Algebraic List Decoding of Elliptic Codes Through Module Basis Reduction

Yunqi Wan †, Li Chen †, Fangguo Zhang §
† School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China
§ School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China
Email: wanyq5@mail2.sysu.edu.cn, chenli55@mail.sysu.edu.cn, isszhfg@mail.sysu.edu.cn

***Abstract*—Elliptic codes is an important class of algebraic-geometric (AG) codes due to their least genus penalty. Their codeword length can exceed that of Reed-Solomon (RS) codes defined over the same finite field, resulting in a greater error-correction capability. This paper proposes the module basis reduction (BR) technique for solving the interpolation problem in algebraic list decoding (ALD) of one-point elliptic codes. A basis of the module that satisfies all interpolation constrains can be constructed by defining the explicit Lagrange interpolation function over the elliptic function field. They lead to the generators for the module basis. The basis can be further reduced to the desired Gröbner basis which contains the minimum interpolation polynomial $Q(x, y, z)$. Compared with Koetter's interpolation, the BR interpolation technique significantly reduces the complexity in finding $Q(x, y, z)$. Our analysis shows the BR interpolation complexity will reduce as the code rate increases.**

I. Introduction

Algebraic-geometric (AG) codes were introduced by Goppa [1] based on algebraic curves over finite fields. Reed-Solomon (RS) codes can be regarded as a special class of AG codes that are constructed from an affine straight line. They have been widely employed in communication and storage systems. However, its length cannot exceed the size of finite field, which limits their error-correction capability. General AG codes have a codeword length greater than the size of finite field, and its minimum Hamming distance is lower bounded by its designed distance that is defined as $d^* = n - k - g + 1$, where n, k and g are the length of the code, the dimension of the code and the genus of the curve, respectively. However, an AG code that enjoys a large codeword length also suffers from a large genus penalty. Elliptic curves have $g = 1$, resulting in elliptic codes maintain a good tradeoff between its codeword length and genus penalty.

The early decoding algorithms for AG codes were the syndrome based decoding, with an error-correction capability bounded by $\lfloor \frac{d^*-1}{2} \rfloor$.The Berlekamp-Massey (BM) algorithm on univariate linear recursive relation was generalized by Sakata [2] to multivariate domain, which is called the BMS algorithm. Assisted by Feng and Rao's the majority voting [3] for determining the unknown syndromes, Sakata *et al.* [4] presented a fast decoding algorithm for AG codes. The interpolation based algebraic list decoding (ALD) was first proposed to decode low rate RS codes by Sudan [5], which has an error-correction capability beyond $\lfloor \frac{d^*-1}{2} \rfloor$. By constructing a curve that passes through all interpolation points with a multiplicity, Guruswami and Sudan [6] later improved it to decode all rate RS and AG codes, namely the Guruswami-Sudan (GS) algorithm. It can correct up to $n - \lfloor \sqrt{n(n-d^*)} \rfloor - 1$ errors. The ALD algorithm consists of interpolation and root-finding. The interpolation is often realized by Koetter's iterative polynomial construction [7] which dominates the decoding complexity. By defining zero basis of each affine point, Høholdt and Nielsen [8] presented a mathematical framework for GS decoding of Hermitian codes. Using Koetter's interpolation, soft-decision ALD of Hermitian codes was later proposed by Chen *et al.* [9]. Recently, the authors have presented GS decoding of elliptic codes using Koetter's interpolation [10]. The other interpolation technique is based on the Gröbner basis of modules [11]. It not only has a lower complexity than Koetter's interpolation, but also eliminates the need of pre-computing the zero basis of each affine point and the corresponding coefficients [12]. Lee and O'Sullivan proposed GS decoding of Hermitian codes using the module basis reduction (BR) interpolation technique [13]. By applying the Alekhnovich basis reduction algorithm [14], Beelen and Brander further reduced the complexity in finding the interpolation polynomial for a class of AG codes [15]. In [16], Nielsen and Beelen presented the power decoding and GS decoding algorithms for Hermitian codes, both of which apply the BR technique realized by the fast approach of [17]. Lax defined a generic interpolation polynomial by considering the components of a received word as variables [18], and further generalized the list decoding algorithm for Hermitian codes [13] to decode AG codes.

This paper introduces ALD for one-point elliptic codes using the BR interpolation technique. Based on the theory of Gröbner basis of modules, the interpolation problem is transformed into finding the minimal polynomial in the reduced module basis. In order to construct the basis of a module that satisfies all interpolation constrains, the Lagrange interpolation functions over the elliptic function field are defined. They lead to the definition of module generators, constituting the module basis. Together with the basis reduction, they formulate the module based ALD algorithm for elliptic codes. Complexity of the BR interpolation for ALD of elliptic codes will be characterized. Our analysis will show that the BR interpolation have lower complexity in comparison with Koetter's interpolation [10]. The BR interpolation complexity would also be lower for a higher rate code.

II. Elliptic Curves and Elliptic Codes

Let $\mathbb{F}_q$ denote a finite field of size q. The elliptic curve χ in homogeneous coordinates over $\mathbb{F}_q$ is defined by a nonsingular Weierstrass equation

$$Y^2Z + \mathfrak{a}_1XYZ + \mathfrak{a}_3YZ^2 = X^3 + \mathfrak{a}_2X^2Z + \mathfrak{a}_4XZ^2 + \mathfrak{a}_6Z^3, \tag{1}$$

where curve coefficients $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4, \mathfrak{a}_6 \in \mathbb{F}_q$. The curve has a genus of $g = 1$. Over χ, there exists a point of infinity, i.e., $P_\infty = (0, 1, 0)$. With $Z = 1$, an affine component of χ can be obtained as

$$Y^2 + \mathfrak{a}_1XY + \mathfrak{a}_3Y = X^3 + \mathfrak{a}_2X^2 + \mathfrak{a}_4X + \mathfrak{a}_6. \tag{2}$$

Points on the above affine curve are called affine points. For simplicity, they are denoted as $P_i = (x_i, y_i)$. Let $\chi(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points of χ, i.e., $\chi(\mathbb{F}_q) = \{P_i\} \bigcup \{P_\infty\}$. $\mathbb{F}_q$-Rational points form an additive Abelian group based on the "chord-and-tangent" rule with P_∞ as the identity element [19]. For any affine point P_i of χ, there exists a smallest positive integer δ such that $\delta P_i = P_\infty$, where δ is the order of P_i. Coordinate ring of χ is the integral domain

$$\mathcal{R} = \mathbb{F}_q[X, Y]/ < Y^2 + \mathfrak{a}_1XY + \mathfrak{a}_3Y - X^3 - \mathfrak{a}_2X^2 - \mathfrak{a}_4X - \mathfrak{a}_6 > . \tag{3}$$

The elliptic function field $\mathbb{F}_q(\chi)$ of χ is the quotient field of $\mathcal{R}$. Let x and y denote the residue classes of X and Y in $\mathcal{R}$, respectively. Since $y^2 = -\mathfrak{a}_1xy - \mathfrak{a}_3y + x^3 + \mathfrak{a}_2x^2 + \mathfrak{a}_4x + \mathfrak{a}_6$, $\mathcal{R} = \mathbb{F}_q[x, y]$ and any element of $\mathcal{R}$ can be denoted as a bivariate polynomial (in x and y) with y-degree less than 2.

Given $h \in \mathbb{F}_q(\chi)$, its order at a rational point P is $v_P(h)$. There exists a function Λ, which is called a local parameter at P such that $v_P(\Lambda) = 1$ and $h = \Lambda^{v_P(h)}h'$, where $v_P(h') = 0$. h has a zero of order $v_P(h)$ at P if $v_P(h) > 0$. It has a pole of order $-v_P(h)$ at P if $v_P(h) < 0$. For elliptic curves, $-v_{P_\infty}(x) = 2$, $-v_{P_\infty}(y) = 3$ and $-v_{P_\infty}(x^\lambda y^\gamma) = 2\lambda + 3\gamma$. Let $\phi_a (a \in \mathbb{N})$ denote a monomial of $\mathcal{R}$, where $\mathbb{N}$ denote nonnegative integer. In general, $\phi_a = x^\lambda y^\gamma$, where $\lambda \in \mathbb{N}$ and $\gamma \in \{0, 1\}$. Consequently, monomials

$$1, x, y, x^2, xy, x^3, x^2y, x^4, x^3y, \ldots \tag{4}$$

form a basis of $\mathcal{R}$, which is called the pole basis. Therefore, $h \in \mathcal{R}$ can be written as $h = \sum h_a\phi_a$, where $h_a \in \mathbb{F}_q$ and $-v_{P_\infty}(h) = \max\{-v_{P_\infty}(\phi_a) \mid h_a \neq 0\}$.

***Definition** 1:* For each point P, define a formal symbol $[P]$. Let n_P denote an integer that corresponds to P, $D = \sum_{P \in \chi(\mathbb{F}_q)} n_P[P]$ is a divisor of χ. It has a degree of $\deg(D) = \sum_{P \in \chi(\mathbb{F}_q)} n_P$ and a sum of $\mathrm{sum}(D) = \sum_{P \in \chi(\mathbb{F}_q)} n_P P$.

***Definition** 2:* [19] Let $h \in \mathbb{F}_q(\chi)$ and $h \neq 0$, the divisor of h is defined as $\mathrm{div}(h) = \sum_{P \in \chi(\mathbb{F}_q)} v_P(h)[P]$. $\mathrm{div}(h)$ is also called the principle divisor of χ.

For any divisor D, let $\mathfrak{L}(D)$ denote the Riemann-Roch space defined by D.

Suppose $\{P_0, P_1, \ldots, P_{n-1}\}$ is a set of n distinct affine points on χ. Let $G = \sum_{i=0}^{n-1}[P_i]$ and $D = k[P_\infty]$ denote divisors of χ, where $k < n$. Let $f \in \mathfrak{L}(D)$ denote the message polynomial which can be written as

$$f(x, y) = f_0\phi_0 + f_1\phi_1 + \cdots + f_{k-1}\phi_{k-1}, \tag{5}$$

where $f_0, f_1, \ldots, f_{k-1} \in \mathbb{F}_q$ denote the message symbols. Based on χ, an one-point elliptic code is defined as

$$\mathcal{C}_\chi(G, D) = \{(f(P_0), f(P_1), \ldots, f(P_{n-1})), \forall f \in \mathfrak{L}(D)\}, \tag{6}$$

where codeword $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) = (f(P_0), f(P_1), \ldots, f(P_{n-1})) \in \mathbb{F}_q^n$. It has length n and dimension k. Designed distance of the code is $d^* = n - k$. Note that an (n, k) elliptic code will be an MDS code if and only if for any $\{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\} \subseteq \mathrm{supp}(G)$, $[P_{i_1}] + [P_{i_2}] + \cdots + [P_{i_k}] - k[P_\infty]$ is not a principal divisor.

The above description shows that the number of affine points on curve χ determines the length of the elliptic code. Based on the Hasse-Weil bound [19], the maximum number of affine points on an elliptic curve is $q + \lfloor 2\sqrt{q} \rfloor$. This number can be reached by choosing the curve coefficients $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ and $\mathfrak{a}_6$, appropriately.

Let $\mathbb{A} = \{\alpha_0, \alpha_1, \ldots\}$ denote the set of x-coordinate of all affine points on χ and $\mathbb{B}_i = \{\beta_i^{(j)}\}$ denote the set of $\mathbb{F}_q$ elements that satisfy ${\beta_i^{(j)}}^2 + \mathfrak{a}_1x_i\beta_i^{(j)} + \mathfrak{a}_3\beta_i^{(j)} = x_i^3 + \mathfrak{a}_2x_i^2 + \mathfrak{a}_4x_i + \mathfrak{a}_6$. In general, $|\mathbb{B}_i| = 2$. However, if $2P_i = P_\infty$, i.e., $-P_i = P_i$, $|\mathbb{B}_i| = 1$. If $\mathbb{F}_q$ has a characteristic of 2, there exists at most one affine point of order 2. Otherwise, there exists at most 3 such affine points. In this paper, the affine points of order 2 are not used to generate the codeword symbols. Therefore, $|\mathbb{A}| = n/2$ and $|\mathbb{B}_i| = 2$.

The following Lagrange interpolation function over the elliptic function field is introduced.

***Theorem** 1:* Let

$$\mathcal{L}_i(x, y) = \prod_{\alpha \in \mathbb{A} \setminus \{x_i\}} \frac{x - \alpha}{x_i - \alpha} \prod_{\beta \in \mathbb{B}_i \setminus \{y_i\}} \frac{y - \beta}{y_i - \beta}, \tag{7}$$

then $\mathcal{L}_i(x, y) \in \mathcal{R}$, and it satisfies $\mathcal{L}_i(P_i) = 1$, $\forall i$ and $\mathcal{L}_i(P_{i'}) = 0$, $\forall i' \neq i$.

Proof: Since $|\mathbb{B}_i| = 2$, then $\mathcal{L}_i(x, y)$ is a bivariate polynomial in x and y with y-degree less than 2, i.e., $\mathcal{L}_i(x, y) \in \mathcal{R}$. Substituting P_i into $\mathcal{L}_i(x, y)$ yields $\mathcal{L}_i(P_i) = 1$. For $i' \neq i$, there exists $x_{i'} \in \mathbb{A} \setminus \{x_i\}$ or $y_{i'} \in \mathbb{B}_i \setminus \{y_i\}$ and $\mathcal{L}_i(P_{i'}) = 0$. ■

III. Algebraic List Decoding

Let $\mathcal{R} = \bigcup_{u=0}^{\infty} \mathfrak{L}(u[P_\infty]) \subset \mathbb{F}_q(\chi)$ and $\mathcal{R}[z]$ denote the polynomial ring defined over $\mathcal{R}$. Given $\underline{r} = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ as a received word. The following set of n interpolation points can be formed

$$\mathbf{P} = \{(P_0, r_0), (P_1, r_1), \ldots, (P_{n-1}, r_{n-1})\}. \tag{8}$$

Interpolation constructs a minimum polynomial $Q(x, y, z) \in \mathcal{R}[z]$, which interpolates the n points with a multiplicity of m. If $Q(P_i, r_i) = 0$, Q interpolates (P_i, r_i). Let $\mathcal{R}[z]_{l_m} = \{Q \in \mathcal{R}[z] \mid \deg_z Q \leq l_m\}$, if an interpolation polynomial

$Q \in \mathcal{R}[z]_{l_m}$ can be written as

$$Q = \sum_{\mu+\nu \geq m} Q_{\mu\nu} \Lambda_i^{\mu} (z - r_i)^{\nu}, \tag{9}$$

and $Q_{\mu\nu} = 0$ for $\mu+\nu < m$, Q has a zero of multiplicity m at (P_i, r_i). Root-finding further decodes the message polynomial f through finding its z-roots, i.e., $Q(x, y, f) = 0$.

The $(1, k)$-weighted degree of monomial $\phi_a z^b$ is defined as $\deg_{1,k} \phi_a z^b = -v_{P_\infty}(\phi_a) + kb$, where the weight of z is $-v_{P_\infty}(\phi_{k-1}) = k$. Given two distinct monomials $\phi_{a_1} z^{b_1}$ and $\phi_{a_2} z^{b_2}$, we have $\text{ord}(\phi_{a_1} z^{b_1}) < \text{ord}(\phi_{a_2} z^{b_2})$, if $\deg_{1,k} \phi_{a_1} z^{b_1} < \deg_{1,k} \phi_{a_2} z^{b_2}$, or $\deg_{1,k} \phi_{a_1} z^{b_1} = \deg_{1,k} \phi_{a_2} z^{b_2}$ and $b_1 < b_2$. Hence, given a polynomial $Q = \sum_{a,b} Q_{ab} \phi_a z^b \in \mathcal{R}[z]$, where $Q_{ab} \neq 0$, its $(1, k)$-weighted degree and leading order can be defined as $\deg_{1,k} Q = \max\{\deg_{1,k} \phi_a z^b\}$ and $\text{lod}(Q) = \max\{\text{ord}(\phi_a z^b)\}$. Furthermore, given two distinct polynomials $Q_1, Q_2 \in \mathcal{R}[z]$, $Q_1 < Q_2$, if $\text{lod}(Q_1) < \text{lod}(Q_2)$.

***Theorem** 2:* [6] Given a polynomial $Q \in \mathcal{R}[z]$ that interpolates the n points of (8) with a multiplicity of m, and a polynomial h in the form of (5), if

$$m(n - |\{i \mid h(P_i) \neq r_i, \ \forall i\}|) > \deg_{1,k} Q, \tag{10}$$

$(z - h) \mid Q$ or $Q(x, \ y, \ h) = 0$.

Therefore, the message can be decoded by finding z-roots of Q. If message f can be decoded, i.e., $f(P_i) = c_i$, the ALD corrects $|\{i \mid f(P_i) \neq r_i, \ \forall i\}|$ errors and this error-correction capability can be improved by increasing m. Given an $(n, \ k)$ elliptic code, the ALD algorithm's error-correction capability is upper bounded by [6]

$$\tau_{\text{ALD}} = n - \left\lfloor \sqrt{nk} \right\rfloor - 1. \tag{11}$$

Furthermore, let l_m and τ_m denote the maximum number of decoded candidates and the error-correction capability with an interpolation multiplicity of m, respectively. Since the decoded candidates are z-roots of Q, $l_m = \deg_z Q$. $l_m \geq m$ holds. For an (n, k) elliptic code, they can be characterized as [10].

$$l_m = \left\lfloor \sqrt{\frac{nm(m+1)}{k} + \frac{1}{4}} - \frac{1}{2} \right\rfloor. \tag{12}$$

If $m(n - \tau_m) - k l_m \neq 1$,

$$\tau_m = n - \left\lfloor \frac{1}{m} + \frac{l_m k}{2m} + \frac{(m+1)n}{2(l_m+1)} \right\rfloor - 1, \tag{13}$$

otherwise,

$$\tau_m = n - \frac{1 + k l_m}{m}. \tag{14}$$

IV. The Interpolation

The BR interpolation consists of basis construction and basis reduction. The former is to construct a basis of $\mathbb{F}_q[x]$-module that consists of polynomials satisfying the interpolation constraints. Gröbner basis of the module will be obtained by basis reduction. The interpolation polynomial $Q(x, y, z)$ is the minimum element in the Gröbner basis. Before introducing the basis construction, the following preliminaries are needed.

***Definition** 3:* Let $\underline{\xi} = (\xi_0(x), \xi_1(x), \ldots, \xi_{\rho-1}(x))$ denote a vector over $\mathbb{F}_q[x]$, and $\underline{w} = (w_0, w_1, \ldots, w_{\rho-1}) \in \mathbb{N}^{\rho}$. The degree of $\underline{\xi}$ is

$$\deg \underline{\xi} = \max\{-v_{P_\infty}(\xi_i(x)) + w_i, \forall i\}. \tag{15}$$

The leading position of $\underline{\xi}$ is

$$\text{LP}(\underline{\xi}) = \max\{i \mid -v_{P_\infty}(\xi_i(x)) + w_i = \deg \underline{\xi}\} \tag{16}$$

and the leading term of $\underline{\xi}$ is

$$\text{LT}(\underline{\xi}) = \xi_{\text{LP}(\underline{\xi})}(x). \tag{17}$$

Coefficient of the leading monomial (also called the leading coefficient) of $\text{LT}(\underline{\xi})$ is denoted by $\text{LC}(\text{LT}(\underline{\xi}))$.

***Definition** 4:* Given a matrix Ξ over $\mathbb{F}_q[x]$, let $\Xi|_i$ denote its row-i and $\Xi|_i^{(j)}$ denote the its entry of row-i column-j, the degree of Ξ is

$$\deg \Xi = \max\{\deg \Xi|_i, \forall i\}. \tag{18}$$

A. Basis Construction

Let $\mathcal{I}_{\mathbf{P}} \subset \mathcal{R}[z]_{l_m}$ denote a set of all $Q \in \mathcal{R}[z]_{l_m}$ such that Q has a zero of multiplicity m at the set of interpolation points. Note that $\mathcal{I}_{\mathbf{P}}$ is an $\mathcal{R}$-module. To define a basis for $\mathcal{I}_{\mathbf{P}}$, the following two module seeds are needed.

$$\mathcal{G}(x) = \prod_{\alpha_i \in \mathbb{A}} (x - \alpha_i), \tag{19}$$

$$\mathcal{K}(x, y) = \sum_{i=0}^{n-1} r_i \mathcal{L}_i(x, y). \tag{20}$$

Based on Theorem 1, it can be seen that $\mathcal{K}(P_i) = r_i, \forall i$.

Given an interpolation polynomial Q in (9), it can be written as $Q = \sum_{j=0}^{l_m} Q_{[j]} z^j$, where $Q_{[j]} \in \mathcal{R}$. The following lemma can be led to.

***Lemma** 3:* Let $Q = \sum_{j=0}^{s} Q_{[j]} z^j \in \mathcal{I}_{\mathbf{P}}$ with $\deg_z Q = s < m$, $\mathcal{G}(x)^{m-s} | Q_{[s]}$.

Proof: Since $Q \in \mathcal{I}_{\mathbf{P}}$, it can be written as in (9) w.r.t. any interpolation point (P_i, r_i). Since $\deg_z Q = s < m$ and $\nu \leq s$, $Q_{[s]} = \sum_{\mu \geq m-s} Q_{\mu s} \Lambda_i^{\mu}$, i.e., $\Lambda_i^{m-s} | Q_{[s]}$. For P_i, since it is not an affine point of order 2, Λ_i can be defined as $\Lambda_i = x - x_i$. Therefore, $(x - x_i)^{m-s} | Q_{[s]}$. Considering all affine points, $\mathcal{G}(x)^{m-s} | Q_{[s]}$ can be led to. ■

***Theorem** 4:* $\mathcal{I}_{\mathbf{P}}$ is generated as an $\mathcal{R}$-module by $l_m + 1$ polynomials $\mathcal{H}^{(t)}(x, y, z) \in \mathcal{R}[z]_{l_m}$, where

$$\mathcal{H}^{(t)}(x, y, z) = \mathcal{G}(x)^{m-t} (z - \mathcal{K}(x, y))^t, \text{ if } 0 \leq t \leq m, \tag{21}$$

$$\mathcal{H}^{(t)}(x, y, z) = z^{t-m} (z - \mathcal{K}(x, y))^m, \text{ if } m < t \leq l_m. \tag{22}$$

Proof: Since both $\mathcal{G}(x)$ and $z - \mathcal{K}(x, y)$ interpolate point (P_i, r_i), $\mathcal{H}^{(t)}$ has a zero of multiplicity at least m at all interpolation points $\mathbf{P}$, i.e., $\mathcal{H}^{(t)} \in \mathcal{I}_{\mathbf{P}}$. The above definition shows that $\mathcal{H}_{[l_m]}^{(l_m)} = 1$. Given a polynomial $Q \in \mathcal{I}_{\mathbf{P}}$, there exists $h_{l_m} = Q_{[l_m]}$ such that $Q^{(l_m - 1)} = Q - h_{l_m} \mathcal{H}^{(l_m)}$, where $\deg_z Q^{(l_m - 1)} \leq l_m - 1$. Similarly, by (21) and (22), $\mathcal{H}_{[t]}^{(t)} = 1$ for $m \leq t \leq l_m - 1$, there exists polynomials

$h_t \in \mathcal{R}$ such that $Q^{(m-1)} = Q^{(l_m-1)} - \sum_{t=m}^{l_m-1} h_t \mathcal{H}^{(t)}$ and $\deg_z Q^{(m-1)} \leq m-1$. Therefore, $Q^{(m-1)} \in \mathcal{I}_{\mathbf{P}}$. By Lemma 3, $\mathcal{G}(x) | Q^{(m-1)}_{[m-1]}$. Since $\mathcal{H}^{(m-1)}_{[m-1]} = \mathcal{G}(x)$, there exists $h_{m-1} = \frac{Q^{(m-1)}_{[m-1]}}{\mathcal{G}(x)} \in \mathcal{R}$ such that $Q^{(m-2)} = Q^{(m-1)} - h_{m-1}\mathcal{H}^{(m-1)}$ with $\deg_z Q^{(m-2)} \leq m-2$. Following the same manner, $Q^{(t)}$ with $1 \leq t \leq m-2$ can be deduced using $\mathcal{H}^{(t)}$, until $Q^{(0)} = h_0 \mathcal{G}(x)^m$ is reached. ∎

***Theorem** 5:* $\mathcal{I}_{\mathbf{P}}$ is generated as an $\mathbb{F}_q[x]$-module by the basis $\mathcal{M}_{\mathbf{P}}$ following

$$\mathcal{M}_{\mathbf{P}} = \{M_i \mid M_i = y^{(i \bmod 2)} \mathcal{H}^{(\lfloor \frac{i}{2} \rfloor)}, 0 \leq i \leq 2l_m + 1\}. \quad (23)$$

Proof: Based on Theorem 4, for each $Q \in \mathcal{I}_{\mathbf{P}}$, there exist $h_0, \ldots, h_{l_m} \in \mathcal{R}$ such that $Q = \sum_{t=0}^{l_m} h_t \mathcal{H}^{(t)}$. Since h_t can be written as $h_t = \mathfrak{h}_t^{(0)} + \mathfrak{h}_t^{(1)} y$, where $\mathfrak{h}_t^{(0)}, \mathfrak{h}_t^{(1)} \in \mathbb{F}_q[x]$, $Q = \sum_{t=0}^{l_m} \sum_{j=0}^{1} \mathfrak{h}_t^{(j)} (y^j \mathcal{H}^{(t)})$. ∎

Therefore, given the set of interpolation points $\mathbf{P}$, the module seeds of (19) (20) can be defined. They lead to the basis construction of (23) for the $\mathbb{F}_q[x]$-module $\mathcal{I}_{\mathbf{P}}$.

B. Basis Reduction

The constructed basis $\mathcal{M}_{\mathbf{P}}$ will be further reduced, yielding the Gröbner basis $\mathcal{M}'_{\mathbf{P}}$ that contains the interpolation polynomial $Q(x, y, z)$.

Note that $\mathcal{R}[z]_{l_m}$ is a free module over $\mathbb{F}_q[x]$ of rank $2(l_m+1)$. It has a free basis of $\{1, y, z, yz, \ldots, z^{l_m}, yz^{l_m}\}$. $\mathcal{I}_{\mathbf{P}}$ is a submodule of $\mathcal{R}[z]_{l_m}$ over $\mathbb{F}_q[x]$, i.e., for each $Q \in \mathcal{I}_{\mathbf{P}}$, it can be written as $Q = (\xi_0(x), \xi_1(x), \ldots, \xi_{2l_m+1}(x))(1, y, \ldots, yz^{l_m})^T$. Based on Theorem 5, let $M_i(x, y, z) = M_i^{(0)}(x) + M_i^{(1)}(x) y + \cdots + M_i^{(2l_m+1)}(x) y z^{l_m}$, the basis $\mathcal{M}_{\mathbf{P}}$ of (23) can be accordingly represented as a matrix $\mathcal{V} \in \mathbb{F}_q[x]^{2(l_m+1) \times 2(l_m+1)}$ by letting

$$\mathcal{V}|_i = (M_i^{(0)}(x), M_i^{(1)}(x), \ldots, M_i^{(2l_m+1)}(x)). \quad (24)$$

Therefore, $M_i(x, y, z) = \mathcal{V}|_i \cdot (1, y, \ldots, yz^{l_m})^T$ and $\mathcal{V}|_i^{(j)} = M_i^{(j)}(x)$. Note that with $\underline{w} = (w_0, w_1, \ldots, w_{2l_m+1}) \in \mathbb{N}^{2(l_m+1)}$ and $w_i = k \times \lfloor \frac{i}{2} \rfloor + 3 \times (i \bmod 2)$, $\deg \mathcal{V}|_i = \deg_{1,k} M_i(x, y, z)$.

At the beginning, the basis $\mathcal{M}_{\mathbf{P}}$ of (23) can be initialized as a matrix $\mathcal{V}$, which is a lower triangular matrix. For each row $\mathcal{V}|_i$, $\mathrm{LP}(\mathcal{V}|_i)$ can be determined. Row operations of $\mathcal{V}$ will be performed until $\mathrm{LP}(\mathcal{V}|_i) = i$ is reached. Since $M_0 = \mathcal{G}(x)^m$ and $M_1 = \mathcal{G}(x)^m y$, $\mathrm{LP}(\mathcal{V}|_0) = 0$ and $\mathrm{LP}(\mathcal{V}|_1) = 1$. The row operations can start with $\mathcal{V}|_2$. In general, if $\mathrm{LP}(\mathcal{V}|_i) = i$, $\mathcal{V}|_i$ does not need to be modified. We go on to process $\mathcal{V}|_{i+1}$. If $\mathrm{LP}(\mathcal{V}|_i) = j$ and $j \neq i$, we let $u = \deg \mathcal{V}|_i - \deg \mathcal{V}|_j$ and $v = \mathrm{LC}(\mathrm{LT}(\mathcal{V}|_i))\mathrm{LC}(\mathrm{LT}(\mathcal{V}|_j))^{-1}$. If $u \geq 0$, $\mathcal{V}|_i$ will be updated by

$$\mathcal{V}|'_i = \mathcal{V}|_i - v x^u \mathcal{V}|_j. \quad (25)$$

Otherwise, $\mathcal{V}|_j$ and $\mathcal{V}|_i$ will be updated by

$$\mathcal{V}|'_j = \mathcal{V}|_i \quad (26)$$

and

$$\mathcal{V}|'_i = x^{-u} \mathcal{V}|_i - v \mathcal{V}|_j. \quad (27)$$

Note that the update of $\mathcal{V}|_i$ only involves the first $i-1$ rows of $\mathcal{V}$ and does not change the leading position of the rows.

The Gröbner basis $\mathcal{M}'_{\mathbf{P}}$ of $\mathcal{I}_{\mathbf{P}}$ can be obtained by demapping the updated $\mathcal{V}$, i.e., $\mathcal{V}|'_i \mapsto M'_i$. The minimum polynomial of $\mathcal{M}'_{\mathbf{P}}$ is chosen as interpolation polynomial $Q(x, y, z)$.

Summarizing the above description, the BR interpolation algorithm for ALD of elliptic codes is stated as follows. Based on Theorem 2, the message polynomial f can be further decoded by finding the z-roots of Q, i.e., $Q(x, y, f) = 0$. It can be determined by the root-finding algorithm of [20].

Algorithm 1 The BR Interpolation Algorithm

Input: $\underline{r}$ and m;
Output: Q;

```
Initialize M_P as in (23);
Represent M_P as matrix V over F_q[x] as in (24);
For i = 0 to 2l_m + 1
    Computing LP(V|_i);
    While LP(V|_i) ≠ i do
        j = LP(V|_i);
        If deg V|_i − deg V|_j ≥ 0
            Update V|_i as in (25);
        Otherwise
            Update V|_j and V|_i as in (26) and (27);
    End while
End for
Demap the updated V as M'_P.
Pick up the minimum candidate from M'_P as Q(x, y, z).
```

V. Complexity Analysis

This section analyzes complexity of the BR interpolation for ALD of elliptic codes. The complexity refers to the number of finite field multiplications required in decoding a codeword.

Complexity of the basis construction will be first analyzed.

***Theorem** 6:* Complexity of constructing the $\mathcal{M}_{\mathbf{P}}$ of (23) is $O(m^4 n^2)$.

Proof: Given an (n, k) elliptic code, polynomials $\mathcal{G}(x)^j$ and $\mathcal{L}_i(x, y)$ can be determined. Their construction complexity are not considered in a decoding event. Since $\deg_{1,k} \mathcal{L}_i(x, y) = n+1$, $\deg_{1,k} \mathcal{K}(x, y) = n+1$. Computing $\mathcal{K}(x, y)$ requires at most $n(n+1)$ multiplications. Further, computing (21) requires at most $\sum_{t=1}^{m} \sum_{j=0}^{t} \left(\frac{n}{2}(m-t)+1\right)(t-j)(n+1) = \frac{(n+1)}{48} m(m+1)(m+2)((m-1)n+8)$ multiplication. For remaining polynomials of (23), they can be obtained by the above assignment of $\mathcal{H}^{(m)}$ and $y\mathcal{H}^{(m)}$. Therefore, complexity of the basis construction is $O(m^4 n^2)$. ∎

Complexity of the basis reduction will be determined by $\deg \mathcal{V}$ and the number of row operations needed to bring $\mathcal{V}$ into a Gröbner basis.

***Lemma** 7:* [13] Given a row $\mathcal{V}|_i$ of matrix $\mathcal{V}$, at most $i(\deg \mathcal{V}|_i - \deg \mathcal{V}|_i^{(i)})$ updates are needed such that $\mathrm{LP}(\mathcal{V}|_i) = i$ and each update requires at most $\frac{i}{2} \deg \mathcal{V}$ finite field multiplications.

***Theorem** 8:* Given a matrix $\mathcal{V} \in \mathbb{F}_q[x]^{2(l_m+1)\times 2(l_m+1)}$, complexity of the basis reduction is $O(m^2 l_m^3 n(n-k))$.

Proof: Since $\deg_{1,k}\mathcal{G}(x) = n$ and $\deg_{1,k}\mathcal{K}(x,y) = n+1$, based on Theorem 5, $\deg\mathcal{V} \leq \deg\mathcal{V}|_{2l_m+1}^{(2(l_m-m))} = m(n+1) + k(l_m - m) + 3$. For $\mathcal{V}|_i (i = 0, 1, \ldots, 2m+1)$, $\deg\mathcal{V}|_i = mn + 3i - 5\lfloor \frac{i}{2} \rfloor$ and $\deg\mathcal{V}|_i^{(i)} = n(m - \lfloor \frac{i}{2} \rfloor) + w_i$. Hence, $\deg\mathcal{V}|_i - \deg\mathcal{V}|_i^{(i)} = \lfloor \frac{i}{2} \rfloor (n+1-k)$. If $2m+1 < i < 2l_m + 2$, $\deg\mathcal{V}|_i = m(n+1) + k\lceil \frac{i-2m-1}{2} \rceil + 3(i \bmod 2)$ and $\deg\mathcal{V}|_i^{(i)} = w_i$. Hence, $\deg\mathcal{V}|_i - \deg\mathcal{V}|_i^{(i)} = m(n+1-k)$. Therefore, reducing $\mathcal{V}$ into a Gröbner basis requires at most $\sum_{i=0}^{2l_m+1} \frac{i^2}{2} \deg\mathcal{V}(\deg\mathcal{V}|_i - \deg\mathcal{V}|_i^{(i)}) \approx \frac{4l_m^3}{3} m(n-k)(mn + kl_m - km)$ finite field multiplications. ∎

The above analysis shows that the basis reduction dominates the BR interpolation complexity, and the basis reduction complexity reduces as the code rate increases. Tables I and II show our numerical results of the BR interpolation in decoding the $(80, 27)$ and the $(80, 39)$ elliptic codes, respectively. The two codes are constructed based on: $y^2 + y = x^3$ defined over $\mathbb{F}_{64}$. They validate the above analysis. In comparison with Koetter's interpolation whose complexity can be characterized as $O(l_m m^4 n^2)$, BR interpolation would be simpler in practice although they exhibit the same asymptotic behavior. By introducing re-encoding transform to reduce the interpolation complexity, Koetter's interpolation and BR interpolation are all reduced by a factor of $\frac{k}{n}$. This will be the authors' future work. It should be pointed out that there exist several basis reduction algorithms [14] [17] that exhibit an asymptotically lower complexity than the above mentioned process. However, they heavily rely on fast multiplication techniques which contribute to a large constant factor hidden in the big-O notation, This makes their complexity greater than the MS algorithm in decoding a code of practical length.

TABLE I
INTERPOLATION COMPLEXITY OF THE $(80, 27)$ ELLIPTIC CODE

(m, l_m, τ_m)		$(2, 3, 29)$	$(4, 7, 31)$	$(7, 12, 32)$
Koetter		7.93×10^5	1.65×10^7	2.14×10^8
BR	Basis Construction	1.46×10^4	4.85×10^4	1.78×10^5
	Basis Reduction	4.48×10^5	1.41×10^7	1.88×10^8

TABLE II
INTERPOLATION COMPLEXITY OF THE $(80, 39)$ ELLIPTIC CODE

(m, l_m, τ_m)		$(2, 3, 20)$	$(4, 5, 22)$	$(8, 11, 23)$
Koetter		6.78×10^5	8.00×10^6	2.20×10^8
BR	Basis Construction	1.46×10^4	4.85×10^4	2.50×10^5
	Basis Reduction	2.80×10^5	4.06×10^6	1.36×10^8

VI. CONCLUSION

This paper has proposed the BR interpolation algorithm for ALD of one-point elliptic codes. The Lagrange interpolation function over the elliptic function field has been proposed for defining the module seeds. A basis of the module satisfying all interpolation constrains has also been presented. Together with a basis reduction, the BR interpolation algorithm for elliptic codes has been proposed. Our complexity analysis has shown that the BR interpolation has lower complexity than Koetter's interpolation and has more advantages for decoding high rate codes. They have been verified by numerical results.

ACKNOWLEDGEMENT

This work is sponsored by the National Natural Science Foundation of China (NSFC) with project IDs 61671486 and 61972429.

REFERENCES

[1] V. Goppa, "Codes associated with divisors," *Probl. Pered. Inform.*, vol. 13(1), pp. 33–39, 1977.
[2] S. Sakata, "Extension of the Berlekamp-Massey algorithm to N dimensions," *Inform. Comput.*, vol. 84, pp. 207–239, 1990.
[3] G. Feng and T. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inf. Theory,*, vol. 39(1), pp. 37–46, Jan. 1993.
[4] S. Sakata, J. Justesen, Y. Madelung, H. Jensen, and T. Høholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inf. Theory*, vol. 41(6), pp. 1672–1677, Nov. 1995.
[5] M. Sudan, "Decoding of Reed-Solomon codes beyond the error-correction bound," *J. Complexity*, vol. 13(1), pp. 180–193, Mar. 1997.
[6] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45(6), pp. 1757–1767, Sep. 1999.
[7] R. Koetter, "On algebraic decoding of algebraic-geometric and cyclic codes," Ph.D. dissertation, Linköping Univ., Linköping, Sweden, 1996.
[8] T. Høholdt and R. Nielsen, "Decoding Hermitian codes with Sudan's algorithm," in *AAECC (Lect. Notes Comput. Sci.)*, vol. 1719. Germany, Berlin:Springer-Verlag, 1999, pp. 260–269.
[9] L. Chen, R. Carrasco, and M. Johnston, "Soft-decision list decoding of Hermitian codes," *IEEE Trans. Commun.*, vol. 57(8), pp. 2169–2176, Aug. 2009.
[10] Y. Wan, L. Chen, and F. Zhang, "Design of Guruswami-Sudan list decoding for elliptic codes," in *Proc. the IEEE Information Theory Workshop (ITW)*, Visby, Sweden, Aug. 2019.
[11] H. O'Keeffe and P. Fitzpatrick, "Gröbner basis solutions of constrained interpolation problems," *Linear algebra app.*, vol. 351, pp. 533–551, 2002.
[12] J. S. R. Nielsen, "List decoding of algebraic codes," Ph.D. dissertation, Technical University of Denmark, 2013.
[13] K. Lee and M. O'Sullivan, "List decoding of Hermitian codes using Gröbner bases," *J. Symbolic Comput.*, vol. 44(12), pp. 1662–1675, Dec. 2009.
[14] M. Alekhnovich, "Linear diophantine equations over polynomials and soft decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2257–2265, 2005.
[15] P. Beelen and K. Brander, "Efficient list decoding of a class of algebraic-geometry codes," *Adv. Math. Commun.*, vol. 4, pp. 485–518, 2010.
[16] J. S. R. Nielsen and P. Beelen, "Sub-quadratic decoding of one-point Hermitian codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3225–3240, 2015.
[17] P. Giorgi, C. P. Jeannerod, and G. Villard, "On the complexity of polynomial matrix computations," in *Proc. ISSAC*, 2003, pp. 135–142.
[18] R. F. Lax, "Generic interpolation polynomial for list decoding," *Finite Fields Appl.*, vol. 18, no. 1, pp. 167–178, 2012.
[19] L. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2008.
[20] X. Wu and P. Siegel, "Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 47(6), pp. 2579–2587, Sep. 2001.