finite field. In case $n=2$ all self-dual MRD codes are classified in Section 2: They exist if and only if -1 is not a square in k.

The most well-studied examples of MRD codes are the Gabidulin codes ([3], [2]). Section 4 treats Gabidulin codes of full length n, i.e. $n=[K:k]$ is the degree of the field extension, as k-linear subspaces of dimension ℓn of $k^{n\times n}$. We determine the k-linear automorphism group of these codes (see Corollary 4.7) and show that such a Gabidulin code is equivalent to a self-dual code if and only if $n\equiv 2 \pmod 4$, $\ell=n/2$, and -1 is not a square in k (see Theorem 4.10).

If -1 is a square in k or n is a multiple of 4, we do not have any examples of self-dual MRD codes in $k^{n\times n}$. Note that according to [7] there are 5 equivalence classes of self-dual MRD codes in $\mathbb{F}_5^{4\times 2}$.

2 Self-dual MRD codes

Surprisingly, in characteristic 2 self-dual MRD codes in $k^{m\times n}$ do not exist. This follows immediately from the following easy, but crucial result, since a self-dual MRD code in $k^{m\times n}$ has minimum distance at least 2.

Theorem 2.1. *Assume that* $\mathrm{char}(k)=2$ *and let* $\mathcal{C}\subseteq\mathcal{C}^\perp\leq k^{m\times n}$ *be a self-orthogonal code. Then the all-ones matrix* J *is in* $\mathcal{C}^\perp$. *In particular,* $d(\mathcal{C}^\perp)=1$.

Proof. All elements $A\in\mathcal{C}$ satisfy

$$0=(A,A)=\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij}^2=(\sum_{i=1}^{m}\sum_{j=1}^{n}A_{ij})^2=(A,J)^2$$

where J is the all-ones matrix, which is of rank 1. So $J\in\mathcal{C}^\perp$ satisfies $d(0,J)=1$. □

In contrast to the characteristic 2 case self-dual MRD codes may exist if $\mathrm{char}(k)$ is odd. To see that we characterize all self-dual MRD codes $\mathcal{C}$ in $k^{2\times 2}$

where $k = \mathbb{F}_q$ is the finite field with q elements. Since $d(\mathcal{C}) = 2$ and $\dim(\mathcal{C}) = 2$, the projection on the first row

$$\pi : \mathcal{C} \to k^{1\times 2}, \quad A \mapsto (a_{11}, a_{12})$$

is an isomorphism and $\mathcal{C}$ has a unique basis of the form

$$A = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}, \; B = \begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$$

with $a, b, c, d \in k$.

Proposition 2.2. *$\mathcal{C} = \langle A, B\rangle$ is a self-dual* MRD *code if and only if the following two conditions hold true.*

(i) $-1 \notin (k^\times)^2$, *i.e.,* $q \equiv 3 \pmod 4$.

(ii) $a^2 + b^2 = -1$ *and* $(c, d) \in \{(-b, a), (b, -a)\}$.

Proof. Assume that $\mathcal{C} = \langle A, B\rangle$ is a self-dual code. Then $(A, A) = (A, B) = (B, B) = 0$ yields the equations

$$a^2 + b^2 + 1 = c^2 + d^2 + 1 = ac + bd = 0.$$

The ideal in $\mathbb{Z}[a, b, c, d]$ generated by these three polynomials contains the element

$$a^2(c^2 + d^2 + 1) - d^2(a^2 + b^2 + 1) + (bd - ac)(ac + bd) = a^2 - d^2 = (a + d)(a - d).$$

We therefore conclude that $a = \pm d$ and similarly $b = \pm c$. Thus condition (ii) is equivalent to $\mathcal{C}$ being self-dual. Moreover $\mathcal{C}$ is an MRD code, if all non-zero matrices in $\mathcal{C}$ have determinant $\neq 0$, so if and only if $b \neq 0$ and

$$\det(A + xB) = \begin{cases} (x^2 + 1)b, & \text{if } (c, d) = (-b, a) \\ -(x^2 + 2\frac{a}{b}x - 1)b, & \text{if } (c, d) = (b, -a) \end{cases}$$

is an irreducible polynomial in $k[x]$. Using the fact that $a^2 + b^2 = -1$ we see that in both cases this leads to the condition that -1 is not a square in k, so $q \equiv 3 \pmod 4$. Thus we have (i). With the same computations as above we see that the conditions in (i) and (ii) lead to a self-dual MRD code. □

It is easy to see that all these codes are pairwise equivalent and that they are equivalent to Gabidulin codes of full length. So Proposition 2.2 may be seen as a special case of Theorem 4.10 below.

3 A criterion to be equivalent to a self-dual code

The rank distance preserving automorphisms of $k^{m\times n}$ are

$\kappa_{X,Y,Z,\sigma} : A \mapsto XA^\sigma Y+Z$ with $X \in \mathrm{GL}_m(k), Y \in \mathrm{GL}_n(k), Z \in k^{m\times n}, \sigma \in \mathrm{Aut}(k)$

or

$\tau_{X,Y,Z,\sigma} : A \mapsto XA^{\mathsf{T},\sigma} Y+Z$ with $X, Y \in \mathrm{GL}_n(k), Z \in k^{m\times n}, \sigma \in \mathrm{Aut}(k)$ (if $m = n$)

and these are k-linear, if and only if $Z = 0$ and $\sigma = \mathrm{id}$ (see [11], Theorem 3.4). If $m = n$, then the $\tau_{X,Y} := \tau_{X,Y,0,\mathrm{id}}$ are called improper and the $\kappa_{X,Y} := \kappa_{X,Y,0,\mathrm{id}}$ proper automorphisms.

Definition 3.1. Two linear rank metric codes $\mathcal{C}$ and $\mathcal{D} \leq k^{m\times n}$ are called properly equivalent, if there are $X \in \mathrm{GL}_m(k)$, $Y \in \mathrm{GL}_n(k)$ such that $\mathcal{D} = X\mathcal{C}Y$.

Note that proper equivalence is the usual notion of linear equivalence for $m \neq n$. Only for $m = n$ the proper equivalences form a subgroup of index 2 in the group of linear equivalences.

Lemma 3.2. *Let k be a finite field of odd characteristic and let $A \in k^{n\times n}$ be a symmetric matrix of full rank. Then there is a matrix $X \in \mathrm{GL}_n(k)$ such that $A = XX^\mathsf{T}$ if and only if $\det(A) \in (k^\times)^2$.*

Proof. Regular quadratic forms over finite fields of odd characteristic are classified by their dimension and their determinant (see for instance [10, Chapter 2, Theorem 3.8]). In particular a quadratic form with Gram matrix $A \in \mathrm{GL}_n(k)$ is equivalent to the standard form with Gram matrix I_n if and only if $\det(A)$ is a square. □

Theorem 3.3. *Let k be a finite field of odd characteristic and let $\mathcal{C} \leq k^{m\times n}$ be a linear rank metric code. Then $\mathcal{C}$ is properly equivalent to a self-dual code if and only if there are symmetric matrices $A = A^\mathsf{T} \in k^{m\times m}$ and $B = B^\mathsf{T} \in k^{n\times n}$ such that $\det(A), \det(B) \in (k^\times)^2$ are non-zero squares with*

$$\mathcal{C}^\perp = A\mathcal{C}B.$$

Proof. Assume that there are $X \in \mathrm{GL}_m(k)$, $Y \in \mathrm{GL}_n(k)$ such that $\mathcal{D} := X\mathcal{C}Y = \mathcal{D}^\perp$. Then for all $C_1, C_2 \in \mathcal{C}$ we have

$$0 = \mathrm{trace}(XC_1Y(XC_2Y)^\mathsf{T}) = \mathrm{trace}(XC_1YY^\mathsf{T}C_2^\mathsf{T}X^\mathsf{T}) = \mathrm{trace}(X^\mathsf{T}XC_1YY^\mathsf{T}C_2^\mathsf{T})$$

Put $A := X^{\mathsf{T}}X$ and $B := YY^{\mathsf{T}}$. Then A and B are symmetric of square determinant and $\mathcal{C}^{\perp} = A\mathcal{C}B$.
On the other hand assume that there are A, B as stated in the theorem. According to Lemma 3.2 there are $X \in \mathrm{GL}_m(k)$, $Y \in \mathrm{GL}_n(k)$ such that $A = X^{\mathsf{T}}X$, $B = YY^{\mathsf{T}}$. The same computation as above shows that $X\mathcal{C}Y$ is a self-dual code. □

4 Gabidulin codes in $k^{n\times n}$

We keep the assumption that $k = \mathbb{F}_q$ is a finite field, but allow $\mathrm{char}(k)$ to be arbitrary (even or odd). Let $K := \mathbb{F}_{q^n}$ be the degree n extension field of k. For $\alpha \in K$ and $0 \le i \le n-1$ we define $\alpha^{[i]} := \alpha^{q^i}$ to be the image of α under the i-th iteration of the Frobenius automorphism of K/k and $\mathrm{Trace}_{K/k}(\alpha) := \sum_{i=0}^{n-1} \alpha^{[i]}$. For a k-basis $\mathfrak{B} := (\beta_1, \ldots, \beta_n)$ of K the dual basis $\mathfrak{B}^* := (\beta_1^*, \ldots, \beta_n^*)$ is defined by the property that $\mathrm{Trace}_{K/k}(\beta_i\beta_j^*) = \delta_{ij}$. If $\beta_i^* = \beta_i$ for all i, then the basis $\mathfrak{B}$ is called a self-dual basis. Note that a dual basis always exists, but a self-dual basis exists if and only if q is even or both q and n are odd (see [5]). Let $\mathcal{T}_{\mathfrak{B}} := (\mathrm{Trace}_{K/k}(\beta_i\beta_j))_{i,j=1,\ldots,n}$ denote the Gram matrix of the trace bilinear form $(\alpha, \beta) \in K \times K \mapsto \mathrm{Trace}_{K/k}(\alpha\beta) \in k$ with respect to the basis $\mathfrak{B}$. Then $\mathcal{T}_{\mathfrak{B}}$ is the base change matrix between $\mathfrak{B}$ and its dual basis $\mathfrak{B}^*$, because if $\beta_i = \sum_{m=1}^{n} a_{mi}\beta_m^*$ with $a_{mi} \in k$ for all m, then

$$(\mathcal{T}_{\mathfrak{B}})_{ji} = \mathrm{Trace}_{K/k}(\beta_j\beta_i) = \sum_{m=1}^{n} a_{mi}\,\mathrm{Trace}_{K/k}(\beta_j\beta_m^*) = a_{ji}.$$

In the notation of the next definition $\mathcal{T}_{\mathfrak{B}} = \epsilon_{\mathfrak{B}^*}(\mathfrak{B})$.

Definition 4.1. Let $\mathfrak{B} = (\beta_1, \ldots, \beta_n) \in K^n$ be a k-basis of K and define the map $\epsilon_{\mathfrak{B}} : K^{1\times n} \to k^{n\times n}$ by

$$\epsilon_{\mathfrak{B}}(\alpha_1, \ldots, \alpha_n) := (a_{ij}) \in k^{n\times n} \quad \text{if } \alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i.$$

For $\alpha \in K$ and $\ell \in \mathbb{N}_0$ we also put $\alpha\,\mathfrak{B} := (\alpha\beta_1, \ldots, \alpha\beta_n) \in K^n$ and $\alpha^{[\ell]} := \alpha^{(q^\ell)}$ respectively $\mathfrak{B}^{[\ell]} := (\beta_1^{[\ell]}, \ldots, \beta_n^{[\ell]})$.

Lemma 4.2. *For any $\alpha \in K$ we have*

$$\epsilon_{\mathfrak{B}}(\alpha\,\mathfrak{B})^{\mathsf{T}} = \epsilon_{\mathfrak{B}^*}(\alpha\,\mathfrak{B}^*) = \mathcal{T}_{\mathfrak{B}}\,\epsilon_{\mathfrak{B}}(\alpha\,\mathfrak{B})\,\mathcal{T}_{\mathfrak{B}}^{-1}.$$

Proof. Let $B := \epsilon_{\mathfrak{B}}(\alpha\,\mathfrak{B})$ and $\mathcal{T}_{\mathfrak{B}} =: \mathcal{T}$. If we denote the entry of a matrix A at position (i,j) by A_{ij}, then

$$\beta_j = \sum_{i=1}^{n} \mathcal{T}_{ij}\,\beta_i^*,\ \beta_j^* = \sum_{i=1}^{n} (\mathcal{T}^{-1})_{ij}\beta_i, \text{ and } \alpha\beta_i = \sum_{j=1}^{n} B_{ji}\beta_j.$$

We compute

$$\begin{aligned}
\alpha\beta_r^* &= \alpha \textstyle\sum_{i=1}^{n} (\mathcal{T}^{-1})_{ir}\beta_i \\
&= \textstyle\sum_{i=1}^{n} (\mathcal{T}^{-1})_{ir}(\alpha\beta_i) \\
&= \textstyle\sum_{i=1}^{n} (\mathcal{T}^{-1})_{ir} \sum_{j=1}^{n} B_{ji}\beta_j \\
&= \textstyle\sum_{i=1}^{n} (\mathcal{T}^{-1})_{ir} \sum_{j=1}^{n} B_{ji} \sum_{m=1}^{n} \mathcal{T}_{mj}\,\beta_m^* \\
&= \textstyle\sum_{m=1}^{n} (\mathcal{T}\,B\,\mathcal{T}^{-1})_{m,r}\beta_m^*.
\end{aligned}$$

Since $\alpha\beta_r^* = \sum_{m=1}^{n} (\epsilon_{\mathfrak{B}^*}(\alpha\,\mathfrak{B}^*))_{m,r}\beta_m^*$ the second equality follows.

To see the first equality let $C := \epsilon_{\mathfrak{B}^*}(\alpha^{-1}\,\mathfrak{B}^*)$, so $\alpha^{-1}\beta_r^* = \sum_{s=1}^{n} C_{sr}\beta_s^*$. Note that $B^{\mathsf{T}}C = I_n$ since

$$\begin{aligned}
\delta_{ir} &= \mathrm{Trace}_{K/k}(\alpha\beta_i\alpha^{-1}\beta_r^*) \\
&= \textstyle\sum_{j=1}^{n} B_{ji} \sum_{s=1}^{n} C_{sr}\,\mathrm{Trace}_{K/k}(\beta_j\beta_s^*) \\
&= \textstyle\sum_{j=1}^{n} B_{ji}C_{jr} = (B^{\mathsf{T}}C)_{ir}.
\end{aligned}$$

So $B^{\mathsf{T}} = C^{-1} = (\epsilon_{\mathfrak{B}^*}(\alpha^{-1}\,\mathfrak{B}^*))^{-1} = \epsilon_{\mathfrak{B}^*}(\alpha\,\mathfrak{B}^*)$. The last equality follows from the fact that the matrix $\epsilon_{\mathfrak{B}^*}(\alpha\,\mathfrak{B}^*)$ describes the k-linear map induced by the multiplication of α on K with respect to the basis $\mathfrak{B}^*$. □

4.1 Automorphisms of Gabidulin codes.

In this section we determine the automorphism group of Gabidulin codes of full length $n = [K : k]$. To obtain a nice description in terms of matrices we use a normal basis $\Gamma := (\gamma, \gamma^{[1]}, \ldots, \gamma^{[n-1]})$ of K over k. Define $\mathcal{T} := \mathcal{T}_\Gamma = \epsilon_{\Gamma^*}(\Gamma) \in k^{n\times n}$ to be the Gram matrix of the trace bilinear form with respect to Γ and let

$$A := \begin{pmatrix} 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix} = \epsilon_\Gamma(\Gamma^{[1]}).$$

In the following computations we regard the indices of the matrix entries as integers modulo n represented by $0, \ldots, n-1$.

Remark 4.3. *(i)* $A\,\mathcal{T} = \mathcal{T}\,A$.

(ii) For $1 \leq j \leq n-1$ *we have* $\Gamma^{[j]} = \Gamma A^j$.

Proof. (i) Note that $\mathcal{T}_{ij} = \mathrm{Trace}_{K/k}(\gamma^{[i+j]})$ for all $0 \leq i, j \leq n-1$. So multiplication with the permutation matrix A yields

$$(A\,\mathcal{T})_{i,j} = \mathcal{T}_{(i-1),j} = \mathcal{T}_{i,(j-1)} = (\mathcal{T}\,A)_{i,j}.$$

(ii) Direct computation. □

Definition 4.4. For $1 \leq \ell \leq n$ the Gabidulin code $\mathcal{G}_{\ell,\Gamma} \leq k^{n\times n}$ is the k-linear code

$$\mathcal{G}_{\ell,\Gamma} = \langle \epsilon_\Gamma(\gamma_i \Gamma^{[j]}) \mid 1 \leq i \leq n, 0 \leq j \leq \ell - 1 \rangle.$$

Let $\mathcal{K} := \mathcal{G}_{1,\Gamma}$.

Lemma 4.5. (i) *$\mathcal{K}$ is an n-dimensional subalgebra of $k^{n\times n}$ isomorphic to $K = \mathbb{F}_{q^n}$.*

(ii) *For any $B \in \mathcal{K}$ we have $ABA^{-1} = B^q$. In particular $A\mathcal{K} = \mathcal{K}A$ as a set.*

(iii) *The normalizer in $\mathrm{GL}_n(k)$ of $\mathcal{K}^\times$ is the semidirect product of $\mathcal{K}^\times$ and the cyclic group $\langle A \rangle$ of order n.*

(iv) $\mathrm{trace}(BA^\ell) = 0$ *for all $B \in \mathcal{K}$ and all $1 \leq \ell \leq n-1$.*

(v) *The full matrix ring*

$$k^{n\times n} = \mathcal{K} \oplus \mathcal{K}A \oplus \ldots \oplus \mathcal{K}A^{n-1}$$

is a cyclic algebra. So for all $X \in k^{n\times n}$ there are unique $x_i \in \mathcal{K}$ such that $X = \sum_{i=0}^{n-1} x_i A^i$.

(vi) *For $\ell \geq 1$*

$$\mathcal{G}_{\ell,\Gamma} = \mathcal{K} \oplus \mathcal{K}A \oplus \ldots \oplus \mathcal{K}A^{\ell-1}.$$

Proof. (i) The map $K \to \mathcal{K}$, $\alpha \mapsto \epsilon_\Gamma(\alpha\Gamma)$ is an isomorphism of k-algebras.
(ii) We use the isomorphism above to write $B = \epsilon_\Gamma(\beta\Gamma)$ for some $\beta \in K$ and recall that $A_{ij} = \delta_{i,(j+1)}$. We show that $AB = B^q A$ for all $B \in \mathcal{K}$. By definition we have that

$$\beta\gamma^{[j]} = \sum_{i=0}^{n-1} B_{ij}\gamma^{[i]},\ (AB)_{(i+1)j} = B_{ij},\ \text{and}\ (B^q A)_{ij} = (B^q)_{i(j+1)}.$$

Therefore we compute for all $j = 0, \ldots, n-1$

$\sum_{i=0}^{n-1}(B^qA)_{ij}\gamma^{[i]} = \sum_{i=0}^{n-1}(B^q)_{i(j+1)}\gamma^{[i]} = \beta^q\gamma^{[j+1]} = (\beta\gamma^{[j]})^{[1]} = (\sum_{i=0}^{n-1} B_{ij}\gamma^{[i]})^{[1]} = \sum_{i=0}^{n-1} B_{ij}\gamma^{[i+1]} = \sum_{i=0}^{n-1}(AB)_{(i+1)j}\gamma^{[i+1]} = \sum_{i=0}^{n-1}(AB)_{ij}\gamma^{[i]}$.

So the j-th column of B^qA and AB coincide.
(iii) This is well-known and widely used in geometry and group theory, see for instance [4], Kap. II, Satz 7.3.
(iv) We embed $k^{n\times n}$ into $K^{n\times n}$, because in the latter ring we may diagonalise the relevant matrices. Take any primitive element $\alpha \in K$. Then $C := \epsilon_\Gamma(\alpha\Gamma) \in \mathrm{GL}_n(k) \leq \mathrm{GL}_n(K)$ has n distinct eigenvalues $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]}$ in K, the roots of the minimal polynomial of α over k. In particular there is a matrix $X \in \mathrm{GL}_n(K)$ such that $X^{-1}CX = \mathrm{diag}(\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]})$. As $ACA^{-1} = C^q$ (by (ii)) also $(X^{-1}AX)(X^{-1}CX)(X^{-1}AX)^{-1} = (X^{-1}CX)^q$, so $X^{-1}AX$ cyclically permutes the eigenspaces of $X^{-1}CX$. More precisely there are $a_i \in K$ such that

$$(X^{-1}AX)_{ij} = \begin{cases} a_i & j = i+1 \\ 0 & \text{otherwise} \end{cases}$$

where as usual the indices are taken modulo n. Because $k[C] = \mathcal{K}$, any $B \in \mathcal{K}$ is a polynomial in C and hence $X^{-1}BX$ is a diagonal matrix. So for any $1 \leq i \leq n-1$ the matrix $X^{-1}BA^iX$ is monomial with no non zero entries on the diagonal, because it induces the fixed point free permutation $(1, 2, \ldots, n)^i$ on the eigenspaces of $X^{-1}CX$. In particular its trace is 0. As the trace is invariant under conjugation we also get $\mathrm{trace}(BA^i) = \mathrm{trace}(X^{-1}BA^iX) = 0$.

(v) Suppose that $\sum_{i=0}^{n-1} B_iA^i = 0$ where $B_i \in \mathcal{K}$. Note that $B_iA^i = \epsilon_\Gamma(\beta_i\Gamma^{[i]})$. Thus we obtain $\epsilon_\Gamma(\sum_{i=0}^{n-1}\beta_i\Gamma^{[i]}) = 0$, hence $\sum_{i=0}^{n-1}\beta_i\Gamma^{[i]} = (0, \ldots, 0)$ since ϵ_Γ is injective. By [6, Chapter 3, Lemma 3.50], the $\Gamma^{[i]}$ are linearly independent over K, hence $\beta_i = 0$ for all i. This proves that the right hand side of the equation in (v) is a direct sum. The equality follows by comparing dimensions.
(vi) This follows immediately from (v) using the definition of $\mathcal{G}_{\ell,\Gamma}$. □

We are now ready to determine the automorphism group of $\mathcal{G}_{\ell,\Gamma}$ for all ℓ. Clearly $\mathcal{G}_{0,\Gamma} := \{0\}$ and $\mathcal{G}_{n,\Gamma} = k^{n\times n}$ are fixed by all linear equivalences. Also for the other Gabidulin codes there are certain obvious matrices $(X, Y) \in \mathrm{GL}_n(k) \times \mathrm{GL}_n(k)$, so that $X\mathcal{G}_{\ell,\Gamma}Y = \mathcal{G}_{\ell,\Gamma}$ (see for instance [8]):
For notational convenience we put $\mathcal{K}^\times := \mathcal{K} \setminus \{0\}$. Then $\mathcal{K}^\times \leq \mathrm{GL}_n(k)$ is isomorphic to the multiplicative group $K^\times$ of K and hence cyclic of order $q^n - 1$. Let S be any generator of $\mathcal{K}^\times = \langle S\rangle$ as a group. In group theory S is often called a Singer cycle. Clearly $\mathcal{K}^\times$ contains the subgroup of nonzero scalar matrices

$$C_{q-1} \cong k^\times \cong k^\times I_n = \langle S^{(q^n-1)/(q-1)}\rangle = \langle SS^qS^{(q^2)}\cdots S^{(q^{n-1})}\rangle \leq \mathcal{K}^\times.$$

Furthermore if $X \in \mathcal{K}^\times$, then $X\mathcal{G}_{\ell,\Gamma} = \mathcal{G}_{\ell,\Gamma}$ and $\mathcal{G}_{\ell,\Gamma}X = \mathcal{G}_{\ell,\Gamma}$. By Lemma 4.5 (ii) conjugation by A preserves the set $\mathcal{K}$, so $A^j\mathcal{G}_{\ell,\Gamma}A^{-j} = \mathcal{G}_{\ell,\Gamma}$ for $j = 0, \ldots, n-1$.

The next theorem shows that these obvious automorphisms already generate the full automorphism group of the Gabidulin codes.

Theorem 4.6. *For $0 < \ell < n$ the group of proper automorphisms of $\mathcal{G}_{\ell,\Gamma}$ is*

$$\mathrm{Aut}^{(p)}(\mathcal{G}_{\ell,\Gamma}) = \{\kappa_{X,Y} \mid (X,Y) \in (A^j\mathcal{K}^\times \times A^{-j}\mathcal{K}^\times), 0 \le j \le n-1\}$$

which is isomorphic to the semidirect product of $C_n \cong \mathrm{Gal}(K/k)$ with the normal subgroup $\mathcal{K}^\times\Upsilon\mathcal{K}^\times$ the central product of $K^\times$ with itself amalgamated over $k^\times$.

Proof. The inclusion $\supseteq$ is clear. To see the converse we suppose that $X\mathcal{G}_{\ell,\Gamma}Y = \mathcal{G}_{\ell,\Gamma}$ for $X, Y \in \mathrm{GL}_n(k)$.

Claim 1: If $\mathcal{Z} := \{Z \in \mathrm{GL}_n(k) \mid Z\mathcal{G}_{\ell,\Gamma} = \mathcal{G}_{\ell,\Gamma}\}$ then $\mathcal{Z} = \mathcal{K}^\times$:
According to Lemma 4.5 (v) we may write $Z := \sum_{i=0}^{n-1} z_i A^i \in \mathcal{Z}$ where $z_i \in \mathcal{K}$ for all i. As $I_n \in \mathcal{K}^\times \subseteq \mathcal{G}_{\ell,\Gamma}$ also $Z = ZI_n \in \mathcal{G}_{\ell,\Gamma}$, so $z_i = 0$ for $i = \ell, \ldots, n-1$. If $\ell \ge 1$, then also $A \in \mathcal{G}_{\ell,\Gamma}$. Thus $ZA = \sum_{i=0}^{\ell-1} z_i A^{i+1} \in \mathcal{G}_{\ell,\Gamma}$, which implies that $z_{\ell-1} = 0$. Repeating this argument several times we obtain $z_1 = \ldots = z_{n-1} = 0$ and $Z = z_0 \in \mathcal{K}$.

Claim 2: $X\mathcal{Z}X^{-1} = \mathcal{Z}(= \mathcal{K}^\times)$:
$X\mathcal{G}_{\ell,\Gamma}Y = \mathcal{G}_{\ell,\Gamma}$ is obviously invariant under left multiplication with $X\mathcal{Z}X^{-1}$. Thus Claim 1 implies $X\mathcal{Z}X^{-1} = \mathcal{Z}$.

Final step: By Claim 2 we know that $X \in \mathrm{GL}_n(k)$ lies in the normalizer of $\mathcal{K}^\times$. Note that A induces by conjugation on $\mathcal{K}^\times$ the Galois automorphism $x \mapsto x^q$ (cf. Lemma 4.5 (ii)). By Lemma 4.5 (iii) the normalizer of $\mathcal{K}^\times$ is $N_{\mathrm{GL}_n(k)}(\mathcal{K}^\times) = \langle A\rangle\mathcal{K}^\times$. Therefore there is some $0 \le j \le n-1$ such that $X \in A^j\mathcal{K}^\times$. In particular $X\mathcal{G}_{\ell,\Gamma}X^{-1} = \mathcal{G}_{\ell,\Gamma}$ and hence $\mathcal{G}_{\ell,\Gamma}XY = \mathcal{G}_{\ell,\Gamma}$. Similar to the proof of Claim 1 we conclude that $XY \in \mathcal{K}^\times$, hence $Y \in \mathcal{K}^\times A^{-j}\mathcal{K}^\times = A^{-j}\mathcal{K}^\times$. □

Corollary 4.7. *For $0 < \ell < n$ the full automorphism group of $\mathcal{G}_{\ell,\Gamma}$ is*

$$\mathrm{Aut}(\mathcal{G}_{\ell,\Gamma}) = \langle \mathrm{Aut}^{(p)}(\mathcal{G}_{\ell,\Gamma}), \tau_{\mathcal{T}^{-1},\mathcal{T}A^{\ell-1}}\rangle$$

and contains the group of proper automorphisms from Theorem 4.6 of index 2. In particular

$$|\mathrm{Aut}(\mathcal{G}_{\ell,\Gamma})| = 2n(q^n-1)\frac{q^n-1}{q-1}.$$

Proof. For any subgroup $U \le G$ of some finite group G and a normal subgroup $N \trianglelefteq G$, we have $|U/(N \cap U)| \le |G/N|$. So in particular the index of $\mathrm{Aut}^{(p)}(\mathcal{G}_{\ell,\Gamma})$

in the full automorphism group is either 1 or 2 and it suffices to show that $\tau_{\mathcal{T}^{-1},\mathcal{T}A^{\ell-1}}(\mathcal{G}_{\ell,\Gamma}) = \mathcal{G}_{\ell,\Gamma}$. To this aim let $C \in \mathcal{K}$ and $0 \leq j \leq \ell - 1$. Then

$$\begin{aligned} \tau_{\mathcal{T}^{-1},\mathcal{T}A^{\ell-1}}(CA^j) &= \mathcal{T}^{-1}(CA^j)^{\mathsf{T}}\,\mathcal{T}\,A^{\ell-1} = \mathcal{T}^{-1}(C')^{\mathsf{T}}A^{-j}\,\mathcal{T}\,A^{\ell-1} \\ &= \mathcal{T}^{-1}(C')^{\mathsf{T}}\,\mathcal{T}\,A^{\ell-1-j} \end{aligned}$$

for some $C' \in \mathcal{K}$, because conjugation by A preserves $\mathcal{K}$ as a set. The last equality follows from Remark 4.3 (i). By Lemma 4.2, we have $\mathcal{T}^{-1}(C')^{\mathsf{T}}\,\mathcal{T} = C' \in \mathcal{K}$. So $\tau_{\mathcal{T}^{-1},\mathcal{T}A^{\ell-1}}$ maps $\mathcal{K}A^j$ onto $\mathcal{K}A^{\ell-1-j}$ and hence preserves the code $\mathcal{G}_{\ell,\Gamma}$. □

4.2 Self-dual Gabidulin codes.

According to Theorem 2.1 and the fact that Gabidulin codes are MRD codes, there are no self-dual Gabidulin codes in even characteristic. So in this section we assume that $k = \mathbb{F}_q$, $K := \mathbb{F}_{q^n}$ and q is odd. We keep the notation from above. In particular $\Gamma = (\gamma, \gamma^{[1]}, \ldots, \gamma^{[n-1]})$ is a normal basis of K/k, $\mathcal{T} := \mathcal{T}_\Gamma$, $\langle S\rangle = \mathcal{K}^\times$, and $A := \epsilon_\Gamma(\Gamma^{[1]})$. If the Gabidulin code $\mathcal{G}_{\ell,\Gamma}$ is equivalent to a self-dual code then $\ell = n/2$ and n needs to be even. The following facts are elementary but crucial for the proofs of Proposition 4.9 and Theorem 4.10 below.

Lemma 4.8. *Assume that n is even. Then*

(i) $\det(A) = -1$ *and* $A^{\mathsf{T}} = A^{-1}$.

(ii) $ASA^{-1} = S^q$.

(iii) $A\,\mathcal{T} = \mathcal{T}\,A$ *and* $(\mathcal{T}\,A^\ell)^{\mathsf{T}} = A^{-\ell}\,\mathcal{T}$.

(iv) $\det(S)$ *is a primitive element of* $\mathbb{F}_q$.

(v) $\det(\mathcal{T}) \notin (\mathbb{F}_q^\times)^2$.

(vi) $\mathcal{T}\,S^j$ *is symmetric for all* $j = 0, \ldots, q^n - 1$.

(vii) $S^j\,\mathcal{T}^{-1}$ *is symmetric for all* $j = 0, \ldots, q^n - 1$.

(viii) $(\mathcal{T}\,A^jS^i)$ *is symmetric if and only if* $\begin{cases} j = n/2 \text{ and } (q^{n/2}+1) \mid i \\ \quad \text{or} \\ j = 0 \text{ and } i \in \{1, \ldots, q^n - 1\}, \end{cases}$
if and only if $S^iA^j\,\mathcal{T}^{-1}$ *is symmetric.*

Proof. (i) This is clear as A is a permutation matrix of a cycle of full length n and n is even.

(ii) This follows from Lemma 4.5 (ii).

(iii) The first statement is Remark 4.3 (i). To see the second note that A is a permutation matrix, so $A^{\mathsf{T}} = A^{-1}$ and $(\mathcal{T}\, A^{\ell})^{\mathsf{T}} = (A^{\ell})^{\mathsf{T}}\, \mathcal{T} = A^{-\ell}\, \mathcal{T}$.

(iv) Because S generates $\mathcal{K}$ as a k-algebra the minimal polynomial of S is equal to its characteristic polynomial. Moreover it also coincides with the minimal polynomial of a primitive element $\sigma \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ since S is a Singer cycle. Thus the determinant of S is the product of all Galois conjugates of σ, i.e. the norm of σ,

$$\det(S) = \sigma^{(1+q+\ldots+q^{n-1})} = \sigma^{(q^n-1)/(q-1)}.$$

As $\langle\sigma\rangle = \mathbb{F}_{q^n}^{\times}$ the order of σ is $q^n - 1$, so the order of $\det(S)$ is $q-1$ which proves that $\det(S)$ is a primitive element in $\mathbb{F}_q$. In particular $\det(S) \in \mathbb{F}_q^{\times} \setminus (\mathbb{F}_q^{\times})^2$.

(v) By Lemma 3.2, there is a self-dual basis for K/k if and only if the determinant of the trace bilinear form is a square. According to Lempel and Seroussi [5] K/k has a self-dual basis if and only if n is odd (since q is odd). As n is assumed to be even, the determinant of $\mathcal{T}$ is a non-square.

(vi) Lemma 4.2 with $\epsilon_{\mathfrak{B}}(\alpha\, \mathfrak{B}) = S$ implies that $S^{\mathsf{T}} = \mathcal{T}\, S\, \mathcal{T}^{-1}$, hence

$$(\mathcal{T}\, S)^{\mathsf{T}} = S^{\mathsf{T}}\, \mathcal{T}^{\mathsf{T}} = (\mathcal{T}\, S\, \mathcal{T}^{-1})\, \mathcal{T} = \mathcal{T}\, S.$$

(vii) This follows from (vi) because the inverse of a symmetric matrix is again symmetric.

(viii) Using the previous results we compute

$$(\mathcal{T}\, A^j S^i)^{\mathsf{T}} \overset{(ii)}{=} (\mathcal{T}\, S^{q^j i} A^j)^{\mathsf{T}} \overset{(vi)}{=} A^{-j}\, \mathcal{T}\, S^{q^j i} \overset{(iii)}{=} \mathcal{T}\, A^{-j} S^{q^j i} \overset{(ii)}{=} \mathcal{T}\, S^i A^{-j}$$

for all $0 \le j \le n-1$ and $1 \le i \le q^n - 1$. In particular $\mathcal{T}\, A^j S^i$ is symmetric if and only if $\mathcal{T}\, A^j S^i = \mathcal{T}\, S^i A^{-j}$. Dividing by $\mathcal{T}$ and using (ii) we obtain the equivalent condition $S^{q^j i} A^j = S^i A^{-j} \in \mathcal{K}A^j \cap \mathcal{K}A^{-j}$. Now $\mathcal{K}A^r \cap \mathcal{K}A^s \neq \{0\}$ if and only if $r \equiv s \bmod n$. So we obtain that $j \equiv -j \bmod n$, i.e. either $j = 0$ and then i is arbitrary, or $j = n/2$ and $(S^i)^{q^{n/2}} = (S^i)$ (i.e. $(q^{n/2}+1) \mid i$). The last statement follows by inverting the matrix. □

The next proposition follows by interpreting [1, Lemma 1] and [9, Theorem 18] in our language. For convenience of the reader we give a direct elementary proof.

Proposition 4.9. $\mathcal{G}_{n/2,\Gamma}^{\perp} = \mathcal{T}\, A^{n/2} \mathcal{G}_{n/2,\Gamma}\, \mathcal{T}^{-1}$.

Proof. We put $\mathcal{C} := \mathcal{T}\, A^{n/2} \mathcal{G}_{n/2,\Gamma}\, \mathcal{T}^{-1}$. As

$$\dim(\mathcal{C}) + \dim(\mathcal{G}_{n/2,\Gamma}) = 2\frac{n}{2}n = n^2 = \dim(k^{n\times n})$$

it suffices to show that $\mathcal{C} \subseteq \mathcal{G}_{n/2,\Gamma}^{\perp}$. To see this recall that $\mathcal{G}_{n/2,\Gamma} = \bigoplus_{i=0}^{n/2-1} \mathcal{K}A^i$ where $\mathcal{K} = \{0\} \cup \{S^\ell \mid 0 \leq \ell \leq q^n - 1\}$ and $\mathcal{K}A = A\mathcal{K}$. So it is enough to show that for $i \neq j$ with $i, j \in \{0, \ldots, n-1\}$ and all $m, \ell \in \{0, \ldots, q^n - 1\}$

$$\operatorname{trace}(S^m A^i (\mathcal{T}\, S^\ell A^j\, \mathcal{T}^{-1})^{\mathsf{T}}) = 0.$$

Applying Lemma 4.8 (where the relevant parts are indicated above the equalities) we compute

$$S^m A^i (\mathcal{T}\, S^\ell A^j\, \mathcal{T}^{-1})^{\mathsf{T}} \overset{(i),(vi)}{=} S^m A^i\, \mathcal{T}^{-1}\, A^{-j}\, \mathcal{T}\, S^\ell \overset{(iii)}{=} S^m A^{i-j} S^\ell \in \mathcal{K}A^{i-j}$$

where the last inclusion follows from Lemma 4.8 (ii). If $i - j$ is not divisible by n, then Lemma 4.5 (iv) tells us that all matrices in $\mathcal{K}A^{i-j}$ have trace 0. □

In particular $\mathcal{G}_{n/2,\Gamma}$ is always equivalent to its dual code. We now apply Theorem 3.3 to obtain a criterion, when $\mathcal{G}_{n/2,\Gamma}$ is equivalent to a self-dual code.

Theorem 4.10. $\mathcal{G}_{n/2,\Gamma}$ *is equivalent to a self-dual* MRD *code if and only if* $n \equiv 2 \pmod 4$ *and* $q \equiv 3 \pmod 4$.

Proof. Let $\delta := \det(S)$. Then, by Lemma 4.8 (iv), $\delta \notin (k^\times)^2$.

By Proposition 4.9, we have

$$\mathcal{G}_{n/2,\Gamma}^{\perp} = \mathcal{T}\, A^{n/2} \mathcal{G}_{n/2,\Gamma}\, \mathcal{T}^{-1}\,.$$

From Theorem 4.6 we hence obtain the set of proper equivalences between $\mathcal{G}_{n/2,\Gamma}$ and $\mathcal{G}_{n/2,\Gamma}^{\perp}$ as

$$\{\kappa_{\mathcal{T}\, A^{n/2} A^j S^i, S^h A^{-j}\, \mathcal{T}^{-1}} \mid i, h \in \{0, \ldots, q^n - 1\}, j \in \{0, \ldots, n-1\}\}.$$

According to Corollary 4.7 all Gabidulin codes have improper automorphisms. So if $\mathcal{G}_{n/2,\Gamma}$ is equivalent to a self-dual MRD code, then it is properly equivalent to a self-dual MRD code.

To use Theorem 3.3 we hence need to decide for which triples (i, h, j) both matrices

$$X_{i,j} := \mathcal{T}\, A^{n/2} A^j S^i \text{ and } Y_{h,j} := S^h A^{-j}\, \mathcal{T}^{-1}$$

are symmetric and of square determinant.

By Lemma 4.8 (v) (note that we assume that n is even), $\det(X_{i,j}) \in (k^\times)^2$ if and only if $(-1)^{\frac{n}{2}+j}\delta^i \notin (k^\times)^2$ and $\det(Y_{h,j}) \in (k^\times)^2$ if and only if $(-1)^j\delta^h \notin (k^\times)^2$.

By Lemma 4.8 (viii), the matrix $X_{i,j}$ is symmetric if and only if either $j = 0$ and $(q^{n/2}+1) \mid i$ or $j = n/2$ and i is arbitrary. The matrix $Y_{h,j}$ is symmetric if and only if either $j = 0$ and h is arbitrary or $j = n/2$ and h is a multiple of $(q^{n/2}+1)$.

So in particular $X_{i,j}$ and $Y_{h,j}$ are symmetric of square determinant if and only if either

(a) $(-1)^{n/2} \notin (k^\times)^2$ and $j = 0, (q^{n/2}+1) \mid i$, and h is odd

or

(b) $(-1)^{n/2} \notin (k^\times)^2$ and $j = n/2$, $(q^{n/2}+1) \mid h$, and i is odd.

These conditions can be satisfied if and only if $n \equiv 2 \pmod 4$ and $q \equiv 3 \pmod 4$. □

Acknowledgement. The ideas for this paper initiated during the ALCOMA15 conference. The authors thank the organisers for their kind invitation. Part of the work was done during two visits of the second author to the RWTH Aachen University in spring 2015 financed by the RTG 1632 of the DFG.

References

[1] T. Berger, Isometries for rank distance and permutation group of Gabidulin codes. In Proceedings of ACCT'8, St Petersbourg, Sept 2002, 30-33.

[2] Ph. Delsarte, Bilinear Forms over a Finite Field with Applications to Coding Theory. J. Comb. Theory A, 25 (1978) 226-241.

[3] E. Gabidulin, Theory of codes with maximum rank distance. Problems Inf. Transmission, 21 (1985) 1-12.

[4] B. Huppert, Endliche Gruppen I, Springer Verlag 1967.

[5] A. Lempel and G. Seroussi, Factorization of symmetric matrices and trace-orthogonal bases in finite fields. SIAM J. Comput. 9 (1980), 758-767.

[6] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Revised edition, Cambridge University Press, Cambridge 1994.

[7] K. Morrison, An enumeration of the equivalence classes of self-dual matrix codes. Advances in Mathematics of Communication 9 (2015) 415-436.

[8] K. Morrison, Equivalence for Rank-Metric and Matrix Codes and Automorphism Groups of Gabidulin Codes. IEEE Transactions on Information Theory 60 (2014) 7035-7046.

[9] A. Ravagnani, Rank-metric codes and their duality theory. Designs, Codes, and Cryptography, April 2015, DOI 10.1007/s10623-015-0077-3

[10] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren der mathematischen Wissenschaften 270, Springer-Verlag Berlin Heidelberg New York Tokyo 1985.

[11] Z.-X. Wan, Geometry of matrices. In memory of Professor L. K. Hua (1910-1985), World Scientific, Singapore 1996.