


# On decoding additive generalized twisted Gabidulin codes

Wrya K. Kadir<sup>1</sup> · Chunlei Li<sup>1</sup> 

Received: 20 September 2019 / Accepted: 30 June 2020 / Published online: 23 July 2020  
© The Author(s) 2020

## Abstract

In this paper, we consider an interpolation-based decoding algorithm for a large family of maximum rank distance codes, known as the additive generalized twisted Gabidulin codes, over the finite field  $\mathbb{F}_{q^n}$  for any prime power  $q$ . This paper extends the work of the conference paper Li and Kadir (2019) presented at the International Workshop on Coding and Cryptography 2019, which decoded these codes over finite fields in characteristic two.

**Keywords** Rank metric · Maximum rank distance codes · Gabidulin codes · Twisted Gabidulin codes · Generalized twisted Gabidulin codes

**Mathematics Subject Classification (2010)** 94B35 · 68P30 · 11T71 · 11T06

## 1 Introduction

Error correction codes with the rank metric have found applications in space-time coding [27], random network coding [44] and cryptography [12]. Many important properties of rank metric codes including the Singleton like bound were independently studied by Del-sarte [9], Gabidulin [13] and Roth [38]. Codes that achieve this bound were called *maximum rank distance* (MRD) codes. The most famous sub-family of MRD codes are *Gabidulin codes* which is the rank metric analog of Reed-Solomon codes. They have been extensively studied in the literature [9, 12, 13, 25, 36, 38].

Finding new families of MRD codes has been an interesting research topic since the invention of Gabidulin codes. In [20, 39], the Frobenius automorphism in the Gabidulin codes were generalized to arbitrary automorphism and *generalized Gabidulin (GG)* codes

---

✉ Chunlei Li  
chunlei.li@uib.no

Wrya K. Kadir  
wrya.kadir@uib.no

<sup>1</sup> University of Bergen, Bergen, Norway

were proposed. In the past few years, a considerable amount of work has been done on MRD codes. In [40], Sheekey twisted the evaluation polynomial of a Gabidulin code and proposed a large family of MRD codes termed *twisted Gabidulin (TG)* codes. Using the same idea for generalizing Gabidulin codes, arbitrary automorphism was employed to construct *generalized twisted Gabidulin (GTG)* codes. This family of MRD codes were first described in [40, Remark 9] and later comprehensively studied in [26]. Otal and Özbudak [30] later introduced a large family of MRD codes, known as *additive generalized twisted Gabidulin (AGTG)* codes, which contains all the aforementioned linear MRD codes as sub-families and new additive MRD codes. There are also some new families of MRD codes which are not equivalent to AGTG codes nor its subfamilies [5, 8, 42, 47]. Recent constructions of linear and nonlinear MRD codes were lately summarized in [31, 41].

MRD codes with efficient decoding algorithm are of great interest in practice. In his pioneering work [13], Gabidulin gave a decoding algorithm based on extended Euclidean algorithm. Subsequently, Richter and Plass in [36], and Loidreau [25] proposed modified version of Berlekamp-Massey and Welch-Berlekamp algorithms to decode Gabidulin codes. Some of the aforementioned algorithms were further optimized in [45, 48]. Nevertheless, the known decoding algorithms for Gabidulin codes cannot be directly applied to those new MRD codes with twisted evaluation polynomials, especially when the MRD codes are only linear over the ground field  $\mathbb{F}_q$  or its subfield. By modifying the decoding algorithm in [19] for subspace codes, Randrianarisoa and Rosenthal in [37] proposed a decoding method for the twisted Gabidulin codes, which works only for a limited option of parameters. Randrianarisoa later proposed an interpolation approach to decoding twisted Gabidulin codes in [35], where he gave a brief discussion on the case when the rank of the error vector reaches the unique error-correcting radius of the twisted Gabidulin codes.

In this paper, we apply the interpolation approach by Randrianarisoa [35] in decoding additive generalized twisted Gabidulin (AGTG) codes, which contain (generalized) twisted Gabidulin codes and (generalized) Gabidulin codes as special cases. For AGTG codes with minimum rank distance  $d$ , if an error vector has rank strictly less than  $\frac{d-1}{2}$ , the decoding process can be directly converted to the decoding of generalized Gabidulin codes, for which existing decoding algorithms in [25, 36, 48] can be applied. On the other hand, when the error vector has rank exactly  $\frac{d-1}{2}$  (with  $d$  being odd), a new problem arises and one needs an efficient way to solve a quadratic polynomial. Solving a given quadratic polynomial over finite fields in general is a challenging problem. The quadratic polynomial derived from the decoding of AGTG codes has a close connection to a projective polynomials  $P(x)$ . Different from the short discussion in [35], we study the projective polynomial  $P(x)$  in greater depth. We start with the discussion on the number of roots of  $P(x)$  according to its coefficients and the characteristic of the finite field  $\mathbb{F}_{q^n}$ , propose methods to find roots of  $P(x)$  for each case, and finally adopt the result in the decoding algorithm for AGTG codes.

The remainder of this paper is structured as follows. Section 2 introduces some preliminaries, where we particularly recall some properties of linearized polynomial and recently constructed twisted MRD codes. Section 3 summarizes the interpolation decoding approach for additive generalized twisted Gabidulin codes and identifies the crucial quadratic polynomial when the rank of error reaches  $\frac{d-1}{2}$  (with  $d$  being odd). Section 4 is dedicated to the study of the quadratic polynomial and to finding roots of the corresponding projective polynomial  $P(x)$ . Section 5 integrates the interpolation decoding procedure and the result of Section 4 into an explicit algorithm and discusses the complexity of the proposed algorithm. Section 6 concludes the work of this paper.

## 2 Preliminaries

Let  $q$  be a power of a prime  $p$ . Throughout this paper we denote by  $\mathbb{F}_{q^r}$  the finite field with  $q^r$  elements for an arbitrary positive integer  $r$ .

### 2.1 Linearized polynomial

A polynomial of the form  $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$  is known as a  $q$ -polynomial [29]. Define a set

$$\mathcal{L}_k(\mathbb{F}_{q^n}) = \left\{ L(x) = \sum_{i=0}^{k-1} l_i x^{q^i} \mid L(x) \in \mathbb{F}_{q^n}[x]/(x^{q^n} - x) \right\}. \tag{1}$$

It is easy to verify that  $(\mathcal{L}_k(\mathbb{F}_{q^n}), +, \circ)$  forms a non-commutative  $\mathbb{F}_q$ -algebra, where  $+$  denotes the conventional polynomial addition and  $\circ$  denotes the symbolic product given by  $a(x) \circ b(x) = a(b(x))$ . Note that symbolic product is associative and distributive, but non-commutative in general. For a nonzero  $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$ , its  $q$ -degree is given by  $\deg_q(L(x)) = \max\{0 \leq i < k \mid l_i \neq 0\}$ .

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  $\mathbb{F}_{q^n}$ . Hence a linearized polynomial  $L(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$  indicates an  $\mathbb{F}_q$ -linear transformation  $L$  from  $\mathbb{F}_{q^n}$  to itself.

Known MRD codes in the literature are mostly given in the terms of linearized polynomials. Some relevant definitions and auxiliary results are recalled below.

**Definition 1** For a nonzero linearized polynomial  $L(x) = \sum_{i=0}^{k-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$ , its rank is given by

$$\text{Rank}(L) := \dim_{\mathbb{F}_q}(\text{Img}(L)) = n - \dim_{\mathbb{F}_q}(\text{Ker}(L)),$$

where  $\text{Img}(L) = \{L(x) \mid x \in \mathbb{F}_{q^n}\}$  and  $\text{Ker}(L) = \{x \in \mathbb{F}_{q^n} \mid L(x) = 0\}$ .

For a linearized polynomial  $L(x) = \sum_{i=0}^k l_i x^{q^i}$  with  $q$ -degree  $k$ , i.e.,  $l_k \neq 0$ , it is clear that  $\text{Ker}(L)$  has at most  $q^k$  elements. From the definition, the linearized polynomial  $L(x)$  has

$$\text{Rank}(L) = n - \dim_{\mathbb{F}_q}(\text{Ker}(L)) \geq n - k.$$

Sheekey in [40] characterizes a necessary condition for  $L(x)$  to have rank  $n - k$  as below.

**Lemma 1** [40] *Suppose a linearized polynomial  $L(x) = l_0x + l_1x^q + \dots + l_kx^{q^k}$ ,  $l_k \neq 0$ , in  $\mathcal{L}_n(\mathbb{F}_{q^n})$  has  $q^k$  roots in  $\mathbb{F}_{q^n}$ . Then*

$$\text{Norm}_{q^n/q}(l_k) = (-1)^{nk} \text{Norm}_{q^n/q}(l_0), \tag{2}$$

where  $\text{Norm}_{q^n/q}(x) = x^{1+q+\dots+q^{n-1}}$  is the norm function from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$ .

Furthermore, the necessary and sufficient condition for  $L(x)$  with  $q$ -degree  $k$  to have  $q^k$  roots in  $\mathbb{F}_{q^n}$  was independently characterized recently in [28, Theorem 7] and [7, Theorem 1.2], where all coefficients of  $L(x)$  are involved.

Below we recall two interesting matrices, of which properties and connection are critical for the decoding algorithm in this paper.

**Definition 2** [24, 49] Given a vector  $a = (a_0, \dots, a_{n-1})$  over  $\mathbb{F}_{q^n}$ , the Dickson matrix associated with  $a$  is given by

$$D_a = \left( a_{i-j(\bmod n)}^{q^j} \right)_{n \times n} = \begin{pmatrix} a_0 & a_{n-1}^q & \dots & a_1^{q^{n-1}} \\ a_1 & a_0^q & \dots & a_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^q & \dots & a_0^{q^{n-1}} \end{pmatrix}, \quad (3)$$

and the Moore matrix associated with  $a$  is given by

$$M_a = \left( a_i^{q^j} \right)_{n \times n} = \begin{pmatrix} a_0 & a_0^q & \dots & a_0^{q^{n-1}} \\ a_1 & a_1^q & \dots & a_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-1}^q & \dots & a_{n-1}^{q^{n-1}} \end{pmatrix}. \quad (4)$$

The Dickson matrix and Moore matrix have the following properties:

**Lemma 2** For two vectors  $a = (a_0, \dots, a_{n-1})$  and  $b = (b_0, \dots, b_{n-1})$  over  $\mathbb{F}_{q^n}$ ,

- i)  $D_a^T = D_{a'}$  with  $a' = (a_0, a_{n-1}^q, \dots, a_1^{q^{n-1}})$ ;
- ii)  $D_a \cdot D_b = D_u$ , where  $u = (u_0, \dots, u_{n-1})$  with  $u_i = \sum_{j=0}^{n-1} a_{i-j(\bmod n)}^{q^j} b_j$ ;
- iii)  $M_a^T \cdot M_b = D_v$ , where  $v = (v_0, \dots, v_{n-1})$  with  $v_i = \sum_{j=0}^{n-1} a_j^{q^i} b_j$ ;
- iv)  $M_a \cdot D_b = M_w$ , where  $w = (w_0, \dots, w_{n-1})$  with  $w_i = \sum_{j=0}^{n-1} a_i^{q^j} b_j$ .

The proof follows from direct calculations and is thus omitted here.

Let  $\mathcal{D}_n(\mathbb{F}_{q^n})$  be the set of all  $n \times n$  Dickson matrices over  $\mathbb{F}_{q^n}$ . It is shown in [49] that  $\mathcal{D}_n(\mathbb{F}_{q^n})$  forms an  $\mathbb{F}_q$ -algebra and there is an isomorphism  $\varphi$  between  $\mathcal{L}_n(\mathbb{F}_{q^n})$  and  $\mathcal{D}_n(\mathbb{F}_{q^n})$  given by

$$\varphi \left( \sum_{i=0}^{n-1} l_i x^{q^i} \right) = D_{(l_0, \dots, l_{n-1})} = \left( l_{i-j(\bmod n)}^{q^j} \right)_{n \times n}. \quad (5)$$

A Dickson matrix  $D$  will be said to be associated with a linearized polynomial  $L(x)$  if  $\varphi(L(x)) = D$ .

**Proposition 1** [49]. Let  $L$  be the linear transformation induced by a linearized polynomial  $L(x) \in \mathcal{L}_n(\mathbb{F}_{q^n})$  and  $D$  be the Dickson matrix associated with  $L(x)$ . Then

$$\text{Rank}(L) = \text{Rank}(D) \text{ and } \det(L) = \det(D).$$

It is well known [24] that given a linearized polynomial  $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$ , it is a permutation of  $\mathbb{F}_{q^n}$ , i.e.,  $\text{Rank}(L) = n$ , if and only if its associated Dickson matrix is non-singular; or equivalently its associated Moore matrix is non-singular. It follows from the fact that the determinant of a Moore matrix vanishes if and only if the entries of its first column are linearly dependent. In fact, more interesting connections between a linearized polynomial  $L(x)$  in  $\mathcal{L}_n(\mathbb{F}_{q^n})$  and its associated Dickson matrix can be established.

**Proposition 2** [35, Theorem 3] *Assume a linearized polynomial  $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$  has rank  $k$ . Then its associated Dickson matrix  $D$  in (5) has rank  $k$  over  $\mathbb{F}_{q^n}$ . Moreover, any  $k \times k$  submatrix formed by  $k$  consecutive rows and  $k$  consecutive columns in  $D$  is invertible.*

*Remark 1* Let  $\sigma = q^s$  with  $\gcd(s, n) = 1$ . The  $\sigma$ -polynomial

$$L_\sigma(x) = l_0x + l_1x^\sigma + \dots + l_{n-1}x^{\sigma^{n-1}}, \quad l_i \in \mathbb{F}_{q^n},$$

which reduces to a  $q$ -polynomial over  $\mathbb{F}_{q^n}$  for  $s = 1$ , is a generalization of  $q$ -polynomial. The aforementioned properties of  $q$ -polynomials can be similarly obtained as for  $\sigma$ -polynomials. For instance, the  $\sigma$ -polynomial  $L_\sigma(x) = \sum_{i=0}^k l_i x^{\sigma^i}$  with  $l_k \neq 0$  also has  $\text{Rank}(L) = n - \dim_{\mathbb{F}_q}(\text{Ker}(L)) \geq n - k$  [15]. When  $q$  is replaced by  $\sigma$  in the definition of the Dickson and Moore matrices, they are called the  $\sigma$ -version Dickson matrix and the  $\sigma$ -version Moore matrix, respectively. The  $\sigma$ -version Dickson and Moore matrices have the same properties as characterized in Lemma 2 and Proposition 2.

### 2.2 Maximum rank distance (MRD) codes

Let  $n$  and  $m$  be two positive integers. The *rank* of a vector  $a = (a_1, a_2, \dots, a_n)$  over  $\mathbb{F}_{q^m}$  is defined as the dimension of  $\text{span}_{\mathbb{F}_q} \langle a_1, a_2, \dots, a_n \rangle$  which is the vector space spanned by  $a_i$ 's over  $\mathbb{F}_q$ . The *rank distance* between two vectors  $a, b \in \mathbb{F}_{q^m}$  is defined as  $d_R(a, b) = \text{Rank}(a - b)$ .

**Definition 3** A *rank metric*  $(n, M, d)$ -code over  $\mathbb{F}_{q^m}$  is a subset of  $\mathbb{F}_{q^m}^n$  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*  $M \leq q^{\min\{m(n-d+1), n(m-d+1)\}}$ .

The Gabidulin codes are the most well-known MRD codes [13]. This family of MRD codes were further generalized in [20, 39], where the Frobenius automorphism of  $\mathbb{F}_{q^n}$  was replaced by a generic automorphism  $x \mapsto x^\sigma$  with  $\sigma = q^s$  and  $\gcd(s, n) = 1$ . The generalized Gabidulin (GG) code  $\mathcal{GG}_{n,k}$  over  $\mathbb{F}_{q^m}$  with length  $n$  and dimension  $k$  is defined by

$$\mathcal{GG}_{n,k} = \left\{ (f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{n-1})) \mid f(x) = \sum_{i=0}^{k-1} f_i x^{\sigma^i} \text{ and } f_i \in \mathbb{F}_{q^m} \right\}, \quad (6)$$

where  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  in  $\mathbb{F}_{q^m}$  are linearly independent over  $\mathbb{F}_q$ . When  $\sigma = q$ , i.e.,  $s = 1$ , the code  $\mathcal{GG}_{n,k}$  reduces to the original Gabidulin code [13]. The choice of independent points  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  does not affect the rank property. Hence it is customary to express generalized Gabidulin codes without the evaluation points as  $\mathcal{GG}_{n,k} = \left\{ f(x) = \sum_{i=0}^{k-1} f_i x^{\sigma^i} \mid f_i \in \mathbb{F}_{q^m} \right\}$ . We will also omit the evaluation points  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  in the following introduction of recent twisted MRD codes [26, 30, 40]. For consistency with the parameters of MRD codes in [26, 30, 40], throughout what follows we always assume  $n = m$ .

Recent constructions of MRD codes largely depend on the number of roots of certain linearized polynomials. From Lemma 1 it is readily seen that a linearized polynomial  $L(x)$  of  $q$ -degree  $k$  has rank at least  $n - k + 1$  if the condition (2) is not met. In [40] Sheekey

adopted Lemma 1 to construct *twisted Gabidulin (TG) codes* and described the *generalized twisted Gabidulin (GTG) codes*, which was intensively studied by Lunardon et al. [26].

**Proposition 3** [26, 40] *Let  $n, k, s$  be positive integers such that  $k < n$  and  $\gcd(s, n) = 1$ . Let  $\eta$  be a nonzero element in  $\mathbb{F}_{q^n}$  satisfying  $\text{Norm}_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$ . Then the set*

$$\mathcal{H}_{k,s}(\eta, h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \eta f_0^{q^h} x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^n} \right\} \tag{7}$$

is an MRD code with minimum rank distance  $d = n - k + 1$ .

The idea of manipulating some terms of linearized polynomials to construct new MRD codes was further extended in [30, 31, 33]. Below we recall from [30] the additive generalized twisted Gabidulin (AGTG) codes, for which we will propose an interpolation-based decoding algorithm in the next section.

**Proposition 4** [30] *Let  $n, k, s, h \in \mathbb{Z}^+$  satisfying  $\gcd(s, n) = 1$  and  $k < n$ . Let  $q = q_0^u$  and  $\eta \in \mathbb{F}_{q^n}$  such that  $\text{Norm}_{q^{sn}/q_0^s}(\eta) \neq (-1)^{nku}$ . Then the set*

$$\mathcal{H}_{k,s,q_0}(\eta, h) = \left\{ \sum_{i=0}^{k-1} f_i x^{q^{si}} + \eta f_0^{q_0^h} x^{q^{sk}} \mid f_i \in \mathbb{F}_{q^n} \right\} \tag{8}$$

is an  $\mathbb{F}_{q_0}$ -linear (but not necessarily  $\mathbb{F}_q$ -linear) MRD code of size  $q^{nk}$  and minimum rank distance  $n - k + 1$ .

The above AGTG codes reduce to GTG codes when  $q_0 = q$  and to GG codes when  $\eta = 0$  or  $q_0 = 2$ . Very recently, Sheekey in [42] showed the existence of a new family of MRD codes which is not equivalent to AGTG codes and Trombetti-Zhou codes in [47]. Recent MRD codes that are constructed based on Lemma 1 were formulated in a united manner in [41] and [22].

### 3 Encoding and decoding for AGTG codes

Throughout this section we will denote  $[i] := \sigma^i = q^{si}$  for  $i = 0, \dots, n - 1$ , where  $(s, n) = 1$ , for simplicity.

Below we briefly describe the encoding process of the AGTG codes, which provides the notational conventions and a reference for the interpolation decoding process.

#### 3.1 Encoding AGTG codes

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

$$f(x) = \sum_{i=0}^{k-1} f_i x^{[i]} + \eta f_0^{q_0^h} x^{[k]}.$$



Let  $\tilde{f} = (f_0, \dots, f_{k-1}, \eta f_0^{q_0^h}, 0, \dots, 0)$  be a vector of length  $n$  over  $\mathbb{F}_{q^n}$  and  $M$  be the  $\sigma$ -version Moore matrix generated by  $\alpha_i$ 's, where  $1 \leq i, j \leq n - 1$ , i.e.,

$$M = (\alpha_i^{[j]})_{n \times n} = \begin{pmatrix} \alpha_0 & \alpha_0^{[1]} & \dots & \alpha_0^{[n-1]} \\ \alpha_1 & \alpha_1^{[1]} & \dots & \alpha_1^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & \alpha_1^{[1]} & \dots & \alpha_{n-1}^{[n-1]} \end{pmatrix}. \tag{9}$$

Then the encoding of AGTG codes can be expressed as

$$(f_0, \dots, f_{k-1}) \mapsto c = (f(\alpha_0), \dots, f(\alpha_{n-1})) = \tilde{f}M^T. \tag{10}$$

Here it is worth noting that in encoding process, one actually only needs to calculate the multiplication of the  $(k + 1)$ -tuple  $(f_0, \dots, f_{k-1}, \eta f_0^{q_0^h})$  and the first  $k + 1$  row of  $M$ . Here we express it as in (10) for being consistent with the decoding procedure.

### 3.2 Decoding AGTG codes with an error-interpolation polynomial $g(x)$

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

When the rank  $t$  of the error is strictly smaller than  $\frac{n-k}{2}$ , the decoding of AGTG codes  $\mathcal{H}_{k,s,q_0}(\eta, h)$  can be converted to the decoding of GG codes  $\mathcal{G}_{n,k+1}$ . More concretely, one can use the existing decoding algorithms, e.g., [25, 36, 48], for (generalized) Gabidulin codes to establish a system of  $n - (k + 1) - t$  independent affine equations and  $t$  unknowns, which is uniquely solvable since  $2t \leq n - (k + 1)$ . However, when the rank  $t$  achieves the unique error-correcting radius, i.e.,  $(n - k)$  is even and  $t = \frac{n-k}{2}$ , one needs more equation(s) on the unknowns and new techniques are required. In the interpolation decoding for the TG codes by Randrianarisoa [35], the problem was converted to certain quadratic equations. However, how to efficiently solve the corresponding quadratic equations was little considered in [35].

Below we shall extend Randrianarisoa's idea to the larger family of AGTG codes and investigate the quadratic equations in greater depth. For self-completeness, we briefly describe the process of interpolation decoding and how it is transformed to solving certain quadratic equation for the case that  $2t = n - k$ .

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

$$g(\alpha_i) = e_i = r_i - c_i, \quad i = 0, \dots, n - 1. \tag{11}$$

It is clear that the error vector  $e$  is uniquely determined by the polynomial  $g(x)$ . Denote a vector  $g = (g_0, \dots, g_{n-1})$ . From (10) and (11) it follows that

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

This is equivalent to

$$r \cdot (M^T)^{-1} = (f_0 + g_0, \dots, f_{k-1} + g_{k-1}, \eta f_0^{q_0^h} + g_k, g_{k+1}, \dots, g_{n-1}). \tag{12}$$

Letting  $\gamma = (\gamma_0, \dots, \gamma_{n-1}) = r \cdot (M^T)^{-1}$ , we obtain

$$(g_{k+1}, \dots, g_{n-1}) = (\gamma_{k+1}, \dots, \gamma_{n-1}) \text{ and } -\eta g_0^{q_0^h} + g_k = \gamma_k - \eta \gamma_0^{q_0^h} \tag{13}$$

since  $\eta f_0^{q_0^h} + g_k = \gamma_k$ , and  $f_0 + g_0 = \gamma_0$ .

Therefore, the task of correcting error  $e$  is equivalent to reconstructing  $g(x)$  from the available information characterized in (13). This reconstruction process heavily depends on the property of the associated  $\sigma$ -version Dickson matrix of  $g(x)$  and will be discussed in Section 3.3.

### 3.3 Reconstructing the interpolation polynomial $g(x)$

Similarly to the definition in (3), the  $\sigma$ -version Dickson matrix associated with  $g(x)$  can be given by

$$G = \left( g_{i-j \pmod n}^{[j]} \right)_{n \times n} = (G_0 \ G_1 \ \dots \ G_{n-1}) \quad (14)$$

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

According to Proposition 2, the matrix  $G$  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  $G_1, \dots, G_t$ , namely,  $G_0 = \lambda_1 G_1 + \lambda_2 G_2 + \dots + \lambda_t G_t$ , where  $\lambda_1, \dots, \lambda_t$  are elements in  $\mathbb{F}_{q^n}$ . This yields the following recursive equations

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \dots + \lambda_t g_{i-t}^{[t]}, \quad 0 \leq i < n, \quad (15)$$

where the subscripts in  $g_i$ 's are taken modulo  $n$ . Recall that the elements  $g_{k+1}, \dots, g_{n-1}$  are known from (13). Hence we obtain the following linear equations with known coefficients and variables  $\lambda_1, \dots, \lambda_t$ :

$$g_i = \lambda_1 g_{i-1}^{[1]} + \lambda_2 g_{i-2}^{[2]} + \dots + \lambda_t g_{i-t}^{[t]}, \quad k+t+1 \leq i < n. \quad (16)$$

The above recurrence gives a generalized version of  $q$ -linearized shift register as described in [43], where  $(\lambda_1, \dots, \lambda_t)$  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 the coefficients  $\lambda_1, \dots, \lambda_t$  from (13) and (16);

**Step 2.** use  $\lambda_1, \dots, \lambda_t$  to compute  $g_{k-1}, \dots, g_0$  recursively from (15).

Note that Step 1 is the critical and challenging step in the decoding process, and Step 2 is simply a recursive that can be done fast. The following discussion shows how the procedure of Step 1 works.

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

*Case 1:*  $2t+k < n$ . In this case, (16) contains  $n-k-t-1 \geq t$  affine equations in variables  $\lambda_1, \dots, \lambda_t$ , which has rank  $t$ . Hence the variables  $\lambda_1, \dots, \lambda_t$  can be uniquely determined. Here we assume the code has high code rate, for which the Berlekamp-Massey (BM) algorithm is more efficient [14]. Another reason for choosing the BM algorithm is that it outputs the intermediate polynomial  $B^{(n-k-1)}(x)$  which will be used in Case 2. Although the recurrence (16) is a generalized version of the ones in [36, 43], the modified BM algorithm [36, 43] can be applied here to recover the coefficients  $\lambda_1, \dots, \lambda_t$ . For self-completeness we recall the modified BM algorithm in Algorithm 1. The coefficients of  $\Lambda^{(n-k-1)}(x)$  are the desired  $\lambda_i$ 's.



Case 2:  $2t + k = n$ . In this case (16) gives  $n - k - t - 1 = t - 1$  independent affine equations in variables  $\lambda_1, \dots, \lambda_t$ . For such an under-determined system of linear equations, we will have a set of solutions  $(\lambda_1, \dots, \lambda_t)$  that has dimension 1 over  $\mathbb{F}_{q^n}$ . Namely, the solutions will be of the form

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

where  $\lambda, \lambda'$  are fixed elements in  $\mathbb{F}_{q^n}^t$  and  $\omega$  runs through  $\mathbb{F}_{q^n}$ . As shown in [43, Th. 10], the solution can be derived from the modified BM algorithm with a free variable  $\omega$ . Next we will show how the element  $\omega$  is determined by other information in (13).

---

**Algorithm 1** A modified BM algorithm solving (16).

---

**Input:** elements  $g_{k+1}, \dots, g_{n-1}$   
**Output:** A shortest FSR with coefficients  $\lambda_1, \dots, \lambda_t$  satisfying (16)

- 1 Set  $L = 0, \Lambda^{(0)}(x) = x, B^{(0)}(x) = x, \Delta'_0 = 1$ ;
- 2 **for** each  $r$  from 0 to  $n - k - 2$  **do**
- 3 Calculate  $\Delta_r = -g_{k+1+r} + \sum_{i=1}^L \Lambda_i^{(r)} g_{k+1+r-i}^{q^{si}}$ ;
- 4 **if**  $\Delta_r = 0$  **then**
- 5  $\Lambda^{(r+1)}(x) = \Lambda^{(r)}(x)$ ;
- 6  $B^{(r+1)}(x) = x^{q^s} \circ B^{(r)}(x)$ ;
- 7 **else**
- 8  $\Lambda^{(r+1)}(x) = \Lambda^{(r)}(x) - \Delta_r x^{q^s} \circ B^{(r)}(x)$ ;
- 9 **if**  $2L > r$  **then**
- 10  $B^{(r+1)}(x) = x^{q^s} \circ B^{(r)}(x)$ ;
- 11 **else**
- 12  $B^{(r+1)}(x) = \Delta_r^{-1} \Lambda^{(r)}(x)$ ;
- 13  $L = r + 1 - L$ ;
- 14 **end**
- 15 **end**
- 16  $r = r + 1$ ;
- 17 **end**
- 18 Set  $t = L$ ;
- 19 Return  $t$ , the connection vector  $\lambda_1, \dots, \lambda_t$  in  $\Lambda^{(n-k-1)}(x)$  and  $B^{(n-k-1)}(x)$

---

Observe that in (15), by taking  $i = 0$  and  $i = k + t$  and substituting the solution  $\lambda + \omega\lambda'$ , one gets the following two equations

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

Re-arranging the equations gives

$$\begin{aligned} g_0 &= c_0 + c_1\omega \\ g_{k+t} &= c_2 + c_3\omega + (\lambda_t + \lambda'_t\omega)g_k^{[t]}, \end{aligned} \tag{17}$$

where  $c_0, c_1, c_2, c_3$  are derived from  $\lambda, \lambda'$  and the known  $g_i$ 's. Furthermore, from (13) we have  $-\eta g_0^{q_0^h} + g_k = \gamma_k - \eta \gamma_0^{q_0^h}$ . Denoting  $c_4 = \gamma_k - \eta \gamma_0^{q_0^h}$  and substituting  $g_k = c_4 + \eta g_0^{q_0^h}$  into (17) gives

$$(\lambda_t + \lambda'_t \omega)(c_4 + \eta(c_0 + c_1 \omega)^{q_0^h})^{[t]} - g_{k+t} + (c_2 + c_3 \omega) = 0.$$

This equation can be re-arranged as

$$u_0 \omega^{q_0^v+1} + u_1 \omega^{q_0^v} + u_2 \omega + u_3 = 0. \tag{18}$$

where  $q = q_0^u, v = h + ust, u_0, \dots, u_3$  are derived from  $c_0, \dots, c_5$  and  $\eta$ .

Since the error  $e$  with rank  $t = \frac{n-k}{2} = \frac{d-1}{2}$  can be uniquely decoded, the polynomial

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

should have roots  $w$  in  $\mathbb{F}_{q^n}$  that lead to solutions  $\lambda + \omega \lambda'$  in (16) and  $(g_0, g_k)$  in (17).

With the coefficients  $\lambda_1, \dots, \lambda_t$  in Step 1 and the initial state  $g_{n-1}, \dots, g_{n-t}$ , one can recursively compute  $g_0, \dots, g_{k-1}$  according to (15) in Step 2. Note that not all solutions of  $\mathcal{P}(x)$  lead to correct coefficients of the error interpolation polynomial. In fact, by the expression of Dickson matrix of  $g(x)$ , correct  $g(x)$  should have the sequence  $(g_{n-1}, \dots, g_{n-t}, \dots)$  generated from (15) has period  $n$ . In other words, if the output sequence has period  $n$ , we know that the corresponding polynomial  $g(x) = \sum_{i=0}^{n-1} g_i x^{[i]}$  is the desired error interpolation polynomial. From the above discussion, the remaining task of decoding is to efficiently find roots of  $\mathcal{P}(x)$  in  $\mathbb{F}_{q^n}$ , which will be discussed in the next section.

### 4 Finding roots of the polynomial $\mathcal{P}(x)$

This subsection is dedicated to finding solutions to the following equation in  $\mathbb{F}_{q^n} = \mathbb{F}_{q^{nu}}$ :

$$\mathcal{P}(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3 = 0. \tag{19}$$

When  $q = q_0^u = q_0$ , the polynomial  $\mathcal{P}$  can be reduced to  $P(x)$  in [35, Page 10]. In [35], the author converted solving  $P(x) = 0$  to the factorization of the linearized polynomial  $x^{q^{2l}} + ax^{q^l} + bx$ . Nevertheless, factoring  $x^{q^{2l}} + ax^{q^l} + bx$  is not necessarily easy and there's no efficient algorithm, as far as we know, for factoring this linearized polynomial. Therefore, it's important to further investigate how to efficiently solve  $\mathcal{P}(x)$ .

Assume  $d = (v, un)$ . We start with the simplest case that  $u_0 = 0$ . In this case, (19) is reduced to an affine equation  $u_1 x^{q_0^v} + u_2 x + u_3 = 0$ . Furthermore,

- i) if  $(u_1, u_2) = (0, 0)$ , then  $\mathcal{P}(x)$  has no zero if  $u_3 \neq 0$  and every element in  $\mathbb{F}_{q^n}$  as a zero otherwise;
- ii) if  $u_1 = 0, u_2 \neq 0$ , then  $\mathcal{P}(x)$  has a unique zero  $x = -u_3/u_2$ ;
- iii) if  $u_1 \neq 0, u_2 = 0$ , then  $\mathcal{P}(x)$  has a unique zero  $x = (-u_3/u_1)^{q_0^{nu-v}}$ .
- iv) if  $u_1 u_2 \neq 0, u_3 = 0$ , then  $\mathcal{P}(x) = 0$  has  $q_0^d$  zeros in  $\mathbb{F}_{q^n}$ , if  $-u_2/u_1$  is a  $(q_0^d - 1)$  power of an element in  $\mathbb{F}_{q^n}$ ; otherwise,  $\mathcal{P}(x) = 0$  has a single zero  $x = 0$ .

When  $u_0 \neq 0$ , we transform the equation  $\mathcal{P}(x) = 0$  into

$$P(x) = \frac{1}{u_0} \mathcal{P}(x - u_1 u_0^{-1}) = x^{q_0^v+1} + ax + b = 0, \tag{20}$$

where

$$a = \frac{u_2}{u_0} + \left(-\frac{u_1}{u_0}\right)^{q_0^v} \text{ and } b = \frac{u_3}{u_0} - \frac{u_1 u_2}{u_0^2} + \frac{u_1}{u_0} \left(-\frac{u_1}{u_0}\right)^{q_0^v} + \left(-\frac{u_1}{u_0}\right)^{q_0^v+1}.$$

The polynomial  $P(x)$  can be seen as a reduced version of the original polynomial  $\mathcal{P}(x)$ . It is clear that if  $a = 0$ , then  $P(x) = 0$  has either no solution or

$$m = \gcd(q_0^v + 1, q_0^{nu} - 1) = \begin{cases} q_0^d + 1, & \text{if } \frac{nu}{\gcd(un,v)} \text{ is even,} \\ 2, & \text{if } \frac{nu}{\gcd(un,v)} \text{ and } q_0 \text{ are odd,} \\ 1, & \text{if } \frac{nu}{\gcd(un,v)} \text{ is odd, and } q_0 \text{ is even} \end{cases}$$

solutions, depending on whether  $-b$  is an  $m$ -th power; and that if  $b = 0$ ,  $P(x) = 0$  has either zero as its unique solution or  $q_0^d$  solutions.

When  $ab \neq 0$ , the polynomial  $P(x) = x^{q_0^v+1} + ax + b$  over  $\mathbb{F}_{q_0^{un}}$  has a variety of applications in the construction of different sets with Singer parameters [10], construction error correcting codes [3], APN functions [4] and computing cross-correlation between  $m$ -sequences [11, 16].

The polynomial  $P(x)$  is a type of projective polynomials [1], which in general has the form

$$a_0 + a_1 x + a_2 x^{(2)} + \dots + a_l x^{(l)} \in \mathbb{F}_{q^n}[x],$$

where  $x^{(i)} = x^{\frac{q^i-1}{q-1}}$ . Bluhner in [2] showed that the projective polynomial

$$P(x) = x^{q^r+1} + ax + b, \quad a, b \in \mathbb{F}_{q^n}^*, \tag{21}$$

where  $q$  is any prime power and  $r, n$  are arbitrary two positive integers, has exactly  $0, 1, 2, q^{r_0} + 1$  possible number of zeros in  $\mathbb{F}_{q^n}$  with  $r_0 = \gcd(r, n)$ . Before the discussion on finding roots of  $P(x)$ , it is important to know the possible number of roots and the corresponding conditions on the coefficients of  $P(x)$ . In the following we will discuss different ways to find and express the zeros of  $P(x)$ .

First, we present a relations among roots of  $P(x)$ , which is inspired by [11, Lemma 22] and generalized for any prime power  $q$ .

**Proposition 5** *For positive integers  $r, n$  and a prime power  $q$ , the projective polynomial*

$$P(x) = x^{q^r+1} + ax + b, \quad a, b \in \mathbb{F}_{q^n}^*$$

*has 0, 1, 2 or  $q^{r_0} + 1$  roots  $x \in \mathbb{F}_{q^n}$ , where  $r_0 = \gcd(r, n)$ . Moreover, if  $P$  has three different roots  $x_0, x_1$  and  $x_2 \in \mathbb{F}_{q^n}$ , then all the roots can be characterized as*

$$x_{A_0, A_1, A_2} = -x_0 x_1 x_2 \frac{\frac{A_0}{x_0} + \frac{A_1}{x_1} + \frac{A_2}{x_2}}{A_0 x_0 + A_1 x_1 + A_2 x_2} \tag{22}$$

where  $(A_0, A_1, A_2) \neq (0, 0, 0)$  and  $A_0 + A_1 + A_2 = 0$ .

*Proof* Suppose  $P(x_0) = 0$  for an element  $x_0$  in  $\mathbb{F}_{q^n}$ . For a nonzero  $\lambda \in \mathbb{F}_{q^n}^*$ , one has

$$\begin{aligned} P(\lambda + x_0) &= (\lambda + x_0)^{q^r+1} + a(\lambda + x_0) + b \\ &= (\lambda^{q^r+1} + x_0\lambda^{q^r} + \lambda x_0^{q^r} + x_0^{q^r+1}) + \lambda a + ax_0 + b \\ &= (\lambda^{q^r+1} + x_0\lambda^{q^r} + (x_0^{q^r} + a)\lambda) + P(x_0) \\ &= \lambda^{q^r+1}(1 + x_0/\lambda + (x_0^{q^r} + a)/\lambda^{q^r}). \end{aligned}$$

Thus  $P(\lambda + x_0) = 0$  if and only if  $\frac{1}{\lambda}$  is a solution of the affine equation  $L'_0(z) = L_0(z) + 1 = 0$ , where

$$L_0(z) = (x_0^{q^r} + a)z^{q^r} + x_0z.$$

Depending on  $x_0$ ,  $L_0(z)$  may have a single solution if  $x_0^{q^r} + a = 0$  or  $q^{r_0}$  solutions if  $x_0(x_0^{q^r} + a)^{-1}$  is a  $(q^{r_0} - 1)$ -th power in  $\mathbb{F}_{q^n}$ . Hence the affine equation  $L'_0(z) = 0$  has either 0, 1 or  $q^{r_0}$  nonzero solutions in  $\mathbb{F}_{q^n}$ . For each nonzero solution  $z$  of  $L'_0(z) = 0$ , we get a root  $x_0 + \frac{1}{z}$  of the projective polynomial  $P(x)$ .

On the other hand, when  $P(x)$  has three distinct roots  $x_0, x_1$  and  $x_2$ , we obtain two different roots  $\frac{1}{x_1-x_0}$  and  $\frac{1}{x_2-x_0}$  of the affine equation  $L'_0(z) = 0$  and their difference  $\frac{1}{x_1-x_0} - \frac{1}{x_2-x_0}$  is a root of the linearized polynomial  $L_0(z) = 0$ , i.e.,

$$\begin{aligned} L'_0\left(\frac{1}{x_1-x_0}\right) &= L_0\left(\frac{1}{x_1-x_0}\right) + 1 = 0, \\ L'_0\left(\frac{1}{x_2-x_0}\right) &= L_0\left(\frac{1}{x_2-x_0}\right) + 1 = 0, \\ L'_0\left(\frac{1}{x_1-x_0}\right) - L'_0\left(\frac{1}{x_2-x_0}\right) &= L_0\left(\frac{1}{x_1-x_0} - \frac{1}{x_2-x_0}\right) = 0. \end{aligned}$$

So  $y = \frac{1}{x_1-x_0} - \frac{1}{x_2-x_0}$  is a root of  $L_0(z)$ . Hence,  $z = \frac{1}{x_1-x_0} + Ay$  runs through all roots of  $L'_0(z)$ . Consequently, assuming  $(A_0, A_1, A_2) = (1, A, -(A + 1))$ ,

$$\begin{aligned} x^{(A)} &= x_0 + \frac{1}{z} = x_0 + \frac{1}{\frac{1}{x_1-x_0} + Ay} \\ &= x_0 + \frac{1}{\frac{1}{x_1-x_0} + \frac{A}{x_1-x_0} - \frac{A}{x_2-x_0}} \\ &= x_0 + \frac{(x_1-x_0)(x_2-x_0)}{(x_2-x_0) + A(x_2-x_0) - A(x_1-x_0)} \\ &= -x_0x_1x_2 \cdot \frac{\frac{1}{x_0} + \frac{A}{x_1} - \frac{(A+1)}{x_2}}{x_0 + Ax_1 - (A+1)x_2} \\ &= -x_0x_1x_2 \cdot \frac{\frac{A_0}{x_0} + \frac{A_1}{x_1} + \frac{A_2}{x_2}}{A_0x_0 + A_1x_1 + A_2x_2} = x_{(A_0, A_1, A_2)} \end{aligned}$$

runs through all roots of  $P(x)$  different from  $x_0$ , while  $A$  runs through  $\mathbb{F}_{q^{r_0}}$ . □

The above result gives a method to express all the roots of the projective polynomials  $P(x) = x^{q^r+1} + ax + b, a, b \in \mathbb{F}_{q^n}^*$  in terms of the three known roots in  $\mathbb{F}_{q^n}$ . Moreover, from its proof, a method to describe the roots of the projective polynomial  $P(x)$  in terms of the roots of the affine polynomial  $L'_0(z)$ . Nevertheless, the condition that characterizes the exact number of solutions to the affine equation  $L'_0(z) = (x_0^{q^r} + a)z^{q^r} + x_0z + 1$  is not clear.

In order to investigate the number of roots of  $P(x) = x^{q^r+1} + ax + b$  in  $\mathbb{F}_{q^n}$  according to its coefficients, we need to divide the discussion into two cases:  $q$  is even; or  $q$  is odd and  $\gcd(r, n) = 1$ .

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

When the finite field  $\mathbb{F}_{q^n}$  has characteristic 2, the polynomial  $P(x)$  can be further converted to  $F_c(x) = x^{q^r+1} + x + c = 0$ , which was intensively studied in [17, 18, 21]. Helleseth and Kholosha in [17, 18] explicitly gave the root of  $F_c(x) = 0$  in terms of the coefficient  $c$  when it has a single zero in  $\mathbb{F}_{q^n}$  and when it has two zeros in  $\mathbb{F}_{q^n}$  if  $\gcd(r, n)$  is odd. Very recently, Kim and Mesnager in [21] further studied the equation for the case  $q = 2$  and  $\gcd(r, n) = 1$  and explicitly calculated all possible zeros of  $F_c(x)$  in  $\mathbb{F}_{q^n}$ . Since for general AGTG codes, the parameter  $q_0$  is always greater than 2. Below we shall recall the result by Helleseth and Kholosha [18] and apply it to find the roots of the projective polynomial  $P(x)$  in some cases.

Note that the AGTG codes are defined over  $\mathbb{F}_{q^n}$  with  $q$  a prime power. In this context, we assume  $q$  is a power of 2. To avoid potential confusion of notations, below we recall the result from [18] and treat the underlying finite field as  $\mathbb{F}_{2^m}$ , where  $m$  is a positive integer. Let  $l$  be a positive integer with  $d = \gcd(l, m)$  and denote  $m_1 = l/d$ . Define two sequences of polynomials in recurrence as follows:  $C_1(x) = C_2(x) = Z_1(x) = 1$ , and

$$C_{i+2}(x) = C_{i+1}(x) + x^{2^i} C_i(x), \quad Z_i(x) = C_{i+1}(x) + x C_{i-1}^{2^l}(x) \tag{23}$$

for  $i = 1, 2, \dots, m_1 - 1$ .

**Proposition 6** [18, Prop. 3-5] *Given a polynomial*

$$F_c(x) = x^{2^l+1} + x + c, \quad c \in \mathbb{F}_{2^m}^*, \tag{24}$$

- i) *it has exactly one zero in  $\mathbb{F}_{2^m}$  if and only if  $Z_{m_1}(c) = 0$  and  $C_{m_1}(c) \neq 0$ ; and this zero is given by  $x = (cC_{m_1}^{2^l-1}(c))^{2^{m-1}}$ ;*
- ii) *it has exactly two zeros in  $\mathbb{F}_{2^m}$  if and only if  $Z_{m_1}(c) \neq 0$  and  $\text{Tr}_1^d(N_d^m(c)/Z_{m_1}^2(c)) = 0$ , where the trace function  $\text{Tr}_1^d(z) = \sum_{i=0}^{d-1} z^{2^i}$  and  $N_d^m(z)$  is the norm function defined by  $N_d^m(z) = \prod_{i=0}^{m_1-1} z^{2^{di}}$ . Moreover, if  $d$  is odd, then these two zeros are  $(W + \mu)Z_{m_1}(c)/C_{m_1}(c)$  for  $\mu \in \{0, 1\}$ , where*

$$W = \frac{C_{m+1}(c)}{Z_{m+1}(c)} + \sum_{i=0}^{\frac{d-1}{2}} \left( \frac{N_d^m(c)}{Z_{m_1}^2(c)} \right)^{2^{2i}} ;$$

- iii) *it has exactly  $2^d + 1$  zeros in  $\mathbb{F}_{2^m}$  if and only if  $C_{m_1}(c) = 0$ .*

As an illustration, we apply Proposition 6 i) to a general polynomial  $G(x)$  in the following proposition, which will be used to explicitly give the zero of  $P(x)$  in  $\mathbb{F}_{2^m}$  with  $m = nuw$ . The second cases can be applied in a similar manner.

**Proposition 7** *The polynomial*

$$G(x) = x^{2^l+1} + a_1x^{2^l} + a_2x + a_3$$

over  $\mathbb{F}_{2^m}$  has exactly one zero in  $\mathbb{F}_{2^m}$  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)  $a_2 \neq a_1^{2^l}$ ,  $Z_{m_1}(c) = 0$  and  $C_{m_1}(c) \neq 0$  with  $c = (a_1a_2 + a_3)/(a_1 + a_2^{2^{n-l}})^{2^l+1}$ .

Moreover, for Cases (i) and (ii), the zero of  $G(x)$  is given by  $x = a_1 + (a_1a_2 + a_3)^{\frac{1}{2^l+1}}$ ; for Case (iii), the unique zero is given by  $x = (a_1 + a_2^{2^{n-l}})(cC_{m_1}^{2^l-1}(c))^{2^{n-1}} + a_1$ .

*Proof* It is relatively easy to verify Case i) and Case ii). In fact, when  $a_2 = a_1^{2^l}$ , one obtains the equation

$$G(x) = (x + a_1)^{2^l+1} + (a_1a_2 + a_3) = 0.$$

The statement of Case i) immediately follows; and for Case ii), it is easily seen that the equation has a single solution only if  $\gcd(2^l + 1, 2^n - 1) = 1$ , equivalently,  $m_1 = n/\gcd(l, n)$  is odd.

For Case iii), the equation  $G(x) = 0$  can be reduced to a polynomial of the form  $F_c(y) = y^{2^l+1} + y + c = 0$  by the following substitution

$$\begin{aligned} F_c(y) &= s^{-(2^l+1)}G(sy + a_1) \\ &= s^{-(2^l+1)}\left((sy + a_1)^{2^l+1} + a_1(sy + a_1)^{2^l} + a_2(sy + a_1) + a_3\right) \\ &= s^{-(2^l+1)}\left(s^{2^l+1}y^{2^l+1} + s(a_1^{2^l} + a_2)y + a_1a_2 + a_3\right) \\ &= y^{2^l+1} + y + c, \end{aligned}$$

where

$$s = (a_1^{2^l} + a_2)^{2^{m-l}} = (a_1 + a_2^{2^{m-l}}) \text{ and } c = \frac{a_1a_2 + a_3}{s^{2^l+1}} = \frac{a_1a_2 + a_3}{(a_1 + a_2^{2^{m-l}})^{2^l+1}}.$$

It is clear that  $y$  is a zero of  $F_c(y) = y^{2^l+1} + y + c$  if and only if  $x = sy + a_1$  is a zero of  $G(x)$ . The desired statement follows from Proposition 6. □

**Corollary 1** *Let  $q_0 = 2^w$  for a positive integer  $w$ ,  $l = wv$ ,  $m = wun$  and  $m_1 = m/\gcd(l, m)$ . Let  $C_i(x)$ ,  $Z_i(x)$  be defined as in (23) respectively. Then the polynomial  $x^{q_0^v+1} + a_1x^{q_0^v} + a_2x + a_3$  over  $\mathbb{F}_{q^n}$  has exactly one solution in  $\mathbb{F}_{q^n}$  given by*

- i)  $x = a_1$  if  $a_2 = a_1^{q_0^v}$  and  $a_3 = a_1a_2$ ;
- ii)  $x = a_1 + (a_1a_2 + a_3)^{\frac{1}{q_0^v+1}}$  if  $a_2 = a_1^{q_0^v}$ ,  $a_3 \neq a_1a_2$  and  $m_1$  is odd;
- iii)  $x = (a_1 + a_2^{q_0^{n-v}})(cC_{m_1}^{q_0^v-1}(c))^{2^{m-1}} + a_1$  if  $a_2 \neq a_1^{q_0^v}$ ,  $Z_{m_1}(c) = 0$  and  $C_{m_1}(c) \neq 0$  with  $c = (a_1a_2 + a_3)/(a_1 + a_2^{q_0^{n-v}})^{q_0^v+1}$ .



### 4.2 Solving the equation $P(x) = 0$ over $\mathbb{F}_{q^n}$ when $\gcd(r, n) = 1$

For the projective polynomial  $P(x) = x^{q^r+1} + ax + b$  with  $\gcd(r, n) = 1$ , McGuire and Sheekey recently in [28] gave a complete criteria on the coefficients  $a, b$  for  $P(x) = 0$  to have 0, 1, 2 and  $q + 1$  solutions in  $\mathbb{F}_{q^n}$  by the analysis of the companion matrix of  $P(x)$ .

Let  $\sigma = q^r$  and define a sequence of  $2 \times 2$  matrices as follows:

$$C_0 = I_2, C = C_1 = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}, \text{ and } C_k = C_{k-1}C^{\sigma^{k-1}} = CC_{k-1}^{\sigma}, \tag{25}$$

where  $C_1$  is termed the companion matrix of  $P(x)$ , and  $C_k^{\sigma^i}$  is the matrix obtained from  $C_k$  by applying to each of its entries the automorphism  $x \mapsto x^{\sigma^i}$ . Furthermore, define a matrix

$$A_P = C_n = CC^{\sigma} \dots C^{\sigma^{n-1}}. \tag{26}$$

Since  $\det(C_1) = b$  and  $N(b) = b^{1+\sigma+\dots+\sigma^{n-1}}$ , one can easily verify  $\det(A_P) = N(b)$ . Denote

$$X = \begin{pmatrix} b/a & 0 \\ 0 & 1 \end{pmatrix}, Z_n = \begin{pmatrix} a^{(n-1)} & 0 \\ 0 & a^{(n)} \end{pmatrix} \text{ and } Y_m = \begin{pmatrix} -G_{n-2}^{\sigma} & -G_{n-1}^{\sigma} \\ G_{n-1} & G_n \end{pmatrix}, \tag{27}$$

where  $a^{(i)} = a^{\frac{\sigma^i-1}{\sigma-1}}$  and  $G_n$  can be computed using the recursive relation

$$G_n^{\sigma^2} - G_n = G_{n-1}^{\sigma} - G_{n-1}^{\sigma^2}. \tag{28}$$

Then it follows that

$$A_P = C_n = XY_nZ_n. \tag{29}$$

Hence one can express  $A_P$  associated with  $P(x)$  in terms of  $G_n$  as follows:

$$A_P = N(a) \begin{pmatrix} -u^{q-1} \cdot G_{n-2}^{\sigma} & -\frac{b}{a} \cdot G_{n-1}^{\sigma} \\ \frac{1}{a^{\sigma-1}} \cdot G_{n-1} & G_n \end{pmatrix}$$

where  $N(a)$  denotes the field norm of  $a \in \mathbb{F}_{q^n}$  from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$  and  $u = b^q/a^{q+1}$ . Note that if  $G_{n-1} = 0$  then  $A_P$  will be a diagonal matrix.

**Theorem 1** [28] *The number of roots of the projective polynomial  $P(x)$  in  $\mathbb{F}_{q^n}$  is given by*

$$\sum_{\lambda \in \mathbb{F}_q} \frac{q^{n_\lambda} - 1}{q - 1},$$

where  $n_\lambda$  is the dimension of the eigenspace of  $A_P$  corresponding to the eigenvalue  $\lambda$ . The number of roots of  $L(x)$  in  $\mathbb{F}_{q^n}$  is given by  $q^{n_1}$ . In other words, the dimension of the kernel of  $L(x)$  is  $2 - \text{Rank}(A_L - I_2)$ .

**Theorem 2** [28] *The polynomial  $P(x)$  has  $\frac{q^d - 1}{q - 1}$  roots in  $\mathbb{F}_{q^n}$  if and only if*

$$A_P = \lambda I_2,$$

where  $d$  is the dimension of the eigenspace of the matrix  $A_P$ .

The characteristic polynomial  $S_P(x) \in \mathbb{F}_q[x]$  of a  $2 \times 2$  matrix  $A_P$  is of the form

$$S_P(x) = x^2 - \text{Tr}(A_P)x + \det(A_P), \quad (30)$$

where  $\text{Tr}(A_P)$  is the trace of the matrix  $A_P$  and it is defined as the sum of its diagonal elements and  $\det(A_P)$  is the determinant of the matrix  $A_P$ . The polynomial  $S_P(x)$  can have 0, 1 or 2 roots in  $\mathbb{F}_q$ . For odd prime power  $q$ , the discriminant  $\Delta_S$  of the quadratic polynomial  $S_P(x)$  is of the form

$$\Delta_S = \text{Tr}(A_P)^2 - 4 \det(A_P). \quad (31)$$

Case 1) if  $\Delta_S$  is a non-square in  $\mathbb{F}_q$ ,  $S_P(x)$  has no solutions in  $\mathbb{F}_q$ , then  $P(x)$  has no solution in  $\mathbb{F}_{q^n}$ .

Case 2) If  $\Delta_S = 0$ ,  $S_P(x)$  has a unique solution  $\lambda$  in  $\mathbb{F}_q$ , then  $P(x)$  has 1 or  $q + 1$  solutions in  $\mathbb{F}_{q^n}$ .

- i) If the dimension of the eigenspace corresponding to  $\lambda$  is two, then  $P(x)$  has  $q + 1$  solutions in  $\mathbb{F}_{q^n}$ . Due to Theorem 2, this will happen if and only if  $A_P = \lambda I_2$  i.e.  $G_{n-1} = 0$  and  $G_n \in \mathbb{F}_q$ .
- ii) If the dimension of the eigenspace corresponding to  $\lambda$  is one, then  $P(x)$  has one solution in  $\mathbb{F}_{q^n}$ . Due to Theorem 2, this will happen if and only if  $A_P$  is not a multiple of  $I_2$  i.e.  $G_{n-1} \neq 0$ .

Case 3) If  $\Delta_S$  is a non-zero square in  $\mathbb{F}_q$ ,  $S_P(x)$  has two distinct roots (eigenvalues) in  $\mathbb{F}_q$ . If dimension of the eigenspaces corresponding to each eigenvalue is one, due to Theorem 1,  $P(x)$  has two solutions in  $\mathbb{F}_{q^n}$ .

Note that the projective polynomial  $P(x) = x^{q^r+1} + ax + b$  associates with the following linearized polynomial

$$L(x) = xP(x^{q^r-1}) = x^{q^{2r}} + ax^{q^r} + bx, \quad a, b \in \mathbb{F}_{q^n}.$$

It is readily seen that if we can efficiently solve the linearized polynomial  $L(x)$ , the roots of  $P(x)$  can be obtained accordingly. In [28] the authors also applied companion matrices to study the number of roots of the above linearized polynomial. Further works on the roots of linearized polynomials can be found in [7, 32, 46].

Below we provide another way of studying the roots of the linearized polynomials  $L(x)$  via the Dickson matrix directly.

**Theorem 3** *Let  $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$  be a basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$  and  $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$  a linearized polynomial in  $\mathcal{L}_n(\mathbb{F}_{q^n})$  with rank  $r$ . Let  $D$  be the associate Dickson matrix of*

$L(x)$ . Suppose  $D_0, D_1, \dots, D_{n-1}$  are the  $n$  rows of  $D$  and  $D_r = z_0D_0 + z_1D_1 + \dots + z_{r-1}D_{r-1}$ , where  $z_0, \dots, z_{r-1}$  in  $\mathbb{F}_{q^n}$ . Then the elements

$$\beta_i = \sum_{j=0}^{r-1} \alpha_i^{q^{n-j}} z_j^{q^{n-j}} - \alpha_i^{q^{n-r}}, \quad i = 0, 1, \dots, n - 1,$$

are roots of  $L(x)$ . Moreover, the kernel of  $L(x)$  in  $\mathbb{F}_{q^n}$  is given by

$$\ker(L) = \text{span}_{\mathbb{F}_q} \langle \beta_0, \beta_1, \dots, \beta_{n-1} \rangle.$$

*Proof* From Proposition 2 it is clear that the  $r$ -th row  $D_r$  can be expressed by a linear combination of  $D_0, D_1, \dots, D_{r-1}$  as  $D_r = \sum_{t=0}^{r-1} z_t D_t$ . That is to say, the vector  $z = (z_0, \dots, z_{n-1}) = (z_0, \dots, z_{r-1}, -1, 0, \dots, 0)$  satisfies  $z \cdot D = (0, \dots, 0)$ . Define

$$D_z^T = D_{(z_0, z_{n-1}^q, \dots, z_1^{q^{n-1}})} = \begin{pmatrix} [c]z_0 & \dots & z_{r-1} & -1 & 0 & \dots & 0 \\ 0 & z_0^q & \dots & z_{r-1}^q & -1 & \dots & 0 \\ \vdots & \ddots & \ddots & \dots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & z_0^{q^{n-r-1}} & \dots & z_{r-1}^{q^{n-r-1}} & -1 \\ & & & \ddots & \ddots & \ddots & \\ & & & & \ddots & \ddots & \\ z_1^{q^{n-1}} & \dots & z_r^{q^{n-1}} & 0 & \dots & 0 & z_0^{q^{n-1}} \end{pmatrix}.$$

It follows from the pattern of the Dickson matrix  $D$  that  $D_z^T \cdot D = 0_{n \times n}$ , where  $0_{n \times n}$  is the  $n \times n$  all zero matrix.

According to the definition of  $D_z$ , it is clear that it has rank at least  $n - r$ . On the other hand, since the Dickson matrix  $D$  has rank  $r$  and all rows of  $D_z$  are solution of  $(y_0, \dots, y_{n-1})D = (0, \dots, 0)$ , the rank of  $D_z$  is at most  $n - r$ . This means that  $D_z$  has rank exactly  $n - r$ .

Let  $M_\alpha$  be the Moore matrix associated with the basis  $\alpha_0, \dots, \alpha_{n-1}$ . It follows from Lemma 2 i) and iv) that

$$M_\alpha D_z^T = M_\alpha D_{z'} = M_\beta = \begin{pmatrix} \beta_0 & \beta_0^q & \dots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \dots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \dots & \beta_{n-1}^{q^{n-1}} \end{pmatrix},$$

where  $z' = (z_0, z_{n-1}^q, \dots, z_1^{q^{n-1}}) = (z_0, 0, \dots, 0, -1, z_{r-1}^{q^{n-(r-1)}}, \dots, z_1^{q^{n-1}})$  and

$$\beta_i = \sum_{j=0}^{n-1} \alpha_i^{q^j} z_{n-j}^{q^j} = \sum_{j=0}^{n-1} \alpha_i^{q^{n-j}} z_j^{q^{n-j}} = \sum_{j=0}^{r-1} \alpha_i^{q^{n-j}} z_j^{q^{n-j}} - \alpha_i^{q^{n-r}}$$

for  $i = 0, 1, \dots, n - 1$ . Recall that  $D_z^T \cdot D = 0_{n \times n}$ . It immediately follows that

$$0_{n \times n} = M_\beta \cdot D = \begin{pmatrix} \beta_0 & \beta_0^q & \dots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \dots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \dots & \beta_{n-1}^{q^{n-1}} \end{pmatrix} \begin{pmatrix} l_0 & l_{n-1}^q & \dots & l_1^{q^{n-1}} \\ l_1 & l_0^q & \dots & l_2^{q^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n-1} & l_{n-2}^q & \dots & l_0^{q^{n-1}} \end{pmatrix}.$$

Hence  $L(\beta_i) = 0$  for  $i = 0, 1, \dots, n - 1$ . Moreover, since the Moore matrix  $M_\alpha$  is nonsingular, the rank of  $M_\beta$  is the same as that of the rank of  $D_z$ , which implies that the rank of  $\beta_0, \dots, \beta_{n-1}$  over  $\mathbb{F}_q$  is equal to  $n - r$ . Thus the linear combination of  $\beta_0, \dots, \beta_{n-1}$  over  $\mathbb{F}_q$  yields all the solution of  $L(x)$  in  $\mathbb{F}_{q^n}$ . The desired conclusion follows.  $\square$

From Theorem 3, we see that finding solutions of a linearized polynomial can be converted to the task of computing the rank of its associated Dickson matrix  $D = (D_0, \dots, D_{n-1})^T$  and of finding a solution of  $D_r = x_0 D_0 + \dots + x_{r-1} D_{r-1}$ . In general, calculating the rank of a Dickson matrix  $D$  is nontrivial. Recently Csajbók in [6] proposed an interesting characterization of the rank of  $D$ .

**Theorem 4** [6] *Let  $D$  be the associated Dickson matrix of a linearized polynomial  $L(x) = \sum_{i=0}^{n-1} l_i x^{q^i}$  over  $\mathbb{F}_{q^n}$ . Denote by  $D_t$  the submatrix of  $D$  by removing the first  $t$  rows and the last  $t$  columns. Then  $L(x)$  has rank  $r$  if and only if*

$$|D_0| = \dots = |D_{n-r-1}| = 0 \quad \text{and} \quad |D_{n-r}| \neq 0.$$

By Theorem 4, in order to determine the rank of the Dickson matrix associated with  $L(x)$ , we need to calculate the determinant of  $D_0, D_1$  and  $D_2$ . The calculation for the case  $D_2$  is trivial. We only need to consider  $D_0$  and  $D_1$ . To this end, we need the following result.

**Theorem 5** *The determinant of the Dickson matrix*

$$D_0 = \begin{bmatrix} b & 0 & 0 & \dots & 0 & 1 & a^{q^{r(n-1)}} \\ a & b^{q^r} & 0 & \dots & 0 & 0 & 1 \\ 1 & a^{q^r} & b^{q^{2r}} & & & 0 & 0 \\ 0 & 1 & a^{q^{2r}} & & & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & & \\ & & & & \ddots & a^{q^{r(n-3)}} & b^{q^{r(n-2)}} & 0 \\ 0 & \dots & & & & 1 & a^{q^{r(n-2)}} & b^{q^{r(n-1)}} \end{bmatrix} \tag{32}$$

*associated with the linearized polynomial  $L(x) = x^{q^{2r}} + ax^{q^r} + bx$  can be calculated using the recursive relation*

$$|D_0| = (-1)^{n+1} \cdot a^{q^{r(n-1)}} |M_{n-1}| + 2b^{q^{r(n-1)}} |M_{n-2}| + N(a) + 1, \tag{33}$$

*where  $N(a)$  denotes the field norm of  $a \in \mathbb{F}_{q^n}$  from  $\mathbb{F}_{q^n}$  to  $\mathbb{F}_q$ ,  $M_n$  is a tridiagonal matrix of order  $n$  and  $M_{n-1} = D_1$ .*

Note that  $D_2$  is a lower triangular matrix and its determinant can be directly computed  $|D_2| = 1$ . In order to prove Theorem 5 we need the following observation.

**Lemma 3** *The determinant of the tridiagonal matrix*

$$M_n = \begin{bmatrix} a & b^q & 0 & \dots & & & 0 \\ c & a^q & b^{q^2} & & & & \vdots \\ 0 & c^q & a^{q^2} & & & & \vdots \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & b^{q^{n-2}} & & 0 \\ \vdots & & & & c^{q^{n-3}} & a^{q^{n-2}} & b^{q^{n-1}} \\ 0 & \dots & & & 0 & c^{q^{n-2}} & a^{q^{n-1}} \end{bmatrix} \tag{34}$$

is given by the recurrence relation

$$|M_n| = a^{q^{n-1}} |M_{n-1}| - b^{q^{n-1}} \cdot c^{q^{n-2}} |M_{n-2}|, \tag{35}$$

where  $|M_0| = 1$  and  $|M_{-1}| = 0$ .

*Proof* Using Laplace expansion on the last column for  $n \geq 2$  gives

$$\begin{aligned} |M_n| &= (-1)^{2n} \cdot a^{q^{n-1}} \begin{vmatrix} a & b^q & 0 & \dots & & & 0 \\ c & a^q & b^{q^2} & & & & \vdots \\ 0 & c^q & a^{q^2} & & & & \vdots \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & b^{q^{n-3}} & & 0 \\ \vdots & & & & c^{q^{n-4}} & a^{q^{n-3}} & b^{q^{n-2}} \\ 0 & \dots & & & 0 & c^{q^{n-3}} & a^{q^{n-2}} \end{vmatrix} \\ &+ (-1)^{2n-1} \cdot b^{q^{n-1}} \begin{vmatrix} a & b^q & 0 & \dots & & & 0 \\ c & a^q & b^{q^2} & & & & \vdots \\ 0 & c^q & a^{q^2} & & & & \vdots \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & a^{q^{n-3}} & & 0 \\ \vdots & & & & 0 & c^{q^{n-2}} & b^{q^{n-2}} \\ 0 & \dots & & & 0 & c^{q^{n-2}} & \end{vmatrix} \\ &= a^{q^{n-1}} |M_{n-1}| - b^{q^{n-1}} \cdot c^{q^{n-2}} |M_{n-2}|. \quad \square \end{aligned}$$

*Proof of Theorem 5.* The proof follows immediately by applying Laplace expansion and Lemma 3. Note that the determinant of an upper (lower) triangular matrix is the product of the elements in its main diagonal.

Theorem 5 characterizes the conditions for the associated Dickson matrix of  $L(x) = x^{q^{2r}} + ax^{q^r} + bx$  to have rank  $n$ ,  $n - 1$  and  $n - 2$ . According to Theorem 3, one can obtain the roots of  $L(x)$  by finding the coefficients in the linear combination of the first  $n - 1$  rows of  $D$  when  $D$  has rank  $n - 2$  and coefficients in the linear combination of all rows of  $D$  when  $D$  has rank  $n - 1$ . Here the modified BM algorithm [43] will be employed, which requires

$\mathcal{O}(n^2)$  operations in  $\mathbb{F}_{q^n}$  for these two cases. With the coefficients, the roots of  $L(x)$  are given by Theorem 3.

Instead of using Theorem 3 to compute the roots of the linearized polynomial  $L(x)$ , one may use the probabilistic method given in [46]. The problem of finding the root space of the linearized polynomial  $L(x)$  is reduced to find the image space of another linearized polynomial  $K(x)$  derived from

$$x^{q^n} - x = W(x) \circ K(x),$$

where  $W(x) = \gcd(L(x), x^{q^n} - x)$ . The idea is to randomly choose  $y_i \in \mathbb{F}_{q^n}$  and calculate  $K(y_i)$  until the base elements for the image space of  $K(x)$  are obtained. Since  $L(x)$  has  $\sigma$ -degree 2, we need to find two basis elements  $K(y_1), K(y_s)$  for the image space of  $K(x)$ . According to [46], the algorithm has complexity in the order of  $\mathcal{O}(n)$  operations in  $\mathbb{F}_{q^n}$ . In general the expected number of  $y_j \in \mathbb{F}_{q^n}$  that need to be evaluated in order to find  $n$  linearly independent basis elements  $K(y_0), \dots, K(y_{n-1})$  is given by  $\frac{1}{1-q^{j-n}}$  [46].  $\square$

## 5 The decoding algorithm of AGTG codes

With the discussion in Sections 3.2–4, we summarize the interpolation polynomial decoding algorithm of AGTG codes in Algorithm 2, and analyze its complexity accordingly.

Recall that reconstruction the error interpolation polynomial  $g(x)$  is to solve (15) based on the available information in (13). For the case that  $t = \frac{n-k}{2}$  with even  $n-k$ , according to Algorithm 1,  $\Lambda^{(n-k-1)}(x)$  is the linearized polynomial obtained after  $n-k$  iteration and its coefficients are the desired vector  $(\lambda_1, \dots, \lambda_t)$ .  $L$  is the linear complexity of  $\Lambda^{(n-k-1)}(x)$  and  $B^{(n-k-1)}(x)$  is the auxiliary linearized polynomial which is used to store the value of  $\Lambda^{(i)}(x)$  with the largest degree  $L_i$  such that  $L_i < L$ . Hence one can obtain from Algorithm 1 two  $t$ -dimensional vectors  $\lambda$  and  $\lambda'$  over  $\mathbb{F}_{q^n}$ . Then the solution of (15) is given as

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

from which the coefficients  $g_0, \dots, g_k$  can be calculated recursively. The relation of  $g_0$  and  $g_k$  in (13) leads to a quadratic equation

$$\mathcal{P}(x) = u_0x^{q_0^v+1} + u_1x^{q_0^v} + u_2x + u_3 = 0.$$

If  $u_0 = 0$  calculate its zeros by cases i)-iv) after (19) or use Theorem 5, Berlekamp Massey Algorithm 1, Theorem 3 and Corollary 1 otherwise. The above process therefore can be integrated into the explicit Algorithm 2.

*Remark 2* In the proposed Algorithm 2, we reconstruct the error interpolation polynomial  $g(x)$  by two major steps: calculate the coefficients  $\lambda_1, \dots, \lambda_t$  by the modified BM algorithm, and deal with the case  $t = \lfloor (n-k)/2 \rfloor$  by investigating the zero of the established polynomial  $\mathcal{P}(x)$ . Section 4 investigates the solutions to  $\mathcal{P}(x) = 0$ . In the process, the calculation of the characterized conditions in Theorem 2 dominates the overall complexity. In Line 1 of Algorithm 2, the calculation of the interpolation polynomial  $\gamma(x)$  at points  $(\alpha_i, r_i)$  for  $1 \leq i \leq n$ . It has complexity in the order of  $\mathcal{O}(n^3)$  operations over  $\mathbb{F}_{q^n}$ , which can be further optimized by the method in [34]. For the remaining steps in Algorithm 2, the modified BM algorithm dominates the overall complexity. Since the modified BM algorithm has



operations in the order of  $\mathcal{O}(n^2)$  over  $\mathbb{F}_{q^n}$ , the overall complexity of Algorithm 2 is in the order of  $\mathcal{O}(n^2)$  over  $\mathbb{F}_{q^n}$  when normal bases are used in the interpolation step.

---

**Algorithm 2** Interpolation decoding of AGTG codes.

---

**Input:** A received word  $r$  with  $t \leq \lfloor \frac{n-k}{2} \rfloor$  errors and linearly independent evaluation points  $\alpha_1, \dots, \alpha_n$

**Output:** The correct codeword  $c \in \mathbb{F}_{q^n}$  or “Decoding Failure”

- 1 Calculate  $\gamma(x) = \sum_{i=0}^{n-1} \gamma_i x^{[i]}$  such that  $\gamma(\alpha_i) = r_i$  for  $i = 1, \dots, n$ ;
- 2 Apply modified BM algorithm to  $(g_{k+1}, \dots, g_{n-1}) = (\gamma_{k+1}, \dots, \gamma_{n-1})$  and output  $L, \Lambda^{(n-k-1)}(x), B^{(n-k-1)}(x)$ ;
- 3 **if**  $L = (n - k)/2$  **then**
- 4 Denote  $\Delta = -\omega + \sum_{i=1}^L \Lambda_i^{(n-k-1)} g_{n-1-i}^{q^{si}}$  with  $\omega \in \mathbb{F}_{q^n}$  ;
- 5 Express the coefficients of the polynomial
- $$\Lambda^{(n-k)}(x) = \frac{1}{\Delta} \Lambda^{(n-k-1)}(x) + x^{q^s} \circ B^{(n-k-1)}(x),$$
- Derive the connection vector  $(\lambda_1, \dots, \lambda_t)$  from monic  $\Lambda^{(n-k)}(x)$ ;
- 6 Derive the polynomial  $\mathcal{P}(x) = u_0 x^{q_0^v+1} + u_1 x^{q_0^v} + u_2 x + u_3$  in (19);
- 7 **if**  $u_0 = 0$  **then**
- 8 | Calculate the zero to  $\mathcal{P}(x)$  by Cases i)-iv) after (19);
- 9 **else**
- 10 | Calculate the zero to  $\mathcal{P}(x)$  by Theorem 5, the modified BM algorithm and Theorem 3;
- 11 **end**
- 12 Set  $(\lambda_1, \dots, \lambda_t) = \lambda + \omega \lambda'$  with  $\omega$  as the zero of  $\mathcal{P}(x)$ ;
- 13 Calculate  $g_0, g_k$  from (19);
- 14 **end**
- 15 **for each**  $i$  in  $\{1, \dots, k\}$  **do**
- 16 | Calculate  $g_i = \lambda_1 g_{i-1}^{[1]} + \dots + \lambda_t g_{i-t}^{[t]}$ , where the subscripts of  $g_j$ 's are taken modulo  $n$ ;
- 17 **end**
- 18 **if** The sequence  $g_0, \dots, g_{n-1}$  derived from  $\lambda_1, \dots, \lambda_t$  has period  $n$  **then**
- 19 | Return the codeword  $c = (c_1, \dots, c_n)$  with  $c_i = r_i + g(\alpha_i)$
- 20 **else**
- 21 | Return “Decoding Failure”
- 22 **end**

---

## 6 Conclusion

This paper further investigates the interpolation-based decoding algorithm for additive generalized twisted Gabidulin codes over finite fields with any characteristic. The main contribution of this paper includes the discussion of efficiently finding the roots of the involved project polynomials and their corresponding linearized polynomials.

**Acknowledgments** The authors would like to thank the anonymous reviewers for their valuable suggestions and comments. The work of C. Li was supported by the Research Council of Norway (No. 247742/O70, No. 311646/O70), and was supported in part by the National Natural Science Foundation of China under Grant (No. 61771021).

**Funding Information** Open Access funding provided by University of Bergen.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Abhyankar, S.: Projective polynomials. *Proceedings of the American Mathematical Society* **125**(6), 1643–1650 (1997)
2. Bluher, A.W.: On  $x^{q+1+ax+b}$ . *Finite Fields and Their Applications* **10**(3), 285–305 (2004)
3. Bracken, C., Hellese, T.: Triple-Error-Correcting BCH-Like codes. In: 2009 IEEE International Symposium on Information Theory, pp. 1723–1725 (2009)
4. Budaghyan, L., Carlet, C.: Classes of quadratic apn trinomials and hexanomials and related structures. *IEEE Trans. Inf. Theory* **54**(5), 2354–2357 (2008)
5. Csajbók, B., Marino, G., Polverino, O., Zhou, Y.: Maximum rank-distance codes with maximum left and right idealisers. arXiv:1807.08774 (2018)
6. Csajbók, B.: Scalar q-subresultants and Dickson matrices. arXiv:1909.06409 (2019)
7. Csajbók, B., Marino, G., Polverino, O., Zullo, F.: A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications* **56**, 109–130 (2019)
8. Csajbók, B., Marino, G., Zullo, F.: New maximum scattered linear sets of the projective line. *Finite Fields and Their Applications* **54**, 133–150 (2018)
9. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A* **25**(3), 226–241 (1978)
10. Dillon, J., Dobbertin, H.: New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications* **10**(3), 342–389 (2004)
11. Dobbertin, H., Felke, P., Hellese, T., Rosendahl, P.: Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. *IEEE Trans. Inf. Theory* **52**(2), 613–627 (2006)
12. 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 (1991)
13. Gabidulin, E.M.: Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii* **21**(1), 3–16 (1985)
14. Gadouleau, M., Yan, Z.: Complexity of decoding Gabidulin codes. In: *The 42Nd Annual Conference on Information Sciences and Systems*, pp. 1081–1085 (2008)
15. Gow, R., Quinlan, R.: Galois theory and linear algebra. *Linear Algebra and its Applications* **430**(7), 1778–1789 (2009). special Issue in Honor of Thomas J. Laffey
16. Hellese, T., Kholosha, A., Ness, G.J.: Characterization of  $m$ -sequences of lengths  $2^{2k} - 1$  and  $2^k - 1$  with three-valued cross correlation. *IEEE Trans. Inf. Theory* **53**(6), 2236–2245 (2007)
17. Hellese, T., Kholosha, A.: On the equation  $x^{2^{l+1}} + x + a = 0$  over  $GF(2^k)$ . *Finite Fields and Their Applications* **14**(1), 159–176 (2008)
18. Hellese, T., Kholosha, A.:  $x^{2^{l+1}+x+a}$  and related affine polynomials over  $GF(2^k)$ . *Cryptogr. Commun.* **2**(1), 85–109 (2010)
19. Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory* **54**(8), 3579–3591 (2008)

20. Kshevetskiy, A., Gabidulin, E.: The new construction of rank codes. In: International Symposium on Information Theory, (ISIT), pp. 2105–2108. IEEE (2005)
21. Kwang Ho Kim, S.M.: Solving  $x^{2^k+1} + x + a = 0$  over  $GF(2^n)$ . arXiv:1903.07481 (2019)
22. Li, C.: Interpolation-based decoding of nonlinear maximum rank distance codes. In: International Symposium on Information Theory (ISIT) (2019)
23. Li, C., Kadir, W.: On decoding additive generalized twisted Gabidulin codes presented at the International Workshop on Coding and Cryptography (WCC) (2019)
24. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2 edn (1997)
25. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding gabidulin codes. In: Ytrehus, Ø. (ed.) International Workshop on Coding and Cryptography (WCC), pp. 36–45. Springer, Berlin (2006)
26. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. Journal of Combinatorial Theory Series A **159**, 79–106 (2018)
27. Lusina, P., Gabidulin, E., Bossert, M.: Maximum rank distance codes as space-time codes. IEEE Trans. Inf. Theory **49**(10), 2757–2760 (2003)
28. McGuire, G., Sheekey, J.: A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. Finite Fields and Their Applications **57**, 68–91 (2019)
29. Ore, O.: On a special class of polynomials. Trans. Am. Math. Soc. **35**(3), 559–559 (1933)
30. Otal, K., Özbudak, F.: Additive rank metric codes. IEEE Trans. Inf. Theory **63**(1), 164–168 (2017)
31. 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)
32. Polverino, O., Zullo, F.: On the number of roots of some linearized polynomials. arXiv:1909.00802 (2019)
33. Puchinger, S., Rosenkilde, J., Sheekey, J.: Further generalisations of twisted Gabidulin codes. In: Proceedings of the 10th International Workshop on Coding and Cryptography (2017)
34. Puchinger, S., Wachter-Zeh, A.: Fast operations on linearized polynomials and their applications in coding theory. J. Symb. Comput. **89**, 194–215 (2018)
35. Randrianarisoa, T.H.: A decoding algorithm for rank metric codes. arXiv:1712.07060 (2017)
36. Richter, G., Plass, S.: Fast decoding of rank-codes with rank errors and column erasures. In: International Symposium on Information Theory (ISIT), pp. 398–398 (June 2004)
37. Rosenthal, J., Randrianarisoa, T.H.: A decoding algorithm for twisted gabidulin codes. In: International Symposium on Information Theory (ISIT), pp. 2771–2774. IEEE (2017)
38. Roth, R.M.: Maximum-rank array codes and their application to crisscross error correction. IEEE Trans. Inf. Theory **37**(2), 328–336 (1991)
39. Roth, R.M.: Tensor codes for the rank metric. IEEE Trans. Inf. Theory **42**(6), 2146–2157 (1996)
40. Sheekey, J.: A new family of linear maximum rank distance codes. Advances in Mathematics of Communications **10**, 475 (2016)
41. Sheekey, J.: Mrd codes: Constructions and connections. arXiv:1904.05813 (2019)
42. Sheekey, J.: New semifields and new mrd codes from skew polynomial rings. J. Lond. Math. Soc. **101**(1), 432–456 (2020)
43. Sidorenko, V., Richter, G., Bossert, M.: Linearized shift-register synthesis. IEEE Trans. Inf. Theory **57**(9), 6025–6032 (2011)
44. Silva, D., Kschischang, F.R., Koetter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory **54**(9), 3951–3967 (2008)
45. Silva, D., Kschischang, F.R.: Fast encoding and decoding of gabidulin codes. In: International Symposium on Information Theory (ISIT), pp. 2858–2862. IEEE (2009)
46. Skachek, V., Roth, R.M.: Probabilistic algorithm for finding roots of linearized polynomials. Des. Codes Crypt. **46**(1), 17–23 (2008)
47. Trombetti, R., Zhou, Y.: A new family of mrd codes in  $\mathbb{F}_q^{2n \times 2n}$  with right and middle nuclei  $\mathbb{F}_{q^n}$ . IEEE Trans. Inf. Theory **65**(2), 1054–1062 (2019)
48. Wachter-Zeh, A., Afanassiev, V., Sidorenko, V.: Fast decoding of Gabidulin codes. Des. Codes Crypt. **66**(1-3), 57–73 (2013)
49. Wu, B., Liu, Z.: Linearized polynomials over finite fields revisited. Finite Fields and Their Applications **22**, 79–100 (2013)