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 methods for interpolating rational functions from their evaluations, in the context of erroneous evaluations. This problem can be seen 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 and multiprecision evaluations. From an error correcting codes point of view, this problem is related to the decoding of some algebraic codes such as Reed-Solomon, Derivatives or Multiplicity 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

This paper deals with interpolation methods for reconstructing a vector of rational functions, in presence of erroneous data. We present an extension of this problem, meaning that for any evaluation point, we have more 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, when some errors occur. We start by presenting the problem in its more general form.

*This research work is supported by ANR-21-CE39-0009-BARRACUDA and ANR-21-CE39-0006-SANGRIA.

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)

Vector Rational Function Reconstruction. The Vector Rational Function Reconstruction (VRFR) is the problem of reconstructing a vector of *reduced* rational functions $\boldsymbol{f}/\boldsymbol{g} = (f_1/g_1, \ldots, f_n/g_n) \in \mathbb{F}_q(x)^n$, given some polynomials a_k, the remainders $r_k = f_k/g_k \bmod a_k$, and bounds on the degrees of the numerators and the denominators.

The VRFR problem generalizes the *Cauchy interpolation* problem, obtained by taking $a_1 = \cdots = a_n = \prod_{j=1}^{\lambda}(x - \alpha_j)$ for some distinct $\alpha_j \in \mathbb{F}_q$, since in this case the modular equations become equations on the evaluations $r_k(\alpha_j) = f_k(\alpha_j)/g_k(\alpha_j)$.

We call *Simultaneous Rational Function Reconstruction* (SRFR) the special case of VRFR where all the rational functions share the same denominator, *i.e.* $g_1 = \cdots = g_n = g \in \mathbb{F}_q[x]$ and $\gcd(\gcd(f_i), g) = 1$.

We now focus on the homogeneous linear system associated to SRFR (see Definition 2.6) — where the unknowns are the coefficients of $\boldsymbol{f}$ and g. The common denominator in SRFR implies that we have fewer unknowns than the general VRFR problem, so fewer equations are potentially needed to solve the problem. In the interpolation version of the problem, this is directly related to the number λ of evaluation points needed to interpolate $\boldsymbol{f}/g$ (while in the general version of SRFR it coincides with the degree of the polynomials a_k's). However, if we reduce λ, the uniqueness of the solution (as a vector of rational functions) is no longer guaranteed.

We can learn more on that by looking at the coding theory literature, for instance at the collaborative decoder for Interleaved Reed-Solomon codes [BKY03, SSB07, SVM09]. This decoder performs an SRFR: it has to recover a vector of rational functions sharing the same denominator, namely the *error locator polynomial*. Since the number of evaluation points is reduced (by exploiting the common denominator of SRFR), the decoder can fail and one has to bound this probability failure. In case of success, the vector of rational functions returned by the decoder reduces to a vector of polynomials corresponding to the vector of sent messages.

An extension of the decoder of Interleaved Reed-Solomon codes is provided in [GLZ19, GLZ21], dealing with the case where the solution does not reduce to vector of polynomials — it remains a vector of rational functions.

In this paper we go further in the generalization of SRFR in order to handle multiprecision evaluations and poles of the vector of rational functions that we want to recover. In particular, we focus on SRFR with $a_1 = \ldots = a_n = \prod(x-\alpha_j)^{\ell_j}$ for some positive integers ℓ_j's, called *precision* of the reconstruction. This is a more general setting than the interpolation case, corresponding to a more general notion of evaluation called *multiprecision evaluation*. In the following paragraph, we focus on this notion.

Multiprecision evaluation and poles. Cauchy interpolation is the problem of recovering $\boldsymbol{f}/g$ from its evaluations $\boldsymbol{f}(\alpha_j)/g(\alpha_j)$ at distinct evaluation points, with the restriction that $g(\alpha_j) \neq 0$. Notice that this extends the Lagrange interpolation (where $\deg(g) = 0$) to the rational function case. However, we

can learn more information from an evaluation point α_j if we also consider a precision $\ell_j \geq 1$, *i.e.* by computing $\boldsymbol{r}_j(x) = \boldsymbol{f}(x)/g(x) \bmod (x-\alpha_j)^{\ell_j}$. We refer to this approach as *multiprecision evaluation*. Taylor formula states that knowing $\boldsymbol{r}_j$ is equivalent to knowing the evaluation at α_j's of $\boldsymbol{f}/g$ and of its derivatives $(\boldsymbol{f}/g)^{(i)}$ for $i < \ell_j$ (assuming a sufficiently large field characteristic).

In the polynomial case (*i.e.* $\deg(g) = 0$ and $n = 1$), we can recover f from its multiprecision evaluation by Hermite interpolation. In [KPY20] we can find a generalization that can handle rational functions and *errors* (see the following paragraph for more details on the *interpolation with errors* problem).

We cannot evaluate $\boldsymbol{f}(x)/g(x) \bmod (x-\alpha_j)^{\ell_j}$ when α_j is a pole of $(\boldsymbol{f}/g)$ (*i.e.* $g(\alpha_j) = 0$) — in this case $g(x)$ is not invertible modulo $(x-\alpha_j)^{\ell_j}$. A first approach to overcome this problem is to set the evaluation $\boldsymbol{r}_j = (\boldsymbol{f}/g)(\alpha_j)$ to a new symbol ∞ when $g(\alpha_j) = 0$ and $\ell_j = 1$. To the best of our knowledge, this approach was first introduced in [KY13, KY14] in the context of sparse polynomial interpolation. For dense polynomial interpolation (which is the context of this paper), in [Per14], Cauchy interpolation is extended to handle poles even in case of errors, but without multiprecision ($\ell_j = 1$ for all j). This technique is further extended in [KPY20] to recover a rational function from a multiprecision evaluation, except on poles, *i.e.* $\ell_j = 1$ when $g(\alpha_j) = 0$.

In this paper, we propose a new definition of multiprecision evaluation of a rational function $\boldsymbol{f}/g$ that also captures the case of *poles with their orders* (Definition 2.1). We circumvent the poles problem by multiplying the rational function by an *appropriate* power of $(x-\alpha_j)$ such that α_j is not a pole of the resulting rational function.

Comparing to [KPY20], we do not have to treat here separately the evaluation points which are poles. Indeed, we give a more unified framework in this paper: any evaluation point is handled by using the same technique. We then define in Section 2.1 the interpolation problem related to multiprecision evaluation.

Interpolation with errors. In this paper we deal with SRFR with errors: we assume that some evaluations may be *erroneous*, *i.e.* there exists α_j for which $\boldsymbol{r}_j(x) \neq \boldsymbol{f}(x)/g(x) \bmod (x-\alpha_j)^{\ell_j}$. We now consider the case without multiplicities ($\ell_j = 1$ for all j). In this case, one could still hope to recover the rational functions vector by considering some additional evaluations using error correcting codes decoding techniques. To the best of our knowledge, the first attempt in this direction is done by [Per14, Section 2.3.2], where the problem is defined in terms of *rational codes*. A rational code can be seen as an extension of a Reed-Solomon code [RS60], where codewords are evaluations of rational functions (of bounded degrees) instead of polynomials. Decoding can be performed by an algorithm which extends Welch-Berlekamp method [WB86] for Reed-Solomon codes. An important point is that the Welch-Berlekamp key equation must be modified in order to handle possible poles of the rational functions [Per14]. Decoding rational codes is, in this sense, a first important case of SRFR with Errors and poles (SRFRwE).

An extension of rational codes to multiprecision evaluation is presented in

[KPY20]. They call Hermite interpolation with errors the related decoding problem. This can be seen as an extension of derivatives codes [GW11] for rational functions instead of polynomials. In this paper, we remove the assumption of a large field characteristic of [KPY20] by using Hasse derivatives [Has36]. This is a classical strategy to remove the characteristic's assumption, used repeatedly in coding theory [RJ97, O'S00, KP04, KSY14].

The goal of interpolation with errors problems (related to polynomials, rational functions or their vector versions) is to provide a condition on problem's inputs that guarantees that the interpolant is unique. For this purpose, [RS60, Per14, BK14, KSY14, KPY20] give the number of extra evaluation points that are required to correct up to a certain number of errors. However, in the context of collaborative decoding of Reed-Solomon codes, [BKY03, SSB07, SVM09] have shown that one can add fewer evaluation points and correct *almost all* errors, or equivalently random errors with high probability, using interleaving techniques. Recently, we showed how to adapt the interleaving techniques to SRFRwE but without handling poles [GLZ19, GLZ21]. Here, we extend these techniques to a multiprecision setting, handling multiplicities and poles. As in [GLZ21], some error patterns could lead to a non-unique interpolant, making the reconstruction of the solution infeasible. We provide an upper bound on the number of such troublesome errors.

Context and applications. Evaluation interpolation is a central technique in computer algebra. It is used for instance to counteract the phenomenon of intermediate expression swell which occurs when working over *e.g.* $\mathbb{Z}$ or $\mathbb{F}_q[x]$ (see for instance [GG13, Section 5]).

The present paper is an extension of [GLZ21], in which the evaluation interpolation technique is used to solve polynomial linear systems $A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x)$ (PLS), *i.e.* linear systems with univariate polynomial coefficients, where $A(x)$ is full rank and $\boldsymbol{b}(x)$ is a vector. An important feature of the PLS problem is that its solution $\boldsymbol{y}(x) = \boldsymbol{f}(x)/g(x)$ is a vector of rational functions with the same denominator (by Cramer's rule).

We recall that the evaluation interpolation technique can be used for a *parallel* resolution of PLS. Consider a network of λ computing nodes whose j-th node evaluates $A(\alpha_j)$ and $\boldsymbol{b}(\alpha_j)$ and solves the evaluated system $\boldsymbol{r}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$. All the nodes then send $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_\lambda$ to a main node which finally performs a simultaneous rational function reconstruction to recover the solution $\boldsymbol{y}(x)$.

An important generalization of this PLS solving technique asks the j-th computing node to lift the evaluated solution $A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$ at a precision ℓ_j, *i.e.* to compute $\boldsymbol{r}_j(x) = \boldsymbol{y}(x) \bmod (x-\alpha_j)^{\ell_j}$. In the special case of $\lambda = 1$, this method is due to [MC79, Dix82] and it is based on Hensel's Lemma, which is closely related to Newton-Raphson iteration. Still when $\lambda = 1$, it improves the complexity with respect to evaluation interpolation but can not be parallelized. For a general λ, this method combines the advantages of both approaches (see [CS05] for the integer case).

So, the main node has to recover $\boldsymbol{y}(x) = \boldsymbol{f}(x)/g(x)$ from multiprecision evaluations $\boldsymbol{r}_j(x) = \boldsymbol{y}(x) \bmod (x-\alpha_j)^{\ell_j}$ — this amounts to solving an SRFR

problem. The sum of multiprecisions $L = \sum_{j=1}^{\lambda} \ell_j$ is a parameter of great importance. On one hand, if the main node chooses an L which is too small, it may not be able to recover $\boldsymbol{y}(x)$ because the SRFR problem's solution is not unique. On the other hand, if L is unnecessarily high, the computing network performs superfluous computations.

The hybrid PLS resolution method presented above requires that the evaluation point α_j is not a pole of the solution $\boldsymbol{y}(x)$, so that $A(\alpha_j)$ would be invertible. The starting point of this paper is the remark that the j-th computing node could still learn the *valuation* of $\boldsymbol{y}(x)$ at the point α_j and the first terms of its Laurent series expansion, using techniques similar to [DSV00] in the integer case. In this scenario, the main node has to recover $\boldsymbol{y}(x)$ from a generalized *multiprecision evaluation with poles* (see Definition 2.1).

Polynomial linear system solving with errors. As in [GLZ21], this paper focuses on a scenario in which the computing nodes could make errors, possibly computing $\boldsymbol{r}_j(x) \neq \boldsymbol{y}(x) \bmod (x-\alpha_j)^{\ell_j}$. We call Polynomial Linear System solving with Errors (PLSwE) the problem of recovering $\boldsymbol{y}(x)$ given its multiprecision evaluations, some of which are erroneous [BK14, KPSW17, GLZ19, GLZ21].

As before, the PLS with errors problem can be seen as an instance of an SRFR with errors (SRFRwE, see Section 2.2). This work studies SRFRwE instances leading to uniqueness, which is a central property in the same way that unique decoding algorithms are essential in error correcting codes. Our goal is to minimize the total multiprecision L required to uniquely recover the solution, or equivalently to maximize the bound on the number of errors (*decoding radius*) that we could correct for a given L.

To sum up, the present work extends the results of [GLZ21] on SRFRwE to the setting of a multiprecision evaluation that also allows evaluation points to be poles of the rational function. We leave the corresponding results on PLSwE as a future work.

Outline of the paper. The paper is structured as follows. In Section 2, we present a new setting of SRFR with multiprecision evaluation that can also handle poles. We extend the results of [KPY20] in this setting, removing the assumptions 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 total multiprecision L compared to Section 2.

2. Rational Function Reconstruction with errors

Preliminaries and notations. We start by fixing notations and the setting of this work. Let $\mathbb{F}_q$ be a finite field of order q. We denote by $\mathbb{F}_q[x]_{<d}$ the set of polynomials over $\mathbb{F}_q$ of degree less than d. In this paper, we extensively deal with vectors of polynomials over $\mathbb{F}_q[x]$: we use lowercase bold letters for vectors $\boldsymbol{f} \in \mathbb{F}_q[x]^n$, and we denote 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 the set of *evaluation points*

$\{\alpha_1, \ldots, \alpha_\lambda\}$, where $\alpha_j \in \mathbb{F}_q$ are pairwise distinct. We associate a *multiplicity* $\ell_j \in \mathbb{Z}_{\geq 0}$ to any 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* $\mathrm{val}_{\alpha_j}(f)$ of a nonzero polynomial $f(x)$ at α_j is defined as the maximal integer v such that $(x-\alpha_j)^v$ divides f. By convention, we fix $\mathrm{val}_{\alpha_j}(0) = +\infty$. The valuation can be extended to rational functions $f/g \in \mathbb{F}_q(x)$ by $\mathrm{val}_{\alpha_j}(f/g) := \mathrm{val}_{\alpha_j}(f) - \mathrm{val}_{\alpha_j}(g)$. Therefore, the valuation $\mathrm{val}_{\alpha_j}(f/g)$ is the maximal integer v such that f/g can be written $(x-\alpha_j)^v b$ where $b(x) \in \mathbb{F}_q(x)$ and $b(\alpha_j) \in \mathbb{F}_q \setminus \{0\}$. In particular, if $\mathrm{val}_{\alpha_j}(f/g)$ is negative, then g must vanish at α_j. In this case, $\mathrm{val}_{\alpha_j}(g) = -\mathrm{val}_{\alpha_j}(f/g)$ provided that $\gcd(f,g) = 1$.

In this paper, we often consider valuations of vectors of rational functions $\boldsymbol{f}/g \in \mathbb{F}_q(x)^n$; we define $\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g) = \min_k(\mathrm{val}_{\alpha_j}(f_k/g))$. With this definition, we keep the property that the valuation $\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g)$ is the maximal integer v such that $\boldsymbol{f}/g$ can be written $(x-\alpha_j)^v \boldsymbol{b}$ where $\boldsymbol{b}(x) \in \mathbb{F}_q(x)^n$ and $\boldsymbol{b}(\alpha_j) \neq \boldsymbol{0} \in \mathbb{F}_q^n$.

Finally, we will sometimes assume in this paper that the vectors of rational functions $\boldsymbol{f}/g$ are reduced, meaning that $\gcd(\boldsymbol{f}, g) := \gcd(\gcd_i(f_i), g) = 1$.

We now present our new formal definition of multiprecision evaluation that also handles multiprecision evaluation at poles in a unified setting. The notation $[\![0; \ell_j]\!]$ denotes the set of integers k such that $0 \leq k \leq \ell_j$.

Definition 2.1 (Multiprecision evaluation). We set the evaluation of a reduced fraction $\boldsymbol{f}/g \in \mathbb{F}_q(x)^n$ at α_j at precision ℓ_j to be $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ such that

$$\begin{aligned} v_j &:= \min(\mathrm{val}_{\alpha_j}(g), \ell_j) \\ \boldsymbol{r}_j &:= \boldsymbol{f}/(g/(x-\alpha_j)^{v_j}) \bmod (x-\alpha_j)^{\ell_j - v_j}. \end{aligned}$$

By convention, we set $\boldsymbol{r}_j := \boldsymbol{1}$ when $v_j = \ell_j$.

Remark 2.2. From now on, we consider $\boldsymbol{r}_j$ of degree less than $\ell_j - v_j$ when $v_j < \ell_j$.

Note that $\boldsymbol{r}_j$ is well-defined: if $v_j = \mathrm{val}_{\alpha_j}(g)$, then $g/(x-\alpha_j)^{v_j}$ has valuation 0 at α_j, so it is invertible modulo $(x-\alpha_j)^{\ell_j - v_j}$. Otherwise, if $v_j = \ell_j$, then $\boldsymbol{r}_j$ is defined modulo 1, so any value works.

Remark 2.3. The definition of v_j requires $\gcd(\boldsymbol{f}, g) = 1$; this hypothesis can be lifted by setting $v_j := \min(\ell_j, \max(0, -\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g)))$. Therefore, we stress out that the evaluation $(v_j, \boldsymbol{r}_j)$ depends only on the fraction $\boldsymbol{f}/g$ and not on the choice of representatives of the fraction.

Lemma 2.4. *Let $(v_j, \boldsymbol{r}_j)$ be the multiprecision evaluation at α_j of a vector of rational functions $\boldsymbol{f}/g$, then* $\gcd(\boldsymbol{r}_j, (x-\alpha_j)^{v_j}) = 1$.

Proof. If $v_j = \ell_j$ then $\boldsymbol{r}_j = \boldsymbol{1}$ so the claim follows. We consider now the case $v_j < \ell_j$. We assume w.l.o.g. that the fraction $\boldsymbol{f}/g$ is reduced, *i.e.* that $\gcd(\boldsymbol{f}, g) = 1$.

We distinguish two cases. First, if $\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g) \geq 0$, then $\mathrm{val}_{\alpha_j}(g) = 0$ and so, $v_j = 0$. Otherwise, if $\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g) < 0$, then $\mathrm{val}_{\alpha_j}(g) = -\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g)$ and since $v_j < l_j$, we have that $v_j = \mathrm{val}_{\alpha_j}(g)$. Thus, $\mathrm{val}_{\alpha_j}(\boldsymbol{r}_j) = \mathrm{val}_{\alpha_j}(\boldsymbol{f}/g) + v_j = 0$. So, in both cases $\gcd(\boldsymbol{r}_j, (x-\alpha_j)^{v_j}) = 1$. □

Notice that Definition 2.1 amounts to give the first $\ell_j - v_j$ terms of the formal Laurent series $\mathbb{F}_q((x-\alpha_j))^n$ expansion of the vector $\boldsymbol{f}/g$, and v_j zero coefficients of g ($g = 0 \bmod (x-\alpha_j)^{v_j}$).

2.1. The interpolation problem without errors

In this section, we focus on the problem of interpolating a multipoint evaluation.

Definition 2.5 (Simultaneous RFR with poles). Given,

- a set of $\lambda \geq 1$ evaluation points α_j's with corresponding precisions ℓ_j,
- two positive *degree bounds* $N, D \in \mathbb{Z}_{>0}$,
- for all $1 \leq j \leq \lambda$, $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ with $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$,

we consider the problem of finding $\boldsymbol{f}/g \in \mathbb{F}_q(x)^n$ such that

$$v_j = \min(\ell_j, \max(0, -\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g))), \tag{1}$$

$$\boldsymbol{r}_j = \boldsymbol{f}/(g/(x-\alpha_j)^{v_j}) \bmod (x-\alpha_j)^{\ell_j - v_j} \text{ for } 1 \leq j \leq \lambda, \tag{2}$$

$$\deg(\boldsymbol{f}) < N,\ \deg(g) < D. \tag{3}$$

Link with Cauchy interpolation. If $n = 1$ (no vector), $\ell_j = 1$ (no multiplicity), and $v_j = 0$ (no pole), the simultaneous RFR with poles coincides with the problem of finding a rational function f/g such that $f(\alpha_j)/g(\alpha_j) = r_j$, given $r_j \in \mathbb{F}_q$ and the degree constraints as in Equation (3). Notice that here we are excluding poles of the vector of rational functions. Thus, simultaneous RFR with poles generalizes a classical computer algebra problem, known as *Cauchy interpolation*. Cauchy interpolation, does not always admit a solution. Furthermore, if it does, this solution is *unique* when we consider

$$\lambda \geq \mathcal{L}_{RFR} := N + D - 1 \tag{4}$$

evaluation points [GG13, Section 5.8].

Usually in the literature, we focus on the *weaker version* of the Cauchy interpolation problem, whose goal is to find (f, g) such that $f(\alpha_j) = r_j g(\alpha_j)$, given r_j and the degree constraints as in Equation (3). This problem has the advantage to be linear, and it always admits a nonzero solution when $\lambda = \mathcal{L}_{RFR}$. Furthermore, if $\lambda \geq \mathcal{L}_{RFR}$ (as in Equation (4)) this solution is unique.

Any solution of the Cauchy interpolation problem is also a solution of the weaker version. The converse is not always true. However, it can be proven that the converse becomes true when the solution (f, g) of the weaker version satisfies $\gcd(f, g) = 1$ [GG13, Corollary 5.18].

We now come back to Definition 2.5. As for the Cauchy interpolation, we observe that any solution $\boldsymbol{f}/g$ of simultaneous RFR also satisfies the following *weaker* version.

Definition 2.6 (Weak simultaneous RFR with poles (SRFR)). Given,

- a set of $\lambda \geq 1$ evaluation points α_j's with corresponding precisions ℓ_j,
- two positive *degree bounds* $N, D \in \mathbb{Z}_{>0}$,
- for all $1 \leq j \leq \lambda$, $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ with $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$,

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

$$(x-\alpha_j)^{v_j} \boldsymbol{f} = \boldsymbol{r}_j g \bmod (x-\alpha_j)^{l_j}, \tag{5}$$
$$\deg(\boldsymbol{f}) < N, \ \deg(g) < D. \tag{6}$$

Let $G := \prod_{j=1}^{\lambda} (x-\alpha_j)^{\ell_j}$, and denote $L := \sum_{j=1}^{\lambda} \ell_j = \deg(G)$ the *number of evaluation points* counted with their multiplicities. Using the Chinese Remainder Theorem, we define $\boldsymbol{r} \in \mathbb{F}_q[x]^n_{<L}$ as the unique vector of polynomials such that $\boldsymbol{r} = \boldsymbol{r}_j \bmod (x-\alpha_j)^{\ell_j}$ for any $1 \leq j \leq \lambda$. Similarly, we define $w \in \mathbb{F}_q[x]_{<L}$ so that $w = (x-\alpha_j)^{v_j} \bmod (x-\alpha_j)^{\ell_j}$ for any $1 \leq j \leq \lambda$. Then Equation (2) is equivalent to

$$\boldsymbol{r} = w\boldsymbol{f}/g \bmod G. \tag{7}$$

Remark 2.7. We now observe that our definition of SRFR slightly differs from the literature about this topic. Usually, SRFR refers to the case where $v_j = 0$ and the modulus G (obtained by applying the Chinese Remainder Theorem as in (7)) can be any polynomial in $\mathbb{F}_q[x]$ [OS07, GLZ20]. Despite these ambiguities, we use the same acronym SRFR for this case, to make the notations simple.

As for the Cauchy interpolation, this problem is linear and always admits a nonzero solution, when $nL \leq nN + D - 1$ (in this case, we have more unknowns than equations). On the contrary, the stronger version of Definition 2.5 does not always have a solution. For instance, the Cauchy interpolation counter-example of [GG13, Example 5.19] applies here when $nL = nN + D - 1$ and $n = 1$.

We have the following proposition as in the Cauchy interpolation problem.

Proposition 2.8. *Let $(\boldsymbol{f}, g) \in \mathbb{F}_q[x]^{n+1}$ be a solution of SRFR (Definition 2.6). If $\gcd(\boldsymbol{f}, g) = 1$, then $\boldsymbol{f}/g$ is a solution of simultaneous RFR with poles (cf. Definition 2.5), with the same entries.*

Proof. We want to prove that $\boldsymbol{f}/g$ satisfies all the equations of Definition 2.5. Note that if $\gcd(\boldsymbol{f}, g) = 1$, then $\max(0, -\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g)) = \mathrm{val}_{\alpha_j}(g)$. Therefore, $\min(\ell_j, \max(0, -\mathrm{val}_{\alpha_j}(\boldsymbol{f}/g))) = \min(\ell_j, \mathrm{val}_{\alpha_j}(g))$.

Our goal then is to prove that

$$v_j = \min(\ell_j, \mathrm{val}(g)) =: v'_j \tag{8}$$

Assume for now that it is true. If $v_j < \ell_j$, then $v_j = \mathrm{val}_{\alpha_j}(g)$, and we can divide Equation (5) by g to get Equation (2). Moreover, Equation (2) is always verified when $v_j = \ell_j$.

We now prove the claim of Equation (8). On one hand, $(x-\alpha_j)^{v_j}$ divides both $(x-\alpha_j)^{v_j}\boldsymbol{f}$ and $(x-\alpha_j)^{\ell_j}$, so it divides $\boldsymbol{r}_j g$ by looking at Equation (5). By hypothesis, $\gcd(\boldsymbol{r}_j, (x-\alpha_j)^{v_j}) = 1$ which gives that $(x-\alpha_j)^{v_j}$ divides g and $v_j \leq v'_j$.

On the other hand, notice that $(x-\alpha_j)^{v'_j}$ divides both g and $(x-\alpha_j)^{\ell_j}$, so it divides $(x-\alpha_j)^{v_j}\boldsymbol{f}$. Since $\gcd(\boldsymbol{f}, g) = 1$ and $(x-\alpha_j)^{v'_j}$ divides g, we also have $\gcd(\boldsymbol{f}, (x-\alpha_j)^{v'_j}) = 1$. Therefore, $(x-\alpha_j)^{v'_j}$ must divide $(x-\alpha_j)^{v_j}$ and so $v'_j \leq v_j$. □

We will now show that SRFR admits a unique solution when $L \geq \mathcal{L}_{\mathrm{RFR}}$. This upper bound is coherent with the number of evaluations needed to uniquely reconstruct a solution of the Cauchy Interpolation problem ($\ell_j = 1$ for any j, in which case $L = \lambda$).

Proposition 2.9. *Assume $L \geq \mathcal{L}_{\mathrm{RFR}}$. For any $(\boldsymbol{\varphi}, \psi)$ and $(\boldsymbol{f}, g)$ nonzero solutions of SRFR with the same entries, i.e. satisfying for all $1 \leq j \leq \lambda$,*

$$\begin{cases} (x-\alpha_j)^{v_j}\boldsymbol{\varphi} = \boldsymbol{r}_j\psi \bmod (x-\alpha_j)^{\ell_j} \\ \deg(\boldsymbol{\varphi}) < N, \deg(\psi) < D \end{cases} \quad \begin{cases} (x-\alpha_j)^{v_j}\boldsymbol{f} = \boldsymbol{r}_j g \bmod (x-\alpha_j)^{\ell_j} \\ \deg(\boldsymbol{f}) < N, \deg(g) < D \end{cases}$$

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

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

$$\begin{cases} (x-\alpha_j)^{v_j}\boldsymbol{\varphi} g &= \boldsymbol{r}_j\psi g \bmod (x-\alpha_j)^{\ell_j + \mathrm{val}_{\alpha_j}(g)} \\ (x-\alpha_j)^{v_j}\boldsymbol{f}\psi &= \boldsymbol{r}_j\psi g \bmod (x-\alpha_j)^{\ell_j + \mathrm{val}_{\alpha_j}(\psi)}. \end{cases}$$

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

$$\begin{aligned} & (x-\alpha_j)^{v_j}(\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j + v_j} \\ \iff \quad & (\boldsymbol{\varphi} g - \boldsymbol{f}\psi) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j}. \end{aligned}$$

Let $\boldsymbol{p} := \boldsymbol{\varphi} g - \boldsymbol{f}\psi$. We have that $\boldsymbol{p} = \boldsymbol{0} \mod G$ 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 $\boldsymbol{p} = \boldsymbol{0}$ 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 (5), we have

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

for a given $P \in \mathbb{F}_q[X]$. The polynomial $(x-\alpha_j)^{v_j}$ divides both $(x-\alpha_j)^{v_j}\boldsymbol{f}$ and $(x-\alpha_j)^{\ell_j}P$ because $v_j \leq \ell_j$, so it must divide $\boldsymbol{r}_j g$. Since we have assumed that $\gcd(\boldsymbol{r}_j, (x-\alpha_j)^{v_j}) = 1$, then $(x-\alpha_j)^{v_j}$ divides g and so $\mathrm{val}_{\alpha_j}(g) \geq v_j$. 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 SRFR problem, focusing on a scenario where some errors occur. For this purpose, we start by introducing our error model, we then provide the formal definition of SRFR with errors (and poles) (Definition 2.11), and we finally describe the technique used to solve it.

Note that from now on, for simplicity, we consider reduced vectors of rational functions $\boldsymbol{f}/g$.

Error model. We start by defining what is an *error on an evaluation*. For all $1 \leq j \leq \lambda$, let $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ such that $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$. 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 a vector of 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 for $j \in E$, $\mu_j < \ell_j$. We can extend the definition of μ_j also for correct positions by setting $\mu_j := \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$ for any $1 \leq j \leq \lambda$.

Remark 2.10. In order to state a parallel with the context of error-correcting codes, we consider $(v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda}$ as the received message that we want to correct as $\boldsymbol{f}/g$. For that, first we should define a distance in the space of received messages, which measures the number of errors. The distance should take into account the definition of multiprecision evaluation, and be consistent with the definition of error model. The following definition corresponds to our requirements but is not a proper distance because the objects being compared are not of the same type: on one hand we have a vector of rational functions and on the other hand an evaluation.

We define a *weighted Hamming "distance"*

$$d(\boldsymbol{f}/g, (v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda}) := \sum_{j \in E} (\ell_j - \mu_j)$$

between a vector of rational functions $\boldsymbol{f}/g$ and evaluations $(v_j, \boldsymbol{r}_j)_j$. By definition, this quantity is zero if and only if $\mu_j = \ell_j$ for all j, which is equivalent to $E = \emptyset$. Therefore, the distance is zero if and only if $(\boldsymbol{f}, g)$ is a solution of SRFR for the evaluations $(v_j, \boldsymbol{r}_j)_j$. Note that, in the case of Cauchy interpolation ($n = 1, \ell_j = 1, v_j = 0$), then $d(\boldsymbol{f}/g, (v_j, \boldsymbol{r}_j)_j) = |E|$ is the classical Hamming distance where E simplifies to the set $E = \{j \mid \boldsymbol{f}(\alpha_j) \neq \boldsymbol{r}_j g(\alpha_j)\}$.

We can now define our interpolation with errors problem; starting from any $(v_j, \boldsymbol{r}_j)_j$, our goal is to find a rational function $\boldsymbol{f}/g$ which is close to $(v_j, \boldsymbol{r}_j)_j$ according to our definition of distance.

Definition 2.11 (SRFR with poles and errors (SRFRwE)). Given parameters $N, D \in \mathbb{Z}_{>0}$, $\hat{\tau} \in \mathbb{Z}_{\geq 0}$, and for all $1 \leq j \leq \lambda$, $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ such that $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$, find a vector of rational functions $\boldsymbol{f}(x)/g(x)$ satisfying the degree constraints $N > \deg(\boldsymbol{f})$, $D > \deg(g)$ and the distance bound $\hat{\tau} \geq d(\boldsymbol{f}/g, (v_j, \boldsymbol{r}_j)_j)$.

In a context where the distance between $\boldsymbol{f}/g$ and $(v_j, \boldsymbol{r}_j)_j$ is given by the (non weighted) Hamming distance, *i.e.* if we are looking for $\boldsymbol{f}/g$ such that $\tau \geq |E|$ for a given τ, then $\boldsymbol{f}/g$ is a solution of SRFRwE for $\hat{\tau} := \sum_{j=1}^{\tau} \ell_j$. This is because $d(\boldsymbol{f}/g, (v_j, \boldsymbol{r}_j)_j) = \sum_{j \in E}(\ell_j - \mu_j) \leq \sum_{j=1}^{\tau} \ell_j$, since the sequence of the ℓ_j's is nonincreasing.

Key Equations. We now describe our technique to solve SRFRwE.

We define the *error locator polynomial* $\Lambda := \prod_{j \in E}(x - \alpha_j)^{\ell_j - \mu_j}$. Observe that $\deg(\Lambda) = d(\boldsymbol{f}/g, (v_j, \boldsymbol{r}_j)_j)$ and $\Lambda((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g) = \boldsymbol{0} \bmod (x-\alpha_j)^{\ell_j}$ because $\mu_j = \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$.

Remark that, by definition, $\hat{\tau}$ is a known upper bound on the degree of the error locator, *i.e.* $\hat{\tau} \geq \deg(\Lambda)$. 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*

$$(x-\alpha_j)^{v_j}\boldsymbol{\varphi} = \boldsymbol{r}_j \psi \bmod (x-\alpha_j)^{\ell_j} \text{ for } 1 \leq j \leq \lambda \tag{9}$$

$$\deg(\boldsymbol{\varphi}) < N + \hat{\tau},\ \deg(\psi) < D + \hat{\tau}. \tag{10}$$

Remark 2.12. Notice that $(\Lambda\boldsymbol{f}, \Lambda g)$ is a solution of SRFR (see Definition 2.6) with entries $(v_j, \boldsymbol{r}_j)_j$, $N + \hat{\tau}$, and $D + \hat{\tau}$. Thus, our resolution method consists in finding solutions of this specific SRFR problem.

We will now give an equivalent system of equations whose polynomial unknowns have smaller degrees. We define $G^\infty := \prod_j (x-\alpha_j)^{v_j}$ and $L^\infty := \deg(G^\infty)$. Since $(x-\alpha_j)^{v_j}$ divides $(x-\alpha_j)^{v_j}\boldsymbol{\varphi}$ and $(x-\alpha_j)^{\ell_j}$, it divides $\boldsymbol{r}_j\psi$. However, $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$ so $(x-\alpha_j)^{v_j}$ divides ψ for all j, hence G^∞ divides ψ. If we denote by $\bar{\psi}$ the quotient ψ/G^∞, then Equations (9) and (10) are equivalent to

$$\boldsymbol{\varphi} = \boldsymbol{r}_j \frac{G^\infty}{(x-\alpha_j)^{v_j}} \bar{\psi} \bmod (x-\alpha_j)^{\ell_j - v_j}, \tag{11}$$

$$\deg(\boldsymbol{\varphi}) < N + \hat{\tau},\ \deg(\bar{\psi}) < D + \hat{\tau} - L^\infty. \tag{12}$$

This latter equation is consistent with the choice of $\boldsymbol{r}_j$ of degree smaller than $\ell_j - v_j$ in Remark 2.2: only the remainders of $\boldsymbol{r}_j$ modulo $(x-\alpha_j)^{\ell_j - v_j}$ matter. 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 $\mu_j = \mathrm{val}_{\alpha_j}(g)$ regardless of the value of $\boldsymbol{r}_j$. 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, $\mathcal{S}_{\boldsymbol{r}, N+\hat{\tau}, D+\hat{\tau}} \supseteq \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0 \leq i < \delta_{N+\hat{\tau}, D+\hat{\tau}}}$, where

$$\delta_{N+\hat{\tau}, D+\hat{\tau}} := \min(N - \deg(\boldsymbol{f}), D - \deg(g)) + \hat{\tau} - \sum_{j \in E}(\ell_j - \mu_j) \tag{13}$$

and $\langle b_i \rangle$ denotes the $\mathbb{F}_q$-vector space spanned by the b_i's.

Note that $\delta_{N+\hat{\tau},D+\hat{\tau}}$ is defined so that $i < \delta_{N+\hat{\tau},D+\hat{\tau}}$ if and only if $\deg(x^i \Lambda \boldsymbol{f}) < N + \hat{\tau}$ 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 (9) we consider $v_j = 0$ (no poles) and $\ell_j = 1$ (no multiplicities), we fall back to the simpler key equations

$$\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{r}_j \psi(\alpha_j),\ \deg(\boldsymbol{\varphi}) < N + \tau,\ \deg(\psi) < D + \tau. \tag{14}$$

These key equations (14) comes from [BK14, KPSW17, GLZ19] and they derive from the generalization of the Welch-Berlekamp method [WB86] for decoding Reed-Solomon codes. Also, if $g(x) \in \mathbb{F}_q$ (no rational function) and $\ell_j > 1$ (with multiplicities), the key equations (9) and (10) can be used for the decoding of *derivative codes* [GW11] or of the related *multiplicity codes* [KSY14].

The paper [KPY20] considers poles but without multiplicities. Their key equation is a special case of our key equation (11). Indeed, if α_j is an *apparent pole*, defined as $v_j > 0$, 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 (11) reduces to the identity $0 = 0 \bmod (x - \alpha_j)^{\ell_j}$,
- otherwise, the key equation (11) 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 a bound on L which guarantees that SRFRwE has a *unique* solution. In order to study the conditions of uniqueness of SRFRwE, we will analyze the uniqueness of $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$.

Theorem 2.13. *Under the setting of Definition 2.11, assume that*

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

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

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

for $\delta_{N+\hat{\tau},D+\hat{\tau}}$ defined as in Equation (13).

In this case, the solution $\boldsymbol{f}(x)/g(x)$ of SRFRwE is unique.

The bound on L of Theorem 2.13 generalizes the following results in the literature:

1. Reed-Solomon codes [RS60].
   Consider $v_j = 0$ (no poles), $\ell_j = 1$ (no multiplicities), $D = 1$ and $n = 1$ (polynomials instead of rational functions). In this case, we can take $\hat{\tau} = \tau \geq |E|$ as a bound on the size of the error support. Thus, the bound becomes $L \geq N + 2\tau$, which matches the *unique decoding radius* of Reed-Solomon codes.
2. We find the same bound $L \geq N + D - 1 + 2\tau$ as [Per14, BK14] for the extension of RS codes to the rational case, *i.e.* $v_j = 0$, $\ell_j = 1$, $D > 1$ and $n = 1$.
3. Multiplicity codes [KSY14] (or derivative codes [GW11]).
   If we consider $v_j = 0$ (no poles), $D = 1$ and $n = 1$ (polynomial case) and constant multiplicities $\ell = \ell_1 = \cdots = \ell_\lambda$, we get the bound $\lambda\ell \geq N + 2\tau\ell$ of [KSY14] where $\tau \geq |E|$ is a bound on the error support size.
4. When considering multiplicities, *i.e.* $\ell_j \geq 1$, we get the same bound $L \geq N + D - 1 + 2\hat{\tau}$ as [KPY20]. Moreover, Theorem 2.13 extends the work of [KPY20] in two ways: first, we can handle multiplicities of poles and second, we remove the hypothesis on the characteristic $\mathrm{char}(\mathbb{F}_q) \geq \ell_j$. The latter hypothesis was needed since Hermite interpolation at order ℓ_j involves the coefficient $1/(\ell_j - 1)!$. We use Hasse derivatives in Section 2.4 to overcome this problem.

Proof. We assume that there exists a solution $\boldsymbol{f}(x)/g(x)$ of the SRFRwE problem with instance $(v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda}$.

We now prove that $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \subset \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$, 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 $g\boldsymbol{\varphi} - \boldsymbol{f}\psi = \boldsymbol{0}$. We have that,

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

We multiply the first equation by Λg, so it reaches precision $\ell_j + v_j$. Indeed $\mathrm{val}_{\alpha_j}(\Lambda g) \geq v_j$ 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 $\mathrm{val}_{\alpha_j}(\psi) \geq v_j$). Finally, we get

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

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

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

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

Since $\boldsymbol{\varphi} g - \boldsymbol{f}\psi = \mathbf{0}$ and $\gcd(\boldsymbol{f}, g) = 1$ 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.

Since $\mu_j = \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$, 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 proof. □

The bound $L \geq N + D - 1 + 2\hat{\tau}$ on the number of evaluations required to ensure uniqueness depends on bounds N, D on the degrees of $\deg(\boldsymbol{f}), \deg(g)$. Since an overestimation of the degree bounds N, D implies an unnecessary increase of the bound on L, in [KPSW17] or [GLZ21, Section 4]) authors introduce some early termination techniques. The following remark gives an input for adapting these techniques in our context.

Remark 2.14. Let $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta}$ be the solution set of the key 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 2.13 can be adapted to show that for any ν, ϑ, $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0 \leq i < \delta_{\nu,\vartheta}}$ whenever $L \geq \max(N + \vartheta, D + \nu) - 1 + \hat{\tau}$.

2.4. Solving key equations

Our resolution method of SRFRwE is based on solving the key equations (9), with degree constraints (10). When the number L is large enough to ensure that the solution is unique, *i.e.* $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle$, 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, $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ 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 map $\Gamma_{\boldsymbol{r}}$. 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 degree solution [WB86, 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 $(\boldsymbol{\varphi},\psi)$ which belongs to the kernel of the following $\mathbb{F}_q$-linear map $\Gamma_{\boldsymbol{r}}$:

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

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 $(x^t)_{t=0..\ell-1}$ for each component $\mathbb{F}_q[x]_{<\ell}$ on the domain. The codomain is isomorphic to $(\mathbb{F}_q[x]/G)^n$ where $G := \prod_{j=1}^{\lambda}(x-\alpha_j)^{\ell_j}$. So, we consider a specific basis $(\mathcal{H}_{i,j})_{\substack{0\le i<\ell_j \\ 1\le j\le\lambda}}$ of $\mathbb{F}_q[x]/G$ such that $\mathcal{H}_{i,j}$ is defined using the Chinese remainder theorem as the only polynomial which satisfies

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

We call this a *Hasse basis* since it is the dual basis of the *Hasse derivatives* [Has36] (see for instance [Cox20, Section 2]).

Monomial to Hasse basis. In order to deduce the matrix associated to $\Gamma_{\boldsymbol{r}}$, we need to decompose according to the Hasse basis the polynomials φ_k, ψ which are written on the monomial basis (x^t). 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:

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

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 formulae are

$$W_{\boldsymbol{\alpha},\boldsymbol{\ell},d} := \begin{pmatrix} W_{\alpha_1,\ell_1,d} \\ \vdots \\ W_{\alpha_\lambda,\ell_\lambda,d} \end{pmatrix} \in \mathbb{F}_q^{L\times d},$$

where,

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

belongs to $\mathbb{F}_q^{\ell_j \times d}$ and $d \geq \ell_j$ for all j.

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

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

Multiplication in the Hasse basis. Assume that $\boldsymbol{r}_j$ is given by its decomposition on the Hasse basis, *i.e.* that we are given the coefficients $r_{i,j,k} \in \mathbb{F}_q$ such that $r_{j,k} = \sum_{0 \leq i < \ell_j} r_{i,j,k}(x - \alpha_j)^i \bmod (x - \alpha_j)^{\ell_j}$, where $r_{j,k}$ is the k-th vector component of $\boldsymbol{r}_j$.

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

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

We define the matrix $T_{\boldsymbol{r},\boldsymbol{\ell},k}$ that corresponds to the multiplication by $(r_{j,k})_j$ in the Hasse basis of $\mathbb{F}_q[x]/G$ as

$$T_{\boldsymbol{r},\boldsymbol{\ell},k} := \begin{pmatrix} T_{\boldsymbol{r},\boldsymbol{\ell},1,k} & & \\ & \ddots & \\ & & T_{\boldsymbol{r},\boldsymbol{\ell},\lambda,k} \end{pmatrix} \in \mathbb{F}_q^{L \times L},$$

where

$$T_{\boldsymbol{r},\boldsymbol{\ell},j,k} := \begin{pmatrix} r_{0,j,k} & & & \\ r_{1,j,k} & r_{0,j,k} & & \\ \vdots & \ddots & \ddots & \\ r_{\ell_j - 1,j,k} & \dots & r_{1,j,k} & r_{0,j,k} \end{pmatrix} \in \mathbb{F}_q^{\ell_j \times \ell_j}.$$

This matrix T is also useful for the multiplication $(x - \alpha_j)^{v_j}\boldsymbol{\varphi}$ of $\Gamma_{\boldsymbol{r}}$. Define $\boldsymbol{s}$ such as $s_{i,j,k} = 1$ if $i = v_j$ and 0 elsewhere, where $1 \leq j \leq \lambda, 0 \leq i < \ell_j$ and $1 \leq k \leq n$ as usual.

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

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

which belongs to $\mathbb{F}_q^{nL \times (n(N+\hat{\tau})+D+\hat{\tau})}$.

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].

Remark 2.15. It is possible to express the solution space $S_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ as the kernel of a more compact matrix $M'_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ by considering the linear application related to the key Equation (11) instead of Equation (9). In this case, the matrix $M'_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}$ has $n(L-L^\infty)$ rows and $(n(N+\hat{\tau})+D+\hat{\tau}-L^\infty)$ columns, where $L^\infty := \deg(G^\infty) = \sum_j v_j$.

3. Rational Function Reconstruction with random errors

Recall that our goal in this work is to determine a bound on L which guarantees the uniqueness of the solution of SRFRwE. We showed in Theorem 2.13 that if $L \geq N + D - 1 + 2\hat{\tau}$, 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 Welch-Berlekamp decoding technique for Reed-Solomon codes. As in [GLZ19, GLZ21], we will exploit techniques coming from the decoding of *Interleaved Reed-Solomon codes* (IRS) to reduce the bound on L.

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 bound on L (Theorem 3.4).

3.1. Multiplicity balancing

In the upcoming Theorem 3.4, we face the following problem: we dispatch the random errors among the n components of the vectors $\boldsymbol{r}_j$. More specifically, recall that for the error locator definition $\Lambda(x)$, an error at the evaluation point α_j for $j \in E$ is counted with multiplicity $\ell_j - \mu_j$ (see Section 2.2). Thus, we need to partition the error support $E = \sqcup_{k=1}^{n} I_k$ in such a way that the weight $\sum_{j\in I_k}(\ell_j - \mu_j)$ of each part I_k, is as small as possible — the symbol $\sqcup$ refers to a disjoint union.

We denote

$$\mathrm{MB}((\ell_j-\mu_j)_j, E) := \min_{E=\sqcup_{k=1}^{n} I_k} \left(\max_k \left(\sum_{j\in I_k} (\ell_j - \mu_j) \right) \right)$$

this minimum, where MB stands for *multiplicity balancing*. This problem is commonly known as the *load balancing* problem, the *multiprocessor scheduling* problem, or as $P||C_{\max}$ (see for instance [CEC+13, Section 6]).

In general, the problem of computing $\mathrm{MB}((\ell_j - \mu_j), E)$ is NP-hard. There are a few simple instances: in the special case without multiplicities ($\ell_j = 1$, $\mu_j = 0$ for all $j \in E$), then $\mathrm{MB}((\ell_j - \mu_j), E) = \lceil |E|/n \rceil$. More generally, if the $(\ell_j - \mu_j)_{j\in E}$'s are constant equal to C, then $\mathrm{MB}((\ell_j - \mu_j), E) = C\,\lceil |E|/n \rceil$. For general instances, we can only give approximations in polynomial time. Historically, Graham used the list scheduling algorithm to find a 2-approximation [Gra66]. Indeed, Graham's result applied to our case gives:

$$\mathrm{MB}((\ell_j-\mu_j)_j, E) \leq \max_k \left(\sum_{j\in I_k} (\ell_j - \mu_j) \right) \leq \left\lceil \sum_{j\in E} (\ell_j - \mu_j)/n \right\rceil + \max_{j\in E}(\ell_j - \mu_j)$$

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

$$\mathrm{MB}((\ell_j - \mu_j)_j, E) \leq \left\lceil \sum_{j\in E}(\ell_j - \mu_j)/n \right\rceil + \max_{j\in E}(\ell_j - \mu_j) \leq 2\,\mathrm{MB}((\ell_j - \mu_j)_j, E). \tag{15}$$

3.2. SRFR with random errors

Theorem 2.13 shows that if we consider $L \geq N + D - 1 + 2\hat{\tau}$, we can uniquely reconstruct solutions of SRFRwE (Definition 2.11). In the following, we consider a scenario of SRFR with random errors, with the purpose of proving uniqueness results for a smaller L. This scenario was already presented in coding theory and it is related to the decoding of Interleaved Reed-Solomon (IRS) codes [BKY03, BMS04]. An extension of these techniques to SRFRwE (without poles and multiplicities) can be found 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 (9), with degree constraints (10).

We briefly recall that an IRS codeword is the multipoint evaluation of a vector of polynomials of bounded degrees. Decoding an IRS code consists in reconstructing a vector of polynomials by its evaluations, some of which possibly erroneous. We can observe that SRFRwE is a generalization of this decoding problem: if $v_j = 0$ (no poles), $\ell_j = 1$ (no multiplicities) and $g(x) = 1$ (polynomial case instead of rational function) 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 [WB86], which is based on a Cauchy interpolation. For this specific case, Theorem 2.13 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 bound on L of Theorem 2.13, 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 evaluations $(v_j, \boldsymbol{r}_j)_{1\leq j\leq \lambda}$, where each $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ satisfies $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$, and a *reduced* fraction $\boldsymbol{f}/g$, we divide the error support

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

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. *The error support E can be partitioned into valuation errors E_v and evaluation errors E_r, i.e. $E = E_v \sqcup E_r$.*

Proof. 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, $j \in E \Leftrightarrow j \in E_r$ since $(x-\alpha_j)^{v_j}\boldsymbol{f} \neq \boldsymbol{r}_j g \bmod (x-\alpha_j)^{\ell_j}$ 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 $\mathrm{val}_{\alpha_j}(\boldsymbol{f}) = 0$ (because $\gcd(\boldsymbol{f}, g) = 1$). 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 $\mathrm{val}_{\alpha_j}(g) = \min(\mathrm{val}_{\alpha_j}(g), \ell_j) < v_j$. Since $v_j > 0$ and $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$, we get $\mathrm{val}_{\alpha_j}(\boldsymbol{r}_j) = 0$. 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 2.11 which also takes into account these new error supports.

Definition 3.3 (SRFR with poles and random errors). Given parameters $N, D \in \mathbb{Z}_{>0}$, $\hat{\tau}_v, \hat{\tau}_r, \tau_r \in \mathbb{Z}_{\geq 0}$ and for all $1 \leq j \leq \lambda$, $(v_j, \boldsymbol{r}_j) \in [\![0; \ell_j]\!] \times \mathbb{F}_q[x]^n$ such that $\gcd((x-\alpha_j)^{v_j}, \boldsymbol{r}_j) = 1$, find a vector of rational functions $\frac{\boldsymbol{f}(x)}{g(x)}$ 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 $\tau_r \geq |E_r|$.

Note that $\hat{\tau} := \hat{\tau}_v + \hat{\tau}_r$ is an upper bound on the degree of the error locator thanks to Proposition 3.2. In a context where the distance between $\boldsymbol{f}/g$ and $(v_j, \boldsymbol{r}_j)_j$ is given by the (non weighted) Hamming distance, *i.e.* if we are looking for $\boldsymbol{f}/g$ such that $\tau_v \geq |E_v|$ and $\tau_r \geq |E_r|$ for given τ_v, τ_r, then $\boldsymbol{f}/g$ is a solution of SRFR with random errors for $\hat{\tau}_v := \sum_{j=1}^{\tau_v} \ell_j$ and $\hat{\tau}_r := \sum_{j=1}^{\tau_r} \ell_j$ since the sequence of the ℓ_j's is nonincreasing.

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.

Formally, we 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 evaluation $(\bar{v}_j, \bar{\boldsymbol{r}}_j)_{1 \leq j \leq \lambda}$ and a vector of reduced rational functions $\boldsymbol{f}(x)/g(x)$ 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 evaluations $(v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda}$ 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 $\boldsymbol{r}_j = \bar{\boldsymbol{r}}_j \bmod (x-$

$\alpha_j)^{\bar{\mu}_j - v_j}$ for $j \in \bar{E}_r$. Equivalently, $(v_j, \boldsymbol{r}_j)_j \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ *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.*

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

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 $\bar{\mu}_j - v_j \le i < \ell_j - v_j$, $j \in \bar{E}_r$, and $1 \le k \le n$.

Theorem 3.4. *Following the previous notations, we assume that the reduced fraction $\boldsymbol{f}/g$ 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 $\hat{\tau}_v \ge \sum_{j \in \bar{E}_v}(\ell_j - \bar{\mu}_j)$, $\hat{\tau}_r \ge \sum_{j \in \bar{E}_r}(\ell_j - \bar{\mu}_j)$, and $\tau_r \ge |\bar{E}_r|$. Suppose that*

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

Let $(v_j, \boldsymbol{r}_j)_{1 \le j \le \lambda}$ be a uniformly distributed random evaluation in $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$.

Then $\mathcal{S}_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \le i < \delta_{N+\hat{\tau},D+\hat{\tau}}}$ with probability at least $1 - \frac{D+\hat{\tau}}{q}$ (for $\delta_{N+\hat{\tau},D+\hat{\tau}}$ defined as in Equation (13)).

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

Remark 3.5. Let us detail how we can make the bound on the number of evaluations of Theorem 3.4 more practical.

The following proof of this theorem will actually show the uniqueness result whenever $L \ge N + D - 1 + 2\hat{\tau}_v + \hat{\tau}_r + \mathrm{MB}((\ell_j - \bar{\mu}_j), [\![1; \tau_r]\!])$. If we combine this with the 2-approximation of multiplicity balancing given in Equation (15), we get the uniqueness result whenever

$$L \ge N + D - 1 + 2\hat{\tau}_v + \hat{\tau}_r + \lceil \hat{\tau}_r / n \rceil + \ell_1.$$

In the special case with no poles ($v_j = 0$ for all j), then $\hat{\tau} = \hat{\tau}_r$ and the bound becomes

$$L \ge N + D - 1 + \hat{\tau} + \lceil \hat{\tau}/n \rceil + \ell_1,$$

Moreover, if $\ell_1 = \cdots = \ell_\lambda = \ell$, we can use the simple form of multiplicity balancing in this case (see Section 3.1) to get

$$\lambda \ell \ge N + D - 1 + \ell(\tau + \lceil \tau/n \rceil).$$

The bound on L of Theorem 3.4 is the generalization of existing results:

1. Interleaved Reed-Solomon codes [BKY03].
   Set $v_j = 0$ (no poles), $\ell_j = 1$ (no multiplicities) and $D = 1$ (polynomial case). In this case, we can take an empty valuation error support, *i.e.* $\hat{\tau}_v = 0$, and we can consider $\hat{\tau}_r = \tau_r \geq |\bar{E}_r|$. When the multiplicity is constant, we have seen in Section 3.1 that $\mathrm{MB}(\mathbf{1}, [\![1; \tau_r]\!]) = \lceil \tau_r/n \rceil$. So, by Theorem 3.4, we have $L \geq N - 1 + \tau_r + \lceil \tau_r/n \rceil$ which matches the decoding radius of interleaved Reed-Solomon codes for random errors.
2. We find the same bound $L \geq N+D-1+\tau_r+\lceil \tau_r/n \rceil$ than [GLZ19, GLZ21] for the extension of IRS codes to the rational case.
3. Multiplicity codes [KSY14] (or derivative codes [GW11]).
   If we consider $v_j = 0$ (no poles), $D = 1$ (polynomial case) and constant multiplicities $\ell = \ell_1 = \cdots = \ell_\lambda$, our bound for the uniqueness becomes $\lambda\ell \geq N + \ell(\tau + \lceil \tau/n \rceil)$. This corresponds to the interleaved multiplicity codes capability for random errors. It has to be compared with the unique decoding capability $\lambda\ell \geq N + 2\ell\tau$ of multiplicity codes [KSY14].

Proof. Since $\boldsymbol{f}/g$ is a solution of the problem of Definition 3.3 for $(\bar{v}_j, \bar{\boldsymbol{r}}_j)$, then $\boldsymbol{f}/g$ is also a solution of the same problem for any $(v_j, \boldsymbol{r}_j)_{1 \leq j \leq \lambda} \in \mathcal{F}_{\bar{v}, \bar{\boldsymbol{r}}}$. 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 $\mathcal{S}_{\boldsymbol{w}, N+\hat{\tau}, D+\hat{\tau}} = \langle x^i \Lambda\boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{N+\hat{\tau}, D+\hat{\tau}}}$. 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 $\mathcal{S}_{\boldsymbol{r}, N+\hat{\tau}, D+\hat{\tau}} \neq \langle x^i \Lambda\boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{N+\hat{\tau}, D+\hat{\tau}}}$.

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

Remember that all $(v_j, \boldsymbol{r}_j)_j \in \mathcal{F}_{\bar{v}, \bar{\boldsymbol{r}}}$ 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 define $\boldsymbol{w}_j \in \mathbb{F}_q[x]^n$ such that

$$(x - \alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{w}_j g = \boldsymbol{\varepsilon}_{k_j} (x - \alpha_j)^{\bar{\mu}_j} \bmod (x - \alpha_j)^{\ell_j}$$

where $\boldsymbol{\varepsilon}_i$ is the i-th 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 $\bar{\mu}_j \geq v_j = \mathrm{val}_{\alpha_j}(g)$ when $j \in \bar{E}_r$. Therefore, we can set for $j \notin \bar{E}_r$,

$$\boldsymbol{w}_j := ((x - \alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{\varepsilon}_{k_j} (x - \alpha_j)^{\bar{\mu}_j})/g \bmod (x - \alpha_j)^{\ell_j - v_j},$$

which is well-defined because the valuation at α_j of the right-hand side is non-negative. Note that for $j \notin \bar{E}_r$, $(x - \alpha_j)^{v_j} \boldsymbol{f} - \boldsymbol{w}_j g = \mathbf{0} \bmod (x - \alpha_j)^{\bar{\mu}_j}$ because $\boldsymbol{w}_j$ coincides with $\bar{\boldsymbol{r}}_j$.

Fix $(\boldsymbol{\varphi}, \psi) \in \mathcal{S}_{\boldsymbol{w}, N+\hat{\tau}, D+\hat{\tau}}$. Our first goal is to prove that $\boldsymbol{p}(x) = \mathbf{0}$ where $\boldsymbol{p}(x) := \boldsymbol{f}(x)\psi(x) - \boldsymbol{\varphi}(x)g(x)$. For $j \notin \bar{E}_r$, we consider 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 $(x-\alpha_j)^{v_j+\bar{\mu}_j}$. 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, $v_j + \bar{\mu}_j \leq \ell_j + \mathrm{val}_{\alpha_j}(g)$, so we get

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

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

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

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

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

Therefore, p_k is zero modulo a polynomial of degree

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

On the other hand, $\deg(\boldsymbol{f}\psi - \boldsymbol{\varphi}g) < N + D - 1 + \hat{\tau}$ 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 $\boldsymbol{f}\psi - \boldsymbol{\varphi}g = \mathbf{0}$ 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 $\mu_j = \min(\mathrm{val}_{\alpha_j}((x-\alpha_j)^{v_j}\boldsymbol{f} - \boldsymbol{r}_j g), \ell_j)$ 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 on $\boldsymbol{r}_j$.

Recall that for all $(v_j, \boldsymbol{r}_j)_j \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$, the minimal error indices μ_j of $\boldsymbol{r}_j$ and $\bar{\mu}_j$ of $\bar{\boldsymbol{r}}_j$ coincide, except for $j \in \bar{E}_r$ 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 $(v_j, \boldsymbol{r}_j)_j \in \mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$, 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 $(v_j, \boldsymbol{r}_j)_j$ in $\mathcal{F}_{\bar{v},\bar{\boldsymbol{r}}}$ satisfies $\dim \ker M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}} \leq \delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}}$ is bounded from below 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 $\mathrm{rank}(M_{\boldsymbol{r},N+\hat{\tau},D+\hat{\tau}}) \leq n(N+\hat{\tau}) + D + \hat{\tau} - \delta_{\bar{\boldsymbol{r}},N+\hat{\tau},D+\hat{\tau}} =: \rho$.

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 $(r_{i,j,k})$ for $j \in \bar{E}_r$, $\bar{\mu}_j - v_j \leq i < \ell_j - v_j$, and $1 \leq k \leq n$. Thus, we have shown before 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 3.6. We are confident that our techniques can be adapted to a context of early termination 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 $\delta_{\nu,\vartheta} := \min(\nu - \deg(\boldsymbol{f}), \vartheta - \deg(g)) - \deg(\Lambda)$. The proof of Theorem 3.4 can be adapted to show that for any ν, ϑ, $\mathcal{S}_{\boldsymbol{r},\nu,\vartheta} = \langle x^i \Lambda \boldsymbol{f}, x^i \Lambda g \rangle_{0 \leq i < \delta_{\nu,\vartheta}}$ with probability at least $1 - \frac{\vartheta}{q}$ whenever $L \geq \max(N+\vartheta, D+\nu) - 1 + \hat{\tau}_v + \mathrm{MB}(\boldsymbol{\ell}, [\![1; \tau_r]\!])$.

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 and removing the hypothesis on the characteristic of the field. Moreover, we adapt the analysis of simultaneous rational function reconstruction for random errors in this new scenario, providing a uniqueness condition (applying interleaving techniques) and an estimation of the probability failure.

References

[BK14] B. Boyer and E.L. 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.

[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.

[CS05] Z. Chen and A. Storjohann. A BLAS Based C Library for Exact Linear Algebra on Integer Matrices. In *Proceedings of ISSAC'05*, pages 92–99. ACM, 2005.

[Dix82] J. D. Dixon. Exact solution of linear equations using p-adic expansions. *Numerische Mathematik*, 40(1):137–141, February 1982.

[DSV00] J.-G. Dumas, B. D. Saunders, and G. Villard. Integer Smith form via the valence: experience with large sparse matrices from homology. In *Proceedings of ISSAC'00*, pages 95–105, 2000.

[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.

[GLZ20] E. Guerrini, R. Lebreton, and I. Zappatore. On the Uniqueness of Simultaneous Rational Function Reconstruction. In *Proceedings of ISSAC'20*, 2020.

[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*, pages 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.

[Has36] H. Hasse. Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik. *Journal für die Reine und Angewandte Mathematik*, 175:50–54, 1936.

[KP04] M. Kuijper and J.W. Polderman. Reed-solomon list decoding from a system-theoretic perspective. *IEEE Transactions on Information Theory*, 50(2):259–271, 2004.

[KPSW17] E.L. 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. In *Proceedings of CASC'20*, Lecture Notes in Computer Science, 2020.

[KSY14] S. Kopparty, S. Saraf, and S. Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM*, 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.

[MC79] R. T. Moenck and J. H. Carter. Approximate algorithms to derive exact solutions to systems of linear equations. In *EUROSAM '79*, volume 72, pages 65–73. Springer, 1979.

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

[O'S00] M.E. O'Sullivan. Decoding of hermitian codes: the key equation and efficient error evaluation. *IEEE Transactions on Information Theory*, 46(2):512–523, 2000.

[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.

[RJ97] V.C. Rocha Jr. Digital sequences and the hasse derivative. *Communications Coding and Signal Processing*, 3:256–268, 1997.

[RS60] I. S. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, June 1960.

[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.

[SVM09] G. Schmidt, V.Sidorenko, and M.Bossert. Collaborative Decoding of Interleaved Reed–Solomon Codes and Concatenated Code Designs. *IEEE Transactions on Information Theory*, 55(7), 2009.

[WB86] L. R. Welch and E. R. Berlekamp. Error Correction of Algebraic Block Codes, U.S. Patent 4 633 470, Dec. 1986.