Algebraic Soft Decoding of Elliptic Codes

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

***Abstract*—This paper proposes algebraic soft decoding (ASD) for one-point elliptic codes, where the interpolation is realized through the perspective of obtaining a Gröbner basis. The desired interpolation polynomial $\mathcal{Q}(x, y, z)$ is the minimum candidate in the basis. This work shows how to obtain such a Gröbner basis. Based on an interpolation multiplicity matrix $\mathbf{M}$, an interpolation ideal $\mathcal{I}_{\mathbf{M}}$ can be defined. With a predefined decoding output list size (OLS) l ($l \geq \deg_z \mathcal{Q}$), an equivalent interpolation module $\mathcal{I}_{\mathbf{M},l}$ can be led to. By further defining the Lagrange interpolation functions, a basis of the interpolation module can be constructed. The desired Gröbner basis can be obtained by reducing this module basis. Finally, the decoding complexity is also analyzed.**

***Index Terms*—Algebraic soft decoding, basis reduction, elliptic codes, Gröbner basis, interpolation**

I. Introduction

Algebraic geometric (AG) codes were first introduced by Goppa [1]. They are linear block codes constructed based on an algebraic curve. The well known AG codes include Hermitian codes, elliptic codes, hyperelliptic codes, Klein quartic codes, and etc. The popular Reed-Solomon (RS) codes can also be seen as an AG code, since they are constructed based on a straight line. The length of an AG code is defined by the number of rational points on the curve. Since the number of rational points on a curve can exceed the size of finite field in which the curve is defined, the length of AG codes can exceed the field size so that they can correct more errors. However, their length advantage is exchanged by the genus penalty that pulls them away from being maximum distance separable (MDS). Among all algebraic curves, elliptic curves have a genus of one. Hence, elliptic codes are almost MDS codes, inheriting a good tradeoff between codeword length and distance property.

For an (n, k) AG code with length n and dimension k, its minimum Hamming distance d is lower bounded by the designed distance $d^* = n - k - g + 1$, where g is the genus of the curve. By constructing a polynomial that interpolates a set of points with a certain multiplicity, Guruswami and Sudan [2] proposed list decoding of RS and AG codes, namely, the GS decoding. For AG codes, it can correct up to $n - \lfloor \sqrt{n(n-d^*)} \rfloor - 1$ errors. The GS decoding consists of interpolation and root-finding. The former that determines the interpolation polynomial dominates the decoding complexity and it can be realized by Kötter's iterative polynomial construction [3]. Høholdt and Nielsen [4] presented a mathematical framework for GS decoding of Hermitian codes using Kötter's interpolation. Using soft received information and transforming them into the interpolation multiplicities, algebraic soft decoding (ASD) of Hermitian codes was proposed by Chen *et al.* [5]. GS decoding of elliptic codes using Kötter's interpolation was recently proposed by the authors [6].

Different from Kötter's interpolation, Lee and O'Sullivan proposed another interpolation approach for GS decoding of Hermitian codes from the perspective of Gröbner bases of modules [7]. The desired Gröbner basis can be obtained by first constructing the basis of the interpolation module, and then reducing the basis. The interpolation polynomial is the minimum candidate of the Gröbner basis. By generalizing the Alekhnovich basis reduction algorithm [8], Beelen and Brander further reduced the interpolation complexity for a class of AG codes [9]. Nielsen and Beelen also presented such interpolation technique for power decoding and GS decoding of Hermitian codes [10], in which the GJV basis reduction algorithm [11] was applied. ASD of Hermitian codes using this basis reduction (BR) interpolation technique was proposed by Lee and O'Sullivan [12]. GS decoding of elliptic codes using this BR interpolation technique was recently developed by the authors [13].

Based on Kötter-Vardy's soft decoding framework for RS codes [14], this paper proposes the ASD of elliptic codes using the BR interpolation technique. The soft received information is transformed into a multiplicity matrix $\mathbf{M}$, based on which an interpolation ideal $\mathcal{I}_{\mathbf{M}}$ can be defined. By characterizing the decoding output list size (OLS) l, module $\mathcal{I}_{\mathbf{M},l}$ can be further defined. It contains the trivariate polynomials that satisfy the prescribed interpolation constraints. In order to formulate the generators for the basis of $\mathcal{I}_{\mathbf{M},l}$, a sequence of submodules of the elliptic curve coordinate ring are defined. This formulation is further completed by defining the zero basis of each affine point and the Lagrange interpolation function over the elliptic function field. The module basis can be presented as a matrix in univariate polynomials. Row operation on the matrix further reduces it into the desired Gröbner basis. The interpolation polynomial $\mathcal{Q}(x, y, z)$ is the minimum candidate of the Gröbner basis. Besides formulating the above ASD for elliptic codes, this work also analyzes the BR interpolation complexity in the decoding. Our analysis shows that a higher rate code will exhibit a lower decoding complexity.

II. Elliptic Curves and Elliptic Codes

Let $\mathbb{F}_q = \{\sigma_0, \sigma_1, \ldots, \sigma_{q-1}\}$ denote the finite field of size q. An affine elliptic curve E over $\mathbb{F}_q$ is defined by a nonsingular

978-1-5386-8209-8/21/$31.00 ©2021 IEEE

Weierstrass equation as

$$E: Y^2 + \mathfrak{a}_1 XY + \mathfrak{a}_3 Y - X^3 - \mathfrak{a}_2 X^2 - \mathfrak{a}_4 X - \mathfrak{a}_6 = 0, \quad (1)$$

with $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4, \mathfrak{a}_6 \in \mathbb{F}_q$. On E, there exists a point of infinity P_∞. The points on the curve are called affine points, denoted as $P_j = (x_j, y_j)$. Let $E(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on E that have all coordinates in $\mathbb{F}_q$, i.e., $E(\mathbb{F}_q) = \{P_j\} \bigcup \{P_\infty\}$. The $\mathbb{F}_q$-rational points form an additive Abelian group based on the "chord-and-tangent" rule with P_∞ as the identity element [15]. Let δ denote the order of P_j, which is defined as the smallest nonnegative integer δ that satisfies $\delta P_j = P_\infty$. Let $-P_j$ denote the inverse of P_j. They are the only affine points on E with same x-coordinate, and hence can be denoted as $P_j = (x_j, y_j)$ and $-P_j = (x_j, y_j')$. Therefore, for E, we define the following coordinate sets

$$\mathbb{A} = \{x_j \mid P_j = (x_j, y_j), \forall j\}, \quad (2)$$

$$\mathbb{B}_j = \{y_j, y_j'\}. \quad (3)$$

Let $\mathbb{F}_q[X, Y]$ denote the bivariate polynomial rings defined over $\mathbb{F}_q$, and $< E >$ denote the ideal generated by E. The coordinate ring of E can be defined as

$$\mathcal{R} = \mathbb{F}_q[X, Y] / < E > . \quad (4)$$

$\mathcal{R}$ consists of functions in the form $\mathfrak{h}_0(x) + \mathfrak{h}_1(x)y$, where $\mathfrak{h}_0(x)$, $\mathfrak{h}_1(x) \in \mathbb{F}_q[x]$, where x and y are the residue classes of X and Y, respectively. The quotient field of $\mathcal{R}$ is called the elliptic function field, denoted as $\mathbb{F}_q(E)$.

Given $h \in \mathbb{F}_q(E)$, its order at a rational point P is denoted as $\mathrm{v}_P(h)$ [15]. There exists a function Λ that enables $\mathrm{v}_P(\Lambda) = 1$ and $h = \Lambda^{\mathrm{v}_P(h)} h'$, where $\mathrm{v}_P(h') = 0$. Λ is called a local parameter in P. If $\mathrm{v}_P(h) > 0$, h has a zero of order $\mathrm{v}_P(h)$ at P. Otherwise if $\mathrm{v}_P(h) < 0$, it has a pole of order $-\mathrm{v}_P(h)$ at P. For elliptic curves, $-\mathrm{v}_{P_\infty}(x) = 2$, $-\mathrm{v}_{P_\infty}(y) = 3$ and $-\mathrm{v}_{P_\infty}(x^\lambda y^\gamma) = 2\lambda + 3\gamma$.

***Definition** 1 ([15]):* Let n_P denote an integer that corresponds to P, $D = \sum_{P \in E(\mathbb{F}_q)} n_P [P]$ is a divisor of E. It has a degree of $\deg(D) = \sum_{P \in E(\mathbb{F}_q)} n_P$ and a sum of $\mathrm{sum}(D) = \sum_{P \in E(\mathbb{F}_q)} n_P P$.

***Definition** 2 ([15]):* If $h \in \mathbb{F}_q(E)$ and $h \neq 0$, the divisor of h is defined as $\mathrm{div}(h) = \sum_{P \in E(\mathbb{F}_q)} \mathrm{v}_P(h)[P]$. $\mathrm{div}(h)$ is also called the principal divisor of E.

Let $\mathfrak{L}(D)$ denote the Riemann-Roch space defined by the divisor D. For $\mathfrak{L}(u[P_\infty]) = \{h \in \mathbb{F}_q(E) | \mathrm{div}(h) + u[P_\infty] \succeq 0\} \bigcup \{0\}$, there exists a basis consisting of

$$\{\phi_0 = 1\} \cup \{\phi_a = x^\lambda y^\gamma \mid a = 2\lambda + 3\gamma - 1 < u, \lambda \in \mathbb{N}, \gamma \in \{0, 1\}\}, \quad (5)$$

where " $\succeq$ " indicates that the coefficients of $\mathrm{div}(h) + u[P_\infty]$ are nonnegative and $\mathbb{N}$ denotes the set of nonnegative integers. It can be seen that $-\mathrm{v}_{P_\infty}(\phi_a) < -\mathrm{v}_{P_\infty}(\phi_{a+1})$. Consequently, $\mathcal{R} = \bigcup_{u=0}^{\infty} \mathfrak{L}(u[P_\infty])$. If $h \in \mathcal{R}$, it can be written as $h = \sum \zeta_a \phi_a$, where $\zeta_a \in \mathbb{F}_q$, and $-\mathrm{v}_{P_\infty}(h) = \max\{-\mathrm{v}_{P_\infty}(\phi_a) \mid \zeta_a \neq 0\}$. Meanwhile, for each affine point P_j, there exists a zero basis

$$\{\psi_{P_j,b}(x, y) \mid b \in \mathbb{N}\} \quad (6)$$

of $\mathcal{R}$ that satisfies $\mathrm{v}_{P_j}(\psi_{P_j,b}) = b$. Therefore, each pole basis monomial ϕ_a can be written as

$$\phi_a = \sum_{b \in \mathbb{N}} \xi_{a,P_j,b} \psi_{P_j,b}, \quad (7)$$

where $\xi_{a,P_j,b} \in \mathbb{F}_q$ is the corresponding coefficient between ϕ_a and $\psi_{P_j,b}$ [4] [16].

Given a message vector $\underline{f} = (f_0, f_1, \ldots, f_{k-1}) \in \mathbb{F}_q^k$, it can be written as

$$f(x, y) = f_0\phi_0 + f_1\phi_1 + \cdots + f_{k-1}\phi_{k-1}, \quad (8)$$

where $f \in \mathfrak{L}(k[P_\infty])$. The encoding of an (n, k) elliptic code can be performed by

$$\begin{aligned} \underline{c} &= (f(P_0), f(P_1), \ldots, f(P_{n-1})) \\ &= (c_0, c_1, \ldots, c_{n-1}) \end{aligned} \quad (9)$$

where $\underline{c} \in \mathbb{F}_q^n$. Its minimum Hamming distance $d \geq n - k$.

Therefore, the number of affine points on curve E defines the length of the code. Over $\mathbb{F}_q$, there exists curve E on which the number of rational points can reach the Hasse-Weil bound [17], i.e., $|E(\mathbb{F}_q)| = q + \lfloor 2\sqrt{q} \rfloor$+1. It should be pointed that the use of the affine points an order of two will make the interpolation module basis construction cumbersome. Given an elliptic curve, there exist at most three such points. In this work, our code construction will be based on curves that reach the Hasse-Weil bound but do not contain affine points of order two. This can be realized by choosing the curve coefficients $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ and $\mathfrak{a}_6$, appropriately. Excluding P_∞ for encoding, the constructed elliptic codes have length $n = q + \lfloor 2\sqrt{q} \rfloor$.

III. Algebraic Soft Decoding

A. Reliability Transform

Assume that codeword $\underline{c}$ is transmitted through a discrete memoryless channel. Given a received symbol vector $\underline{r} = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{R}^n$, a reliability matrix $\mathbf{\Pi}$ of size $q \times n$ can be obtained. Its entry $\pi_{ij} = \Pr[c_j = \sigma_i \mid r_j]$ is the *a posteriori* probability. Note that it is assumed that $\Pr[c_j = \sigma_i] = \frac{1}{q}, \forall (i, j)$. Matrix $\mathbf{\Pi}$ will be transformed into a multiplicity matrix $\mathbf{M}$ of the same size [14]. Its entry m_{ij} represents the interpolation multiplicity for point (P_j, σ_i). Note that the $\mathbf{\Pi} \rightarrow \mathbf{M}$ transform can be parameterized by a predefined decoding OLS l, where $l \geq \deg_z \mathcal{Q}$ [5]. That says the transform that iteratively updates m_{ij} will terminate once the entries can sustain a decoding OLS of l, where the estimation of l based on $\mathbf{M}$ will be presented in Section III.C.

B. Interpolation Ideal

Let $\mathcal{R}[z]$ denote the polynomial ring over $\mathcal{R}$. For monomial $\phi_a z^b \in \mathcal{R}[z]$, its $(1, k)$-weighted degree is $\deg_{1,k} \phi_a z^b = -\mathrm{v}_{P_\infty}(\phi_a) + kb$. Given two distinct monomials $\phi_{a_1} z^{b_1}$ and $\phi_{a_2} z^{b_2}$, we can arrange them in the $(1, k)$-revlex order: $\mathrm{ord}(\phi_{a_1} z^{b_1}) < \mathrm{ord}(\phi_{a_2} z^{b_2})$, 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 $b_1 < b_2$. For a polynomial $Q = \sum_{a,b} Q_{ab}\phi_a z^b \in \mathcal{R}[z]$, its $(1,k)$-weighted degree and leading order can be defined as $\deg_{1,k} Q = \max\{\deg_{1,k}\phi_a z^b \mid Q_{ab} \neq 0\}$ and $\mathrm{lod}(Q) = \max\{\mathrm{ord}(\phi_a z^b) \mid Q_{ab} \neq 0\}$, respectively. Therefore, given two distinct polynomials $Q_1, Q_2 \in \mathcal{R}[z]$, we claim $Q_1 < Q_2$, if $\mathrm{lod}(Q_1) < \mathrm{lod}(Q_2)$.

Let $\mathrm{mult}_{(P_j,\sigma_i)}(Q)$ denote the interpolation multiplicity of Q at point (P_j, σ_i). Given matrix $\mathbf{M}$, the interpolation ideal $\mathcal{I}_{\mathbf{M}}$ is defined as

$$\mathcal{I}_{\mathbf{M}} = \{Q \in \mathcal{R}[z] \mid \mathrm{mult}_{(P_j,\sigma_i)}(Q) \geq m_{ij}, \forall m_{ij} \neq 0\}. \quad (10)$$

Interpolation finds the minimum polynomial $\mathcal{Q}$ over $\mathcal{I}_{\mathbf{M}}$ under the $(1,k)$-revlex order.

Let $i_j = \mathrm{index}\{\sigma_i \mid \sigma_i = c_j\}$, based on $\mathbf{M}$, the score of $\underline{c}$ is defined as

$$\mathrm{S}_{\mathrm{M}}(\underline{c}) = \sum_{j=0}^{n-1} m_{i_j j}.$$

The following Theorem shows a sufficient condition for a successful ASD.

***Theorem** 1:* Given an (n,k) elliptic code and a nonzero interpolation polynomial $\mathcal{Q} \in \mathcal{I}_{\mathbf{M}}$. If

$$\mathrm{S}_{\mathrm{M}}(\underline{c}) > \deg_{1,k} \mathcal{Q}, \quad (11)$$

then $\mathcal{Q}(x,y,f) = 0$, or equivalently $(z-f) \mid \mathcal{Q}$.

Proof: Since $\mathcal{Q} \in \mathcal{I}_{\mathbf{M}}$, for P_j, $\mathcal{Q}$ can be written as

$$\mathcal{Q} = \sum_{a+b_i \geq m_{ij}} h_a \prod_{i=0}^{q-1} (z-\sigma_i)^{b_i}, \quad (12)$$

where $h_a \in \mathcal{R}$ and $\mathrm{v}_{P_j}(h_a) \geq a$. Replacing z in (12) by f yields $\mathcal{Q}(x,y,f) = \sum_{a+b_i \geq m_{ij}} h_a \prod_{i=0}^{q-1}(f-\sigma_i)^{b_i}$. If $f(P_j) = \sigma_i$ for each P_j, then $\mathrm{v}_{P_j}(\mathcal{Q}(x,y,f)) \geq a + b_i \geq m_{ij}$. Therefore, $\mathcal{Q}(x,y,f)$ has at least $\mathrm{S}_{\mathrm{M}}(\underline{c})$ zeroes over the n affine points. Since $f \in \mathfrak{L}(k[P_\infty])$, i.e., $\deg_{1,k} f \leq k$, $\deg_{1,k} \mathcal{Q}(x,y,f) \leq \deg_{1,k} \mathcal{Q}(x,y,z)$. Based on (11),

$$\begin{aligned} &\textstyle\sum_{j=0}^{n-1} \mathrm{v}_{P_j}(\mathcal{Q}(x,y,f)) = \mathrm{S}_{\mathrm{M}}(\underline{c}) > \deg_{1,k} \mathcal{Q} \\ &\geq \deg_{1,k} \mathcal{Q}(x,y,f) = -\mathrm{v}_{P_\infty}(\mathcal{Q}(x,y,f)), \end{aligned}$$

i.e., $\mathcal{Q}(x,y,f)$ has a zero order that is greater than its pole order. As a result, $\mathcal{Q}(x,y,f) = 0$. ∎

C. Decoding OLS

Given a multiplicity matrix $\mathbf{M}$, let

$$\mathfrak{C}_{\mathbf{M}} = \sum_{i=0}^{q-1}\sum_{j=0}^{n-1} \binom{m_{ij}+1}{2} \quad (13)$$

denote its interpolation cost implied by the matrix. It is the number of interpolation constraints that $\mathcal{Q}$ should satisfy.

***Theorem** 2:* For an (n,k) elliptic code, given $\mathbf{M}$, its decoding OLS can be determined by

$$l = \left\lfloor \sqrt{\frac{2\mathfrak{C}_{\mathbf{M}}}{k} + \frac{1}{4}} - \frac{1}{2} \right\rfloor. \quad (14)$$

Proof: Given $\mathbf{M}$, the interpolation polynomial $\mathcal{Q}$ should contain at least the first $\mathfrak{C}_{\mathbf{M}} + 1$ monomials in $\mathcal{R}[z]$, so that the linear system will have a nonzero solution. Therefore,

$$l = \max\left\{l' \mid \mathrm{ord}(z^{l'}) \leq \mathfrak{C}_{\mathbf{M}}\right\}. \quad (15)$$

Note that $\mathrm{ord}(z^{l'}) = \mathrm{ord}(z^{l'-1}) + |\{\phi_a z^b \mid (l'-1)k < \deg_{1,k}(\phi_a z^b) \leq l'k\}|$. Since elliptic curves have a genus of one, in $\mathcal{R}$ there does not exist a monomial ϕ such that $-\mathrm{v}_{P_\infty}(\phi) = 1$. If $\mathcal{D} = (l'-1)k+1$, $|\{\phi_a z^b \mid \deg_{1,k}(\phi_a z^b) = \mathcal{D}\}| = l'-1$. If $(l'-1)k+1 < \mathcal{D} < l'k$, $|\{\phi_a z^b \mid \deg_{1,k}(\phi_a z^b) = \mathcal{D}\}| = l'$. Otherwise, $|\{\phi_a z^b \mid \deg_{1,k}(\phi_a z^b) = \mathcal{D}\}| = l'+1$. Therefore, $\mathrm{ord}(z^{l'}) = \mathrm{ord}(z^{l'-1}) + l'k = (1+2+\cdots+l')k = \frac{kl'(l'+1)}{2}$. Substituting it into (15), the conclusion will be led to. ∎

IV. The BR Based Interpolation

This section introduces how to construct the interpolation polynomial $\mathcal{Q}$ through module basis construction and its reduction, for which the following prerequisites are needed.

A. Prerequisites

Let $\mathcal{R}[z]_l = \{Q \in \mathcal{R}[z] \mid \deg_z Q \leq l\}$, which can be seen as a free module over $\mathbb{F}_q[x]$ with a rank of $2(l+1)$ and a free basis of $\{1, y, z, yz, \ldots, z^l, yz^l\}$. Let us define

$$\mathcal{I}_{\mathbf{M},l} = \mathcal{I}_{\mathbf{M}} \cap \mathcal{R}[z]_l$$

as a submodule of $\mathcal{R}[z]_l$.

Consider $\mathcal{I}_{\mathbf{M},l}$ as an $\mathbb{F}_q[x]$-module, the basis of $\mathcal{I}_{\mathbf{M},l}$ can be presented as a square matrix $\mathbf{V} \in \mathbb{F}_q[x]^{2(l+1)\times 2(l+1)}$. Let $\mathbf{V}_t$ and $\mathbf{V}_{t,s}$ denote the row-t and the row-t column-s entry of $\mathbf{V}$, respectively, the degree of $\mathbf{V}_t$ is defined as

$$\deg \mathbf{V}_t = \max\{\deg \mathbf{V}_{t,s} \mid 0 \leq s \leq 2l+1\}. \quad (16)$$

The leading position of $\mathbf{V}_t$ is

$$\mathrm{LP}(\mathbf{V}_t) = \max\{s \mid \deg \mathbf{V}_{t,s} = \deg \mathbf{V}_t\}. \quad (17)$$

Finally, the degree of $\mathbf{V}$ is defined as

$$\deg \mathbf{V} = \max\{\deg \mathbf{V}_t \mid 0 \leq t \leq 2l+1\}. \quad (18)$$

***Definition** 3 ([18]):* Given a square matrix $\mathbf{V}$ in $\mathbb{F}_q[x]$, it is in weak Popov form if and only if $\mathrm{LP}(\mathbf{V}_t) \neq \mathrm{LP}(\mathbf{V}_{t'}), \forall t \neq t'$.

The interpolation polynomial $\mathcal{Q}$ can be computed by first constructing a basis for $\mathcal{I}_{\mathbf{M},l}$. Presented as a matrix in $\mathbb{F}_q[x]$, it will then be reduced into weak Popov form, which indicates the desired Gröbner basis is reached. $\mathcal{Q}$ is the minimum candidate of the basis.

B. Module Basis Construction

In order to construct the basis for $\mathcal{I}_{\mathbf{M},l}$, the following interpolation point numeration is needed. Let $\mathcal{S}_j$ denote the multiset of interpolation points (P_j, σ_i)

$$\mathcal{S}_j = \{\underbrace{(P_j,\sigma_i),\ldots,(P_j,\sigma_i)}_{m_{ij}} \mid \forall i\}. \quad (19)$$

Its balanced list $\mathcal{S}'_j$ can be further generated by moving one of the most frequent elements in $\mathcal{S}_j$ to $\mathcal{S}'_j$, until $\mathcal{S}_j$ becomes empty. Let $\mathfrak{m}_j = \sum_{i=0}^{q-1} m_{ij}$, we have $|\mathcal{S}'_j| = |\mathcal{S}_j| = \mathfrak{m}_j$. Note that $\mathfrak{m}_j \leq l$. $\mathcal{S}'_j$ can be denoted as

$$\mathcal{S}'_j = \{(P_j, z_j^{(0)}), (P_j, z_j^{(1)}), \ldots, (P_j, z_j^{(\mathfrak{m}_j-1)})\}, \tag{20}$$

where $z_j^{(u)} \in \mathbb{F}_q$ and $0 \leq u \leq \mathfrak{m}_j - 1$. With all balance lists $\mathcal{S}'_0, \mathcal{S}'_1, \ldots, \mathcal{S}'_{n-1}$, let $\underline{z}^{(u)} = (z_0^{(u)}, z_1^{(u)}, \ldots, z_{n-1}^{(u)})$. Furthermore, $\mathcal{S}'_j$ can be partitioned into $\mathcal{S}_j^{(u)} = \{(P_j, z_j^{(0)}), \ldots, (P_j, z_j^{(u-1)})\}$ and $\overline{\mathcal{S}}_j^{(u)} = \{(P_j, z_j^{(u)}), \ldots, (P_j, z_j^{(\mathfrak{m}_j-1)})\}$. Note that in $\overline{\mathcal{S}}_j^{(u)}$, $(P_j, z_j^{(u)})$ is one of the most frequent elements. Moreover, since $\mathfrak{m}_j \leq l$, $\overline{\mathcal{S}}_j^{(u)} = \emptyset$ if $\mathfrak{m}_j \leq u \leq l$. Let $\mathfrak{m}_j^{(u)}$ denote the multiplicity of $(P_j, z_j^{(u)})$ in $\overline{\mathcal{S}}_j^{(u)}$, we can define

$$\mathcal{J}_u = \{h \in \mathcal{R} \mid \mathrm{v}_{P_j}(h) \geq \mathfrak{m}_j^{(u)}\} \tag{21}$$

as an $\mathbb{F}_q[x]$-submodule of $\mathcal{R}$. Since $\mathfrak{m}_j^{(u)} \geq \mathfrak{m}_j^{(u+1)}$, $\mathcal{J}_u \subseteq \mathcal{J}_{u+1}$.

Recall that over an elliptic curve E, $P_j = (\alpha, \beta)$ and $-P_j = (\alpha, \beta')$. Let us denote $P_{\alpha_0} = (\alpha, \beta)$ and $P_{\alpha_1} = (\alpha, \beta')$, and $\mu_{\alpha_v}^{(u)} = \mathfrak{m}_j^{(u)}$ for $P_{\alpha_v} = P_j$, where $v = 0, 1$. For each $\alpha \in \mathbb{A}$, we arrange the index v such that

$$\mu_{\alpha_0}^{(u)} \geq \mu_{\alpha_1}^{(u)}. \tag{22}$$

For $u = 0, 1, \ldots, l$, P_{α_0} can be different. For explicity, we denote P_{α_0} by $P_{\alpha_0}^{(u)}$. Therefore, $\mathcal{J}_u$ can be written as

$$\mathcal{J}_u = \{h \in \mathcal{R} \mid \mathrm{v}_{P_{\alpha_v}^{(u)}}(h) \geq \mu_{\alpha_v}^{(u)}\}. \tag{23}$$

Lemma 3: Given function $h(x, y) = \sum_{s=0}^{\rho} \mathfrak{h}_s(x) y^s \in \mathcal{J}_u$, $\prod_{\alpha \in \mathbb{A}} (x - \alpha)^{\mu_{\alpha_\rho}^{(u)}} | \mathfrak{h}_\rho(x)$.

Proof: When $\rho = 0$, for $P_{\alpha_0}^{(u)}$, there exists a local parameter $\Lambda = x - \alpha$ such that $\mathfrak{h}_0(x) = \Lambda^{\mu_{\alpha_0}^{(u)}} \mathfrak{h}'_0(x)$. Hence, $\prod_{\alpha \in \mathbb{A}} (x - \alpha)^{\mu_{\alpha_0}^{(u)}} | \mathfrak{h}_0(x)$. When $\rho = 1$, $h = \mathfrak{h}_0 + \mathfrak{h}_1 y$. For $P_{\alpha_1}^{(u)}$, assume that $(x - \alpha)^{\mu_{\alpha_1}^{(u)}} \nmid \mathfrak{h}_1$, then $h = (x - \alpha)^{\mu} h'$, where $\mu < \mu_{\alpha_1}^{(u)}$ and $(x - \alpha) \nmid h'$. Since $\mathrm{v}_{P_{\alpha_1}}(h) \geq \mu_{\alpha_1}^{(u)}$, $h'(P_{\alpha_1}^{(u)}) = 0$. Since $h'(P_{\alpha_0}^{(u)}) \neq h'(P_{\alpha_1}^{(u)})$, $\mathrm{v}_{P_{\alpha_0}^{(u)}}(h) = \mu < \mu_{\alpha_0}^{(u)}$. It contradicts $\mathrm{v}_{P_{\alpha_0}^{(u)}}(h) = \mu_{\alpha_0}^{(u)}$. ∎

Let $\mu_\alpha^{(u)} = \mu_{\alpha_0}^{(u)} - \mu_{\alpha_1}^{(u)}$, given $\mathcal{H}(x) \in \mathbb{F}_q[x]$, it satisfies

$$\mathrm{v}_{P_{\alpha_0}^{(u)}}(y - \mathcal{H}(x)) \geq \mu_\alpha^{(u)}, \ \forall \alpha \in \mathbb{A}. \tag{24}$$

Let

$$\nu^{(u)} = \sum_{\alpha \in \mathbb{A}} \mu_\alpha^{(u)} \tag{25}$$

and

$$\mathcal{H}(x) = \sum_{i=0}^{\nu^{(u)}-1} \zeta_i x^i, \tag{26}$$

where $\zeta_i \in \mathbb{F}_q$. Based on (7), we know for each P_j, $y = \sum_{b \in \mathbb{N}} \xi_{2,P_j,b} \psi_{P_j,b}$ and $\mathcal{H}(x) = \sum_{b \in \mathbb{N}} (\zeta_0 \xi_{0,P_j,b} + \sum_{i=1}^{\nu^{(u)}-1} \zeta_i \xi_{2i-1,P_j,b}) \psi_{P_j,b}$. Therefore, for $P_{\alpha_0}^{(u)}$, if $\zeta_0 \xi_{0,P_{\alpha_0}^{(u)},b} + \sum_{i=1}^{\nu^{(u)}-1} \zeta_i \xi_{2i-1,P_{\alpha_0}^{(u)},b} = \xi_{2,P_{\alpha_0}^{(u)},b}$ with $0 \leq b < \mu_\alpha^{(u)}$, $\mathcal{H}(x)$ satisfies the required condition of (24). The zero basis functions of each affine point can be generated based on Theorem 3 of [6]. The corresponding coefficients $\xi_{a,P_j,b}$ can be further determined. Consequently, $\mathcal{H}(x)$ can be obtained by solving the linear system

$$\underline{\zeta} \boldsymbol{\Xi} = \underline{\xi}, \tag{27}$$

where $\boldsymbol{\Xi}$ is a square matrix of size $\nu^{(u)}$, $\underline{\zeta} = (\zeta_0, \ldots, \zeta_{\nu^{(u)}-1})$ and $\underline{\xi} = (\xi_{2,P_{\alpha_0}^{(u)},0}, \xi_{2,P_{\alpha_0}^{(u)},1}, \ldots, \xi_{2,P_{\alpha_0}^{(u)},\mu_\alpha^{(u)}-1})$.

Theorem 4: $\mathcal{J}_u$ $(0 \leq u \leq l)$ can be generated as an $\mathbb{F}_q[x]$-module by

$$\mathcal{G}_0^{(u)}(x, y) = \prod_{\alpha \in \mathbb{A}} (x - \alpha)^{\mu_{\alpha_0}^{(u)}} \tag{28}$$

and

$$\mathcal{G}_1^{(u)}(x, y) = (y - \mathcal{H}(x)) \prod_{\alpha \in \mathbb{A}} (x - \alpha)^{\mu_{\alpha_1}^{(u)}}. \tag{29}$$

Proof: Note that $\mathcal{G}_0^{(u)}$, $\mathcal{G}_1^{(u)} \in \mathcal{J}_u$. Based on Lemma 3, for each $h = \mathfrak{h}_0 + \mathfrak{h}_1 y \in \mathcal{J}_u$, there exists $\mathfrak{h}'_1$ such that $h'(x) = h - \mathfrak{h}'_1 \mathcal{G}_1^{(u)} \in \mathcal{J}_u$. And there exists $\mathfrak{h}'_0$ such that $h' = \mathfrak{h}'_0 \mathcal{G}_0^{(u)}$. Therefore, $h = \mathfrak{h}'_1 \mathcal{G}_1^{(u)} + \mathfrak{h}'_0 \mathcal{G}_0^{(u)}$, i.e., $\mathcal{J}_u$ can be generated as an $\mathbb{F}_q[x]$-module by $\mathcal{G}_0^{(u)}$ and $\mathcal{G}_1^{(u)}$. ∎

Note that if $\mathfrak{m}_j^{(l)} = 0$, $\mathcal{G}_0^{(l)} = 1$ and $\mathcal{G}_1^{(l)} = y$. Given $Q \in \mathcal{R}[z]$, it can be written as $Q = \sum_{s \in \mathbb{N}} Q_{[s]} z^s$, where $Q_{[s]} \in \mathcal{R}$.

Lemma 5: Let $Q = \sum_{s=0}^{\varrho} Q_{[s]} z^s \in \mathcal{I}_{\mathbf{M},l}$, then $Q_{[\varrho]} \in \mathcal{J}_\varrho$.

Proof: For P_j, $Q = \sum_{a + b_i \geq m_{ij}} h_a \prod_{i=0}^{q-1} (z - \sigma_i)^{b_i}$, where $h_a \in \mathcal{R}$ and $\mathrm{v}_{P_j}(h_a) \geq a$. Therefore, $\mathrm{v}_{P_j}(h_a) \geq \max\{m_{ij} - b_i\}$. When $\varrho = 0$, $\mathrm{v}_{P_j}(h_a) \geq \max\{m_{ij}\}$ and $Q_{[0]} \in \mathcal{J}_0$. When $\varrho = 1$, i.e., $\sum_{i=0}^{q-1} b_i = 1$, let $b_0 = 1$, we have $\mathrm{v}_{P_j}(h_a) \geq \max\{m'_{ij} \mid m'_{0j} = m_{0j} - 1 \text{ and } m'_{ij} = m_{ij}, 1 \leq i \leq q-1\}$. Therefore, $Q_{[1]} \in \mathcal{J}_1$. Following the same deduction manner, the conclusion can be reached. ∎

To define a basis for $\mathcal{I}_{\mathbf{M},l}$, the following function is needed

$$\mathcal{K}_{\underline{z}^{(u)}}(x, y) = \sum_{j=0}^{n-1} z_j^{(u)} \mathcal{L}_j(x, y), \tag{30}$$

where

$$\mathcal{L}_j(x, y) = \prod_{\alpha \in \mathbb{A} \setminus \{x_j\}} \frac{x - \alpha}{x_j - \alpha} \prod_{\beta \in \mathbb{B}_j \setminus \{y_j\}} \frac{y - \beta}{y_j - \beta} \tag{31}$$

is the Lagrange interpolation function over $\mathbb{F}_q(E)$. Note that if $j = j'$, then $\mathcal{L}_j(P_{j'}) = 1$; otherwise, $\mathcal{L}_j(P_{j'}) = 0$. Hence, $\mathcal{K}_{\underline{z}^{(u)}}(P_j) = z_j^{(u)}$ for $0 \leq u < \mathfrak{m}_j$. Based on (28)-(30), the generators of $\mathcal{I}_{\mathbf{M},l}$ can be defined as follows.

Theorem 6: $\mathcal{I}_{\mathbf{M},l}$ can be generated as an $\mathbb{F}_q[x]$-module by

$$\begin{aligned} \mathcal{M} = \{M_t \mid M_t = \mathcal{G}_v^{(u)} \prod_{\epsilon=0}^{u-1} (z - \mathcal{K}_{\underline{z}^{(\epsilon)}}), \\ t = v + 2u, \ v = 0, 1 \text{ and } 0 \leq u \leq l\}. \end{aligned} \tag{32}$$

Proof: Based on Theorem 4, we have $\mathcal{G}_v^{(u)} \in \mathcal{J}_u$, i.e., $\mathrm{v}_{P_j}(\mathcal{G}_v^{(u)}) \geq \mathfrak{m}_j^{(u)}$. Let $m_{ij}^{(u)}$ denote the multiplicity

of (P_j, σ_i) in $\overline{\mathcal{S}}_j^{(u)}$. Therefore, $\mathrm{mult}_{(P_j,\sigma_i)}(\mathcal{G}_v^{(u)}) \geq m_{ij}^{(u)}$. Based on (20) and (29), $\mathrm{mult}_{(P_j,\sigma_i)}(\prod_{\epsilon=0}^{u-1}(z - \mathcal{K}_{\underline{\hat{z}}^{(\epsilon)}})) \geq m_{ij} - m_{ij}^{(u)}$. Therefore, $M_t \in \mathcal{I}_{\mathbf{M},l}$. Based on Lemma 5, for $Q = \sum_{s=0}^{l} Q_{[s]} z^s \in \mathcal{I}_{\mathbf{M},l}$, $Q_{[s]} \in \mathcal{J}_s$. Therefore, there exist $\mathfrak{h}_0^{(l)}$, $\mathfrak{h}_1^{(l)} \in \mathbb{F}_q[x]$ such that $Q_{[l]} = \mathfrak{h}_0^{(l)}\mathcal{G}_0^{(l)} + \mathfrak{h}_1^{(l)}\mathcal{G}_1^{(l)}$. It enables $Q^{(l-1)} = Q - (\mathfrak{h}_0^{(l)} M_{2l} + \mathfrak{h}_1^{(l)} M_{2l+1})$ with $\deg_z Q^{(l-1)} \leq l-1$ and $Q_{[l-1]}^{(l-1)} \in \mathcal{J}_{l-1}$. Again, there exist $\mathfrak{h}_0^{(l-1)}$, $\mathfrak{h}_1^{(l-1)} \in \mathbb{F}_q[x]$ such that $Q^{(l-2)} = Q^{(l-1)} - (\mathfrak{h}_0^{(l-1)} M_{2l-2} + \mathfrak{h}_1^{(l-1)} M_{2l-1})$ with $\deg_z Q^{(l-2)} \leq l-2$ and $Q_{[l-2]}^{(l-2)} \in \mathcal{J}_{l-2}$. Following the same deduction, there exist $\mathfrak{h}_0^{(1)}$, $\mathfrak{h}_1^{(1)} \in \mathbb{F}_q[x]$ which enable $Q^{(0)} = Q^{(1)} - (\mathfrak{h}_0^{(1)} M_2 + \mathfrak{h}_1^{(1)} M_3)$. Therefore, $Q^{(0)} \in \mathcal{J}_0$, i.e., there exist $\mathfrak{h}_0^{(0)}$, $\mathfrak{h}_1^{(0)} \in \mathbb{F}_q[x]$ such that $Q^{(0)} = \mathfrak{h}_0^{(0)} M_0 + \mathfrak{h}_1^{(0)} M_1$. Consequently, if $Q \in \mathcal{I}_{\mathbf{M},l}$, it can be expressed as an $\mathbb{F}_q[x]$-linear combination of M_t. ∎

It is obvious that for M_t, $\mathcal{G}_v^{(u)}$ and $\prod_{\epsilon=0}^{u-1}(z - \mathcal{K}_{\underline{\hat{z}}^{(\epsilon)}})$ interpolate all points of $\overline{\mathcal{S}}_j^{(u)}$ and $\mathcal{S}_j^{(u)}$, respectively.

C. Module Basis Reduction

Basis $\mathcal{M}$ will be further reduced, yielding the Gröbner basis $\mathcal{M}'$ that contains the interpolation polynomial $\mathcal{Q}$.

Note that $\mathcal{I}_{\mathbf{M},l}$ is an $\mathbb{F}_q[x]$ submodule of $\mathcal{R}[z]_l$. That says its polynomials Q can be written as $Q = Q^{(0)} + Q^{(1)}y + \cdots + Q^{(2l+1)}yz^l$, where $Q^{(0)}, Q^{(1)}, \ldots, Q^{(2l+1)} \in \mathbb{F}_q[x]$. They can also been written as $Q = (Q^{(0)}, Q^{(1)}, \ldots, Q^{(2l+1)})(1, y, \ldots, yz^l)^T$. Therefore, the basis polynomials M_t can also be written as $M_t = (M_t^{(0)}, M_t^{(1)}, \cdots, M_t^{(2l+1)})(1, y, \ldots, yz^l)^T$. Basis $\mathcal{M}$ can be presented as a matrix $\mathbf{V} \in \mathbb{F}_q[x]^{2(l+1)\times 2(l+1)}$ by letting

$$\mathbf{V}_t = (M_t^{(0)}, M_t^{(1)}, \ldots, M_t^{(2l+1)}), \tag{33}$$

where $\mathbf{V}_{t,s} = M_t^{(s)}(x)$. Inversely,

$$M_t = \mathbf{V}_t \cdot (1, y, \ldots, yz^l)^T. \tag{34}$$

The Mulders-Storjohann (MS) algorithm [18] can reduce $\mathbf{V}$ into weak Popov form. First, let us define the mapping $\Psi_{\underline{w}}$ [10]: $\mathbb{F}_q[x]^{2(l+1)} \to \mathbb{F}_q[x]^{2(l+1)}$

$$\mathbf{V}_t \mapsto \mathbf{V}_t^* = \mathbf{V}_t \cdot \mathrm{diag}(x^{\lfloor \frac{w_0}{2} \rfloor}, x^{\lfloor \frac{w_1}{2} \rfloor}, \ldots, x^{\lfloor \frac{w_{2l+1}}{2} \rfloor}), \tag{35}$$

where $\underline{w} = (w_0, w_1, \ldots, w_{2l+1})$ and $w_s = k\lfloor \frac{s}{2} \rfloor + 3(s \bmod 2)$. With the mapping, matrix $\mathbf{V}$ is transformed into

$$\mathbf{V}^* = \Psi_{\underline{w}}(\mathbf{V}) = (\Psi_{\underline{w}}(\mathbf{V}_0), \Psi_{\underline{w}}(\mathbf{V}_1), \ldots, \Psi_{\underline{w}}(\mathbf{V}_{2l+1}))^T, \tag{36}$$

where $\mathbf{V}_{t,s}^* = \mathbf{V}_{t,s} x^{\lfloor \frac{w_s}{2} \rfloor}$. Row operations will then be performed on $\mathbf{V}^*$ until it reaches weak Popov form $\mathbf{V}^{*\prime}$. The corresponding matrix $\mathbf{V}'$ can be obtained by $\Psi_{\underline{w}}^{-1}$ as

$$\mathbf{V}_t^{*\prime} \mapsto \mathbf{V}_t' = \mathbf{V}_t^{*\prime} \cdot \mathrm{diag}(x^{-\lfloor \frac{w_0}{2} \rfloor}, x^{-\lfloor \frac{w_1}{2} \rfloor}, \ldots, x^{-\lfloor \frac{w_{2l+1}}{2} \rfloor}). \tag{37}$$

The desired Gröbner basis $\mathcal{M}'$ can be further obtained as in (34), which contains the interpolation polynomial $\mathcal{Q}$.

Based on Theorem 1, message polynomial f can be further decoded by finding z-roots of $\mathcal{Q}$. It can be realized by the recursive coefficient search algorithm [19]. Summarizing the Section, the ASD algorithm that utilizes the BR interpolation can be presented as in Algorithm 1, where $\hat{f}$ denotes the estimation of f.

Algorithm 1 The ASD algorithm

Input: $\mathbf{\Pi}$ and l;
Output: $\hat{f}$;

1: Compute $\mathbf{M}$ that sustains l;
2: Create balanced lists $\mathcal{S}_j'$, as in (19) and (20);
3: Formulate the module basis $\mathcal{M}$ as in (32);
4: Map it into $\mathbf{V}^*$ as in (33) and (35);
5: Reduce $\mathbf{V}^*$ using the MS algorithm, yielding $\mathbf{V}^{*\prime}$;
6: Demap $\mathbf{V}^{*\prime}$ as in (37) and (34), yielding $\mathcal{M}'$;
7: Choose the minimum candidate of $\mathcal{M}'$ as $\mathcal{Q}$;
8: Determine the z-roots of $\mathcal{Q}$ to estimate $\hat{f}$.

V. Decoding Complexity

This section analyzes complexity of the BR interpolation for ASD of elliptic codes. We first consider the basis construction complexity. The computation of $\mathcal{H}(x)$ requires at most $O((\nu^{(u)})^3)$ finite field operations, where $\nu^{(u)}$ has been in (25). Based on Theorem 4, the complexity of computing $\mathcal{G}_v^{(u)}$ is $O(ln)$. Since $\deg_x \mathcal{G}_v^{(u)} < ln/2$ and $\deg_x \mathcal{K}_{\underline{\hat{z}}^{(u)}} < n/2$, based on Theorem 6, the complexity of the basis construction can be characterized as $O(l^2n^2)$.

For characterizing the basis reduction complexity, we should first define the orthogonality defect of matrix $\mathbf{V} \in \mathbb{F}_q[x]^{2(l+1)\times 2(l+1)}$ as

$$\Delta(\mathbf{V}) = \mathrm{rowdeg}\mathbf{V} - \deg\det\mathbf{V}, \tag{38}$$

where $\mathrm{rowdeg}\mathbf{V} = \sum_{t=0}^{2l+1} \deg \mathbf{V}_t$ and $\deg\det\mathbf{V}$ denotes the degree of the determinant of $\mathbf{V}$. The following Lemma shows the complexity of reducing $\mathbf{V}$ into weak Popov form.

Lemma 7 ([18]): Given a matrix $\mathbf{V} \in \mathbb{F}_q[x]^{2(l+1)\times 2(l+1)}$, the MS algorithm exhibits a complexity of $O((2l+2)^2 \deg\mathbf{V}\Delta(\mathbf{V}))$.

Therefore, for matrix $\mathbf{V}^*$ of Section IV.C, $\deg\mathbf{V}^* < ln/2$ and $\Delta(\mathbf{V}^*) < l^2(n-k)$. Reducing it into weak Popov form exhibits a complexity of $O(l^5n(n-k))$. The above analysis show that the interpolation will be more effective for high rate codes as they inherit a smaller basis reduction complexity. Furthermore, based on [19], the root-finding step has a complexity of $O(l^2n^2)$.

Acknowledgement

This work is sponsored by the National Natural Science Foundation of China (NSFC) with project IDs 62071498 and 61972429, and the Guangdong Major Project of Basic and Applied Basic Research with project ID 2019B030302008.

References

[1] V. Goppa, "Codes on algebraic curves," *Soviet Math. Doklady*, vol. 24, no. 1, pp. 170–172, 1981.

[2] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1757–1767, Sep. 1999.
[3] R. Kötter, "On algebraic decoding of algebraic-geometric and cyclic codes," Ph.D. dissertation, Linköping Univ., Linköping, Sweden, 1996.
[4] 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.
[5] L. Chen, R. Carrasco, and M. Johnston, "Soft-decision list decoding of Hermitian codes," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2169–2176, Aug. 2009.
[6] Y. Wan, L. Chen, and F. Zhang, "Design of Guruswami-Sudan list decoding for elliptic codes," in *Proc. IEEE Inf. Theory Workshop*, Visby, Sweden, Aug. 2019, pp. 1–5.
[7] K. Lee and M. O'Sullivan, "List decoding of Hermitian codes using Gröbner bases," *J. Symb. Comput.*, vol. 44, no. 12, pp. 1662–1675, Dec. 2009.
[8] 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.
[9] P. Beelen and K. Brander, "Efficient list decoding of a class of algebraic-geometry codes," *Adv. Math. Commun.*, vol. 4, pp. 485–518, 2010.
[10] 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.
[11] P. Giorgi, C. P. Jeannerod, and G. Villard, "On the complexity of polynomial matrix computations," in *Proc. ISSAC*, 2003, pp. 135–142.
[12] K. Lee and M. O'Sullivan, "Algebraic soft-decision decoding of Hermitian codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2587–2600, Jun. 2010.
[13] Y. Wan, L. Chen, and F. Zhang, "Algebraic list decoding of elliptic codes through module basis reduction," in *Proc. Int. Symp. Inf. Theory Applications*, Kapolei, Hawai'i, USA, Oct. 2020.
[14] R. Kötter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.
[15] L. Washington, *Elliptic Curves: Number Theory and Cryptography*. CRC press, 2008.
[16] L. Chen, "Design of an efficient list decoding system for Reed-Solomon and algebraic-geometric codes," Ph.D. dissertation, Dept. Electron. Comput. Eng., Newcastle Univ., Newcastle-upon-Tyne, U.K., 2008.
[17] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 2009.
[18] T. Mulders and A. Storjohann, "On lattice reduction for polynomial matrices," *J. Symb. Comput.*, vol. 35, no. 4, pp. 377–401, 2003.
[19] X. Wu and P. Siegel, "Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2579–2587, Sep. 2001.