Enhancing simultaneous rational function recovery: adaptive error correction capability and new bounds for applications

Eleonora Guerrini, Romain Lebreton, Ilaria Zappatore

Enhancing simultaneous rational function recovery: adaptive error correction capability and new bounds for applications

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

***Abstract*—In this work we present some results that allow to improve the decoding radius in solving polynomial linear systems with errors in the scenario where errors are additive and randomly distributed over a finite field. The decoding radius depends on some bounds on the solution that we want to recover, so their overestimation could significantly decrease our error correction capability. For this reason, we introduce an algorithm that can bridge this gap, introducing some *ad hoc* parameters that reduce the discrepancy between the estimate decoding radius and the effective error correction capability.**

I. Introduction

The family of Reed Solomon codes (RS) is a large class of very well studied algebraic codes. They are MDS codes, they perform list-decoding and have efficient decoding algorithms that can be viewed in a computer algebra setting as rational reconstruction problems. More specifically, we are interested on Interleaving Reed Solomon (IRS) codes. IRS codes are well studied and can be decoded efficiently by a bounded distance (BD) decoder beyond the unique correction capability radius for almost all error patterns (*cf.* [1], [2], [3]).

In this work we focus on the problem of solving a polynomial linear system with errors (PLSwE), introduced in [4] and [5]. Since the solution of PLSwE is a vector of rational function, the PLSwE is a special case of the problem of reconstructing a vector of rational function given its evaluations, some of which could be erroneous (the simultaneous rational function recovery, shortly SRFR). In [6] we proposed an algorithm, based on IRS decoding, that allows to solve SRFR (and in particular PLSwE), correcting more than [4] and [5] in a probabilistic setting. In this paper, we improve the technique of [6], increasing the error correction capability. Since we want to recover a vector of rational functions $\boldsymbol{y}$, which is solution of a polynomial linear system over a finite field, $A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x)$, we introduce a new bound on the error correction capability which also depends on the bounds on the degrees of A and $\boldsymbol{b}$. Moreover, the knowledge of the degrees of the solution would allows us to reach an *ideal* error correction capability, but we do not know these degrees and their overestimation could significantly decrease the amount of errors we could correct. For this reason, we introduce a *parameter oblivious* algorithm for the PLSwE that allows us to get closer to the ideal error correction capability, without knowing the real degrees.

The paper is structured as follows: in Section II we recall standard facts for IRS codes, in Section III we introduce our problem (PLSwE) and we set up the model. In Section IV we introduce the generalization of the PLSwE, *i.e* the simultaneous rational function recovery (SRFR). We present a technique, based on IRS decoding, that allows to achieve a bigger error correction capability. In Section V, we propose our algorithm and in Section VI, we present our main theorem, the cornerstone of all our technical results. Finally in Section VII, we expose our open problems and conclusions.

II. Interleaved Reed-Solomon codes

A Reed-Solomon (RS) code of length n and dimension k over $\mathbb{F}_q$ can be defined as the set $\mathcal{C}_{RS}(n,k) = \{(f(\alpha_1),\dots,f(\alpha_n)) \mid f \in \mathbb{F}_q[x], \deg(f) \leq k-1\}$ where $\boldsymbol{\alpha} := \{\alpha_1,\dots,\alpha_n\}$ is the set of distinct evaluation points over $\mathbb{F}_q$. For $l \geq 1$, an l-Interleaved Reed-Solomon (IRS) code is defined by the direct sum of l RS codes $\mathcal{C}_{RS}(n,k_i)$ sharing the same set of evaluation points, *i.e.*

$$\mathcal{C}_{IRS}(n,\boldsymbol{k}) = \left\{(\boldsymbol{c}_i)_{1\leq i\leq l} \in (\mathbb{F}_q)^{l\times n} \mid \boldsymbol{c}_i \in \mathcal{C}_{RS}(n,k_i)\right\}$$

If $k = k_1 = \ldots = k_l$, we say that an IRS is homogeneous and we denote it $\mathcal{C}_{IRS}(n,k;l)$. From now, we will focus only on homogeneous IRS codes. Codewords in $\mathcal{C}_{IRS}(n,k;l)$ can be seen as evaluations of $\boldsymbol{f}(x) = (f_1,\dots,f_l) \in (\mathbb{F}_q[x])^{l\times 1}$ with $\deg(\boldsymbol{f}) := \max_{1\leq i\leq l}(\deg(f_i)) \leq k-1$.

We now consider the decoding instance $\Upsilon = C + \Xi \in (\mathbb{F}_q)^{l\times n}$ where $C \in \mathcal{C}_{IRS}(n,k;l)$ and Ξ is the error matrix. We can see $\Upsilon = (\boldsymbol{y}_j)_{1\leq j\leq n}$ and $\Xi = (\boldsymbol{e}_j)_{1\leq j\leq n}$ both in $(\mathbb{F}_q^l)^n$. As error model we consider *burst errors*, *i.e.* the error positions are the nonzero columns of the error matrix Ξ. In detail, for any $1 \leq j \leq n$, the set of error positions is $E := \{1 \leq j \leq n \mid \boldsymbol{e}_j \neq \boldsymbol{0}\}$. The number of errors is then $|E|$.

Since $C = (\boldsymbol{f}(\alpha_1),\dots,\boldsymbol{f}(\alpha_n))$ for $\boldsymbol{f} \in (\mathbb{F}_q[x])^{l\times 1}$, $\deg(\boldsymbol{f}) \leq k-1$, for any $1 \leq j \leq n$,

$$\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j) + \boldsymbol{e}_j. \tag{1}$$

In order to decode C, we need to recover the vector of polynomials $\boldsymbol{f}(x)$.

For $1 \leq i \leq l$, let $Y_i \in \mathbb{F}_q[x]$ be the *Lagrangian polynomials* such that $Y_i(\alpha_j) = y_{ij}$, for $1 \leq j \leq n$, and

$\deg(Y_i) < n$ and let $\Lambda = \prod_{j \in E}(x - \alpha_j)$ be the *error locator polynomial*. We observe that for any $1 \leq i \leq l$, $\Lambda Y_i \equiv \Lambda f_i \mod \prod_{j=1}^{n}(x - \alpha_j)$. This is a nonlinear equation in the unknowns $\Lambda(x)$ and $\boldsymbol{f}(x)$. A classic approach for decoding RS codes (*cf.* [7], [8]), that can be extended to IRS codes, consists in the *linearization* of these equations, by replacing $\Lambda(x)$ and $\Lambda(x)f_i(x)$ with the unknowns $\lambda(x)$ and $\varphi_i(x)$. In this way we obtain the *key equation*

$$\lambda Y_i \equiv \varphi_i \mod \prod_{j=1}^{n}(x - \alpha_j). \tag{2}$$

In order to decode, it suffices to study the set S of $(\lambda, \varphi_1, \ldots, \varphi_l) \in \mathbb{F}_q^{(l+1)\times 1}$ which verify (2) and such that $\deg(\lambda) \leq |E|$ and $\deg(\varphi_i) \leq |E| + k - 1$. IRS codes, can be decoded by efficient BD decoders beyond the unique decoding radius. These decoders succeed *for almost all* error patterns [1]. With "almost all" we mean that there exists a polynomial R such that the decoder succeeds for all instances Υ satisfying $R(\Upsilon) \neq 0$. A quite tight estimation of the probability of failure can be founded in [2] and improvements on the decoding radius recently appeared in [3].

In the next section we will remark the parallel between the problem of solving polynomial linear systems with errors and the IRS decoding. (*cf.* [6]).

III. Polynomial Linear System Solving With Errors

Given $l \geq 1$, we study the problem of solving a consistent full rank polynomial linear system over a finite field $\mathbb{F}_q$,

$$A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x) \tag{3}$$

where $A(x) \in (\mathbb{F}_q[x])^{l\times l}$ is full rank and $\boldsymbol{b}(x) \in (\mathbb{F}_q[x])^{l\times 1}$.

Any solution of this system is a vector of rational functions, *i.e.* $\boldsymbol{y}(x) = \left(\frac{\hat{f}_1(x)}{g_1(x)}, \ldots, \frac{\hat{f}_l(x)}{g_l(x)}\right) \in \mathbb{F}_q(x)^{l\times 1}$. Let $g(x)$ be the monic least common denominator, then there is a unique solution

$$\boldsymbol{y}(x) = \left(\frac{f_1(x)}{g(x)}, \ldots, \frac{f_l(x)}{g(x)}\right) \in \mathbb{F}_q(x)^{l\times 1} \tag{4}$$

that is also *reduced*, *i.e.* $\gcd(f_1(x), \ldots, f_l(x), g(x)) = 1$. Our main aim is to reconstruct such a solution. Note that this common denominator representation can be more compact and it appears frequently for solutions of linear systems computed by the Cramer's rule.

As in [4], [5], [6], we will analyze a scenario where some *errors* occur. In detail, we fix n evaluation points $\boldsymbol{\alpha}$ and we suppose that any evaluation point is not a root[1] of the polynomial $g(x)$. In our model, there is a black box which, for any evaluation point α_j, gives a solution $\boldsymbol{y}_j \in (\mathbb{F}_q)^{l\times 1}$ of the evaluated system of linear equations[2] $A(\alpha_j)\boldsymbol{y}_j = b(\alpha_j)$. However this black box could do some errors in the computations.

[1] In [4] and [5], the authors study a more general case. They fix n distinct evaluation points, without any assumptions about the roots of $g(x)$. In our work, we need this assumption in order to prove our results.

[2] We suppose that for any evaluation points α_j, the rank of the evaluated matrix $A(\alpha_j)$ still remains full. In [4] and [5] there was also studied the rank drop case.

Definition 1. *(Erroneous evaluation points [4])*

An evaluation point α_j is erroneous iff $\boldsymbol{y}_j \neq \frac{\boldsymbol{f}(\alpha_j)}{g(\alpha_j)}$. We denote by $E := \left\{1 \leq j \leq n \mid \boldsymbol{y}_j \neq \frac{\boldsymbol{f}(\alpha_j)}{g(\alpha_j)}\right\}$ the set of positions of the erroneous evaluations.

We can now formalize our problem,

Definition 2. *(Polynomial linear system solving with errors)*

The problem of solving a polynomial linear system with errors (denoted PLSwE) consists in recovering the vector of rational functions (4), i.e. the unique solution of a consistent, full rank polynomial linear system (3), given

- *n evaluation points $\boldsymbol{\alpha}$,*
- *$d_f \geq \deg(\boldsymbol{f})$, $d_g \geq \deg(g)$, $d_A \geq \deg(A)$, $d_b \geq \deg(\boldsymbol{b})$,*
- *the black box output $(y_{ij})_{\substack{1\leq i\leq l\\ 1\leq j\leq n}}$,*
- *a bound on the number of erroneous evaluation points $\varepsilon \geq |E|$.*

Remark 3. *We observe that if $j \in E$, then there exists a nonzero $\boldsymbol{e}_j \in (\mathbb{F}_q)^{l\times 1}$ such that $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)/g(\alpha_j) + \boldsymbol{e}_j$.*

In general, for any $1 \leq j \leq n$, $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)/g(\alpha_j) + \boldsymbol{e}_j$ where $\boldsymbol{e}_j \neq \boldsymbol{0}$ iff $j \in E$.

We can conclude that the PLSwE can be seen as the *extension* of the problem of decoding an IRS code (see (1)) to the rational function case.

IV. simultaneous rational function recovery

Definition 4. *(Simultaneous rational function recovery)*

Fix some parameters $n, q, d_f, d_g, \varepsilon, \boldsymbol{\alpha}$ such that $0 \leq d_f, d_g, \varepsilon < n \leq q$. An instance of the simultaneous rational function recovery problem (shortly SRFR) is a matrix $(\boldsymbol{y}_j)_{1\leq j\leq n} = (y_{ij})_{\substack{1\leq i\leq l\\ 1\leq j\leq n}} \in (\mathbb{F}_q)^{l\times n}$ such that there exists

- *a reduced vector of rational functions $\frac{\boldsymbol{f}(x)}{g(x)} \in (\mathbb{F}_q(x))^{l\times 1}$, where $\deg(\boldsymbol{f}) \leq d_f$, $\deg(g) \leq d_g$ and $\forall j,\ g(\alpha_j) \neq 0$.*
- *a matrix $(\boldsymbol{e}_j)_{1\leq j\leq n} = (e_{ij})_{\substack{1\leq i\leq l\\ 1\leq j\leq n}}$ such that its* column support $E := \{1 \leq j \leq n \mid \boldsymbol{e}_j \neq \boldsymbol{0}\}$ *satisfies $|E| \leq \varepsilon$;*

which satisfy $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)/g(\alpha_j) + \boldsymbol{e}_j$. The solution of an SRFR instance is $(\boldsymbol{f}(x), g(x))$.

This problem was introduced in [9] and in [6]. We now present a recovering algorithm in the model of IRS codes. In detail, let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of the SRFR problem with parameters n, d_f, d_g, ε (we will omit q and $\boldsymbol{\alpha}$ for simplicity). As for IRS codes we introduce the error locator polynomial $\Lambda = \prod_{j\in E}(x - \alpha_j)$ and the Lagrangian polynomials $(Y_i(x))_{1\leq i\leq l}$. We observe that $\boldsymbol{f}, g, \Lambda$ still satisfy $\Lambda g Y_i \equiv \Lambda f_i \mod \prod_{j=1}^{n}(x - \alpha_j)$ so, as for IRS codes, we study the *key equations*

$$\psi Y_i \equiv \varphi_i \mod \prod_{j=1}^{n}(x - \alpha_j) \text{ for } 1 \leq i \leq l, \tag{5}$$

whose unknowns are the polynomials $\varphi_i(x)$ and $\psi(x)$ such that $\deg(\varphi_i) \leq d_f + \varepsilon$ and $\deg(\psi) \leq d_g + \varepsilon$. We observe that this is equivalent to study the evaluated system

$$[\varphi_i(\alpha_j) = y_{ij}\psi(\alpha_j)]_{\substack{1\leq i\leq l\\ 1\leq j\leq n}}. \tag{6}$$

In this case the unknowns are the $d_f + \varepsilon + 1$ coefficients of any $\varphi_i(x)$ and the $d_g + \varepsilon + 1$ coefficients of $\psi(x)$.

Let $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ be the $\mathbb{F}_q$-vector space of $(\boldsymbol{\varphi},\psi) = (\varphi_1,\ldots,\varphi_l,\psi) \in (\mathbb{F}_q[x])^{(l+1)\times 1}$ which verify (5) and the degree constraints $deg(\boldsymbol{\varphi}) \leq d_f + \varepsilon$ and $deg(\psi) \leq d_g + \varepsilon$.

Remark 5. *Since we can consider the key equations in the polynomial (5) or evaluated version (6), studying the solution space $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ is equivalent to study the right kernel of the coefficient matrix $M_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ (see [1], [10]) of the evaluated key Equation* (6)*. In detail,*

$$M_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \begin{pmatrix} V_{d_f+\varepsilon+1} & & -D_1 V_{d_g+\varepsilon+1} \\ & \ddots & \vdots \\ & V_{d_f+\varepsilon+1} & -D_l V_{d_g+\varepsilon+1} \end{pmatrix} \tag{7}$$

where $V_t = (\alpha_j^{i-1})_{\substack{1\leq j\leq n\\ 1\leq i\leq t}}$ is an $n \times t$ Vandermonde matrix and D_i is the matrix with $y_{i1},\ldots,y_{in}$ on the diagonal.

Theorem 6. (cf. *[4]) If $\varepsilon \leq \frac{(n-d_f-d_g-1)}{2} =: \varepsilon_{BK}$, then all solutions $(\boldsymbol{\varphi},\psi) \in S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ lead to the same vector of rational functions $\boldsymbol{f}/g$, i.e. $\frac{\boldsymbol{\varphi}(x)}{\psi(x)} = \frac{\boldsymbol{f}(x)}{g(x)}$.*

This means that below this error correction capability ε_{BK}, all the elements $(\boldsymbol{\varphi},\psi) \in S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ are polynomial multiples of the unique solution $(\Lambda\boldsymbol{f},\Lambda g)$. Besides, it is possible to prove that $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq d_{fgE}}$ where

$$d_{fgE} = \min(d_f - \deg(\boldsymbol{f}), d_g - \deg(g)) + \varepsilon - |E|. \tag{8}$$

Hence we can uniquely reconstruct the vector of rational functions $\boldsymbol{f}/g$. We observe that if $d_f = \deg(\boldsymbol{f})$ (or $d_g = \deg(g)$) and $|E| = \varepsilon = \varepsilon_{BK}$ the solution space $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ is a vector space of dimension 1, spanned by $(\Lambda\boldsymbol{f},\Lambda g)$.

In [6], motivated by the analogy of the SRFR problem and the decoding of IRS codes, we proved that, under some assumptions on the error distribution, we can correct more than ε_{BK} errors with a certain probability.

We now set up our probabilistic model. We focus on $(\boldsymbol{y}_j)_{1\leq j\leq n}$, an instance of the SRFR with parameters n, d_f, d_g, ε with *random errors*. In detail, we suppose that $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)/g(\alpha_j) + \boldsymbol{e}_j$, where $\boldsymbol{f}(x)/g(x)$ is a reduced fraction with degrees bounded by d_f, d_g and such that $g(\alpha_j) \neq 0$. Moreover $\boldsymbol{e}_j$ is uniformly distributed in $(\mathbb{F}_q)^{l\times 1}$ if $j \in E$ and $\boldsymbol{e}_j = \boldsymbol{0}$ if $j \notin E$, for a fixed error position set E with $|E| \leq \varepsilon$. Under this assumption we have the following.

Theorem 7. (cf. *[6]) Fix n, d_f, d_g and $\varepsilon_{GLZ} = \frac{l(n-d_f-d_g-1)}{l+1}$. Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of the SRFR with random errors and parameters $n, d_f, d_g = \deg(g), \varepsilon = |E| = \lfloor\varepsilon_{GLZ}\rfloor$. Then the corresponding solution space $S_{\boldsymbol{y},d_f+|E|,\deg(g)+|E|}$ is a vector space of dimension* 1*, spanned by the solution $(\Lambda\boldsymbol{f},\Lambda g)$, with probability at least $1 - \frac{\deg(g)+|E|}{q}$.*

In this work we extend the previous result of [6] to the general case where we only know a bound $d_g \geq \deg(g)$ and a bound ε on the number of errors $|E|$, with $\varepsilon \leq \varepsilon_{GLZ} = \frac{l(n-d_f-d_g-1)}{l+1}$.

Theorem 8. *Fix n, d_f, d_g and $\varepsilon \leq \varepsilon_{GLZ}$ and take d_{fgE} as in (8). Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of SRFR with random errors and parameters n, d_f, d_g, ε. Then with probability $\geq 1 - \frac{d_g+\varepsilon}{q}$ we get $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq d_{fgE}}$.*

A. Simultaneous rational function recovery of a solution of a polynomial linear system with errors. By Remark 3 we can deduce that the PLSwE coincides with SRFR with parameters n, d_f, d_g, ε. The matrix $(\boldsymbol{y}_j)_{1\leq j\leq n}$, which is the black box output, is then an instance of this problem. Hence, all the results of the previous section hold. Furthermore, since we want to reconstruct a vector of rational functions that is a solution of a polynomial linear system, it is possible to introduce a bound on the error correction capability which depends on the bounds on the degree of the polynomial matrix $A(x)$ and on $\boldsymbol{b}(x)$ (as shown in [5]).

Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of PLSwE with parameters n, d_f, d_g, d_A, d_b. Recall from the previous section that $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon}$ is the set of $(\boldsymbol{\varphi},\psi)$ which verify (5) and such that $\deg(\boldsymbol{\varphi}) \leq d_f + \varepsilon$ and $\deg(\psi) \leq d_g + \varepsilon$.

Theorem 9. *(see [5]) Let $\varepsilon_{KPS} := \frac{n-\max(d_A+d_f,d_b+d_g)-1}{2}$. If $\varepsilon \leq \varepsilon_{KPS}$, then $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq d_{fgE}}$.*
The same result holds if we consider $\varepsilon \leq \max(\varepsilon_{BK}, \varepsilon_{KPS})$.

There are some cases in which this error correction capability is bigger than ε_{BK}. In fact, as proved in [5], when all the bounds are tight, $\varepsilon_{BK} < \varepsilon_{KPS}$ iff $\deg(g(x)) > \deg(A(x))$.

In this paper, we will introduce a new bound on the error correction capability based on d_A and d_b under probabilistic assumptions. In particular, given a polynomial linear system as in (3), we suppose that the black box returns $(\boldsymbol{y}_j)_{1\leq j\leq n}$ where $\boldsymbol{y}_j$ is uniformly distributed in $(\mathbb{F}_q)^{l\times 1}$ if $j \in E$ (instead of $\boldsymbol{y}_j \neq \boldsymbol{f}(\alpha_j)/g(\alpha_j)$). By Remark 3, $\boldsymbol{y}_j = \frac{\boldsymbol{f}(\alpha_j)}{g(\alpha_j)} + \boldsymbol{e}_j$ and so our probabilistic assumption on the black box output is indeed an assumption on the error distribution, *i.e.* $\boldsymbol{e}_j$ is uniformly distributed in $(\mathbb{F}_q)^{l\times 1}$ (instead of $\boldsymbol{e}_j \neq \boldsymbol{0}$), when $j \in E$. We will call PLSwE with random errors, the PLSwE in this error model.

Theorem 10. *Fix n, d_f, d_g, d_A, d_b, take d_{fgE} as in (8) and,*

$$\varepsilon \leq \varepsilon_{GLZ2} := \frac{l(n - \max(d_A + d_f, d_b + d_g) - 1)}{l+1}.$$

Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of PLSwE with random errors with parameters n, d_f, d_g, d_A, d_b. Then with probability at least $1 - \frac{dg+\varepsilon}{q}$ we get $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq d_{fgE}}$.
Thus the same result holds when $\varepsilon \leq \max(\varepsilon_{GLZ}, \varepsilon_{GLZ2})$.

We will prove Theorems 8 and 10 in Section VI.

V. Parameter oblivious decoding algorithm

The PLSwE problem takes as input some degree bounds d_f and d_g, hence all our error correction capabilities until now depend on these bounds, *e.g.* $\varepsilon_{GLZ} = \frac{l(n-d_f-d_g-1)}{l+1}$. Most importantly, our technique for solving the PLSwE requires such degree bounds to decode up to this capability.

Ideally we could decode up to $\frac{l(n-\deg(\boldsymbol{f})-\deg(g)-1)}{l+1}$ errors by taking the bounds tight, *i.e.* $d_f = \deg(\boldsymbol{f}), d_g = \deg(g)$. Our lack of knowledge of the real degrees $\deg(\boldsymbol{f}), \deg(g)$ limits us to correct this ideal amount of errors. Indeed, the

bounds d_f and d_g could overestimate the degrees of $\boldsymbol{f}(x)$ and $g(x)$, thus significantly decreasing all our error correction capability bounds.

In this work, we propose a *parameter oblivious* ([11], [9]) algorithm that allows to get closer to the ideal error correction capability even without the knowledge of the real degrees.

In [11] the authors already observed that even for classic RS codes (Section II), the knowledge of a bound instead of the real degree of f, could decrease the error correction capability. They proposed an algorithm for standard RS codes that allows to correct up to $\frac{n-\deg(f)-1}{2} \geq \frac{n-k}{2}$ errors.

On the other hand, in [5] it was introduced an algorithm for solving the PLSwE up to $|E| \leq \max(\varepsilon'_{BK}, \varepsilon'_{KPS})$ where

$$\varepsilon'_{BK} := \tfrac{n-\max(\deg(\boldsymbol{f})+d_g, \deg(g)+d_f)-1}{2} \geq \varepsilon_{BK},$$
$$\varepsilon'_{KPS} := \tfrac{n-\max(d_A+\deg(\boldsymbol{f})), d_b+\deg(g))-1}{2} \geq \varepsilon_{KPS}$$

In this work, we propose an algorithm that succeeds for almost all instances $(\boldsymbol{y}_j)_{1\leq j\leq n}$ of a PLSwE with parameters $n, d_f, d_g, d_A, d_b, \varepsilon$ whenever $|E| \leq \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$ where

$$\varepsilon'_{GLZ} := n - \max(\deg(\boldsymbol{f}) + d_g, d_f + \deg(g)) - \lceil \tfrac{\varepsilon}{l} \rceil - 1 \geq \varepsilon_{GLZ}$$
$$\varepsilon'_{GLZ2} := n - \max(d_A + \deg(\boldsymbol{f}), d_b + \deg(g)) - \lceil \tfrac{\varepsilon}{l} \rceil - 1 \geq \varepsilon_{GLZ2}$$

We will explain later where these bounds come from. Our new capability ε'_{GLZ} can be greater than ε'_{BK}, especially when ε is a tight bound on the number of errors. In particular, if we assume that $|E| \leq \varepsilon'_{GLZ}$, or equivalently if $\varepsilon = \varepsilon'_{GLZ}$, then ε'_{GLZ} becomes

$$\varepsilon'_{GLZ} = \frac{l(n - \max(\deg(\boldsymbol{f}) + d_g, \deg(g) + d_f) - 1)}{l+1} \geq \varepsilon'_{BK}.$$

The same holds for ε'_{GLZ2} w.r.t. ε'_{KPS}.

The main idea consists in the introduction of some others parameters δ_f, δ_g, ξ and on the study of the solution space of the key equation 5 with new degree constraints $\delta_f + \xi$ and $\delta_g + \xi$. As in (8) we define,

$$\delta_{fgE} := \min(\delta_f - \deg(\boldsymbol{f}), \delta_g - \deg(g)) + \xi - |E|. \quad (9)$$

Informally speaking, we will see in the following theorem that the introduction of these new degree constraints will allow us to increase the error correction capability.

Theorem 11. *(Parameter oblivious algorithm)*

If $|E| \leq \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$ then Algorithm **1** *outputs $(\boldsymbol{\varphi}, \psi)$ for all instances $(\boldsymbol{y}_j)_{1\leq j\leq n}$ of the PLSwE. Moreover $(\boldsymbol{\varphi}, \psi) = (\Lambda\boldsymbol{f}, \Lambda g)$ with probability $\geq 1 - \frac{2(d_g+\varepsilon)}{q}$.*

If $|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$, then Algorithm **1** *returns "$|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$" with probability $\geq 1 - \frac{2(d_g+\varepsilon)}{q}$.*

The fact that the algorithm can (probabilistically) detect if $|E|$ exceeds the error correction capability could be used inside another algorithm that would dynamically increase the redundancy n by requesting evaluation on new points, (*cf.* [5], Algorithm 4.1).

Remark 12. *In order to compute the nonzero minimal degree solution (e.g. in line 7 of Algorithm 1), we can use two different approaches: [5] uses column echelon form of the basis of the $\ker(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi})$ whereas [12] proposes $\mathbb{F}_q[x]$-module techniques. The latter approach yields the best complexity, i.e. $O^{\sim}(l^{\omega-1}n)$ arithmetic operations in $\mathbb{F}_q$ where $\omega < 2.38$ is the linear algebra exponent.*

Algorithm 1: Parameter Oblivious Algorithm

Data: $(y_{ij})_{\substack{1\leq i\leq l \\ 1\leq j\leq n}}$, an instance of PLSwE with parameters $n, d_f, d_g, d_A, d_b, \varepsilon$

Result: $(\boldsymbol{\varphi}, \psi)$ (equal to $(\Lambda\boldsymbol{f}, \Lambda g)$ with high probability) or "$|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$"

1 $\delta_f + \xi \leftarrow n - d_g - \lceil \frac{\varepsilon}{l} \rceil - 1$; $\delta_g + \xi \leftarrow n - d_f - \lceil \frac{\varepsilon}{l} \rceil - 1$
2 Let $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ be the solution space of the key equation 5 with degree constraints $\delta_f + \xi$, $\delta_g + \xi$.
3 **if** $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi} \neq \{(\boldsymbol{0}, 0)\}$ **then**
4 | **return** $(\boldsymbol{\varphi}, \psi)$ the non zero element of $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ with minimal degrees
5 $\delta_f + \xi \leftarrow n - d_A - \lceil \frac{\varepsilon}{l} \rceil - 1$; $\delta_g + \xi \leftarrow n - d_b - \lceil \frac{\varepsilon}{l} \rceil - 1$
6 **if** $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi} \neq \{(\boldsymbol{0}, 0)\}$ **then**
7 | **return** $(\boldsymbol{\varphi}, \psi)$ the non zero element of $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ with minimal degrees
8 **return** "$|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$";

VI. Technical results

Theorem 13. *Fix $\delta_f, \delta_g, \xi \geq 0$ and let δ_{fgE} as in (9).*

Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of the PLSwE with parameters $n, \deg(\boldsymbol{f}), \deg(g), |E|, \deg(A), \deg(\boldsymbol{b})$, where $n \geq \min(N_1, N_2)$ and

- $N_1 := \max(\delta_f + \deg(g), \delta_g + \deg(\boldsymbol{f})) + \xi + \lceil |E|/l \rceil + 1$,
- $N_2 := \max(\delta_f + \deg(A), \delta_g + \deg(\boldsymbol{b})) + \xi + \lceil |E|/l \rceil + 1$,

Then, with probability at least $1 - \frac{\delta_g+\xi}{q}$ we have that

$$S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq \delta_{fgE}} \quad (10)$$

By convention, if $\delta_{fgE} < 0$, we set $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq \delta_{fgE}} = \{(\boldsymbol{0}, 0)\}$.

Proof. We start by proving that there exists a PLSwE instance $(\boldsymbol{y}_j)_{1\leq j\leq}$ with the same parameters such that Eq. (10). We take a partition $E = \sqcup_{i=1}^{l} I_i$ with the constraint $|I_i| \leq \lceil |E|/l \rceil$ (it exists since $l\lceil |E|/l \rceil \geq |E|$). For $j \in E$, we define $1 \leq i(j) \leq l$ as the unique index such that $j \in I_{i(j)}$.

We separate two cases to prove that $\boldsymbol{\varphi}(x)g(x) = \boldsymbol{f}(x)\psi(x)$. First if $\min(N_1, N_2) = N_1$, then for all $j \in E$ we choose $\boldsymbol{y}_j \in (\mathbb{F}_q)^{l\times 1}$ such that $\boldsymbol{f}(\alpha_j) - g(\alpha_j)\boldsymbol{y}_j = \boldsymbol{\nu}_{i(j)}$, where $\boldsymbol{\nu}_{i(j)} \in (\mathbb{F}_q)^{l\times 1}$ is a vector whose $i(j)$-entry is 1 and all the others are zero. We multiply by $\psi(\alpha_j)$ and we get $\psi(\alpha_j)\boldsymbol{f}(\alpha_j) - g(\alpha_j)\psi(\alpha_j)\boldsymbol{y}_j = \psi(\alpha_j)\boldsymbol{\nu}_{i(j)}$. By key Equation (6) we can replace $\psi(\alpha_j)\boldsymbol{y}_j$ by $\boldsymbol{\varphi}(\alpha_j)$. Fix i, then $\forall j \notin I_i$, $\psi(\alpha_j)f_i(\alpha_j) - g(\alpha_j)\varphi_i(\alpha_j) = 0$. The number of roots of the polynomial $\psi(x)f_i(x) - g(x)\varphi_i(x)$ is then $n - |I_i| \geq n - \lceil |E|/l \rceil \geq \max(\delta_g + \deg(\boldsymbol{f}), \delta_f + \deg(g)) + \xi + 1$. Hence, since this polynomial has more roots than its degree it is the zero polynomial.

Second, if $min(N_1, N_2) = N_2$, then for all $j \in E$ we choose $\boldsymbol{y}_j$ such that $\boldsymbol{f}(\alpha_j) - g(\alpha_j)\boldsymbol{y}_j = -A(\alpha_j)^{-1}g(\alpha_j)\boldsymbol{\nu}_{i(j)}$ or equivalently $A(\alpha_j)\boldsymbol{y}_j - A(\alpha_j)\boldsymbol{f}(\alpha_j)/g(\alpha_j) = \boldsymbol{\nu}_{i(j)}$. Since

$A(\alpha_j)\frac{\boldsymbol{f}(\alpha_j)}{g(\alpha_j)} = b(\alpha_j)$, after multiplying by $\psi(\alpha_j)$ and using the key Equation (6) we get $A(\alpha_j)\boldsymbol{\varphi}(\alpha_j) - \psi(\alpha_j)b(\alpha_j) = \psi(\alpha_j)\boldsymbol{\nu}_{i(j)}$. Fix i, then $\forall j \notin I_i$, $(A(\alpha_j)\boldsymbol{\varphi}(\alpha_j) - \psi(\alpha_j)\boldsymbol{b}(\alpha_j))_i = 0$, *i.e.* the i-th component of the polynomial vector $A(x)\boldsymbol{\varphi}(x) - \psi(x)\boldsymbol{b}(x)$ vanishes on those α_j. As before the number $n - |I_i| \geq n - \lceil |E|/l \rceil \geq \max(\delta_f + \deg(A), \delta_g + \deg(A)) + \xi + 1$ roots of the polynomial $(A(x)\boldsymbol{\varphi}(x) - \psi(x)\boldsymbol{b}(x))_i$, is greater than its degree and so it is the zero polynomial. We have that $A(x)\boldsymbol{f}(x) - g(x)\boldsymbol{b}(x) = 0$ and $A(x)\boldsymbol{\varphi}(x) - \psi(x)\boldsymbol{b}(x) = 0$. So if we multiply the first equation by $\psi(x)$, the second by $g(x)$ and we subtract we get $A(x)[\boldsymbol{\varphi}(x)g(x) - \boldsymbol{f}(x)\psi(x)] = 0$. Now, $A(x)$ is full rank and so $\boldsymbol{\varphi}(x)g(x) - \boldsymbol{f}(x)\psi(x) = 0$.

Hence in both cases, since $\boldsymbol{f}/g$ is a reduced fraction, there exists $R \in \mathbb{F}_q[x]$ s.t. $\boldsymbol{\varphi} = R\boldsymbol{f}$ and $\psi = Rg$. Going back to Eq. (6), for all $j \in E$ and $i = i(j)$, we get $0 = \varphi_i(\alpha_j) - \psi(\alpha_j)y_{ij} = R(\alpha_j)\left(f_i(\alpha_j) - g(\alpha_j)y_{ij}\right) = R(\alpha_j)$. Therefore $\Lambda(x)$ divides $R(x)$ and $(\boldsymbol{\varphi}, \psi) \in \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle$. The power i must verify $i + |E| + \deg(\boldsymbol{f}) = \deg(x^i\Lambda\boldsymbol{f}) \leq \delta_f + \xi$ and the same for g which implies exactly that $i \leq \delta_{fgE}$.

Let's now prove that Eq. (10) holds with high probability. We always have $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle \subseteq \ker(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}) = S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ and Eq. (10) is the equality case. By the rank–nullity theorem, we always have $\text{rank}(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}) \leq \rho$ where $\rho := n(\delta_f + \xi + 1) + \delta_g + \xi - \delta_{fgE}$ and Eq. (10) is equivalent to $\text{rank}(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}) = \rho$. In the first part of the proof, we have proved that there exists an instance $(\boldsymbol{y}_j)_{1\leq j\leq n}$ such that $\text{rank}(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}) = \rho$, which means that there exists a nonzero ρ-minor. If we consider this ρ-minor as a polynomial in the variables (y_{ij}), we have shown that it is non zero. Note that it has total degree at most $\delta_g + \xi$ because only the last $\delta_g + \xi$ columns of $M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ contain variables (y_{ij}) (see Eq. (7)). Therefore the Schwartz-Zippel lemma implies that it cannot be zero in more than $\frac{\delta_g+\xi}{q}$ fraction of its domain. For those instances $(\boldsymbol{y}_j)_{1\leq j\leq n}$ that don't cancel this ρ-minor, we get that $\text{rank}(M_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi})$ is equal to ρ and Eq. (10) holds. □

Remark 14. *Let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of the PLSwE with parameters $n, d_f, d_g, \varepsilon, d_A, d_b$. If we consider $\delta_f = d_f$, $\delta_g = d_g$ and $\xi = \varepsilon$, then $N_1 = d_f + d_g + \lceil \frac{(l+1)}{l}\varepsilon \rceil + 1$ and $N_2 = \max(d_A + d_f, d_b + d_g) + \lceil \frac{(l+1)}{l}\varepsilon \rceil + 1$. Hence, if $n \geq \min(N_1, N_2)$, by Theorem 13, the solution space $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle$ for $0 \leq i \leq \delta_{fgE}$ with probability at least $1 - \frac{d_g+\varepsilon}{q}$.*

Equivalently, we can fix the number of evaluation points and let the error correction capability vary. Thus, let $(\boldsymbol{y}_j)_{1\leq j\leq n}$ be an instance of a PLSwE with parameters $n, d_f, d_g, d_A, d_b, \varepsilon \leq \max(\varepsilon_{GLZ}, \varepsilon_{GLZ2})$ where

- $\varepsilon_{GLZ} = \frac{l(n-d_f-d_g-1)}{l+1}$,
- $\varepsilon_{GLZ2} = \frac{l(n-\max(d_A+d_f, d_b+d_g)-1)}{l+1}$.

Then, by Theorem 13, the solution space $S_{\boldsymbol{y},d_f+\varepsilon,d_g+\varepsilon} = \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle$ for $0 \leq i \leq \delta_{fgE}$ with probability at least $1 - \frac{d_g+\varepsilon}{q}$. Hence we have proved the Theorem 8 and Theorem 10.

Proof of Theorem 11. First we prove that $|E| \leq \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$ iff there exists a choice of parameters in lines 1 and 4 such that $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}} \neq \{(\boldsymbol{0}, 0)\}$. We observe that $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}} \neq \{(\boldsymbol{0}, 0)\}$ is equivalent to $\delta_{fgE} \geq 0$. We suppose that $\varepsilon \leq \varepsilon'_{GLZ}$ (we can do the same in the other case) and consider the first choice of $\delta_f + \xi$ and $\delta_g + \xi$ as in line 1. Hence, $\varepsilon \leq \varepsilon'_{GLZ}$ iff $\max(\deg(\boldsymbol{f}) + d_g, \deg(g) + d_f) \leq n - |E| - \lceil \frac{\varepsilon}{l} \rceil - 1$. So, $\varepsilon \leq \varepsilon'_{GLZ}$

$$\Leftrightarrow \begin{cases} \deg(\Lambda\boldsymbol{f}) = \deg(\boldsymbol{f}) + |E| \leq n - d_g - \lceil \frac{\varepsilon}{l} \rceil - 1 = \delta_f + \xi \\ \deg(\Lambda g) = \deg(g) + |E| \leq n - d_f - \lceil \frac{\varepsilon}{l} \rceil - 1 = \delta_g + \xi \end{cases}$$

Hence, this is equivalent to $\delta_{fgE} \geq 0$.

Now if $|E| \leq \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$, the latter claim implies $\{(\boldsymbol{0}, 0)\} \neq \langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}} \subseteq S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ and Algorithm **1** always outputs $(\boldsymbol{\varphi}, \psi)$.

Second, we claim that for both choices of parameters $\delta_f + \xi, \delta_g + \xi$ (lines 1 and 4) we have $n \geq \min(N_1, N_2)$. In fact, if $\delta_f + \xi = n - d_g - \lceil \frac{\varepsilon}{l} \rceil - 1, \delta_g + \xi = n - d_f - \lceil \frac{\varepsilon}{l} \rceil - 1$ then $n \geq N_1 \geq min(N_1, N_2)$. The same holds for the other affectation. The probability that both solution spaces $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ of lines 3, 6 are equal to $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}}$ is at least $1 - \frac{2(d_g+\varepsilon)}{q}$ by applying Theorem 13 on two different affectations.

Therefore, we can conclude that if $|E| \leq \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$, then with probability at least $1 - \frac{2(\delta_g+\xi)}{q}$, $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ is equal to $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}}$ and since $\delta_{fgE} \geq 0$, the minimal non zero element is $(\varphi, \psi) = (\Lambda\boldsymbol{f}, \Lambda g)$.

On the other hand, if $|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$, then $\delta_{fgE} < 0$ for both affectations, and so $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}} = \{(\boldsymbol{0}, 0)\}$. But with probability at least $1 - \frac{2(\delta_g+\xi)}{q}$, both solution spaces $S_{\boldsymbol{y},\delta_f+\xi,\delta_g+\xi}$ are equal to $\langle x^i\Lambda\boldsymbol{f}, x^i\Lambda g\rangle_{0\leq i\leq\delta_{fgE}} = \{(\boldsymbol{0}, 0)\}$ so the algorithm will output "$|E| > \max(\varepsilon'_{GLZ}, \varepsilon'_{GLZ2})$" □

VII. Conclusion and Future Work

In this work, we improve the result of [6] considering new bounds on the parameters and taking into account the degrees of A and $\boldsymbol{b}$ (as in (3)). We also present a parameter oblivious algorithm that allows us to correct more errors. Our algorithm is probabilistic and the failure probability depends on the parameters δ_g and ξ. Remark that our bound on the failure probability is similar to the original result of [1] for IRS codes. Actually, this bound on the decoding failure of IRS codes was strongly improved in [2]. Since the SRFR coincides with the reconstruction of a vector of rational functions by its evaluations, some of which erroneous, we can see the SRFR as the decoding of an *interleaved rational code* [9]. Despite the similarity of this problem with the decoding of IRS codes, here we deal with a code which is not linear. This prevent the adaptation of most recent techniques for bounding the probability failure of IRS decoding algorithms. A future work is to provide a better comprehension of the interleaved rational code in order to better bound the failure probability.

REFERENCES

[1] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding of interleaved reed solomon codes over noisy data," in *In Proceedings of the 30th International Colloquium on Automata, Languages and Programming (ICALP)*, 2003, pp. 97–108.

[2] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative decoding of interleaved reedsolomon codes and concatenated code designs," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 2991–3012, 2009.

[3] S. Puchinger and J. Rosenkilde ne Nielsen, "Decoding of interleaved reed-solomon codes using improved power decoding," in *Proceedings of 2017 IEEE International Symposium on Information Theory*. IEEE, 2017, pp. 356–60.

[4] B. Boyer and E. L. Kaltofen, "Numerical linear system solving with parametric entries by error correction," in *Proceedings of the 2014 Symposium on Symbolic-Numeric Computation*, ser. SNC '14. New York, NY, USA: ACM, 2014, pp. 33–38. [Online]. Available: http://doi.acm.org/10.1145/2631948.2631956

[5] 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 the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ser. ISSAC '17. New York, NY, USA: ACM, 2017, pp. 237–244. [Online]. Available: http://doi.acm.org/10.1145/3087604.3087645

[6] E. Guerrini, R. Lebreton, and I. Zappatore, "Polynomial linear system solving with errors by simultaneous polynomial reconstruction of interleaved reed-solomon codes," in *2019 IEEE International Symposium on Information Theory (ISIT)*, July 2019, pp. 1542–1546.

[7] S. Gao, "A new algorithm for decoding reed-solomon codes," in *Communications, Information and Network Security*, V. K. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, Eds. Springer US, 2003, pp. 55–68. [Online]. Available: https://doi.org/10.1007/978-1-4757-3789-9_5

[8] Elwyn R. Berlekamp and Lloyd R. Welch, "Error correction of algebraic block codes." U.S. patent 633 470, 1986.

[9] C. Pernet, "High Performance and Reliable Algebraic Computing," Habilitation à diriger des recherches, Université Joseph Fourier, Grenoble 1, Nov. 2014. [Online]. Available: https://tel.archives-ouvertes.fr/tel-01094212

[10] A. Brown, L. Minder, and A. Shokrollahi, "Probabilistic decoding of interleaved RS-codes on the q-ary symmetric channel," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, 2004, pp. 326–326.

[11] M. Khonji, C. Pernet, J.-L. Roch, T. Roche, and T. Stalinski, "Output-sensitive decoding for redundant residue systems," in *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, ser. ISSAC '10. ACM, 2010, pp. 265–272, event-place: Munich, Germany. [Online]. Available: http://doi.acm.org/10.1145/1837934.1837985

[12] J. S. Rosenkilde and A. Storjohann, "Algorithms for simultaneous padé approximations," in *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19-22, 2016*, 2016, pp. 405–412. [Online]. Available: https://doi.org/10.1145/2930889.2930933