Interpolation-based Decoding of Nonlinear Maximum Rank Distance Codes

Chunlei Li

Department of Informatics, University of Bergen, Norway
Email: Chunlei.Li@uib.no

***Abstract*—In this paper, we formulate a generic construction of MRD codes that covers almost all the newly found MRD codes. Among those MRD codes, we particularly investigate the encoding and decoding of a family of nonlinear MRD codes recently by Otal and Özbudak.**

***Index Terms*—Rank metric, maximum rank distance codes, Gabidulin codes, Dickson matrix**

I. Introduction

Rank metric codes have gained steady attention due to their applications in a variety of areas, such as space-time coding [1], random network coding [2] and cryptography [3]. Many important properties of rank metric codes were independently established in the pioneering works [4], [5], [6], in which the rank metric Singleton bound was established and the *maximum rank distance* (MRD) codes that attain the bound with equality were constructed. The Gabidulin codes, the rank analogues of Reed-Solomon codes, are the most famous linear MRD codes and the decoding of such codes have been extensively studied (see, e.g, [5], [7], [8], [9], [10], [11]).

In the last few years, significant progresses have been made in the construction of MRD codes that are inequivalent to the Gabidulin codes and their generalized variants. The first non-(generalized) Gabidulin MRD codes were introduced independently by Sheekey in [12] and by Otal and Özbudak in [13], where the latter presented a particular case of the former. Sheekey in [12] defined the codes by adding an extra monomial to the polynomial representation of the original Gabidulin codes with certain restriction on its coefficient and called them the *twisted Gabidulin (TG)* codes. Later, the generalized twisted Gabidulin (GTG) codes were intensively investigated in [14]; and it was further extended by Otal and Özbudak in [15], [16], where they proposed additive (but not linear) MRD codes and non-additive partition codes, respectively. Very recently, a new family of MRD codes with even length was proposed in [17].

In this paper we formulate the aforementioned MRD codes into a generic construction based on an interesting result on the rank of linearized polynomials. Furthermore, we discuss the encoding process of the non-additive partition codes and propose an interpolation-based approach to decoding these nonlinear codes. We also show that the proposed algorithm has complexity dominated by the modified Berlekamp-Massey algorithm [8], [18].

II. Preliminaries

Throughout this paper we denote by $GF(q^r)$ the finite field with q^r elements for a prime power q and an integer $r \geqslant 1$.

A. Linearized Polynomial

A polynomial of the form $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ with coefficients in an extension field $GF(q^n)$ of $GF(q)$ is called a *q-polynomial* over $GF(q^n)$. When q is fixed or the context is clear, it is also customary to speak of a *linearized polynomial* as it satisfies the linearity property: $L(cx_1 + x_2) = cL(x_1) + L(x_2)$ for any $c \in GF(q)$ and any x_1, x_2 in an arbitrary extension of $GF(q^n)$. Let $\mathcal{L}_n(GF(q^n))$ be the set of all the following linearized polynomials

$$L(x) = \sum_{i=0}^{n-1} l_i x^{q^i} \in GF(q^n)[x]/(x^{q^n} - x). \tag{1}$$

Equipped with the addition and the composition of polynomials, the set $\mathcal{L}_n(GF(q^n))$ forms a $GF(q)$-algebra.

Definition 1: Given a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ over $GF(q^n)$, the *q-degree* of $L(x)$ is given by $\deg_q(L) = \max\{0 \leqslant i < n : l_i \neq 0\}$, and the *rank* of $L(x)$, denoted by $\mathrm{Rank}(L)$, is defined as the dimension of the image $\mathrm{Im}(L) = \{L(x) | x \in GF(q^n)\}$ over $GF(q)$.

Some properties of linearized polynomials with a prescribed rank and their associated Dickson matrices are characterized in [19], [20].

Proposition 1: [19, Th. 2.4] Let $L(x)$ be a linearized polynomial in $\mathcal{L}_n(GF(q^n))$ with rank r. Then there exist two groups of linearly independent vectors $\alpha_1, \cdots, \alpha_r$ and $\beta_1, \cdots, \beta_r$ in $GF(q^n)$ such that

$$L(x) = \sum_{i=1}^{r} \mathrm{Tr}(\alpha_i x)\beta_i = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{r} \beta_j \alpha_j^{q^i} \right) x^{q^i}. \tag{2}$$

From Proposition 1 we can derive an interesting property of the Dickson matrix associated with linearized polynomials.

Proposition 2: [20, Th. 3] Let $L(x)$ be a linearized polynomial in $\mathcal{L}_n(GF(q^n))$ with rank r. Then its associated Dickson matrix

$$D = \left(l_{i-j(\bmod n)}^{q^j} \right)_{n \times n} = \begin{pmatrix} l_0 & l_{n-1}^{q} & \cdots & l_1^{q^{n-1}} \\ l_1 & l_0^{q} & \cdots & l_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^{q} & \cdots & l_0^{q^{n-1}} \end{pmatrix}, \tag{3}$$

where $0 \leqslant i, j < n$, also has rank r. Moreover, any $r \times r$ sub-matrix of D that is formed by r consecutive rows and r consecutive columns in D is nonsingular.

Proposition 2 can be easily proved by expressing the Dickson matrix D in terms of the product of two Moore matrices [21] generated from $\alpha_1, \cdots, \alpha_r$ and $\beta_1, \cdots, \beta_r$, respectively. The properties of the Dickson matrix characterized in Proposition 2 are critical for the interpolation-based decoding algorithm in this paper.

B. Rank Metric Codes

Let n, m be two positive integers and $GF(q)^{m\times n}$ be the set of $m \times n$ matrices over $GF(q)$. The *rank distance* on the $GF(q)^{m\times n}$ is defined by $d_r(\mathbf{A}-\mathbf{B}) = \text{Rank}(\mathbf{A}-\mathbf{B})$ for $\mathbf{A}, \mathbf{B} \in GF(q)^{m\times n}$.

Definition 2: A *rank metric code* $\mathcal{C}$ is a subset of $GF(q)^{m\times n}$ equipped with the rank distance, and its minimum rank distance is naturally defined as $d_r(\mathcal{C}) = \min\{d_r(\mathbf{A}-\mathbf{B}) \,|\, \mathbf{A}, \mathbf{B} \in \mathcal{C} \text{ and } \mathbf{A} \neq \mathbf{B}\}$.

Since the matrix transpose operation preserves the parameters of a rank metric code, it is commonly assumed that $n \leqslant m$ without loss of generality. Assume $\beta = \{\beta_1, \cdots, \beta_m\}$ is a basis of $GF(q^m)$ over $GF(q)$. It induces a one-to-one mapping $\phi : GF(q)^{m\times n} \to GF(q^m)^n$ defined by $\phi(\mathbf{A}) = (\beta_1, \cdots, \beta_m)\mathbf{A} = (a_1, \cdots, a_n)$. Hence a rank metric code in matrix form can be converted to a code of length n over $GF(q^m)$ whose rank metric distance is defined by the corresponding rank distance on $GF(q)^{m\times n}$. Hence a rank metric code is usually also represented in the vectorial form as a subset of $GF(q^m)^n$ and the conventional notation $(n, M, d)_{q^m}$ is used to denote rank metric codes over $GF(q^m)$ with length n, M codewords and minimum rank distance d. It is well-known that a rank metric $(n, M, d)_{q^m}$ code satisfies a Singleton-like bound:

$$M \leqslant q^{\min\{n(m-d+1), m(n-d+1)\}}.$$

Rank metric codes that attain the Singleton-like bound by equality are called *maximum rank distance (MRD)* codes. MRD codes have a rich mathematical structure and have found wide applications in space-time coding [1], random network coding [22] and cryptography [3], [23].

C. Maximum Rank Distance Codes

In the sequel we shall assume $n = m$ and summarize recently found MRD codes in terms of linearized polynomials.

Let $\alpha = \{\alpha_1, \cdots, \alpha_n\}$ and $\beta = \{\beta_1, \cdots, \beta_n\}$ be two ordered bases of $GF(q^n)$ over $GF(q)$. Then for any linearized polynomial f in $\mathcal{L}_n(GF(q)^n)$, we have

$$\begin{aligned} f(x) &= f(x_1\alpha_1 + \cdots + x_n\alpha_n) \\ &= (f(\alpha_1), \cdots, f(\alpha_n))(x_1, \cdots, x_n)^T \\ &= (\beta_1, \cdots, \beta_n) \cdot F \cdot (x_1, \cdots, x_n)^T, \end{aligned}$$

where $(x_1, \cdots, x_n) \in GF(q)^n$ and $F = \left(f(\alpha_j)_\beta\right)_{1\leqslant j\leqslant n}$ is a matrix over $GF(q)$ of which the j-th column is given by the coordinates of $f(\alpha_j)$ under the basis β, i.e., $f(\alpha_j) = (\beta_1, \cdots, \beta_n) f(\alpha_j)_\beta$. Observe that the matrix F is one-to-one corresponding to f with respect to the bases α and β, and its rank is equal to Rank(f). Moreover, the algebra $GF(q)^{n\times n}$ with matrix addition and multiplication has a one-to-one correspondence to the algebra $\mathcal{L}_n(GF(q)^n)$. With such a correspondence, we will consider the algebra $\mathcal{L}_n(GF(q)^n)$ as the ambient space instead of $GF(q)^{n\times n}$ in the following, which seems more elegant to represent rank metric codes.

For a linearized polynomial $L(x) \in \mathcal{L}_n(GF(q)^n)$, the rank nullity theorem implies

$$\text{Rank}(L) = \text{Rank}(\text{Im}(L)) = n - \dim(\text{Ker}(L)),$$

where $\text{Ker}(L) = \{x \in GF(q^n) | L(x) = 0\}$. Hence the rank of a linearized polynomial $L(x)$ satisfies

$$\text{Rank}(L) = n - \dim(\text{Ker}(L)) \geqslant n - \deg_q(L)$$

since the dimension of Ker(L) is at most the q-degree of $L(x)$. This property naturally results in the famous Gabidulin codes $\mathcal{G}$ over $GF(q^n)$, which can be defined in terms of linearized polynomial as follows

$$\mathcal{G} = \left\{ \sum_{i=0}^{k-1} f_i x^{q^i} \,|\, f_i \in GF(q^n) \right\}. \tag{4}$$

In recent years several new families of MRD codes were constructed, which heavily depend on the following result on the rank of certain linearized polynomials.

Lemma 1: Let s be a positive integer co-prime to n and $f(x) = f_0 x + f_1 x^{q^s} + \cdots + f_k x^{q^{ks}} \in \mathcal{L}_n(GF(q^n))$ with $f_k \neq 0$. If the coefficients f_0 and f_k satisfy

$$\text{Norm}_{q^n/q}(f_k) \neq (-1)^{nk}\text{Norm}_{q^n/q}(f_0), \tag{5}$$

where $\text{Norm}_{q^n/q}(x) = x^{\frac{q^n-1}{q-1}}$, then $\text{Rank}(f) \geqslant n - k + 1$.

Despite its simplicity, Lemma 1 turns out to be a powerful tool to construct new families of MRD codes. Sheekey in [12] first adopted it to construct the *twisted Gabidulin* (TG) codes, which was further extended to the *generalized twisted Gabidulin* (GTG) codes in [14]. It was also employed in the construction of additive generalized twisted Gabidulin (AGTG) codes in [15] and non-additive partition codes [16].

Here we give a generic construction of MRD codes equipped with Lemma 1, which covers all the aforementioned MRD codes. (It does not cover the further generalized twisted Gabidulin codes discussed in [24] and the nonlinear MRD codes proposed in [25].)

Theorem 1: Let $n, k, s, h \in \mathbb{Z}^+$ satisfying $(s, n) = 1$ and $k < n$. Let Γ be a subset of $GF(q^n)^2$ such that

$$|\Gamma| = q^n \text{ and } (b_2 - b_1)^{\frac{q^n-1}{q-1}} \neq (-1)^{nk}(a_2 - a_1)^{\frac{q^n-1}{q-1}} \tag{6}$$

for any distinct elements $(a_1, b_1), (a_2, b_2) \in \Gamma$. Then the code

$$\mathcal{H}_{n,k,s}(\Gamma) = \left\{ \sum_{i=0}^{k} f_i x^{q^{si}} \,:\, f_i \in GF(q^n), (f_0, f_k) \in \Gamma \right\} \tag{7}$$

is an MRD code of size q^{nk} and rank distance $n - k + 1$.

Proof. From the definition in (7), the difference of any two dis-

tinct codes can be expressed as $h(x) = \sum_{i=0}^{k} h_i^{q^{si}}$, where the coefficients h_0 and h_k satisfy $h_k^{\frac{q^n-1}{q-1}} \neq (-1)^{nk} h_0^{\frac{q^n-1}{q-1}}$. From Lemma 1 and (6), it follows that the linearized polynomial $h(x)$ has rank at least $n-k+1$, which implies that the code $\mathcal{H}_{n,k,s}(\Gamma)$ has minimum rank distance at least $n-k+1$. On the other hand, the code $\mathcal{H}_{n,k,s}(\Gamma)$ has cardinality q^{nk} since $|\Gamma| = q^n$. By the Singleton-like bound, the code $\mathcal{H}_{n,k,s}(\Gamma)$ must have minimum rank distance $n-k+1$. ■

From the definition in (7), the MRD codes recently given in the literature [12], [14], [15], [16], [17] can be summarized as below:

- when $\Gamma = \{(a, 0) : a \in GF(q^n)\}$, the codes $\mathcal{H}_{n,k,s}(\Gamma)$ are the generalized Gabidulin codes [7] and they become the original Gabidulin codes [5] when $s = 1$;
- when $\Gamma = \{(a, \eta a^{q^h}) : a \in GF(q^n)\}$ for certain η with $\text{Norm}_{q^n/q}(\eta) \neq (-1)^{nk}$, the codes $\mathcal{H}_{n,k,s}(\Gamma)$ are the GTG codes discussed in [14] and they become the TG codes introduced by Sheekey [12] when $s = 1$;
- when $\Gamma = \{(a, \eta a^{q_0^h}) : a \in GF(q^n)\}$, where $q = q_0^u$ with $u > 1$ and $\text{Norm}_{q^n/q_0}(\eta) \neq (-1)^{nku}$, the codes $\mathcal{H}_{n,k,s}(\Gamma)$ are the AGTG codes introduced in [15];
- when $\Gamma = \{(a, 0), (0, b) : a, b \in GF(q^n), \text{Norm}_{q^n/q}(a) \in I, \text{Norm}_{q^n/q}(b) \notin (-1)^{nk} I\}$ for some subset $I \subseteq GF(q)$, the codes $\mathcal{H}_{n,k,s}(\Gamma)$ are the non-additive partition codes proposed in [16];
- when $n = 2m$, $\Gamma = \{(a, \gamma b) : a, b \in GF(q^m)$, and $\text{Norm}_{q^n/q}(\gamma)$ is a non-square in $GF(q)$, the codes are the ones proposed in [17] very recently.

In the above list, the first two classes of MRD codes are linear, the third class are additive but generally not linear over $GF(q)$ and the last class are non-additive over $GF(q)$. It is easily seen that the linearity or additivity property of the code $\mathcal{H}_{n,k,s}(\Gamma)$ over $GF(q)$ is completely dependent on the property of the set Γ over $GF(q)$. Hence finding sets Γ satisfying (6) is critical for constructing MRD codes from Lemma 1. From the third and fourth classes of MRD codes we see that f_0 and f_k are not necessarily closely dependent.

III. Encoding and Decoding of MRD codes

In this section we will discuss the encoding and decoding of the MRD codes $\mathcal{H}_{n,k,s}(\Gamma)$ in Theorem 1. Throughout what follows we will denote $[i] := q^{si}$, $0 \leqslant i < n$, for simplicity.

A. Encoding

With the codes $\mathcal{H}_{n,k,s}(\Gamma)$, the encoding of a message $(f_0, f_1, \cdots, f_{k-1})$ can be interpreted as the evaluation of the linearized polynomial $f(x) = \hat{f}_0 x + \sum_{i=1}^{k-1} f_i x^{[i]} + \hat{f}_k x^{[k]}$ at linearly independent points $a_1, \cdots, a_n$ in $GF(q^n)$, where the coefficients $\hat{f}_0, \hat{f}_k$ are determined by the set Γ and the given coordinate f_0.

For the MRD codes summarized in the previous section, we describe the derivation of the tuple $(\hat{f}_0, \hat{f}_k)$ as follows:

- the GTG and AGTG codes: the coefficients $(\hat{f}_0, \hat{f}_k) = (f_0, \eta f_0^{q_0^h})$ with $q_0 = q$ for the GTG codes [14] and $q_0 < q$ for the AGTG codes [15];
- the non-additive partition codes: this case sets the coefficients $(\hat{f}_0, \hat{f}_k) = (f_0, 0)$ if $\text{Norm}_{q^n/q}(f_0) \in I$ and $(\hat{f}_0, \hat{f}_k) = (0, (-1)^k f_0)$ otherwise. Assigning $(\hat{f}_0, \hat{f}_k)$ in this way guarantees that any message $(f_0, f_1, \cdots, f_{k-1})$ is properly encoded as a codeword in $\mathcal{H}_{n,k,s}(\Gamma)$.

Let $\mathbf{M}$ be the $n \times n$ Moore matrix generated by elements $a_1, \cdots, a_n$ in $GF(q^n)$, namely, $\mathbf{M} = \left(a_{j+1}^{[i]}\right)_{n\times n}$, where $0 \leqslant i, j < n$. Then the encoding of the MRD codes $\mathcal{H}_{n,k,s}(\Gamma)$ can be expressed as

$$(f_0, \cdots, f_{k-1}) \mapsto (c_1, \cdots, c_n) = (\hat{f}_0, f_1, \cdots, f_{k-1}, \hat{f}_k) \cdot \mathbf{M}',$$

where $\mathbf{M}'$ is the $(k+1) \times n$ matrix formed by the first $k+1$ rows of $\mathbf{M}$. To make it consistent with the subsequent decoding algorithm, we rewritten the encoding process as

$$(f_0, \cdots, f_{k-1}) \mapsto \mathbf{c} = (c_1, \cdots, c_n) = \hat{\mathbf{f}} \cdot \mathbf{M}, \tag{8}$$

where $\hat{\mathbf{f}}$ is an n-dimensional vector over $GF(q^n)$ given by $\hat{\mathbf{f}} = (\hat{f}_0, f_1, \cdots, f_{k-1}, \hat{f}_k, 0, \cdots, 0)$.

B. Interpolation-based Decoding

Many decoding algorithms for the (generalized) Gabidulin codes were proposed [5], [8], [9], [10]. In these algorithms, the linearity property plays an important role in establishing the *key equation* in the decoding procedure. However, the key equation cannot be similarly obtained for non-linear MRD codes $\mathcal{H}_{n,k,s}(\Gamma)$. Therefore, we adopt an *interpolation-based* approach to decoding these codes.

For an error vector $\mathbf{e} = (e_1, \cdots, e_n)$ over $GF(q^n)$, suppose $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ is the interpolation polynomial at the points $(a_1, e_1), \cdots, (a_n, e_n)$, i.e.,

$$g(a_i) = e_i = r_i + c_i, \quad i = 1, \cdots, n. \tag{9}$$

We call the polynomial $g(x)$ the *error interpolation polynomial* in this paper. It's clear that an error vector can be uniquely derived from its corresponding error interpolation polynomial.

Let $\mathbf{g} = (g_0, \cdots, g_{n-1})$. From (8) and (9) it follows that

$$\mathbf{r} = \mathbf{c} + \mathbf{e} = (\hat{\mathbf{f}} + \mathbf{g}) \cdot \mathbf{M}.$$

Letting $\hat{\mathbf{r}} = (\hat{r}_0, \cdots, \hat{r}_{n-1}) = \mathbf{r} \cdot \mathbf{M}^{-1}$, we obtain

$$(g_{k+1}, \cdots, g_{n-1}) = (\hat{r}_{k+1}, \cdots, \hat{r}_{n-1}) \tag{10}$$

and

$$g_0 = \hat{r}_0 - \hat{f}_0, \quad g_k = \hat{r}_k - \hat{f}_k. \tag{11}$$

Suppose the error vector $\mathbf{e}$ has rank $t \leqslant \lfloor \frac{n-k}{2} \rfloor$. Since $\mathbf{g} = \mathbf{e} \cdot \mathbf{M}^{-1}$, the polynomial $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ has rank t. By Proposition 2, its associated Dickson matrix

$$G = \left(g_{i-j \pmod n}^{[j]}\right)_{n\times n} = \begin{pmatrix} g_0 & g_{n-1}^{[1]} & \cdots & g_1^{[n-1]} \\ g_1 & g_0^{[1]} & \cdots & g_2^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2}^{[1]} & \cdots & g_0^{[n-1]} \end{pmatrix}$$

has rank t; and any $t \times t$ matrix formed by t successive rows and columns in G is nonsingular.

Let $G = \big(G_0, G_1, \cdots, G_{n-1}\big)$, where G_i is the i-th column of G. Then G_0 can be expressed as a linear combination of $G_1, \cdots, G_t$, namely,

$$G_0 = \lambda_1 G_1 + \lambda_2 G_2 + \cdots + \lambda_t G_t,$$

where $\lambda_1, \cdots, \lambda_t$ are elements in $GF(q^n)$. This yields the recursive equations

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]}, \quad 0 \leqslant i < n. \quad (12)$$

Recall that the elements $g_{k+1}, \cdots, g_{n-1}$ are known from (10). Hence we obtain the following linear equations with known coefficients and variables $\lambda_1, \cdots, \lambda_t$:

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]}, \quad k+t+1 \leqslant i < n. \quad (13)$$

The above recurrence can be seen as a feedback-shift register with tap weights, and the solution $\lambda_1, \cdots, \lambda_t$ can be efficiently found with a generalized version of the modified Berlekamp-Massey (BM) algorithm introduced in [8], [18].

In the following we shall reconstruct $g(x)$ by combining (13) together with (11) and the relation between $\hat{f}_0$ and $\hat{f}_k$. The general strategy of the reconstruction process is in the following two steps:

Step 1. uniquely determine $\lambda_1, \cdots, \lambda_t$ from (13), (11);
Step 2. recursively compute $g_0, g_1, \cdots, g_k$ by (12).

As the error vector $\mathbf{e}$ has rank $t \leqslant \lfloor \frac{n-k}{2} \rfloor$, i.e., $2t + k \leqslant n$, we divide the discussion into two cases.

Case I). $2t + k < n$

In this case, one has $n - k - t - 1 \geqslant t$. Hence the $(n - k - t - 1) \times t$ coefficient matrix in (13) has rank t and there exists a unique solution $\lambda_1, \cdots, \lambda_t$ to (13). Once $\lambda_1, \cdots, \lambda_t$ are determined in Step 1, the remaining coefficients $g_0, g_1, \cdots, g_{k-1}$ can be easily computed according to (12) recursively.

Case II). $2t + k = n$

In this case, one obtains $n-k-t-1 = t-1$ linear equations in (13). The $(t-1) \times t$ coefficient matrix in (13) has rank $t-1$. Hence the elements $\lambda_1, \cdots, \lambda_t$ cannot be uniquely determined by (13).

As a matter of fact, given the code $\mathcal{H}_{n,k,s}(\Gamma)$ the process of determining $\lambda_1, \cdots, \lambda_t$ heavily depends on the set Γ. Below we discuss the known MRD codes $\mathcal{H}_{n,k,s}(\Gamma)$:

- when $\Gamma = \{(a, \eta a^{q_0^h}) : \gamma \in GF(q^n)\}$, where $q = q_0^u$, one obtains $(\hat{f}_0, \hat{f}_k) = (f_0, \eta f_0^{q_0^h})$. Then (11) gives an equality $\eta g_0^{q_0^h} + g_k = \eta \hat{r}_0^{q_0^h} + \hat{r}_k$. This equality together with those in (13) also gives a unique solution $\lambda_1, \cdots, \lambda_t$. This case was recently discussed in [26], [20] for $u = 1$ and in [27] for $u > 1$;
- when $\Gamma = \{(a, 0), (0, b) : \mathrm{Norm}_{q^n/q}(a) \in I, \mathrm{Norm}_{q^n/q}(b) \in GF(q) \backslash (-1)^{nk} I, a, b \in GF(q^n)\}$ for some subset $I \subseteq GF(q)$, this corresponds to the non-additive partition code given in [16]. We shall intensively investigate this case in the sequel.

For the non-additive partition code in [16], from the encoding process we have

$$(\hat{f}_0, \hat{f}_k) = \begin{cases} (f_0, 0), & \text{if } \mathrm{Norm}_{q^n/q}(f_0) \in I, \\ (0, (-1)^k f_0), & \text{if } \mathrm{Norm}_{q^n/q}(f_0) \notin I. \end{cases}$$

Hence we need to investigate these two possible cases at first and then check which of them satisfies the corresponding condition.

We start with the case that $(\hat{f}_0, \hat{f}_k) = (f_0, 0)$. In this case (11) implies $g_k = \hat{r}_k$. That is to say, we get $n - k - t = t$ linear equations in variables $\lambda_1, \cdots, \lambda_t$ as follows:

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]}, \quad k + t \leqslant i < n. \quad (14)$$

Since the coefficient matrix has rank t, the above system has a unique solution $\lambda_1, \cdots, \lambda_t$. With this solution, one can obtain g_0 from the equality

$$g_0 = \lambda_1 g_{n-1}^{[1]} + \lambda_2 g_{n-2}^{[2]} + \cdots + \lambda_t g_{n-t}^{[t]}$$

and needs to check whether $\mathrm{Norm}_{q^n/q}(\hat{r}_0 - g_0) \in I$ or not. If it is true, then the assumption $(\hat{f}_0, \hat{f}_k) = (f_0, 0)$ is correct and one can use $\lambda_1, \cdots, \lambda_t$ to further calculate the remaining coefficients $g_1, \cdots, g_k$ recursively from (12); otherwise, one needs to proceed with the second case.

In the second case, one obtains $g_0 = \hat{r}_0$ from the assumption $(\hat{f}_0, \hat{f}_k) = (0, (-1)^k f_0)$. Similarly, one derive $n - k - t = t$ linear equations in variables $\lambda_1, \cdots, \lambda_t$ as follows:

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]}, \quad k + t < i \leqslant n. \quad (15)$$

This system also has a unique solution $\lambda_1, \cdots, \lambda_t$ since the coefficient matrix has rank t. Furthermore, the coefficient g_k can be similarly derived from the equality

$$g_{k+t} = \lambda_1 g_{k+t-1}^{[1]} + \lambda_2 g_{k+t-2}^{[2]} + \cdots + \lambda_t g_k^{[t]}.$$

For the obtained g_k, whether the condition $\mathrm{Norm}_{q^n/q}(\hat{r}_k - g_k) \notin (-1)^{nsk} I$ is satisfied must be checked. If the condition is satisfied, then the coefficient g_k is correct and one can continue to compute the coefficients $g_0, \cdots, g_{k-1}$ recursively according to (12); otherwise the decoding fails.

From the above analysis, we summarize the decoding of the non-additive partition MRD codes in Algorithm 1, where the notation $\mathcal{H}_{n,k,s}(I)$ is used to specify the subset I used.

Remark 1: It is worth remarking that the traditional syndrome decoding approach for Gabidulin codes [5], [10] cannot be applied to the TG codes, GTG codes [14], the AGTG codes [28] and the nonlinear partition codes [28] due to the difficulty of representing the generator and parity-check matrices. Such an issue is properly addressed by the interpolation approach. It can be seen that Algorithm 1 heavily depends the interpolation approach and the modified BM algorithm introduced in [8], [18]. Regarding the complexity of Algorithm 1, the interpolation step in Line 1 can be completed in sub-quadratic multiplications in $GF(q^n)$ [29]; Line 3 has quadratic complexity in $GF(q^n)$. When the error vector has rank $t = (n - k)/2$, Lines 4 - 17 requires $O(t)$ operations

Algorithm 1: Decoding of the partition codes $\mathcal{H}_{n,k,s}(I)$

Input: A received word $\mathbf{r}$ with $t \leqslant \lfloor \frac{n-k}{2} \rfloor$ errors, and linearly independent evaluation points $a_1, \cdots, a_n$

Output: The correct codeword $\mathbf{c}$ or "Decoding Failure"

Calculate $\hat{\mathbf{r}} = (\hat{r}_0, \cdots, \hat{r}_{n-1}) = \mathbf{r} \cdot \mathbf{M}^{-1}$;
Set $(g_{k+1}, \cdots, g_{n-1}) = (\hat{r}_{k+1}, \cdots, \hat{r}_{n-1})$;
Apply the modified Berlekamp-Massey Alg. to find the smallest integer t and $(\lambda_1, \cdots, \lambda_t)$ satisfying (13);
if *Line 3 outputs an integer* $t = \frac{n-k}{2}$ **then**
    Set $g_k = \hat{r}_k$;
    Update the coefficients $(\lambda_1, \cdots, \lambda_t)$ according to (14) and the modified Berlekamp-Massey Alg.;
    Calculate $g_0 = \lambda_1 g_{n-1}^{[1]} + \lambda_2 g_{n-2}^{[2]} + \cdots + \lambda_t g_{n-t}^{[t]}$;
    if $Norm_{q^n/q}(\hat{r}_0 - g_0) \notin I$ **then**
        Set $g_0 = \hat{r}_0$;
        Update the coefficients $(\lambda_1, \cdots, \lambda_t)$ according to (15) and the modified Berlekamp-Massey Alg.;
        Get g_k from $g_{k+t} = \sum_{j=1}^{t-1} \lambda_j g_{k+t-j}^{[j]} + \lambda_t g_k^{[t]}$;
        if $(-1)^{nsk} Norm_{q^n/q}(\hat{r}_k - g_k) \in I$ **then**
            Return "Decoding Failure"
        end
    end
end
for $i \in \{0, \cdots, k\}$ **do**
    Calculate $g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \cdots + \lambda_t g_{i-t}^{[t]}$
end
if $g_0, \cdots, g_{n-1}$ *is successfully determined* **then**
    Return the codeword $\mathbf{c} = \mathbf{r} - \mathbf{g} \cdot \mathbf{M}$
else
    Return "Decoding Failure"
end

in $GF(q^n)$. Hence, Algorithm 1 has quadratic complexity in $GF(q^n)$, which is dominated by the modified Berlekamp-Massey algorithm [8], [18].

IV. Conclusion

In this paper we summarized recently found MRD codes in a generic construction and investigated the encoding and decoding of a large family of nonlinear MRD codes by Otal and Özbudak. The decoding algorithm adopted an interpolation approach and was shown to have its complexity dominated by the modified Berlekamp-Massey algorithm.

References

[1] P. Lusina, E. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2757–2760, Oct 2003.

[2] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, Sept 2008.

[3] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their application in cryptology," in *Advances in Cryptology — EUROCRYPT '91*, D. W. Davies, Ed. Springer, 1991, pp. 482–489.

[4] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226 – 241, 1978.

[5] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[6] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[7] A. Kshevetskiy and E. Gabidulin, "The new construction of rank codes," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*. IEEE, 2005, pp. 2105–2108.

[8] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in *International Symposium on Information Theory (ISIT)*, June 2004, pp. 398–398.

[9] P. Loidreau, "A Welch–Berlekamp like algorithm for decoding Gabidulin codes," in *International Workshop on Coding and Cryptography(WCC)*, Ø. Ytrehus, Ed. Berlin, Heidelberg: Springer, 2006, pp. 36–45.

[10] D. Silva and F. R. Kschischang, "Fast encoding and decoding of Gabidulin codes," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*. IEEE, 2009, pp. 2858–2862.

[11] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko, "Fast decoding of Gabidulin codes," *Designs, Codes and Cryptography*, vol. 66, no. 1-3, pp. 57–73, 2013.

[12] J. Sheekey, "A new family of linear maximum rank distance codes," *Advances in Mathematics of Communications*, vol. 10, p. 475, 2016.

[13] K. Otal and F. Özbudak, "Explicit constructions of some non-Gabidulin linear maximum rank distance codes," *Advances in Mathematics of Communications*, vol. 10, no. 3, pp. 589–600, 2016.

[14] G. Lunardon, R. Trombetti, and Y. Zhou, "Generalized twisted Gabidulin codes," *Journal of Combinatorial Theory, Series A*, vol. 159, pp. 79–106, 2018.

[15] K. Otal and F. Özbudak, "Additive rank metric codes," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 164–168, 2017.

[16] ——, "Some new non-additive maximum rank distance codes," *Finite Fields and Their Applications*, vol. 50, pp. 293 – 303, 2018.

[17] R. Trombetti and Y. Zhou, "A new family of mrd codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$," *IEEE Transactions on Information Theory*, vol. 65, no. 2, pp. 1054–1062, Feb 2019.

[18] V. Sidorenko, G. Richter, and M. Bossert, "Linearized shift-register synthesis," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 6025–6032, Sep. 2011.

[19] S. Ling and L. Qu, "A note on linearized polynomials and the dimension of their kernels," *Finite Fields and Their Applications*, vol. 18, no. 1, pp. 56 – 62, 2012.

[20] T. H. Randrianarisoa, "A decoding algorithm for rank metric codes," *CoRR*, vol. abs/1712.07060, 2017.

[21] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[22] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, Aug 2008.

[23] R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," *Journal of Cryptology*, vol. 21, no. 2, pp. 280–301, Apr 2008.

[24] P. Sven, R. J. S. Heesemann, and S. John, "Further generalisations of twisted Gabidulin codes," *presented at the International Workshop on Coding and Cryptography (WCC)*, 2017.

[25] N. Durante and A. Siciliano, "Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries," *The Electronic Journal of Combinatorics*, vol. 24, no. 2.33, pp. 1–18, 2017.

[26] J. Rosenthal and T. H. Randrianarisoa, "A decoding algorithm for twisted Gabidulin codes," in *Information Theory (ISIT), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 2771–2774.

[27] C. Li and W. Kadir, "On decoding additive generalized twisted Gabidulin codes," *presented at the International Workshop on Coding and Cryptography (WCC)*, 2019.

[28] K. Otal and F. Özbudak, "Constructions of cyclic subspace codes and maximum rank distance codes," in *Network Coding and Subspace Designs*. Springer, 2018, pp. 43–66.

[29] S. Puchinger and A. Wachter-Zeh, "Fast operations on linearized polynomials and their applications in coding theory," *Journal of Symbolic Computation*, vol. 89, pp. 194–215, 2018.