A parametric approach to list decoding of Reed-Solomon codes using interpolation

Mortuza Ali and Margreta Kuijper[*†]

November 5, 2010

Abstract

In this paper we present a minimal list decoding algorithm for Reed-Solomon (RS) codes. Minimal list decoding for a code C refers to list decoding with radius L, where L is the minimum of the distances between the received word $\mathbf{r}$ and any codeword in C. We consider the problem of determining the value of L as well as determining all the codewords at distance L. Our approach involves a parametrization of interpolating polynomials of a minimal Gröbner basis G. We present two efficient ways to compute G. We also show that so called re-encoding can be used to further reduce the complexity. Finally, we demonstrate how our parametric approach can be solved by a computationally feasible rational curve fitting solution from a recent paper by Wu.

1 Introduction

Reed-Solomon (RS) codes are important linear block codes that are of significant theoretical and practical interest. A (n, k) RS code C defined over a finite field $\mathbb{F}$ is a k dimensional subspace of the n dimensional space $\mathbb{F}^n$. For a message polynomial $m(x) = m_0 + m_1 x + \cdots + m_{k-1}x^{k-1}$, the encoding operation is to evaluate $m(x)$ at $x_1, x_2, \ldots, x_n$, where the x_i's are n distinct elements of $\mathbb{F}$. The rich algebraic properties and geometric structures of RS codes lead to the invention of a number of efficient decoding algorithms such as Sugiyama algorithm [24], Berlekamp-Massey (BM) algorithm [3, 18], and Welch-Berlekamp (WB) algorithm [26]. These classical decoding algorithms guarantee correct decoding as long as the number of errors is upper bounded by $t = \lfloor (d-1)/2 \rfloor$, where $d = n - k + 1$ is the minimum distance of the code.

In classical decoding, the error correcting radius of $t = \lfloor (d-1)/2 \rfloor$ originates from the requirement of unique decoding since for $t > \lfloor (d-1)/2 \rfloor$ multiple codewords within distance t from the received word $\mathbf{r}$ may exist. One way to circumvent this limitation is to increase the decoding radius beyond $\lfloor (d-1)/2 \rfloor$ and allow the decoder to output a list of codewords rather than one single codeword. However, such list decoding is only feasible if there are few codewords in the list. According to the Johnson bound [8], for a code of relative distance $\delta = d/n$, any Hamming sphere of radius $\leq n(1-\sqrt{1-\delta})$ around a received word $\mathbf{r}$ contains only a polynomial number of codewords. Therefore, a (n, k) RS code with $d = n-k+1$ can be list decoded up to the error correcting radius of $n-\sqrt{n(k-1)}$.

A list decoding algorithm was first discovered for low rate RS codes by Sudan [23] and later improved and extended for all rates by Guruswami and Sudan [7]. The Guruswami-Sudan algorithm can

[*]M. Ali and M. Kuijper are with the Department of Electrical and Electronic Engineering, University of Melbourne, VIC 3010, Australia mortuzaa@unimelb.edu.au; m.kuijper@ee.unimelb.edu.au

[†]This research is supported by the Australian Research Council (ARC)

correct errors up to the Johnson bound $n - \sqrt{n(k-1)}$. Given a received word $\mathbf{r}$, the essential idea of the algorithm is to find all the polynomials u of degree less than k such that $u(x_i) \neq r_i$ for at most t values of $i \in \{1, 2, \ldots, n\}$. The Guruswami-Sudan algorithm finds these polynomials in two steps: the interpolation step and the factorization step. In the interpolation step, it computes a bivariate polynomial $Q(x, r)$ that passes through all the points $(x_1, r_1), (x_2, r_2), \ldots, (x_n, r_n)$ with a prescribed multiplicity s satisfying a certain weighted degree constraint (see [7] for the definition of weighted degree). Then the bivariate polynomial $Q(x, r)$ is factorized to find all the factors of the form $r - u(x)$, where u is a polynomial of degree less than k. Now a polynomial u is a valid message polynomial if it is of degree less than k and $u(x_i) \neq r_i$ for at most t values of $i \in \{1, 2, \ldots, n\}$. The construction of $Q(x, r)$ with the prescribed multiplicity and weighted degree constraint ensures that for all valid message polynomials u, $r - u(x)$ appears as a factor of $Q(x, r)$. Even though the algorithm may produce implausible polynomials, the total number of polynomials ℓ in the list will satisfy the bound [19] $\ell < (s + 0.5)\sqrt{n/(k-1)}$.

The most computationally intensive operation in the Guruswami-Sudan algorithm is the construction of the bivariate polynomial $Q(x, r)$. Computation of $Q(x, r)$ involves solving a system of $O(ns^2)$ homogeneous equations which using Gaussian elimination can be done in time cubic in the number of equations [25]. Clearly the algorithmic complexity of the interpolation step is dominated by the multiplicity s. Recently Wu [27] transformed the interpolation problem to a 'rational interpolation problem' which involves smaller multiplicity. Given the received word $\mathbf{r}$, the Wu algorithm first computes the syndrome $\mathbf{s}$ of $\mathbf{r}$ followed by the computation of the error locator polynomial Λ and error correction polynomial B using the Berlekamp-Massey algorithm. Wu demonstrated that all valid error locator polynomials can be expressed as a parametrization of Λ and B. More specifically, given a list decoding radius t, the Wu algorithm aims at finding all polynomials λ and β such that $\Lambda' = \lambda\Lambda + \beta B$ has at most t distinct roots. Wu showed that similar to the Guruswami-Sudan approach, this problem can be reduced to a curve fitting problem but with significantly smaller multiplicity.

It may be observed that the set of all $Q(x, r) \in \mathbb{F}[x, r]$ passing through the points (x_i, r_i), for $i = 1, 2, \ldots, n$, with multiplicity s is an ideal I_s. From this observation several authors including Nielsen and Høholdt [21], Kuijper and Polderman [13], O'Keeffe and Fitzpatrick [22], and Lee and O'Sullivan [17], formulated the interpolation step of the list decoding algorithm as the problem of finding the minimal weight polynomial from the ideal I_s. Clearly the minimal weight polynomial will appear as the minimal polynomial in a minimal Gröbner basis of I_s computed with respect to the corresponding weighted term order. Lee and O'Sullivan also showed that the minimal polynomial in the ideal I_s can be computed more efficiently from a minimal Gröbner basis of a submodule of $\mathbb{F}[x]^q$ for a sufficiently large q. Let $\mathbb{F}[x, r]_q = \{f \in \mathbb{F}[x, r] \,|\, r\text{-deg}(f) \leq q\}$. Then $\mathbb{F}[x, r]_q$ can be viewed as a free module over $\mathbb{F}[x]^q$ with a free basis $1, r, \ldots, r^q$. Then the essential observation of Lee and O'Sullivan is that the minimal polynomial of I_s can be constructed from the minimal Gröbner basis of a submodule of $\mathbb{F}[x]^q$ along with the free basis $1, r, \ldots, r^q$, for large enough q.

In this paper we employ the theory of minimal Gröbner bases to perform minimal list decoding. Given the received word $\mathbf{r}$, let L denote the value of $d_H(\mathbf{r}, C)$ where

$$d_H(\mathbf{r}, C) := \min_{\mathbf{c} \in C} \{d_H(\mathbf{r}, \mathbf{c})\}.$$

Our main objective is to determine the value of L as well as all codewords $\mathbf{c}$ which are at a distance L from the received word $\mathbf{r}$. Clearly, if L is larger than the classical error correcting radius $\lfloor (d-1)/2 \rfloor$, the task is a list decoding operation. Our algorithm, unlike the Lee and O'Sullivan approach starts with computing a minimal Gröbner basis G of a submodule of $\mathbb{F}[x]^2$, rather than in $\mathbb{F}[x]^q$. We then demonstrate that all valid message polynomials can be extracted from a parametrization in terms of the elements of G. For computational feasibility, we show that this parametric approach, like Wu's algorithm, can be translated into a 'rational interpolation problem'. A distinguishing feature

of this approach, in contrast to Wu's algorithm, is in the computation of the valid codewords $\mathbf{c}$. Wu's algorithm, for each valid Λ', resorts to Forney's formula to compute the error values. In contrast, our algorithm immediately leads to a valid message polynomial.
The organization of the rest of the paper is as follows. In Section 2 we briefly review the relevant theory of Gröbner bases. in Section 3 we develop the theory and present the main algorithm along with two ways to compute the minimal Gröbner basis involved. We also explain how so-called re-encoding can be applied to the proposed approach. In Section 4 we translate the parametric approach into a 'rational interpolation problem'. Finally we conclude the paper in Section 5.

2 Preliminaries

The theory of Gröbner bases for modules in $\mathbb{F}[x]^q$ is generally recognized as a powerful conceptual and computational tool that plays a role similar to Euclidean division for modules in $\mathbb{F}[x]$. More specifically, minimal Gröbner bases prove themselves as an effective tool for various types of interpolation problems. In recent papers [14, 15, 16] this effectiveness was ascribed to a powerful property of minimal Gröbner bases, explicitly identified as the 'Predictable Leading Monomial Property'. The proofs in this paper make use of this property. Before recalling the PLM property let us first recall some terminology on Gröbner bases.

Let $\mathrm{e}_1, \ldots, \mathrm{e}_q$ denote the unit vectors in $\mathbb{F}^q$. The elements $x^\alpha \mathrm{e}_i$ with $i \in \{1, \ldots, q\}$ and $\alpha \in \mathbb{N}_0$ are called **monomials**. Let $n_1, \ldots, n_q$ be nonnegative integers. In this paper we define the following two types of monomial orders:

- The **$(n_1, \cdots, n_q)$-weighted term over position (`top`)** order, defined as

$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad \alpha + n_i < \beta + n_j \text{ or } (\alpha + n_i = \beta + n_j \text{ and } i < j).$$

- The **$(n_1, \cdots, n_q)$-weighted position over term (`pot`)** order, defined as

$$x^\alpha \mathrm{e}_i < x^\beta \mathrm{e}_j \quad :\Leftrightarrow \quad i < j \text{ or } (i = j \text{ and } \alpha + n_i < \beta + n_j).$$

Clearly, whatever order is chosen, every nonzero element $f \in \mathbb{F}[x]^q$ can be written uniquely as

$$f = \sum_{i=1}^{L} c_i X_i,$$

where $L \in \mathbb{N}$, the c_i's are nonzero elements of $\mathbb{F}$ for $i = 1, \ldots, L$ and the polynomial vectors $X_1, \ldots, X_L$ are monomials, ordered as $X_1 > \cdots > X_L$. Using the terminology of [1] we define

- $\mathrm{lm}(f) := X_1$ as the **leading monomial** of f
- $\mathrm{lt}(f) := c_1 X_1$ as the **leading term** of f
- $\mathrm{lc}(f) := c_1$ as the **leading coefficient** of f

Writing $X_1 = x^{\alpha_1} \mathrm{e}_{i_1}$, where $\alpha_1 \in \mathbb{N}_0$ and $i_1 \in \{1, \ldots, q\}$, we define

- $\mathrm{lpos}(f) := i_1$ as the **leading position** of f
- $\mathrm{wdeg}(f) := \alpha_1 + n_{i_1}$ as the **weighted degree** of f.

Note that for zero weights $n_1 = \cdots = n_q = 0$ the above orders coincide with the reflected versions of the standard TOP order and POT order, respectively, as introduced in the textbook [1].

Also note that, unlike with TOP, the introduction of weights does not change the POT ordering of monomials. In this paper we only need the weighted POT order because we need the associated notion of 'weighted degree'.

We now recall some basic definitions and results on Gröbner bases, see [1]. Below we denote the submodule generated by a polynomial vector f by $\langle f \rangle$.

Definition 2.1 *Let F be a subset of $\mathbb{F}[x]^q$. Then the submodule $\mathcal{L}(F)$, defined as*

$$\mathcal{L}(F) := \langle \mathrm{lt}(f) \mid f \in F \rangle$$

*is called the **leading term submodule** of F.*

Definition 2.2 *Let $M \subseteq \mathbb{F}[x]^q$ be a module and $G \subseteq M$. Then G is called a **Gröbner basis** of M if*

$$\mathcal{L}(G) = \mathcal{L}(M).$$

In order to define a concept of minimality we have the following definition.

Definition 2.3 ([1, Def. 4.1.1]) *Let $0 \neq f \in \mathbb{F}[x]^q$ and let $F = \{f_1, \ldots, f_s\}$ be a set of nonzero elements of $\mathbb{F}[x]^q$. Let $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and let $c_1, \ldots, c_s$ be elements of $\mathbb{F}$ such that*

1. $\mathrm{lm}(f) = x^{\alpha_i} \mathrm{lm}(f_i)$ *for $i = 1, \ldots, s$ and*
2. $\mathrm{lt}(f) = c_1 x^{\alpha_1} \mathrm{lt}(f_1) + \cdots + c_s x^{\alpha_s} \mathrm{lt}(f_s)$.

Define

$$h := f - (c_1 x^{\alpha_1} f_1 + \cdots + c_s x^{\alpha_s} f_s).$$

*Then we say that f **reduces** to h modulo F and we write*

$$f \xrightarrow{F} h.$$

*If f cannot be reduced modulo F, we say that f is **minimal** with respect to F.*

Lemma 2.4 ([1, Lemma 4.1.3]) *Let f, h and F be as in the above definition. If $f \xrightarrow{F} h$ then $h = 0$ or $\mathrm{lm}(h) < \mathrm{lm}(f)$.*

Definition 2.5 ([1]) *A Gröbner basis G is called **minimal** if all its elements g are minimal with respect to $G \backslash \{g\}$.*

It is well known [1, Exercise 4.1.9] that a minimal Gröbner basis exists for any module in $\mathbb{F}[x]^q$ and that all leading positions of its elements are different. In [14, 15, 16] another important property of a minimal Gröbner basis is identified; the theorem below merely formulates a wellknown result.

Theorem 2.6 ([14]) *Let M be a submodule of $\mathbb{F}[x]^q$ with minimal Gröbner basis $G = \{g_1, \ldots, g_m\}$. Then for any $0 \neq f \in M$, written as*

$$f = a_1 g_1 + \cdots + a_m g_m, \tag{1}$$

where $a_1, \ldots, a_m \in \mathbb{F}[x]$, we have

$$\mathrm{lm}(f) = \max_{1 \leq i \leq m; a_i \neq 0} (\mathrm{lm}(a_i) \mathrm{lm}(g_i)). \tag{2}$$

The property outlined in the above theorem is called the **Predictable Leading Monomial (PLM) property**, as in [14]. Note that this property involves not only degree information (as in the 'predictable degree property' first introduced in [4]) but also leading position information. Most importantly, the above theorem holds irrespective of which monomial order is chosen, for a proof see [14].

Clearly, in the above theorem $m = \dim(M)$ and all minimal Gröbner bases of M must have $\dim(M)$ elements, no matter which monomial order is chosen. Furthermore, we have the following theorem.

Theorem 2.7 *Let $n_1, \ldots, n_q$ be nonnegative integers and let M be a module in $\mathbb{F}[x]^q$. Let $G = \{g_1, \ldots, g_m\}$ be a minimal Gröbner basis of M with respect to the $(n_1, \cdots, n_q)$-weighted* `top` *order; denote $\ell_i := \operatorname{wdeg} g_i$ for $i = 1, \ldots, m$. Let $\tilde{G} = \{\tilde{g}_1, \ldots, \tilde{g}_m\}$ be a minimal Gröbner basis of M with respect to the $(n_1, \cdots, n_q)$- weighted* `pot` *order; denote $\tilde{\ell}_i := \operatorname{wdeg} \tilde{g}_i$ for $i = 1, \ldots, m$. Then*

$$\sum_{i=1}^{m} \ell_i = \sum_{i=1}^{m} \tilde{\ell}_i. \tag{3}$$

Proof We first prove the theorem for the case $m = q$. It follows easily from the fact that both G and $\tilde{G}$ are bases for M (in a linear algebraic sense) that there exists a unimodular polynomial matrix $U \in \mathbb{F}[x]^{q \times q}$ such that

$$\operatorname{col}\{g_1, \ldots, g_q\} = U \operatorname{col}\{\tilde{g}_1, \ldots, \tilde{g}_q\}.$$

Without restrictions we may assume that the leading positions within each Gröbner basis are strictly increasing. Clearly it follows from the above equation that also

$$V = UW, \tag{4}$$

where $V = \operatorname{col}\{g_1, \ldots, g_q\}\operatorname{diag}\{x^{n_1}, \cdots, x^{n_q}\}$ and $W = \operatorname{col}\{\tilde{g}_1, \ldots, \tilde{g}_q\}\operatorname{diag}\{x^{n_1}, \cdots, x^{n_q}\}$ Since U is unimodular we must have $\deg\det V = \deg\det W$. Clearly $\deg\det V = \sum_{i=1}^{m} \ell_i$ and $\deg\det W = \sum_{i=1}^{m} \tilde{\ell}_i$ from which (3) follows. Next, we prove the general case $m \leq q$. For this, we note that it follows immediately from (4) that the maximum degree of all minors of V equals the maximum degree of all minors of W. On the other hand, the maximum degree of all minors of V clearly equals $\sum_{i=1}^{m} \ell_i$ and similarly the maximum degree of all minors of W equals $\sum_{i=1}^{m} \tilde{\ell}_i$. The theorem now follows. □

We call the sum in (3) the **$(n_1, \cdots, n_q)$-weighted degree** of M, denoted by $\operatorname{wdeg}(M)$. For zero weights $n_1 = \cdots = n_q = 0$ the above result expresses that the sum of the degrees of a (reflected) TOP minimal Gröbner basis of a module M coincides with the sum of the degrees of a (reflected) POT minimal Gröbner basis of M. This result is merely a reformulation of the well known fact that the McMillan degree of a row reduced polynomial matrix equals the sum of its row degrees, see [5].

Corollary 2.8 *let M be a module in $\mathbb{F}[x]^q$. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis of M whose $(n_1, \cdots, n_q)$-weighted* `top` *degrees add up to* $\operatorname{wdeg}(M)$*. Then G is a minimal Gröbner basis of M with respect to the $(n_1, \cdots, n_q)$-weighted* `top` *order.*

Proof Suppose that G is not minimal. Then there exists $g \in G$ that can be reduced modulo $G \backslash \{g\}$. This implies that there exists a Gröbner basis of M whose sum of weighted degrees is strictly less than $\operatorname{wdeg}(M)$, which contradicts the above theorem. □

3 Minimal list decoding through division

Let us now consider a (n, k) RS code and a nonnegative integer t. The problem of 'list decoding up to t errors' is the following:

List Decoding Problem: Given a received word $(r_1, \cdots, r_n) \in \mathbb{F}^n$, find all polynomials $m \in \mathbb{F}[x]$ of degree $< k$ such that

$$m(x_i) = r_i \quad \text{for at least } n - t \text{ values of } i \in \{1, \ldots, n\}.$$

3.1 Main approach

We introduce the following two polynomials in $\mathbb{F}[x]$:

$$\Pi(x) = \prod_{i=1}^{n} (x - x_i), \tag{5}$$

and $\mathcal{L}$ as the Lagrange interpolating polynomial, i.e., the polynomial of least degree for which

$$\mathcal{L}(x_i) = r_i \text{ for all } i \in \{1, \ldots, n\}. \tag{6}$$

Definition 3.1 *Let* $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$. *The* **interpolation module** $M(\mathbf{r})$ *is given by the module in* $\mathbb{F}[x]^2$ *that is spanned by the vectors* $\tilde{g}_1 := [\Pi(x) \quad 0]$ *and* $\tilde{g}_2 := [\mathcal{L}(x) \quad -1]$.

Note that $\{\tilde{g}_1, \tilde{g}_2\}$ is a minimal `pot` Gröbner basis for $M(\mathbf{r})$. The above defined interpolation module is crucial to our approach. With $\tilde{g}_2$ we associate the bivariate polynomial $Q_2(x, y) = \mathcal{L}(x) - y$; clearly $Q_2(x_i, r_i) = 0$ for all $i \in \{1, \ldots, n\}$. Similarly, with $\tilde{g}_1$ we associate the polynomial $Q_1(x, y) = \Pi(x)$; trivially $Q_1(x_i, r_i) = 0$ for all $i \in \{1, \ldots, n\}$. Now consider an arbitrary bivariate polynomial Q of the form $Q(x, y) = N(x) - D(x)y$ for which $Q(x_i, r_i) = 0$ for all $i \in \{1, \ldots, n\}$. It can be shown, see [13], that $[N \quad -D] \in M(\mathbf{r})$. Recall that list decoding up to t errors amounts to finding all polynomials $m \in \mathbb{F}[x]$ of degree $< k$ such that

$$m(x_i) = r_i \quad \text{for all } i \in \{1, \ldots, n\} \text{ except } i = j_1, \ldots, j_L \text{ with } L \leq t.$$

In our context this amounts to looking for an interpolating bivariate polynomial Q of the form $Q(x, y) = D(x)m(x) - D(x)y$, where $D(x) = \prod_{\ell=1}^{L}(x - x_{j_\ell})$. Note that then indeed $Q(x_i, r_i) = 0$ for *all* $i \in \{1, \ldots, n\}$. Thus, to solve the above list decoding problem we are looking for particular vectors $[N \quad -D] \in M(\mathbf{r})$ of weighted $(0, k-1)$-degree $\leq t + k - 1$, that satisfy

1. N is a multiple of D and
2. D has L distinct zeros in $\mathbb{F}$, where L denotes deg D.

In this paper we are interested in finding the smallest value $L = d_H(\mathbf{r}, C)$ for which list decoding is possible as well as performing the associated list decoding. Thus we occupy ourselves with maximum likelihood list decoding. We have the following theorem.

Theorem 3.2 *Let* $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$ *be a received word and let* $M(\mathbf{r})$ *be the corresponding interpolation module. Let* $f = \begin{bmatrix} f^1 & f^2 \end{bmatrix} \in \mathbb{F}[x]^2$ *be a vector in* $M(\mathbf{r})$ *of weighted* $(0, k-1)$*-degree* L *that satisfies the following 3 requirements:*

1. $\text{lpos}(f) = 2$,

2. *f^1 is a multiple of f^2 and*

3. *there is no vector in $M(\mathbf{r})$ of weighted $(0, k-1)$-degree $< L$ that satisfies requirements 1) and 2).*

Then

$$m := \frac{f^1}{f^2}$$

is a message polynomial corresponding to a minimal error pattern of $L - k + 1$ errors.

Proof From $\mathrm{lpos}(f) = 2$ it follows immediately that $\deg m < k$ and $\deg f^2 = L - k + 1$. It remains to prove that f^2 has $L - k + 1$ distinct zeros in $\mathbb{F}$. Since $f \in M(\mathbf{r})$ there exist polynomials α and β such that

$$f = [\alpha \quad \beta] \begin{bmatrix} \Pi & 0 \\ \mathcal{L} & -1 \end{bmatrix}. \tag{7}$$

Observe that α and β do not have a common factor, otherwise the weighted degree of f would not be minimal (requirement 3). From (7) it follows that $\alpha\Pi - f^2\mathcal{L} = f^1$ is a multiple of f^2 by requirement 2. As a result, $\alpha\Pi$ is a multiple of f^2. Since α and $\beta = -f^2$ have no common factor it follows that Π must be a multiple of f^2, i.e., f^2 has $L - k + 1$ distinct zeros in $\mathbb{F}$, which proves the theorem. □

Lemma 3.3 *Let $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$ be a received word and let $M(\mathbf{r})$ be the corresponding interpolation module. Let $\{g_1, g_2\}$ be a $(0, k-1)$-weighted* `top` *minimal Gröbner basis for $M(\mathbf{r})$ with $\mathrm{lpos}(g_2) = 2$. Denote $\ell_1 := \mathrm{wdeg}\, g_1$ and $\ell_2 := \mathrm{wdeg}\, g_2$. Let t be a nonnegative integer. Then a parametrization of all vectors $f \in \mathbb{F}[x]^2$ with $\mathrm{lpos}(f) = 2$ and $\mathrm{wdeg}\, f = t + k - 1$ (with respect to the $(0, k-1)$-weighted* `top` *order) is given by*

$$f = \lambda g_1 + \beta g_2,$$

where $\lambda \in \mathbb{F}[x]$ with $\deg \lambda \leq t + k - 1 - \ell_1$ and β is a monic polynomial in $\mathbb{F}[x]$ of degree $t + k - 1 - \ell_2$. In particular, there exist no such vectors f for $t < \ell_2 - k + 1$.

Proof According to Theorem 2.6, $\{g_1, g_2\}$ has the PLM property with respect to the $(0, k-1)$-weighted `top` order. The parametrization now follows immediately from this property. □

Together, the above lemma and theorem give rise to the following heuristic list decoding algorithm.

An important feature of the above algorithm is that we use $\ell_2 = \mathrm{wdeg}\, g_2$ to decide how many errors to decode. Indeed, it follows from the above lemma that it is not possible to perform list decoding for $t < \ell_2 - k + 1$. We now present the main theorem of this section.

Theorem 3.4 *Let $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$ be a received word and let $M(\mathbf{r})$ be the corresponding interpolation module. Let $\{g_1, g_2\}$ be a $(0, k-1)$-weighted* `top` *minimal Gröbner basis for $M(\mathbf{r})$ with $\mathrm{lpos}(g_2) = 2$. Write $g_2 = \begin{bmatrix} g_2^1 & g_2^2 \end{bmatrix}$. Then Algorithm 1 yields a list of* all *message polynomials m such that*

$$d_H(\mathbf{c}, \mathbf{r}) \text{ is minimal, where } \mathbf{c} = (m(x_1), \ldots, m(x_n)). \tag{8}$$

In particular, in case there exists an error pattern with only $\leq \lfloor (n-k)/2 \rfloor$ errors, the list consists of only

$$m = \frac{-g_2^1}{g_2^2}. \tag{9}$$

Algorithm 1 Minimal list decoding of (n, k) RS code

Input: Received word $\mathbf{r} = (r_1, \ldots, r_n)$
Output: A list of polynomials m of degree $< k$ such that $d_H(\mathbf{c}, \mathbf{r})$ is minimal, where $\mathbf{c} = (m(x_1), \ldots, m(x_n))$.

1. Compute the polynomials Π and $\mathcal{L}$ given by (5) and (6) ; define the interpolation module $M(\mathbf{r}) := \text{ span } \{[\Pi \quad 0], [\mathcal{L} \quad -1]\}$.
2. Compute a minimal Gröbner basis $G = \{g_1, g_2\}$ of $M(\mathbf{r})$ with respect to the $(0, k-1)$-weighted `top` monomial order, with $\text{lpos}(g_2) = 2$. Denote $\ell_1 := \text{wdeg}\, g_1$ and $\ell_2 := \text{wdeg}\, g_2$; set $j = 0$.
3. Check requirement 2) of Theorem 3.2 for $f = \lambda g_1 + \beta g_2$, for all $\lambda \in \mathbb{F}[x]$ with $\deg \lambda \leq \ell_2 - \ell_1 + j$ and for all monic $\beta \in \mathbb{F}[x]$ with $\deg \beta = j$; write $f = \begin{bmatrix} f^1 & f^2 \end{bmatrix}$.
4. Whenever step 3) is successful, output all obtained quotient polynomials, i.e., polynomials m of the form $m = -f^1/f^2$. In case step 3) is not successful increase j by 1 and repeat step 3).

Proof Firstly, it follows immediately from Theorem 3.2 and Lemma 3.3 that any polynomial m that is output by Algorithm 1 has to have degree $< k$ and satisfy (8). Vice versa, if m is a polynomial of degree $< k$ that satisfies (8) then it follows from Lemma 3.3 that it must be in the output list of Algorithm 1. Finally, let us assume that there are only $\leq \lfloor (n-k)/2 \rfloor$ errors. This implies that there exists a vector $f = \begin{bmatrix} f^1 & f^2 \end{bmatrix}$ in $M(\mathbf{r})$ with $\text{wdeg}\, f \leq \lfloor (n-k)/2 \rfloor + k - 1 < (n+k-1)/2$ that satisfies the requirements of Theorem 3.2. Because of Lemma 3.3 it follows that $\ell_2 < (n+k-1)/2$. Now, since $\ell_1 + \ell_2 = n + k - 1$ by Theorem 2.7, this implies that $\ell_1 > \ell_2$. As a result, $\lambda = 0$ in step 3), so that step 4) immediately gives the unique solution for $j = 0$ as (9). □

Our next example illustrates the classical decoding scenario, showing that Algorithm 1 is an extension of existing classical interpolation-based algorithms as in [17, 6].

Example 3.5 *Consider the single-error correcting* $(7, 5)$ *RS code over* $GF(7)$*. The message polynomial* $m(x) = 2x^2 + x + 3$ *is encoded as* $\mathbf{c} = (m(0), m(1), \ldots, m(6)) = (3, -1, -1, 3, -3, 2, -3)$*. Let the received word be* $\mathbf{r} = (3, \mathbf{2}, -1, 3, -3, 2, -3)$*. Thus an error occurred at locator position 1. The polynomials* $\mathcal{L}$ *and* Π *are computed as* $\mathcal{L}(x) = -3x^6 - 3x^5 - 3x^4 - 3x^3 - x^2 - 2x + 3$ *and* $\Pi(x) = x^7 - x$*. Thus the module* $M(\mathbf{r})$ *is spanned by the rows of the matrix*

$$\begin{pmatrix} x^7 - x & 0 \\ -3x^6 - 3x^5 - 3x^4 - 3x^3 - x^2 - 2x + 3 & -1 \end{pmatrix}.$$

A minimal Gröbner basis $\{g_1, g_2\}$ *of* $M(\mathbf{r})$ *with respect to the* $(0, 4)$*-weighted* `top` *monomial order is computed as*

$$\text{col}\,\{g_1, g_2\} = \begin{pmatrix} -3x^6 - 3x^5 - 3x^4 - 3x^3 - x^2 - 2x + 3 & -1 \\ 2x^3 - x^2 + 2x - 3 & -x + 1 \end{pmatrix}$$

Thus, in the terminology of Theorem 3.4 we have $g_2^1 = 2x^3 - x^2 + 2x - 3$ *and* $g_2^2 = -x + 1$*. Applying Algorithm 1 we determine that* g_2^1 *is a multiple of* g_2^2 *and we recover*

$$m(x) = \frac{-g_2^1}{g_2^2} = 2x^2 + x + 3.$$

Let us now move on to an example of decoding beyond the classical error bound. Our approach is particularly feasible for the case that $\beta = 1$ and λ is restricted to a constant, as illustrated in the next example. Note that the example is an instance of "one-step-ahead" list decoding [27].

Example 3.6 *Consider the single-error correcting* $(7,4)$ *RS code over* $GF(7)$*; let the message polynomial be* $m(x) = 2x^2+x+3$ *which is encoded as* $\mathbf{c} = (m(0), m(1), \ldots, m(6)) = (3, -1, -1, 3, -3, 2, -3)$. *Let the received word be* $\mathbf{r} = (3, \mathbf{2}, -1, 3, \mathbf{2}, 2, -3)$ *which differs from* $\mathbf{c}$ *at locations 1 and 4. The polynomials* $\mathcal{L}$ *and* Π *are computed as* $\mathcal{L}(x) = -x^6 - 2x^5 + x^4 - x^3 + 2x + 3$ *and* $\Pi(x) = x^7 - x$. *The interpolation module* $M(\mathbf{r})$ *is spanned by the rows of the matrix*

$$M(\mathbf{r}) = \begin{pmatrix} x^7 - x & 0 \\ -x^6 - 2x^5 + x^4 - x^3 + 2x + 3 & -1 \end{pmatrix}.$$

A minimal Gröbner basis $\{g_1, g_2\}$ *of* $M(\mathbf{r})$ *with respect to the* $(0,3)$*-weighted* `top` *monomial ordering is computed as*

$$\text{col}\,\{g_1, g_2\} = \begin{pmatrix} x^5 - 2x^4 - x^3 - x^2 + x + 3 & -3x - 1 \\ -2x^4 + 2x^3 + x^2 - 3x + 2 & x^2 + 2x - 3 \end{pmatrix}.$$

Thus in this example $\ell_1 = \ell_2 = 5$*, so that* λ *is a constant. Applying Algorithm 1, we consider* $f = \lambda g_1 + g_2$ *for* $\lambda = 0, \ldots, 6$. *Writing* $f = \begin{bmatrix} f^1 & f^2 \end{bmatrix}$*, we find that* f^2 *divides* f^1 *for* $\lambda = 0, 2,$ *and* 4*, giving a list of three message polynomials—we recover not only* $m(x) = 2x^2 + x + 3$ *(for* $\lambda = 0$*), but also the message polynomials* $3x^3 - 2x^2 + 3x - 2$ *(for* $\lambda = 2$*), and* $-2x^3 - 2x^2 + 3x + 3$ *(for* $\lambda = 4$*).*

3.2 Computation of g_1 and g_2

There are various ways in which the required minimal Gröbner basis $\{g_1, g_2\}$ of the interpolation module $M(\mathbf{r})$ can be computed. One obvious way is to simply run an existing computer algebra system such as SINGULAR, specifying the required $(0, k-1)$-weighted `top` order.

Because of the specific form of $M(\mathbf{r})$ a more efficient way is to apply the Euclidean algorithm to the polynomials Π and $\mathcal{L}$. More specifically, we have the following algorithm.

Algorithm 2 Computation of g_1 and g_2 via Euclidean algorithm

Input: Received word $\mathbf{r} = (r_1, \ldots, r_n)$; polynomials Π and $\mathcal{L}$ given by (5) and (6).
Output: Polynomials g_1 and g_2 in $\mathbb{F}[x]^2$, such that $\{g_1, g_2\}$ is a minimal Gröbner basis of $M(\mathbf{r})$ with respect to the $(0, k-1)$-weighted `top` monomial order, with $\text{lpos}(g_2) = 2$.

1. Define polynomials h_0, h_1, t_0 and t_1 in $\mathbb{F}[x]$ as

$$\begin{bmatrix} h_0 & t_0 \\ h_1 & t_1 \end{bmatrix} := \begin{bmatrix} \Pi & 0 \\ \mathcal{L} & -1 \end{bmatrix};$$

set $j := 0$.
2. Check

$$\deg t_{j+1} + k - 1 \geq \deg h_{j+1}; \tag{10}$$

if NO, go to Step 3. If YES, define $g_1 := [h_j \quad t_j]$ and $g_2 := [h_{j+1} \quad t_{j+1}]$ and STOP.
3. Apply the Euclidean algorithm to h_j and h_{j+1}, yielding $h_j = q_{j+1}h_{j+1} + h_{j+2}$, where $\deg h_{j+2} < \deg h_{j+1}$.
4. Write

$$\begin{bmatrix} h_{j+1} & t_{j+1} \\ h_{j+2} & t_{j+2} \end{bmatrix} := \begin{bmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{bmatrix} \begin{bmatrix} h_j & t_j \\ h_{j+1} & t_{j+1} \end{bmatrix};$$

increase j by 1 and go back to Step 2.

Theorem 3.7 *Let* $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$ *be a received word and let* $M(\mathbf{r})$ *be the corresponding interpolation module. Then Algorithm 2 yields a* $(0, k-1)$*-weighted* `top` *minimal Gröbner basis* $\{g_1, g_2\}$ *for* $M(\mathbf{r})$ *with* $\mathrm{lpos}(g_2) = 2$.

Proof Firstly we note that the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{bmatrix}$$

is unimodular, i.e., has a polynomial inverse. It then follows that, at each step j, the rows of the matrix

$$\begin{bmatrix} h_j & t_j \\ h_{j+1} & t_{j+1} \end{bmatrix} \tag{11}$$

are a `pot` minimal Gröbner basis for $M(\mathbf{r})$ whose $(0, k-1)$-weighted `pot` degrees add up to $n+k-1$. By definition, with respect to the $(0, k-1)$-weighted `top` order both these row vectors have leading position 1, until the stopping condition (10) is met. At this point the second row vector has leading position 2 and the sum of the $(0, k-1)$-weighted `top` degrees add up to $n+k-1$. It now follows from Corollary 2.8 that the rows of the matrix (11) must be a $(0, k-1)$-weighted minimal `top` Gröbner basis for $M(\mathbf{r})$. □

Yet another alternative is to use an iterative method, interpolating the x_i's step by step for $i = 1, \ldots, n$. This method has the advantage that the Lagrange polynomial $\mathcal{L}$ does not need to be computed upfront.

Algorithm 3 Computation of g_1 and g_2 via iterative algorithm

Input: Received word $\mathbf{r} = (r_1, \ldots, r_n)$.
Output: Polynomials g_1 and g_2 in $\mathbb{F}[x]^2$, such that $\{g_1, g_2\}$ is a minimal Gröbner basis of $M(\mathbf{r})$ with respect to the $(0, k-1)$-weighted `top` monomial order, with $\mathrm{lpos}(g_2) = 2$.

1. Initialize $L_0 := k-1$ and $R_0 := I \in \mathbb{F}^{2\times 2}$; denote $R_j := \begin{bmatrix} Q_j & -K_j \\ N_j & -D_j \end{bmatrix} \in \mathbb{F}[x]^{2\times 2}$ for $j = 0, \ldots, n$.
2. Process the received values r_j iteratively for $j = 1$ to n as follows. For $j = 1$ to n do
   1. compute $\Gamma_j := Q_{j-1}(x_j) - r_j K_{j-1}(x_j)$ and $\Delta_j := N_{j-1}(x_j) - r_j D_{j-1}(x_j)$
   2. define $R_j := V_j R_{j-1}$, where
      - $V_j := \begin{bmatrix} \Delta_j & -\Gamma_j \\ 0 & x - x_j \end{bmatrix}$ and $L_j := L_{j-1} + 1$ if $\Delta_j \neq 0$ and ($L_{j-1} < (j+k-1)/2$ or $\Gamma_j = 0$),
      - $V_j := \begin{bmatrix} x - x_j & 0 \\ \Delta_j & -\Gamma_j \end{bmatrix}$ and $L_j := L_{j-1}$ otherwise
3. Define $g_1 := [Q_n \quad -K_n]$ and $g_2 := [N_n \quad -D_n]$.

Theorem 3.8 *Let* $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{F}^n$ *be a received word and let* $M(\mathbf{r})$ *be the corresponding interpolation module. Then Algorithm 3 yields a* $(0, k-1)$*-weighted* `top` *minimal Gröbner basis* $\{g_1, g_2\}$ *for* $M(\mathbf{r})$ *with* $\mathrm{lpos}(g_2) = 2$.

Proof For $j = 1, \ldots, n$ denote the interpolation module associated with $r_1, \ldots, r_j$ by $M(\mathbf{r}_1, \ldots, \mathbf{r}_j)$. We show that the rows of R_j are a Gröbner basis of $M(\mathbf{r}_1, \ldots, \mathbf{r}_j)$of the required form for $j = 1, \ldots, n$. We interpret L_j as the $(0, k-1)$-weighted `top` degree of the second row of R_j. Clearly this is true for $j = 1$. Let us now proceed by induction and assume that this is true for $j - 1 \in \{0, \ldots, n-1\}$. By definition of V_j and the induction assumption the rows of R_j are a Gröbner basis for $M(\mathbf{r}_1, \ldots, \mathbf{r}_j)$. Also, by construction, their $(0, k-1)$-weighted `top` degrees add up to 1 more than the $(0, k-1)$-weighted `top` degrees of R_{j-1}. Then, by induction, the $(0, k-1)$-weighted `top` degrees of R_j add up to $j + k - 1 = \text{wdeg}\,(M(\mathbf{r}_1, \ldots, \mathbf{r}_j))$. It then follows from Corollary 2.8 that the rows of R_j are a $(0, k-1)$-weighted `top` minimal Gröbner basis for $M(\mathbf{r}_1, \ldots, \mathbf{r}_j)$. Finally, by construction and the induction hypothesis, it is easily seen that the second row of R_j has leading position 2. This proves the theorem. □

3.3 The special case $\mathbf{r} = (y_1, \ldots, y_{n-k}, 0, \cdots, 0)$

In this subsection we pay special attention to the case that the received word $\mathbf{r}$ is of the form $(y_1, \ldots, y_{n-k}, 0, \cdots, 0) \in \mathbb{F}^n$. This comes about when so-called "re-encoding" is used in advance of RS decoding, see e.g., [10, 9].

First we introduce the polynomial $G \in \mathbb{F}[x]$ of degree $k-1$ as

$$G := \prod_{i=n-k+2}^{n} (x - x_i). \tag{12}$$

Clearly, the polynomials Π and $\mathcal{L}$ of the previous subsection can be written as

$$\Pi = \Pi_y G \tag{13}$$

and

$$\mathcal{L} = \mathcal{L}_y G, \tag{14}$$

where Π_y and $\mathcal{L}_y$ are in $\mathbb{F}[x]$. The following lemma is straightforward.

Lemma 3.9 *Let $(y_1, \ldots, y_{n-k}) \in \mathbb{F}^{n-k}$, $\mathbf{r} = (y_1, \ldots, y_{n-k}, 0, \cdots, 0) \in \mathbb{F}^n$ and let $\Pi, \mathcal{L}, G, \Pi_y$ and $\mathcal{L}_y$ be defined as before. Let $M(\mathbf{r}) :=$ span $\{[\Pi \quad 0], [\mathcal{L} \quad -1]\}$ as before and define $M^\star(\mathbf{y}) :=$ span $\{[\Pi_y \quad 0], [\mathcal{L}_y \quad -1]\}$. Then the following two statements are equivalent:*

- *$\{g_1, g_2\}$ is a minimal Gröbner basis of $M^\star(\mathbf{y})$ with respect to the unweighted `top` order, with $\text{lpos}(g_2) = 2$*
- *$\{\tilde{g}_1, \tilde{g}_2\}$ is a minimal Gröbner basis of $M(\mathbf{r})$ with respect to the $(0, k-1)$-weighted `top` order, with $\text{lpos}(\tilde{g}_2) = 2$,*

where $g_i = \begin{bmatrix} g_i^1 & g_i^2 \end{bmatrix}$ and $\tilde{g}_i = \begin{bmatrix} g_i^1 G & g_i^2 \end{bmatrix}$ for $i = 1, 2$.

Because of the above lemma it is now straightforward to modify Algorithm 1 into Algorithm 4. Again the Euclidean algorithm can be used to compute g_1 and g_2; for this, Algorithm 2 should be initialized by Π_y and $\mathcal{L}_y$ instead of Π and $\mathcal{L}$ and the stopping criterion (10) should be replaced by

$$\deg t_{j+1} \geq \deg h_{j+1},$$

instead of (10).

An alternative way to compute g_1 and g_2 is to employ an algorithm that processes the values of $y_1, \ldots, y_{n-k}$ iteratively. For this, Algorithm 3 is modified into Algorithm 5 which essentially coincides with the well-known Welch-Berlekamp algorithm [26], see also [11, 12].

Algorithm 4 Minimal list decoding of (n, k) RS code for re-encoded received word

Input: Received word $\mathbf{y} = (y_1, \ldots, y_{n-k})$ in $\mathbb{F}^{n-k}$.
Output: A list of polynomials m of degree $< k$ such that $d_H(\mathbf{c}, \mathbf{r})$ is minimal, where $\mathbf{c} = (m(x_1), \ldots, m(x_n))$ and $\mathbf{r} = (y_1, \ldots, y_{n-k}, 0 \ldots, 0)$ in $\mathbb{F}^n$.

1. Compute the polynomials Π_y and $\mathcal{L}_y$ given by (13) and (14) ; define the interpolation module $M(\mathbf{y}) := \text{ span } \{[\Pi_y \quad 0], [\mathcal{L}_y \quad -1]\}$.
2. Compute a minimal Gröbner basis $G = \{g_1, g_2\}$ of $M(\mathbf{y})$ with respect to the unweighted `top` monomial order, with $\text{lpos}(g_2) = 2$; set $j = 0$.
3. Compute $f = \lambda g_1 + \beta g_2$, for all $\lambda \in \mathbb{F}[x]$ with $\deg \lambda \leq \ell_2 - \ell_1 + j$ and for all monic $\beta \in \mathbb{F}[x]$ with $\deg \beta = j$; write $f = \begin{bmatrix} f^1 & f^2 \end{bmatrix}$. Check whether $f^1 G$ is a multiple of f^2, where G is given by (12).
4. Whenever step 3) is successful, output all obtained quotient polynomials, i.e., polynomials m of the form $m = -f^1 G / f^2$. In case step 3) is not successful increase j by 1 and repeat step 3).

Algorithm 5 Computation of g_1 and g_2 via iterative algorithm for re-encoded received word

Input: Received word $\mathbf{y} = (y_1, \ldots, y_{n-k})$ in $\mathbb{F}^{n-k}$.
Output: Polynomials g_1 and g_2 in $\mathbb{F}[x]^2$, such that $\{g_1, g_2\}$ is a minimal Gröbner basis of $M(\mathbf{y})$ with respect to the unweighted `top` monomial order, with $\text{lpos}(g_2) = 2$.

1. Denote $R_j := \begin{bmatrix} Q_j & -K_j \\ N_j & -D_j \end{bmatrix}$ for $j = 0, \ldots, n$; initialize $L_0 := 0$ and

$$R_0 := \begin{bmatrix} x - x_{n-k+1} & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{F}[x]^{2\times 2}$$

2. Process the received values y_j iteratively for $j = 1$ to $n - k$ as follows. For $j = 1$ to $n - k$ do
   1. compute $\Gamma_j := Q_{j-1}(x_j) - r_j K_{j-1}(x_j)$ and $\Delta_j := N_{j-1}(x_j) - r_j D_{j-1}(x_j)$
   2. define $R_j := V_j R_{j-1}$, where
      - $V_j := \begin{bmatrix} \Delta_j & -\Gamma_j \\ 0 & x - x_j \end{bmatrix}$ and $L_j := L_{j-1} + 1$ if $\Delta_j \neq 0$ and ($L_{j-1} < j/2$ or $\Gamma_j = 0$),
      - $V_j := \begin{bmatrix} x - x_j & 0 \\ \Delta_j & -\Gamma_j \end{bmatrix}$ and $L_j := L_{j-1}$ otherwise
3. Define $g_1 := [Q_{n-k} \quad -K_{n-k}]$ and $g_2 := [N_{n-k} \quad -D_{n-k}]$.

4 Minimal list decoding through rational interpolation

The most computationally intensive task in Algorithm 1 is Step 3. Recall that in Step 3, we need to determine all λ and β of degree $k_1 \leq \ell_2 - \ell_1 + j$ and $k_2 = j$ such that f^1 is a multiple of f^2. A brute force approach may be to consider

$$f = \begin{bmatrix} f^1 & f^2 \end{bmatrix} = \lambda \begin{bmatrix} g_1^1 & g_1^2 \end{bmatrix} + \beta \begin{bmatrix} g_2^1 & g_2^2 \end{bmatrix}$$

and checks for all polynomials λ and β of bounded degree k_1 and k_2, respectively, whether f^2 divides f^1. Clearly this approach is feasible only when both k_1 and k_2 are very small. For large values of k_1 and k_2, the computational complexity becomes prohibitively high, especially when the code is defined over a large field. Fortunately, Step 3 can be formulated as an algebraic curve fitting problem for which efficient polynomial time algorithms exist. We explain this approach in the following.
It follows from Theorem 3.2 that, in the context of Algorithm 1, f^1 is a multiple of f^2 if and only if f^2 has $t = \ell_2 - k + 1 + j$ distinct roots. Therefore, an alternative approach to Step 3 is to determine all λ and β of degree k_1 and k_2, respectively, such that f^2 has t distinct roots, i.e.,

$$\lambda(x_i)g_1^2(x_i) + \beta(x_i)g_2^2(x_i) = 0, \quad \text{for } t \text{ values of } x_i$$

Now let us define

$$z_i = -\frac{g_2^2(x_i)}{g_1^2(x_i)}, \quad \text{for } 1 \le i \le n$$

Then Step 3 can be formulated as the following rational interpolation problem.

Rational Interpolation Problem: Given n points $(x_1, z_1), (x_2, z_2) \cdots, (x_n, z_n)$, determine all rational polynomials of the form $\Lambda' = \lambda/\beta$, with λ and β of degree k_1 and k_2, respectively, such that Λ' passes through t of the n points.

This problem looks similar to the interpolation problem addressed in [7]. However, it is complicated by the fact that now we look for a rational solution rather than a polynomial solution. Recently, this rational interpolation problem has been addressed by Wu in [27]. In line with the Guruswami-Sudan approach, Wu's algorithm first computes a bivariate polynomial $Q(x, z)$, satisfying certain constraints, that passes through all the n points $(x_1, z_1), (x_2, z_2) \cdots, (x_n, z_n)$. Then the desired rational solutions $\Lambda' = \lambda/\beta$ are obtained from the factorization of $Q(x, z)$. More specifically, Wu's algorithm is based on the following theorem.

Theorem 4.1 ([20, Th. 4.3.3]) *Consider the n points $(x_1, z_1), (x_2, z_2), \cdots, (x_n, z_n)$. Let the parameters k_1, k_2, and t be given. Then there exist some multiplicity s, list size ρ, and a bivariate polynomial $Q(x, z) = \sum_{j=0}^{\rho} z^j Q_j(x)$ such that*

1. *$Q(x, z)$ passes through (x_i, z_i) with multiplicity at least s, for all $i = 1, 2, \ldots, n$ and*
2. *$\deg(Q_j(x)) \le s(n-t) - j(k_1 - k_2) - \rho k_2 - 1$, for all $j = 0, \ldots, \rho$.*

Moreover, any $Q(x, z)$ satisfying 1) and 2) must have $(z\lambda(x) - \beta(x))$ as a factor, where $\Lambda' = \lambda/\beta$ is a solution to the above rational interpolation problem.

In the above theorem, the requirement that (x_i, z_i)'s be zeros of $Q(x, z)$ with multiplicity s, for all $i = 1, 2, \ldots, n$, leads to $ns(s+1)/2$ constraints in the form of $ns(s+1)/2$ homogeneous equations. Besides, the second condition requires that the system of homogeneous equations involves $(\rho + 1)(s(n-t) - \frac{1}{2}\rho(k_1 + k_2))$ unknowns. Now a nonzero solution to the system of homogeneous equation exists if the number of constraints is less than number of unknowns, i.e.

$$ns(s+1)/2 < (\rho+1)(s(n-t) - \frac{1}{2}\rho(k_1 + k_2)) \tag{15}$$

In [27], a suitable choice for the values of s and ρ satisfying (15) has been proposed as

$$s = \left\lfloor \frac{t(n-k+1-t)}{t^2 - n(2t-(n-k+1))} \right\rfloor \tag{16}$$

$$\rho = \left\lfloor \frac{st}{2t-(n-k+1)} \right\rfloor. \tag{17}$$

After constructing the bivariate polynomial, according to Theorem 4.1 with values of s and ρ given by (16) and (17), the solutions to the rational interpolation problem can be obtained by the rational factorization procedure of [27]. It is worth noting that the construction of the bivariate polynomial dominates the overall complexity of solving the rational interpolation problem. Computation of the bivariate polynomial requires solving a system of homogeneous equations, which can be done using Gaussian elimination in time cubic in the number of equations.

Clearly every solution (λ, β) to the rational interpolation problem gives a valid error locator polynomial $\Lambda' = \lambda g_1^2 + \beta g_2^2$. Given a valid error locator polynomial Λ', Wu's algorithm uses Forney's formula to compute the error magnitudes and hence the codeword. However, in our approach, the message polynomial can be computed in a simpler way: for every solution (λ, β), it can be computed as

$$m(x) = \frac{\lambda g_1^1 + \beta g_2^1}{\lambda g_1^2 + \beta g_2^2}.$$

5 Conclusions

In this paper we have taken a parametric approach to the problem of minimal list decoding. The proposed algorithms have error correcting radius L, where L is the minimum of the Hamming distances between the received word and any codeword in C. There are two important features of the approach. Firstly, the minimality of L ensures that all solutions correspond to valid codewords and therefore we do not need to check for validity. The parametrization can also be used for general list decoding, however, then a check on the validity of the corresponding codewords needs to be carried out. Secondly, upon computation of a solution of the rational interpolation problem or, equivalently, of an error locator polynomial, we do not need to determine the error magnitudes via Forney's formula. Instead, solutions to the rational interpolation problem directly lead to message polynomials. Finally, by using re-encoding as in subsection 3.3, the approach lends itself well to the type of distributed source coding (DSC) proposed in [2].

References

[1] W. W. Adams and P. Loustaunau. *An introduction to Gröbner Bases*, volume 3 of *Graduate Stud. Math.* American Mathematical Society, 1994.

[2] M. Ali and M. Kuijper. Source coding with side information using list decoding. In *Proceedings IEEE International Symposium in Information Theory*, Austin, Texas, 2010.

[3] E.R. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill, New York, 1968.

[4] G.D. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inf. Th*, 16:720–738, 1970. correction, vol. IT-17, p.360, 1971.

[5] G.D. Forney, Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.

[6] S. Gao. A new algorithm for decoding of Reed-Solomon codes. In V. K. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, editors, *Communications information and network security*, pages 55–68. Kluwer, 2003.

[7] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Trans. Inf. Th*, 45:1757–1768, 1999.

[8] S. M. Johnson. A new upper bound for error-correcting codes. *IRE Trans. Inform. Theory*, pages 203–207, April 1962.

[9] R. Kötter, J. Ma, and A. Vardy. The re-encoding transformation in algebraic list-decoding of Reed-Solomon codes. *IEEE Trans. Inf. Th.* submitted (April 2010). Available: http://arxiv.org/abs/1005.5734.

[10] R. Kötter and A. Vardy. A complexity reducing transformation in algebraic list decoding of Reed-Solomon codes. In *Proceedings 2003 ITW (Paris, France)*, 2003.

[11] M. Kuijper. A system-theoretic derivation of the Welch-Berlekamp algorithm. In *Proceedings 2000 IEEE International Symposium in Information Theory*, page 418, Sorrento, Italy, 2000.

[12] M. Kuijper. Algorithms for decoding and interpolation. In Brian Marcus and Joachim Rosenthal, editors, *Codes, Systems, and Graphical Models*, volume 123 of *The IMA Volumes in Mathematics and its Applications*, pages 265–282. Springer-Verlag, 2001.

[13] M. Kuijper and J.W. Polderman. Reed-Solomon list decoding from a system theoretic perspective. *IEEE Trans. Inf. Th.*, IT-50:259–271, 2004.

[14] M. Kuijper and K. Schindelar. Minimal Gröbner bases and the predictable leading monomial property. submitted (June 2009). Available: http://arxiv.org/abs/0906.4602v3.

[15] M. Kuijper and K. Schindelar. The predictable leading monomial property for polynomial vectors over a ring. In *Proceedings IEEE International Symposium in Information Theory*, Austin, Texas, 2010.

[16] M. Kuijper and K. Schindelar. Gröbner bases and behaviors over finite rings. In *Proceedings of 48th IEEE Conf. Decision and Control (CDC'09)*, pages 8101–8106, Shanghai, China, December 2009.

[17] K. Lee and M.E. O'Sullivan. List decoding of Reed-Solomon codes from a Gröbner basis perspective. *J. Symbolic Comput.*, 43:645–658, 2008.

[18] J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Th.*, IT-15:122–127, 1969.

[19] R. J. McEliece. The Guruswami-Sudan decoding algorithm for Reed-Solomon codes. Technical Report 42-153, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, May 2003.

[20] J. S. R. Nielsen. List-decoding of error correcting codes. Master's thesis, Department of Mathematics, Technical University of Denmark, Denmark, 2010.

[21] R. Nielsen and T. Høholdt. Decoding Reed-Solomon codes beyond half the minimum distance. In J. Buchmann, T. Hoeholdt, T. Stichtenoth, and H. Tapia-Recillas, editors, *Coding Theory, Cryptography and Related Areas*, pages 221–236, Berlin, 2000. Springer-Verlag.

[22] H. O'Keeffe and P. Fitzpatrick. Gr obner basis approach to list decoding of algebraic geometry codes. *Applicable Algebra in Engineering, Communication and Computing*, 8(5):445–466, 2007.

[23] M. Sudan. Decoding of Reed-Solomon codes beyond the error correction bound. *J. Compl*, 13:180–193, 1997.

[24] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. A method for solving key equation for decoding goppa codes. *Information and Control*, 27:87–99, 1975.

[25] P. V. Trifonov. Interpolation in list decoding of Reed-Solomon codes. *Problems of Information Transmission*, 43(3):190–198, 2007.

[26] L. Welch and E. R. Berlekamp. Error correction of algebraic block code. *US Patent 4 633 470*, Dec 1986.

[27] Y. Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Trans. Inf. Th.*, 54:3611–3630, 2008.