On interpolation-based decoding of a class of maximum rank distance codes

Wrya K. Kadir and Chunlei Li
Department of Informatics
University of Bergen, Norway
Email: {wrya.kadir,chunlei.li}@uib.no

Ferdinando Zullo
Dipartimento di Matematica e Fisica
Università degli Studi della Campania "Luigi Vanvitelli", Italy
Email: ferdinando.zullo@unicampania.it

Abstract

In this paper we present an interpolation-based decoding algorithm to decode a family of maximum rank distance codes proposed recently by Trombetti and Zhou. We employ the properties of the Dickson matrix associated with a linearized polynomial with a given rank and the modified Berlekamp-Massey algorithm in decoding. When the rank of the error vector attains the unique decoding radius, the problem is converted to solving a quadratic polynomial, which ensures that the proposed decoding algorithm has polynomial-time complexity.

I. Introduction

Rank metric codes were independently introduced by Delsarte [1], Gabidulin [2] and Roth [3]. Those rank metric codes that achieve Singleton-like bound are called *maximum rank distance (MRD) codes*. The well known family of MRD codes are the *Gabidulin codes*. Later this family was generalized by Kshevetskiy and Gabidulin [4] which is known as the *generalized Gabidulin (GG)* codes. These codes are linear over $\mathbb{F}_{q^n}$. Sheekey [5] introduced a large family of $\mathbb{F}_q$-linear MRD codes called *twisted Gabidulin (TG) codes*, which were extended to *generalized twisted Gabidulin (GTG) codes* by employing arbitrary automorphism [5, Remark 9], [6]. Later additive MRD codes were proposed by Otal and Özbudak [7] and they are known as *additive generalized twisted Gabidulin (AGTG) codes*. AGTG codes contain all the aforementioned MRD codes as subfamilies. There are also some other MRD codes that are not equivalent to the above codes, for instance the non-additive MRD codes by Otal and Özbudak [8], new MRD codes by Sheekey [9], *Trombetti-Zhou (TZ) codes* [10], etc. For more constructions of MRD codes, please refer to [11].

MRD codes have gained much interest in the last decades due to their wide applications in storage system [3], network coding [12] and cryptography [13]. Efficient decoding of MRD codes is critical for their applications. There are different decoding approaches for Gabidulin codes. Gabidulin [2] presented decoding based on a linearized equivalent of the Extended Euclidean Algorithm. The generalized Berlekamp-Massey algorithm was given by Richter and Plass in [14]. Later Loidreau [15] proposed the Welch-Berlekamp like algorithm to decode Gabidulin codes. Nevertheless, the above algorithms can not be directly applied to the new MRD codes with twisted evaluation polynomials. Randrianarisoa and Rosenthal in [16] proposed a decoding method for a subfamily of TG codes. Randrianarisoa in [17] gave an interpolation-based decoding algorithm for GTG codes. He reduced the decoding problem to finding zeros of projective equations. Kadir and Li in [18] applied the interpolation approach to decoding AGTG codes and studied the final projective equations in greater depth. Li [19] used a similar idea in decoding the non-additive partition MRD codes in [8].

In this paper we propose an interpolation-based decoding algorithm for TZ codes. We also compare the interpolation-based decoding algorithms for MRD codes when the rank of the error vector reaches the unique decoding radius, which shows that decoding TZ codes requires less operations than decoding GTG and AGTG codes as the problem can be reduced to solving a quadratic equation.

II. Preliminaries

Definition 1. *Let q be a power of prime p and $\mathbb{F}_{q^n}$ be an extension of the finite field $\mathbb{F}_q$. A q-polynomial is a polynomial of the form $L(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}}$ over $\mathbb{F}_{q^n}$. If $a_{k-1} \neq 0$, then we say that $L(x)$ has q-degree $k-1$. The set of these polynomials is denoted by $\mathcal{L}_k(\mathbb{F}_{q^n})$.*

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: $L(c_1x + c_2y) = c_1L(x) + c_2L(y)$ for any $c_1, c_2 \in \mathbb{F}_q$ and any x, y in an arbitrary extension of $\mathbb{F}_{q^n}$. Hence a linearized polynomial $L(x) \in \mathcal{L}_k(\mathbb{F}_{q^n})$ defines an $\mathbb{F}_q$-linear transformation L from $\mathbb{F}_{q^n}$ to itself. The rank of a nonzero linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$ is given by $\text{Rank}(L) = n - \dim_{\mathbb{F}_q}(\text{Ker}(L))$, where $\text{Ker}(L)$ is the kernel of $L(x)$.

Proposition 1. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$ be a linearized polynomial with rank t. Then its associated Dickson matrix*

$$D = \left(a^{q^i}_{i-j(\mathrm{mod} n)}\right)_{n\times n} = \begin{pmatrix} a_0 & a^q_{n-1} & \cdots & a^{q^{n-1}}_1 \\ a_1 & a^q_0 & \cdots & a^{q^{n-1}}_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a^q_{n-2} & \cdots & a^{q^{n-1}}_0 \end{pmatrix}, \tag{1}$$

has rank t over $\mathbb{F}_{q^n}$. Moreover, any $t\times t$ submatrix formed by t consecutive rows and t consecutive columns in D is non-singular.

The first part of Prop. 1 is given in [20], whereas the second part can be found in [17] and [21].

III. Maximum rank distance (MRD) codes

The rank of a vector $a = (a_1, \ldots, a_n)$ in $\mathbb{F}^n_{q^m}$, denoted as $\mathrm{Rank}(a)$, is the number of its linearly independent components, that is the dimension of the vector space spanned by a_i's over $\mathbb{F}_q$. The rank distance between two vectors $a, b \in \mathbb{F}^n_{q^m}$ is defined as $d_R(a, b) = \mathrm{Rank}(a - b)$.

Definition 2. *A subset $\mathcal{C} \subseteq \mathbb{F}^n_{q^m}$ with respect to the rank distance is called a rank metric code. When $\mathcal{C}$ contains at least two elements, the minimum rank distance of $\mathcal{C}$ is given by $d(\mathcal{C}) = \min_{A,B\in\mathcal{C},\ A\neq B}\{d_R(A, B)\}$. Furthermore, it is called a maximum rank distance (MRD) code if it attains the Singleton-like bound $|\mathcal{C}| \leq q^{\min\{m(n-d+1),n(m-d+1)\}}$.*

The most famous MRD codes are Gabidulin codes [2] which were further generalized in [4], [22]. The generalized Gabidulin (GG) codes $\mathcal{GG}_{n,k}$ with length $n \leq m$ and dimension k over $\mathbb{F}_{q^m}$ is defined by the evaluation of

$$\left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} \ | f_i \in \mathbb{F}_{q^m} \right\}, \tag{2}$$

where $(s, m) = 1$, on linearly independent points $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ in $\mathbb{F}_{q^m}$. The choice of α_i's does not affect the rank property and it is customary to exhibit Gabidulin codes and its generalized families without the evaluation points as in (2). For consistency with the parameters of MRD codes in [5], [7], [10], through what follows we always assume $n = m$.

For a linearized polynomial $L(x) = \sum_{i=0}^{k} l_i x^{q^i}$ over $\mathbb{F}_{q^n}$, it is clear that $\mathrm{Rank}(L) \geq n - k$ if $l_k \neq 0$. Gow and Quinlan in [23, Theorem 10] (see also [5]) characterize a necessary condition for $L(x)$ to have rank $n - k$ as below, see [24], [25] for other necessary conditions.

Lemma 1. *[23] Suppose a linearized polynomial $L(x) = l_0 x + l_1 x^q + \cdots + l_k x^{q^k}$, $l_k \neq 0$, in $\mathcal{L}_n(\mathbb{F}_{q^n})$ has q^k roots in $\mathbb{F}_{q^n}$. Then $\mathrm{Norm}_{q^n/q}(l_k) = (-1)^{nk}\,\mathrm{Norm}_{q^n/q}(l_0)$, where $\mathrm{Norm}_{q^n/q}(x) = x^{1+q+\cdots+q^{n-1}}$ is the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.*

According to Lemma 1, a linearized polynomial $L(x)$ of q-degree $k-1$ has rank at least $n-k+1$ if the condition in Lemma 1 is not met. Sheekey [5] applied Lemma 1 and constructed a new family of MRD codes, known as *twisted Gabidulin (TG) codes*, and the generalized TG codes are investigated in [6]. Later Otal and Özbudak [7] further generalized this family by manipulating some terms of linearized polynomials and constructed the *additive generalized twisted Gabidulin (AGTG) codes* which contains all the aforementioned MRD codes as subfamilies.

Below we recall from [10] the *Trombetti-Zhou (TZ) code*, which has been proved to be inequivalent to subfamilies of AGTG codes, further generalized twisted Gabidulin codes [26], Sheekey's new MRD codes [9] and those with minimum distance equals to $n - 1$, such as [27], [28]. We are going to propose an interpolation-based decoding algorithm for TZ codes in the next section.

Proposition 2. *[10] Let $n, k, s \in \mathbb{Z}^+$ satisfying $(s, 2n) = 1$ and let $\gamma \in \mathbb{F}_{q^{2n}}$ satisfy that $Norm_{q^{2n}/q}(\gamma)$ is a non-square element in $\mathbb{F}_q$. Then the set*

$$\mathcal{D}_{k,s}(\gamma) = \left\{ ax + \sum_{i=1}^{k-1} f_i x^{q^{si}} + \gamma b x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^{2n}}, a, b \in \mathbb{F}_{q^n} \right\}$$

is an $\mathbb{F}_{q^n}$-linear MRD code of size q^{2nk} and minimum rank distance $2n - k + 1$.

The first and the last coefficients of the above polynomial are chosen independently from the base field $\mathbb{F}_{q^n}$. If q is even, all the elements of $\mathbb{F}_q$ are square elements, so TZ codes exist only when the characteristic of $\mathbb{F}_q$ is odd.

IV. Encoding and decoding of TZ codes

For the rest of this paper, we will denote $[i] := q^{si}$ for $i = 0, \ldots, 2n-1$, where $(s, 2n) = 1$, for simplicity.

A. Encoding

For a TZ MRD code with evaluation points $\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}$ that are linearly independent over $\mathbb{F}_q$, the encoding of a message $f = (f_0, \ldots, f_{k-1})$ is the evaluation of the following linearized polynomial at points $\alpha_0, \alpha_1, \ldots, \alpha_{2n-1}$:

$$f(x) = ax + \sum_{i=1}^{k-1} f_i x^{[i]} + \gamma b x^{[k]}, \tag{3}$$

where $(a, b) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ corresponds to f_0 via an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^{2n}}$. Let $\tilde{f} = (a, f_1, \ldots, f_{k-1}, \gamma b, 0, \ldots, 0)$ be a vector of length $2n$ over $\mathbb{F}_{q^{2n}}$ and $M = \left(\alpha_i^{[j]}\right)_{2n\times 2n}$ be the $2n \times 2n$ *Moore matrix* generated by α_i's, where $1 \le i, j \le 2n-1$. Then the encoding of TZ codes can be expressed as

$$(a, f_1, \ldots, f_{k-1}, \gamma b) \mapsto c = (f(\alpha_0), \ldots, f(\alpha_{2n-1})) = \tilde{f} M^T, \tag{4}$$

where M^T is the transpose of matrix M. Here it is worth noting that in encoding process, one actually only needs to calculate the multiplication of the $(k+1)$-tuple $(a, f_1, \ldots, f_{k-1}, \gamma b)$ and the first $k+1$ rows of M. Here we express it as in (4) for being consistent with the decoding procedure.

B. Decoding

For a received word $r = c + e$ with an error e added to the codeword c during transmission, when the error e has rank $t \le \lfloor \frac{2n-k}{2} \rfloor$, the unique decoding task is to recover the unique codeword c such that $d_R(c, r) \le \lfloor \frac{2n-k}{2} \rfloor$.

Suppose $g(x) = \sum_{i=0}^{2n-1} g_i x^{[i]}$ is an error interpolation polynomial such that

$$g(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \ldots, 2n-1. \tag{5}$$

It is clear that the error vector e is uniquely determined by the polynomial $g(x)$ and denote $\tilde{g} = (g_0, \ldots, g_{2n-1})$. From (4) and (5) it follows that

$$r = c + e = (\tilde{f} + \tilde{g}) M^T.$$

This is equivalent to

$$\begin{aligned} r \cdot (M^T)^{-1} =& (a,\ f_1,\ \ldots, f_{k-1}, \gamma b, 0, \ldots, 0) + \\ & (g_0, g_1, \ldots, g_{k-1}, g_k, g_{k+1}, \ldots, g_{2n-1}). \end{aligned}$$

Letting $\beta = (\beta_0, \ldots, \beta_{2n-1}) = r \cdot (M^T)^{-1}$, we obtain

$$(g_{k+1}, \ldots, g_{2n-1}) = (\beta_{k+1}, \ldots, \beta_{2n-1}) \tag{6}$$

and

$$\begin{cases} g_0 + a = \beta_0 \\ g_k + \gamma b = \beta_k \end{cases} \rightarrow \begin{cases} g_0 - \beta_0 = -a \\ \gamma^{-1}(g_k - \beta_k) = -b. \end{cases}$$

With $a, b \in \mathbb{F}_{q^n}$, one obtains

$$\begin{cases} (g_0 - \beta_0)^{[n]} = g_0 - \beta_0 \\ (\gamma^{-1}(g_k - \beta_k))^{[n]} = \gamma^{-1}(g_k - \beta_k). \end{cases} \tag{7}$$

which yields two linearized equations

$$\begin{cases} g_0^{[n]} - g_0 - \theta_1 = 0, & (8) \\ g_k^{[n]} - \gamma^{[n]-1} g_k - \theta_2 = 0, & (9) \end{cases}$$

where $\theta_1 = \beta_0^{[n]} - \beta_0,\ \theta_2 = \beta_k^{[n]} - \gamma^{[n]-1}\beta_k$.

Therefore, the task of correcting error e is equivalent to reconstructing $g(x)$ from the available information characterized in (6), (8) and (9). This reconstruction process heavily depends on the property of the associated Dickson matrix of $g(x)$ and will be discussed in Subsection IV-C.

C. Reconstructing the interpolation polynomial $g(x)$

The Dickson matrix associated with $g(x)$ can be given by

$$G = \left(g^{[j]}_{i-j \pmod{2n}}\right)_{2n\times 2n} = (G_0\ G_1\ \ldots\ G_{2n-1}), \tag{10}$$

where the indices i, j run through $\{0, 1, \ldots, 2n-1\}$ and G_j is the j-th column of G.

Since $\gcd(2n, s) = 1$, Proposition 1 can be easily adapted for the Dickson matrix G in (10). Hence G has rank t and any $t \times t$ matrix formed by t successive rows and columns in G is nonsingular. 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 $\mathbb{F}_{q^{2n}}$. This yields the following recursive equations

$$g_i = \lambda_1 g^{[1]}_{i-1} + \lambda_2 g^{[2]}_{i-2} + \cdots + \lambda_t g^{[t]}_{i-t}, \quad 0 \le i < 2n, \tag{11}$$

where the subscripts in g_i's are taken modulo $2n$. Recall that the elements $g_{k+1}, \ldots, g_{2n-1}$ are known from (6). Hence we obtain the following linear equations with known coefficients and variables $\lambda_1, \ldots, \lambda_t$:

$$g_i = \lambda_1 g^{[1]}_{i-1} + \lambda_2 g^{[2]}_{i-2} + \cdots + \lambda_t g^{[t]}_{i-t},\ k + t + 1 \le i < 2n. \tag{12}$$

The above recurrence gives a generalized version of q-linearized shift register as described in [29], where $(\lambda_1, \ldots, \lambda_t)$ is the connection vector of the shift register. It is the *key equation* for the decoding algorithm in this paper, by which we shall reconstruct $g(x)$ in two major steps:

Step 1. derive $\lambda_1, \ldots, \lambda_t$ from (6)-(9), and (12);

Step 2. use $\lambda_1, \ldots, \lambda_t$ to compute $g_k, \ldots, g_0$ from (11).

Step 1 is the critical and challenging step in the decoding process, and Step 2 is simply a recursive process that can be done in linear time in $\mathbb{F}_{q^{2n}}$. The following discussion shows how the procedure of Step 1 works.

As discussed in the beginning of this section, for an error vector with $\mathrm{Rank}(e) = t \le \lfloor \frac{2n-k}{2} \rfloor$, i.e., $2t + k \le 2n$, we can divide the discussion into two cases.

Case 1: $2t + k < 2n$. In this case, (12) contains $2n - k - t - 1 \ge t$ affine equations in variables $\lambda_1, \ldots, \lambda_t$, which has rank t. Hence the variables $\lambda_1, \ldots, \lambda_t$ can be uniquely determined. In this case, the code can be seen as a sub-code of an $\mathcal{GG}_{2n,k+1}$ code and any Gabidulin codes decoding algorithm is applicable. Here we assume the code has high code rate, for which the Berlekamp-Massey algorithm is more efficient. In addition it is consistent with the notation used in Case 2. Although the recurrence equation (12) is a generalized version of the ones in [14], [29], the modified Berlekamp-Massey algorithm can be applied here to recover the coefficients $\lambda_1, \ldots, \lambda_t$.

Case 2: $2t + k = 2n$. In this case (12) gives $2n - k - t - 1 = t - 1$ independent affine equations in variables $\lambda_1, \ldots, \lambda_t$. For such an under-determined system of linear equations, we will have a set of solutions $(\lambda_1, \ldots, \lambda_t)$ that has dimension 1 over $\mathbb{F}_{q^{2n}}$. Namely, the solutions will be of the form

$$\lambda + \omega\lambda' = (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t),$$

where λ, λ' are fixed elements in $\mathbb{F}^t_{q^{2n}}$ and ω runs through $\mathbb{F}_{q^{2n}}$. As shown in [29, Th. 10], the solution can be derived from the modified BM algorithm with a free variable ω. Next we will show how the element ω is determined by other information in (6), (8) and (9).

Observe that in (11), by taking $i = 0$ and $i = k + t$ and substituting the solution $\lambda + \omega\lambda'$, one gets the following two equations

$$\begin{aligned} g_0 &= (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t) \cdot (g^{[1]}_{2n-1}, \ldots, g^{[t]}_{2n-t})^T, \\ g_{k+t} &= (\lambda_1 + \omega\lambda'_1, \ldots, \lambda_t + \omega\lambda'_t) \cdot (g^{[1]}_{k+t-1}, \ldots, g^{[t]}_{k})^T, \end{aligned}$$

where g_0, g_k and ω are the only unknowns. Re-arranging the equations gives

$$g_0 = c_0 + c_1\omega, \tag{13}$$

and

$$g_{k+t} = c_2 + c_3\omega + (\lambda_t + \lambda'_t\omega) g^{[t]}_k, \tag{14}$$

where c_0, c_1, c_2, c_3 are derived from λ, λ' and the known coefficients g_i's. Furthermore, from (8) and (9) we have $g^{[n]}_0 - g_0 + \theta_1 = 0$ and $g^{[n]}_k - \gamma^{[n]-1} g_k + \theta_2 = 0$. Substituting (13) in (8) gives

$$c_1\omega^{[n]} + \beta_1\omega + \beta_2 = 0. \tag{15}$$

If $\lambda_t + \lambda'_t\omega = 0$ then we have the solution $\omega = -\lambda_t/\lambda'_t$. This solution can be further checked in (14) by g_{k+1}, c_2 and c_3. Otherwise, one can raise both sides of (14) to the $[2n-t]$-th power and obtain

$$g_k = \frac{a_1 + a_2\omega^{[2n-t]}}{a_3 + a_4\omega^{[2n-t]}}. \tag{16}$$

Replacing this value in (9), raising it to the $[t]$-th power and rearranging the terms implies

$$\zeta_1\omega^{[n]+1} + \zeta_2\omega^{[n]} + \zeta_3\omega + \zeta_4 = 0, \tag{17}$$

where $\zeta_1 = (a_2^{[n]}a_4 + \theta_2 a_4^{[n+t]})^{[t]}$. Furthermore, by (15) and (17) we have the following quadratic equation over $\mathbb{F}_{q^{2n}}$

$$\zeta_1 x^2 + \zeta_5 x + \zeta_6 = 0. \tag{18}$$

When $\zeta_1 = 0$ and $\zeta_2 \neq 0$, the unknown ω can be uniquely determined. When $\zeta_1 \neq 0$, the above quadratic equation can be reduced to

$$x^2 + rx + s = 0, \tag{19}$$

where $r = \zeta_5/\zeta_1$ and $s = \zeta_6/\zeta_1$.

Since the characteristic of $\mathbb{F}_q$ is odd, Equation (19) can be solved explicitly as follows:

a) if $r^2 - 4s$ is a quadratic residue in $\mathbb{F}_{q^{2n}}$, then it has two solutions $x = \frac{-r \pm \sqrt{r^2-4s}}{2}$;
b) if $r^2 = 4s$, then it has a single solution $x = -r/2$;
c) it has no solution in $\mathbb{F}_{q^{2n}}$ otherwise.

Since the error e with rank $t = \frac{2n-k}{2} = \frac{d-1}{2}$ can be uniquely decoded, our quadratic equation should have roots w in $\mathbb{F}_{q^{2n}}$ that lead to solutions $\lambda + \omega\lambda'$ in (12) and (g_0, g_k) in (13). With the coefficients $\lambda_1, \ldots, \lambda_t$ in Step 1 and the initial state $g_{2n-1}, \ldots, g_{2n-t}$, one can recursively compute $g_0, \ldots, g_{k-1}$ according to (11) in Step 2. Note that even if the equation (18) has two different solutions, they don't necessarily lead to correct coefficients of the error interpolation polynomial. In fact, by the expression of Dickson matrix of $g(x)$, the correct $g(x)$ should have the sequence $(g_{2n-1}, \ldots, g_{2n-t}, \ldots)$ generated from (11) has period $2n$. In other words, if the output sequence has period $2n$, we know that the corresponding polynomial $g(x) = \sum_{i=0}^{2n-1} g_i x^{[i]}$ is the desired error interpolation polynomial. For self-completeness, the decoding process of TZ codes is summarized in Algorithm 1.

D. Complexity Analysis

As summarized in Algorithm 1, we have two major steps to construct the error interpolation polynomial $g(x)$. The first step is to use the modified BM algorithm for obtaining the coefficients $\lambda_1, \ldots, \lambda_t$. Calculating the interpolation polynomial at points (α_i, r_i) has complexity in the order of $\mathcal{O}(n^3)$, but according to [30], if $\alpha_0, \ldots, \alpha_{2n-1}$ is taken as a self-dual normal basis, M is orthogonal, which means $M^T = M^{-1}$ and computation of $(M^T)^{-1}$ is no longer required. So the complexity of computing polynomial β is reduced to $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. The second major component of the first step is the modified BM algorithm which is known to have complexity in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. The second step is to deal with the case $t = \lfloor (2n-k)/2 \rfloor$ by investigating the solutions of the equation (18). This step involves checking whether $(r^2 - 4s)$ is a quadratic residue or not. In order to check whether an element $a \in \mathbb{F}_{q^{2n}}$ is square or not, one calculates $a^{\frac{q^{2n}-1}{2}} = a^{\frac{q-1}{2}\cdot(q^{2n-1}+\cdots+q+1)} = b^{q^{2n-1}+\cdots+q+1}$ which has complexity $\mathcal{O}(n)$ over $\mathbb{F}_{q^{2n}}$, or directly check its exponent if in implementation an element in $\mathbb{F}_{q^{2n}}$ is represented in exponential form. As a result, the complexity of our decoding method is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$.

Therefore, the previous two sections imply the following result.

Theorem 1. *Consider the evaluation code obtained from $\mathcal{D}_{k,s}(\gamma)$ over an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$. Every received word can be uniquely decoded up to rank $t \leq \frac{2n-k}{2}$ errors in polynomial time.*

V. Comparing the known decoding algorithms

Known decoding algorithms for Gabidulin codes can be generally classified in two different approaches: syndrome decoding as in [2], [3], [13], [14] and interpolation-based decoding as in [15], [17]–[19], [31]. When the rank of the error vector reaches the maximal unique decoding radius, syndrome decoding approach works only for $\mathbb{F}_{q^n}$-linear MRD codes. Since Sheekey [5] introduced TG codes, which is not always $\mathbb{F}_{q^n}$-linear, a new (non syndrome) decoding algorithm for rank metric codes has been required for the extreme case when $t = \lfloor \frac{n-k}{2} \rfloor$. When the rank of the error is not the maximal unique decoding radius, i.e., $t < \lfloor \frac{n-k}{2} \rfloor$, the syndrome decoding algorithms are still applicable. Loidreau [15] proposed the first interpolation-based decoding approach for MRD codes and considered the analogue of Welch-Berlekamp algorithm, which was originally used to decode Reed-Solomon codes. Later Randrianarisoa [17] employed Berlekamp-Massey algorithm as the main seed and introduced a decoding algorithm for GTG codes. Later Kadir and Li [18], [31] used the same idea to decode AGTG codes. In the rest of this section, we compare the existing interpolation-based decoding algorithms for MRD codes when $t = \lfloor \frac{n-k}{2} \rfloor$.

Algorithm 1: Interpolation decoding of TZ codes

Input: A received word r with $t \leq \lfloor \frac{2n-k}{2} \rfloor$ errors and linearly independent evaluation points $\alpha_1, \ldots, \alpha_{2n}$
Output: The correct codeword $c \in \mathbb{F}_{q^{2n}}^n$ or "Decoding Failure"

Calculate $\beta(x) = \sum_{i=0}^{2n-1} \beta_i x^{[i]}$ such that $\beta(\alpha_i) = r_i$ for $i = 1, \ldots, 2n$;
Apply modified BM algorithm to $(g_{k+1}, \ldots, g_{2n-1}) = (\gamma_{k+1}, \ldots, \gamma_{2n-1})$ and output L, $\Lambda^{(2n-k-1)}(x)$, $B^{(2n-k-1)}(x)$;
if $L = (2n-k)/2$ **then**
    Denote $\Delta = \omega + \sum_{i=1}^{L} \Lambda_i^{(2n-k-1)} g_{2n-1-i}^{q^{si}}$ with $\omega \in \mathbb{F}_{q^{2n}}$;
    Express the coefficients of the polynomial

$$\Lambda^{(2n-k)}(x) = \Lambda^{(2n-k-1)}(x) - \frac{1}{\Delta} x^{q^s} \circ B^{(2n-k-1)}(x),$$

    Derive the vector $\lambda + \lambda'\omega$ by negating the coefficients of $\Lambda^{(2n-k)}(x)$;
    if $\lambda_t + \lambda_t'\omega = 0$ **then**
        $\omega = -\lambda_t/\lambda_t'$;
    else
        Derive the polynomial $P(x) = \zeta_1 x^2 + \zeta_5 x + \zeta_6$ as in (18);
        if $\zeta_1 \neq 0$ **then**
            Solve $P(x) = 0$ by Cases a)-c) after (19);
        else
            The zero of $P(x)$ is $x = \zeta_6/\zeta_5$;
        end
    end
    Set $(\lambda_1, \ldots, \lambda_t) = \lambda + \omega\lambda'$ with ω as the zero of $P(x)$;
    Calculate g_0, g_k from (13) and (14);
end
for *each* i *in* $\{0, \ldots, k\}$ **do**
    Calculate $g_i = \lambda_1 g_{i-1}^{[1]} + \cdots + \lambda_t g_{i-t}^{[t]}$, where the subscripts of g_j's are taken modulo $2n$;
end
if *The sequence* $g_0, \ldots, g_{2n-1}$ *derived from* $\lambda_1, \ldots, \lambda_t$ *has period* $2n$ **then**
    Return the codeword $c = (c_0, \ldots, c_{2n-1})$ with $c_i = r_i - g(\alpha_i)$
else
    Return "Decoding Failure"
end

The goal of the WB algorithm is to find two linearized polynomials V and N with q-degrees less than or equal to t and less than $k+t$, respectively, which satisfy the system of equations $V(r_i) - N(\alpha_i) = 0$ where $i = 1, \ldots, n$. The system is a linear system consists of n equations and $n+1$ unknowns. This is equivalent to interpolating two pairs of linearized polynomials (V_0, N_0) and (V_1, N_1). After an initialization step, the polynomials are interpolated via a loop with indices ranging from k to $n-1$. If one manages to bound the q-degree of the polynomials as $\deg_q(V_j) \leq t$ and $\deg_q(N_j) \leq k+t-1$ for $j = 0$ or 1, it is done. The complexity of the WB algorithm is in the order of $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^n}$.

The decoding algorithms in [17] and [18] interpolated the polynomial $f(x) + g(x)$ where $f(x)$ and $g(x)$ correspond to message vector c and error vector e, respectively. The decoding problem is reduced to the problem of solving an underdetermined system of linear equations with $t-1$ equations and t unknowns. This approach benefits from the properties of Dickson matrix associated with $g(x)$, known coefficients of $g(x)$ and the relation between f_0 and f_k which enable us to convert the system of equations to a single projective polynomials of the form $P(x) = x^{q^v+1} + u_1 x + u_2 = 0$ for GTG and AGTG codes. The zeros of this polynomial were discussed in [18] when $(v, n) = 1$. Very recently Kim *et al.*in [32] provide the complete solution of $P(x) = 0$ over $\mathbb{F}_{q^n}$ for any power prime q and any integers n and v. Note that the relation between the coefficients of the first and the last terms of $f(x)$ in the decoding algorithm for TZ codes provides more useful information than the corresponding equations for GTG and AGTG codes. It turns out that we only need to deal with a quadratic polynomial instead of a projective polynomial. This makes the decoding algorithm for TZ codes faster than decoding GTG and AGTG codes.

VI. Conclusion

In this paper we proposed an interpolation-based decoding algorithm for Trombetti-Zhou MRD codes. We have shown that the decoding algorithm has polynomial time complexity as low as $\mathcal{O}(n^2)$ over $\mathbb{F}_{q^{2n}}$. It involves Berlekamp-Massey algorithm similar to the decoding approaches in [17], [18] but end up with a quadratic polynomial, rather than a projective polynomial, which requires less operations ($\mathcal{O}(n)$) to compute the zeros.

REFERENCES

[1] 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.

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

[3] 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.

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

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

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

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

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

[9] J. Sheekey, "New semifields and new MRD codes from skew polynomial rings," *Journal of the London Mathematical Society*, vol. 101, no. 1, pp. 432–456, 2020.

[10] 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, 2019.

[11] J. Sheekey, "MRD codes: Constructions and connections," *arXiv.org.*, vol. abs/1904.05813, 2019.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

[18] W. K. Kadir and C. Li, "On decoding additive generalized twisted gabidulin codes," *Cryptography and Communications*, vol. 12, pp. 987 – 1009, 2020.

[19] C. Li, "Interpolation-based decoding of nonlinear maximum rank distance codes," in *International Symposium on Information Theory (ISIT)*, 2019.

[20] B. Wu and Z. Liu, "Linearized polynomials over finite fields revisited," *Finite Fields and Their Applications*, vol. 22, pp. 79–100, 2013.

[21] B. Csajbók, "Scalar q-subresultants and dickson matrices," *Journal of Algebra*, vol. 547, pp. 116–128, 2020.

[22] R. M. Roth, "Tensor codes for the rank metric," *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 2146–2157, 1996.

[23] R. Gow and R. Quinlan, "Galois theory and linear algebra," *Linear Algebra and its Applications*, vol. 430, no. 7, pp. 1778 – 1789, 2009, special Issue in Honor of Thomas J. Laffey.

[24] B. Csajbók, G. Marino, O. Polverino, and F. Zullo, "A characterization of linearized polynomials with maximum kernel," *Finite Fields and Their Applications*, vol. 56, pp. 109 – 130, 2019.

[25] G. McGuire and J. Sheekey, "A characterization of the number of roots of linearized and projective polynomials in the field of coefficients," *Finite Fields and Their Applications*, vol. 57, pp. 68 – 91, 2019.

[26] S. Puchinger, J. Rosenkilde, and J. Sheekey, "Further generalisations of twisted Gabidulin codes," in *Proceedings of the 10th International Workshop on Coding and Cryptography*, 2017.

[27] B. Csajbók, G. Marino, O. Polverino, and C. Zanella, "A new family of MRD-codes," *Linear Algebra and its Applications*, vol. 548, p. 203 – 220, 2018.

[28] B. Csajbók, G. Marino, and F. Zullo, "New maximum scattered linear sets of the projective line," *Finite Fields and Their Applications*, vol. 54, pp. 133 – 150, 2018.

[29] 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.

[30] S. Gao, "Normal Bases over Finite Fields," PhD Thesis, University of Waterloo, Department of Combinatorics and Optimization, 1993.

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

[32] K. H. Kim, J. H. Choe, and S. Mesnager, "Complete solution over $\mathrm{GF}p^n$ of the equation $x^{p^k+1} + x + a = 0$," *arXiv.org.*, vol. abs/2101.01003, 2021.