Simultaneous Rational Function Reconstruction with Errors: Handling Multiplicities and Poles

Eleonora Guerrini, Kamel Lairedj, Romain Lebreton, Ilaria Zappatore

Simultaneous Rational Function Reconstruction with Errors: Handling Multiplicities and Poles

Eleonora Guerrini[a], Kamel Lairedj[b], Romain Lebreton[a], Ilaria Zappatore[c]

[a] *LIRMM, Université Montpellier, CNRS, Montpellier, France*
[b] *Université Paris 8, Paris, France*
[c] *LIX, Inria, Palaiseau, France*

Abstract

In this paper we focus on extensions of evaluation interpolation methods for recovering rational functions, in the context of erroneous evaluations. This problem can be viewed both from a computer algebra and a coding theory point of view. In computer algebra, this is a generalization of Simultaneous Rational Function Reconstruction with errors, with multiprecision evaluation. From an error correcting codes point of view, this problem is related to the decoding of some algebraic codes such as Reed Solomon or Derivatives codes. We give conditions on the inputs of the problem which guarantee the uniqueness of the interpolant.

Since we deal with rational functions, some evaluation points may be poles: a first contribution of this work is to correct *any error* in a scenario with poles and multiplicities that extends [KPY20]. Our second contribution is to adapt rational function reconstruction for *random errors*, and provide better conditions for uniqueness using interleaving techniques as in [GLZ21].

1. Introduction

In this paper we focus on extensions of evaluation interpolations methods for reconstructing a vector of rational functions, in presence of erroneous data. By extensions, we mean that for any evaluation point, we have a more accurate information than just the evaluation of the rational function. Our goal is to study the condition on the inputs of the problem which guarantees the uniqueness of the solution reconstruction, where some errors occur. We start by presenting the problem in its more general form.

Vector Rational Function Reconstruction. The Vector Rational Function Reconstruction (VRFR) is the problem of reconstructing a vector $\boldsymbol{f}/\boldsymbol{g} = (f_1/g_1, \ldots, f_n/g_n)$

Email addresses: guerrini@lirmm.fr (Eleonora Guerrini), kamel.lairedj02@etud.univ-paris8.fr (Kamel Lairedj), lebreton@lirmm.fr (Romain Lebreton), ilaria.zappatore@inria.fr (Ilaria Zappatore)

of rational functions given their remainders $r_k = f_k/g_k \bmod a_k$ and bounds on their degrees. This generalizes the *interpolation* problem, obtained by taking $a_1 = \cdots = a_n = \prod_{i=1}^{n}(x - \alpha_j)$ for some distinct α_j since in this case the modular equations become equations on evaluations $r_k(\alpha_j) = (f_k/g_k)(\alpha_j)$. We call *Simultaneous Rational Function Reconstruction* (SRFR), the particular case of VRFR where all the rational functions share the same denominator, *i.e.* $\boldsymbol{f}/g = (f_1/g, \ldots, f_n/g)$. A well-known specification of SRFR in this case is the problem to reconstruct a vector of rational functions which is a solution of a polynomial linear system (we refer to this problem as PLS).

In this paper, we consider the modulus $\prod(x-\alpha_j)^{\ell_j}$, for some positive integers ℓ_j's, called *precision* of the reconstruction. This is more general setting than the interpolation case.

Multiprecision evaluation and poles. Evaluation Interpolation is a well-known technique with different advantages. Beyond its complexity benefits, it can be easily parallelized, determining high-performance algorithms in distributed computation scenarios, *e.g.* for solving polynomial linear systems [BK14, KPSW17, GLZ19, GLZ21]. If $\deg(g) = 0$, we can recover the solution by Lagrange interpolation. When $\deg(g) \geq 1$, one can still recover the solution from $(\boldsymbol{f}/g)(\alpha_j)$ if $g(\alpha_j) \neq 0$ with Cauchy interpolation. However, we can learn more information from an evaluation point by extending the modulus to a precision greater than 1, *i.e.* by computing $r_j(x) = \boldsymbol{f}(x)/g(x) \bmod (x - \alpha_j)^{\ell_j}$ for a $\ell_j > 1$. We refer to this approach as multiprecision evaluation. Taylor formula states that it is equivalent to evaluate $\boldsymbol{y}$ and its derivatives $\boldsymbol{y}^{(i)}$ for $i < \ell_j$ at α_j (assuming large field characteristic). The recovering of a polynomial f from its multiprecision evaluation can be done with Hermite interpolation. In [KPY20] we can find a generalization that can handle rational functions and errors.

An important issue of SRFR in these cases is that we cannot evaluate $(\boldsymbol{f}/g)(\alpha_j)$ when α_j is a pole for $(\boldsymbol{f}/g)$ (*i.e.* $g(\alpha_j) = 0$). A first approach is to set the evaluation $r_j = (\boldsymbol{f}/g)(\alpha_j)$ to a new symbol ∞ when $g(\alpha_j) = 0$. To the best of our knowledge, this approach was first published in [KY13, KY14] in the context of sparse polynomial interpolation. In our context of dense polynomial interpolation, Cauchy interpolation is extended to handle poles, even in case of errors, but without multiprecision ($\ell_j = 1$) in [Per14]. This approach is extended in [KPY20] to recovering a rational function from a multiprecision evaluation. However, they do not consider multiplicities on poles, *i.e.* $\ell_j = 1$ when $g(\alpha_j) = 0$.

In this paper, we propose a new framework for evaluating a rational function $\boldsymbol{f}/g$ at a pole ($g(\alpha_j) = 0$) with multiplicities. We circumvent the problem of the pole by multiplying the rational function by a power of $(x - \alpha_j)$ such that the resulting rational function has no pole at α_j. More specifically, we set the evaluation of $\boldsymbol{f}/g$ at α_j at precision ℓ_j to be the couple $(v_j, r_j) \in \mathbb{N} \times \mathbb{F}_q[x]_{<\ell_j - v_j}$ such that $v_j = \mathrm{val}_{\alpha_j}(g)$ and $(x-\alpha_j)^{v_j}\boldsymbol{f}/g = r_j \bmod (x-\alpha_j)^{\ell_j - v_j}$. This amounts to giving $\ell_j - v_j$ coefficients of the Laurent series $v/g \in \mathbb{F}_q(\!(x-\alpha_j)\!)$, and v_j zero coefficients of g ($g = 0 \bmod (x - \alpha_j)^{v_j}$).

Interpolation with errors. The problem of reconstructing a rational function from a given set of evaluations is known in the literature as Cauchy interpolation. If a subset E of these evaluations are erroneous, one could still hope to recover the function by adding some extra evaluation points as in algebraic coding theory. To the best of our knowledge, the first attempt in this sense is given by [Per14] where the problem is defined in terms of *rational codes*. A rational code can be viewed as an extension of a Reed Solomon code, where codewords are evaluations of rational functions instead of polynomials. Decoding can be performed by an algorithm which extends Welch-Berlekamp method for Reed Solomon codes. An important point is that the Welch-Berlekamp key equation has to be modified in order to handle poles. Decoding rational codes is, in this sense, a first important case of SRFRwE.

When the rational function is a solution of a polynomial linear system, then it can be recovered from its evaluations, even in the presence of poles [BK14, KPSW17].

In [KPY20] is presented an extension of rational codes to multiprecision evaluation. They call Hermite interpolation with errors the related decoding problem. This can be viewed as an extension of derivatives codes [GW11] for rational functions instead of polynomials. In our results, we remove the assumption of large field characteristic of [KPY20] by using Hasse derivatives.

The classical goal in interpolation with errors is to provide a scenario that guarantees that the interpolant is unique. For this matter, [Per14, BK14, KPSW17, KPY20] give the number of extra evaluation points that are required to correct up to a certain number of errors. However, [BKY03, SSB07] have shown that one can add less evaluation points and correct *almost all* errors, or equivalently random errors, up to a certain number of errors using interleaving techniques. Recently, we adapted in [GLZ19, GLZ21] the interleaving techniques to SRFRwE but without handling poles. Here, we extend these interleaving techniques results to this multiprecision setting handling multiplicities and poles. As in [GLZ21], some error patterns could not give a unique interpolant. We provide an upper bound on the number of such inconvenient errors.

Outline of the paper. The paper is structured as follows: In Section 2, we present a new setting for multiprecision evaluation that can handle poles, and we extend the results of [KPY20] in the setting, removing their hypothesis on the characteristic of the field.

In Section 3, we study the uniqueness conditions for random errors. Using interleaving techniques from algebraic coding theory, we can lower the number of evaluations counted with multiplicity.

2. Rational Function Reconstruction with errors

Preliminaries and notations. Let $\mathbb{F}_q$ be a finite field of order q. In this paper, we extensively deal with vectors over $\mathbb{F}_q[x]$: we denote them by $\boldsymbol{f}$ and by f_i their components. The degree of a nonzero vector $\boldsymbol{f}$ is $\deg(\boldsymbol{f}) = \max_i(\deg(f_i))$.

We also consider a set $\{\alpha_1, \ldots, \alpha_\lambda\}$ of $\lambda \geq 1$ pairwise distinct $\alpha_j \in \mathbb{F}_q$, which we refer to as the set of the *evaluation points* α_j's. We associate a *multiplicity* $\ell_j \in \mathbb{N}$ to each evaluation point α_j. We assume that the evaluation points are ordered so that the sequence of multiplicities $(\ell_j)_j$ is nonincreasing.

Recall that the *valuation* $\mathrm{val}_{\alpha_j}(f/g)$ of a rational function $f/g \in \mathbb{F}_q(x)$ in a point α_j is defined as the maximal integer $v \in \mathbb{Z}$ such that $(x-\alpha_j)^{-v} f/g \in \mathbb{F}_q[x]$. In particular, if $\mathrm{val}_{\alpha_j}(f/g)$ is negative, then g must vanish at α_j. In this case, $\mathrm{val}_{\alpha_j}(g) = -\mathrm{val}_{\alpha_j}(f/g)$. In this paper we often consider valuations of vectors of rational functions, or of polynomials; we define $\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g) = \min_k(\mathrm{val}_{\alpha_j}(f_k/g))$. Finally, throughout this paper we always assume that the considered vectors of rational functions $\boldsymbol{f}/g$ are such that $\gcd(\boldsymbol{f}, g) := \gcd(\gcd_i(f_i), g) = 1$.

2.1. The interpolation problem without errors

We consider the problem of finding $(\boldsymbol{f}, g) \in \mathbb{F}_q[x]^{n+1}$, such that

$$(x-\alpha_j)^{v_j} \boldsymbol{f} = \boldsymbol{r}_j g \bmod (x-\alpha_j)^{\ell_j} \text{ for } 1 \leq j \leq \lambda \tag{1}$$

given polynomial vectors $\boldsymbol{r}_j \in \mathbb{F}_q[x]^n$ and $0 \leq v_j \leq \ell_j$ such that $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$. We also assume to know two upper bounds $N > \deg(\boldsymbol{f})$ and $D > \deg(g)$ on the degrees of the numerator $\boldsymbol{f}$ and the denominator g. We denote $L := \sum_{j=1}^{\lambda} \ell_j$ the number of evaluation points counted with multiplicity.

If $v_j = 0$ this problem coincides with the problem of reconstructing a vector of rational functions with the same denominator $(\boldsymbol{f}, g)$, given r_j such that $\boldsymbol{f} = \boldsymbol{r}_j g \bmod G$, where $G := \prod_{i=1}^{m}(x-\alpha_j)$. This is a classical computer algebra problem, known as *Cauchy interpolation problem*. Notice that we are implicitly assuming to apply the Chinese remainder theorem to Equation (1). We also point out that in this case all the evaluation points are not poles of the denominator $g(x)$. We now recall that

$$\mathcal{L}_{RFR} = N + D - 1, \tag{2}$$

is the minimum number of evaluations needed to uniquely reconstruct a solution of this problem [GG13, Section 5.7].

The starting point of this work is to understand what happens if we consider evaluation points which are poles of the vector of rational functions that we want to reconstruct. Several strategies were proposed in the literature to handle this case [Per14, KPSW17, KPY20].

In this paper, we propose a scenario where evaluation points that are poles of $\boldsymbol{f}(x)/g(x)$ are treated with corresponding multiplicities. Indeed, it suffices to observe that if there exists α_j among all the evaluations which is a pole of $\boldsymbol{f}/g$ of order v_j, then $(x-\alpha_j)^{v_j}$ divides $g(x)$ and so the equation (1) remains satisfied. For this reason we call this problem *Simultaneous Rational Function Reconstruction with Poles and their multiplicities* (SRFRwP).

If we want the corresponding interpolation problem to be well-defined, we need our new evaluation map to be injective, *i.e.* that any evaluation $(v_j, \boldsymbol{r}_j)$ has a unique preimage $\boldsymbol{f}/g$ (if any). In the following proposition we formally prove

that the evaluation map is injective as soon as $L \geq \mathcal{L}_{\mathrm{RFR}}$. This upper bound is coherent with the number of evaluations needed to uniquely reconstruct a solution of the Cauchy Interpolation problem ($l_j = 1$ for any j), which in this case coincides with the modulus degree L.

Proposition 2.1. *Assume $L \geq \mathcal{L}_{\mathrm{RFR}}$. If both $(\boldsymbol{\varphi}, \psi)$ and $(\boldsymbol{f}, g)$ satisfy*

$$(x-\alpha_j)^{v_j}\boldsymbol{\varphi} = r_j\psi \bmod (x-\alpha_j)^{\ell_j}$$
$$(x-\alpha_j)^{v_j}\boldsymbol{f} = r_j g \bmod (x-\alpha_j)^{\ell_j}$$

then $\boldsymbol{\varphi}/\psi = \boldsymbol{f}/g$.

Proof. By multiplying $(x-\alpha_j)^{v_j}\boldsymbol{\varphi} = r_j\psi \bmod (x-\alpha_j)^{\ell_j}$ by g and $(x-\alpha_j)^{v_j}\boldsymbol{f} = r_j g \bmod (x-\alpha_j)^{\ell_j}$ by ψ, we obtain :

$$(x-\alpha_j)^{v_j}\boldsymbol{\varphi} g = r_j\psi g \bmod (x-\alpha_j)^{\ell_j+\mathrm{val}_{\alpha_j}(g)}$$
$$(x-\alpha_j)^{v_j}\boldsymbol{f}\psi = r_j\psi g \bmod (x-\alpha_j)^{\ell_j+\mathrm{val}_{\alpha_j}(\psi)}$$

Let us assume for now that $\mathrm{val}_{\alpha_j}(g) \geq v_j$ and $\mathrm{val}_{\alpha_j}(\psi) \geq v_j$. Then, by subtracting one equation by the other we get

$$(x-\alpha_j)^{v_j}(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \mathbf{0} \bmod (x-\alpha_j)^{\ell_j+v_j}$$
$$(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \mathbf{0} \bmod (x-\alpha_j)^{\ell_j}$$

Let $\boldsymbol{p} := \boldsymbol{\varphi} g - \boldsymbol{f}\psi$. We have that $\boldsymbol{p} = \mathbf{0} \mod G$ where $G := \prod_{j=1}^{\lambda}(x-\alpha_j)^{\ell_j}$. Since $\deg(\boldsymbol{p}) < N+D-1$ and the degree of G is $L \geq N+D-1$, we have shown that $\boldsymbol{p} = \mathbf{0}$ as desired.

We now prove that $\mathrm{val}_{\alpha_j}(g) \geq v_j$ and $\mathrm{val}_{\alpha_j}(\psi) \geq v_j$. From Equation (1), we have

$$(x-\alpha_j)^{v_j}\boldsymbol{f} = \boldsymbol{r}_j g + (x-\alpha_j)^{\ell_j} P$$

for a given $P \in \mathbb{F}_q[X]$. Since $(x-\alpha_j)^{v_j}$ divides both $(x-\alpha_j)^{v_j}\boldsymbol{f}$ and $(x-\alpha_j)^{\ell_j}P$, then it divides $\boldsymbol{r}_j g$. Since we have assumed that $\gcd(\boldsymbol{r}_j, (x-\alpha_j)^{v_j}) = 1$, then $(x-\alpha_j)^{v_j} | g$ and so $v_j \leq \mathrm{val}_{\alpha_j}(g)$. We get similarly that $\mathrm{val}_{\alpha_j}(\psi) \geq v_j$. □

2.2. The interpolation problem with errors

In this work we deal with the SRFRwP problem, focusing on a scenario where some errors occur. For this purpose, we start by introducing our error definition, we then provide the formal definition of SRFRwP and errors problem (Definition 2.2), and we finally describe the technique used to solve it.

Error model. We start by defining what is an evaluation error. Giving Equation (1), we define the error support $E := \{j \mid (x-\alpha_j)^{v_j}\boldsymbol{f} \neq \boldsymbol{r}_j g \bmod (x-\alpha_j)^{\ell_j}\}$ as the set of positions j where $(v_j, \boldsymbol{r}_j)$ differs from the evaluation of a rational function $\boldsymbol{f}/g$. For any erroneous position j, we define the *minimal error index* $\mu_j := \mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g)$. Note that in this case, $\mu_j < \ell_j$ We can extend the definition of μ_j also for correct positions by setting $\mu_j = \ell_j$. This is equivalent to set $\mu_j := \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$ for all the positions.

We can now define our interpolation with errors problem; starting from any $(v_j, \boldsymbol{r}_j)$, our goal is to find a rational function $\boldsymbol{y}$ which is "close" to $(v_j, \boldsymbol{r}_j)$ in some sense.

Definition 2.2 (Simultaneous RFR with poles and errors). Given parameters N, D, $\hat{\tau}$, and any $(v_j, \boldsymbol{r}_j)$, find a vector of rational functions $\boldsymbol{y}(x) = \frac{\boldsymbol{f}(x)}{g(x)}$ satisfying the degree constraints $N > \deg(\boldsymbol{f})$, $D > \deg(g)$ and the error bound $\hat{\tau} \geq \sum_{j \in E}(\ell_j - \mu_j)$.

Note that the error support E and the minimal error indices μ_j both depend on the rational function $\boldsymbol{f}/g$ and on the instance $(v_j, \boldsymbol{r}_j)$. We can say that E and μ_j measure a distance between $\boldsymbol{f}/g$ and $(v_j, \boldsymbol{r}_j)$. Thus, $\hat{\tau} \geq \sum_{j \in E}(\ell_j - \mu_j)$ *iff* the rational function $\boldsymbol{y}$ is close to $(v_j, \boldsymbol{r}_j)$. In particular, if we set $\hat{\tau} = 0$, we must have that $\ell_j = \mu_j$, and in this case $(v_j, \boldsymbol{r}_j)$ are correct evaluations of $\boldsymbol{f}/g$.

If we want to find a rational function $\boldsymbol{y}(x) = \frac{\boldsymbol{f}(x)}{g(x)}$ and we know a bound τ on the error support $|E|$, then we can set $\hat{\tau} = \sum_{j=1}^{\tau} \ell_j$ in Definition 2.2 (since the ℓ_j's are nonincreasing).

Key Equations. We now describe our technique to solve SRFRwE. Since $\mu_j = \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$, we can define the *error locator polynomial* $\Lambda = \prod_{j \in E}(x-\alpha_j)^{\ell_j - \mu_j}$ and we observe that $\Lambda((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j}$.

We now define $\hat{\tau} := \sum_{j=1}^{\tau} \ell_j$, so that $\hat{\tau}$ is a known upper bound on the degree of the error locator, *i.e.* $\hat{\tau} \geq \deg(\Lambda)$ (recall that ℓ_j are non increasing). Therefore, we have that $(\Lambda\boldsymbol{f}, \Lambda g)$ belongs to the set $\mathcal{S}_{\boldsymbol{r}, N+\hat{\tau}, D+\hat{\tau}}$ of solutions $(\boldsymbol{\varphi}, \psi) \in \mathbb{F}_q[x]^{n+1}$ of the *key equations*

$$(x-\alpha_j)^{v_j}\boldsymbol{\varphi} = \boldsymbol{r}_j \psi \bmod (x-\alpha_j)^{\ell_j} \text{ for } 1 \leq j \leq \lambda \tag{3}$$

$$\deg(\boldsymbol{\varphi}) < N + \hat{\tau},\ \deg(\psi) < D + \hat{\tau}. \tag{4}$$

We now define $G^{\infty} := \prod_j (x-\alpha_j)^{v_j}$. Since $(x-\alpha_j)^{v_j}$ divides $\boldsymbol{r}_j\psi$ and $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$ then G^{∞} divides ψ. If we denote by $\bar{\psi}$ the quotient ψ/G^{∞}, then Equation (3) is equivalent to

$$\boldsymbol{\varphi} = \boldsymbol{r}_j \frac{G^{\infty}}{(x-\alpha_j)^{v_j}}\bar{\psi} \bmod (x-\alpha_j)^{\ell_j - v_j}. \tag{5}$$

This latter equation clarifies why in Definition 2.2 we choose the $\boldsymbol{r}_j$'s of degree smaller than $\ell - v_j$: only the remainders of $\boldsymbol{r}_j$ modulo $(x-\alpha_j)^{\ell_j - v_j}$ matters. Also, the definition of minimal error index μ_j only depends on the residue of $\boldsymbol{r}_j$ modulo $(x-\alpha_j)^{\ell_j - v_j}$. Indeed, If $v_j > \mathrm{val}_{\alpha_j}(g)$, then $\mu_j = \mathrm{val}_{\alpha_j}(g)$, no matter $\boldsymbol{r}_j$. If $v_j \leq \mathrm{val}_{\alpha_j}(g)$ then $\boldsymbol{r}_j g$ is well-defined modulo $(x-\alpha_j)^{\ell_j - v_j + \mathrm{val}_{\alpha_j}(g)}$, so modulo $(x-\alpha_j)^{\ell_j}$ and so we can conclude that μ_j is also well-defined.

We have already remarked that $(\Lambda\boldsymbol{f}, \Lambda g)$ belongs to $\mathcal{S}_{\boldsymbol{r}, N+\hat{\tau}, D+\hat{\tau}}$. However, if the degree bounds $N > \deg(\boldsymbol{f}), D > \deg(g)$ and the error bound $\hat{\tau} \geq \deg(\Lambda)$ are not tight, we get also other solutions. Indeed, $\mathcal{S}_{\boldsymbol{r}, N+\hat{\tau}, D+\hat{\tau}} \supseteq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda g\rangle_{0 \leq i < \delta_{N+\hat{\tau}, D+\hat{\tau}}}$, where

$$\delta_{N+\hat{\tau}, D+\hat{\tau}} := \min(N - \deg(\boldsymbol{f}), D - \deg(g)) + \hat{\tau} - \sum_{j \in E}(\ell_j - \mu_j). \tag{6}$$

Note that $\delta_{N+\hat{\tau},D+\hat{\tau}}$ is defined so that $i < \delta_{N+\hat{\tau},D+\hat{\tau}}$ *iff* $\deg(x^i\Lambda \boldsymbol{f}) < N+\hat{\tau}$ and $\deg(x^i\Lambda g) < D+\hat{\tau}$.

Link to previous work. Our scenario can be viewed as an extension of different previous works. If in the key equations (3) we consider $v_j = 0$ (no pole) and $\ell_j = 1$ (no multiplicity), we fall back to the simpler key equations

$$\varphi_k(\alpha_j) = r_{j,k}\psi(\alpha_j),\ \deg(\varphi_k) < N+\tau,\ \deg(\psi) < D+\tau. \tag{7}$$

These key equations (7) comes from [BK14, KPSW17, GLZ19] and they are the generalization of the Welch-Berlekamp method [BW86] for decoding Reed-Solomon codes. We also remark that the problem of finding solutions of these specific key equations with the degree constraints (4), coincides with the simultaneous Cauchy interpolation. On the other hand, if $d(x) \in \mathbb{F}_q$ (no rational function) and $\ell_j \leq 0$ (with multiplicity), the key equations (3) and (4) can be used for the decoding of *derivative codes* [GW11, KSY14].

[KPY20] considers poles but without multiplicities. Their key equation is a special case of our key equation (5). Indeed, if α_j is an *apparent pole*, defined as $\boldsymbol{v}_j > 0$, then $v_j = 1$ since $v_j \leq \ell_j = 1$. In this case, G^∞ is the product of apparent poles, and we have

- if α_j is an apparent pole, the key equation (5) reduces to the identity $0 = 0 \bmod (x-\alpha_j)^{\ell_j}$,
- otherwise, the key equation (5) becomes $\boldsymbol{\varphi} = \boldsymbol{r}_j G^\infty \bar{\psi} \bmod (x-\alpha_j)^{\ell_j}$.

By applying the Chinese remainder theorem, we can deduce $\boldsymbol{\varphi} = \boldsymbol{r}_j G^\infty \bar{\psi} \bmod \bar{G}$ where $\bar{G} = \prod_{\{j|v_j=0\}}(x-\alpha_j)$. Multiplying by G^∞, we obtain $G^\infty\boldsymbol{\varphi} = \boldsymbol{r}_j (G^\infty)^2 \bar{\psi} \bmod \bar{G}G^\infty$. This is the key equation of [KPY20, Equation (16)] (where $H = \boldsymbol{r}_j(G^\infty)^2$), which admits $(\Lambda\boldsymbol{f}, \Lambda g/G^\infty)$ as solution (note that $(\Lambda g)/G^\infty = \bar{\Lambda}\bar{G}$).

2.3. Uniqueness of SRFRwE for all errors

In this framework, it is crucial to determine the bound of L needed to guarantee the *uniqueness* of a solution of key equations (3), and degree constraints (4), where uniqueness is defined as follows. We say that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ has a *unique solution* if $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \neq \{(\boldsymbol{0},0)\}$ and for all $(\boldsymbol{\varphi},\psi),(\boldsymbol{\varphi}',\psi') \in \mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \setminus \{(\boldsymbol{0},0)\}$, we have equality $\boldsymbol{\varphi}/\psi = \boldsymbol{\varphi}'/\psi'$ of the corresponding rational functions.

The following result extends [KPY20] in two ways: first, we can handle multiplicities of poles and second, we remove the hypothesis on $\mathrm{char}(\mathbb{F}_q) \geq \ell_j$. This later was needed since derivatives of order ℓ_j of polynomials gives coefficients ℓ_j in the Hermite interpolation. We show in 2.4 how to overcome this problem.

Theorem 2.3. *Under the setting of Definition 2.2, assume that*

$$L \geq N + D - 1 + 2\hat{\tau}.$$

If there exists a solution $\boldsymbol{y}(x) = \boldsymbol{f}(x)/g(x)$ of the RFRwE problem then $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ has the special form

$$\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \le i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$$

for $\delta_{N+\hat{\tau},D+\hat{\tau}}$ defined as in (6). In this case, the solution $\boldsymbol{y}(x)$ is unique.

Proof. We assume that there exists a solution $\boldsymbol{y}(x) = \boldsymbol{f}(x)/g(x)$ of the RFRwE problem with instance $(v_j, \boldsymbol{r}_j)$. We now prove that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \subset \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \le i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$, the other inclusion being straightforward. From now on, we fix $(\boldsymbol{\varphi}, \psi) \in \mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$. First we show that $\boldsymbol{f}\psi - g\boldsymbol{\varphi} = \boldsymbol{0}$.

We combine

$$\begin{cases} (x-\alpha_j)^{v_j}\boldsymbol{\varphi} &= \boldsymbol{r}_j \psi \quad \bmod (x-\alpha_j)^{\ell_j} \\ (x-\alpha_j)^{v_j}\Lambda\boldsymbol{f} &= \boldsymbol{r}_j \Lambda g \quad \bmod (x-\alpha_j)^{\ell_j} \end{cases}$$

We multiply the first equation by Λg, so it reaches precision $\ell_j + v_j$. Indeed $\mathrm{val}_{\alpha_j}(\Lambda g) \ge v_j$ since $(x-\alpha_j)^{v_j}$ divides $\boldsymbol{r}_j \Lambda g$ and $\gcd((x-\alpha_j)^{\ell_j}, \boldsymbol{r}_j) = 1$. Similarly, we multiply the second equation by ψ so it becomes an equation modulo $(x-\alpha_j)^{\ell_j+v_j}$ (since $\mathrm{val}_{\alpha_j}(\psi) \ge v_j$). Finally, we get

$$\begin{aligned} (x-\alpha_j)^{v_j}\Lambda(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j+v_j} \\ \Lambda(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j} \end{aligned} \tag{8}$$

The polynomial $\boldsymbol{p} := \Lambda(\boldsymbol{\varphi} g - \boldsymbol{f}\psi)$ is zero modulo $G = \prod_{j=1}^{\lambda}(x-\alpha_j)^{\ell_j}$, which has degree L. However, $\boldsymbol{p}$ has degree

$$\begin{aligned} \deg(\boldsymbol{p}) &\le \deg(\Lambda) + \max(\deg(\boldsymbol{f}) + \deg(\psi), \deg(g) + \deg(\boldsymbol{\varphi})) \\ &< \hat{\tau} + (N + D - 1 + \hat{\tau}) \\ &\le L \end{aligned}$$

So it must be that $\boldsymbol{p} = \boldsymbol{0}$. Finally, $\Lambda \neq 0$ so $\boldsymbol{\varphi} g - \boldsymbol{f}\psi = \boldsymbol{0}$.

Since $\boldsymbol{\varphi} g - \boldsymbol{f}\psi = \boldsymbol{0}$ and $\gcd(\gcd_i(f_i), g) = 1$ then there exists $P \in \mathbb{F}_q[x]$ such that $(\boldsymbol{\varphi}, \psi) = (P\boldsymbol{f}, Pg)$. The key equations $(x-\alpha_j)^{v_j}\boldsymbol{\varphi} = \boldsymbol{r}_j\psi \bmod (x-\alpha_j)^{\ell_j}$ yield $P((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j}$ for all j.

Since $\mu_j = \mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g)$, and $\mu_j < \ell_j$ *iff* $j \in E$, we obtain that $P = 0 \bmod (x-\alpha_j)^{\ell_j - \mu_j}$ for $j \in E$. This means that $\exists Q \in \mathbb{F}_q[x], P = \Lambda Q$. Finally, $(\boldsymbol{\varphi}, \psi) = Q(\Lambda\boldsymbol{f}, \Lambda g)$ and the degree constraints on $(\boldsymbol{\varphi}, \psi)$ imply $\deg(Q) < \delta_{N+\hat{\tau},D+\hat{\tau}}$ which concludes our first part of the proof.

□

Remark 2.4. We can prove a more general version of the theorem, useful for a possible early termination setting as in [GLZ21, Section 4].

Let $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta}$ be the solution set of equation (9) with degree constraints $\deg(\boldsymbol{\varphi}) < \nu, \deg(\psi) < \vartheta$. Then $(x^i\Lambda\boldsymbol{f}, x^i\Lambda g)$ still belongs to $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta}$ provided that $i < \delta_{\nu,\vartheta}$ where $\delta_{\nu,\vartheta} := \min(\nu - \deg(\boldsymbol{f}), \vartheta - \deg(g)) - \deg(\Lambda)$.

Then, the proof of Theorem 2.3 can be easily adapted to show that $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0 \le i < \delta_{\nu,\vartheta}}$ whenever $L \ge \max(N + \vartheta, D + \nu) - 1 + \hat{\tau}$.

2.4. Solving key equations

Our resolution method of SRFRwE is based on solving the key Equation (5), with degree constraints (4). When the number L is large enough to ensure that the solution space $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle$, we can recover $(\Lambda \boldsymbol{f}, \Lambda g)$ by finding the minimal degree solution (whose last component is monic) of $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$. Then we can recover $(\boldsymbol{f}, g)$ from $(\Lambda \boldsymbol{f}, \Lambda g)$ by dividing by $\Lambda = \gcd(\Lambda \boldsymbol{f}, \Lambda g)$.

There are two main methods to find the minimal solution of $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ according to the algebraic interpretation of this solution set. First, we can notice that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ can be seen as a $\mathbb{F}_q$-vector space. Indeed, we will show later that the set of solutions is the kernel of a linear application $\Gamma_{\boldsymbol{r}}$. By taking a column echelon form of the matrix $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ associated to $\Gamma_{\boldsymbol{r}}$, we can find the minimal solution [BW86, BK14, KPSW17].

The solution space $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ can be also seen as a $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^{n+1}$. Its minimal solution can be extracted from a particular $\mathbb{F}_q[x]$-basis of this module, called the *row reduced basis* [Fit95, OS07, Nie13, RS16].

For the rest of this section we focus on the first method, based on linear algebra, since it will be useful to prove uniqueness results of SRFRwE in the random error framework (Section 3).

Solving key equations with linear algebra. We recall that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ is the set of $(\boldsymbol{\varphi}, \psi)$ is composed of $= (\boldsymbol{\varphi}, G^\infty \bar{\psi})$ where $(\boldsymbol{\varphi}, \bar{\psi})$ belongs to the kernel of the following $\mathbb{F}_q$-linear application $\Gamma_{\boldsymbol{r}}$:

$$\begin{aligned} \mathbb{F}_q[x]^n_{<N+\hat{\tau}} \times \mathbb{F}_q[x]_{<D+\hat{\tau}-\deg(G^\infty)} &\to \left(\prod_{j=1}^{\lambda} \mathbb{F}_q[x]/(x-\alpha_j)^{\ell_j - v_j} \right)^n \\ (\boldsymbol{\varphi}, \bar{\psi}) &\mapsto (\boldsymbol{\varphi} - \boldsymbol{r}_j G_j^\infty \bar{\psi})_{1 \le k \le n} \end{aligned}$$

where $G_j^\infty := G^\infty/(x-\alpha_j)^{v_j} = \prod_{j' \neq j} (x-\alpha_{j'})^{v_{j'}}$. We now fix a $\mathbb{F}_q$-vector space basis for the domain and the codomain of $\Gamma_{\boldsymbol{r}}$, and represent $\Gamma_{\boldsymbol{r}}$ as the matrix $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ according to those bases. Therefore, we can see $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ as the kernel of a matrix $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$.

We use the monomial basis $(x^i)_{i=0..\ell-1}$ for each component $\mathbb{F}_q[x]_{<\ell}$ on the domain. On the other hand, the codomain is isomorphic to $(\mathbb{F}_q[x]/G)^n$ where $G := \prod_{j=1}^{\lambda} (x-\alpha_j)^{\ell_j - v_j}$. So, for any component $\mathbb{F}_q[x]/G$ of the codomain, we consider a specific basis which we call the *Hasse basis*. We define such a basis as $(\mathcal{H}_{i,j})_{\substack{1 \le i \le \ell_j - v_j \\ 1 \le j \le \lambda}}$ such that $\mathcal{H}_{i,j}$ is the only polynomial which satisfies

$$\begin{cases} \mathcal{H}_{i,j} = 0 & \bmod (x-\alpha_{j'})^{\ell_{j'} - v_{j'}} \quad \text{if } j \neq j' \\ \mathcal{H}_{i,j} = (x-\alpha_j)^i & \bmod (x-\alpha_j)^{\ell_j - v_j} \\ \deg(\mathcal{H}_{i,j}) < \deg(G) \end{cases}.$$

We call such a basis an Hasse one since it is the dual basis of the linear forms called *Hasse derivatives* (see for instance [Cox20, Section 2]).

In order to deduce the matrix associated to $\Gamma_{\boldsymbol{r}}$, we need to decompose according to the Hasse basis the polynomials φ_k, $\bar{\psi}$ which are written according to the monomial basis (x^i). Since $x^t = (x-\alpha+\alpha)^t = \sum_{i=0}^{t} \binom{t}{i} \alpha^{t-i}(x-\alpha)^i$, we get that the following decomposition on the Hasse basis for x^t :

$$x^t = \sum_{1\le j\le \lambda} \sum_{0\le i<\min(\ell_j - v_j, t)} \binom{t}{i} \alpha_j^{t-i} \mathcal{H}_{i,j} \bmod G.$$

The decomposition of $\boldsymbol{r}_j$ on the Hasse basis is direct if we write the k-th vector component $r_{j,k}$ of $\boldsymbol{r}_j$ as $r_{j,k} = \sum_{0\le i<\ell_j - v_j} r_{i,j,k}(x-\alpha_j)^i \bmod (x-\alpha_j)^{\ell_j - v_j}$.

We now explain how the multiplication works on the Hasse basis. By looking at the residues modulo $(x-\alpha_j)^{\ell_j - v_j}$, we can remark that

$$\mathcal{H}_{t,j}\mathcal{H}_{s,j'} = \begin{cases} 0 & \text{if } j \neq j' \\ 0 & \text{if } j = j' \text{ and } t+s \ge \ell_j - v_j \\ \mathcal{H}_{t+s,j} & \text{if } j = j' \text{ and } t+s < \ell_j - v_j \end{cases}.$$

We now have all the ingredients to write our matrix.

If $\varphi_k = \sum_{t=0}^{N+\hat{\tau}-1} \varphi_{t,k} x^t$ and $\bar{\psi} = \sum_{s=0}^{D+\hat{\tau}-1} \varphi_{s,k} x^s$, then

$$\varphi_k - \boldsymbol{r}_j \bar{\psi} = \sum_{\substack{0\le i<\ell_j - v_j \\ 1\le j\le \lambda}} \left[\sum_{i\le t<N+\hat{\tau}} \binom{t}{i} \alpha_j^{t-i} - \sum_{\substack{0\le u\le i \\ u\le s<D+\hat{\tau}}} \binom{s}{u} \bar{\psi}_s \alpha_j^{s-u} r_{i-u,j,k} \right] \mathcal{H}_{i,j} \bmod G.$$

Matrices formulae. Let's define the matrix $W_{\boldsymbol{\alpha},\boldsymbol{\ell}}$ corresponding to the change of basis from the monomial basis to the Hasse basis. The formulas are

$$W_{\boldsymbol{\alpha},\boldsymbol{\ell}-\boldsymbol{v},d} := \begin{pmatrix} W_{\alpha_1,\ell_1-v_1,d} \\ \vdots \\ W_{\alpha_\lambda,\ell_\lambda-v_\lambda,d} \end{pmatrix},$$

where,

$$W_{\alpha_j,\ell_j-v_j,d} := \begin{pmatrix} 1 & \alpha_j & \alpha_j^2 & \alpha_j^3 & \dots & \binom{\ell_j-v_j-1}{0}\alpha_j^{\ell_j-v_j-1} & \dots & \binom{d-1}{0}\alpha_j^{d-1} \\ 0 & 1 & 2\alpha_j & 3\alpha_j^2 & & \binom{\ell_j-v_j-1}{1}\alpha_j^{\ell_j-v_j-2} & \dots & \binom{d-1}{1}\alpha_j^{d-2} \\ 0 & 0 & 1 & 3\alpha_j & & \binom{\ell_j-v_j-1}{2}\alpha_j^{\ell_j-v_j-3} & \dots & \binom{d-1}{2}\alpha_j^{d-3} \\ 0 & 0 & 0 & 1 & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \ddots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & 0 & \binom{\ell_j-v_j-1}{\ell_j-v_j-1}\alpha_j^0 & \dots & \binom{d-1}{d-\ell_j+v_j}\alpha_j^{d-\ell_j+v_j} \end{pmatrix}$$

and $d \ge \ell_j - v_j$ for all j.

Notice that if $\ell_j - v_j = 1$ for all j, then $W_{\boldsymbol{\alpha},\boldsymbol{\ell}}$ simplifies, and we get the Vandermonde matrix

$$W_{\boldsymbol{\alpha},\mathbf{1},d} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_\lambda & \alpha_\lambda^2 & \dots & \alpha_\lambda^{d-1} \end{pmatrix}.$$

We now define the matrix $T_{\boldsymbol{r},\boldsymbol{\ell},k}$ that corresponds to the multiplication by $(\boldsymbol{r}_j)_j$ in the Hasse basis as

$$T_{\boldsymbol{r},\boldsymbol{\ell}-\boldsymbol{v},k} := \begin{pmatrix} T_{\boldsymbol{r}_1,\ell_1-v_1,k} & & \\ & \ddots & \\ & & T_{\boldsymbol{r}_\lambda,\ell_\lambda-v_\lambda,k} \end{pmatrix}$$

where

$$T_{\boldsymbol{r}_j,\ell_j-v_j,k} := \begin{pmatrix} r_{0,j,k} & & & \\ r_{1,j,k} & r_{0,j,k} & & \\ \vdots & \ddots & \ddots & \\ r_{\ell_j-v_j-1,j,k} & \cdots & r_{1,j,k} & r_{0,j,k} \end{pmatrix}.$$

Altogether, we can now give the formula for the matrix $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$

$$\left(\begin{array}{ccc|c} W_{\boldsymbol{\alpha},\boldsymbol{\ell}-\boldsymbol{v},N+\hat{\tau}} & & & -T_{\boldsymbol{r},\boldsymbol{\ell}-\boldsymbol{v},1}W_{\boldsymbol{\alpha},\boldsymbol{\ell}-\boldsymbol{v},D+\hat{\tau}} \\ & \ddots & & \vdots \\ & & W_{\boldsymbol{\alpha},\boldsymbol{\ell}-\boldsymbol{v},N+\hat{\tau}} & -T_{\boldsymbol{r},\boldsymbol{\ell}-\boldsymbol{v},n}W_{\boldsymbol{\alpha},\boldsymbol{\ell}-\boldsymbol{v},D+\hat{\tau}} \end{array}\right)$$

An important aspect of this matrix is that the coefficients $r_{i,j,k}$ appears only in the last $D+\hat{\tau}$ columns of $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$, with degree 1. This will play a central role in all proofs related to the random error model. Note also that this matrix generalizes the matrix of [BKY03] revisited also in [GLZ21, Remark 2.3].

3. Rational Function Reconstruction with random errors

Recall that our goal in this work is to determine a bound on the modulus degree which guarantees to uniquely reconstruct the solution of SRFRwE. In the previous section (Theorem 2.3) we showed that if this degree is at least $N+D-1+2\hat{\tau}$, we can uniquely reconstruct the solution. We have already remarked in Section 2.2 that our resolution method for SRFRwE is a generalization of the interpolation-based decoding technique of IRS codes. As in [GLZ19, GLZ21], we can exploit this error correcting codes technique to reduce the bound on the modulus degree. In this section we start by introducing some technical results, we formalize our problem (Definition 3.3) and we conclude by proving that under some assumptions on the error distribution we can lower the degree modulus (Theorem 3.4).

3.1. Multiplicity balancing

In this section we introduce a new bound on the modulus degree, which guarantees to solve SRFRwE with random errors; we dispatch the random errors among the n components of the vectors $\boldsymbol{r}_j$. For this purpose we need some technical intermediary results, which we will use in the proof of Theorem 3.4.

First, recall that in the error locator Λ, an error at the evaluation point α_j for $j \in E$ is counted with multiplicity up to $\ell_j - \mu_j$.

In particular, we will face up to the following problem: we want to partition the error support $E = \sqcup_{k=1}^{n} I_k$ such that each part counted with multiplicity is as small as possible. More specifically, we are looking for a partition $E = \sqcup_{k=1}^{n} I_k$ which minimizes the maximum size of its parts $\max_k(\sum_{j\in I_k}(\ell_j - \mu_j))$. We denote $\mathrm{MB}((\ell_j - \mu_j), E)$ this minimum, where MB stands for *multiplicity balancing*.

This problem is commonly known as the *load balancing* problem, the *multiprocessor scheduling* problem, or as $P||C_{\max}$, [CEC+13, Section 6].

This problem is NP-hard, but approximations can be found in polynomial time. Historically, Graham used the list scheduling algorithm to find a 2-approximation of $\mathrm{MB}((\ell_j - \mu_j), E)$ [Gra66]. Indeed, Graham result applied to our case gives :

$$\max_k \left(\sum_{j\in I_k} \ell_j \right) \leq \left\lceil (\sum_{j\in E} \ell_j)/n \right\rceil + \max_{j\in E} \ell_j$$

for the partition $E = \sqcup_{k=1}^{n} I_k$ by the list scheduling algorithm. Since $\left\lceil \sum_{j\in E} \ell_j/n \right\rceil \leq \mathrm{MB}((\ell_j - \mu_j), E)$ and $\max_{j\in E}(\ell_j) \leq \mathrm{MB}((\ell_j - \mu_j), E)$, we obtain a 2-approximation.

Finally, note that for the special case without multiplicities ($l_j = 1$, $\mu_j = 0$ for $j \in E$), then $\mathrm{MB}((\ell_j - \mu_j), E) = \lceil |E|/n \rceil$. More generally, if $(\ell_j - \mu_j)_{j\in E}$ are constant equal to C, then $\mathrm{MB}((\ell_j - \mu_j), E) = C \lceil |E|/n \rceil$.

3.2. SRFR with random errors

In Theorem 2.3, we show that if we consider $L \geq N + D - 1 + 2\hat{\tau}$ we can uniquely reconstruct solutions of SRFRwE (Definition 2.2). In the following, we consider a scenario of SRFRwE with random errors, with the purpose of proving uniqueness results with a lower modulus degree. This scenario was already presented in coding theory and it is related to the decoding of Interleaved Reed Solomon (IRS) codes [BKY03, BMS04]. We can found an extension of these techniques to SRFRwE (without poles and multiplicities) in [GLZ19, GLZ21]. Here, we revisit these results in the more general context of multiprecision interpolation.

In the following remark, we recall some results about the decoding of IRS codes and clarify the link with our generalized problem.

Remark 3.1. In the previous section we have introduced a technique for solving the sRFRwE problem, based on the resolution of the key equations (3), with degree constraints (4).

We briefly recall that an IRS codeword is the multipoint evaluation of a vector of polynomials of bounded degrees. Decoding an IRS codes consists in reconstructing a vector of polynomials by its evaluations, some of which erroneous. We can observe that sRFRwE is a generalization of this decoding problem: if $v_j = 0$ (no poles), $l_j = 1$ (no multiplicities) and $d(x) = 1$ it consists in reconstructing a vector of polynomials, given its evaluations where some could be erroneous. Our resolution technique based on the key equations resolution

generalizes the interpolation-based decoding technique for IRS codes [BW86], which is based on a Cauchy interpolation. For this specific case, Theorem 2.3 tells us that we can uniquely decode IRS codewords (of an IRS code of length L and dimension N) when $L \geq N + 2\tau_0$, *i.e.* up to $\tau_0 := \left\lfloor \frac{L-N}{2} \right\rfloor$ errors which is also called *unique decoding radius*. But, the interleaved structure of these codes allows us to correct beyond τ_0, or equivalently to reduce the number of evaluations, if the errors are uniformly distributed. Thus, our goal in this section is to reduce the modulus degree of Theorem 2.3, by applying and revisiting the techniques related to the decoding of IRS to our more general case.

We start by analyzing the possible errors that we could have in our problem. Given $(v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda}$, we divide the error support

$$E = \{j | (x - \alpha_j)^{v_j} \boldsymbol{f} \neq \boldsymbol{r}_j g \bmod (x - \alpha_j)^{\ell_j}\}$$

into the *valuation errors*

$$E_v := \{j \mid v_j \neq \min(\mathrm{val}_{\alpha_j}(g), \ell_j)\}$$

and the remaining *evaluation errors*

$$E_r = \{j \mid (v_j = \mathrm{val}_{\alpha_j}(g) < \ell_j) \text{ and } \left((x - \alpha_j)^{v_j} \boldsymbol{f}/g \neq \boldsymbol{r}_j \bmod (x - \alpha_j)^{\ell_j - v_j}\right)\}.$$

Proposition 3.2. $E = E_v \sqcup E_r$.

Proof. Our plan to prove the proposition is to separate the evaluation index j into four cases, and to prove the equality $E = E_v \sqcup E_r$ for each case.

If $v_j = \min(\mathrm{val}_{\alpha_j}(g), \ell_j) = \ell_j$ then j belongs to no error support.

In the case where $v_j = \min(\mathrm{val}_{\alpha_j}(g), \ell_j) < \ell_j$, then $v_j = \mathrm{val}_{\alpha_j}(g) < \ell_j$. In this case, $j \in E \Leftrightarrow j \in E_r$ because $(x - \alpha_j)^{v_j} \boldsymbol{f} \neq \boldsymbol{r}_j g \bmod (x - \alpha_j)^{\ell_j}$ is equivalent to $(x - \alpha_j)^{v_j} \boldsymbol{f}/g \neq \boldsymbol{r}_j \bmod (x - \alpha_j)^{\ell_j - v_j}$.

Suppose that $v_j < \min(\mathrm{val}_{\alpha_j}(g), \ell_j)$. Then $\mathrm{val}_{\alpha_j}(g) > 0$ so $\mathrm{val}_{\alpha_j}(\boldsymbol{f}) = 0$. As a result, $v_j = \mathrm{val}_{\alpha_j}((x - \alpha_j)^{v_j} \boldsymbol{f}) < \mathrm{val}_{\alpha_j}(\boldsymbol{r}_j g)$. Hence, $\mu_j = v_j < \ell_j$. So, in this case, j belongs to both E and E_v.

Finally, assume that $v_j > \min(\mathrm{val}_{\alpha_j}(g), \ell_j)$. It must be that $\mathrm{val}_{\alpha_j}(g) = \min(\mathrm{val}_{\alpha_j}(g), \ell_j) < v_j$. Then $v_j > 0$ so $\mathrm{val}_{\alpha_j}(\boldsymbol{r}_j) = 0$. Consequently, $\mathrm{val}_{\alpha_j}(g) = \mathrm{val}_{\alpha_j}(\boldsymbol{r}_j g) < \mathrm{val}_{\alpha_j}((x - \alpha_j)^{v_j} \boldsymbol{f})$. Thus, $\mu_j = \mathrm{val}_{\alpha_j}(g) < \ell_j$ and j belongs to both E and E_v. □

We can define a variant of Definition 2.2 which also takes into account these new error supports.

Definition 3.3. Given parameters N, D, $\hat{\tau}_v$, $\hat{\tau}_r$, τ_r and an instance $(v_j, \boldsymbol{r}_j)$, find a vector of rational functions $\boldsymbol{y}(x) = \frac{\boldsymbol{f}(x)}{g(x)}$ satisfying the degree constraints $N > \deg(\boldsymbol{f})$, $D > \deg(g)$ and the error bounds $\hat{\tau}_v \geq \sum_{j \in E_v}(\ell_j - \mu_j)$, $\hat{\tau}_r \geq \sum_{j \in E_r}(\ell_j - \mu_j)$, and $\tau_r \geq |E_r|$.

If we do not have a bound $\hat{\tau}_r$, we can always set $\hat{\tau}_r = \sum_{j=1}^{\tau_r} \ell_j$ since the sequence $(\ell_j)_j$ is non increasing. The same goes for $\hat{\tau}_v$ if we have at our disposal of a bound $\tau_v \geq |\bar{E}_v|$.

Going back to our previous discussion, the two error supports E_r and E_v do not play the same role on whether a received instance can be uniquely reconstructed. We will show that for all errors on the valuation error support E_v, and for a certain proportion of errors on the evaluation error support E_r, then the received instance can be uniquely reconstructed.

In order to make the previous framework formal, we will fix two error supports $\bar{E}_v$ and $\bar{E}_r$, and a list of minimal error indices $(\bar{\mu}_j)_{1\leq j\leq \lambda}$ such that there exists an instance $(\bar{v}_j, \bar{\boldsymbol{r}}_j)_{1\leq j\leq \lambda}$ and a vector of rational functions $\boldsymbol{y}(x) = \boldsymbol{f}(x)/g(x)$ which corresponds to $\bar{E}_v$, $\bar{E}_r$ and $(\bar{\mu}_j)$.

We consider the family $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ of received instances $(v_j, \boldsymbol{r}_j)$ such that $v_j = \bar{v}_j$ for all j, $\boldsymbol{r}_j = \bar{\boldsymbol{r}}_j \bmod (x-\alpha_j)^{\ell_j - v_j}$ for $j \notin \bar{E}_r$, and otherwise $\boldsymbol{r}_j = \bar{\boldsymbol{r}}_j \bmod (x-\alpha_j)^{\bar{\mu}_j - v_j}$ for $j \in \bar{E}_r$. Equivalently, $(v_j, \boldsymbol{r}_j) \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ *iff* for all $j \in \bar{E}_r$, there exists $\boldsymbol{e}_j \in \mathbb{F}_q[x]^n$ such that $\boldsymbol{r}_j = \bar{\boldsymbol{r}}_j + \boldsymbol{e}_j(x-\alpha_j)^{\bar{\mu}_j - v_j} \bmod (x-\alpha_j)^{\ell_j - v_j}$.

Yet another description of $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ is based on the coefficients $r_{i,j,k}$ of the k-th vector component $r_{j,k}$ of $\boldsymbol{r}_j$ on the Hasse basis (see Section 2.4), *i.e.*

$$r_{j,k} = \sum_{0\leq i<\ell_j - v_j} r_{i,j,k}(x-\alpha_j)^i \bmod (x-\alpha_j)^{\ell_j - v_j}.$$

Then $r_{ijk} = \bar{r}_{ijk}$ when $j \notin \bar{E}_r$ or when $j \in \bar{E}_r$ and $i < \bar{\mu}_j - v_j$. Moreover, one can enumerate $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ by taking all possible $r_{i,j,k}$ in $\mathbb{F}_q$ for $\bar{\mu}_j - v_j \leq i < \ell_j - v_j$, $j \in \bar{E}_r$, and $1 \leq k \leq n$.

Theorem 3.4. *Following the previous notations, we assume that $\boldsymbol{y}$ is a solution of the problem of Definition 3.3 related to $(\bar{v}_j, \bar{\boldsymbol{r}}_j)$, i.e. that $N > \deg(\boldsymbol{f})$, $D > \deg(g)$, and $\hat{\tau}_v \geq \sum_{j\in\bar{E}_v}(\ell_j - \bar{\mu}_j)$, $\hat{\tau}_r \geq \sum_{j\in\bar{E}_r}(\ell_j - \bar{\mu}_j)$, and $\tau_r \geq |\bar{E}_r|$. Suppose that*

$$L \geq N + D - 1 + 2\hat{\tau}_v + \hat{\tau}_r + \mathrm{MB}(\boldsymbol{\ell}, [\![1, \tau_r]\!])$$

where $[\![1,\tau_r]\!] := \{1,\ldots,\tau_r\}$. Let $(v_j, \boldsymbol{r}_j)$ is a uniformly distributed random instance in $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$.

Then $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i<\delta_{N+\hat{\tau},D+\hat{\tau}}}$ with probability at least $1 - \frac{D+\hat{\tau}}{q}$ (for $\delta_{N+\hat{\tau},D+\hat{\tau}}$ defined as in (6)).

Note that $\hat{\tau} := \hat{\tau}_r + \hat{\tau}_v$ is a bound on the degree of the error locator of any $(v_j, \boldsymbol{r}_j)$ defined of Theorem 3.4. Indeed, when $(v_j, \boldsymbol{r}_j) \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$, the valuation error supports E_r of $(v_j, \boldsymbol{r}_j)$ and $\bar{E}_r$ of $(\bar{v}_j, \bar{\boldsymbol{r}}_j)$ coincide. However, the evaluation error supports are only contained, *i.e.* $E_v \subset \bar{E}_v$, since $\mu_j \geq \bar{\mu}_j$ for $j \notin E_r$.

Proof. Since $\boldsymbol{y}$ is a solution of the problem of Definition 3.3 for $(\bar{v}_j, \bar{\boldsymbol{r}}_j)$, then $\boldsymbol{y}$ is also a solution of the same problem for any $(v_j, \boldsymbol{r}_j) \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$. Therefore $\Lambda\boldsymbol{f}, \Lambda g$ is always a solution in $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ and we always have that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \subseteq \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i<\delta_{N+\hat{\tau},D+\hat{\tau}}}$.

The proof is based on the following two steps:

1. show that there exists a draw $(v_j, \boldsymbol{w}_j)$ in $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ for which the corresponding solution space $\mathcal{S}_{\boldsymbol{w},N+\hat{\tau},D+\hat{\tau}} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \le i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$. We only need to prove the inclusion $\subseteq$ since the other inclusion $\supseteq$ is always verified;
2. derive an upper bound on the probability of the event $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \neq \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \le i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$.

1. Consider a partition of the error support $\bar{E}_r = \sqcup_{k=1}^{n} I_k$ which achieves the optimal multiplicity balancing (see Section 3.1). Therefore, for any $1 \le k \le n$, we get that $\sum_{j \in I_k} (\ell_j - \bar{\mu}_j) \le \mathrm{MB}((\ell_j - \bar{\mu}_j), \bar{E}_r)$. For any $j \in \bar{E}_r$, we denote by k_j the unique index such that $j \in I_{k_j}$.

Remember that all $(v_j, \boldsymbol{r}_j) \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ coincide when $j \notin \bar{E}_r$. So we only need to set $\boldsymbol{w}_j$ for $j \in \bar{E}_r$. Actually, for all $j \in \bar{E}_r$, we want to set $\boldsymbol{w}_j \in \mathbb{F}_q[x]^n$ such that $(x-\alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{w}_j g = \boldsymbol{\varepsilon}_{k_j} (x-\alpha_j)^{\bar{\mu}_j}$ where $\boldsymbol{\varepsilon}_i$ is the ith element of the canonical basis of $\mathbb{F}_q^n$. We need to show that such a $\boldsymbol{w}_j$ exists. Since $\bar{\mu}_j$ is the minimal error index of $\bar{\boldsymbol{r}}_j$, we have that $\bar{\mu}_j \ge v_j = \mathrm{val}_{\alpha_j}(g)$. Therefore, $\boldsymbol{w}_j := ((x-\alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{\varepsilon}_{k_j} (x-\alpha_j)^{\bar{\mu}_j})/g$ is a vector of polynomials that suits our needs. Note that for $j \notin \bar{E}_r$, $(x-\alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{w}_j g = \boldsymbol{0} \bmod (x-\alpha_j)^{\bar{\mu}_j}$.

Fix $(\boldsymbol{\varphi}, \psi) \in \mathcal{S}_{\boldsymbol{w},N+\hat{\tau},D+\hat{\tau}}$. Our first goal is to prove that $\boldsymbol{p}(x) = \boldsymbol{0}$ where $\boldsymbol{p}(x) := \psi(x)\boldsymbol{f}(x) - g(x)\boldsymbol{\varphi}(x)$. For $j \notin \bar{E}_r$, we combine the key equations and the equations satisfied by $\boldsymbol{w}_j$:

$$\begin{cases} (x-\alpha_j)^{v_j} \boldsymbol{\varphi} &= \boldsymbol{w}_j \psi \mod (x-\alpha_j)^{\ell_j} \\ (x-\alpha_j)^{v_j} \boldsymbol{f} &= \boldsymbol{w}_j g \mod (x-\alpha_j)^{\bar{\mu}_j} \end{cases}.$$

We multiply the first equation by g, so it reaches precision $(x-\alpha_j)^{\ell_j + \mathrm{val}_{\alpha_j}(g)}$. We multiply the second equation by ψ, which must be a multiple of $(x-\alpha_j)^{v_j}$, so it becomes an equation modulo $(x-\alpha_j)^{\bar{\mu}_j + v_j}$. From $(x-\alpha_j)^{v_j} \Lambda \boldsymbol{f} = \boldsymbol{w}_j \Lambda g \bmod (x-\alpha_j)^{\ell_j}$, we get that $(x-\alpha_j)^{v_j}$ divides Λg. As a result, $v_j + \bar{\mu}_j \le \ell_j + \mathrm{val}_{\alpha_j}(g)$, so we get

$$\begin{aligned} (x-\alpha_j)^{v_j} (\boldsymbol{\varphi} g - \boldsymbol{f} \psi) &= \boldsymbol{0} \bmod (x-\alpha_j)^{v_j + \bar{\mu}_j} \\ (\boldsymbol{\varphi} g - \boldsymbol{f} \psi) &= \boldsymbol{0} \bmod (x-\alpha_j)^{\bar{\mu}_j}. \end{aligned} \tag{9}$$

Now, for $j \in \bar{E}_r$, we combine the key equations and the equations defining $\boldsymbol{w}_j$:

$$\begin{cases} (x-\alpha_j)^{v_j} \boldsymbol{\varphi} &= \boldsymbol{w}_j \psi \mod (x-\alpha_j)^{\ell_j} \\ (x-\alpha_j)^{v_j} \boldsymbol{f} &= \boldsymbol{w}_j g + \boldsymbol{\varepsilon}_{k_j} (x-\alpha_j)^{\bar{\mu}_j} \mod (x-\alpha_j)^{\ell_j} \end{cases}.$$

By a similar reasoning about precisions, we obtain

$$\begin{aligned} (x-\alpha_j)^{v_j} (\boldsymbol{\varphi} g - \boldsymbol{f} \psi) &= \boldsymbol{\varepsilon}_{k_j} (x-\alpha_j)^{\bar{\mu}_j} \psi \mod (x-\alpha_j)^{v_j + \ell_j} \\ (\boldsymbol{\varphi} g - \boldsymbol{f} \psi) &= \boldsymbol{\varepsilon}_{k_j} (x-\alpha_j)^{\bar{\mu}_j} (\psi/(x-\alpha_j)^{v_j}) \mod (x-\alpha_j)^{\ell_j}. \end{aligned}$$

Note that $(x-\alpha_j)^{v_j}$ divides ψ, so $\mathrm{val}_{\alpha_j}(\boldsymbol{\varphi} g - \boldsymbol{f} \psi) \ge \bar{\mu}_j$. Let us fix k and look at the k-th component p_k of $\boldsymbol{p}$. We have shown before that

$$\mathrm{val}_{\alpha_j}(p_k) \ge \begin{cases} \ell_j & \text{if } j \notin E \\ \bar{\mu}_j & \text{if } j \in \bar{E}_v \\ \ell_j & \text{if } j \in \bar{E}_r \setminus I_k \\ \bar{\mu}_j & \text{if } j \in I_k \subset \bar{E}_r \end{cases}.$$

Therefore, p_k is zero modulo a polynomial of degree

$$L - \sum_{j \in \bar{E}_v} (\ell_j - \bar{\mu}_j) - \sum_{j \in I_k} (\ell_j - \bar{\mu}_j) \geq L - \sum_{j \in \bar{E}_v} (\ell_j - \bar{\mu}_j) - \mathrm{MB}((\ell_j - \bar{\mu}_j), \bar{E}_r).$$

On the other hand, $\deg(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) < \mathcal{L}_{\mathrm{RFR}}(N + \hat{\tau}, D + \hat{\tau})$ which is less than or equal to the previous modulus degree. Therefore $p_k = 0$ and $\boldsymbol{p} = \mathbf{0}$.

We can now conclude this first part of the proof by showing that $\mathcal{S}_{\boldsymbol{w},N+\hat{\tau},D+\hat{\tau}} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$.

Since $\boldsymbol{\varphi} g - \boldsymbol{f}\psi = \mathbf{0}$ and $\gcd(\gcd_i(f_i), g) = 1$ then there exists $P \in \mathbb{F}_q[x]$ such that $(\boldsymbol{\varphi}, \psi) = (P\boldsymbol{f}, Pg)$. The key equations $(x - \alpha_j)^{v_j} \boldsymbol{\varphi} = \boldsymbol{r}_j \psi \bmod (x - \alpha_j)^{\ell_j}$ yield $P((x - \alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{r}_j g) = \mathbf{0} \bmod (x - \alpha_j)^{\ell_j}$ for all j.

We use the fact that $\mu_j = \mathrm{val}_{\alpha_j}((x - \alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{r}_j g)$ and the equivalence $(\mu_j < \ell_j) \Leftrightarrow (j \in E)$ to obtain that $P = 0 \bmod (x - \alpha_j)^{\ell_j - \mu_j}$ for $j \in E$. This means that there exists $Q \in \mathbb{F}_q[x]$ such that $P = \Lambda Q$. Finally, $(\boldsymbol{\varphi}, \psi) = Q(\Lambda \boldsymbol{f}, \Lambda g)$ and the degree constraints on $(\boldsymbol{\varphi}, \psi)$ imply that $\deg(Q) < \delta_{N+\hat{\tau},D+\hat{\tau}}$ which concludes this part of the proof.

2. We now conclude the proof by bounding the probability of the event $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \neq \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$. In this last part of the proof we denote $\delta_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} := \delta_{N+\hat{\tau},D+\hat{\tau}}$ and the error locator $\Lambda := \Lambda_{\boldsymbol{r}}$ to underline the dependency to $\boldsymbol{r}_j$.

Recall that for all $(v_j, \boldsymbol{r}_j) \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$, the minimal error indices μ_j of $\boldsymbol{r}_j$ and $\bar{\mu}_j$ of $\bar{\boldsymbol{r}}_j$ coincide, except for $j \notin E_r$ where $\mu_j \geq \bar{\mu}_j$. This means that the error locator $\Lambda_{\boldsymbol{r}}$ corresponding to $\boldsymbol{r}_j$ divides the error locator $\Lambda_{\bar{\boldsymbol{r}}}$ of $\bar{\boldsymbol{r}}_j$. Hence, the $\delta_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} := \min(N + \hat{\tau} - \deg(\boldsymbol{f}), D + \hat{\tau} - \deg(g)) - \deg(\Lambda_{\boldsymbol{r}})$ related to $\boldsymbol{r}_j$ is greater than or equal to $\delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}}$ which is related to $\bar{\boldsymbol{r}}_j$.

So, for all $(v_j, \boldsymbol{r}_j) \in \mathbb{F}_{\bar{v},\bar{\boldsymbol{r}}}$, we have that (see Section 2.4)

$$\delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}} \leq \delta_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \leq \dim \mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \dim \ker M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}.$$

We will now show that the probability that a uniformly distributed random $(v_j, \boldsymbol{r}_j)$ in $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ satisfy $\dim \ker M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \leq \delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}}$ is lower bounded by $1 - D + \hat{\tau}/q$. This will conclude the proof.

By the Rank-Nullity Theorem, the rank of $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ plus the dimension of its kernel is equal to the dimension of its domain, so $\mathrm{rank}(M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}) \leq nN + \hat{\tau} + D + \hat{\tau} - \delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}} =: \rho$.

On the other hand, as proved above, there exists a draw $(\boldsymbol{w}_j)_{j \in \bar{E}_r}$ of $(\boldsymbol{r}_j)_{j \in \bar{E}_r}$, such that $\mathrm{rank}(M_{\boldsymbol{w},N+\hat{\tau},D+\hat{\tau}}) = \rho$. This means that there exists a nonzero ρ-minor in $M_{\boldsymbol{w},N+\hat{\tau},D+\hat{\tau}}$. We consider the same nonzero ρ-minor in $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ as a multivariate polynomial C whose indeterminates are $(r_{i,j,k})_{\bar{\mu}_j - v_j \leq i < \ell_j - v_j, j \in \bar{E}_r, 1 \leq k \leq n}$. We remark that we show the existence of a draw $(\boldsymbol{w}_j)_{j \in \bar{E}_r}$ of $(\boldsymbol{r}_j)_{j \in \bar{E}_r}$, such that $C(\boldsymbol{w}_j)$ is nonzero. Hence, the polynomial C is nonzero. For any matrix $\boldsymbol{r}$ such that $(\boldsymbol{r}_j)_{j \in \bar{E}_r}$ is not a root of C, then $\mathrm{rank}(M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}) \geq \rho$, so $\dim \ker M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \leq \delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}}$.

Note that the total degree of the polynomial C is at most $D+\hat{\tau}$, since only the last $D+\hat{\tau}$ columns of the matrix $M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ contain the variables $(r_{i,j,k})_{j\in\bar{E}_r}$ with total degree 1 (see Section 2.4). Finally, the polynomial C cannot vanish in more than a $D+\hat{\tau}/q$-fraction of its domain by the Schwartz-Zippel Lemma. □

Remark 3.5. We can prove a more general version of the theorem, useful for a possible extension of this result to an early termination setting as in [GLZ21, Section 4].

Let $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta}$ be the solution set of equation (9) with degree constraints $\deg(\boldsymbol{\varphi}) < \nu, \deg(\psi) < \vartheta$. Then $(x^i\Lambda\boldsymbol{f}, x^i\Lambda g)$ still belongs to $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta}$ provided that $i < \delta_{\nu,\vartheta}$ where $\delta_{\nu,\vartheta} := \min(\nu - \deg(\boldsymbol{f}), \vartheta - \deg(g)) - \deg(\Lambda)$.

Then, the proof of Theorem 3.4 can be easily adapted to show that $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\le i<\delta_{\nu,\vartheta}}$ with probability at least $1-\frac{\vartheta}{q}$ whenever $L \ge \max(N+\vartheta, D+\nu) - 1 + \hat{\tau}_v + \mathrm{MB}(\boldsymbol{\ell}, [\![1,\tau_r]\!])$.

4. Conclusion

In this paper we present a multiprecision evaluation approach for the vector rational reconstruction with errors. This is a complete setting that extends recent literature on the subject, handling poles of certain orders and removing the hypothesis on the characteristic of the field. Moreover, we adapt the analysis of simultaneous rational function reconstruction for random error in this new scenario, providing condition of uniqueness applying interleaving techniques and an estimation of the probability failure.

References

[BK14] B. Boyer and E. Kaltofen. Numerical Linear System Solving with Parametric Entries by Error Correction. In *Proceedings of SNC'14*, 2014.

[BKY03] D. Bleichenbacher, A. Kiayias, and M. Yung. Decoding of interleaved Reed-Solomon codes over noisy data. In *Proceedings of ICALP'03*, 2003.

[BMS04] A. Brown, L. Minder, and A. Shokrollahi. Probabilistic decoding of Interleaved RS-Codes on the Q-ary symmetric channel. In *Proceedings of ISIT'04*, 2004.

[BW86] E. R. Berlekamp and L. R. Welch. Error Correction of Algebraic Block Codes, U.S. Patent 4 633 470, Dec. 1986.

[CEC+13] Jr. Coffman, G. Edward, J. Csirik, G. Galambos, S. Martello, and D. Vigo. Bin Packing Approximation Algorithms: Survey and Classification. In Panos M. Pardalos, Ding-Zhu Du, and Ronald L. Graham, editors, *Handbook of Combinatorial Optimization*, pages 455 – 531. Springer, 2013.

[Cox20] N. Coxon. Fast Hermite interpolation and evaluation over finite fields of characteristic two. *Journal of Symbolic Computation*, 98:270 – 283, 2020.

[Fit95] P. Fitzpatrick. On the key equation. *IEEE Transactions on Information Theory*, 41(5):1290 – 1302, 1995.

[GG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013.

[GLZ19] E. Guerrini, R. Lebreton, and I. Zappatore. Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes. In *Proceedings of ISIT'19*, 2019.

[GLZ21] E. Guerrini, R. Lebreton, and I. Zappatore. Polynomial linear system solving with random errors: New bounds and early termination technique. In *Proceedings of ISSAC'21*, page 171 – 178, 2021.

[Gra66] R.L. Graham. Bounds for certain multiprocessing anomalies. *The Bell System Technical Journal*, 45(9):1563 – 1581, 1966.

[GW11] V. Guruswami and C. Wang. Optimal rate list decoding via derivative codes. In Leslie Ann Goldberg, Klaus Jansen, R. Ravi, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 593 – 604, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[KPSW17] E. Kaltofen, C. Pernet, A. Storjohann, and C. Waddell. Early Termination in Parametric Linear System Solving and Rational Function Vector Recovery with Error Correction. In *Proceedings of ISSAC'17*, 2017.

[KPY20] E. L Kaltofen, C. Pernet, and Z. Yang. Hermite rational function interpolation with error correction. 12291, 2020.

[KSY14] S. Kopparty, S. Saraf, and S. Yekhanin. High-rate codes with sublinear-time decoding. 61(5), 2014.

[KY13] E. L. Kaltofen and Z. Yang. Sparse multivariate function recovery from values with noise and outlier errors. In *Proceedings of ISSAC'13*, 2013.

[KY14] E. L. Kaltofen and Z. Yang. Sparse multivariate function recovery with a high error rate in the evaluations. In *Proceedings of ISSAC'14*, 2014.

[Nie13] J.S.R. Nielsen. Generalised Multi-sequence Shift-Register synthesis using module minimisation. In *Proceedings of ISIT'13*, pages 882 – 886, 2013.

[OS07] Z. Olesh and A. Storjohann. The Vector Rational Function Reconstruction problem. In *Proceedings of the Waterloo Workshop*. World Scientific, 2007.

[Per14] C. Pernet. *High Performance and Reliable Algebraic Computing*. Habilitation à diriger des recherches, Université Joseph Fourier, Grenoble 1, 2014.

[RS16] J. Rosenkilde and A. Storjohann. Algorithms for simultaneous padé approximations. In *Proceedings of ISSAC'2016*, 2016.

[SSB07] G. Schmidt, V. Sidorenko, and M. Bossert. Enhancing the Correcting Radius of Interleaved Reed-Solomon Decoding using Syndrome Extension Techniques. In *Proceedings of ISIT'07*, 2007.