Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes

Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore

Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes

Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore
LIRMM, Université de Montpellier, CNRS
Montpellier, France
{**guerrini, lebreton, zappatore**}**@lirmm.fr**

***Abstract*—In this paper we present a new algorithm for Polynomial Linear System Solving (via evaluation/interpolation) with errors. In this scenario, errors can occur in the black box evaluation step. We improve the bound on the number of errors that we can correct, using techniques inspired by the decoding procedure of Interleaved Reed-Solomon Codes.**

I. Introduction

The problem of decoding a Reed-Solomon code (shortly RS), also known as the Polynomial Reconstruction Problem (PR) has been largely studied in Coding Theory [1]–[3]. In [7], Bleichenbacher et al. proposed a new scenario of the PR problem, called Simultaneous Polynomial Reconstruction (SPR). This problem was associated to the decoding of Interleaved Reed-Solomon codes. Instead of the separate reconstruction of each interleaved codeword, the main idea was to correct several codewords simultaneously in order to gain an error correction capability which depends also on the amount of messages received (interleaving parameter). They proposed an algorithm that, under some hypotheses on the error distribution, allows to correctly decode Interleaved RS codewords, beyond the unique decoding bound, with a certain probability. This probability depends on the number of errors and on the order of the field of the coefficients. Interleaved Reed Solomon codes (IRS) are widely studied in the last 20 years. In the original work [7] the key equations for recovering the codewords are a generalization of Berlekamp-Welch decoding method for RS. A more general scenario is due to [10] (improved by [11]) where codewords are issue of differents RS codes (namely Heterogeneous IRS) and the decoding method is based on Berlekamp-Massey algorithm as for the classical BCH codes. Recently, in [9] by applying Power Decoding method for generating independent key equations [12], the IRS decoding radius is significantly improved.

The purpose of the present work is to introduce a new algorithm, inspired by SPR problem, to solve a full rank consistent linear system $A(x)\boldsymbol{y} = \boldsymbol{b}(x)$ where erroneous evaluations occur.
In order to solve this system, a classical technique (see for example [4]) consists in evaluating in a certain number of points, solving the evaluated system and then interpolating these evaluated solutions. The solution is a vector of rational functions $\frac{\boldsymbol{f}(x)}{g(x)}$, where $\boldsymbol{f}$ is a vector of polynomials and $g(x)$ is the least common denominator.
In [5], [6], authors studied the problem in a scenario where some evaluations can be erroneous. They introduced an algorithm that recovers the solution by fixing a certain number L_{BK} of evaluation points. This method is a generalization of the Berlekamp-Welch algorithm for PR. Thus, the error correction capability coincides with the unique decoding bound.

In this work, we generalize the SPR problem to the Simultaneous Rational Function Reconstruction (SRFR) in order to solve a polynomial linear system with errors. In the special case where the matrix A is the identity matrix, we observe that our problem reduces to the SPR, or equivalently, to the problem of decoding an Interleaved RS code. Still in this special case, we can apply the decoding technique of Interleaved RS codes and correct more errors than [5] under the probabilistic hypotheses of [8]. In order to generalize this, we reexamine the scenario of [5], [6] with a probabilistic assumption. In this context, we introduce a new algorithm that can be seen as the generalization of the decoding algorithm of Interleaved RS codes. Our algorithm can correctly reconstruct the vector solution of our system with a smaller number of points $L_{GLZ} \leq L_{BK}$. However it can fail for a small fraction of possible errors as in [8]. In our case, the fraction is at most $\frac{dg+e}{q}$ where dg is the degree of the common denominator of the rational function vector, e is the number of errors and q the order of the field.

II. Polynomial linear system solving with errors

In [5] and [6], authors studied the problem of solving a consistent linear system

$$A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x) \tag{1}$$

where,

- $A(x)$ is a full rank $m \times n$ matrix whose entries are polynomials in $\mathbb{K}[x]$, $\mathbb{K}$ is a field and $m \geq n \geq 1$;
- $\boldsymbol{b}(x)$ is an m-th vector of polynomials in $\mathbb{K}[x]$.

The system admits a solution whose coordinates are rational functions and, since the matrix is full rank, there is a unique solution

$$\boldsymbol{y}(x) = \frac{\boldsymbol{f}(x)}{g(x)} = \left(\frac{f_1(x)}{g(x)}, \ldots, \frac{f_n(x)}{g(x)}\right)$$

where g is the monic least common denominator, and

$$\text{GCD}(\boldsymbol{f}, g) = \text{GCD}(\text{GCD}_i(f_i), g) = 1. \tag{2}$$

In general, this solution can be found by evaluating the system at a certain number, say L, of distinct points $\alpha_l \in \mathbb{K}$ with $l \in \{1, \dots, L\}$, solving the evaluated system and then interpolating the parametric solution from the evaluated solution [4]. The authors in [5] proved that it is possible to reconstruct the solution even if some evaluations are *erroneous*. They focused on a model where there is a black box that, for any evaluation point α_l, provides $A_l \in \mathbb{K}^{m\times n}$ and $\boldsymbol{b}_l \in \mathbb{K}^m$ which may not be equal to $A(\alpha_l)$ and $\boldsymbol{b}(\alpha_l)$. More specifically, the resulting evaluations A_l and $\boldsymbol{b}_l$ are considered erroneous if $A_l\boldsymbol{f}(\alpha_l) \neq g(\alpha_l)\boldsymbol{b}_l$. In this scenario they proved that with

$$L \geq L_{BK} := df + dg + 2e + t + 1 \tag{3}$$

number of points, it is possible to uniquely reconstruct the solution of the linear system (1), where

- $df \geq \deg(\boldsymbol{f}) := \max_{1\leq i\leq n} \deg(f_i)$,
- $dg \geq \deg(g)$,
- $e \geq |E|$ is a bound on the erroneous evaluations where

$$E := \{l \mid A_l\boldsymbol{f}(\alpha_l) \neq g(\alpha_l)\boldsymbol{b}_l\}$$

- $t \geq |R|$ is a bound on the rank drops where

$$R := \{l \mid A_l\boldsymbol{f}(\alpha_l) = g(\alpha_l)\boldsymbol{b}_l \text{ and } \text{rank}(A_l) < n\}$$

Their method consists in solving the homogeneous linear system

$$\left[A_l \begin{pmatrix} \varphi_1(\alpha_l) \\ \varphi_2(\alpha_l) \\ \vdots \\ \varphi_n(\alpha_l) \end{pmatrix} - \psi(\alpha_l)\boldsymbol{b}_l = 0 \right]_{l\in\{1,\dots,L\}} \tag{4}$$

where

- $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_n) \in (\mathbb{K}[x])^n$ and for any $1 \leq i \leq n$, $\deg(\varphi_i) \leq df + e$,
- $\psi \in \mathbb{K}[x]$, $\deg(\psi) \leq dg + e$.

The unknowns of the linear system (4) are the coefficients of φ_i and ψ. In particular, they proved the following:

Theorem 1 ([5]). *Under previous assumptions, let $(\boldsymbol{\varphi}_{min}, \psi_{min})$ be the solution of (4) of minimal degree and ψ_{min} monic. Then*

$$\boldsymbol{\varphi}_{min} = \Lambda\boldsymbol{f}, \quad \psi_{min} = \Lambda g$$

where

$$\Lambda(x) = \prod_{l\in E}(x - \alpha_l)$$

is the error locator polynomial.

From now on we omit the rank drops study and we assume $t = 0$.

This method is a generalization of the Berlekamp-Welch decoding algorithm for Reed-Solomon codes [1]. In fact, if $\mathbb{K} = \mathbb{F}_q$, $m = n = 1$, $A_l = I_1$ and g is the constant polynomial 1, then

$$\begin{cases} b_l = f(\alpha_l) & l \notin E, \\ b_l \neq f(\alpha_l) & l \in E. \end{cases}$$

Hence, in this case, the problem of recovering the solution of the linear system (1) with errors, coincides with the problem of decoding of RS code and the linear system (4) is exactly the *key equation* of the classical Berlekamp-Welch method.

We now define the Interleaving RS encoding procedure. Let $\mathcal{C}$ be an $[n, k]_q$ RS code.

- we consider r codewords $c_i \in \mathcal{C}$. For any $i \in \{1, \dots, r\}$, $c_i = (f_i(\alpha_1), \dots, f_i(\alpha_n))$ where $f_i \in \mathbb{F}_q[x]$ has degree $\deg(f_i) \leq k - 1$ and $\{\alpha_1, \dots, \alpha_n\}$ is the set of distinct evaluation points;
- we arrange these codewords row-wise and we obtain the $r \times n$ matrix $(c_i)_{1\leq i\leq r} = (f_i(\alpha_j))_{\substack{1\leq i\leq r \\ 1\leq j\leq n}}$;
- by interpreting this matrix as a row vector $(\boldsymbol{f}(\alpha_j))_{1\leq j\leq n} \in (\mathbb{F}_{q^r})^n$, we obtain a codeword of an Interleaved RS code of length n, dimension k over $\mathbb{F}_{q^r}$. The number of codewords r is the amount of interleaving.

Definition 1 (Simultaneous polynomial reconstruction [7])**.** *Let $n, k, e \in \mathbb{N}$ and $\alpha_1, \dots, \alpha_n$ distinct points in $\mathbb{F}_q$. An instance of the SPR is $(y_{ij})_{\substack{1\leq i\leq r \\ 1\leq j\leq n}}$, that verifies the following. There exists*

- *$E \subset \{1, \dots, n\}$ with $|E| \leq e$,*
- *polynomials $(f_1, \dots, f_r)$, with $\deg(f_i) \leq k - 1$*

such that

$$y_{ij} = f_i(\alpha_j), j \notin E$$

The solution of the SPR is the tuple $(f_1, \dots, f_r)$.

The SPR problem is exactly the problem of decoding an Interleaved RS code with length n, dimension k and amount of interleaving r.

We can now observe that,

Remark 1. *If $\mathbb{K} = \mathbb{F}_q$, $m = n$, $A_l = I_n$ and g is the constant polynomial 1, then the linear system (1) becomes*

$$\begin{cases} \boldsymbol{b}_l = \boldsymbol{f}(\alpha_l) & l \notin E, \\ \boldsymbol{b}_l \neq \boldsymbol{f}(\alpha_l) & l \in E. \end{cases}$$

Hence, the problem of solving the linear system (1) with errors coincides with the problem of decoding an Interleaved RS code (SPR [7]) with length L, dimension $df + 1$ and amount of interleaving n.

In [7], the authors proposed an algorithm that, under some hypotheses on the error distribution, allows to decode an Interleaved RS code with a certain probability. In particular, they introduced *key equations*,

$$\begin{cases} [m_1(\alpha_j) = y_{1j}E(\alpha_j)]_{1\leq j\leq n} \\ \dots \\ [m_r(\alpha_j) = y_{rj}E(\alpha_j)]_{1\leq j\leq n} \end{cases} \tag{5}$$

The unknowns of this linear system are the coefficients of m_i and E, polynomials of degrees at most respectively $k+e$ and e. This linear system (5) has rn equations and $r(k+e)+e+1$ unknowns. Moreover,

Theorem 2 ([7]). *Let $(y_{ij})_{\substack{1\le i\le r\\ 1\le j\le n}}$ the received word of an Interleaved RS code, or equivalently an instance of the SPR problem, where*

$$e := |E| \le \frac{r(n-k)}{r+1}$$

and for each $i \in \{1,\dots,r\}$,

(i) if $j \in E$, y_{ij} are uniformly distributed over $\mathbb{F}_q$
(ii) if $j \notin E$, $y_{ij} = f_i(\alpha_j)$ and $f_1,\dots,f_r$ are uniformly distributed over the vector space of polynomials of $\mathbb{F}_q[x]$ of degree at most $k-1$;

then the linear system (5) admits at most one solution with probability at least $1 - e/q$.

Since if $r \ge 1$,

$$\frac{r(n-k)}{r+1} \ge \frac{n-k}{2},$$

then they proved that, under the probabilistic assumptions (i) and (ii), it is possible to correctly decode the received word beyond the unique decoding bound. The failing probability, *i.e.* the probability that the algorithm fails, is then upper bounded by e/q.

In a following paper [8], the probabilistic assumptions are reduced and it was proved that the failing probability is $\mathcal{O}(1/q)$ which is independent of the number of errors. In detail,

Theorem 3 ([8]). *Given $(y_{ij})_{\substack{1\le i\le r\\ 1\le j\le n}}$ the received word of an Interleaved RS code, where*

$$e := |E| = \frac{r(n-k)}{r+1}$$

and for each $i \in \{1,\dots,r\}$,

(i) if $j \in E$, y_{ij} are uniformly distributed over $\mathbb{F}_q$
(ii) if $j \notin E$, $y_{ij} = f_i(\alpha_j)$,

then the linear system (5) admits at most one solution with probability at least $1 - \frac{exp(1/(q^{r-2}))}{q-1}$.

In this paper, starting from Remark 1 we reexamine the problem of solving the linear system (1) with errors as a generalization of the decoding of an Interleaved RS code under some hypotheses on the error distribution. In particular, following the [7] approach, we prove that the failing probability is at most $\frac{dg+e}{q}$ (where dg is the degree of the common denominator of the vector of rational functions). We stress out that, in our scenario, we relax the hypotheses on the error distribution as in [8]. However we are not able to prove a bound on the failing probability as tight as [8] (see Section IV for more comments).

III. Generalization of decoding of Interleaved RS codes

We study the problem of solving a consistent, full rank, linear system (1), $A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x)$ with polynomial entries over a finite field $\mathbb{F}_q$.
In a first instance, we focus on the square case, i.e. $n = m$. Let $\boldsymbol{y} = \frac{\boldsymbol{f}(x)}{g(x)}$ be the reduced unique solution as in (2).

We fix L evaluation points with

$$L \ge L_{GLZ} := \left\lceil \frac{n(df+e+1)+dg+e}{n} \right\rceil \tag{6}$$

where

- $df \ge \deg(\boldsymbol{f}) := \max_{1\le i\le n} \deg(f_i)$,
- $dg = \deg(g)$,
- $g(\alpha_l) \ne 0$ for $1 \le l \le L$,
- $e = |E|$ is the number of erroneous evaluations where

$$E = \{l \mid A_l \boldsymbol{f}(\alpha_l) \ne g(\alpha_l)\boldsymbol{b}_l \text{ and } \mathrm{rank}(A_l) = n\}.$$

Remark 2. *In this way, since if $n \ge 1$, we reduce the number of evaluation points,*

$$L_{GLZ} \le L_{BK}.$$

We slightly modify the black box scenario described in the previous section, by introducing a probabilistic assumption. More specifically, we assume that for any erroneous evaluation, $l \in E$, the entries of A_l and $\boldsymbol{b}_l$ are uniformly random elements of $\mathbb{F}_q$. Moreover, since we skip the rank drops study, we also suppose that all the A_l are always full rank.

We study, for any $l \in \{1,\dots,L\}$, the homogeneous linear systems

$$A_l\boldsymbol{\gamma}_l - \sigma_l\boldsymbol{b}_l = 0. \tag{7}$$

Remark 3. *Let C_l be the coefficients matrix of any of these linear systems,*

$$C_l = [A_l | -\boldsymbol{b}_l].$$

Since any system have n equations and $n+1$ unknowns and A_l is full rank, the rank of C_l is n and in particular, the kernel of any C_l is one dimensional.

Proposition 1. *Let $(\boldsymbol{\gamma}_l, \sigma_l) = (\gamma_{l1},\dots,\gamma_{ln},\sigma_l)$ be the vector that generates the right kernel of C_l, with $l \in \{1,\dots,L\}$. Then,*

$$\frac{\boldsymbol{\gamma}_l}{\sigma_l} = \frac{\boldsymbol{f}(\alpha_l)}{g(\alpha_l)} \quad \forall l \notin E.$$

Proof. By our assumptions, $g(\alpha_l) \ne 0$ for any $l \notin E$. Now, since the right kernel is one dimensional, its generator $(\boldsymbol{\gamma}_l, \sigma_l) = (\gamma_{l1},\dots,\gamma_{ln},\sigma_l)$ is the nonzero vector, and also $\sigma_l \ne 0$. Let $l \notin E$, be a correct evaluation. Since $A_l\boldsymbol{\gamma}_l - \sigma_l\boldsymbol{b}_l = 0$ and $A_l\boldsymbol{f}(\alpha_l) = g(\alpha_l)\boldsymbol{b}_l$, then $A_l(\boldsymbol{f}(\alpha_l)\sigma_l - g(\alpha_l)\boldsymbol{\gamma}_l) = 0$. The matrix A_l is full rank, hence $\boldsymbol{f}(\alpha_l)\sigma_l - g(\alpha_l)\boldsymbol{\gamma}_l = 0$. Then we can conclude that $\frac{\boldsymbol{\gamma}_l}{\sigma_l} = \frac{\boldsymbol{f}(\alpha_l)}{g(\alpha_l)}$. □

Following the previous notations, if we denote by $\boldsymbol{y}_l := \frac{\boldsymbol{\gamma}_l}{\sigma_l} = \frac{1}{\sigma_l}(\gamma_{l1},\dots,\gamma_{ln}) \in (\mathbb{F}_q)^n$, for any $l \in \{1,\dots,L\}$ we have that

$$\boldsymbol{y}_l = \frac{\boldsymbol{f}(\alpha_l)}{g(\alpha_l)}, l \notin E \tag{8}$$

Remark 4. *By our probabilistic assumption,* $(y_{li})_{l\in E}$ *are uniformly random elements of* $\mathbb{F}_q$.

In this way, we reduce the problem of solving the linear system (1) to the reconstruction of a vector of rational functions with errors. In particular, we observe that if g is the constant polynomial 1, our problem coincides exactly with the decoding of an Interleaved RS code, with length L, dimension $df+1$ and amount of interleaving n. This is why we can consider our problem as a generalization of the decoding of Interleaved RS codes.

Now, we study the key equations

$$\begin{cases} \boldsymbol{\varphi}(\alpha_1) = \boldsymbol{y}_1\psi(\alpha_1) \\ \dots \\ \boldsymbol{\varphi}(\alpha_L) = \boldsymbol{y}_L\psi(\alpha_L) \end{cases}$$

or, in other terms, if we denote $\boldsymbol{y}_l = (y_{l1}, \dots, y_{ln})$ for $l \in \{1, \dots, L\}$,

$$\begin{cases} [\varphi_1(\alpha_l) = y_{l1}\psi(\alpha_l)]_{1\le l\le L} \\ \dots \\ [\varphi_n(\alpha_l) = y_{ln}\psi(\alpha_l)]_{1\le l\le L} \end{cases} \tag{9}$$

where

- $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_n) \in (\mathbb{F}_q[x])^n$ and $\deg(\varphi_i) \le df+e$,
- $\psi \in \mathbb{F}_q[x]$ has degree at most $dg+e$.

The linear system (9) has nL equations and $n(df+e+1)+dg+e+1$ unknowns, that are the coefficients of $\boldsymbol{\varphi}$ and ψ. The coefficient matrix of the system (9) is

$$M_{\boldsymbol{y}} := \begin{pmatrix} V_{df+e+1} & & & -D_1V_{dg+e+1} \\ & \ddots & & \vdots \\ & & V_{df+e+1} & -D_nV_{dg+e+1} \end{pmatrix}$$

where,

- $V_t = (\alpha_l^{i-1})_{\substack{1\le l\le L \\ 1\le i\le t}}$ is the $L\times t$ *Vandermonde* matrix,
- for $i \in \{1, \dots, n\}$, D_i is the diagonal matrix with $y_{1i}, \dots, y_{Li}$ on the diagonal.

Recall that the error locator polynomial $\Lambda(x) = \prod_{l\in E}(x-\alpha_l)$ is monic and has degree e. We observe that $(\Lambda\boldsymbol{f}, \Lambda g) = (\Lambda f_1, \dots, \Lambda f_n, \Lambda g)$ is a solution of the system. Therefore, if the kernel of $M_{\boldsymbol{y}}$ has dimension 1, the non-zero solutions are collinear to $(\Lambda\boldsymbol{f}, \Lambda g)$, meaning that we can correctly reconstruct the fraction $\boldsymbol{f}/g = \Lambda\boldsymbol{f}/\Lambda g$.

We do not have *a priori* any other information about this kernel. In our following main result, we adapt the approaches of [7], [8] to prove that this favorable situation happens with high probability.

Theorem 4. *Under the previous assumptions, the dimension of the (right) kernel of* $M_{\boldsymbol{y}}$ *is one with probability at least* $1 - \frac{(dg+e)}{q}$.

The cornerstone of the proof is the following lemma.

Lemma 1. *There exists a random draw of* $(\boldsymbol{y}_l)_{l\in E}$ *such that the dimension of the right kernel of* $M_{\boldsymbol{y}}$ *is one.*

Proof. We can partition $E = \bigcup_{1\le i\le n} I_i$ with sets $I_i \subset E$ such that $|I_1| \le L-(df+dg+e+1)$ and $|I_i| \le L-(df+e+1)$ for $2 \le i \le n$ since $L-(df+dg+e+1)+(n-1)(L-(df+e+1)) \ge e$. We start by fixing a part of the random variables $(\boldsymbol{y}_l)_{l\in E}$: for all $1 \le i \le n$ and $l \in E \setminus I_i$, we set $y_{li} = \frac{f_i(\alpha_l)}{g(\alpha_l)}$ while y_{li} for $l \in I_i$ remain free variables for now, for a total of e free variables.

Now, we study the equations (9),

- for $l \notin I_1$, $\varphi_1(\alpha_l)g(\alpha_l) = f_1(\alpha_l)\psi(\alpha_l)$. Therefore, since the polynomial $\varphi_1 g - f_1\psi$ has degree at most $df+dg+e$ and at least $df+dg+e+1$ roots, it is the zero polynomial. By assuming that f_1/g is reduced (we will lift this hypothesis later) we get that there exists a polynomial R such that $f_1R = \varphi_1$, $gR = \psi$ and so $\deg(R) \le e$.
- For $2 \le i \le n$ and $l \notin I_i$

  $$\varphi_i(\alpha_l)g(\alpha_l) = f_i(\alpha_l)\psi(\alpha_l) = f_i(\alpha_l)R(\alpha_l)g(\alpha_l).$$

  Since $g(\alpha_l) \ne 0$, and the polynomial $\varphi_i - f_iR$ has degree at most $df+e$ and at least $df+e+1$ zeros, $f_iR = \varphi_i$.

Hence for $1 \le i \le n$, $f_iR = \varphi_i$ and $gR = \psi$ and so by replacing in (9) we have

$$R(\alpha_l)[f_i(\alpha_l) - y_{li}g(\alpha_l)] = 0$$

We observe that for any $l \in E$, there exists $1 \le i \le n$ such that $l \in I_i$, so y_{li} is still a free variable and we can give it a value so that $f_i(\alpha_l) \ne y_{li}g(\alpha_l)$ since $g(\alpha_l) \ne 0$. Therefore $R(\alpha_l) = 0$ for $l \in E$ and $deg(R) \le e$ and so R is a scalar multiple of Λ. We have proved that for some values of $\boldsymbol{y}_l$ the kernel is spanned by $(\Lambda\boldsymbol{f}, \Lambda g)$ and has dimension 1.

Now we show that we can indeed assume that f_1/g is reduced without loss of generality. For this matter, we will prove that there exists $\boldsymbol{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ such that $\hat{f}_{\boldsymbol{c}} = \sum_{i=1}^n c_if_i \in \mathbb{F}_q[x]$ is prime to g. Assuming $c_1 \ne 0$, let $\boldsymbol{y}'$ be equal to $\boldsymbol{y}$ except for $y'_{l1} = \sum_{i=1}^n c_iy_{li}$. Then $\boldsymbol{y}'$ corresponds to the new fraction $(\hat{f}_{\boldsymbol{c}}, f_2, \dots, f_n)/g$ and the matrix $M_{\boldsymbol{y}'}$ is linearly equivalent to $M_{\boldsymbol{y}}$. So they both have kernel dimension 1 for the same number of values of $\boldsymbol{y}$ and respectively $\boldsymbol{y}'$.

We consider the prime factorization of $g = \prod_{j=1}^r P_j^{\nu_j}$ over $\mathbb{F}_q[x]$. Given $0 \le j \le r$, the vector space $V_j = \left\{\boldsymbol{c} \in \mathbb{F}_q^n \mid \hat{f}_{\boldsymbol{c}} = 0 \bmod P_j\right\}$ is a proper subspace of $\mathbb{F}_q^n$ because $\mathrm{GCD}(f_1, \dots, f_n, g) = 1$. Now $\mathbb{F}_q^n$ can not be the union of r proper subspaces V_j since $r \le \deg g < q$. So there exists $\boldsymbol{c} \in \mathbb{F}_q^n$ such that $\hat{f}_{\boldsymbol{c}} \ne 0 \bmod P_j$ for all $0 \le \ell \le r$ and $\hat{f}_{\boldsymbol{c}}$ is prime to g as claimed. □

Proof of Theorem 4. We recall that $(\Lambda f_1, \dots, \Lambda f_n, \Lambda g)$ is a solution of the linear system (9) so it has kernel dimension at least 1. Since Λg is a monic polynomial of degree $dg+e$, the last column of $M_{\boldsymbol{y}}$ is linearly dependent on the previous ones. As a consequence, the kernel of $M_{\boldsymbol{y}}$ has dimension 1 iff the rank of $M_{\boldsymbol{y}}$ is $\rho := n(df+e+1)+dg+e$ iff there exists a non-zero minor of $M_{\boldsymbol{y}}$ of size ρ that avoids the last column. Considering the minors as polynomials in the variables $(\boldsymbol{y}_l)_{l\in E}$, we have shown in Lemma 1 that one of

these ρ-minors is not the zero polynomial because it does not vanish on some value of $(\boldsymbol{y}_l)_{l\in E}$. Finally, since this ρ-minor has degree at most $dg+e$, by Schwartz-Zippel Lemma, it cannot be zero in more than a $\frac{dg+e}{q}$-fraction of its domain. Therefore, we can conclude that the kernel has dimension 1 with probability at least $1-\frac{dg+e}{q}$. □

Summing up, working under our probabilistic assumptions, we are able to recover the correct solution with a failing probability upper bounded by $\frac{dg+e}{q}$.

Data: $(A_l, \boldsymbol{b}_l)_{1\le l\le L}$ and df, dg, e
Result: $(\boldsymbol{f}, g)$ or `fail`
$L := \lceil \frac{n(df+e+1)+dg+e}{n} \rceil$;
for $l = 1, \dots, L$ **do**
  find a basis $\{(\boldsymbol{\gamma}_l, \sigma_l)\}$ of the right kernel of C_l;
  $\boldsymbol{y}_l := \frac{\boldsymbol{\gamma}_l}{\sigma_l}$;
construct the matrix $M_{\boldsymbol{y}}$ of the key equation (9);
if *rank*$(M_{\boldsymbol{y}}) = n(df+e+1)+dg+e$ **then**
  compute a solution $(\boldsymbol{\varphi}, \psi)$ with ψ monic;
  $\Lambda := \mathrm{GCD}(\boldsymbol{\varphi}, \psi)$;
  return $(\frac{\boldsymbol{\varphi}}{\Lambda}, \frac{\psi}{\Lambda})$;
else
  return `fail`;

Up to this point, we have assumed that the linear system (1) is square, *i.e.* $n = m$. With our method it is possible to recover the solution with the same probability also in the general case by considering random y_{li}, for any l such that $\mathrm{rank}(C_l) = n+1$ (see Remark 3).

IV. Experiments and Conclusions

In this work we prove that, in our probabilistic scenario, by using the evaluation interpolation technique [4] with $L \ge L_{GLZ}$ evaluation points, we can reconstruct the vector solution of the linear system (1). Recall that L_{BK} is the number of points that guarantees to uniquely reconstruct the solution for every error. In our case since $L_{GLZ} \le L_{BK}$, we cannot reconstruct the solution for every error, but for almost all of them.

We implement our algorithm in `SageMath` (http://www.sagemath.org). In particular, we solve 3000 different polynomial linear systems of size 3. We suppose that the number of errors is $e = 4$ and that the degree of g is at most 6. We then compute the percentage p^* of the number of times in which the algorithm fails. We obtain the following results:

q	p^*	p_{GLZ}	p_{BMS}
2^5	0.9%	31.2%	3.22%
2^6	0.33%	15.6%	1.59%
2^9	0.17%	1.9%	0.19%

We compare our experimental results with p_{GLZ}, *i.e.* the percentage on the failing probability of the Theorem 4 and the percentage on the failing probability p_{BMS} of [8]. We recall that the last one is related to the decoding of Interleaved RS and not to our problem. First of all, we can observe the dependency of the failing probability on the order or the field. Recall that $p_{BMS} = \mathcal{O}(\frac{1}{q})$, which it is independent on the number of errors (and the degree of g). Therefore, the experiments suggest that our bound can be strongly improved. A future work could consider new techniques to restate that bound.

Furthermore, since we use an evaluation interpolation technique, there exist finitely many evaluation points α_l such that the evaluated matrix $A(\alpha_l)$ is not full rank anymore. Nevertheless, in this work, we have supposed to chose some evaluation points such that the evaluated matrix is full rank, thus omitting the rank drop study. This work can be extended for dealing with some rank drops using the main idea in [5].

V. Acknowledgements

This work has been supported by Occitanie Region through the ARPE HPAC project. We would also like to thank Daniel Augot and Bruno Grenet for useful discussions.

References

[1] Elwyn R. Berlekamp, Lloyd R. Welch, *Error Correction of Algebraic Block Codes.* US Patent 4, 633470, 1986.
[2] Venkatesan Guruswami, Madhu Sudan, *Improved decoding of Reed-Solomon and algebraic-geometric codes.*in IEEE Transactions on Information Theory, vol. 45, no. 6, pp. 1757-1767, Sept. 1999.
[3] Madhu Sudan, *Decoding of Reed-Solomon codes beyond the error-correction bound.* Journal of Complexity, vol. 13, no. 1, pp. 180-193, 1997.
[4] Michael T. McClellan *The Exact Solution of Systems of Linear Equations with Polynomial Coefficients.* J. ACM 20, pp. 563-588, 1973.
[5] Brice B. Boyer, Erich L. Kaltofen, *Numerical Linear System Solving With Parametric Entries By Error Correction.* SNC'14 Proceedings 2014 International Workshop on Symbolic-Numeric Computation, pp.33-38.
[6] Erich L. Kaltofen, Clément Pernet, Arne Storjohann, Cleveland Waddell, *Early Termination in Parametric Linear System Solving and Rational Function Vector Recovery with Error Correction.* ISSAC '17 Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, p. 237.
[7] Daniel Bleichenbacher, Aggelos Kiayias, Moti Yung, *Decoding Interleaved Reed-Solomon codes over Noisy Data.* ICALP Springer, pp. 97-108, 2003.
[8] Andrew Brown, Lorenz Minder, Amin Shokrollahi, *Probabilistic Decoding of Interleaved RS-Codes on the Q-ary symmetric channel.* In Proc. of IEEE Intern. Symposium on Inf. Theory, p. 327, 2004.
[9] Sven Puchinger and Johan Rosenkilde né Nielsen, *Decoding of interleaved Reed-Solomon codes using improved power decoding.* In Proc. of IEEE Intern. Symposium on Inf. Theory, Aachen, pp. 356-360, 2017.
[10] George Schmidt, Vladimir R. Sidorenko, Martin Bossert, *Collaborative Decoding of Interleaved Reed-Solomon Codes and Concatenated Code Designs.* IEEE Transactions on Information Theory, vol. 55, no. 7, pp. 2991-3012, July 2009.
[11] Antonia Wachter-Zeh, Alexander Zeh, Martin Bossert, *Decoding interleaved Reed-Solomon codes beyond their joint error-correcting capability.* Designs Codes and Cryptography, vol. 71, no. 2, pp. 261-281, 2014.
[12] George Schmidt, Vladimir R. Sidorenko, Martin Bossert, *Syndrome Decoding of Reed-Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis.* IEEE Transactions on Information Theory, vol. 56, no. 10, pp. 5245-5252, Oct. 2010.