On decoding additive generalized twisted Gabidulin codes

Chunlei Li and Wrya K. Kadir

University of Bergen, Bergen, Norway
{chunlei.li, wrya.kadir}@uib.no

Abstract. The additive generalized twisted Gabidulin codes, recently introduced by Otal and Özbudak, is a large family of maximum rank distance (MRD) codes, which covers almost all the known linear MRD codes and some non-linear MRD codes. We introduce an interpolation approach to decoding these MRD codes and also discuss the complexity of the proposed decoding algorithm.

Keywords: Rank-metric · Maximum rank distance codes · Gabidulin codes · Generalized twisted Gabidulin codes

1 Introduction

Error correction codes with rank metric have gained steady attention in the literature due to their applications in various areas, including space-time coding [9], random network coding [20] and cryptography [2]. Many important properties of rank metric codes were established in the pioneering works by Delsarte [1], Gabidulin [3] and Roth [17]. Independently in [1], [3], [17], a rank metric Singleton bound was established and the *maximum rank distance* (MRD) codes achieving the bound with equality were constructed. Gabidulin codes, the rank metric analogues of Reed-Solomon codes, are the most famous sub-family of MRD codes and have been extensively studied in the last decades.

Since the invention of Gabidulin codes, it had been an open question whether other MRD codes exist. Gabidulin codes were firstly generalized in [18], [6], where the Frobenious automorphism in the original Gabidulin codes was generalized to arbitrary automorphisms and the resulting codes are known as the *generalized Gabidulin codes*. Significant progresses were made in the construction of new MRD codes in the last few years. The first non-(generalized) Gabidulin MRD codes were introduced independently by Sheekey [19] and Otal and Özbudak [10], where the latter were contained in the former as a special case. The *twisted Gabidulin codes* introduced in [19] are defined by adding an extra monomial to the evaluation polynomial of a Gabidulin codes with its coefficient satisfying certain condition that lead to new MRD codes. The *generalized twisted Gabidulin codes*, which employed arbitrary automorphism, were later intensively studied in [8] and were shown to contain new MRD codes inequivalent to the known ones. Very recently Otal and Özbudak [11] introduced a family of additive rank metric codes, known as the *additive generalized twisted Gabidulin* codes, which covers all the aforementioned linear MRD codes as well as some nonlinear MRD codes.

These new constructions and several further constructions of MRD codes were lately summarized in [12].

For different polynomial-time decoding algorithms for Reed-Solomon codes, their rank metric variants for Gabidulin codes were proposed [3], [17], [15], [7] and some of them were further accelerated [21], [22]. However, it appears that the known decoding algorithms for Gabidulin codes cannot be trivially applied to those new MRD codes. By modifying the decoding algorithm by Kötter and Kschischang for subspace codes [5], Randrianarisoa and Rosenthal made an attempt to decode the twisted Gabidulin codes in [16]. Yet the proposed decoding algorithm only works for a particular case of the twisted Gabudulin codes. Very recently the problem was further studied by Randrianarisoa in [14], where an interpolation approach was proposed and briefly discussed.

In this paper, we further explore the interpolation-based approach introduced in [14] and intensively investigate the zeros of a certain polynomial. As a result we obtain an efficient decoding algorithm for the additive generalized twisted Gabidulin codes. Our decoding algorithm can correct errors up to the error correcting ability of such codes for all parameters, indicating that it works for all the aforementioned MRD codes. We also show that the complexity of the decoding algorithm is dominated by the modified Berlekamp-Massey algorithm in [15] which has quadratic complexity in the code length. The remainder of this paper is organized as follows: Section 2 recalls some preliminaries and summarizes the relation among aforementioned known MRD codes. Section 3 is dedicated to the interpolation decoding algorithm for the additive generalized twisted Gabidulin codes, where Subsection 3.1 describes the decoding approach; Subsection 3.2 explains the reconstruction process and identifies a critical task in the decoding algorithm; Subsection 3.3 investigates the task in detail, and Subsection 3.4 summarizes the procedure of the decoding algorithm and briefly discusses its complexity. Section 4 concludes the work.

2 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 $r \geqslant 1$.

2.1 Linearized Polynomial

A polynomial over $GF(q^n)$ of the form $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ is known as a *linearized polynomial* over $GF(q^n)$ as it induces a $GF(q)$-linear transformation. The q-degree of a nonzero linearized polynomial $L = \sum_{i=0}^{n-1} l_i x^{q^i}$ is given by $\deg_q(L(x)) = \max\{0 \leqslant i < n : l_i \neq 0\}$. Considered as maps from $GF(q^n)$ to itself over $GF(q)$, linearized polynomials are generally taken as

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

Let $\mathcal{L}_n(GF(q^n))$ be the set of all polynomials of the form in (1). Equipped with the operations of component-wise addition and composition of polynomials, $\mathcal{L}_n(GF(q^n))$ forms a non-commutative $GF(q)$-algebra.

For a linearized polynomial $L(x)$ in $\mathcal{L}_n(GF(q^n))$, its *rank*, denoted by Rank(L), is defined as the rank of its coefficients over $GF(q)$ and can be given by Rank$(L) = n - \dim_q(\text{Ker(L)})$, where Ker$(L)$ is the set of roots of $L(x)$ in $GF(q^n)$. It is readily seen that the rank of a linearized polynomial $L(x)$ of q-degree k satisfies Rank$(L) \geqslant n - k$ since Ker(L) has at most q^k elements. The following proposition characterizes an interesting property of the Dickson matrix associated with a linearized polynomial, which is important for the decoding approach in this paper.

Proposition 1. *[14] Assume a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i} \in \mathcal{L}(GF(q^n))$ has rank k. Then its associated Dickson matrix*

$$D = \left[l_{i-j \pmod n}^{q^i}\right]_{n\times n} = \begin{bmatrix} l_0 & l_{n-1}^q & \cdots & l_1^{q^{n-1}} \\ l_1 & l_0^q & \cdots & l_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^q & \cdots & l_0^{q^{n-1}} \end{bmatrix} \tag{2}$$

also has rank k. Moreover, any $k \times k$ submatrix that is formed by k consecutive rows and k consecutive columns in D is invertible.

2.2 Maximum Rank Distance (MRD) Codes

Let n and m be two positive integers. A *rank norm* of a vector $(a_1, a_2, \ldots, a_n) \in GF(q^m)^n$ is defined as the maximal number of linear independent coordinates a_i over $GF(q)$. The *rank distance* between two vectors is defined as the norm of the difference of these vectors.

Definition 1. *A rank metric (n, M, d)-code over $GF(q)$ is a subset of $GF(q^m)^n$ with size M and minimum rank distance d. Furthermore, it is called a maximum rank distance (MRD) code if it attains the Singleton-like bound $M \leqslant q^{\min\{n(m-d+1),m(n-d+1)\}}$.*

Throughout what follows we will restrict our discussion to the case that $n = m$.

Evaluations of a linearized polynomial $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$ at points $a_1, \ldots, a_n \in GF(q^n)$ can be expressed as $(l_0, \ldots, l_{n-1})\mathcal{M}$, where $\mathcal{M} = \left[a_{i+1}^{q^j}\right]_{n\times n}$ with $0 \leqslant i, j < n$, is the Moore matrix generated from $a_1, \ldots, a_n$. It's well-known that a Moore square matrix $\mathcal{M}$ generated from n elements a_i's in $GF(q^n)$ is non-singular if and only if $a_1, a_2, \ldots, a_r$ are linearly independent over $GF(q)$. Hence, for n elements $a_1, a_2, \ldots, a_n$ in $GF(q^n)$ that are linearly independent over $GF(q)$, one easily obtains a one-to-one correspondence between $\mathcal{L}_n(GF(q^n))$ and $GF(q^n)^n$.

In the sequel we assume $n = m$, $a_1, a_2, \ldots, a_n$ are linearly independent evaluation points and will recall the known MRD codes in terms of their corresponding linearized polynomials in $\mathcal{L}_n(GF(q^n))$.

The Gabidulin code $\mathcal{G}$ over $GF(q^n)$ with length n and dimension k is defined by

$$\mathcal{G} = \left\{l_0 x + l_1 x^q + \cdots + l_{k-1} x^{q^{k-1}} : \ l_i \in GF(q^n)\right\}. \tag{3}$$

The Gabidulin codes are MRD codes [3] and have found applications in random linear coding [5], [20] and cryptography [2]. In the following we recall a family of MRD codes proposed by Otal and Özbudak [11].

Proposition 2. *[11] Let $n, k, s, h \in \mathbb{Z}^+$ satisfying $(s, n) = 1$ and $k < n$. Let $q = q_0^u$ and $\eta \in GF(q^n)$ such that $\eta^{\frac{q^{sn}-1}{q_0^s-1}} \neq (-1)^{nku}$. Then the set*

$$\mathcal{H}_{k,s,q_0}(\eta, h) = \left\{ l_0 x + l_1 x^{q^s} + \cdots + l_{k-1} x^{q^{s(k-1)}} + \eta l_0^{q_0^h} x^{q^{sk}} \; : \; l_i \in GF(q^n) \right\} \quad (4)$$

is an $GF(q_0)$-linear (but does not need to be $GF(q)$-linear) MRD code of size q^{nk} and distance $n - k + 1$.

The code defined by (4) is called *additive generalized twisted Gabidulin code* or AGTG code for short. From the definitions in (3) and (4), the relations of the existing MRD codes (except for the further generalized twisted Gabidulin codes lately discussed by Puchinger et.al [13]) can be summarized as follows [12]:

- If $u|h$, an AGTG code is a GTG (generalized twisted Gabidulin) code [8].
- If $u|h$ and $s = 1$, an AGTG code is a TG (twisted Gabidulin) code [19].
- If $\eta = 0$, an AGTG code is a GG (generalized Gabidulin) code [6].
- If $\eta = 0$ and $s = 1$, an AGTG code is a Gabidulin code.
- If $q = 2$, the AGTG, GTG and TG codes all reduce to GG codes since any nonzero element $\eta \in GF(2^n)$ has norm 1. Furthermore, when $s = 1$, they reduce to the original Gabidulin codes.

3 Interpolation decoding of AGTG codes

Throughout what follows we will consider the decoding of AGTG codes over finite fields in characteristic 2 and denote $[i] := q^{si}$, $i = 0, \ldots, n-1$ for simplicity.

3.1 The error interpolation polynomial

With an AGTG code, the encoding of a message $f = (f_0, \ldots, f_{k-1})$ is the evaluation of the linearized polynomial $f(x) = \sum_{i=0}^{k-1} f_i x^{[i]} + \eta f_0^{q_0^h} x^{[k]}$ at points $a_1, \ldots, a_n$ in $GF(q^n)$, which are linearly independent over $GF(q)$.

Let $\tilde{f} = (f_0, \ldots, f_{k-1}, \eta f_0^{q_0^h}, 0, \ldots, 0)$ be an n-dimensional vector over $GF(q^n)$ and $\mathcal{M} = \left[a_{i+1}^{[j]} \right]_{n \times n}$ be the Moore matrix generated by a_i's, where $0 \leqslant i, j < n$. Then the encoding of AGTG codes can be expressed as

$$(f_0, \ldots, f_{k-1}) \mapsto c = (f(a_1), \ldots, f(a_n)) = \tilde{f} \mathcal{M}^T, \quad (5)$$

where $\mathcal{M}^T$ is the transpose of $\mathcal{M}$. The interpolation-based decoding approach in this paper is described in the following.

For a received word $r = c + e$ with Rank$(e) = t \leqslant \lfloor \frac{n-k}{2} \rfloor$, suppose $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$ is a polynomial in $\mathcal{L}_n(GF(q^n))$ satisfying $g(a_i) = e_i = r_i + c_i$ for $i = 1, \ldots, n$. It is clear that the error vector e is uniquely determined by the polynomial $g(x)$, which is termed the *error interpolation polynomial* in this paper. Denoting $g = (g_0, \ldots, g_{n-1})$, we easily obtain $r = c + e = (\tilde{f} + g) \cdot \mathcal{M}^T$. This is equivalent to

$$r \cdot (\mathcal{M}^T)^{-1} = (f_0 + g_0, \ldots, f_{k-1} + g_{k-1}, f_0^{q_0^h} + g_k, g_{k+1}, \ldots, g_{n-1}). \tag{6}$$

By letting $\mathbf{r} = (\mathbf{r}_0, \ldots, \mathbf{r}_{n-1}) = r \cdot (\mathcal{M}^T)^{-1}$, we derive

$$(g_{k+1}, \ldots, g_{n-1}) = (\mathbf{r}_{k+1}, \ldots, \mathbf{r}_{n-1}) \text{ and } \eta g_0^{q_0^h} + g_k = \eta \mathbf{r}_0^{q_0^h} + \mathbf{r}_k \tag{7}$$

since $\eta f_0^{q_0^h} + g_k = \mathbf{r}_k$, and $f_0 + g_0 = \mathbf{r}_0$.

Therefore, the task of interpolation decoding is to reconstruct $g(x)$ from the available information characterized in (7). This reconstruction process will be discussed in Subsection 3.2 in detail.

3.2 Reconstructing the error interpolation polynomial

This subsection describes how the error interpolation polynomial $g(x)$ can be reconstructed from (7) by applying the property of the associated Dickson polynomial of $g(x)$ in Proposition 1.

From the definition in (2), the Dickson matrix associated with $g(x)$ is given by

$$G = \left[g_{i-j \pmod{n}}^{[j]} \right]_{n \times n} = \left[G_0 \; G_1 \; \ldots \; G_{n-1} \right] \tag{8}$$

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

From Proposition 1 it follows that G has rank t and any $t \times t$ matrix formed by t successive rows and columns in G is nonsingular. Hence the $(n - (k+t))$-th column $G_{n-(k+t)}$ can be expressed as $G_{n-(k+t)} = \lambda_0 G_{n-(k+t)+1} + \lambda_1 G_{n-(k+t)+2} + \cdots + \lambda_{t-1} G_{n-k}$, where $\lambda_0, \ldots, \lambda_{t-1}$ are elements in $GF(q^n)$ and they cannot be all equal to zero (since $G_t = 0$ implies $g(x) = 0$). This yields the following recursive equations:

$$g_{k+t+i}^{[n-(k+t)]} = \lambda_0 g_{k+t+i-1}^{[n-(k+t)+1]} + \lambda_1 g_{k+t+i-2}^{[n-(k+t)+2]} + \cdots + \lambda_{t-1} g_{k+i}^{[n-k]} \tag{9}$$

for $i = 0, 1, \ldots, n-1$. The above recurrence equation is the *key equation* for the decoding algorithm in this paper. It enables us to reconstruct $g(x)$ in two steps:

Step 1. derive the coefficients $\lambda_0, \ldots, \lambda_{t-1}$ from (7) and (9);
Step 2. use $\lambda_0, \ldots, \lambda_{t-1}$ to compute $g_{k-1}, \ldots, g_0$ recursively from (9).

The following discussion shows how the procedure of Step 1 works.

Recall from (7) that the elements $g_{k+1}, \ldots, g_{n-1}$ are known. This gives the following $(n-1) - k - t$ linear equations in variables $\lambda_0, \ldots, \lambda_{t-1}$:

$$g_{k+t+i}^{[n-(k+t)]} = \lambda_0 g_{k+t+i-1}^{[n-(k+t)+1]} + \lambda_1 g_{k+t+i-2}^{[n-(k+t)+2]} + \cdots + \lambda_{t-1} g_{k+i}^{[n-k]} \tag{10}$$

for $i = 1, \ldots, n-1-(k+t)$. As the rank t satisfies Rank$(e) = t \leqslant \lfloor \frac{n-k}{2} \rfloor$, i.e., $2t + k \leqslant n$, we divide the discussion into two cases.

Case 1: $2t+k < n$. In this case, the $n-k-t-1 \geqslant t$ equations in variables $\lambda_0, \ldots, \lambda_{t-1}$ given in (10) have rank t. Thus one can uniquely determine the elements $\lambda_0, \ldots, \lambda_{t-1}$. The modified Berlekamp-Massey algorithm [15] will be employed here for efficient implementation.

Case 2: $2t + k = n$. In this case (10) gives $n - k - t - 1 = t - 1$ linear equations in variables $\lambda_0, \ldots, \lambda_{t-1}$. For such an under-determined system of linear equations, we will have a set of solutions $(\lambda_0, \ldots, \lambda_{t-1})$ that has dimension 2 over $GF(q^n)$. Namely, the solutions $(\lambda_0, \ldots, \lambda_{t-1})$ will be of the form

$$\lambda + \omega\lambda' = (\lambda_0 + \omega\lambda'_0, \ldots, \lambda_{t-1} + \omega\lambda'_{t-1}),$$

where λ, λ' are fixed elements in $GF(q^n)^t$ and ω runs through $GF(q^n)$. Next we will show how the element ω is determined from the other available information in (7).

Observe that in (9), by taking $i = t$ and $i = 0$, one gets the following two equations

$$\begin{aligned} g_0^{[t]} &= \lambda_0 g_{n-1}^{[t+1]} + \lambda_1 g_{n-2}^{[t+2]} + \cdots + \lambda_{t-1} g_{n-t}^{[2t]}, \\ g_{k+t}^{[t]} &= \lambda_0 g_{k+t-1}^{[t+1]} + \lambda_1 g_{k+t-2}^{[t+2]} + \cdots + \lambda_{t-1} g_k^{[2t]}. \end{aligned}$$

These are equivalent to

$$\begin{aligned} g_0 &= \lambda_0^{[n-t]} g_{n-1}^{[1]} + \lambda_1^{[n-t]} g_{n-2}^{[2]} + \cdots + \lambda_{t-1}^{[n-t]} g_{n-t}^{[t]}, \\ g_{k+t} &= \lambda_0^{[n-t]} g_{k+t-1}^{[1]} + \lambda_1^{[n-t]} g_{k+t-2}^{[2]} + \cdots + \lambda_{t-1}^{[n-t]} g_k^{[t]}. \end{aligned}$$

Substituting $\lambda + \omega\lambda'$ into these two equations and re-arranging them gives

$$\begin{cases} g_0 + c_0 + c_1\omega^{q^{s(n-t)}} = 0 \\ (c_2 + c_3\omega^{q^{s(n-t)}})g_k + (c_4 + c_5\omega^{q^{s(n-t)}}) = 0, \end{cases} \tag{11}$$

where $c_0, \ldots, c_5$ are derived from λ, λ' and the known g_i's. Furthermore, using the fact $\eta g_0^{q_0^h} + g_k = \eta \mathbf{r}_0^{q_0^h} + \mathbf{r}_k = c_6$, one can reduce (11) as

$$(c_2 + c_3\omega^{q^{s(n-t)}})(c_6 + \eta(c_0 + c_1\omega^{q^{s(n-t)}})^{q_0^h}) + (c_4 + c_5\omega^{q^{s(n-t)}}) = 0.$$

This equation can be re-arranged as

$$u_0\omega^{q_0^{i_1} + q_0^{i_2}} + u_1\omega^{q_0^{i_1}} + u_2\omega^{q_0^{i_2}} + u_3 = 0, \tag{12}$$

where $i_1 = h + us(n-t)$, $i_2 = us(n-t)$, $u_0, \ldots, u_3$ are derived from $c_0, \ldots, c_5$ and η. Furthermore, letting $x = \omega^{q_0^{i_2}}$ and $v = i_1 - i_2$, we obtain

$$u_0 x^{q_0^v + 1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0. \tag{13}$$

Since any vector e with t errors, where $t = \frac{n-k}{2}$, can be uniquely decoded, the polynomial

$$P(x) = u_0 x^{q_0^v + 1} + u_1 x^{q_0^v} + u_2 x + u_3$$

should have exactly one zero. Furthermore, the unique solution $x = \omega^{q_0^{i_2}}$ lead to a unique solution $\lambda + \omega\lambda'$ in (10). With a unique solution $\lambda_0, \ldots, \lambda_{t-1}$ in Step 1, one can recursively compute $g_0, \ldots, g_{k-1}$ according to (9) in Step 2.

From the above discussion, it is clear that the remaining part of the decoding task is to solve the equation $P(x) = 0$ when it has exactly one solution. This will be addressed in the next subsection.

3.3 Solving the equation $P(x) = 0$ over finite fields of characteristic 2

This subsection will solve the equation

$$P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0 \tag{14}$$

when it has only one solution in $GF(q^n)$.

In the case of $u_0 = 0$, (14) is reduced to an affine equation $u_1 x^{q_0^v} + u_2 x + u_3 = 0$. When $u_1 = 0,\ u_2 \neq 0$ or $u_1 \neq 0, u_2 = 0$, this affine equation has a unique solution $x = u_3/u_2$ or $x = (u_3/u_1)^{q_0^{un-v}}$, respectively. Let $d = \gcd(v, un)$. When $u_1 u_2 \neq 0$, if u_2/u_1 is a $(q_0^d - 1)$-th power of an element in $GF(q^n)$, then $P(x) = 0$ has either q_0^d solutions or no solution in $GF(q^n)$; otherwise $P(x) = 0$ has a single solution $x = 0$ if $u_3 = 0$ and $x = \gamma$ if $u_3 \neq 0$.

In the case that $u_0 \neq 0$, the equation $P(x) = 0$ is equivalent to

$$Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3 = 0, \tag{15}$$

where $a_i = u_i/u_0$ for $i = 1, 2, 3$. The polynomial $Q(x)$ is closely related to the polynomial $F_a(x) = x^{2^l+1} + x + a$ discussed by Kolosha and Helleseth in [4] over a finite field of characteristic 2. The following theorem extends the result in [4] to a general form, which enables us to directly determine the single solution of the equation $Q(x) = 0$.

Theorem 1. *Let l and m be two positive integers with $l < m$ and $m_1 = m/\gcd(l, m)$. Define two sequencea of polynomials derived from the recurrences: $C_1(x) = C_2(x) = Z_1(x) = 1$ and*

$$C_{i+2}(x) = C_{i+1}(x) + x^{2^{il}} C_i(x), \quad Z_i(x) = C_{i+1}(x) + x C_{i-1}^{2^l}(x) \tag{16}$$

for $i = 1, 2, \cdots, m_1 - 1$. Then the polynomial $G(x) = x^{2^l+1} + a_1 x^{2^l} + a_2 x + a_3$ has exactly one zero in $GF(2^m)$ if and only if one of the following conditions holds: (i) $a_2 = a_1^{2^l}$ and $a_3 = a_1^{2^l+1}$; or (ii) $a_2 = a_1^{2^l}$, $a_3 \neq a_1^{2^l+1}$ and m_1 is odd; or (iii) $a_2 \neq a_1^{2^l}$, $Z_{m_1}(a) = 0$ and $C_{m_1}(a) \neq 0$ for $a = (a_1 a_2 + a_3)/(a_1 + a_2^{2^{m-l}})^{2^l+1}$. Moreover, for Cases (i) and (ii), the unique zero of $Q(x)$ is given by $x = a_1 + (a_1 a_2 + a_3)^{\frac{1}{2^l+1}}$, and for Case (iii), the unique zero is given by $x = (a C_{m_1}^{2^l-1}(a))^{2^{m-1}}$.

Proof. It is readily seen that if $a_2 = a_1^{2^l}$, the polynomial $G(x) = x^{2^l+1} + a_1 x^{2^l} + a_2 x + a_3$ can be rewritten as $G(x) = (x + a_1)^{2^l+1} + a_1^{2^l+1} + a_3$. Thus the statements in Cases i) and ii) follow from the fact $\gcd(2^l + 1, 2^m - 1) = 1$ if m_1 is odd. If $a_2 \neq a_1^{2^l}$, the polynomial $G(x)$ can be reduced to a polynomial of the form $F_a(x) = y^{2^l+1} + y + a$

by the following substitution: we take a nonzero element $s \in GF(2^m)$ such that $s = (a_1^{2^l} + a_2)^{2^{m-l}} = (a_1 + a_2^{2^{m-l}})$, and substitute $x = sy + a_1$ in $G(x)$. Then we obtain

$$\begin{aligned} Q(sy + a_1) =& (sy + a_1)^{2^l+1} + a_1(sy + a_1)^{2^l} + a_2(sy + a_1) + a_3 \\ =& (s^{2^l+1}y^{2^l+1} + a_1 s^{2^l} y^{2^l} + a_1^{2^l} sy + a_1^{2^l+1}) \\ &+ (a_1 s^{2^l} y^{2^l} + a_1^{2^l+1}) + a_2(sy + a_1) + a_3 \\ =& s^{2^l+1}y^{2^l+1} + s(a_1^{2^l} + a_2)y + a_1 a_2 + a_3 \\ =& s^{2^l+1}(y^{2^l+1} + y + a), \end{aligned}$$

where

$$a = \frac{a_1 a_2 + a_3}{s^{2^l+1}} = \frac{a_1 a_2 + a_3}{(a_1 + a_2^{2^{m-l}})^{(2^l+1)}}.$$

It is clear that in this case y is a zero of $F_a(y) = y^{2^l+1} + y + a$ if and only if $x = sy + a_1$ is a zero of $G(x)$. The claim in Case iii) thus follows from Proposition 4 in [4]. ■

By taking $q_0 = 2^w, l = vw,$ and $m = wun,$ the zero of the polynomial $G(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3$ can be immediately derived from Theorem 1.

Remark 1. Theorem 1 characterizes an explicit criteria for checking whether the equation $Q(x) = x^{q_0^v+1} + a_1 x^{q_0^v} + a_2 x + a_3 = 0$ has exactly one solution in $GF(q^n)$ or not. Moreover, the unique solution of $Q(x) = 0$ is given by a formula in terms of the coefficients a_1, a_2, a_3. Despite their complicatedness, the criteria and the formula in Theorem 1 can be directly computed in the order of $\mathcal{O}(l)$ multiplications, and negligible cyclic shifts and addition in $GF(q^n)$.

3.4 The decoding algorithm of AGTG codes over finite fields of characteristic 2

With the discussion in Subsections 3.1-3.3, we summarize the interpolation polynomial decoding algorithm of AGTG codes in Algorithm 1.

Remark 2. From the summary of known MRD codes in Subsection 2.2, we know that the AGTG codes includes the original Gabidulin codes, GG codes, TG codes and GTG codes as sub-families. Algorithm 1 can be used to decode up to $\lfloor \frac{n-k}{2} \rfloor$ errors for all AGTG codes. Hence it can be applied to the aforementioned MRD codes. In this paper we further investigate the zero of the polynomial $P(x)$ for the case of characteristic 2. This is our major contribution in Algorithm 1, and is the key difference between Algorithm 1 and the one sketched in [14].

Remark 3. It can be seen from each step in Algorithm 1 that errors in the AGTG codes can be efficiently decoded, especially when a low-complexity self-dual normal basis is used if it exists. To be more specific, Line 1 can be calculated by the q-transform with complexity $\mathcal{O}(n^3)$ over $GF(q)$ when a low-complexity self-dual normal basis is used; the modified Berlekamp-Massey algorithm in Line 4 has complexity $\mathcal{O}((n-k)^2)$ over $GF(q^n)$; Line 8 can be performed by the modified Berlekamp-Massey algorithm,

```
Algorithm 1: Interpolation decoding of AGTG codes
   Input: A received word $r$ with $t \leqslant \lfloor \frac{n-k}{2} \rfloor$ errors and linearly independent
          evaluation points $a_1, \ldots, a_n$
   Output: The correct codeword $c \in GF(q^n)^n$ or "Decoding Failure"
 1 Calculate $\mathbf{r} = (\mathbf{r}_0, \ldots, \mathbf{r}_{n-1}) = r \cdot (\mathcal{M}^T)^{-1}$ in (6);
 2 Set $(g_{k+1}, \ldots, g_{n-1}) = (\mathbf{r}_{k+1}, \ldots, \mathbf{r}_{n-1})$ and $\eta g_0^{q_0^h} + g_k = \eta \mathbf{r}_0^{q_0^h} + \mathbf{r}_k$;
 3 for $t \in \{1, \ldots, \lfloor \frac{n-k}{2} \rfloor\}$ do
 4     Applying the modified Berlekamp-Massey algorithm in determination of
         $(\lambda_0, \ldots, \lambda_{t-1})$ from (10);
 5 end
 6 if a unique $(\lambda_0, \ldots, \lambda_{t-1})$ is not found then
 7     Set $t = \lfloor \frac{n-k}{2} \rfloor$;
 8     Solve the under-determined system in (10) and set its solution as $\lambda + \omega\lambda'$;
 9     Calculate the polynomial $P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$ in (14);
10     if $u_0 = 0$ then
11         Calculate the zero to $P(x)$ if one of the conidtions after (14) are satisfied
12     else
13         Calculate the zero to $P(x)$ by Cases i)-iii) in Theorem 1
14     end
15     Set $(\lambda_0, \ldots, \lambda_{t-1}) = \lambda + \omega\lambda'$ with $\omega$ as the zero of $P(x)$;
16 end
17 Calculate $g_i$ for $i = 0, \ldots, k-1$ from the recursive equation (9);
18 if $g_0, \ldots, g_{n-1}$ is sucessfully determined then
19     Return the codeword $c = r + gM$
20 else
21     Return "Decoding Failure"
22 end
```

which has $\mathcal{O}((n-k)^2)$ over $GF(q^n)$; Lines 9, 11 can be done with constant operations in $GF(q^n)$; Step 13 can be done with linear complexity in $GF(q^n)$; the recursive calculation of $g_0, \ldots, g_{k-1}$ in Line 17 takes $\mathcal{O}(kt)$ operations in $GF(q^n)$; Line 19 can be calculated by the q-transform with complexity $\mathcal{O}(n^3)$ over $GF(q)$. To sum up, the overall complexity of Algorithm 1 is dominated by the modified Berlekamp-Massey algorithm, which has quadratic complexity in $GF(q^n)$.

4 Conclusion

This paper presents the first decoding algorithm for additive generalized twisted Gabidulin codes that covers almost all the known linear maximum rank distance codes. The main contribution of this paper, which is different from the work in [14] is the detailed investigation of zeros of the polynomial $P(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0$.

References

1. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A **25**(3), 226 – 241 (1978)
2. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: Davies, D.W. (ed.) Advances in Cryptology — EUROCRYPT '91. pp. 482–489. Springer Berlin Heidelberg, Berlin, Heidelberg (1991)
3. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
4. Helleseth, T., Kholosha, A.: $x^{2^l}+1+x+a$ and related affine polynomials over $GF(2^k)$. Cryptography and Communications **2**(1), 85–109 (2010)
5. Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. IEEE Transactions on Information Theory **54**(8), 3579–3591 (Aug 2008)
6. Kshevetskiy, A., Gabidulin, E.: The new construction of rank codes. In: Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on. pp. 2105–2108. IEEE (2005)
7. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: Ytrehus, Ø. (ed.) Coding and Cryptography. pp. 36–45. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
8. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. Journal of Combinatorial Theory, Series A **159**, 79–106 (2018)
9. Lusina, P., Gabidulin, E., Bossert, M.: Maximum rank distance codes as space-time codes. IEEE Transactions on Information Theory **49**(10), 2757–2760 (Oct 2003)
10. Otal, K., Özbudak, F.: Explicit constructions of some non-Gabidulin linear maximum rank distance codes. Adv. in Math. of Comm. **10**(3), 589–600 (2016)
11. Otal, K., Özbudak, F.: Additive rank metric codes. IEEE Transactions on Information Theory **63**(1), 164–168 (2017)
12. Otal, K., Özbudak, F.: Constructions of cyclic subspace codes and maximum rank distance codes. In: Network Coding and Subspace Designs, pp. 43–66. Springer (2018)
13. Puchinger, S., Rosenkilde, J., Sheekey, J.: Further generalisations of twisted Gabidulin codes. In: Proceedings of the 10th International Workshop on Coding and Cryptography (2017)
14. Randrianarisoa, T.H.: A decoding algorithm for rank metric codes. CoRR **abs/1712.07060** (2017)
15. Richter, G., Plass, S.: Fast decoding of rank-codes with rank errors and column erasures. In: International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings. pp. 398–398 (June 2004)
16. Rosenthal, J., Randrianarisoa, T.H.: A decoding algorithm for twisted Gabidulin codes. In: Information Theory (ISIT), 2017 IEEE International Symposium on. pp. 2771–2774. IEEE (2017)
17. Roth, R.M.: Maximum-rank array codes and their application to crisscross error correction. IEEE transactions on Information Theory **37**(2), 328–336 (1991)
18. Roth, R.M.: Tensor codes for the rank metric. IEEE Transactions on Information Theory **42**(6), 2146–2157 (1996)
19. Sheekey, J.: A new family of linear maximum rank distance codes. Advances in Mathematics of Communications **10**, 475 (2016)
20. Silva, D., Kschischang, F.R., Koetter, R.: A rank-metric approach to error control in random network coding. IEEE Transactions on Information Theory **54**(9), 3951–3967 (Sept 2008)
21. Silva, D., Kschischang, F.R.: Fast encoding and decoding of Gabidulin codes. In: Information Theory, 2009. ISIT 2009. IEEE International Symposium on. pp. 2858–2862. IEEE (2009)
22. Wachter-Zeh, A., Afanassiev, V., Sidorenko, V.: Fast decoding of Gabidulin codes. Designs, codes and cryptography **66**(1-3), 57–73 (2013)