Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes
Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore

To cite this version:

HAL Id: lirmm-02127793
https://hal-lirmm.ccsd.cnrs.fr/lirmm-02127793v2
Submitted on 9 Jul 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 different 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 $A(x)y = b(x)$ 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 $f(x)/g(x)$, where $f$ is a vector of polynomials and $g(x)$ is the least common denominator.

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 $\frac{dq+q}{q}$ where $dq$ 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

$$A(x)y(x) = b(x) \quad (1)$$

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 $m \geq n \geq 1$;
- $b(x)$ 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

$$y(x) = \frac{f(x)}{g(x)} = \left( \frac{f_1(x)}{g(x)}, \ldots, \frac{f_n(x)}{g(x)} \right)$$
where $g$ is the monic least common denominator, and
\[
\text{GCD}(f, g) = \text{GCD}(\text{GCD}(f_i, g)) = 1. \quad (2)
\]

In general, this solution can be found by evaluating the system at a certain number, say $L$, of distinct points $\alpha_i \in \mathbb{K}$ with $l \in \{1, \ldots, L\}$, 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 $\alpha_i$, provides $A_i \in \mathbb{K}^{m \times n}$ and $b_i \in \mathbb{K}^m$ which may not be equal to $A(\alpha_i)$ and $b(\alpha_i)$. More specifically, the resulting evaluations $A_i$ and $b_i$ are considered erroneous if $A_i f(\alpha_i) \neq g(\alpha_i)b_i$. In this scenario they proved that with
\[
L \geq L_{BK} := df + dg + 2e + t + 1 \quad (3)
\]
the number of points, it is possible to uniquely reconstruct the solution of the linear system (1), where

- $df \geq \deg(f) := \max_{1 \leq i \leq n} \deg(f_i)$,
- $dg \geq \deg(g)$,
- $e \geq |E|$ is a bound on the erroneous evaluations where
\[
E := \{ l \mid A_l f(\alpha_i) \neq g(\alpha_i)b_i \}
\]
- $t \geq |R|$ is a bound on the rank drops where
\[
R := \{ l \mid A_l f(\alpha_i) = g(\alpha_i)b_i \ \text{and rank}(A_l) < n \}
\]

Their method consists in solving the homogeneous linear system
\[
\begin{pmatrix}
\varphi_1(\alpha_i) \\
\varphi_2(\alpha_i) \\
\vdots \\
\varphi_n(\alpha_i)
\end{pmatrix}
A_l
\begin{pmatrix}
\varphi_1(\alpha_i) \\
\varphi_2(\alpha_i) \\
\vdots \\
\varphi_n(\alpha_i)
\end{pmatrix} - \psi(\alpha_i)b_i = 0
\]
\[l \in \{1, \ldots, L\} \quad (4)
\]
where
- $\varphi = (\varphi_1, \ldots, \varphi_n) \in (\mathbb{K}[x])^n$ 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 $\varphi_i$ and $\psi$. In particular, they proved the following:

**Theorem 1** ([5]). Under previous assumptions, let $(\varphi_{\text{min}}, \psi_{\text{min}})$ be the solution of (4) of minimal degree and $\psi_{\text{min}}$ monic. Then
\[
\varphi_{\text{min}} = \Lambda f, \quad \psi_{\text{min}} = \Lambda g
\]
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 $\mathbb{K} = \mathbb{F}_q$, $m = n$, $A_l = I_n$ and $g$ is the constant polynomial 1, then
\[
\begin{align*}
|b_l = f(\alpha_l) & \quad l \notin E, \\
|b_l \neq f(\alpha_l) & \quad l \in E.
\end{align*}
\]
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 $C$ be an $[n, k]$ RS code.

- we consider $r$ codewords $c_i \in C$. For any $i \in \{1, \ldots, r\}$, $c_i = (f_1(\alpha_1), \ldots, f_n(\alpha_n))$ where $f_i \in \mathbb{F}_q[x]$ has degree $\deg(f_i) \leq k - 1$ and $\{\alpha_1, \ldots, \alpha_n\}$ is the set of distinct evaluation points;
- we arrange these codewords row-wise and we obtain the $r \times n$ matrix $(c_i)_{1 \leq i \leq r} = (f_i(\alpha_j))_{1 \leq i \leq r}$;
- by interpreting this matrix as a row vector $(f(\alpha_j))_{1 \leq j \leq n} \in (\mathbb{F}_q)^n$, we obtain a codeword of an Interleaved RS code of length $n$, dimension $k$ over $\mathbb{F}_q$. The number of codewords $r$ is the amount of interleaving.

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

- $E \subset \{1, \ldots, n\}$ with $|E| \leq e$,
- polynomials $(f_1, \ldots, f_r)$, 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 $(f_1, \ldots, f_r)$.

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
\[
\begin{align*}
|b_l = f(\alpha_l) & \quad l \notin E, \\
|b_l \neq f(\alpha_l) & \quad l \in E.
\end{align*}
\]
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 $r$.

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,
\[
\begin{align*}
[m_1(\alpha_j) = y_{1j}E(\alpha_j)]_{1 \leq j \leq n} \\
\cdots \\
[m_r(\alpha_j) = y_{rj}E(\alpha_j)]_{1 \leq j \leq n}
\end{align*}
\]

where $g$ is the monic least common denominator, and
\[
\text{GCD}(f, g) = \text{GCD}(\text{GCD}(f_i, g)) = 1. \quad (2)
\]
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 \( r n \) equations and \( r(k + e) + e + 1 \) unknowns. Moreover,

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

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

and for each \( i \in \{1, \ldots, r\} \),

(i) if \( j \in E \), \( y_{ij} \) are uniformly distributed over \( \mathbb{F}_q \)

(ii) if \( j \not\in E \), \( y_{ij} = f_i(\alpha_j) \) and \( f_1, \ldots, f_r \) 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 \( r \geq 1 \),

\[
\frac{r(n - k)}{r + 1} \geq \frac{n - k}{2},
\]

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 first instance, we focus on the square case, i.e. \( q \) is prime. In particular, fol-

**Remark 1.** Starting from Remark 1 we reexamine the problem of solving a consistent, full rank, linear system (1), \( A(x)y(x) = b(x) \) with polynomial entries over a finite field \( \mathbb{F}_q \).

Interleaved RS code, or equivalently an instance of the SPR problem, where

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

and for each \( i \in \{1, \ldots, r\} \),

(i) if \( j \in E \), \( y_{ij} \) are uniformly distributed over \( \mathbb{F}_q \)

(ii) if \( j \not\in E \), \( y_{ij} = f_i(\alpha_j) \),

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

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 \( \frac{d q + e}{q} \) (where \( d q \) 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), \( A(x)y(x) = b(x) \) 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 \( y = \frac{f(\alpha)}{g(\alpha)} \) be the reduced unique solution as in (2).

We fix \( L \) evaluation points with

\[
L \geq L_{GLZ} := \left\lceil \frac{n(d f + e + 1 + d g) + e}{n} \right\rceil
\]

where

- \( d f \geq \text{deg}(f) := \max_{1 \leq i \leq n} \text{deg}(f_i) \),
- \( d g = \text{deg}(g) \),
- \( g(\alpha_l) \neq 0 \) for \( 1 \leq l \leq L \),
- \( e = |E| \) is the number of erroneous evaluations where
  \( E = \{ l \mid A_l f(\alpha_l) \neq g(\alpha_l) b_l \text{ and rank}(A_l) = n \} \).

**Remark 2.** In this way, since \( n \geq 1 \), we reduce the number of evaluation points,

\[
L_{GLZ} \leq L_{BK}.
\]

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 \( b_l \) 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 \( l \in \{1, \ldots, L\} \), the homogeneous linear systems

\[
A_l \gamma_l - \sigma_l b_l = 0.
\]

**Remark 3.** Let \( C_l \) be the coefficients matrix of any of these linear systems.

\[
C_l = [A_l] - b_l.
\]

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 \( (\gamma_1, \sigma_1) = (\gamma_1, \ldots, \gamma_n, \sigma_1) \) be the vector that generates the right kernel of \( C_l \), with \( l \in \{1, \ldots, L\} \).

Then,

\[
\frac{2 u_l}{\sigma_l} = \frac{f(\alpha_l)}{g(\alpha_l)} \quad \forall l \not\in E.
\]

**Proof.** By our assumptions, \( g(\alpha_l) \neq 0 \) for any \( l \not\in E \). Now, since the right kernel is one dimensional, its generator \( (\gamma_1, \sigma_1) = (\gamma_1, \ldots, \gamma_n, \sigma_1) \) is a nonzero vector, and also \( \sigma_l \neq 0 \). Let \( l \not\in E \), be a correct evaluation. Since \( A_l \gamma_l - \sigma_l b_l = 0 \) and \( A_l f(\alpha_l) = g(\alpha_l) b_l \), then \( A_l f(\alpha_l) \sigma_l - g(\alpha_l) \gamma_l = 0 \). The matrix \( A_l \) is full rank, hence \( f(\alpha_l) \sigma_l - g(\alpha_l) \gamma_l = 0 \). Then we can conclude that \( \frac{2 u_l}{\sigma_l} = \frac{f(\alpha_l)}{g(\alpha_l)} \).

Following the previous notations, if we denote by \( y_l := \frac{u_l}{\sigma_l} = \frac{1}{2}\beta(\gamma_1, \ldots, \gamma_n) \in (\mathbb{F}_q)^n \), for any \( l \in \{1, \ldots, L\} \) we have that

\[
y_l = \frac{f(\alpha_l)}{g(\alpha_l)}, l \not\in E
\]
Remark 4. By our probabilistic assumption, \((y_{li})_{i \in E}\) 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

\[
\begin{cases}
\varphi(\alpha_1) = y_1 \psi(\alpha_1) \\
\quad \ldots \\
\varphi(\alpha_L) = y_L \psi(\alpha_L)
\end{cases}
\]

or, in other terms, if we denote \(y_{l} = (y_{l1}, \ldots, y_{ln})\) for \(l \in \{1, \ldots, L\}\),

\[
\begin{bmatrix}
\varphi(\alpha) = y_1 \psi(\alpha) \\
\quad \ldots \\
\varphi(\alpha) = y_n \psi(\alpha)
\end{bmatrix}_{1 \leq i \leq L}
\]

where

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

The linear system (9) has \(nL\) equations and \(n(df+e+1) + dg+e+1\) unknowns, which are the coefficients of \(\varphi\) and \(\psi\). The coefficient matrix of the system (9) is

\[
M_y := \begin{pmatrix}
V_{df+e+1} & -D_1 V_{dg+e+1} & \cdots & -D_n V_{dg+e+1} \\
\vdots & \vdots & & \vdots \\
V_{df+e+1} & -D_1 V_{dg+e+1} & \cdots & -D_n V_{dg+e+1}
\end{pmatrix}
\]

where,

- \(V_i = (\alpha_i^{i-1})_{1 \leq i \leq L}\) is the \(L \times t\) Vandermonde matrix,
- for \(i \in \{1, \ldots, n\}\), \(D_i\) is the diagonal matrix with \(y_{i1}, \ldots, y_{Li}\) on the diagonal.

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

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 \(M_y\) is one with probability at least

\[
1 - \frac{df+e}{q}.
\]

The cornerstone of the proof is the following lemma.

Lemma 1. There exists a random draw of \((y_{li})_{i \in E}\) such that the dimension of the right kernel of \(M_y\) is one.
Data: \((A_l, b_l)_{1 \leq l \leq L}\) and \(df, dg, e\)

Result: \((f, g)\) or fail

\[ L := \left\lceil \frac{n(df + e + 1) + dg + e}{n} \right\rceil; \]

for \(i = 1, \ldots, L\) do

- find a basis \(\{(\gamma_i, \sigma_i)\}\) of the right kernel of \(C_i\);
- \(y_i := \frac{\gamma_i}{\sigma_i}\);
- construct the matrix \(M_y\) of the key equation (9);
- if \(\text{rank}(M_y) = n(df + e + 1) + dg + e\) then
  - compute a solution \((\varphi, \psi)\) with \(\psi\) monic;
  - \(\Lambda := \text{GCD}(\varphi, \psi)\);
  - return \((\frac{\varphi}{\Lambda}, \frac{\psi}{\Lambda})\);
- else
  - return fail;

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 \(L_{GLZ} < L_{BK}\), 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 20 different linear systems with polynomial coefficients, of size 3. For every system we apply our algorithm 1000 times, with \(e = 5\) errors and \(dg = 2\). We compute the percentage \(p\) of the number of times the algorithm fails. We compare our experimental results with \(p_{GLZ}\), i.e. the failing probability of Theorem 4, and with \(p_{BMS}\), i.e. the failing probability of [8]. We recall that the last one is linked to a related problem, the decoding of Interleaved RS, but not to our problem. We obtain the following results:

<table>
<thead>
<tr>
<th>(q)</th>
<th>(p)</th>
<th>(p_{GLZ})</th>
<th>(p_{BMS})</th>
<th>(p^*) (see below)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2(^a)</td>
<td>0.3%</td>
<td>43.7%</td>
<td>7.1%</td>
<td>0.4%</td>
</tr>
<tr>
<td>2(^b)</td>
<td>0.1%</td>
<td>21.9%</td>
<td>3.3%</td>
<td>0.2%</td>
</tr>
<tr>
<td>2(^c)</td>
<td>0</td>
<td>10.9%</td>
<td>1.6%</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

First of all, these experiments suggest that the failing probability is very small and that it decreases when the cardinality of the field grows. Moreover, since experiments are significantly under our theoretical bound, our bound could be strongly improved, which we leave to future work. This may also suggest that our bound \(L_{GLZ}\) is not optimal. Therefore, we have done some experiments using an inferior number of evaluation points

\[ L = \left\lceil \frac{n(df + e + 1) + dg + e}{n} \right\rceil. \]

and we note \(p^*\) the corresponding probability. This new \(L\) is chosen in such a way that the coefficient matrix \(M_y\) has now \(nL\) equations and \(nL - 1\) unknowns so that its kernel might have dimension 1. We can observe that also in this case, we have a very high probability to reconstruct the correct vector rational solution in practice. Therefore future work could try to extend our results to this new number of evaluation points.

Finally we can remark that, since we use an evaluation interpolation technique, there exist finitely many evaluation points \(\alpha_l\) such that the evaluated matrix \(A(\alpha_l)\) is not full rank anymore. In this work, we have chosen the evaluation points such that the evaluated matrix is full rank, thus omitting the rank drop analysis, which we leave again to future work.

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