Automorphism groups of Gabidulin-like codes

Dirk Liebhold and Gabriele Nebe[1]

Dedicated to Ernst-Ulrich Gekeler

ABSTRACT. Let K/k be a cyclic Galois extension of degree ℓ and θ a generator of $\mathrm{Gal}(K/k)$. For any $v = (v_1, \ldots, v_m) \in K^m$ such that v is linearly independent over k, and any $1 \leq d < m$ the Gabidulin-like code $\mathcal{C}(v, \theta, d) \leq k^{\ell \times m}$ is a maximum rank distance code of dimension ℓd over k. This construction unifies the ones available in the literature. We characterise the K-linear codes that are Gabidulin-like codes and determine their rank-metric automorphism group.

Keywords: rank metric codes, MRD codes, automorphism group, Gabidulin-like code
MSC: 94B05; 20B25

1. Introduction.

In random linear network coding any node of the network may transmit a random linear combination of the received vectors. So the transmitted information is the subspace generated by the input vectors, an element of the Grassmanian

$$\mathcal{G}_{\ell,n}(k) := \{U \leq k^n \mid \dim(U) = \ell\}$$

the set of all ℓ-dimensional subspaces of the space k^n of rows of length n over the field k. A (constant dimension) network code is a subset of such a Grassmanian. There is a natural distance function d on $\mathcal{G}_{\ell,n}(k)$ defined by $d(U, V) := \ell - \dim(U \cap V)$. The general linear group $\mathrm{GL}_n(k)$ acts transitively on $\mathcal{G}_{\ell,n}(k)$ preserving this distance. However there are a few disadvantages of this framework:

- $\mathcal{G}_{\ell,n}(k)$ is a homogeneous space but not a vector space.
- So in this generality there is no notion of a linear code (as for the classical block codes).
- It is also not obvious how to systematically encode information into a sequence of subspaces.

To come around these problems, Koetter and Kschischang [8] suggested to consider a subset of $\mathcal{G}_{\ell,n}(k)$: Put $m := n - \ell$. For a matrix $X \in k^{\ell \times m}$ let $U_X :=$ row space of $(I_\ell | X)$. Then $U_X \in \mathcal{G}_{\ell,n}(k)$ and $U_X = U_Y$ if and only if $X = Y$. So the map $X \mapsto U_X$ is a bijection between the vector space $k^{\ell \times m}$ and

$$\mathcal{M}_{\ell,m}(k) := \{U_X \mid X \in k^{\ell \times m}\} \subset \mathcal{G}_{\ell,n}(k).$$

The distance between two spaces $U_X, U_Y \in \mathcal{M}_{\ell,n}(k)$ is $d(U_X, U_Y) = \mathrm{rk}(X - Y)$, the rank metric on this space of matrices, which was already studied in [3] and [5].

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

A linear rank metric code is a subspace $\mathcal{C}$ of $k^{\ell \times m}$. The minimum distance of $\mathcal{C}$ is $d(\mathcal{C}) = \min\{\mathrm{rk}(C) \mid 0 \neq C \in \mathcal{C}\}$. The well known Singleton bound (see Proposition 2.2) shows that

$$\dim(\mathcal{C}) \leq \max(\ell, m)(\min(\ell, m) - d(\mathcal{C}) + 1).$$

Codes where equality holds are called maximum rank distance (or MRD) codes.

The most famous construction of MRD codes is due to Gabidulin [5]. In this paper we define Gabidulin-like codes (Definition 2.5) which provide a unified framework of various generalisations of Gabidulin codes. Their basic properties are studied in Section 2, where we show that Gabidulin-like codes are MRD codes and provide a characterisation (as in [15]) which lifted codes are Gabidulin-like codes (Theorem 2.10). Section 3 then describes an algorithm to compute the automorphism group of rank metric codes which can also be used to test equivalence. Using the strategy of this algorithm we describe the automorphism groups of Gabidulin-like codes in Section 4. In the special case of classical Gabidulin codes of full length $m = \ell$ these groups have already been determined in [10] and [14].

2. Rank metric codes.

Let k be any field, $\ell, m \in \mathbb{N}$. To simplify notation we will always assume that $\ell \geq m > 0$.

Definition 2.1. *A linear rank metric code is a subspace $\mathcal{C}$ of $k^{\ell \times m}$. The minimum distance of $\mathcal{C}$ is $d(\mathcal{C}) = \min\{\mathrm{rk}(C) \mid 0 \neq C \in \mathcal{C}\}$.*

The following analogue of the classical Singleton bound is well known for rank metric codes ([3, Theorem 5.4], [4, Lemma 1]).

Proposition 2.2. *Let $\mathcal{C} \leq k^{\ell \times m}$ be a rank metric code of dimension d and minimum distance r. Then $d \leq \ell(m - r + 1)$. Codes that achieve equality are called* MRD codes (maximum rank distance codes).

Proof. Let π denote the projection of $k^{\ell \times m}$ onto $k^{\ell \times (m-r+1)}$ omitting the last $r - 1$ columns of any matrix. Then clearly the kernel of this projection consists of matrices of rank $\leq r - 1$. In particular the restriction of π to $\mathcal{C}$ is an injective mapping of $\mathcal{C}$ into a space of dimension $\ell(m - r + 1)$ thus

$$d = \dim(\mathcal{C}) = \dim(\pi(\mathcal{C})) \leq \ell(m - r + 1).$$

□

Clearly the dimension of a maximum rank distance code is always a multiple of ℓ but apart from this obvious restriction, MRD codes exist for all possible parameters, if k admits a cyclic field extension K of degree $\ell = [K : k]$ (see [6, Lemma 3.2] or Definition 2.5 below). These examples have the property that they are linear over the larger field. Until recently, [14], all known families of MRD codes arose from linear codes over some extension field K, so called lifted codes:

Definition 2.3. *Let K/k be a field extension of degree ℓ and $\tilde{\mathcal{C}} \le K^m$ a K-linear code of length m. Fix some basis $B = (B_1, \ldots, B_\ell) \in K^\ell$ of K over k. Then*

$$\epsilon_B : K \to k^{\ell\times 1}, \epsilon_B(\sum_{i=1}^{\ell} a_i B_i) = (a_1, \ldots, a_\ell)^{tr}$$

maps $\tilde{\mathcal{C}}$ to the lifted code

$$\mathcal{C} := \epsilon_B(\tilde{\mathcal{C}}) = \{(\epsilon_B(c_1), \ldots, \epsilon_B(c_m)) \mid (c_1, \ldots, c_m) \in \tilde{\mathcal{C}}\} \le k^{\ell\times m}.$$

The lifted codes (with respect to the chosen k-basis B of K) are exactly the codes $\mathcal{C} \le k^{\ell\times m}$ that are invariant under left multiplication with $\Delta_B(K) \le k^{\ell\times\ell}$, the regular representation of K with respect to B.

Remark 2.4. *The rank of $\epsilon_B((v_1, \ldots, v_m))$ equals the k-dimension of the subspace $\langle v_1, \ldots, v_m\rangle_k$ of K. Therefore we call this dimension also the rank of the vector $v = (v_1, \ldots, v_m) \in K^m$.*

The most well known construction of an MRD code as a lifted code is due to Gabidulin [5] (cf. [7] for a generalisation for finite fields and [1] for a generalisation to characteristic 0). All these constructions only depend on the fact that K/k is a cyclic Galois extension:

Definition 2.5. *Let K/k be a cyclic field extension of degree ℓ and θ a generator of* $\mathrm{Gal}(K/k)$. *For $v = (v_1, \ldots, v_m) \in K^m$ and any $1 \le d \le m-1$ we put*

$$\tilde{\mathcal{C}}(v, \theta, d) := \langle v, \theta(v), \ldots, \theta^{d-1}(v)\rangle_K \le K^m$$

where $\theta^j(v) = (\theta^j(v_1), \ldots, \theta^j(v_m))$ and

$$\mathcal{C}(v, \theta, d) := \epsilon_B(\tilde{\mathcal{C}}(v, \theta, d)) \le k^{\ell\times m}.$$

If the rank of v equals m, then v is called a Gabidulin vector and $\mathcal{C}(v, \theta, d)$ the Gabidulin-like code with parameters (v, θ, d).

It can easily be seen (see the proof of Theorem 2.10 below) that $\mathcal{C}(v, \theta, d)$ is not an MRD code, if v is not a Gabidulin vector.

The next key lemma provides the most important argument for the proofs below.

Lemma 2.6. *(cf.* [1, Theorem 1], [6, Lemma 3.2]*) Assume that* $\mathrm{Gal}(K/k) = \langle\theta\rangle$ *and let $p = \sum_{i=0}^{t} p_i x^i \in K[x]$ be a non-zero polynomial of degree t. Then the kernel of*

$$p(\theta) := \sum_{i=0}^{t} p_i\theta^i \in \mathrm{End}_k(K), \ \ \alpha \mapsto \sum_{i=0}^{t} p_i\theta^i(\alpha)$$

is a k-subspace of K of dimension at most t.

Proof. As θ is a generator of the Galois group of K/k the powers $(1, \theta, \ldots, \theta^{\ell-1}) \in \mathrm{End}_k(K)^\ell$ are linearly independent over K (see for instance the proof of Theorem (29.12) in [12]) and $\mathrm{End}_k(K)$ is a cyclic algebra

$$k^{\ell \times \ell} \cong \mathrm{End}_k(K) \cong \bigoplus_{i=0}^{\ell-1} K\theta^i.$$

Let $A := p(\theta)$, then $A, A\theta, \ldots, A\theta^{\ell-t-1}$ are linearly independent over K. So the k-dimension of $A\,\mathrm{End}_k(K)$ is at least $\ell(\ell - t)$. Therefore the rank of A is at least $\ell - t$ so the kernel of A has at most dimension t over k. □

Corollary 2.7. *If $v \in K^m$ has rank r then $(v, \theta(v), \ldots, \theta^{r-1}(v))$ are linearly independent over K.*

Proof. Assume that there are $a_0, \ldots, a_{r-1} \in K$ such that $\sum_{i=0}^{r-1} a_i\theta^i(v) = 0$. Put $p := \sum_{i=0}^{r-1} a_i x^i \in K[x]$. Then the kernel of $p(\theta)$ contains the subspace $\langle v_1, \ldots v_m\rangle_k \leq K$ of dimension r. As the degree of p is $\leq r - 1$ Lemma 2.6 implies that $p = 0$. □

Corollary 2.8. *Let $v \in K^m$ be a Gabidulin vector and $1 \leq d \leq m - 1$. Then*

$$\langle v\rangle_K = \theta^{1-d}(\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{C}}(v, \theta, d))).$$

In particular $\mathcal{C}(v, \theta, d) = \mathcal{C}(w, \theta, d)$ if and only if $v = \alpha w$ for some $0 \neq \alpha \in K$.

Proof. The inclusion $\subseteq$ is clear. So let $x \in \bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{C}}(v, \theta, d))$. By Corollary 2.7 the vectors $(v, \theta(v), \ldots, \theta^d(v))$ and hence also $(\theta^i(v), \theta^{i+1}(v), \ldots, \theta^{i+d}(v))$ are linearly independent over K (for all i). In particular there are unique $a_{i,j} \in K$ such that

$$x = \sum_{j=0}^{d-1} a_{i,j}\theta^{i+j}(v) \text{ for all } 0 \leq i \leq d - 1.$$

$$\text{So} \quad \begin{aligned} x &= a_{0,0}v + a_{0,1}\theta(v) + \ldots + a_{0,d-1}\theta^{d-1}(v) \\ &= \phantom{a_{0,0}v + {}} a_{1,0}\theta(v) + \ldots + a_{1,d-2}\theta^{d-1}(v) + a_{1,d-1}\theta^d(v) \end{aligned}$$

which shows that $a_{0,0} = 0$, $a_{0,1} = a_{1,0}$, …, $a_{0,d-1} = a_{1,d-2}$, $a_{1,d-1} = 0$ because $(v, \theta(v), \ldots, \theta^d(v))$ are linearly independent. Comparing the coefficients $a_{1,j}$ and $a_{2,j}$ we similarly find that $a_{1,0} = 0$, $a_{1,1} = a_{2,0}$, …, $(0 =)a_{1,d-1} = a_{2,d-2}$, $a_{2,d-1} = 0$. So recursively we find that $x = a_{0,d-1}\theta^{d-1}(v)$. □

Theorem 2.9. *Let $v = (v_1, \ldots, v_m) \in K^m$ be a Gabidulin vector. Then $\dim_k(\mathcal{C}(v, \theta, d)) = \ell d$ and $d(\mathcal{C}(v, \theta, d)) = m - d + 1$. In particular Gabidulin-like codes are* MRD codes.

Proof. It follows from Corollary 2.7 that $\dim_K(\tilde{\mathcal{C}}(v, \theta, d)) = d$. As ϵ_B is an isomorphism and $\dim_k(K) = \ell$, we get $\dim_k(\mathcal{C}(v, \theta, d)) = \ell d$. To obtain the

MRD property it suffices to show that any non zero $C \in \mathcal{C}(v,\theta,d)$ has rank $\mathrm{rk}(C) \geq m-(d-1)$. Let

$$0 \neq C = \epsilon_B(\sum_{i=0}^{d-1} a_i\theta^i(v)) \in \mathcal{C}(v,\theta,d).$$

Then the right kernel of C is

$$\{b=(b_1,\ldots,b_m)^{tr} \in k^{m\times 1} \mid Cb=0\} = \{b \in k^{m\times 1} \mid \sum_{i=0}^{d-1} a_i\theta^i(\sum_{j=1}^{m} b_jv_j)=0\}.$$

As $(v_1,\ldots,v_m)$ are linearly independent over k this right kernel is isomorphic to the kernel of the restriction of $\sum_{i=0}^{d-1} a_i\theta_i$ to $\langle v_1,\ldots,v_m\rangle_k$. By Lemma 2.6 the kernel of $\sum_{i=0}^{d-1} a_i\theta_i \in \mathrm{End}_k(K)$ has dimension at most $d-1$, so also the right kernel of C has dimension at most $d-1$ and hence $\mathrm{rk}(C) \geq m-(d-1)$. □

Theorem 2.10. *A lifted* MRD code $\mathcal{C} = \epsilon_B(\tilde{\mathcal{C}}) \leq k^{\ell\times m}$ with $\dim_K(\tilde{\mathcal{C}}) = d < m$ is a Gabidulin-like code if and only if

$$\dim_K(\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{C}})) = 1.$$

Proof. For Gabidulin-like codes the dimension of the intersection is 1 by Corollary 2.8. So it remains to show the converse direction: Assume that $\bigcap_{i=0}^{d-1}\theta^i(\tilde{\mathcal{C}}) = \langle x\rangle_K$. Then $x \in \theta^{d-1}(\tilde{\mathcal{C}})$, so there is a unique $v=(v_1,\ldots,v_m) \in \tilde{\mathcal{C}}$, such that

$$x = \theta^{d-1}(v) = \theta^{d-2}(\theta(v)) = \ldots = \theta(\theta^{d-2}(v)).$$

As $x = \theta^{d-i-1}(\theta^i(v)) \in \theta^{d-i-1}(\tilde{\mathcal{C}})$ for all $0 \leq i \leq d-1$ the injectivity of θ implies that $\theta^i(v) \in \tilde{\mathcal{C}}$ for all $0 \leq i \leq d-1$.
We now show that v has rank m. Assume that $\dim_k\langle v_1,\ldots,v_m\rangle = r < m$. Then there is some $h \in \mathrm{GL}_m(k)$ such that

$$(v_1,\ldots,v_m)h = (w_1,\ldots,w_r,0,\ldots,0).$$

Clearly $d(\mathcal{C}) = d(\mathcal{C}h)$. Let $w := (w_1,\ldots,w_r)$. Then w is a Gabidulin vector of length r and $\mathcal{C}h$ contains $(\mathcal{D}|0^{\ell\times(m-r)})$, where $\mathcal{D}$ is the Gabidulin code $\mathcal{D} = \mathcal{C}(w,\theta,d) \leq k^{\ell\times r}$ if $d \leq r-1$ and $\mathcal{D} = k^{\ell\times r}$ if $d \geq r$. In the first case $d(\mathcal{D}) = r-d+1 < m-d+1$ (because we assumed $r<m$) and $d(\mathcal{C}) = 1 < m-d+1$ (because $d<m$) in the second case. This contradicts the assumption that $\mathcal{C}$ is an MRD code.
So v is a Gabidulin vector and hence the subcode

$$\tilde{\mathcal{C}}(v,\theta,d) = \langle v,\theta(v),\ldots,\theta^{d-1}(v)\rangle$$

of $\tilde{\mathcal{C}}$ has dimension d, therefore $\tilde{\mathcal{C}} = \tilde{\mathcal{C}}(v,\theta,d)$. □

3. Computing automorphism groups of rank metric codes.

The k-linear rank distance preserving automorphisms of $k^{\ell\times m}$ are the maps

$$\kappa_{g,h} : X \mapsto g^{-1}Xh \text{ for } g \in \mathrm{GL}_\ell(k), h \in \mathrm{GL}_m(k)$$

(see [16, Theorem 3.4]) and, if $\ell = m$, also

$$X \mapsto g^{-1}X^{tr}h \quad (g \in \mathrm{GL}_\ell(k), h \in \mathrm{GL}_m(k)).$$

Two codes $\mathcal{C}$ and $\mathcal{D}$ in $k^{\ell\times m}$ are called (properly) equivalent, if $\mathcal{C} = g^{-1}\mathcal{D}h$ for some $g \in \mathrm{GL}_\ell(k), h \in \mathrm{GL}_m(k)$ and

$$\mathrm{Aut}(\mathcal{C}) := \{(g,h) \in \mathrm{GL}_\ell(k) \times \mathrm{GL}_m(k) \mid g^{-1}\mathcal{C}h = \mathcal{C}\}$$

is called the (proper) automorphism group of $\mathcal{C}$. Note that $\kappa_{g,h} = \kappa_{ag,ah}$ for all $0 \neq a \in k$, so that different automorphisms might induce the same mappings on $k^{\ell\times m}$.

The following definition is fundamental in our algorithm to compute rank metric automorphism groups.

Definition 3.1. *Let k be a field and $\mathcal{C} \leq k^{\ell\times m}$. The right and left idealiser of $\mathcal{C}$ are defined as*

$$R(\mathcal{C}) = \{Y \in k^{m\times m} \mid \mathcal{C}Y \subseteq \mathcal{C}\} \text{ and } L(\mathcal{C}) = \{X \in k^{\ell\times \ell} \mid X\mathcal{C} \subseteq \mathcal{C}\}.$$

Then clearly $R(\mathcal{C})$ and $L(\mathcal{C})$ are subalgebras of the full matrix algebra.

All lifted codes, in particular the Gabidulin-like codes from Definition 2.5, are invariant under left multiplication with the field K, or more precisely its image under the regular representation $\Delta_B(K) \leq k^{\ell\times\ell}$, so $\Delta_B(K) \leq L(\mathcal{C})$. Note that $K \cong \Delta_B(K)$ is a maximal subfield of the central-simple k-algebra $k^{\ell\times\ell}$. The following lemma is probably well known but crucial, as it gives us all possible left idealisers of such K-linear codes $\mathcal{C}$:

Lemma 3.2. *Let K be a field extension of degree ℓ over k and B some k-basis of K. Let A be a k-algebra with*

$$\Delta_B(K) \leq A \leq k^{\ell\times\ell}.$$

Then there is a subfield $k \leq F \leq K$ such that

$$A = C_{k^{\ell\times\ell}}(\Delta_B(F)) \cong F^{s\times s}$$

with $s = [K : F]$.

Proof. Let A be a subalgebra of $k^{\ell\times\ell}$ containing $\Delta_B(K)$. Then $k^{\ell\times 1}$ is a simple A-module, because it has no $\Delta_B(K)$-invariant submodules. Also $k^{\ell\times 1}$ is a faithful $k^{\ell\times\ell}$-module and hence also its annihilator in A is trivial, $\{a \in A \mid ak^{\ell\times 1} = \{0\}\} = \{0\}$. So A has a faithful simple module and hence is a simple k-algebra. Therefore A has the double-centraliser property $A = C_{k^{\ell\times\ell}}(C)$ for $C := C_{k^{\ell\times\ell}}(A)$ (see [12, Theorem 7.11]). Clearly

$$k \subseteq C \subseteq C_{k^{\ell\times\ell}}(\Delta_B(K)) = \Delta_B(K),$$

so $C = \Delta_B(F)$ for some subfield F of K and hence $A = C_{k^{\ell\times\ell}}(\Delta_B(F))$. $\square$

Corollary 3.3. *Let K/k be an extension of degree ℓ, $\mathcal{C} = \epsilon_B(\tilde{\mathcal{C}})$ be a lifted code for some K-linear code $\tilde{\mathcal{C}} \leq K^m$. Then there is a subfield F with $k \leq F \leq K$ such that*

$$L(\mathcal{C}) = C_{k^{\ell\times\ell}}(\Delta_B(F)) \cong F^{s\times s}$$

with $s = [K : F]$.

Let $R(\mathcal{C})^\times := R(\mathcal{C}) \cap \mathrm{GL}_m(k)$ and $L(\mathcal{C})^\times := L(\mathcal{C}) \cap \mathrm{GL}_\ell(k)$ denote the unit groups of right and left idealiser. We also let

$$\begin{array}{ll} N(R(\mathcal{C})) := & \{h \in \mathrm{GL}_m(k) \mid h^{-1}R(\mathcal{C})h = R(\mathcal{C})\} \text{ and} \\ N(L(\mathcal{C})) := & \{g \in \mathrm{GL}_\ell(k) \mid g^{-1}L(\mathcal{C})g = L(\mathcal{C})\}. \end{array}$$

Clearly $R(\mathcal{C})^\times \leq N(R(\mathcal{C}))$ and $L(\mathcal{C})^\times \leq N(L(\mathcal{C}))$. The algorithm described below only applies to rank metric codes for which one of the indices is finite. Note that this is always the case if k is a finite field, but also for all lifted codes. In this case let

$$n(\mathcal{C}) := \gcd\{[N(R(\mathcal{C})) : R(\mathcal{C})^\times], [N(L(\mathcal{C})) : L(\mathcal{C})^\times]\}$$

denote the greatest common divisor of these two indices. Let

$$\begin{array}{lll} \pi_1 : & \mathrm{GL}_\ell(k) \times \mathrm{GL}_m(k) \to \mathrm{GL}_\ell(k), & (g,h) \mapsto g \\ \pi_2 : & \mathrm{GL}_\ell(k) \times \mathrm{GL}_m(k) \to \mathrm{GL}_m(k), & (g,h) \mapsto h \end{array}$$

denote the projections onto the first and second component.

Theorem 3.4. *For the automorphism group $\mathrm{Aut}(\mathcal{C})$ one has*

$$L(\mathcal{C})^\times \times R(\mathcal{C})^\times \leq \mathrm{Aut}(\mathcal{C}) \leq N(L(\mathcal{C})) \times N(R(\mathcal{C}))$$

more precisely

$$\mathrm{Aut}(\mathcal{C}) = \{(g,h) \in N(L(\mathcal{C})) \times N(R(\mathcal{C})) \mid g^{-1}\mathcal{C}h = \mathcal{C}\}.$$

Moreover $\pi_1(\mathrm{Aut}(\mathcal{C}))/L(\mathcal{C})^\times \cong \pi_2(\mathrm{Aut}(\mathcal{C}))/R(\mathcal{C})^\times$. In particular the order of the factor group $\mathrm{Aut}(\mathcal{C})/(L(\mathcal{C})^\times \times R(\mathcal{C})^\times)$ divides $n(\mathcal{C})$.

Proof. The first two statements are clear, we only need to prove the isomorphism (which is also a standard argument): By abuse of notation we denote by π_i the restriction of π_i to $G := \mathrm{Aut}(\mathcal{C})$ and put $L := L(\mathcal{C})^\times$ and $R := R(\mathcal{C})^\times$. Then

$$L \cong \{(g,1) \mid g \in L\} = \ker(\pi_2) \text{ and } R \cong \{(1,h) \mid h \in R\} = \ker(\pi_1).$$

Define the two group epimorphisms

$$\overline{\pi_1} : G \to \pi_1(G)/L, (g,h) \mapsto g \cdot L \text{ and } \overline{\pi_2} : G \to \pi_2(G)/R, (g,h) \mapsto h \cdot R.$$

Then $\ker(\overline{\pi_1}) = \ker(\overline{\pi_2}) = L \times R$ and hence

$$N(L(\mathcal{C}))/L \geq \pi_1(G)/L \cong G/(R \times L) \cong \pi_2(G)/R \leq N(R(\mathcal{C}))/R.$$

In particular $G/(R \times L)$ is isomorphic to a subgroup of $N(L(\mathcal{C}))/L$ and $N(R(\mathcal{C}))/R$, therefore its order divides the order of both factor groups. □

To compute $\mathrm{Aut}(\mathcal{C})$ we first compute $L(\mathcal{C})$ and $R(\mathcal{C})$ as the intersection of two subspaces. More general for $\mathcal{C},\mathcal{D} \le k^{\ell\times m}$ put

$$L(\mathcal{C},\mathcal{D}) := \{X \in k^{\ell\times\ell} \mid X\mathcal{C} \subseteq \mathcal{D}\} \text{ and } R(\mathcal{C},\mathcal{D}) := \{Y \in k^{m\times m} \mid \mathcal{C}Y \subseteq \mathcal{D}\}.$$

Lemma 3.5. *For $\mathcal{C},\mathcal{D} \le k^{\ell\times m}$ the spaces $L(\mathcal{C},\mathcal{D})$ and $R(\mathcal{C},\mathcal{D})$ can be computed by linear algebra methods as the intersection of two subspaces.*

Proof. We identify

$$k^{\ell\times m} \cong k^{\ell} \otimes k^{m} \cong k^{\ell m}.$$

The linear mappings of this ℓm-dimensional vector space induced by left multiplication by elements in $k^{\ell\times\ell}$ form the subalgebra

$$A := k^{\ell\times\ell} \otimes k \le k^{\ell\times\ell} \otimes k^{m\times m} \cong k^{\ell m\times\ell m}$$

and similarly those induced by right multiplication

$$B := k \otimes k^{m\times m} \le k^{\ell\times\ell} \otimes k^{m\times m} \cong k^{\ell m\times\ell m}.$$

Identifying $\mathcal{C}$ and $\mathcal{D}$ with the corresponding subspaces of $k^{\ell m}$ one easily computes the subspace

$$LR(\mathcal{C},\mathcal{D}) := \{X \in k^{\ell m\times\ell m} \mid \mathcal{C}X \subseteq \mathcal{D}\}.$$

Then bases of

$$L(\mathcal{C},\mathcal{D}) = A \cap LR(\mathcal{C},\mathcal{D}) \text{ and } R(\mathcal{C},\mathcal{D}) = B \cap LR(\mathcal{C},\mathcal{D})$$

can be computed using Zassenhaus' algorithm for computing intersections of subspaces. □

In general normalisers of subalgebras are hard to compute. However, at least for finite fields, there are fast algorithms to compute the normaliser of a subgroup of the general linear group [13]. Clearly $N(L(\mathcal{C})) \le N_{\mathrm{GL}_\ell(k)}(L(\mathcal{C})^\times)$ with equality if $L(\mathcal{C})$ is generated by its unit group. The same holds for $N(R(\mathcal{C}))$.

For lifted codes, we always have $L(\mathcal{C}) \cong F^{s\times s}$ for some $k \le F \le K$ and hence

$$N(L(\mathcal{C})) = N_{\mathrm{GL}_\ell(k)}(L(\mathcal{C})^\times) \cong \mathrm{GL}_s(F).\,\mathrm{Gal}(F/k).$$

From now on we assume that we know one of $N(L(\mathcal{C}))$ and $N(R(\mathcal{C}))$. If both are known, then we choose the one $(X = L, R)$ for which the index $[N(X(\mathcal{C})) : X(\mathcal{C})^\times]$ is smaller. To ease notation assume that $X = L$. Let

$$N(L(\mathcal{C})) = \dot\cup_{j=1}^{n} t_j L(\mathcal{C})^\times.$$

Put $J := \{\}$. For every $j = 1, \ldots, n$ we compute $R(t_j\mathcal{C},\mathcal{C})$ as described above. If this space contains an invertible matrix s_j then put $J := J \cup \{(t_j, s_j)\}$.

Now Theorem 3.4 implies that we obtain a generating set of the automorphism group as follows.

Theorem 3.6. *Let R respectively L be generating sets of $R(\mathcal{C})^\times$ respectively $L(\mathcal{C})^\times$ and J, s_j, t_j be as above. Then*

$$\mathrm{Aut}(\mathcal{C}) = \langle (g,1), (1,h), (t_j,s_j) \mid g \in L, h \in R, (t_j,s_j) \in J\rangle.$$

A similar strategy can be used to compute equivalences between rank metric codes.

4. Automorphism groups of Gabidulin-like codes

In the whole section we assume that K/k is a cyclic extension of degree ℓ and choose a generator θ of the Galois group $\mathrm{Gal}(K/k)$. For k-linearly independent $v := (v_1, \dots, v_m) \in K^m$ and $0 \leq d < m$ the Gabidulin-like code $\mathcal{C}(v, \theta, d) := \epsilon_B(\langle v, \theta(v), \dots, \theta^{d-1}(v)\rangle_K)$ is defined in Definition 2.5.

To compute the right idealiser (cf. Definition 3.1) of a Gabidulin-like code $\mathcal{C}(v, \theta, d)$ we define

$$V_v := \langle v_1, \dots, v_m \rangle_k \leq K$$

to be the k-subspace of K generated by the entries of the Gabidulin vector $v = (v_1, \dots, v_m)$. This is an m-dimensional k-linear subspace of K.

Lemma 4.1. *([9, IV.4] for finite fields) Let $k \leq M \leq K$ be the maximal subfield of K such that V_v is an M-linear subspace of K. Then $R(\mathcal{C}(v, \theta, d)) \cong M$ for all $0 < d < m$.*

Proof. Let $0 \neq Y \in k^{m \times m}$ such that $\mathcal{C}(v, \theta, d)Y \subseteq \mathcal{C}(v, \theta, d)$. Then by Corollary 2.8

$$\langle vY \rangle_K = \theta^{1-d}(\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{C}}(v, \theta, d)Y)) \subseteq \langle v \rangle_K$$

so there is some $\alpha \in K$ such that $vY = \alpha v$. Moreover $vY \in V_v$ because the entries of Y are in k. So $\alpha \in M$. □

To compute the left idealiser we introduce the splitting field of a Gabidulin-like code.

Definition 4.2. *Let $\tilde{\mathcal{C}} \leq K^m$ be a Gabidulin-like code. The smallest subfield $k \leq F \leq K$ such that there exists a subspace $\tilde{\mathcal{D}} \leq F^m$ satisfying*

$$\tilde{\mathcal{C}} = \tilde{\mathcal{D}} \otimes_F K$$

is called the splitting field of $\tilde{\mathcal{C}}$.

Lemma 4.3. *Let $\tilde{\mathcal{C}} \leq K^m$ be a Gabidulin-like code with splitting field F and let $\tilde{\mathcal{D}} \leq F^m$ with $\tilde{\mathcal{C}} = \tilde{\mathcal{D}} \otimes_F K$. Then $\tilde{\mathcal{D}}$ is also a Gabidulin-like code.*

Proof. Let $x \in \tilde{\mathcal{D}}$. Then the rank of $x \in F^m$ equals the rank of $x \otimes 1 \in (F \otimes_F K)^m$. As $\tilde{\mathcal{C}}$ is an MRD code, so is $\tilde{\mathcal{D}}$. Now let $d = \dim_K(\tilde{\mathcal{C}}) = \dim_F(\tilde{\mathcal{D}})$. As the intersection of vector spaces commutes with the tensor product and K is fixed (as a set) by all powers of θ, we get

$$\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{C}}) = \left(\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{D}})\right) \otimes_F K.$$

Applying Theorem 2.10 the intersection on the left hand side has $K-$dimension 1. Thus the intersection $\bigcap_{i=0}^{d-1} \theta^i(\tilde{\mathcal{D}})$ has $F-$dimension 1 and as $\tilde{\mathcal{D}}$ is an MRD code, Theorem 2.10 implies that $\tilde{\mathcal{D}}$ is a Gabidulin-like code. □

The next lemma allows us to compute the splitting field using only the Gabidulin vector. Note that the extension F/k is also cyclic and $\mathrm{Gal}(F/k)$ is generated by $\theta_{|F}$.

Proposition 4.4. *Let $\tilde{\mathcal{C}} \leq K^m$ be a Gabidulin-like code with splitting field F and Gabidulin vector v normalised so that $v_1 = 1$. Then $F = k[v_2, \dots, v_m]$.*

Proof. Let $F' := k[v_2, \dots, v_m]$, F the splitting field of $\tilde{\mathcal{C}}$ and $d := \dim_K(\tilde{\mathcal{C}})$. Let $w \in F^m$ be the normalised Gabidulin vector of $\tilde{\mathcal{D}} \leq F^m$ and set $w' := w \otimes_F 1 \in \tilde{\mathcal{C}}$. Then w' has rank m and $\theta^i(w') \in \tilde{\mathcal{C}}$ for all $0 \leq i \leq d-1$. So w' is a Gabidulin vector for $\tilde{\mathcal{C}}$ and thus by Corollary 2.8 a multiple of v. As both vectors are normalised we get $v = w'$, which gives us $F' \leq F$.
For the other direction define $\tilde{\mathcal{D}} := \tilde{\mathcal{C}}(v, \theta_{|F'}, d) \leq (F')^m$ by interpreting v as an element of $(F')^m$. Then $\tilde{\mathcal{C}} = \tilde{\mathcal{D}} \otimes_{F'} K$ and the minimality of the splitting field gives us $F \leq F'$. □

If we take a Gabidulin-like code $\tilde{\mathcal{C}} = \tilde{\mathcal{D}} \otimes_F K$ with splitting field F and a basis B adjusted to the decomposition $K = F \otimes_F K$, we get

$$\mathcal{C} = \mathcal{D}^{s \times 1}$$

where $s = [K : F]$. This allows us to compute the left idealiser.

Theorem 4.5. *Let $\mathcal{C}(v, \theta, d)$ be a Gabidulin-like code with splitting field $F \leq K$. Then*

$$L(\mathcal{C}(v, \theta, d)) = C_{k^{\ell \times \ell}}(\Delta_B(F)) \cong F^{s \times s}$$

(with $s = [K : F]$).

Proof. We can change B to fit the decomposition $K = F \otimes_F K$ as mentioned above. Then $\mathcal{D}^{s \times 1}$ is a $F^{s \times s}$-module. For the other direction of the equality we use Corollary 3.3. As we always have $\Delta_B(K) \leq L(\mathcal{C}(v, \theta, d))$, there is some field F' such that $L(\mathcal{C}(v, \theta, d)) \cong (F')^{s' \times s'}$ where $s' = [K : F']$. Then $\mathcal{C}$ is equivalent to $(\mathcal{D}')^{s' \times 1}$ for some $\mathcal{D}'$ as these are the only $(F')^{s' \times s'}$-modules. The minimality of the splitting field now gives us $F = F'$. □

Putting together all the results of this section, we now obtain the following structure of the automorphism group of Gabidulin-like codes:

Theorem 4.6. *Let $v = (v_1, \dots, v_m) \in K^m$ be a Gabidulin vector normalised so that $v_1 = 1$. Let $k \leq M \leq K$ be the maximal subfield of K such that*

$$V_v := \langle v_1, \dots, v_m \rangle_k \leq K$$

is an M-linear subspace of K. Let $F = k[v_2, \dots, v_m]$ be the minimal subfield of K that contains V_v and $s := [K : F]$. Then there is a subgroup $G \leq$ $\mathrm{Gal}(F/k) = \langle \theta_{|F} \rangle$ such that for any $1 \leq d < m$

$$\mathrm{Aut}(\mathcal{C}(v, \theta, d)) \cong (\mathrm{GL}_s(F) \times M^\times).G.$$

References

[1] D. Augot, P. Loidreau, and G. Robert, Rank metric and Gabidulin codes in characteristic zero. ISIT 2013 IEEE International Symposium on Information Theory, Jul 2013, Istanbul, Turkey. 2013

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

[3] Ph. Delsarte, Bilinear forms over a finite field with applications to coding theory. J. Comb. Theory A, 25 (1978) 226-241.

[4] J-G. Dumas, R. Gow, G. McGuire, J. Sheekey, Subspaces of matrices with special rank properties. Linear Algebra Appl. 433 (2010) 191-202.

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

[6] R. M. Guralnick, Invertible preservers and algebraic groups. Proceedings of the 3rd ILAS Conference (Pensacola, FL, 1993). Linear Algebra Appl. 212/213 (1994) 249-257.

[7] A. Kshevetskiy and E. Gabidulin, The new construction of rank codes. In Proceedings of the International Symposium of Information Theory (ISIT) 2005, 2105-2108.

[8] R. Kötter, F.R. Kschischang, Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory 54 (2008) 3579–3591.

[9] K. Morrison, Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes. IEEE Transactions on Information Theory 60 (2014) 7035-7046.

[10] G. Nebe, W. Willems, On self-dual MRD codes. (to appear in Advances in Mathematics of Communication 2016)

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

[12] I. Reiner, Maximal orders. LMS Monographs 28. The Clarendon Press, Oxford University Press, Oxford, 2003

[13] C. M. Roney-Dougal, Conjugacy of subgroups of the general linear group. Experiment. Math. 13 (2004) 151-163.

[14] J. Sheekey, A new family of linear maximum rank distance codes. arXiv:1504.01581

[15] A.-L. Horlemann-Trautmann and K. Marshall, New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions. arXiv:1507.08641

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