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 $r \geq 1$.

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

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

Equipped with the addition and the composition of polynomials, the set $\mathcal{L}_n(GF(q^n))$ forms a $GF(q^n)$-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 $\deg_q(L) = \max\{0 \leq i < n : l_i \neq 0\}$, and the rank of $L(x)$, denoted by $\text{rank}(L)$, is defined as the dimension of the image $\text{Im}(L) = \{L(x) | x \in GF(q^n)\}$ 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 $\alpha_1, \ldots, \alpha_r$ and $\beta_1, \ldots, \beta_r$ in $GF(q^n)$ such that

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

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

$$D = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{r-1} \\ \beta_0 & \beta_1 & \cdots & \beta_{r-1} \end{pmatrix} = \begin{pmatrix} l_0 & l_1^{q^n-1} & \cdots & l_1^{q^n-1} \\ l_1 & l_0^{q^n-1} & \cdots & l_2^{q^n-1} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^{q^n-1} & \cdots & l_0^{q^n-1} \end{pmatrix}. \quad (3)$$
where \(0 \leq i, j < n\), 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 \(d_r(A - B) = \text{Rank}(A - B)\) for \(A, B \in GF(q)^{m \times n}\).

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

Since the matrix transpose operation preserves the parameters of a rank metric code, it is commonly assumed that \(n \leq m\) without loss of generality. Assume \(\beta = \{\beta_1, \cdots, \beta_m\}\) is a basis of \(GF(q^n)\) over \(GF(q)\). It induces a one-to-one mapping \(\phi : GF(q)^{m \times n} \rightarrow GF(q^n)^n\) defined by \(\phi(A) = (\beta_1, \cdots, \beta_m)A = (a_1, \cdots, a_n)\).

A rank metric code in matrix form can be converted to a code of length \(n\) over \(GF(q^n)\) with the rank metric distance by the corresponding rank distance on \(GF(q)^{m \times n}\). Hence a rank metric code is usually represented in the vectorial form as a subset of \(GF(q^n)^n\) and the conventional notation \((n, M, d)^m\) is used to denote rank metric codes over \(GF(q^n)\) with length \(n\), \(M\) codewords and minimum rank distance \(d\).

It is well-known that a rank metric \((n, M, d)^m\) code satisfies a Singleton-like bound:

\[
M \leq q^{\min(n(m-d+1),m(n-d+1))}.
\]

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 \(\alpha = \{\alpha_1, \cdots, \alpha_m\}\) 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 \(\mathcal{L}(GF(q^n))\), we have

\[
f(x) = f(x\alpha_1 + \cdots + x_n\alpha_n) = (f(\alpha_1), \cdots, f(\alpha_n))(x_1, \cdots, x_n)^T = (\beta_1, \cdots, \beta_n)F(x_1, \cdots, x_n)^T,
\]

where \((x_1, \cdots, x_n) \in GF(q)^n\) and \(F = (f(\alpha_j))_{1 \leq j \leq n}\) is a matrix over \(GF(q)\) of which the \(j\)-th column is given by the coordinates of \(f(\alpha_j)\) under the basis \(\beta\), 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 \(\alpha\) and \(\beta\), and its rank is equal to \(\text{Rank}(f)\). Moreover, the algebra \(GF(q)^{n \times n}\) with matrix addition and multiplication has a one-to-one correspondence to the algebra \(\mathbb{L}_n(GF(q)^n)\). With such a correspondence, we will consider the algebra \(\mathbb{L}_n(GF(q)^n)\) 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 \(L(x) = \mathcal{L}(GF(q^n))\), the rank nullity theorem implies

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

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

\[
\text{Rank}(L) = n - \text{dim}(\text{Ker}(L)) \geq n - \deg_q(L)
\]

since the dimension of \(\text{Ker}(L)\) 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 \(f(x) = f_0 x + f_1 x^{q + q^2} + \cdots + f_k x^{q^k} \in \mathcal{L}_n(GF(q^n))\) 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 \(\text{Rank}(f) \geq n - k + 1\).

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 \(k \leq n\). Let \(\Gamma\) be a subset of \(GF(q^n)^2\) such that

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

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

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

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 \( h(x) = \sum_{i=0}^{k} b_i x^i \), where the coefficients \( b_0 \) and \( b_k \) satisfy \( b_k = \frac{a^k}{H_0} \). 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 \( H_{n,k,s}(\Gamma) \) has minimum rank distance at least \( n-k+1 \). On the other hand, the code \( H_{n,k,s}(\Gamma) \) has cardinality \( q^{nk} \) since \( |\Gamma| = q^k \). By the Singleton-like bound, the code \( H_{n,k,s}(\Gamma) \) 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 \( H_{n,k,s}(\Gamma) \) are the generalized Gabidulin codes [7] and they become the original Gabidulin codes [5] when \( s = 1 \);
- when \( \Gamma = \{(a, \eta a^q) : a \in GF(q^n)\} \) for certain \( \eta \) with \( \text{Norm}_{q^2/q}(\eta) \neq (-1)^{nk} \), the codes \( H_{n,k,s}(\Gamma) \) are the GTG codes discussed in [14] and they become the TG codes introduced by Sheekey [12] when \( s = 1 \);
- when \( \Gamma = \{(a, \eta a^q) : a \in GF(q^n)\} \), where \( q = q^u \) with \( u > 1 \) and \( \text{Norm}_{q^2/q}(\eta) \neq (-1)^{nk} \), the codes \( H_{n,k,s}(\Gamma) \) are the AGTG codes introduced in [15];
- when \( \Gamma = \{(a,0), (0,b) : a,b \in GF(q^n)\}, \text{Norm}_{q^2/q}(a) \in I, \text{Norm}_{q^2/q}(b) \notin (-1)^{nk}I \) for some subset \( I \subseteq GF(q) \), the codes \( H_{n,k,s}(\Gamma) \) are the non-additive partition codes proposed in [16];
- when \( n = 2m, \Gamma = \{(a, \gamma b) : a,b \in GF(q^n)\}, \text{Norm}_{q^2/q}(\gamma) \) 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 \( H_{n,k,s}(\Gamma) \) over \( GF(q) \) is completely dependent on the property of the set \( \Gamma \) over \( GF(q) \). Hence finding sets \( \Gamma \) 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 \( H_{n,k,s}(\Gamma) \) in Theorem 1. Throughout what follows we will denote \([i] := q^i, 0 \leq i < n\), for simplicity.

A. Encoding

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

For the MRD codes summarized in the previous section, we describe the derivation of the tuple \((f_0, f_k)\) as follows:

- the GTG and AGTG codes: the coefficients \((f_0, f_k) = (f_0, \eta^q f_0^q)\) with \( q = q^k \) for the GTG codes [14] and \( q < q \) for the AGTG codes [15];
- the non-additive partition codes: this case sets the coefficients \((f_0, f_k) = (f_0, 0)\) if \( \text{Norm}_{q^2/q}(f_0) \in I \) and \((f_0, f_k) = (0, (-1)^k f_0)\) otherwise. Assigning \((f_0, f_k)\) in this way guarantees that any message \((f_0, f_1, \ldots, f_{k-1})\) is properly encoded as a codeword in \( H_{n,k,s}(\Gamma) \).

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

\[
(f_0, \ldots, f_{k-1}) \mapsto (c_1, \ldots, c_n) = (\hat{f}_0, f_1, \ldots, f_{k-1}, \hat{f}_k) \cdot M',
\]

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

\[
(f_0, \ldots, f_{k-1}) \mapsto c = (c_1, \ldots, c_n) = \hat{\mathbf{f}} \cdot M',
\]

where \( \hat{\mathbf{f}} \) is an \( n \)-dimensional vector over \( GF(q^n) \) given by \( \hat{\mathbf{f}} = (f_0, f_1, \ldots, f_k, 0, \ldots, 0) \).

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 \( H_{n,k,s}(\Gamma) \). Therefore, we adopt an interpolation-based approach to decoding these codes.

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

\[
g(a_i) = e_i + c_i, \quad i = 1, \ldots, n.
\]

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

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

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

\[
(g_{k+1}, \ldots, g_{n-1}) = (\hat{r}_{k+1}, \ldots, \hat{r}_{n-1})
\]

and

\[
g_0 = \hat{r}_0 - f_0, \quad g_k = \hat{r}_k - \hat{f}_k.
\]

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

\[
G = \left[ g_{i,j}^{[j]} \right]_{n \times n} = \begin{pmatrix}
g_0^{[1]} & \cdots & g_0^{[n-1]} \\
g_1^{[1]} & \cdots & g_1^{[n-1]} \\
\vdots & \ddots & \vdots \\
g_{n-1}^{[1]} & \cdots & g_{n-1}^{[n-1]}
\end{pmatrix}
\]

has rank \( t \); and any \( t \times t \) matrix formed by \( t \) successive rows and columns in \( G \) is nonsingular.
Let $G = (G_0, G_1, \ldots, G_{n-1})$, where $G_i$ is the $i$-th column of $G$. Then $G_0$ can be expressed as a linear combination of $G_1, \ldots, G_t$, namely:

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

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

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

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

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

The above recurrence can be seen as a feedback-shift register with tap weights, and the solution $\lambda_1, \ldots, \lambda_t$ 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 $f_0$ and $f_k$. The general strategy of the reconstruction process is in the following two steps:

**Step 1.** uniquely determine $\lambda_1, \ldots, \lambda_t$ from (13), (11);

**Step 2.** recursively compute $g_0, g_1, \ldots, g_k$ by (12).

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

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

In this case, there are exactly $n-k-t-1 \geq t$ if the $(n-k-t-1) \times t$ coefficient matrix in (13) has rank $t$ and there exists a unique solution $\lambda_1, \ldots, \lambda_t$ to (13). Once $\lambda_1, \ldots, \lambda_t$ are determined in Step 1, the remaining coefficients $g_0, g_1, \ldots, g_{k-1}$ 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 $\lambda_1, \ldots, \lambda_t$ cannot be uniquely determined by (13).

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

- when $\Gamma = \{(a, \eta a^b) : \eta \in GF(q^n)\}$, where $q = q_0$, one obtains $(f_0, f_k) = (f_0, \eta f_0^b)$. Then (11) gives an equality $\eta q_0^b + g_k = \eta f_0^b + f_k$. This equality together with those in (13) also gives a unique solution $\lambda_1, \ldots, \lambda_t$. This case was recently discussed in [26], [20] for $u = 1$ and in [27] for $u > 1$;

- when $\Gamma = \{(a, 0), (0, b) : \text{Norm}_{q^n/q}(a) \in I, \ \text{Norm}_{q^n/q}(b) \in \text{GF}(q) \langle (-1)^n I, a, b \in \text{GF}(q^n) \rangle\}$ for some subset $I \subseteq \text{GF}(q)$, 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

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

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 $(f_0, f_k) = (f_0, 0)$. In this case (11) implies $g_k = \hat{r}_k$. That is to say, we get $n-k-t = t$ linear equations in variables $\lambda_1, \ldots, \lambda_t$ as follows:

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

Since the coefficient matrix has rank $t$, the above system has a unique solution $\lambda_1, \ldots, \lambda_t$. 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 $\text{Norm}_{q^n/q}((\hat{r}_k - g_0) \in I$ or not. If it is true, then the assumption $(f_0, f_k) = (f_0, 0)$ is correct and one can use $\lambda_1, \ldots, \lambda_t$ to further calculate the remaining coefficients $g_1, \ldots, g_k$ 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 $(f_0, f_k) = (0, (-1)^k f_0)$. Similarly, we derive $n-k-t = t$ linear equations in variables $\lambda_1, \ldots, \lambda_t$ as follows:

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

This system also has a unique solution $\lambda_1, \ldots, \lambda_t$ 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 $\text{Norm}_{q^n/q}((\hat{r}_k - g_k) \notin (-1)^n I$ 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 $g_0, \ldots, g_{k-1}$ recursively according to (12); otherwise the decoding fails.

From the above analysis, we summarize the decoding of the non-additive partition RM codes in Algorithm 1, where the notation $\mathcal{H}_{n,k,a}(I)$ 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 $r$ with $t \leq \frac{n-k}{2}$ errors, and linearly independent evaluation points $a_1, \ldots, a_n$.

Output: The correct codeword $c$ or “Decoding Failure”

1. Calculate $\hat{r} = (\hat{r}_0, \ldots, \hat{r}_{n-1}) = r \cdot M^{-1}$;
2. Set $(g_{k+1}, \ldots, g_{n-1}) = (\hat{r}_{k+1}, \ldots, \hat{r}_{n-1})$;
3. Apply the modified Berlekamp-Massey Alg. to find the smallest integer $t$ and $(\lambda_1, \ldots, \lambda_t)$ satisfying (13);
4. If Line 3 outputs an integer $t = \frac{n-k}{2}$ then
   5. Set $\hat{g}_t = \hat{r}_0$;
   6. Update the coefficients $(\lambda_1, \ldots, \lambda_t)$ according to (14) and the modified Berlekamp-Massey Alg.:
   7. Calculate $g_0 = \lambda_1 g_{n-1}^{[1]} + \lambda_2 g_{n-2}^{[2]} + \cdots + \lambda_t g_{n-t}^{[t]}$;
   8. If $Norm_{\mathbb{F}_q/(g_{n}/q)}(\hat{r}_0 - g_0) \not\equiv I$ then
      9. Set $g_0 = \hat{r}_0$;
     10. Update the coefficients $(\lambda_1, \ldots, \lambda_t)$ according to (15) and the modified Berlekamp-Massey Alg.:
     11. Get $g_k$ from $g_{k+i} = \sum_{j=1}^{i-1} \lambda_j g_{k+i-j} + \lambda_i g_k^{[i]}$;
     12. If $(-1)^{n-k}Norm_{\mathbb{F}_q/(\hat{r}_k - g_k)} \in I$ then
        13. Return “Decoding Failure”
   end
end

for $i \in \{0, \ldots, k\}$ do
   14. Calculate $g_i = \lambda_1 g_{n-1}^{[1]} + \lambda_2 g_{n-2}^{[2]} + \cdots + \lambda_t g_{n-t}^{[t]}$;
end

17. If $g_0, \ldots, g_{n-1}$ is successfully determined then
   18. Return the codeword $c = r - g \cdot M$
else
   19. 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