Transactions Letters

Soft-Decision List Decoding of Hermitian Codes

Li Chen, *Member, IEEE,* Rolando Carrasco, and Martin Johnston

***Abstract*—This paper proposes the first complete soft-decision list decoding algorithm for Hermitian codes based on the Koetter-Vardy's Reed-Solomon code decoding algorithm. For Hermitian codes, interpolation processes trivariate polynomials which are defined over the pole basis of a Hermitian curve. In this paper, the interpolated zero condition of a trivariate polynomial with respect to a multiplicity matrix M is redefined followed by a proof of the validity of the soft-decision scheme. This paper also introduces a new stopping criterion for the algorithm that tranforms the reliability matrix Π to the multiplicity matrix M. Geometric characterisation of the trivariate monomial decoding region is investigated, resulting in an asymptotic optimal performance bound for the soft-decision decoder. By defining the weighted degree upper bound of the interpolated polynomial, two complexity reducing modifications are introduced for the soft-decision scheme: elimination of unnecessary interpolated polynomials and pre-calculation of the coefficients that relate the pole basis monomials to the zero basis functions of a Hermitian curve. Our simulation results and analyses show that soft-decision list decoding of Hermitian code can outperform Koetter-Vardy decoding of Reed-Solomon code which is defined in a larger finite field, but with less decoding complexity.**

***Index Terms*—List decoding, soft-decision, Algebraic-geometric codes, Hermitian codes.**

I. Introduction

REED-Solomon (RS) codes [1] is a well-known error-correction coding scheme with a wide range of applications, such as wireless communications and storage devices. However, the length of a RS code can not exceed the size of the Galois field (GF) in which it is defined, limiting the error-correction capability of the code. This limitation does not apply to algebraic-geometric (AG) codes [2]. Therefore, long codes can be generated from a smaller field reducing Galois field arithmetic operations. Among AG codes, it is shown in [3, 4] that Hermitian codes [5] can achieve significant coding gains over RS codes by using both the unique decoding algorithm [6-8] and the hard-decision list decoding algorithm [9, 10]. This motivates the author to further develop a soft-decision list decoding algorithm for the Hermitian codes.

For a (n, k) RS code with length n and dimension k, its minimum Hamming distance is $d = n-k+1$. Guruswami and Sudan [9, 10] proposed a hard-decision list decoding algorithm with error-correction bound $\tau_{GS} = n - \sqrt{n(n-d)} - 1$, exceeding the conventional unique decoding bound $\lfloor \frac{d-1}{2} \rfloor$. However, it is realised that achieving bound τ_{GS} demands a high decoding complexity [11]. Koetter and Vardy [12] proposed a soft-decision list decoding scheme for the RS codes, showing significant improvement can be achieved beyond the bound τ_{GS}, but with moderate decoding complexity.

For a (n, k) Hermitian code, its designed minimum distance is defined as: $d^* = n-k-g+1$, where g is the genus [13] of the Hermitian curve. For the conventional unique decoding algorithm using the Sakata's algorithm [6, 7] with majority voting [8], its error-correction capability is bounded by $\lfloor \frac{d^*-1}{2} \rfloor$. Hoholdt and Nielsen [14, 15] later developed a mathematical framework of applying the Guruswami and Sudan hard-decision decoding scheme to Hermitian codes, extending the error-correction bound to $\tau_{GS} = n - \sqrt{n(n-d^*)} - 1$. The first list decoding results of Hermitian codes was published by the authors in [16], showing significant coding gains can be achieved over the unique decoding algorithm. Through some later developments, the authors have presented complexity reducing modifications [17] for the computationally expensive interpolation process, including the elimination of any unnecessary polynomials [11] and the pre-calculation of the corresponding coefficients that relate a Hermitian curve's pole basis monomials to its zero basis functions.

This paper presents the first complete soft-decision list decoding algorithm for Hermitian codes. Based on Koetter-Vardy's soft-decision scheme for RS codes, one of the challenges in developing a soft-decision list decoding scheme for Hermitian codes is the extension of the interpolation from processing bivariate polynomials to trivariate polynomials which are defined over the pole basis of a Hermitian curve. This paper defines the interpolated zero condition of a trivariate polynomial and proposes a theorem to prove the validity of the soft-decision scheme. Modification is introduced to the reliability transform algorithm with introducing a new stopping criterion. By geometrically characterising the trivariate monomial decoding region, the authors derive the asymptotic optimal performance bound for the proposed algorithm. For efficient implementation of the interpolation process, the two important complexity reducing modifications [17] need to be applied. This paper presents how to integrate these two modificatioin schemes with the soft-decision algorithm for Hermitian codes. Performance analysis and complexity discussion for the soft-decision scheme are presented. It is shown that the soft-decision scheme can achieve significant improvement over the hard-decision scheme with less decoding complexity. Comparisons with the Koetter-Vardy decoding of RS codes are investigated. Our comparisons show that soft-decision list decoding of Hermitian codes can outperform

Paper approved by T.-K. Truong, the Editor for Coding Theory and Techniques of the IEEE Communications Society. Manuscript received July 2, 2007; revised September 26, 2008.

The authors are with the School of Electrical, Electronic and Computer Engineering, Newcastle University, Newcastle-upon-Tyne, United Kingdom, NE1 7RU (e-mail: {li.chen, r.carrasco, martin.johnston}@ncl.ac.uk).

Digital Object Identifier 10.1109/TCOMM.2009.08.070302

the RS codes defined in the same finite field with higher decoding complexity. Moreover, it can also outperform the RS codes defined in a larger finite field, but with *less* decoding complexity.

The rest of the paper is organised as the follows: Section II presents the background knowledge of this paper; Section III presents the soft-decision list decoding algorithm; Section IV presents the reduced complexity interpolation process; Section V presents the proposed algorithm's performance analysis and a discussion on complexity; finally, a conclusion of the paper is given in Section VI.

II. Background Knowledge

This section presents the background knowledge of the paper, including the hard-decision list decoding of Hermitian codes and Koetter-Vardy's soft-decision list decoder.

A. Hard-Decision List Decoding of Hermitian Codes

A Hermitian curve defined in Galois field with size q (GF(q)) can be generally written as:

$$H_w(x,y,z) = x^{w+1} + y^w z + y z^w, \tag{1}$$

where $w = \sqrt{q}$ and its genus $g = \dfrac{w(w-1)}{2}$ [5]. Based on an affine component $H_w(x,y,1)$, there are $n = w^3$ affine points $p_i = (x_i, y_i)$ and a point of infinity p_∞ [17]. Pole basis L_w of the curve contains a set of bivariate monomials $\phi_a(x,y)$ with increasing pole order at p_∞ as: $v_{p_\infty}(\phi_a^{-1}) < v_{p_\infty}(\phi_{a+1}^{-1})$ and $v_{p_\infty}(\phi_a^{-1}) = a+g$ given $a \geq g$, where $a \in N$. For each affine point p_i, there also exists a set of bivariate polynomials $\psi_{p_i,\alpha}(x,y)$ with increasing zero order at p_i as: $\psi_{p_i,\alpha} < \psi_{p_i,\alpha+1}$ and $v_{p_i}(\psi_{p_i,\alpha}) = \alpha$, where $\alpha \in N$ [15, 17]. By choosing the first k monomials in L_w, the message polynomial $f(x,y)$ of a (n,k) Hermitian code can be written as:

$$f(x,y) = f_0\phi_0 + f_1\phi_1 + \cdots + f_{k-1}\phi_{k-1}, \tag{2}$$

where $f_0, f_1, ..., f_{k-1} \in$ GF(q) are the message symbols. The code word is generated by:

$$\overline{c}(n,k) = (c_0, c_1, ..., c_{n-1}) = (f(p_0), f(p_1), ..., f(p_{n-1})), \tag{3}$$

and $c_0, c_1, ..., c_{n-1} \in$ GF(q) are the code word symbols.

Definition 1: For the list decoding of a (n,k) Hermitian code, by defining the weighted degree of variable z as: $w_z = v_{p_\infty}(\phi_{k-1}^{-1})$, the pole order of a trivariate monomial $\phi_a z^b (a, b \in N)$ can be interpreted as its $(1, w_z)$-weighted degree as:

$$deg_{1,w_z}(\phi_a z^b) = v_{p_\infty}(\phi_a^{-1}) + w_z b. \tag{4}$$

A $(1, w_z)$-lexicographic order (ord) can be assigned to monomials $\phi_a z^b$ as: $\phi_{a_1} z^{b_1} < \phi_{a_2} z^{b_2}$, if $deg_{1,w_z}(\phi_{a_1} z^{b_1}) < deg_{1,w_z}(\phi_{a_2} z^{b_2})$, or $deg_{1,w_z}(\phi_{a_1} z^{b_1}) = deg_{1,w_z}(\phi_{a_2} z^{b_2})$ and $b_1 < b_2$. Let $F_q[x,y,z]$ denotes the ring of polynomials defined over GF(q), generally written as: $Q = \sum_{a,b \in N} Q_{ab}\phi_a z^b$ and $Q_{ab} \in$ GF(q). For a polynomial $Q \in F_q[x,y,z]$, if $\phi_{a'} z^{b'}$ ($Q_{a'b'} \neq 0$) is the maximal monomial, polynomial Q's $(1, w_z)$-weighted degree (or equivalently, pole order) and leading order (lod) are defined as:

$$deg_{1,w_z}(Q) = deg_{1,w_z}(\phi_{a'} z^{b'}), lod(Q) = ord(\phi_{a'} z^{b'}). \tag{5}$$

Given the hard-decision received word as: $\overline{R} = (r_0, r_1, ..., r_{n-1})$ and $r_i \in$ GF(q), n interpolated units can be formed by combining them with the corresponding affine points used in the encoding as: $(p_0, r_0), (p_1, r_1), ..., (p_{n-1}, r_{n-1})$. The first step of hard-decision list decoding is to build the minimal polynomial $Q \in F_q[x,y,z]$ which interpolates the n units with a zero of multiplicity $m (m > 0)$, called the *interpolation*. As a result, polynomial Q's coefficients Q_{ab} shall satisfy [15, 17]:

$$\sum_{a,b \geq \beta} Q_{ab} \binom{b}{\beta} \gamma_{a,p_i,\alpha} r_i^{b-\beta} = 0, for\ \alpha + \beta < m, \quad \alpha, \beta \in N\ and\ i = 0, 1, ..., n-1, \tag{6}$$

where $\gamma_{a,p_i,\alpha} \in$ GF(q) are the corresponding coefficients between the pole basis monomial ϕ_a and the zero basis functions $\psi_{p_i,\alpha}$, satisfying [15, 17]:

$$\phi_a = \sum_\alpha \gamma_{a,p_i,\alpha} \psi_{p_i,\alpha}. \tag{7}$$

For efficient interpolation, coefficients $\gamma_{a,p_i,\alpha}$ need to be determined prior to the interpolation process [17].

Lemma 1: If $Q \in F_q[x,y,z]$ has a zero of multiplicity at least m over unit (p,ρ) (p is an affine point and $\rho \in$ GF(q)), and there exists a polynomial h in the form of equation (2) such that $h(p) = \rho$, then $Q(x,y,h)$ has a zero order $v_p(Q(x,y,h)) \geq m$ at affine point p, or alternatively $\psi_{p,m} | Q(x,y,h)$ [14].

Based on Lemma 1, if there are $\Lambda (\Lambda \leq n)$ affine points that satisfy $h(p_i) = r_i$, then the total zero order of polynomial $Q(x,y,h)$ over all the affine points is: $\sum_{i=0}^{n-1}(Q(x,y,h)) \geq m\Lambda$. Hence, if $\sum_{i=0}^{n-1}(Q(x,y,h)) > deg_{1,w_z}(Q(x,y,h))$, $Q(x,y,h) = 0$ or $(z-h) | Q(x,y,z)$ since a nonzero polynomial's zero order cannot exceed its pole order. The second step of the decoding process is to find the z roots of polynomial Q such that they are the output candidates of the message polynomial f, which is called the *factorisation* [4, 18, 19].

B. Koetter-Vardy's Soft-Decision Scheme

Koetter-Vardy's soft-decision scheme obtains a reliability matrix Π instead of a hard-decision received word $\overline{R}$. Matrix Π contains each received symbol's posteriori transition probability with respect to each Galois field element $\rho_i (i = 0, 1, ..., q-1)$ and $\rho_i \in$ GF(q). The reliability matrix Π is further converted into a multiplicity matrix M with which a set of interpolation points and the associated multiplicities are indicated [12]. In the hard-decision scheme, a polynomial's zero order is increased by increasing the multiplicity value. However, the decoding complexity is increased exponentially. Alternatively, in the soft-decision scheme, a polynomial's zero order is increased by increasing the number of interpolation

points each of which is assigned with a rational multiplicity value. In order to extend this soft-decision scheme to Hermitian codes, two parameters $N_{1,k-1}(\delta)$ and $\Delta_{1,k-1}(v)$ defined in [12] for analysing bivariate polynomials $Q = \sum_{a,b\in N} Q_{ab}x^a y^b$ and $Q_{ab} \in$ GF(q) need to be redefined for analysing the trivariate polynomials of $F_q[x, y, z]$.

Definition 2: $N_{1,w_z}(\delta)$ denotes the number of trivariate monomials $\phi_a z^b$ with $(1, w_z)$-weighted degree not greater than the nonnegative integer δ, which is defined as:

$$N_{1,w_z}(\delta) = |\{\phi_a z^b : deg_{1,w_z}(\phi_a z^b) \le \delta, (a, b, \delta) \in N\}|. \tag{8}$$

$\Delta_{1,w_z}(v)$ denotes the minimal value of δ that guarantees $N_{1,w_z}(\delta)$ is greater than a nonnegative integer v, which is defined as:

$$\Delta_{1,w_z}(v) = \min\{\delta : N_{1,w_z}(\delta) > v, v \in N\}. \tag{9}$$

III. Soft-Decision List Decoding of Hermitian Codes

This section presents the soft-decision list decoding algorithm for Hermitian codes. It briefly describes the reliability and multiplicity matrices. The solution of the soft-decision scheme will then be proven. Based on that, the modified reliability transform algorithm will be proposed. Finally, the asymptotically optimal performance bound of this scheme will be analysed.

A. Reliability Matrix and Multiplicity Matrix

Let χ and $\Re$ denote the transmitted and received alphabets as $(\chi, \Re) \in$ GF(q). Given that χ is uniformly distributed over GF(q), entry $\pi_{i,j}$ of the reliability matrix Π is defined as [12]:

$$\pi_{i,j} = \Pr(\chi = \rho_i \mid \Re = r_j) = \frac{p(r_j \mid \rho_i)}{\sum_{\rho\in GF(q)} p(r_j \mid \rho)}, \tag{10}$$

where $i = 0, 1, ..., q-1, j = 0, 1, ..., n-1$ and $n = q^{3/2}$. $'\Pr'$ indicates the probability function and $p(\cdot \mid \rho)$ denotes the probability-density function if the channel is continuous or the probability-mass function if the channel is discrete. Entry $\pi_{i,j}$ indicates the probability of the transmitted symbol r_j being ρ_i, given the received symbol r_j. The difference between the soft-decision decoding of RS codes and Hermitian codes is in the size of the matrix Π. If both codes are defined in GF(q), it result a matrix Π with size $q \times (q-1)$ for the RS code and size $q \times q^{3/2}$ for the Hermitian code. In each column of matrix Π, the entry with the highest reliability value indicates the hard-decision received symbol. Let i_j denotes the index of the maximal entry in column j as:

$$i_j = index(\max\{\pi_{i,j} | i = 0, 1, ..., q-1\}). \tag{11}$$

The hard-decision received word $\overline{R}$ can be determined as: $\overline{R} = (r_0, r_1, ..., r_{n-1}) = (\rho_{i_0}, \rho_{i_1}, ..., \rho_{i_{n-1}})$. Based on Π, algorithm A of [12] is performed to proportionally transform the reliability matrix into multiplicity matrix M which also has size of $q \times q^{3/2}$. The entry $m_{i,j}$ of M indicates the multiplicity value for the unit (p_j, ρ_i). This transform will stop once a desired value of the total multiplicities s is reached, where $s = \sum_{i=0,j=0}^{q-1,n-1} m_{i,j}$ and $m_{i,j} \in M$. However, the performance of a list decoder is determined by its output list size. One might not achieve a performance gain by only increasing s without increasing the output list size. A modified reliability transform algorithm that is based on a designed output list size will be proposed in Section III C.

B. System Solution

For polynomial $Q = \sum_{a,b\in N} Q_{ab}\phi_a z^b$, to have a zero of multiplicity $m_{i,j}$ at the unit (p_j, ρ_i), it could be written with respect to affine point p_j's zero basis functions $\psi_{p_j,\alpha}$ as $Q = \sum_{\alpha,\beta\in N} Q_{\alpha\beta}^{(p_j,\rho_i)} \psi_{p_j,\alpha}(z - \rho_i)^\beta$ and with coefficients $Q_{\alpha\beta}^{(p_j,\rho_i)} = 0$ for $\alpha + \beta < m_{i,j}$ [17]. Based on equation (7) and $z^b = \sum_{\beta\le b} \binom{b}{\beta} \rho_i^{b-\beta}(z - \rho_i)^\beta$, $Q = \sum_{a,b\in N} Q_{ab}(\sum_\alpha \gamma_{a,p_j,\alpha}\psi_{p_j,\alpha})(\sum_{\beta\le b} \binom{b}{\beta}\rho_i^{b-\beta}(z-\rho_i)^\beta)$ and coefficients $Q_{\alpha\beta}^{(p_j,\rho_i)}$ could be derived as:

$$Q_{\alpha\beta}^{(p_j,\rho_i)} = \sum_{a,b\ge\beta} Q_{ab}\binom{b}{\beta}\gamma_{a,p_j,\alpha}\rho_i^{b-\beta}. \tag{12}$$

Regards to multiplicity matrix M, the interpolated polynomial Q's coefficients Q_{ab} should satisfy:

$$\sum_{a,b\ge\beta} Q_{ab}\binom{b}{\beta}\gamma_{a,p_j,\alpha}\rho_i^{b-\beta} = 0, \ for\ \alpha + \beta < m_{i,j},$$
$$\alpha, \beta \in N, \ i = 0, 1, ..., q-1 \ and \ j = 0, 1, ..., n-1. \tag{13}$$

By acknowledging the transmitted code word $(c_0, c_1, ..., c_{n-1})$, in each column of matrix M, the entry that corresponds the unit (p_j, c_j) is denoted as:

$$\widehat{m}_{i,j} = \{m_{i,j} | \rho_i = c_j, i = 0, 1, ..., q-1\}. \tag{14}$$

Selecting the n entries in M as: $\widehat{m}_{i,0}, \widehat{m}_{i,1}, \ldots, \widehat{m}_{i,n-1}$, the code word score $S_M(\overline{c})$ can be defined as:

$$S_M(\overline{c}) = \sum_{j=0}^{n-1} \widehat{m}_{i,j}. \tag{15}$$

It results in the following theorem for the soft-decision list decoding of Hermitian codes.

Theorem 2: Given the multiplicity matrix M and the resulting interpolated polynomial $Q(x, y, z)$, if the code word score $S_M(\overline{c})$ is large enough such that:

$$S_M(\overline{c}) > deg_{1,w_z}(Q), \tag{16}$$

the message polynomial f can be found by factorising Q as: $(z - f)|Q(x, y, z)$ or $Q(x, y, f) = 0$.

Proof: The interpolated polynomial Q passes unit (p_j, c_j) with multiplicity $\widehat{m}_{i,j}$. Based on Lemma 1, if f is the message polynomial such that $f(p_j) = c_j$ for $j = 0, 1, \ldots, n-1$, the polynomial $Q(x, y, f)$ should satisfy:

$$\psi_{p_0,\widehat{m}_{i,0}} \cdot \psi_{p_1,\widehat{m}_{i,1}} \cdots \psi_{p_{n-1},\widehat{m}_{i,n-1}} | Q(x, y, f). \tag{17}$$

Let $\widehat{\psi}(x, y) = \psi_{p_0,\widehat{m}_{i,0}} \cdot \psi_{p_1,\widehat{m}_{i,1}} \cdots \psi_{p_{n-1},\widehat{m}_{i,n-1}}$, the total zero order of $\widehat{\psi}(x, y)$ over all the affine points is:

$$\sum_{j=0}^{n-1} v_{p_j}(\widehat{\psi}(x,y)) = \widehat{m}_{i,0} + \widehat{m}_{i,1} + \cdots + \widehat{m}_{i,n-1} = S_M(\overline{c}). \tag{18}$$

Based on (17), since $\widehat{\psi}(x,y)|Q(x,y,f)$, the total zero order of polynomial $Q(x,y,f)$ over all the affine points shall be greater than or equal to $S_M(\overline{c})$:

$$\sum_{j=0}^{n-1} v_{p_j}(Q(x,y,f)) \geq S_M(\overline{c}). \tag{19}$$

Therefore, if $S_M(\overline{c}) > deg_{1,w_z}(Q(x,y,f))$, $\sum_{j=0}^{n-1} v_{p_j}(Q(x,y,f)) > deg_{1,w_z}(Q(x,y,f))$. Since polynomial $Q(x,y,f)$'s total zero order is greater than its pole order, then $Q(x,y,f)=0$ or equivalently $(z-f)|Q(x,y,z)$.

As there are $\frac{1}{2}m_{i,j}(m_{i,j}+1)$ permutations of nonnegative integers (α,β) with $\alpha+\beta < m_{i,j}$, equation (13) indicates the total constraints to coefficients Q_{ab} imposed by the matrix M is:

$$C_M = \frac{1}{2}\sum_{i=0}^{q-1}\sum_{j=0}^{n-1} m_{i,j}(m_{i,j}+1), \tag{20}$$

which is defined as the cost of matrix M. The interpolation process generates a system of C_M linear constraints. If the $(1,w_z)$-weighted degree of the interpolated polynomial Q is δ^*, according to Definition 2, Q has at most $N_{1,w_z}(\delta^*)$ nonzero coefficients. The system will be solvable if:

$$N_{1,w_z}(\delta^*) > C_M. \tag{21}$$

According to equation (9), in order to guarantee the solution, the $(1,w_z)$-weighted degree δ^* of the interpolated polynomial should be large enough, such that:

$$deg_{1,w_z}(Q(x,y,z)) = \delta^* = \Delta_{1,w_z}(C_M). \tag{22}$$

It results in the following corollary of Theorem 2 as:

Corollary 3: Message polynomial f can be found out by $(z-f)|Q(x,y,z)$, if

$$S_M(\overline{c}) > \Delta_{1,w_z}(C_M). \tag{23}$$

Since both the code word score $S_M(\overline{c})$ and expected weighted degree $\Delta_{1,w_z}(C_M)$ are parameters of matrix M, Corollary 3 links the soft-decision system's solution with the multiplicity matrix.

C. Modified Reliability Transform Algorithm

Since the factorisation outputs are the z roots of the interpolated polynomial, the output list size l_M should not exceed the interpolated polynomial's z degree $(deg_z Q)$ which could be defined as:

$$l_M = deg_z(Q(x,y,z)) = \lfloor \frac{deg_{1,w_z}(Q(x,y,z))}{w_z} \rfloor. \tag{24}$$

Based on equation (22), $deg_{1,w_z}(Q(x,y,z)) = \Delta_{1,w_z}(C_M)$. Therefore, the actual factorisation output list size can be determined by matrix M. This introduces a new stopping criterion for the reliability transform algorithm – algorithm A of [12]. The iterative transform algorithm will stop once the actual output size l_M exceeds a designed output size l. To determine $\Delta_{1,w_z}(C_M)$, the following corollary is proposed.

Corollary 4: $\Delta_{1,w_z}(v) = deg_{1,w_z}(\phi_a z^b | ord(\phi_a z^b) = v)$.

Proof: Based on Definition 1, the monomial order grows based on the growth of its $(1,w_z)$-weighted degree. Therefore, the weighted degree of monomial $\phi_a z^b$ with lexicographic order v is the minimum value that guarantees there are more than v monomials.

Therefore, given the multiplicity matrix M, the actual number of factorisation output list l_M is:

$$l_M = \lfloor \frac{deg_{1,w_z}(\phi_a z^b | ord(\phi_a z^b) = C_M)}{w_z} \rfloor. \tag{25}$$

After performing each iteration of algorithm A [12], the updated matrix M's cost C_M is calculated by equation (20). Then, the actual output list size l_M is determined by equation (25). The algorithm will stop once the l_M exceeds the designed value l.

D. Asymptotic Optimal Performance Bound

By increasing the output list size l_M, the list decoder is more likely to find a correct code word. Asymptotically, the optimal performance of a list decoding algorithm can be achieved when $l_M \to \infty$. It is easy to recognise that with $l_M \to \infty$, $C_M \to \infty$. For the asymptotic analysis, the inequality of Corollary 3 is applied with $C_M \to \infty$. Assisting this analysis, the following corollary is proposed for characterising the decoding region of the trivariate monomials $\phi_a z^b$.

Corollary 5: $N_{1,w_z}(\delta) > \frac{\delta(\delta-g)}{2w_z}$ given $\delta > 2g-1$, and $\lim_{\delta\to\infty} N_{1,w_z}(\delta) = \frac{\delta^2}{2w_z}$.

Proof: Fig. 1 shows the $(1,w_z)$-weighted degree table of monomial $\phi_a z^b$. In the table, the x-axis and y-axis represent ϕ_a's index a and z^b's degree b and their unit distances weight 1 and w_z respectively. Each monomial occupies a unit square and is represented by its lower left corner. The entry in the unit square indicates the monomial's $(1,w_z)$-weighted degree. In the pole basis L_w, given ϕ_a with pole order $v_{p_\infty}(\phi_a^{-1}) = \delta$ and $\delta > 2g-1$, there are in total g gaps [15]. Therefore, the distance between ϕ_a's lower left corner and the origin (0, 0) is $\delta - g$. In the table, $N_{1,w_z}(\delta)$ is the total area occupied by monomial $\phi_a z^b$ whose weighted degree is not greater than δ, denoted by the grey region. The triangle region defined by vertexes $(0,0), (0, \lfloor\frac{\delta}{w_z}\rfloor)$ and $(\delta-g, 0)$ has the area of $\frac{1}{2}(\delta-g)\lfloor\frac{\delta}{w_z}\rfloor \cong \frac{\delta(\delta-g)}{2w_z}$. It can be observed that the size of the grey region is greater than the size of the triangular region, and therefore $N_{1,w_z}(\delta) > \frac{\delta(\delta-g)}{2w_z}$. With $\delta \to \infty$, the sizes of these two regions approach to be equal as $N_{1,w_z}(\delta) = \frac{\delta(\delta-g)}{2w_z}$. As $\delta \gg g$, $N_{1,w_z}(\delta) = \frac{\delta^2}{2w_z}$.

Therefore, with $C_M \to \infty$, $\Delta_{1,w_z}(C_M) \to \infty$ and $\Delta_{1,w_z}(C_M) = \sqrt{2w_z N_{1,w_z}(\Delta_{1,w_z}(C_M))} = \sqrt{2w_z C_M}$.

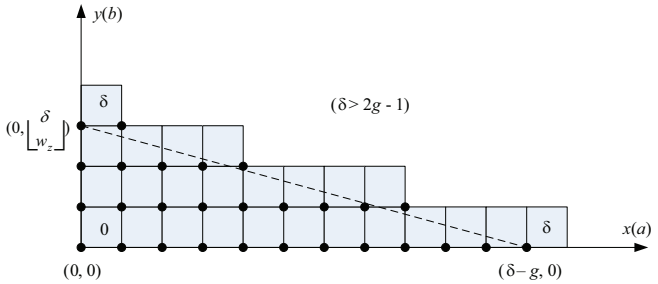


Fig. 1. Geometric argument for the decoding region of trivariate monomials.

Based on (15) and (20), inequality $S_M(\overline{c}) > \Delta_{1,w_z}(C_M)$ can be alternatively interpreted as:

$$\sum_{j=0}^{n-1} \widehat{m}_{i,j} > \sqrt{w_z \sum_{i=0}^{q-1} \sum_{j=0}^{n-1} m_{i,j}(m_{i,j}+1)}. \tag{26}$$

With $C_M \to \infty$, the total value of multiplicities $s \to \infty$, and $\frac{\pi_{i,j}}{n} \cong \frac{m_{i,j}}{s}$[12]. If we denote $\widehat{m}_{i,j}$'s corresponding entry in Π as $\widehat{\pi}_{i,j}$ and substitute $m_{i,j} = \frac{s}{n}\pi_{i,j}$ (or $\widehat{m}_{i,j} = \frac{s}{n}\widehat{\pi}_{i,j}$) into (26), it results:

$$\frac{s}{n}\sum_{j=0}^{n-1} \widehat{\pi}_{i,j} > \frac{s}{n}\sqrt{w_z \sum_{i=0}^{q-1} \sum_{j=0}^{n-1} \pi_{i,j}(\pi_{i,j}+\frac{n}{s})}. \tag{27}$$

As $\frac{n}{s} \cong 0$ when $s \to \infty$, (26) can be approximated as:

$$\sum_{j=0}^{n-1} \widehat{\pi}_{i,j} > \sqrt{w_z \sum_{i=0}^{q-1} \sum_{j=0}^{n-1} \pi_{i,j}^2}. \tag{28}$$

Message polynomial f can be found out if the inequality of (28) establishes. This indicates that the soft-decision scheme's optimal performance bound is determined by its reliability matrix Π and the code rate parameter w_z. This performance bound will be proven in Section V.

IV. Complexity Reducing Interpolation

Two complexity reducing methods have been proposed by the authors in [17] for the hard-decision list decoding of Hermitian codes. This section presents modifications based on these two methods when applied to the soft-decision interpolation.

A. Elimination of Unnecessary Polynomials

For the interpolation process of the soft-decision list decoding of Hermitian codes, a group of polynomials are initialised and each of them is tested with all the interpolated zero conditions defined by (13) and modified iteratively [17]. Given the designed output list size l, the polynomial group is initialised as:

$$G = \{Q^{(e)} \in F_q[x,y,z] | Q^{(e)} = Q^{(\lambda + w\delta)} = y^\lambda z^\delta, \\ 0 \le \lambda < w, 0 \le \delta \le l\}. \tag{29}$$

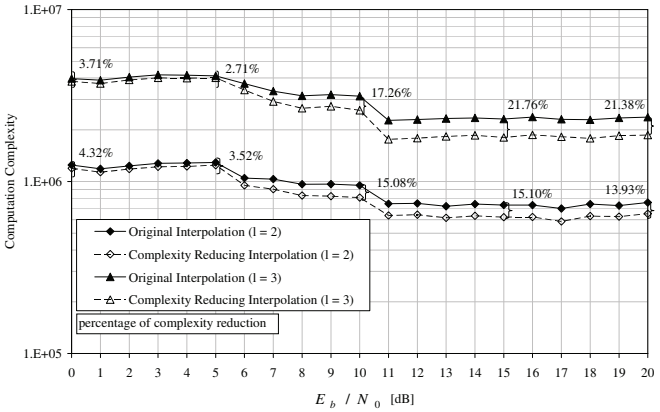


Fig. 2. Interpolation complexity reducing analysis for the (64, 19) Hermitian code.

There are $w(l+1)$ polynomials in G taking part in C_M iterations. Finally, the minimal polynomial in G is chosen as the interpolated polynomial Q as:

$$Q = \min_{lod(Q^{(e)})} \{Q^{(e)} | Q^{(e)} \in G\}. \tag{30}$$

Since the leading order of the chosen interpolated polynomial will not be greater than the iteration number [11, 17]

$$lod(Q) \le C_M, \tag{31}$$

those polynomials with leading order greater than C_M can be identified as unnecessary polynomials and eliminated during the iterations. Equation (31) also indicates the $(1, w_z)$-weighted degree upper bound for the interpolated polynomial is:

$$deg_{1,w_z}(Q) \le deg_{1,w_z}(\phi_a z^b | ord(\phi_a z^b) = C_M) = \Delta_{1,w_z}(C_M). \tag{32}$$

Algorithm B of [17] describes the complexity reducing interpolation process, in which polynomial group update criterion is modified for the soft-decision list decoding as:

$$G = \{Q^{(e)} | lod(Q^{(e)}) \le C_M\}. \tag{33}$$

Therefore, at the beginning of each iteration, the polynomial group is updated by (33) to eliminate the unnecessary polynomials and reduce the interpolation complexity. Fig. 2 shows the complexity reduction effect in soft-decision decoding of a (64, 19) Hermitian code. The decoding complexity is measured in term of the number of finite filed additions and multiplications. The modification scheme is error dependent for which complexity can be reduced more significantly in low-error weight situations [11, 17]. In the soft-decision system, the complexity reduction is measured as a function of the channel signal-to-noise ratio (SNR). It shows the modification provides a more significant reduction for high SNR values.

B. Pre-Calculation of the Corresponding Coefficients

Based on equation (13), the corresponding coefficients $\gamma_{a,p_j,\alpha}$ are important for testing each polynomial's interpolated zero condition during the iterations. Algorithm A of

[17] was proposed to determine these coefficients before the interpolation process. To apply the algorithm, the interpolated polynomial's weighted degree upper bound needs to be known, so that the maximal pole basis monomial ϕ_{max} of Q can be predicted by $v_{p_\infty}(\phi_{max}^{-1}) = deg_{1,w_z}(Q)$. Based on the interpolated polynomial's weighted degree upper bound of (32), the maximal pole basis monomial ϕ_{max} could be predicted by:

$$v_{p_\infty}(\phi_{max}^{-1}) = \Delta_{1,w_z}(C_M). \quad (34)$$

Then, the following n sets of corresponding coefficients are calculated with regards to each affine point as:

$$\{\gamma_{a,p_j,\alpha} | 0 \leq \alpha \leq max, \alpha \in N\}(j = 0, 1, \ldots, n-1). \quad (35)$$

In order to reduce the memory requirement for these n sets of corresponding coefficients, the usage of them need to be known. More specifically, since $\alpha < m_{i,j}$, among the coefficient set $\{\gamma_{a,p_j,\alpha} | 0 \leq \alpha \leq max, \alpha \in N\}$, those with $\alpha \geq m_{i,j}$ can be disregarded. Based on the matrix M, interpolated units associated with the entries $m_{i,j}$ of the same column share the same affine point. Hence, they will apply the same coefficient set defined by (35). Therefore, the maximal entry in each column of matrix M needs to be identified. Since the multiplicity values $m_{i,j}$ are proportionally transformed from the reliability values $\pi_{i,j}$, knowing the index i_j defined by (11), we can identify $m_{i_j,j}$ as the maximal entry in column j of matrix M. Therefore, in the n coefficient sets of (35), only

$$\{\gamma_{a,p_j,\alpha} | 0 \leq \alpha \leq max, \alpha < m_{i,j}\}(j = 0, 1, \ldots, n-1) \quad (36)$$

will be stored for interpolation. With the knowledge of these coefficient sets in (36), the soft-decision interpolation process can be efficiently facilitated.

Summarising the previous description, we present a complete soft-decision list decoding algorithm for Hermitian codes.

Algorithm A: Soft-decision list decoding of Hermitian Codes

Decoder parameter: Designed output list size l;

Input: The reliability matrix Π;

Step 1: Transform matrix Π into the multiplicity matrix M by algorithm A of [12] with applying the stopping criterion of Section III C;

Step 2: Determine the interpolated polynomial's weighted degree upper bound by (32);

Step 3: Perform algorithm A of [17] to determine the n sets of corresponding coefficients (35) and store them for the use in interpolation as (36);

Step 4: Perform algorithm B of [17] for the complexity reducing interpolation to determine the interpolated polynomial $Q(x, y, z)$, in which polynomial initialisation of (29) and polynomial group update criterion of (33) is applied;

Step 5: Perform the recursive coefficient search algorithm of [4] to find out the transmitted message polynomial $f(x, y)$.

V. Performance and Complexity Analyses

This section presents the performance and complexity analyses of the soft-decision list decoding algorithm for Hermitian codes. The performance is evaluated on both the additive white Gaussian noise (AWGN) channel and a quasi-static fading channel using QPSK modulation.

A. Comparison with Hard-Decision List Decoding of Hermitian Codes

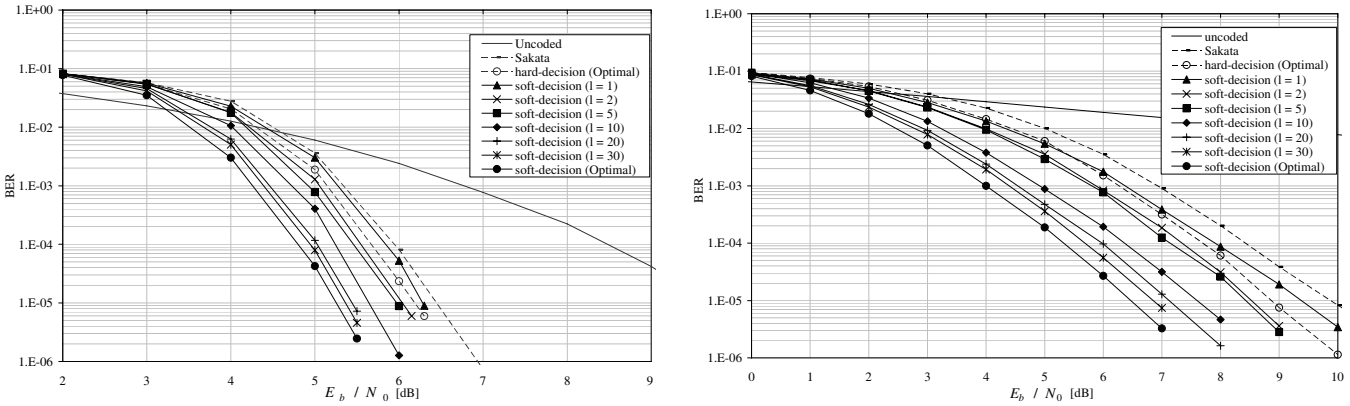
Figs. 3 and 4 present the performance of the (64, 39) and (512, 289) Hermitian codes which are defined in GF(16) and GF(64) respectively. On the fading channel, block interleavers with size 64×64 for the smaller codes and 100×512 for the larger code are employed. It can be observed from the simulation results that the soft-decision scheme can outperform both the unique decoder using Sakata's algorithm and the hard-decision list decoding algorithm. The improvement is especially significant on the fading channel. The performance improves as the output list size increases and approaches the soft-decision's optimal performance asymptotically. Notice that the optimal performance is obtained by assessing the inequality of (28) using knowledge of the transmitted code word $\overline{c}$ at the receiver and the reliability matrix Π.

Figs. 3 and 4 show that the soft-decision scheme with a small output list size can outperform the hard-decision scheme's optimal results, implying that the soft-decision scheme can outperform the hard-decision scheme with a smaller decoding complexity. The complexity of the list decoding system is dominated by the interpolation process for which the iteration number C (or the cost C_M defined by (20) in the soft-decision scheme) is the key parameter. Given the iteration number C, the interpolation complexity (finite field addition and multiplication operations) is upper bounded by $\frac{2}{3}(C+1)^3$[11]. For the analyses of Figs. 3 and 4, l^* is used to denote the smallest value with which the soft-decision scheme can outperform the hard-decision scheme's optimal result and Table I shows the required complexity. According to Table I, the soft-decision scheme can outperform the hard-decision scheme with far less decoding complexity.

B. Comparison With Soft-Decision List Decoding of RS Codes

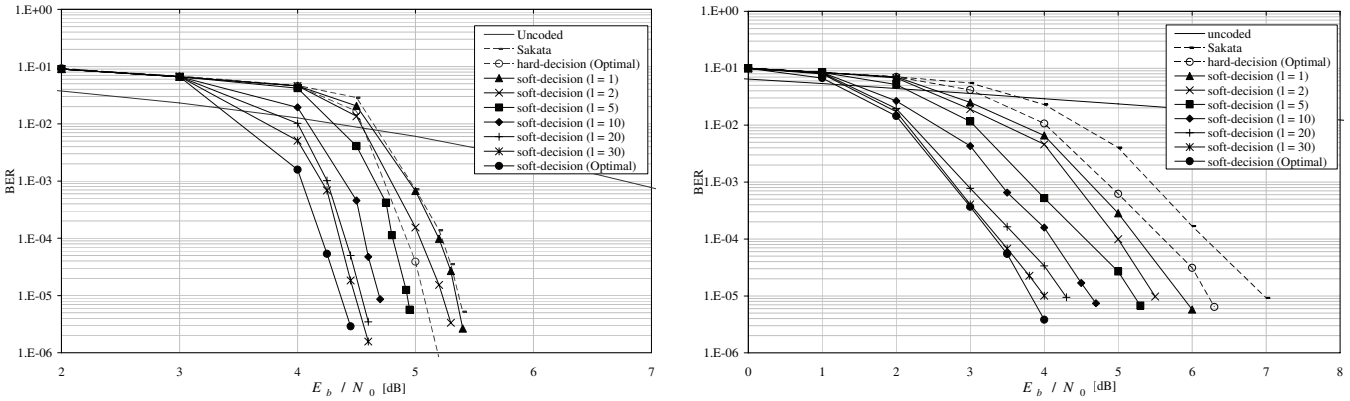
In this subsection, the (512, 289) Hermitian code's performance and decoding complexity are compared with the (63, 35) and the (255, 144) RS codes. All of the three codes have code rate of 0.56. Their performance comparison over the AWGN channel is shown in Figs. 6 and 7 respectively, and their decoding complexity comparison is shown in Table II.

Figs. 6 and 7 show that with the same output list size, the (512, 289) Hermitian code can outperform the RS codes defined both in the same finite field or even a larger finite field. For example, with $l = 5$, at a bit error rate (BER) of 10^{-5}, the Hermitian code has 0.55 dB and 0.3 dB coding gains over the (63, 35) RS code and the (255, 144) RS code respectively. According to Table II, with the same output list size, soft-decision list decoding of the Hermitian code demands a higher number of iterations mainly due to its long code word length. It is straightforward to realise that the decoding complexity



(a) Over AWGN channel (b) Over quasi-static fading channel

Fig. 3. Soft-decision list decoding performance of the (64, 39) Hermitian code.



(a) Over AWGN channel (b) Over quasi-static fading channel

Fig. 4. Soft-decision list decoding performance of the (512, 289) Hermitian code.

TABLE I
COMPLEXITY COMPARISON BETWEEN SOFT-DECISION AND HARD-DECISION LIST DECODING OF HERMITIAN CODES

Codes \ Schemes	Hard-decision (Optimal)	Soft-decision	
		AWGN	Rayleigh fading
Hermitian (64, 39)	$l = 13, C = 4224$	$l^* = 2, C = 246$	$l^* = 2, C = 246$
Hermitian (512, 289)	$l = 118, C = 2237952$	$l^* = 5, C = 4602$	$l^* = 1, C = 892$

of the Hermitian code is higher than that of the (63, 35) RS code. However, the complexity comparison with the (255, 144) RS code remains arguable, since this RS code is defined in a larger finite field in which the arithmetic finite field calculation is more complicated.

Elaborating further on this comparison, the authors select two cases for discussion. Firstly, we compare the list decoding of the Hermitian code with $l = 1$ and the list decoding of the (63, 35) RS code with $l = 5$, since they require a similar number of iterations. In this case, the decoding complexity for the two codes remains similar as they are defined in the same finite field. From Fig. 6, it can be observed that the Hermitian code can outperform the RS code in the low BER region. Secondly, we compare the list decoding of the Hermitian code with $l = 1$ and the list decoding of the (255, 144) RS code with $l = 2$ as they also require a similar number of iterations. However, the decoding complexity for the (255, 144) RS code is higher since it is defined in a larger finite field. As shown by Fig. 7, the Hermitian code with $l = 1$ can still outperform the RS code with $l = 2$.

VI. CONCLUSION

This paper has presented the first complete soft-decision list decoding algorithm for Hermitian codes. In order to prove the validity of the algorithm, a trivariate interpolated polynomial's zero condition with respect to the multiplicity matrix M was redefined. A new stopping criterion based on the designed output list size was introduced for the prior reliability transform algorithm. After geometrically defining the character of the monomial decoding region, an asymptotic optimal performance bound for the soft-decision scheme was presented and later proven by simulation results. For efficient implementation of the interpolation process, two modified complexity reducing methods were introduced for the soft-decision scheme.

TABLE II
COMPLEXITY COMPARISON BETWEEN SOFT-DECISION LIST DECODING OF HERMITIAN CODES AND RS CODES

Output size \ Codes	Hermitian (512, 289)	RS (63, 35)	RS (255, 144)
$l = 1$	$C = 892$	$C = 103$	$C = 430$
$l = 2$	$C = 1813$	$C = 204$	$C = 859$
$l = 5$	$C = 4602$	$C = 715$	$C = 3004$

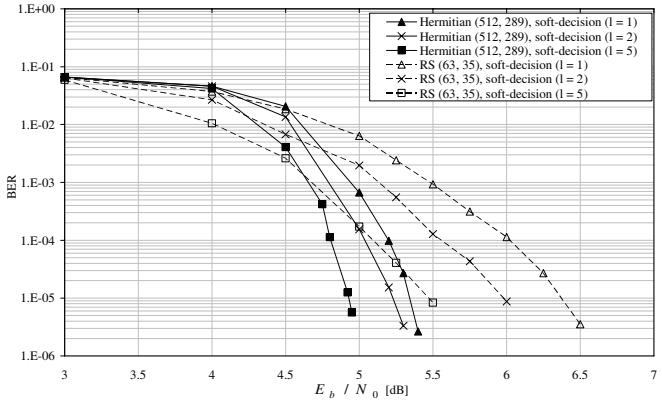


Fig. 5. Performance comparison between soft-decision list decoding of the (512, 289) Hermitian code and the (63, 35) RS code over AWGN channel.

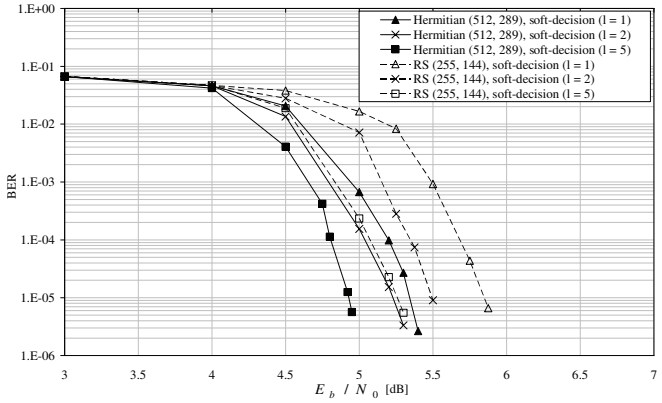


Fig. 6. Performance comparison between soft-decision list decoding of the (512, 289) Hermitian code and the (255, 144) RS code over AWGN channel.

First, by defining the interpolated polynomial's leading order upper bound, the elimination of unnecessary polynomials can be performed during the iterative interpolation. Our results showed it could reduce complexity up to 21.76%. Second, by defining the interpolated polynomial's weighted degree upper bound and knowing the multiplicity matrix M, pre-calculation of the corresponding coefficient can be performed before the interpolation process. As a summary, a complete soft-decision list decoding algorithm for Hermitian codes was presented. The performance and complexity analyses of this soft-decision scheme were given showing it can not only outperform hard-decision list decoding of Hermitian codes, but also outperform soft-decision list decoding of RS codes. Our analysis also showed that the Hermitian code could even outperform RS codes defined in larger finite fields, but with a smaller decoding complexity. From this work, we conclude that Hermitian codes are possible candidates to replace RS codes in future industrial applications.

REFERENCES

[1] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Industrial Appl. Math*, vol. 8, pp. 300-304, 1960.
[2] V. Goppa, "Codes on algebraic curves," *Soviet Math*, vol. Dok. 24, pp. 75-91, 1981.
[3] M. Johnston and R. A. Carrasco, "Construction and performance of algebraic-geometric codes over AWGN and fading channels," *IEE Proc Commun*, vol. 152, pp. 713-722, 2005.
[4] L. Chen, R. A. Carrasco, M. Johnston, and E. G. Chester, "Efficient factorisation algorithm for list decoding algebraic-geometric and Reed-Solomon codes," in *Proc IEEE ICC 2007*, pp. 851-856.
[5] I. Blake, C. Heegard, T. Hoholdt, and V. Wei, "Algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2596-2618, 1998.
[6] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Hoholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1672-1677, 1995.
[7] S. Sakata, "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array," *J. Symbol. Comput*, vol. 5, pp. 321-337, 1998.
[8] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37-46, 1993.
[9] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1757-1767, 1999.
[10] V. Guruswami, *List Decoding of Error-Correcting Codes*. Berlin Heidelberg: Springer-Verlag, 2004.
[11] L. Chen, R. A. Carrasco, and E. G. Chester, "Performance of Reed-Solomon codes using the Guruswami-Sudan algorithm with improved interpolation efficiency," *IET Proc. Commun*, vol. 1, pp. 241-250, 2007.
[12] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2809-2825, 2003.
[13] O. Pretzel, *Codes and Algebraic Curves*. Oxford: Clarendon Press, 1998.
[14] T. Hoholdt and R. R. Nielsen, "Decoding Hermitian codes with Sudan's algorithm," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Lecture Notes in Computer Science)*, vol. 1719, H. I. N. Fossorier, S. Lin, and A. Pole, eds. Berlin: Springer-Verlag, 1999, pp. 260-270.
[15] R. R. Nielsen, "List decoding of linear block codes," Lyngby, Denmark: Tech. Univ. Denmark, 2001.
[16] L. Chen, R. A. Carrasco, and M. Johnston, "List decoding performance of algebraic geometric codes," *IEE Electron. Lett.*, vol. 42, 2006.
[17] L. Chen, R. A. Carrasco, and M. Johnston, "Reduced complexity interpolation for list decoding Hermitian codes," *IEEE Trans. Wireless Commun*, vol. 7, no. 11, Nov, 2008, pp. 4353-4361.
[18] X. W. Wu and P. Siegel, "Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2579-2587, 2001.
[19] R. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *IEEE Trans. Inform. Theory*, vol. 46, pp. 246-257, 2000.