J. Algebra Comb. Discrete Appl.
5(1) • 29–43

Received: 17 December 2016
Accepted: 6 October 2017

Journal of Algebra Combinatorics Discrete Structures and Applications

A module minimization approach to Gabidulin decoding via interpolation

Research Article

Anna-Lena Horlemann-Trautmann,* Margreta Kuijper

Abstract: We focus on iterative interpolation-based decoding of Gabidulin codes and present an algorithm that computes a minimal basis for an interpolation module. We extend existing results for Reed-Solomon codes in showing that this minimal basis gives rise to a parametrization of elements in the module that lead to all Gabidulin decoding solutions that are at a fixed distance from the received word. Our module-theoretic approach strengthens the link between Gabidulin decoding and Reed-Solomon decoding, thus providing a basis for further work into Gabidulin list decoding.

2010 MSC: 11T71, 94B35

Keywords: Gabidulin codes, Linearized polynomials, Interpolation, Minimal basis, Parametrization, Polynomial modules, Rank metric, Iterative algorithm.

1. Introduction

Over the last decade there has been increased interest in Gabidulin codes, mainly because of their relevance to network coding [12, 23] and distributed storage [20]. Gabidulin codes are optimal rank-metric codes over a field $\mathbb{F}_{q^m}$ (where q is a prime power). They are named after the work of Gabidulin in [9] and have independently been presented earlier by Delsarte in [6]. These codes can be seen as the q-analog of Reed-Solomon codes, using q-linearized polynomials instead of arbitrary polynomials. 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 (maximum rank distance) codes.

The decoding of Gabidulin codes has obtained a fair amount of attention in the literature, starting with work on decoding within the unique decoding radius in [9, 10] and more recently [16, 19, 21, 25]. If

* *This author was partially supported by Swiss National Science Foundation Fellowship no. 147304.*

Anna-Lena Horlemann-Trautmann; Faculty of Mathematics and Statistics, University of St. Gallen, St. Gallen, Switzerland (email: anna-lena.horlemann@unisg.ch).

Margreta Kuijper (Corresponding Author); Department of Electrical and Electronic Engineering, University of Melbourne, VIC 3010, Australia (email: mkuijper@unimelb.edu.au).

http://dx.doi.org/10.13069/jacodesmath.369863

ISSN 2148-838X

n is the length of the Gabidulin code and k denotes the dimension of the code as a linear space over the field $\mathbb{F}_{q^m}$, the unique decoding radius is given by $\lfloor (n-k)/2 \rfloor$. A main open question is whether there exist parameter sets for which Gabidulin codes can be (list) decoded beyond the unique decoding radius efficiently. This paper seeks to contribute to current research efforts on this open question.

Using the close resemblance between Reed-Solomon codes and Gabidulin codes, the paper [16] translates Gabidulin decoding into a set of polynomial interpolation conditions. Essentially, this setup is also used in the papers [12, 27] that present iterative algorithms that perform Gabidulin list decoding with a list size of 1. In this paper we present an iterative algorithm that bears similarity to the ones in [12, 16, 27]. As new results we show that the algorithm computes a minimal basis for an interpolation module that we associate with the received word. This result enables a parametrization of elements in the module that lead to all Gabidulin decoding solutions that are at a fixed distance from the received word. Thus we present a module minimization interpretation of the pioneering work by Loidreau [16].

The paper is structured as follows. In the next section we present several preliminaries on q-linearized polynomials and Gabidulin codes, including the polynomial interpolation conditions from [16]. Subsection 2.3 deals with modules over the ring of linearized polynomials and draws attention to minimal bases of these modules and their Predictable Leading Monomial property. In Section 3 we reformulate the Gabidulin decoding requirements in terms of a module represented by four q-linearized polynomials and present our polynomial-time algorithm. We conclude this paper in Section 4.

2. Preliminaries

2.1. q-linearized polynomials

Let q be a prime power and let m be a positive integer. Denote the finite field with q elements by $\mathbb{F}_q$ and denote a primitive element of the extension field $\mathbb{F}_{q^m}$ by α. Since $\mathbb{F}_{q^m}$ is isomorphic (as a vector space) to the vector space $\mathbb{F}_q^m$, matrices over the base field $\mathbb{F}_q$ can be interpreted as vectors over the extension field, i.e., we have the isomorphism $\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$. In the sequel we denote the rank of a matrix X over $\mathbb{F}_q$ by $\mathrm{rank}_q(X)$.

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

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

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, assuming that $a_n \neq 0$, n is called the *q-degree* of $f(x)$, denoted by $\mathrm{qdeg}(f)$. This class of polynomials was studied in detail by Ore in [17]. One can easily check that $f(x_1+x_2) = f(x_1)+f(x_2)$ 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 is a non-commutative ring with the normal addition $+$ and with 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". To not be mistaken with the standard division, we call the inverse of the composition *symbolic division*. Thus $f(x)$ is symbolically divisible by $g(x)$ with right 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) can be found e.g. in [12].

Lemma 2.1 (cf. [15] Theorem 3.50)**.** *Let $f(x) \in \mathcal{L}_q(x, q^m)$ and let $\mathbb{F}_{q^s}$ be the smallest extension field of $\mathbb{F}_{q^m}$ that contains all roots of $f(x)$. Then the set of all roots of $f(x)$ is a $\mathbb{F}_q$-linear vector space in $\mathbb{F}_{q^s}$.*

Definition 2.2. *Let U be a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$. We call $\Pi_U(x) := \prod_{g\in U}(x-g)$ the q-*annihilator polynomial *of U.*

Lemma 2.3 ([15] Theorem 3.52)**.** *Let U be a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$. Then $\Pi_U(x)$ is an element of $\mathcal{L}_q(x, q^m)$.*

Note that, if $g_1, \dots, g_n$ is a basis of U, one can rewrite

$$\Pi_U(x) = \lambda \det(M_{n+1}(g_1, \dots, g_n, x))$$

for some constant $\lambda \in \mathbb{F}_{q^m}$; clearly its q-degree equals n.

The notion of q-Lagrange polynomial is as follows:

Definition 2.4. *Let $\mathbf{g} = (g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$, where $g_1, g_2, \dots, g_n$ are $\mathbb{F}_q$-linearly independent. Let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{F}_{q^m}^n$. Define the matrix $\mathfrak{D}_i(\mathbf{g}, x)$ as $M_n(g_1, \dots, g_n, x)$ without the i-th column. We define the q-*Lagrange polynomial *corresponding to $\mathbf{g}$ and $\mathbf{r}$ as*

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

It can be easily verified that the above polynomial is q-linearized and that $\Lambda_{\mathbf{g},\mathbf{r}}(g_i) = r_i$ for $i = 1, \dots, n$.

Throughout the paper we use matrix composition, which is defined analogously to matrix multiplication:

$$\begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix} \circ \begin{bmatrix} e(x) & f(x) \\ g(x) & h(x) \end{bmatrix} := \begin{bmatrix} a(e(x)) + b(g(x)) & a(f(x)) + b(h(x)) \\ c(e(x)) + d(g(x)) & c(f(x)) + d(h(x)) \end{bmatrix}.$$

Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$; as before denote $\mathbf{g} := (g_1, \dots, g_n)$. Throughout the remainder of the paper we use the standard notation $\langle g_1, \dots, g_n\rangle$ for the $\mathbb{F}_q$-linear span of $g_1, g_2, \dots g_n$. Furthermore we abbreviate the notation $\Pi_{\langle g_1, g_2, \dots, g_n\rangle}(x)$ by $\Pi_{\mathbf{g}}(x)$. We need the following fact for our investigations in Section 3.

Lemma 2.5. *Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$ and let $L(x) \in \mathcal{L}_q(x, q^m)$ be such that $L(g_i) = 0$ for all i. Then*

$$\exists H(x) \in \mathcal{L}_q(x, q^m) : L(x) = H(x) \circ \Pi_{\mathbf{g}}(x).$$

Proof. We know from Lemma 2.3 that $\Pi_{\mathbf{g}}(x) \in \mathcal{L}_q(x, q^m)$. Moreover unique left and right division in $\mathcal{L}_q(x, q^m)$ holds, i.e. in this case there exist unique polynomials $H(x), R(x) \in \mathcal{L}_q(x, q^m)$ such that $L(x) = H(x) \circ \Pi_{\mathbf{g}}(x) + R(x)$ and $\mathrm{qdeg}(R(x)) < \mathrm{qdeg}(\Pi_{\mathbf{g}}(x)) = n$. Since any $\alpha \in \langle g_1, \dots, g_n\rangle$ is a root of $L(x)$ as well as $\Pi_{\mathbf{g}}(x)$, 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. □

2.2. Gabidulin codes

Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. A *Gabidulin code* $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k is defined as the linear block code with generator matrix $M_k(g_1, \dots, g_n)$, as defined in (1). 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. The code C has dimension k over $\mathbb{F}_{q^m}$ and minimum rank distance (over $\mathbb{F}_q$) $n-k+1$. In fact, an equivalent definition of the code is

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

where $\mathcal{L}_q(x,q^m)_{<k} := \{m(x) \in \mathcal{L}_q(x,q^m) \mid \mathrm{qdeg}(m(x)) < k\}$. For more information on bounds and constructions of rank-metric codes the interested reader is referred to [9].

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. We now recall the polynomial interpolation setup from [16] via a more general formulation in the next theorem.

Theorem 2.6. *Let $m(x) \in \mathcal{L}_q(x,q^m), \mathrm{qdeg}(f(x)) < k$ and $c_i = m(g_i)$ for $i = 1,\dots,n$. Then $d_R(\mathbf{c},\mathbf{r}) = t$ if and only if there exists a $D(x) \in \mathcal{L}_q(x,q^m)$, such that $\mathrm{qdeg}(D(x)) = t$ and*

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

Proof. Let $D(x) \in \mathcal{L}_q(x,q^m)$ be 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 2.1). 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 2.3 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 $c_i = f(g_i)$ the statement follows. □

Remark 2.7. *Theorem 2.6 states that the set of roots of $D(x)$ is a vector space of degree t which is equal to the span of $e_1,\dots,e_n$ (for this note that $e_i = m(g_i) - r_i$). This is why $D(x)$ is unique up to scalar multiplication (for given codeword and received word) and is also called the* error span polynomial *(cf. e.g. [22]). The analogy in the classical Hamming metric set-up is the* error locator polynomial*, whose roots indicate the error locations.*

2.3. Modules over $\mathcal{L}_q(x,q^m)$

As mentioned before, the set of q-linearized polynomials $\mathcal{L}_q(x,q^m)$ is a ring with addition and composition. Hence, for any positive integer ℓ, the set $\mathcal{L}_q(x,q^m)^\ell$ is a (right or left) module. In this work we will consider $\mathcal{L}_q(x,q^m)^\ell$ as a left module and investigate its (left) submodules.

In this section, we give some general definitions and results on $\mathcal{L}_q(x,q^m)^\ell$ and present the terminology of the Predictable Leading Monomial property. All of these are analogous to the definitions and results for modules over $\mathbb{F}_q[x]$ (equipped with normal polynomial multiplication) from [3], see also the early work by Fitzpatrick [7] and the textbooks [2, 5]. Linearized polynomials belong to the class of skew polynomials, for which the general theory of linear algebra and Gröbner bases is well established, see e.g. [1, 4, 11].

For reasons of clear exposition and self-containedness, we formulate the results that we need explicitly in terms of rings with composition, in the language of linearized polynomials. Thus, compared to the $\mathbb{F}_q[x]$-case, multiplication is replaced by composition.

To avoid confusion, we denote polynomials by $f(x)$, while vectors of polynomials are denoted by f. If we need to index polynomials, we use the notation $f_1(x),\dots,f_s(x)$, while for vectors of polynomials we use the notation $f^{(1)},\dots,f^{(s)}$.

Elements of $\mathcal{L}_q(x,q^m)^\ell$ are of the form

$$f := [f_1(x)\ \dots\ f_\ell(x)] = \sum_{i=1}^{\ell} f_i(x)e_i$$

where $f_i(x) = \sum_j f_{ij}x^{[j]} \in \mathcal{L}_q(x,q^m)$ and $e_1,\dots,e_\ell$ are the unit vectors of length ℓ. Analogous to polynomial multiplication on $\mathbb{F}_{q^m}[x]^\ell$ we define for $h(x) \in \mathcal{L}_q(x,q^m)$ the left operation

$$h(x) \circ f := [h(f_1(x))\ \dots\ h(f_\ell(x))] = \sum_{i=1}^{\ell} h(f_i(x))e_i.$$

The monomials of f are of the form $x^{[k]}e_i$ for all k such that $f_{ik} \neq 0$.

Definition 2.8. *A subset $M \subseteq \mathcal{L}_q(x,q^m)^\ell$ is a* (left) submodule *of $\mathcal{L}_q(x,q^m)^\ell$ if it is closed under addition and composition with $\mathcal{L}_q(x,q^m)$ on the left.*

Definition 2.9. *Consider the non-zero elements $f^{(1)},\dots,f^{(s)} \in \mathcal{L}_q(x,q^m)^\ell$. We say that $f^{(1)},\dots,f^{(s)}$ are* linearly independent *if for any $a_1(x),\dots,a_s(x) \in \mathcal{L}_q(x,q^m)$*

$$\sum_{i=1}^{s} a_i(x) \circ f^{(i)} = [\,0\ \dots\ 0\,] \quad \Longrightarrow \quad a_1(x) = \dots = a_s(x) = 0.$$

A generating set of a submodule $M \subseteq \mathcal{L}_q(x,q^m)^\ell$ is called a basis *of M if all its elements are linearly independent.*

One can easily see that

$$B = \{xe_1, xe_2 \dots, xe_\ell\}$$

is a basis of $\mathcal{L}_q(x,q^m)^\ell$, thus $\mathcal{L}_q(x,q^m)^\ell$ is a *free* and *finitely generated* module.

We need the notion of monomial order for the subsequent results, which we will define in analogy to [2, Definition 3.5.1].

Definition 2.10. *A* monomial order $<$ *on $\mathcal{L}_q(x,q^m)^\ell$ is a total order on $\mathcal{L}_q(x,q^m)^\ell$ that fulfills the following two conditions:*

- *$x^{[k]}e_i < x^{[j]} \circ (x^{[k]}e_i)$ for any monomial $x^{[k]}e_i \in \mathcal{L}_q(x,q^m)^\ell$ and $j \in \mathbb{N}_{>0}$.*
- *If $x^{[k]}e_i < x^{[k']}e_{i'}$, then $x^{[j]} \circ (x^{[k]}e_i) < x^{[j]} \circ (x^{[k']}e_{i'})$ for any monomials $x^{[k]}e_i, x^{[k']}e_{i'} \in \mathcal{L}_q(x,q^m)^\ell$ and $j \in \mathbb{N}_0$.*

We have different choices for monomial orders, of which the following is of interest for our investigations.

Definition 2.11. *The* $(k_1,\dots,k_\ell)$-weighted term-over-position monomial order *is defined as*

$$x^{[i_1]}e_{j_1} <_{(k_1,\dots,k_\ell)} x^{[i_2]}e_{j_2} :\Longleftrightarrow\ i_1 + k_{j_1} < i_2 + k_{j_2} \text{ or } [i_1 + k_{j_1} = i_2 + k_{j_2} \text{ and } j_1 < j_2].$$

Note that this monomial order for $\mathcal{L}_q(x,q^m)^\ell$ coincides with the weighted term-over-position monomial order for $\mathbb{F}_{q^m}[x]$, since one could replace the q-degrees with normal degrees and get the classical cases.

We furthermore need the following definition in analogy to the weighted term-over-position monomial order:

Definition 2.12. *The* $(k_1, \dots, k_\ell)$-weighted q-degree *of* $[f_1(x) \quad \dots \quad f_\ell(x)]$ *is defined as* $\max\{k_i + \text{qdeg}(f_i(x)) \mid i = 1, \dots, \ell\}$.

In the following we will not fix a monomial order. The results, if not noted differently, hold for any chosen monomial order.

Definition 2.13. *We can order all monomials of an element* $f \in \mathcal{L}_q(x, q^m)^\ell$ *in decreasing order with respect to some monomial order. Rename them such that* $x^{[i_1]}e_{j_1} > x^{[i_2]}e_{j_2} > \dots$. *Then*

1. *the* leading monomial $\text{lm}(f) = x^{[i_1]}e_{j_1}$ *is the greatest monomial of* f.
2. *the* leading position $\text{lpos}(f) = j_1$ *is the vector coordinate of the leading monomial.*
3. *the* leading term $\text{lt}(f) = f_{j_1,i_1}x^{[i_1]}e_{j_1}$ *is the complete term of the leading monomial.*

In order to define minimality for submodule bases we need the following notion of reduction, in analogy to [2, Definition 4.1.1].

Definition 2.14. *Let* $f, h \in \mathcal{L}_q(x, q^m)^\ell$ *and let* $F = \{f^{(1)}, \dots, f^{(s)}\}$ *be a set of non-zero elements of* $\mathcal{L}_q(x, q^m)^\ell$. *We say that* f reduces to h modulo F (in one step) *if and only if*

$$h = f - ((b_1 x^{[a_1]}) \circ f^{(1)} + \dots + (b_k x^{[a_k]}) \circ f^{(k)})$$

for some $a_1, \dots, a_k \in \mathbb{N}_0$ *and* $b_1, \dots, b_k \in \mathbb{F}_{q^m}$, *where*

$$\text{lm}(f) = x^{[a_i]} \circ \text{lm}(f^{(i)}), \quad i = 1, \dots, k, \quad \text{and}$$

$$\text{lt}(f) = (b_1 x^{[a_1]}) \circ \text{lt}(f^{(1)}) + \dots + (b_k x^{a_{[k]}}) \circ \text{lt}(f^{(k)}).$$

We say that f *is* minimal *with respect to* F *if it cannot be reduced modulo* F.

Definition 2.15. *A module basis* B *is called* minimal *if all its elements* b *are minimal with respect to* $B \backslash \{b\}$.

Proposition 2.16. *Let* B *be a basis of a module* $M \subseteq \mathcal{L}_q(x, q^m)^\ell$. *Then* B *is a minimal basis if and only if all leading positions of the elements of* B *are distinct.*

Proof. Let B be minimal. If two elements of B have the same leading position, the one with the greater leading monomial can be reduced modulo the other element, which contradicts the minimality. Hence, no two elements of a minimal basis can have the same leading position.

The other direction follows straight from the definition of reducibility and minimality of a basis, since if the leading positions of all elements are different, none of them can be reduced modulo the other elements. □

The property outlined in the following theorem is well-established for minimal Gröbner bases for modules in $\mathbb{F}_q[x]^\ell$ with respect to multiplication. It extends to non-commutative Gröbner bases of solvable type, see e.g. [11, Lemma 1.5]. As a result, it also holds over the ring of linearized polynomials. It was labeled *Predictable Leading Monomial (PLM) property* in [13] to emphasize its closeness to Forney's *Predictable Degree property* [8]. It captures the exact property that is needed in subsequent proofs.

Note that in [13] minimal bases were addressed as minimal Gröbner bases. It can be shown that in our current setting these are the same.

Theorem 2.17 (PLM property). *Let* M *be a module in* $\mathcal{L}_q(x, q^m)^\ell$ *with minimal basis* $B = \{b^{(1)}, \dots, b^{(L)}\}$. *Then for any* $0 \neq f \in M$, *written as*

$$f = a_1(x) \circ b^{(1)} + \dots + a_L(x) \circ b^{(L)},$$

where $a_1(x), \dots, a_L(x) \in \mathcal{L}_q(x, q^m)$*, we have*

$$\mathrm{lm}(f) = \max_{1 \le i \le L; a_i(x) \neq 0} \{\mathrm{lm}(a_i(x)) \circ \mathrm{lm}(b^{(i)})\}$$

where $\mathrm{lm}(a_i(x))$ *is the term of* $a_i(x)$ *of highest* q*-degree.*

Proof. Since B is minimal, all leading positions and thus also all leading monomials of its elements are distinct (by Proposition 2.16). Without loss of generality assume that $\mathrm{lm}(b^{(1)}) > \mathrm{lm}(b^{(2)}) > \cdots > \mathrm{lm}(b^{(L)})$ and that all $a_i(x)$ are non-zero. Since $\mathcal{L}_q(x, q^m)$ contains no zero divisors, we have that $\mathrm{lpos}(a_i(x) \circ b^{(i)}) = \mathrm{lpos}(b^{(i)})$ for $1 \le i \le L$. As a result, all leading positions and therefore all leading monomials of the $a_i(x) \circ b^{(i)}$'s are distinct. Thus there exist $j_1, \dots, j_L$ such that

$$\mathrm{lm}(a_{j_1}(x) \circ b^{(j_1)}) > \mathrm{lm}(a_{j_2}(x) \circ b^{(j_2)}) > \cdots > \mathrm{lm}(a_{j_L}(x) \circ b^{(j_L)}).$$

It follows that

$$\mathrm{lm}(f) = \mathrm{lm}(a_{j_1}(x) \circ b^{(j_1)}) = \mathrm{lm}(a_{j_1}(x)) \circ \mathrm{lm}(b^{(j_1)}) = \max_{1 \le i \le L} \{\mathrm{lm}(a_i(x)) \circ \mathrm{lm}(b^{(i)})\}.$$

□

Proposition 2.18. *The leading positions and weighted* q*-degrees of all elements of two distinct minimal bases for the same module in* $\mathcal{L}_q(x, q^m)^\ell$ *have to be the same. This implies that the cardinality of both bases are equal as well.*

Proof. Let $B_1 = \{b^{(i)} \mid i = 1, \dots, L\}$ and $B_2 = \{c^{(i)} \mid i = 1, \dots, L'\}$ be two different minimal bases of the same module in $\mathcal{L}_q(x, q^m)^\ell$. Then $b^{(j)}$ must be a linear combination of the $c^{(i)}$ for $j = 1, \dots, L$. Similarly, $c^{(i)}$ must be a linear combination of the $b^{(j)}$ for $i = 1, \dots, L'$. Hence, by the PLM property and since all leading positions are different in the bases, there exist $j' \in \{1, \dots, L'\}$ and $a(x), a'(x) \in \mathcal{L}_q(x, q^m)$ such that $\mathrm{lm}(a(x) \circ c^{(j')}) = \mathrm{lm}(b^{(j)})$ and $\mathrm{lm}(a'(x) \circ b^{(j)}) = \mathrm{lm}(c^{(j')})$. This implies on the one hand that $\mathrm{lpos}(b^{(j)}) = \mathrm{lpos}(c^{(j')})$ and on the other that $\mathrm{qdeg}(a(x)) = \mathrm{qdeg}(a'(x)) = 0$, which implies that $\mathrm{qdeg}(b^{(j)}) = \mathrm{qdeg}(c^{(j')})$. □

3. Iterative decoding of Gabidulin codes

For the remainder 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 $C \subseteq \mathbb{F}_{q^m}^n$. Denote $\mathbf{g} = (g_1, \dots, g_n)$ and let $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{F}_{q^m}^n$ be the received word. Throughout the remainder of this paper our monomial order will be the $(0, k-1)$-weighted term-over-position monomial order.

3.1. Parametrization

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

Definition 3.1. *The* interpolation module $\mathfrak{M}(\mathbf{r})$ *for* $\mathbf{r}$ *is defined as the left submodule of* $\mathcal{L}_q(x, q^m)^2$*, given by*

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

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

Theorem 3.2. *$\mathfrak{M}(\mathbf{r})$ 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 $i = 1, \ldots, n$.*

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

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 $i = 1, \ldots, n$. To show that $Q(x,y) \in \mathfrak{M}(\mathbf{r})$ we need to find $\beta(x), \gamma(x) \in \mathcal{L}_q(x, q^m)$ such that

$$\beta(x) \circ \Pi_{\mathbf{g}}(x) - \gamma(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x) = f(x) \quad \text{ and } \quad \gamma(x) = g(x).$$

We substitute the second into the first equation to get

$$\beta(x) \circ \Pi_{\mathbf{g}}(x) = f(x) + g(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x). \tag{2}$$

By assumption, the equation $f(g_i) + g(\Lambda_{\mathbf{g},\mathbf{r}}(g_i)) = f(g_i) + g(r_i) = 0$ holds for all i. Then, by Lemma 2.5, it follows that $f(x) + g(x) \circ \Lambda_{\mathbf{g},\mathbf{r}}(x)$ is symbolically divisible on the right by $\Pi_{\mathbf{g}}(x)$ and hence there exists $\beta(x) \in \mathcal{L}_q(x, q^m)$ such that (2) holds. □

The above leads to the following characterization of codewords with distance t to the received word:

Theorem 3.3. *The elements $f = [N(x) \quad -D(x)]$ of $\mathfrak{M}(\mathbf{r})$ that fulfill*

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

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

Proof. To prove the first direction 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 $m(x) \in \mathcal{L}_q(x, q^m)_{<k}$. Then by Theorem 2.6 there exists $D(x) \in \mathcal{L}_q(x, q^m)$ of q-degree t such that $D(m(g_i)) = D(r_i)$ for $i = 1, \ldots, n$. By Theorem 3.2 we know that $[D(m(x)) \quad -D(x)]$ is in $\mathfrak{M}(\mathbf{r})$. It holds that $\mathrm{qdeg}(D(m(x))) \leq t + k - 1$ and that $(D(m(x)))$ is symbolically divisible on the left by $D(x)$.

For the other direction let $[N(x) \quad -D(x)] \in \mathfrak{M}(\mathbf{r})$ fulfill conditions $1) - 3)$. Then the divisor $m(x) \in \mathcal{L}_q(x, q^m)$ has q-degree less than k and $N(x) = D(m(x))$. Since it is in $\mathfrak{M}(\mathbf{r})$ it follows from Theorem 3.2 that $D(m(g_i)) - D(r_i) = 0$ for all i. Define $\mathbf{c} := (m(g_1), \ldots, m(g_n))$, then it follows from Theorem 2.6 that $d_R(\mathbf{c}, \mathbf{r}) = t$. □

Note that conditions 1) and 2) of Theorem 3.3 can alternatively be formulated as the condition that $\mathrm{lpos}(f) = 2$ with $(0, k-1)$-weighted q-degree of f being equal to $t + k - 1$.

It follows from Theorem 3.3 that decoding within rank radius t is equivalent to finding all elements $f = [N(x) \quad -D(x)]$ in $\mathfrak{M}(\mathbf{r})$ with $(0, k-1)$-weighted q-degree less than $t + k$ and leading position 2, such that $N(x)$ is symbolically divisible on the left by $D(x)$. The following theorem presents a parametrization that is helpful in order to find such elements.

Theorem 3.4. *(Parametrization) Let $B = \{b^{(1)}, b^{(2)}\}$ be a minimal basis of $\mathfrak{M}(\mathbf{r})$ with respect to the $(0, k-1)$-weighted degree, with $\mathrm{lpos}(b^{(1)}) = 1$ and $\mathrm{lpos}(b^{(2)}) = 2$. Define ℓ_1 and ℓ_2 as the $(0, k-1)$-weighted q-degrees of $b^{(1)}, b^{(2)}$, respectively. Let t be a nonnegative integer. Then all elements $f \in \mathfrak{M}(\mathbf{r})$ with $\mathrm{lpos}(f) = 2$ and $(0, k-1)$-weighted q-degree equal to $t + k - 1$ are given by*

$$f = \beta(x) \circ b^{(1)} + \gamma(x) \circ b^{(2)},$$

where $\beta(x)$ is a q-linearized polynomial with $\mathrm{qdeg}(\beta(x)) \leq t + k - 1 - \ell_1$ and $\gamma(x)$ is a q-linearized polynomial with $\mathrm{qdeg}(\gamma(x)) = t + k - 1 - \ell_2$.

Proof. The parametrization follows straightforwardly from Theorem 2.17. □

3.2. Construction of a minimal basis

We now present an iterative algorithm for the construction of a minimal basis for the interpolation module. The algorithm is similar to the ones in[12, 16, 27]. Our main contribution is the recognition, via Theorem 3.4, that such an algorithm essentially computes a minimal basis for the interpolation module rather than just one solution corresponding to the received word. A preliminary version of this result is the short conference paper [14].

We first need the following result:

Lemma 3.5. *For $i = 1, \dots, n$ denote by $\mathfrak{M}_i$ the interpolation module for $(g_1, \dots, g_i)$ and $(r_1, \dots, r_i)$. Let*

$$\begin{bmatrix} P(x) & -K(x) \\ N(x) & -D(x) \end{bmatrix}$$

be a basis for $\mathfrak{M}_{i-1}$ and

$$\Gamma_i := P(g_i) - K(r_i) \quad , \quad \Delta_i := N(g_i) - D(r_i).$$

If $\Gamma_i \neq 0$, then the set of row vectors of

$$\begin{bmatrix} b^{(1)} \\ b^{(2)} \end{bmatrix} := \begin{bmatrix} x^q - \Gamma_i^{q-1}x & 0 \\ \Delta_i x & -\Gamma_i x \end{bmatrix} \circ \begin{bmatrix} P(x) & -K(x) \\ N(x) & -D(x) \end{bmatrix}$$

is a basis of $\mathfrak{M}_i$. If $\Delta_i \neq 0$, then the set of row vectors of

$$\begin{bmatrix} \Delta_i x & -\Gamma_i x \\ 0 & x^q - \Delta_i^{q-1}x \end{bmatrix} \circ \begin{bmatrix} P(x) & -K(x) \\ N(x) & -D(x) \end{bmatrix}$$

is a basis of $\mathfrak{M}_i$.

Proof. We first consider the first case and show that both $b^{(1)}$ and $b^{(2)}$ are in $\mathfrak{M}_i$. From the assumptions it follows that $P(g_j) = K(r_j)$ and that $N(g_j) = D(r_j)$ for $1 \leq j < i$. Moreover, the two entries of $b^{(1)}$ are given by

$$(x^q - \Gamma_i^{q-1}x) \circ P(x) = P(x)^q - \Gamma_i^{q-1}P(x),$$

$$(x^q - \Gamma_i^{q-1}x) \circ K(x) = K(x)^q - \Gamma_i^{q-1}K(x),$$

thus $P(g_j)^q - \Gamma_i^{q-1}P(g_j) - K(r_j)^q + \Gamma_i^{q-1}K(r_j) = 0$ for $1 \leq j \leq i$. For $b^{(2)}$ we get

$$\Delta_i P(g_j) - \Gamma_i N(g_j) - \Delta_i K(r_j) + \Gamma_i D(r_j) =$$

$$\Delta_i(P(g_j) - K(r_j)) - \Gamma_i(N(g_j) - D(r_j)) = \Delta_i\Gamma_i - \Gamma_i\Delta_i = 0$$

for $1 \leq j \leq i$. Thus, $b^{(1)}$ and $b^{(2)}$ are elements of $\mathfrak{M}_i$.

It remains to show that $b^{(1)}$ and $b^{(2)}$ span the entire interpolation module (and not just a submodule of it). For this, it is sufficient to show that $[\, \Pi_{i-1}(x) \quad 0 \,]$ and $[\, \Lambda_{i-1}(x) \quad -x \,]$ are linear combinations of $b^{(1)}$ and $b^{(2)}$. Since $[\, P(x) \quad -K(x) \,]$ and $[\, N(x) \quad -D(x) \,]$ are a basis of $\mathfrak{M}_i$, there exist $\bar{\beta}(x), \bar{\gamma}(x) \in \mathcal{L}_q(x, q^m)$ such that

$$\bar{\beta}(x) \circ [\, P(x) \quad -K(x) \,] + \bar{\gamma}(x) \circ [\, N(x) \quad -D(x) \,] = [\, \Pi_{i-1}(x) \quad 0 \,].$$

Let $\beta(x), \gamma(x) \in \mathcal{L}_q(x, q^m)$ be such that

$$\beta(x) \circ (x^q - \Gamma_i^{q-1} x) = (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \left(\bar{\gamma}(\frac{\Delta_i}{\Gamma_i} x) + \bar{\beta}(x) \right),$$

$$\gamma(x) = -(x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \bar{\gamma}(\frac{1}{\Gamma_i} x).$$

Note that it can easily be checked that Γ_i is a root of the right side of the previous equation, thus $\beta(x)$ is well-defined by Lemma 2.5 . Denote the first and second row of the new basis by $b^{(1)}$ and $b^{(2)}$, respectively. Then

$$\beta(x) \circ b_1^{(1)} + \gamma(x) \circ b_1^{(2)} = \beta(x) \circ (x^q - \Gamma_i^{q-1} x) \circ P(x) + \gamma(x) \circ (\Delta_i P(x) - \Gamma_i N(x))$$

$$= (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \left(\bar{\gamma}(\frac{\Delta_i}{\Gamma_i} x) + \bar{\beta}(x) \right) \circ P(x) + \gamma(\Delta_i P(x)) - \gamma(\Gamma_i N(x))$$

$$= \big((x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \bar{\beta}(x) - \gamma(\Delta_i x) \big) \circ P(x) + \gamma(\Delta_i P(x)) - \gamma(\Gamma_i N(x))$$

$$= \big((x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \bar{\beta}(x) \big) \circ P(x) + (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \bar{\gamma}(N(x))$$

$$= (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \big(\bar{\beta}(P(x)) + \bar{\gamma}(N(x)) \big)$$

$$= (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \Pi_{i-1}(x) = \Pi_i(x),$$

and

$$\beta(x) \circ b_2^{(1)} + \gamma(x) \circ b_2^{(2)} = -\beta(x) \circ (x^q - \Gamma_i^{q-1} x) \circ K(x) - \gamma(x) \circ (\Delta_i K(x) - \Gamma_i D(x))$$

$$= \big((x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \bar{\beta}(x) - \gamma(\Delta_i x) \big) \circ K(x) + \gamma(\Delta_i K(x)) - \gamma(\Gamma_i D(x))$$

$$= (x^q - \Pi_{i-1}(g_i)^{q-1} x) \circ \big(\bar{\beta}(K(x)) + \bar{\gamma}(D(x)) \big) = 0.$$

Thus $\beta(x) \circ b^{(1)} + \gamma(x) \circ b^{(2)} = [\, \Pi_i(x) \quad 0 \,]$, i.e. $[\, \Pi_i(x) \quad 0 \,]$ is in the module spanned by the new basis.

Analogously, if we have that $\bar{c}(x) \circ [\, P(x) \quad -K(x) \,] + \bar{d}(x) \circ [\, N(x) \quad -D(x) \,] = [\, \Lambda_{i-1}(x) \quad -x \,]$ and define $c(x), d(x) \in \mathcal{L}_q(x, q^m)$ such that

$$d(x) = -\left(\bar{d}(x) + \frac{\Lambda_{i-1}(g_i) - r_i}{\Pi_{i-1}(g_i)} \bar{\gamma}(x) \right) \circ (\frac{1}{\Gamma_i} x)$$

$$c(x) \circ (x^q - \Gamma_i^{q-1} x) = \bar{c}(x) + \frac{\Lambda_{i-1}(g_i) - r_i}{\Pi_{i-1}(g_i)} \bar{\beta}(x) - d(\Delta_i x)$$

we get

$$c(x) \circ b^{(1)} + d(x) \circ b^{(2)} = [\, \Lambda_i(x) \quad -x \,].$$

Hence, we have shown that the new basis $\{b^{(1)}, b^{(2)}\}$ spans the entire interpolation module.

For the second case note that

$$\mathrm{rs}\left(\begin{bmatrix} \Delta_i x & -\Gamma_i x \\ 0 & x^q - \Delta_i^{q-1} x \end{bmatrix} \circ \begin{bmatrix} P(x) & -K(x) \\ N(x) & -D(x) \end{bmatrix} \right)$$

$$= \mathrm{rs}\left(\begin{bmatrix} x^q - \Delta_i^{q-1} x & 0 \\ \Gamma_i x & -\Delta_i x \end{bmatrix} \circ \begin{bmatrix} N(x) & -D(x) \\ P(x) & -K(x) \end{bmatrix} \right),$$

which corresponds to the first case after exchanging $P(x)$ with $N(x)$ and $K(x)$ with $D(x)$ (and vice versa). □

Using Lemma 3.5 as our main ingredient, we now set out to design an iterative algorithm that computes a minimal basis for $\mathfrak{M}_i$ at each step i.

Algorithm 1 Iterative computation of a minimal basis of $\mathfrak{M}(\mathbf{r})$.

```
Require: Positive integers $k, n$; $\mathbf{g} = (g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$, received word $\mathbf{r} = (r_1, \dots, r_n) \in \mathbb{F}_{q^m}^n$.
  Initialize $j := 0$, $B_0 := \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$.
  We denote $B_i := \begin{bmatrix} P_i(x) & -K_i(x) \\ N_i(x) & -D_i(x) \end{bmatrix}$.
  for $i$ from 1 to $n$ do
    $\Gamma_i := P_{i-1}(g_i) - K_{i-1}(r_i)$   ,   $\Delta_i := N_{i-1}(g_i) - D_{i-1}(r_i)$.
    if [qdeg$(P_{i-1}(x)) \leq$ qdeg$(D_{i-1}(x)) + k - 1$ and $\Gamma_i \neq 0$] or $\Delta_i = 0$ then
        $B_i := \begin{bmatrix} x^q - \Gamma_i^{q-1}x & 0 \\ \Delta_i x & -\Gamma_i x \end{bmatrix} \circ B_{i-1}$
    else
        $B_i := \begin{bmatrix} \Delta_i x & -\Gamma_i x \\ 0 & x^q - \Delta_i^{q-1}x \end{bmatrix} \circ B_{i-1}$
    end if
  end for
  return $B_n$
```

Theorem 3.6. *Algorithm 1 yields a minimal basis of the interpolation module $\mathfrak{M}(\mathbf{r})$, where the leading position of the first row equals 1 and the leading position of the second row equals 2.*

Proof. Denote by M_1 the matrix we multiply by on the left in the first IF statement and by M_2 the one in the ELSE statement of the algorithm. We know from Lemma 3.5 that at each step, B_i is a basis for the interpolation module $\mathfrak{M}_i$. We now show that it is a minimal basis with respect to the $(0, k-1)$-weighted term-over-position monomial order via induction on i. Assume that at step i the first row has leading position 1 and the second row has leading position 2, i.e. qdeg$(P_i(x)) >$ qdeg$(K_i(x)) + k - 1$ and qdeg$(N_i(x)) \leq$ qdeg$(D_i(x)) + k - 1$. If qdeg$(P_i(x)) \leq$ qdeg$(D_i(x)) + k - 1$ we composite on the left by M_1. Hence,

$$\text{qdeg}(P_{i+1}(x)) = \text{qdeg}(P_i(x)) + 1$$

and

$$\text{qdeg}(K_{i+1}(x)) = \text{qdeg}(K_i(x)) + 1 < \text{qdeg}(P_i(x)) - k + 2 = \text{qdeg}(P_{i+1}(x)) - k + 1.$$

Thus, the leading position of the first row of B_{i+1} is still 1. Moreover,

$$\text{qdeg}(N_{i+1}(x)) \leq \max\{\text{qdeg}(P_i(x)), \text{qdeg}(N_i(x))\} \leq \text{qdeg}(D_i(x)) + k - 1$$

and, since the assumptions imply that qdeg$(K_i(x)) <$ qdeg$(D_i(x))$,

$$\text{qdeg}(D_{i+1}(x)) = \max\{\text{qdeg}(K_i(x)), \text{qdeg}(D_i(x))\} = \text{qdeg}(D_i(x)).$$

Thus the leading position of the second row is 2. Since the assumptions are true for B_0 the statement follows via induction.

Analogously one can prove that composition with M_2 yields a basis of $\mathfrak{M}_i$ with different leading positions in the two rows. Thus at each step we get a basis of $\mathfrak{M}_i$ with different leading positions, which is by Proposition 2.16 a minimal basis. Thus, after n steps, B_n is a minimal basis for the interpolation module $\mathfrak{M}(\mathbf{r})$. □

Remark 3.7. *It can be verified that, due to the linear independence of $g_1, \dots, g_k$, up to a constant, at step k the algorithm has computed the q-annihilator polynomial and the q-Lagrange polynomial corresponding to the data so far.*

Proposition 3.8. *Algorithm 1 has computational complexity order $\mathcal{O}_{q^m}(n^2)$.*

Proof. For the iterative computation of the minimal basis from Algorithm 1 we need n steps. In each step we need

- four evaluations and differences of linearized polynomials of q-degree at most n (to compute Δ_i and Γ_i and in the update of B_i),
- two multiplications of a linearized polynomial of q-degree at most n by a scalar (in the update of B_i),
- a composition of a linearized polynomial of q-degree at most n with $(x^q - g_i^{q-1}x)$ (for this note that we compute a $(q-1)$-th power of g_i with a q-th power and one division).

All of these operations can be done with $\mathcal{O}_{q^m}(n)$ operations. Overall we get an upper bound on the complexity of $\mathcal{O}_{q^m}(n^2)$. □

3.3. Decoding algorithm

We can now set up the decoding algorithm which will find the closest codeword(s) to a given received word. For this we need the following lemma.

Lemma 3.9. *Consider a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$ of dimension k. Let $\mathfrak{M}(\mathbf{r})$ be the interpolation module of the received word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ with minimal basis $B = \{b^{(1)}, b^{(2)}\}$ where $\mathrm{lpos}(b^{(i)}) = i$ for $i = 1, 2$. Denote the $(0, k-1)$-weighted q-degree of $b^{(i)}$ by ℓ_i for $i = 1, 2$. Then*

$$\ell_1 + \ell_2 = n + k - 1. \tag{3}$$

Proof. By Proposition 2.18 the q-degrees of any minimal basis of the interpolation module $\mathfrak{M}(\mathbf{r})$ have to add up to the same number, hence it is enough to show that they add up to $n+k-1$ for one particular basis. Consider the iterative construction of a minimal basis from Algorithm 1. It is easy to see that the initial basis has weighted q-degrees 0 and $k-1$. Moreover, at each step the q-degree of one row is increased by one, whereas the q-degree of the other row remains the same. Thus, the sum of the two q-degrees is increased by 1 at each step. Since we get the desired basis of $\mathfrak{M}(\mathbf{r})$ at the n-th step, equation (3) follows. □

In the following theorem we pay specific attention to the unique decoding case.

Theorem 3.10. *Consider the setting of Theorem 3.4. If $t = \min\{d_R(\mathbf{c}, \mathbf{r}) \mid \mathbf{c} \in C\}$ and $t \leq (n-k)/2$ then $f = \gamma(x) \circ b^{(2)}$ with $\mathrm{qdeg}(\gamma(x)) = 0$ and symbolic division on the two components of the vector $b^{(2)}$ produces the message polynomial corresponding to the unique closest codeword to $\mathbf{r}$.*

Proof. Let $m(x) \in \mathcal{L}_q(x, q^m)$ be the message polynomial corresponding to the unique closest codeword $\mathbf{c}$. Then by Theorem 3.3, there exist $D(x) \in \mathcal{L}_q(x, q^m)$ of q-degree t such that $f = [\, D(m(x)) \quad -D(x)\,]$ is an element of the interpolation module with leading position 2. Note that then the $(0, k-1)$-weighted degree of f equals $t + k - 1 \leq (n+k-2)/2$. Theorem 2.17 now implies that $\mathrm{lm}(f) \geq \mathrm{lm}(b^{(2)})$, which implies (since the leading positions of both elements are 2) that $\ell_2 \leq (n+k-2)/2$. It now follows from Lemma 3.9 that $\ell_1 \geq (n+k)/2$. Thus, in the parametrization we get $\beta(x) \equiv 0$, which means that there exists $\gamma(x)$ such that

$$f = \gamma(x) \circ b^{(2)}.$$

But since $\gamma(x)$ cancels out when we divide the right entry of f by the left, we can simply choose $\gamma(x) = x$ to recover the message polynomial. This also implies that $\mathrm{qdeg}(b^{(2)}) = t + k - 1$, and the last statement of the theorem follows. □

Note that, if the received word is within the unique decoding radius, the main result of Loidreau's algorithm [16] is similar, namely the symbolic division on two components to produce the message polynomial, as in the above theorem.

We present the general structure of the decoding algorithm in Algorithm 2 below. The outer IF loop is based on Theorem 3.10, whereas the corresponding ELSE loop uses Theorems 3.3 and 3.4 to enumerate all message polynomials corresponding to the codewords of distance t to the received word (for increasing t).

Algorithm 2 Iterative decoding of a Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$.

```
Require: Positive integers $k, n$; received word $\mathbf{r} \in \mathbb{F}_{q^m}^n$.
  Use Algorithm 1 to compute a minimal basis $B_n = \{b^{(1)}, b^{(2)}\}$ of $\mathfrak{M}(\mathbf{r})$.
  Set $\ell_1 := \text{qdeg}(b^{(1)}), \ell_2 := \text{qdeg}(b^{(2)})$, list:= [ ], $j := 0$ .
  if $\ell_2 \leq (n+k-2)/2$ and $b_1^{(2)}$ is symbolically divisible by $b_2^{(2)}$ on the left then
    add the symbolic quotient of $b_1^{(2)}$ and $b_2^{(2)}$ to list.
  else
    while list= [ ] do
      for all $a(x) \in \mathcal{L}_q(x, q^m), \text{qdeg}(a(x)) \leq \ell_2 - \ell_1 + j$ do
        for all monic $c(x) \in \mathcal{L}_q(x, q^m), \text{qdeg}(b(x)) = j$ do
          $f := a(x) \circ b^{(1)} + c(x) \circ b^{(2)}$
          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
  end if
  return list
```

Remark 3.11. *Algorithm 2 is an extension of Loidreau's algorithm, in the sense that it has the same performance in the unique decoding case, but it can also find all closest codewords if the received word is beyond the unique decoding radius of the Gabidulin code. This is due to the parametrization derived in Subsection 3.1 and the fact that Loidreau's algorithm actually computes a minimal basis of the interpolation module, as shown in Subsection 3.2.*

We conclude this section with a final example.

Example 3.12. *Consider the Gabidulin code in $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\alpha]$ (with $\alpha^3 = \alpha + 1$) of length $n = 3$ and dimension $k = 2$ with generator matrix*

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

Thus $\mathbf{g} = (g_1, g_2, g_3) = (1, \alpha, \alpha^2)$. Suppose that the received word equals

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

Using Algorithm 1, we iteratively compute

$$B_1 = \begin{bmatrix} x^2 + x & 0 \\ (\alpha+1)x & x \end{bmatrix},$$

$$B_2 = \begin{bmatrix} x^4 + (\alpha^2+\alpha+1)x^2 + (\alpha^2+\alpha)x & 0 \\ (\alpha^2+\alpha)x^2 + (\alpha^2+\alpha+1)x & (\alpha^2+\alpha)x \end{bmatrix},$$

$$B_3 = \begin{bmatrix} \alpha^2x^4 + \alpha^5 x & x \\ \alpha x^4 + \alpha^4 x^2 + x & \alpha x^2 + \alpha^6 x \end{bmatrix}.$$

B_3 is a minimal $(0,1)$-weighted basis of the interpolation module $\mathfrak{M}(\mathbf{r})$. In the notation of Theorem 3.4, we get $\ell_1 = \ell_2 = 2$. As a result, by Theorem 3.4, any monic $f \in \mathfrak{M}(\mathbf{r})$ that has $(0,1)$-weighted q-degree 2 and fulfills $\mathrm{lpos}(f) = 2$ can be written as

$$f = \beta(x) \circ b^{(1)} + \gamma(x) \circ b^{(2)},$$

where $\beta(x)$ is a q-linearized polynomial with $\mathrm{qdeg}(\beta(x)) \leq 0$ and $\gamma(x)$ is a monic q-linearized polynomial with $\mathrm{qdeg}(\gamma(x)) = 0$. Thus

$$\begin{aligned} f &= b_0 x \circ b^{(1)} + x \circ b^{(2)} \\ &= b_0 b^{(1)} + b^{(2)} \\ &= \begin{bmatrix} (b_0\alpha^2 + \alpha)x^4 + \alpha^4 x^2 + (b_0\alpha^5 + 1)x & \alpha x^2 + (b_0 + \alpha^6)x \end{bmatrix}. \end{aligned}$$

In fact, in this example we can use this basis to obtain a complete list of codewords of rank distance 1 away from $\mathbf{r} = (\ \alpha+1 \ \ 0 \ \ \alpha\ )$, as follows. It is easily checked that for $b_0 \in \mathbb{F}_{2^3} \backslash \{\alpha^6\}$ we get divisibility. Thus it follows from Theorem 3.3 that the complete list of all message polynomials & codewords of rank distance 1 away from $\mathbf{r} = (\ \alpha+1 \ \ 0 \ \ \alpha\ )$ is given by

$$\begin{array}{ll} m_1(x) = x^2 + \alpha x & c_1 = (\ \alpha+1 \quad 0 \quad \alpha^2+1), \\ m_2(x) = \alpha^5 x^2 + \alpha^2 x & c_2 = (\ \alpha+1 \quad \alpha \quad \alpha), \\ m_3(x) = \alpha^3 x^2 + \alpha^4 x & c_3 = (\ \alpha^2+1 \quad 0 \quad \alpha^2), \\ m_4(x) = \alpha^4 x^2 & c_4 = (\ \alpha^2+\alpha \quad \alpha^2+1 \quad \alpha), \\ m_5(x) = \alpha^6 x^2 + \alpha^6 x & c_5 = (\ 0 \quad \alpha+1 \quad 1), \\ m_6(x) = \alpha^2 x^2 + \alpha^3 x & c_6 = (\ \alpha^2+\alpha+1 \quad 0 \quad \alpha), \\ m_7(x) = \alpha x^2 + x & c_7 = (\ \alpha+1 \quad 1 \quad \alpha+1). \end{array}$$

Note that the corresponding Hamming distances to $\mathbf{r}$ vary from 1 to 3.

4. Conclusions

We extended the Welch-Berlekamp type algorithm given in the pioneering work by Loidreau [16], to be able to decode also beyond the unique decoding radius. For this we derived a parametrization of all codewords within a given radius of the received words, based on a minimal basis of the interpolation module. To compute such a minimal basis we presented a polynomial-time iterative algorithm with simple update steps, similar to Loidreau's algorithm. The main contribution of our paper is the recognition that such algorithms actually compute a minimal basis of the interpolation module which can then be used to provide a parametrization of all solutions corresponding to the received word.

In the Reed-Solomon case, Massey's parametrization resulting from the Berlekamp-Massey algorithm was used by Wu [26] as the foundation to his polynomial-time Reed-Solomon list decoding algorithm. This was used in [3] as the foundation for a polynomial time Reed-Solomon list decoding method via Welch-Berlekamp type interpolation. In this paper we strengthened the link between Reed-Solomon decoding and Gabidulin decoding in providing a similar parametrization from a Welch-Berlekamp type algorithm for Gabidulin decoding. Currently no polynomial-time list decoding algorithms exist for general Gabidulin codes; on the contrary, it is shown that polynomial list sizes are not possible for certain parameter sets (see e.g. [18, 24]). However, there are still many parameters for which it is an open question whether polynomial-time list decoding of Gabidulin codes is possible. It is a topic of future research to build on the results of this paper in extending the parametrization-based methods of [3, 26] to a possibly polynomial-time Gabidulin list decoding algorithm.

References

[1] S. Abramov, M. Bronstein, Linear algebra for skew–polynomial matrices, Technical Report INRIA, RR–4420, 2002.

[2] W. W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, volume 3 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 1994.

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

[4] B. Beckermann, H. Cheng, G. Labahn, Fraction–free row reduction of matrices of Ore polynomials, J. Symbolic Comput. 41(5) (2006) 513–543.

[5] D. A. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, volume 185 of Graduate Texts in Mathematics, Springer, New York, second edition, 2005.

[6] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Combin. Theory Ser. A 25(3) (1978) 226–241.

[7] P. Fitzpatrick, On the key equation, IEEE Trans. Inform. Theory 41(5) (1995) 1290–1302.

[8] G. D. Forney, Jr., Minimal bases of rational vector spaces, with applications to multivariable linear systems, SIAM J. Control 13(3) (1975) 493–520.

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

[10] E. M. Gabidulin, A fast matrix decoding algorithm for rank–error–correcting codes, In Algebraic coding (Paris, 1991), Lecture Notes in Computer Science, 573 (1992) 126–133.

[11] A. Kandri–Rody, V. Weispfenning, Noncommutative Gröbner bases in algebras of solvable type, J. Symbolic Comput. 9(1) (1990) 1–26.

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

[13] M. Kuijper, K. Schindelar, Minimal Gröbner bases and the predictable leading monomial property, Linear Algebra Appl. 434(1) (2011) 104–116.

[14] M. Kuijper, A.–L. Trautmann, Iterative list–decoding of Gabidulin codes via Gröbner based interpolation, In IEEE Information Theory Workshop (ITW 2014), Hobart, TAS, 2014, 581–585.

[15] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Second edition, Cambridge, London, 1997.

[16] P. Loidreau, A Welch–Berlekamp like algorithm for decoding Gabidulin codes, In Coding and cryptography, Lecture Notes in Computer Science 3969 (2006) 36–45.

[17] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. 35(3) (1933) 559–584.

[18] N. Raviv, A. Wachter–Zeh, Some Gabidulin codes cannot be list decoded efficiently at any radius, IEEE Trans. Inform. Theory 62(4) (2016) 1605–1615.

[19] G. Richter, S. Plass, Fast decoding of rank–codes with rank errors and column erasures, IEEE International Symposium on Information Theory (ISIT) proceedings (2004) 398–398.

[20] N. Silberstein, A. S. Rawat, S. Vishwanath, Error resilience in distributed storage via rank–metric codes, In Fiftieth Annual Allerton conference, UIUC, Illinois, USA, (2012) 1150–1157.

[21] D. Silva, F. R. Kschischang, Fast encoding and decoding of Gabidulin codes, IEEE International Symposium on Information Theory (ISIT) proceedings (2009) 2858–2862.

[22] D. Silva, F. R. Kschischang, On metrics for error correction in network coding, IEEE Trans. Inform. Theory 55(12) (2009) 5479–5490.

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

[24] A. Wachter–Zeh, Bounds on list decoding of rank–metric codes, IEEE Trans. Inform. Theory 59(11) (2013) 7268–7277.

[25] A. Wachter–Zeh, V. Afanassiev, V. Sidorenko, Fast decoding of Gabidulin codes, Des. Codes Cryptogr. 66(1–3) (2013) 57–73.

[26] Y. Wu, New list decoding algorithms for Reed–Solomon and BCH codes, IEEE Trans. Inform. Theory 54(8) (2008) 3611–3630.

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