List-Decoding Gabidulin Codes via Interpolation and the Euclidean Algorithm

Margreta Kuijper and Anna-Lena Trautmann
Department of Electrical and Electronic Engineering, University of Melbourne, Australia.

***Abstract*—We show how Gabidulin codes can be list decoded by using a parametrization approach. For this we consider a certain module in the ring of linearized polynomials and find a minimal basis for this module using the Euclidean algorithm with respect to composition of polynomials. For a given received word, our decoding algorithm computes a list of all codewords that are closest to the received word with respect to the rank metric.**

I. Introduction

Gabidulin codes are a family of optimal rank-metric codes, useful in different fields of coding theory, e.g. in (random) linear network coding [19], space-time coding [10], crisscoss error correction [14] and distributed storage [17]. They were first derived by Gabidulin in [3] and independently by Delsarte in [2]. These codes can be seen as the q-analog of Reed-Solomon codes, using q-linearized polynomials instead of arbitrary polynomials over the finite field $\mathbb{F}_q$ (where q is a prime power). They are optimal in the sense that they are not only MDS codes with respect to the Hamming metric, but also achieve the Singleton bound with respect to the rank metric and are thus MRD codes.

There has been a rising interest in the last decade due to their application in network coding [5], [19]. Since then a lot of work has been done on how to decode these codes. The question of minimum distance decoding inside the unique decoding radius has been addressed e.g. in [3], [4], [9], [13], [15], [16], [20], whereas the more general setting of list decoding, beyond the unique decoding radius, is investigated in e.g. [8], [11], [22], [23]. Related work on list-decoding lifted Gabidulin codes can be found in [21].

In this work we explore list decoding further and, in contrast to the Sudan-Guruswami approach of [11], [22], present a parametric approach analogous to the one for list decoding Reed-Solomon codes from [1]. In a similar way as [9] we use interpolation, however unlike [9] we perform list decoding rather than unique decoding. A difference between our paper and the papers [9], [23] is that our approach is based on the Euclidean algorithm. A more important difference with [23] is that our decoding method yields all closest codewords, rather than just one. The latter is due to our parametrization approach.

The paper is structured as follows: In the following section we introduce q-linearized polynomials, Gabidulin codes, the rank metric and state some known properties of those. Moreover we explain the error span polynomial and recall the interpolation based unique decoding set-up for Gabidulin codes from [9]. In Section III we derive the module of q-linearized polynomials containing all those polynomials that interpolate the received word and show that finding all elements of this module fulfilling certain requirements is equivalent to list decoding with respect to the rank metric. In Section IV we describe a list decoding algorithm based on the previously described interpolation module using the Euclidean algorithm for q-linearized polynomials. We conclude this paper in Section V.

II. Preliminaries

Let q be a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. It is well-known that there always exists a primitive element α of the extension field $\mathbb{F}_{q^m}$, such that $\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha]$. Moreover, $\mathbb{F}_{q^m}$ is isomorphic (as a vector space) to the vector space $\mathbb{F}_q^m$. If not noted differently we will use the isomorphism

$$\begin{aligned} \mathbb{F}_q^m &\longrightarrow \mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha] \\ (v_1, \dots, v_m) &\longmapsto \sum_{i=1}^m v_i \alpha^{i-1}. \end{aligned}$$

One then easily gets the isomorphic description of matrices over the base field $\mathbb{F}_q$ as vectors over the extension field, i.e. $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$. Since we will work with matrices over different underlying fields we denote the rank of a matrix X over $\mathbb{F}_q$ by $\mathrm{rank}_q(X)$.

For some vector $(v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$ we denote the $k \times n$ *Moore matrix* by

$$M_k(v_1, \dots, v_n) := \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ v_1^{[1]} & v_2^{[1]} & \dots & v_n^{[1]} \\ \vdots & & & \\ v_1^{[k-1]} & v_2^{[k-1]} & \dots & v_n^{[k-1]} \end{pmatrix},$$

where $[i] := q^i$. A *q-linearized polynomial* over $\mathbb{F}_{q^m}$ is defined to be of the form

$$f(x) = \sum_{i=0}^n a_i x^{[i]} \quad , \quad a_i \in \mathbb{F}_{q^m},$$

where n is called the *q-degree* of $f(x)$, assuming that $a_n \neq 0$, denoted by $\mathrm{qdeg}(f)$. This class of polynomials was first studied by Ore in [12]. One can easily check that

ALT is also with the Department of Electrical and Computer Systems Engineering, Monash University. She was supported by Swiss National Science Foundation Fellowship no. 147304.

$f(x_1 + x_2) = f(x_1) + f(x_2)$ and $f(\lambda x_1) = \lambda f(x_1)$ for any $x_1, x_2 \in \mathbb{F}_{q^m}$ and $\lambda \in \mathbb{F}_q$, hence the name *linearized*. The set of all q-linearized polynomials over $\mathbb{F}_{q^m}$ is denoted by $\mathcal{L}_q(x, q^m)$. This set forms a non-commutative ring with the normal addition $+$ and composition $\circ$ of polynomials. Because of the non-commutativity, products and quotients of elements of $\mathcal{L}_q(x, q^m)$ have to be specified as being "left" or "right" products or quotients. To not be mistaken with the standard division, we call the inverse of the composition *symbolic division*. I.e. $f(x)$ is symbolically divisible on the right by $g(x)$ with quotient $m(x)$ if

$$g(x) \circ m(x) = g(m(x)) = f(x).$$

Efficient algorithms for all these operations (left and right symbolic multiplication and division) exist and can be found e.g. in [5].

Lemma 1 (cf. [7] Thm. 3.50)**.** *Let $f(x) \in \mathcal{L}_q(x, q^m)$ and $\mathbb{F}_{q^s}$ be the smallest extension field of $\mathbb{F}_{q^m}$ that contains all roots of $f(x)$. Then the set of all roots of $f(x)$ forms a $\mathbb{F}_q$-linear vector space in $\mathbb{F}_{q^s}$.*

Lemma 2 ([7] Thm. 3.52)**.** *Let U be a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$. Then $\prod_{\beta \in U}(x - \beta)$ is an element of $\mathcal{L}_q(x, q^m)$.*

Note that, if $\beta_1, \dots, \beta_t$ is a basis of U, one can rewrite

$$\prod_{\beta \in U}(x - \beta) = \lambda \det(M_{t+1}(\beta_1, \dots, \beta_t, x))$$

for some constant $\lambda \in \mathbb{F}_{q^m}$.

Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. We define a *Gabidulin code* $C \subseteq \mathbb{F}_{q^m}^n$ as the linear block code with generator matrix $M_k(g_1, \dots, g_n)$. Using the isomorphic matrix representation we can interpret C as a matrix code in $\mathbb{F}_q^{m \times n}$.The *rank distance* d_R on $\mathbb{F}_q^{m \times n}$ is defined by

$$d_R(X, Y) := \mathrm{rank}_q(X - Y) \quad , \quad X, Y \in \mathbb{F}_q^{m \times n}$$

and analogously for the isomorphic extension field representation. It holds that the code C constructed before has dimension k over $\mathbb{F}_{q^m}$ and minimum rank distance (over $\mathbb{F}_q$) $n - k + 1$. One can easily see by the shape of the parity check and the generator matrices that an equivalent definition of the code is

$$C = \{(f(g_1), \dots, f(g_n)) \in \mathbb{F}_{q^m}^n \mid f(x) \in \mathcal{L}_q(x, q^m)_{<k}\},$$

where $\mathcal{L}_q(x, q^m)_{<k} := \{f(x) \in \mathcal{L}_q(x, q^m), \mathrm{qdeg}(f(x)) < k\}$. For more information on bounds and constructions of rank-metric codes the interested reader is referred to [3].

Consider a received word $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{F}_{q^m}^n$ as the sum $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} = (c_1, \dots, c_n) \in C$ is a codeword and $\mathbf{e} = (e_1, \dots, e_n) \in \mathbb{F}_{q^m}^n$ is the error vector. The following statement was formulated in a similar, but less general, manner in Theorem 1 in [9].

Theorem 3. *Let $f(x) \in \mathcal{L}_q(x, q^m), \mathrm{qdeg}(f(x)) < k$ and $c_i = f(g_i)$ for $i = 1, \dots, n$. It holds that $d_R(\mathbf{c}, \mathbf{r}) = t$ if and only if there exists a $D(x) \in \mathcal{L}_q(x, q^m)$, such that $\mathrm{qdeg}(D(x)) = t$ and*

$$D(r_i) = D(f(g_i)) \quad \forall i \in \{1, \dots, n\}.$$

Furthermore, this $D(x)$ is unique.

Proof: Let $D(x) \in \mathcal{L}_q(x, q^m)$ such that $D(r_i) = D(f(g_i))$ and $\mathrm{qdeg}(D(x)) = t$. This implies that $D(r_i - f(g_i)) = 0$ for all i. Define $e_i := r_i - f(g_i)$, then $e_i \in \mathbb{F}_{q^m}$ and every element of $\langle e_1, \dots, e_n \rangle$ is a root of $D(x)$ (see Lemma 1). Since $D(x)$ is non-zero and has degree q^t, it follows that the linear space of roots has q-dimension t, which implies that $(e_1, \dots, e_n)$ has rank t. This means that the rank distance between $(c_1, \dots, c_n)$ and $(r_1, \dots, r_n)$ is equal to t. Thus, one direction is proven.

For the other direction let $(c_1, \dots, c_n), (r_1, \dots, r_n)$ have rank distance t, i.e. $(e_1, \dots, e_n) := (c_1 - r_1, \dots, c_n - r_n)$ has rank t. Then by Lemma 2 there exists a non-zero $D(x) \in \mathcal{L}_q(x, q^m)$ of degree q^t such that $D(e_i) = 0$ for all i. By linearity we get that $D(c_i) = D(r_i)$ for $i = 1, \dots, n$. Since we know that $c_i = f(g_i)$, the statement follows. The uniqueness of $D(x) = \prod_{\beta \in \langle e_1, \dots, e_n \rangle}(x - \beta)$ follows from the fact that its degree is equal to the number of its distinct roots. ■

Remark 4. The previous theorem states that the roots of $D(x)$ form a vector space of degree t which is equal to the span of $e_1, \dots, e_n$. This is why $D(x)$ is also called the *error span polynomial* (cf. e.g. [18]). The analogy in the classical Hamming metric set-up is the *error locator polynomial*, whose roots indicate the locations of the errors, and whose degree equals the number of errors.

The interpolation-based unique decoding algorithm for Gabidulin codes from Loidreau [9] can now be formulated as follows. Assume that $\mathrm{rank}_q(\mathbf{e}) = d_R(\mathbf{c}, \mathbf{r}) < d_R(C)/2$, i.e. that $\mathbf{r}$ is within the unique decoding radius. Find all pairs $(N(x), D(x)) \in \mathcal{L}_q(x, q^m)^2$ with $\mathrm{qdeg}(N) < k + \mathrm{rank}_q(\mathbf{e}) \leq (n+k)/2$ and $\mathrm{qdeg}(D(x)) \leq (n-k)/2$, and check if $N(x)$ is symbolically divisible on the right by $D(x)$. If such a couple is found, then $D(x)$ is a valid error span polynomial by Theorem 3, and the symbolic quotient of $N(x)$ and $D(x)$ is the q-linearized polynomial that corresponds to the sent message.

In the next section we move beyond the unique decoding of [9] and describe an interpolation-based decoding algorithm that is able to find all closest codewords, within or beyond the unique decoding radius.

III. The Interpolation Module

For the rest of the paper let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and let $M_k(g_1, \dots, g_n)$ be the generator matrix of the Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$. Let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{F}_{q^m}^n$ be the received word.

For our following investigations we need a q-linearized analog of the Lagrange polynomial.

Definition 5. Let $\mathbf{g} = (g_1, \dots, g_n)$ and define the matrix $\mathfrak{D}_i(\mathbf{g}, x) := M_n(g_1, \dots, g_n, x)$ without the i-th column. We define the *q-Lagrange polynomial* as

$$\Lambda_{\mathbf{g},\mathbf{r}}(x) := \sum_{i=1}^{n}(-1)^{n-i} r_i \frac{\det(\mathfrak{D}_i(\mathbf{g}, x))}{\det(M_n(\mathbf{g}))} \quad \in \mathbb{F}_{q^m}[x].$$

Lemma 6. *Consider the setting of the previous definition. Then $\Lambda_{\mathbf{g},\mathbf{r}}(x) \in \mathcal{L}_q(x, q^m)$, i.e. it is q-linearized. Moreover, $\Lambda_{\mathbf{g},\mathbf{r}}(g_i) = r_i$ for $i = 1, \dots, n$ and $\operatorname{qdeg}(\Lambda_{\mathbf{g},\mathbf{r}}(x)) = n - 1$.*

Proof: Since $\det(\mathfrak{D}_i(\mathbf{g}, x))$ is q-linearized and $\Lambda_{\mathbf{g},\mathbf{r}}(x)$ is the sum of scalar multiples of these determinants, $\Lambda_{\mathbf{g},\mathbf{r}}(x)$ is also q-linearized. One can easily check that $\det(\mathfrak{D}_i(\mathbf{g}, x)) = (-1)^{n-i} \det(M_n(\mathbf{g}))$ for $x = g_i$ and $\det(\mathfrak{D}_i(\mathbf{g}, x)) = 0$ for $x = g_j$ where $j \neq i$. Hence for $x = g_i$ all but the i-th summand are zero and the i-th summand is equal to r_i. ■

Furthermore we need the following fact.

Lemma 7. *Let $L(x) \in \mathcal{L}_q(x, q^m)$, such that $L(g_i) = 0$ for all i. Then*

$$\exists H(x) \in \mathcal{L}_q(x, q^m) : L(x) = H(x) \circ \prod_{\alpha \in \langle g_1, \dots, g_n \rangle} (x - \alpha).$$

Proof: We know from Lemma 2 that $\prod_{\alpha \in \langle g_1, \dots, g_n \rangle}(x - \alpha) \in \mathcal{L}_q(x, q^m)$. Moreover there always exists unique left and right division in $\mathcal{L}_q(x, q^m)$, i.e. in this case there exist unique polynomials $H(x), R(x) \in \mathcal{L}_q(x, q^m)$ such that $L(x) = H(x) \circ \prod_{\alpha \in \langle g_1, \dots, g_n \rangle}(x - \alpha) + R(x)$ and $\operatorname{qdeg}(R(x)) < \operatorname{qdeg} \prod_{\alpha \in \langle g_1, \dots, g_n \rangle}(x - \alpha) = n$. Since any $\alpha \in \langle g_1, \dots, g_n \rangle$ is a root of $L(x)$ and of $\prod_{\alpha \in \langle g_1, \dots, g_n \rangle}(x - \alpha)$, they must also be a root of $R(x)$. Hence we have q^n distinct roots for $R(x)$ and $\deg(R) < q^n$, thus $R(x) \equiv 0$ and the statement follows. ■

In the following we abbreviate the row span of a (polynomial) matrix A by $\operatorname{rs}(A)$.

Definition 8. Define the polynomials $\Pi(x) := \prod_{\alpha \in \langle g_1, \dots, g_n \rangle}(x - \alpha)$ and $\Lambda_{\mathbf{g},\mathbf{r}}(x)$ as the q-Lagrange polynomial, such that $\Lambda_{\mathbf{g},\mathbf{r}}(g_i) = r_i$ for all i. Furthermore define the left submodule of $\mathcal{L}_q(x, q^m)$

$$\mathfrak{M}(\mathbf{r}) := \operatorname{rs} \begin{bmatrix} \Pi(x) & 0 \\ -\Lambda_{\mathbf{g},\mathbf{r}}(x) & x \end{bmatrix}.$$

We call $\mathfrak{M}(\mathbf{r})$ the *interpolation module* for $\mathbf{r}$.

Definition 9. We define the (k_1, k_2)*-weighted q-degree* of $[f(x) \quad g(x)] \in \mathfrak{M}(\mathbf{r})$ as $\max\{k_1 + \operatorname{qdeg}(f), k_2 + \operatorname{qdeg}(g)\}$.

We identify any $[f(x) \quad g(x)] \in \mathfrak{M}(\mathbf{r})$ with the bivariate linearized q-polynomial $Q(x, y) = f(x) + g(y)$. We will now show that the name interpolation module is justified for $\mathfrak{M}(\mathbf{r})$.

Theorem 10. *$\mathfrak{M}(\mathbf{r})$ consists exactly of all $Q(x, y) = f(x) + g(y)$ with $f(x), g(x) \in \mathcal{L}_q(x, q^m)$, such that $Q(g_i, r_i) = 0$ for $i = 1, \dots, n$.*

Proof: For the first direction let $Q(x, y) = f(x) + g(y)$ be an element of $\mathfrak{M}(\mathbf{r})$. Then there exist $a(x), b(x) \in \mathcal{L}_q(x, q^m)$ such that $f(x) = a(x) \circ \Pi(x) - b(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x)$ and $b(x) = g(x)$, thus $Q(g_i, r_i) = a(\Pi(g_i)) - b(\Lambda_{\mathbf{g},\mathbf{r}}(g_i)) + b(r_i) = 0 - b(r_i) + b(r_i) = 0$.

For the other direction let $f(x), g(x) \in \mathcal{L}_q(x, q^m)$ be such that $Q(g_i, r_i) = f(g_i) + g(r_i) = 0$ for $i = 1, \dots, n$. To show that $Q(x, y) \in \mathfrak{M}(\mathbf{r})$ we need to find $a(x) \in \mathcal{L}_q(x, q^m)$ such that

$$a(x) \circ \Pi(x) - b(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x) = f(x) \quad \text{and} \quad b(x) = g(x).$$

We substitute the second into the first equation to get

$$a(x) \circ \Pi(x) = f(x) + g(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x). \tag{1}$$

By assumption it holds that $f(g_i) + g(\Lambda_{\mathbf{g},\mathbf{r}}(g_i)) = f(g_i) + g(r_i) = 0$ for all i. Then, by Lemma 7, it follows that $f(x) + g(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x)$ is symbolically divisible on the right by $\Pi(x)$ and hence there exists $a(x) \in \mathcal{L}_q(x, q^m)$ such that (1) holds. ■

Combining all the previous results we get a description of all codewords with distance t to the received word in the new parametrization:

Theorem 11. *The elements $[N(x) \quad -D(x)]$ of $\mathfrak{M}(\mathbf{r})$ that fulfill*

1) *$\operatorname{qdeg}(N(x)) \leq t + k - 1$,*
2) *$\operatorname{qdeg}(D(x)) = t$,*
3) *$N(x)$ is symbolically divisible on the right by $D(x)$, i.e. there exists $f(x) \in \mathcal{L}_q(x, q^m)$ such that $D(f(x)) = N(x)$,*

are in one-to-one correspondence with the codewords of rank distance t to $\mathbf{r}$.

Proof: Let $\mathbf{c} \in \mathbb{F}_{q^m}^n$ be a codeword such that $d_R(\mathbf{c}, \mathbf{r}) = t$ with the corresponding message polynomial $f(x) \in \mathcal{L}_q(x, q^m)_{<k}$. Then by Theorem 3 there exists $D(x) \in \mathcal{L}_q(x, q^m)$ of q-degree t such that $D(f(g_i)) = D(r_i)$ for $i = 1, \dots, n$. By Theorem 10 we know that $[D(f(x)) \quad -D(x)]$ is in $\mathfrak{M}(\mathbf{r})$. It holds that $\operatorname{qdeg}(D(f(x))) \leq t + k - 1$ and that $(D(f(x))$ is divisible on the right by $D(x)$.

On the other hand let $[N(x) \quad -D(x)] \in \mathfrak{M}(\mathbf{r})$ fulfil conditions $1) - 3)$. Then we know that the divisor $f(x) \in \mathcal{L}_q(x, q^m)$ has q-degree less than k and it holds $N(x) = D(f(x))$. Since it is in $\mathfrak{M}(\mathbf{r})$ we know by Theorem 10 that $D(f(g_i)) - D(r_i) = 0$ for all i and hence by Theorem 3 that $d_R(\mathbf{c}, \mathbf{r}) = t$, if $\mathbf{c}$ is the codeword corresponding to the message polynomial $f(x)$. ■

Remark 12. The two first conditions in the previous theorem imply that the $(0, k-1)$-weighted q-degree of $[N(x) \quad -D(x)]$ is equal to $t + k - 1$.

Therefore, we have shown in this section that list decoding within rank radius t is equivalent to finding all elements $[N(x) \quad -D(x)]$ in $\mathfrak{M}(\mathbf{r})$ with $(0, k-1)$-weighted q-degree less than or equal to $t + k - 1$ and $\operatorname{qdeg}(N(x)) \leq \operatorname{qdeg}(D(x)) + k - 1$, such that $N(x)$ is symbolically divisible on the right by $D(x)$. It follows that, to find all closest codewords to a given $\mathbf{r} \in \mathbb{F}_{q^m}^n$, we need to find all elements $[N(x) \quad -D(x)] \in \mathfrak{M}(\mathbf{r})$ of minimal $(0, k-1)$-weighted q-degree such that $\operatorname{qdeg}(N(x)) \leq \operatorname{qdeg}(D(x)) + k - 1$ and $N(x)$ is symbolically divisible on the right by $D(x)$.

IV. The Algorithm

We can now describe the list decoding algorithm. Since in most applications you want to find the set of all closest codewords to the received word, our algorithm will do exactly this. In contrast, a complete list decoder with a prescribed radius t finds all codewords within radius t from the received word, even if some of them are closer than others.

We recall that our approach is analogous to [1], where a minimal Gröbner basis approach is taken. In fact, for linearized polynomials this minimal Gröbner basis approach can be formulated in exactly the same way, replacing multiplication by composition and redefine 'degree' by 'q-degree'. Due to space limitations we omit the details. Whenever we mention 'minimal basis' in the sequel, we mean 'minimal Gröbner basis' in this generalized sense.

Algorithm 1 describes the decoding algorithm. It will iteratively search for all elements in $\mathfrak{M}(\mathbf{r})$ of $(0, k-1)$-weighted q-degree $t+k-1$ for increasing t and check the requirements of Theorem 11. As soon as solutions are found, t will not be increased and the algorithm terminates.

We first present our decoding algorithm under the assumption that we can find a minimal basis for the interpolation module. We then detail the construction of such a basis in Algorithm 2. Note that we use the notation $g(x) = [g^{(1)}(x) \quad g^{(2)}(x)]$ for elements of the interpolation module $\mathfrak{M}(\mathbf{r})$.

Algorithm 1 Minimal list decoding of Gabidulin codes.

```
Require: Received word $\mathbf{r} \in \mathbb{F}_{\mathbf{q^m}}^{\mathbf{n}}$.
  1. Compute $\Pi(x)$ and $\Lambda_{\mathbf{g},\mathbf{r}}(x)$, both in $\mathcal{L}_q(x, q^m)$. Define
  the interpolation module
      $$\mathfrak{M}(\mathbf{r}) := \mathrm{rs}\begin{bmatrix} \Pi(x) & 0 \\ -\Lambda_{\mathbf{g},\mathbf{r}}(x) & x \end{bmatrix}.$$
  2. Compute a minimal basis $G = \{g_1(x), g_2(x)\}$ of
  $\mathfrak{M}(\mathbf{r})$ with respect to the $(0, k-1)$-weighted degree, with
  $\mathrm{qdeg}(g_2^{(1)}(x)) \leq \mathrm{qdeg}(g_2^{(2)}(x)) + k - 1$.
  3. Define $\ell_1, \ell_2$ as the $(0, k-1)$-weighted degrees of
  $g_1(x), g_2(x)$, respectively.
  4. Define list:= [] (an empty list) and $j := 0$.
  while list= [] do
    for all $a(x) \in \mathcal{L}_q(x, q^m), \mathrm{qdeg}(a(x)) \leq \ell_2 - \ell_1 + j$ do
      for all monic $b(x) \in \mathcal{L}_q(x, q^m), \mathrm{qdeg}(b(x)) = j$ do
        $f(x) := a(x) \circ g_1(x) + b(x) \circ g_2(x)$
        if $f^{(1)}(x)$ is symb. (right) divisible by $f^{(2)}(x)$ then
          add the respective symb. quotient to list
        end if
      end for
    end for
    $j := j + 1$
  end while
  return list
```

Theorem 13. *Algorithm 1 yields a list of all message polynomials such that the corresponding codeword is closest to the received word.*

Proof: Let t be such that $d_R(\mathbf{c}, \mathbf{r}) = t$ for a closest codeword $\mathbf{c}$. Note that the variable j in the algorithm corresponds to $t - \ell_2 + k - 1$. If we substitute this for j, then we get that

$$\begin{aligned} &\mathrm{qdeg}(f^{(1)}(x)) \leq \\ &\max\{\mathrm{qdeg}(a(x)) + \mathrm{qdeg}(g_1^{(1)}(x)), \mathrm{qdeg}(b(x)) + \mathrm{qdeg}(g_2^{(1)}(x))\} \\ &\qquad\qquad \leq \ell_2 + j = t + k - 1 \end{aligned}$$

and, since $\mathrm{qdeg}(g_2^{(1)}(x)) \leq \mathrm{qdeg}(g_2^{(2)}(x)) + k - 1$ implies that $\ell_2 - k + 1 = \mathrm{qdeg}(g_2^{(2)}(x))$,

$$\begin{aligned} &\mathrm{qdeg}(f^{(2)}(x)) = \\ &\max\{\mathrm{qdeg}(a(x)) + \mathrm{qdeg}(g_1^{(2)}(x)), \mathrm{qdeg}(b(x)) + \mathrm{qdeg}(g_2^{(2)}(x))\} \\ &\qquad\qquad = \ell_2 + j - k + 1 = t. \end{aligned}$$

Hence, $f^{(1)}(x)$ fulfills requirement $1)$ and $f^{(2)}(x)$ requirement $2)$ in Theorem 11. In fact, it can be proven that G is a minimal Gröbner basis for the interpolation module and has the so-called *Predictable Leading Monomial Property* analogous to [1], [6]. As a result of this property, the elements in the two **for**-loops that fulfill the divisibility requirement correspond to codewords with rank distance $t = j - \ell_2 + k - 1$ from $\mathbf{r}$. Due to space limitations we refrain from proving this in detail.

Moreover, increasing j by one is equivalent to increasing t by one. Therefore, once we have solutions in the list, the algorithm terminates, since elements added to the list at stage $j + 1$ would be further away then the ones added at stage j.

It remains to show that there are no codewords at rank distance less than $k-1-\ell_2$, since this is the distance for the initial loops with $j = 0$. Assume there would be such a codeword with corresponding message polynomial $m(x) \in \mathcal{L}_q(x, q^m)$. Then there exists $D(x) \in \mathcal{L}_q(x, q^m)$ with q-degree less than $k - 1 - \ell_2$ such that $g'(x) := [D(m(x)) \quad D(x)]$ is in $\mathfrak{M}(\mathbf{r})$. Then the $(0, k-1)$-weighted q-degree of $g'(x)$ is less than ℓ_2, which means that G is not a minimal basis of $\mathfrak{M}(\mathbf{r})$, which is a contradiction. ■

Theorem 14. *Algorithm 2 below produces a minimal Gröbner basis for our interpolation module $\mathfrak{M}(\mathbf{r})$ via the Euclidean algorithm for q-linearized polynomials, replacing multiplication by composition.*

For the sake of brevity we omit the proof of this result.

Example 15. Consider the Gabidulin code in $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\alpha]$ (with $\alpha^3 = \alpha + 1$) with generator matrix

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}$$

and the received word

$$\mathbf{r} = (\ \alpha + 1\ \ 0\ \ \alpha\ ).$$

Then we construct the interpolation module

$$M(\mathbf{r}) = \mathrm{rs}\begin{bmatrix} \Pi(x) & 0 \\ -\Lambda_{\mathbf{r}}(x) & x \end{bmatrix} = \mathrm{rs}\begin{bmatrix} x^8 + x & 0 \\ \alpha^2 x^4 + \alpha^5 x & x \end{bmatrix}.$$

To compute a minimal basis we use the Euclidean algorithm and get

$$x^8 + x = (\alpha^3 x^2) \circ (\alpha^2 x^4 + \alpha^5 x) + \alpha^6 x^2 + x.$$

Since $\operatorname{qdeg}(\alpha^3x^2)+k-1 = 2 \geq 1 = \operatorname{qdeg}(\alpha^6x^2+x)$, the algorithm terminates and a minimal basis (w.r.t. the $(0,1)$-weighted 2-degree) of this module is

$$\left[\begin{array}{cc} g_1^{(1)} & g_1^{(2)} \\ g_2^{(1)} & g_2^{(2)} \end{array}\right] = \left[\begin{array}{cc} \alpha^2x^4+\alpha^5x & x \\ \alpha^6x^2+x & \alpha^3x^2 \end{array}\right].$$

Hence we get $\ell_1 = 2$ and $\ell_2 = 2$, i.e. we want to use all $a(x) \in \mathcal{L}_2(x,2^3)$ with 2-degree less than or equal to 0 and all monic $b(x) \in \mathcal{L}_2(x,2^3)$ with 2-degree equal to 0. Thus, $a(x) = a_0x$ for $a_0 \in \mathbb{F}_{2^3}$ and $b(x) = x$. We get divisibility for $a_0 \in \mathbb{F}_{2^3}\backslash\{0\}$. The corresponding message polynomials and codewords are

$$m_1(x) = x^2+\alpha x \quad , \quad c_1 = (\,\alpha^3\ 1\ \alpha^3),$$

$$m_2(x) = \alpha^5x^2+\alpha^2x \quad , \quad c_1 = (\,\alpha^3\ \alpha\ \alpha),$$

$$m_3(x) = \alpha^3x^2+\alpha^4x \quad , \quad c_1 = (\,\alpha^2+1\ 0\ \alpha^2),$$

$$m_4(x) = \alpha^4x^2 \quad , \quad c_3 = (\,\alpha^2+\alpha\ \alpha^2+1\ \alpha),$$

$$m_5(x) = \alpha^6x^2+\alpha^6x \quad , \quad c_1 = (\,0\ \alpha^3\ 1),$$

$$m_6(x) = \alpha x^2+x \quad , \quad c_2 = (\,\alpha^3\ 1\ \alpha^3).$$

All these codewords are rank distance 1 away from $\mathbf{r}$.

Note that in the previous example all output codewords are only rank distance 1 away from $\mathbf{r}$, but the Hamming distance between them and $\mathbf{r}$ can vary between $1,2$ or even 3.

V. Conclusion

In this paper we introduced a novel interpolation based decoding algorithm for Gabidulin codes with respect to the rank metric. For this we construct the interpolation module for a given received word and find a minimal basis of this module with respect to the $(0,k-1)$-weighted q-degree, utilizing the Euclidean algorithm for composition of linearized polynomials. Then we check the divisibility requirement for certain combinations of the two basis elements to get the list of all closest codewords to that received word. To our knowledge the Euclidean algorithm has not been used before to do this type of list decoding for rank-metric Gabidulin decoding.

Future work consists of a detailed complexity analysis; it is anticipated that the method is efficient particularly when the decoding radius is close to the unique decoding radius, such as in one-step ahead decoding cases, illustrated by Example 15.

Algorithm 2 Computation of g_1, g_2 via the (linearized) Euclidean Algorithm.

```
Require: Received word $\mathbf{r}$; polynomials $\Pi(x)$ and $\Lambda_{\mathbf{g},\mathbf{r}}(x)$.
  Initialize $j = 0$ and defined the linearized polynomials $h_0(x), h_1(x), t_0(x), t_1(x)$ as
    $\left[\begin{array}{cc} h_0(x) & t_0(x) \\ h_1(x) & t_1(x) \end{array}\right] := \left[\begin{array}{cc} \Pi(x) & 0 \\ -\Lambda_{\mathbf{g},\mathbf{r}}(x) & x \end{array}\right].$
  while $\operatorname{qdeg}(t_{j+1})+k-1 < \operatorname{qdeg}(h_{j+1})$ do
    Apply the (linearized) Euclidean algorithm to compute the linearized polynomials $q_{j+1}(x)$ and $h_{j+2}(x)$ such that $h_j(x) = q_{j+1}(h_{j+1}(x)) + h_{j+2}(x)$ and $\operatorname{qdeg}(h_{j+2}) < \operatorname{qdeg}(h_{j+1})$.
    Update $t_{j+2}(x) := t_j(x) - q_{j+1}(t_{j+1}(x))$.
    Set $j := j+1$.
  end while
  return $g_1 := [\, h_j(x) \quad t_j(x) \,]$ and $g_2 := [\, h_{j+1}(x) \quad t_{j+1}(x) \,]$
```

References

[1] M. Ali and M. Kuijper. A parametric approach to list decoding of Reed-Solomon codes using interpolation. *IEEE Trans. Inform. Theory*, 57(10):6718–6728, 2011.

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

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

[4] E. M. Gabidulin. A fast matrix decoding algorithm for rank-error-correcting codes. In *Algebraic coding (Paris, 1991)*, volume 573 of *Lecture Notes in Comput. Sci.*, pages 126–133. Springer, Berlin, 1992.

[5] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[6] M. Kuijper and K. Schindelar. Minimal Gröbner bases and the predictable leading monomial property. *Linear Algebra and its Applications*, 434(1):104–116, 2011.

[7] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, London. Second edition.

[8] P. Loidreau. Decoding rank errors beyond the error correcting capability. In *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pages 186–190, Sept. 2006.

[9] P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In *Coding and cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, pages 36–45. Springer, Berlin, 2006.

[10] P. Lusina, E. Gabidulin, and M. Bossert. Maximum rank distance codes as space-time codes. *Information Theory, IEEE Transactions on*, 49(10):2757–2760, Oct 2003.

[11] H. Mahdavifar and A. Vardy. List-decoding of subspace codes and rank-metric codes up to singleton bound. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 1488–1492, 2012.

[12] Oystein Ore. On a Special Class of Polynomials. *Transactions of the American Mathematical Society*, 35:559–584, 1933.

[13] G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, pages 398–398, 2004.

[14] R.M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328 –336, mar 1991.

[15] V. Sidorenko and M. Bossert. Decoding interleaved gabidulin codes and multisequence linearized shift-register synthesis. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1148–1152, June 2010.

[16] V. Sidorenko, L. Jiang, and M. Bossert. Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes. *IEEE Trans. Inform. Theory*, 57(2):621–632, 2011.

[17] N. Silberstein, A. S. Rawat, and S. Vishwanath. Adversarial error resilience in distributed storage using MRD codes and MDS array codes. *arXiv:1202.0800v1 [cs.IT]*, 2012.

[18] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions on Information Theory*, 55(12):5479–5490, dec. 2009.

[19] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951 –3967, 2008.

[20] D. Silva and F.R. Kschischang. Fast encoding and decoding of gabidulin codes. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 2858–2862, June 2009.

[21] A.-L. Trautmann, N. Silberstein, and J. Rosenthal. List decoding of lifted Gabidulin codes via the Plücker embedding. In *Preproceedings of the International Workshop on Coding and Cryptography (WCC) 2013*, pages 539–549, Bergen, Norway, 2013.

[22] A. Wachter-Zeh and A. Zeh. Interpolation-based decoding of interleaved Gabidulin codes. In *Preproceedings of the International Workshop on Coding and Cryptography (WCC) 2013*, pages 527–537, Bergen, Norway, 2013.

[23] H. Xie, Z. Yan, and B.W. Suter. General linearized polynomial interpolation and its applications. In *Network Coding (NetCod), 2011 International Symposium on*, pages 1–4, July 2011.