Polynomial Linear System Solving with Random Errors: New Bounds and Early Termination Technique

Eleonora Guerrini
guerrini@lirmm.fr
LIRMM, U. Montpellier, CNRS
Montpellier, France, FR

Romain Lebreton
lebreton@lirmm.fr
LIRMM, U. Montpellier, CNRS
Montpellier, France, FR

Ilaria Zappatore
ilaria.zappatore@inria.fr
LIX, Inria
Palaiseau, France, FR

ABSTRACT

This paper deals with the polynomial linear system solving with errors (PLSwE) problem. More specifically, we solve linear systems with univariate polynomial coefficients via an evaluation-interpolation technique assuming that errors can occur before the interpolation step. In this framework, the number of evaluations needed to recover the solution depends on the parameters of the linear system (degrees, size) and on the number of errors.

Our work is part of a series of papers about PLSwE aiming to reduce this number of evaluations, which is crucial since it affects the complexity. We proved in [7] that if errors are randomly distributed, the bound on the number of evaluations can be lowered with respect to the error rate.

In this paper, following the approach of [9], we improve the results of [7] in two directions. First, we propose a new bound on the number of evaluations, lowering the dependency on the parameters of the linear system, based on the work of [5]. Second, we introduce an early termination strategy in order to handle the unnecessary increase of the number of evaluations due to the overestimation of the output degrees and of the number of errors.

CCS CONCEPTS

• **Mathematics of computing → Coding theory**; • **Computing methodologies → Algebraic algorithms**; *Linear algebra algorithms.*

KEYWORDS

Polynomial linear system solving; interleaved Reed Solomon codes; simultaneous rational function reconstruction

ACM Reference Format:
Eleonora Guerrini, Romain Lebreton, and Ilaria Zappatore. 2021. Polynomial Linear System Solving with Random Errors: New Bounds and Early Termination Technique. In *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation (ISSAC '21), July 18–23, 2021, Virtual Event, Russian Federation.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3452143.3465548

1 INTRODUCTION

Solving polynomial linear systems (PLS) $A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x)$ with univariate polynomial coefficients over a finite field $\mathbb{F}_q$ is a classical computer algebra problem. When A is a nonsingular square matrix and $\boldsymbol{b}$ is a vector, the solution $\boldsymbol{y}(x)$ is a unique vector of rational functions. In order to reconstruct this solution, we use the evaluation-interpolation technique. This technique can be parallelized considering a network of L computing nodes and assuming that each jth node evaluates $A(\alpha_j)$ and $\boldsymbol{b}(\alpha_j)$ and solves the evaluated system $\boldsymbol{y}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$, given some distinct evaluation points α_j. The nodes then send $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$ to a master node which finally performs a vector rational function reconstruction (*a.k.a.* vector Cauchy interpolation) to recover the solution $\boldsymbol{y}(x)$. Note that if one wants to take advantage of the common denominator of $\boldsymbol{y}(x)$, then vector Cauchy interpolation should be replaced by simultaneous rational function reconstruction [8, 15, 16]; in this paper we do not consider this case.

As in [3, 9], this paper focuses on a scenario in which the nodes could make errors, possibly computing $\boldsymbol{y}_j \neq \boldsymbol{y}(\alpha_j)$. In this case, the master node performs a *vector Cauchy interpolation with errors* in order to recover the solution $\boldsymbol{y}(x)$. The problem that the master node has to face, *i.e.* recovering the solution $\boldsymbol{y}(x)$ of the PLS given its evaluations, some of which are erroneous, is what we call Polynomial Linear System Solving with Errors (PLSwE). In order to solve PLSwE, in [3, 9] the authors generalize the polynomial interpolation with errors (*i.e.* decoding Reed-Solomon (RS) codes) to rational functions interpolation with errors. The goal is to minimize the number L of evaluation points needed to recover the solution or equivalently to maximize the bound on the number of errors (*decoding radius*) that we could correct. In [3, 9] they can correct up to the *unique decoding radius*, similarly to classical RS codes. Moreover, in [9] they show a second way to bound L by exploiting the linear algebra setting as in [5].

More recently, in [7] we present an algorithm that corrects errors beyond the unique decoding radius (equivalently with fewer evaluation points than [3, 9]). The idea is that the PLSwE problem is a generalization of the decoding of the Interleaved Reed Solomon codes (IRS). IRS codes can be seen as the simultaneous evaluation of a vector of polynomials. The interleaved structure allows one to construct decoders able to correct beyond the unique decoding radius [2, 4, 17–19], asymptotically reaching the optimal error correction capability of the Shannon bound [20] when the vector dimension grows. In return, IRS decoders may fail to correct a small fraction of errors, provided that errors are uniformly distributed. The same goes for our generalization [7] and for the present work.

ISSAC '21, July 18–23, 2021, Virtual Event, Russian Federation

ACM ISBN 978-1-4503-8382-0/21/07…$15.00
https://doi.org/10.1145/3452143.3465548

Our first contribution consists in the combination of the advantages of IRS decoding techniques from [7] with the evaluation count of [9] which exploits the linear algebra setting (see Section 3).

Recall that our goal is to lower the number of evaluations in order to reduce the number of computing nodes, at the expense of potentially increasing the complexity of interpolation by the master node. All the bounds on the number of evaluations introduced for PLSwE solving depend on some upper bounds on the degrees of the solution $\boldsymbol{y}(x)$ and on the number of errors. These upper bounds could overestimate the actual degrees and number of errors, leading to a significant overestimation of the number of evaluations needed. In this paper, we propose an *early termination technique* (as in [9]), an adaptive strategy which iteratively increments the number of evaluations until the actual parameters are reached. Compared to the similar strategy proposed by [12, 14] in a no-errors context, our approach differs in two ways: they propose output sensitive algorithms, *i.e.* they stop at a number of evaluations that depends only on the degrees of the output. In our case, we stop at a number of evaluations which depends on both the values of the output parameters and their corresponding bounds (we could say that we are semi-output sensitive). In return, their approach is only heuristic whereas our stop criterion is proven (with high probability *w.r.t.* the error distribution only in the case of IRS codes generalization).

Early termination strategies consider a number of evaluations which is iteratively incremented. Furthermore, our techniques require an error upper bound τ to work. Thus, how can we determine an upper bound τ on the number of errors when this number increases along with the number of evaluations? Our first approach (Section 4.2) to solve this problem consists to fix an error bound τ which is related to the largest possible number of evaluations. In Section 4.3 we present a second approach, coming from [9–11], that considers an error bound τ which (linearly) depends on the number of evaluations L. In this second setup, we are able to save some more evaluations *w.r.t.* to the number we get using a fixed error bound.

Compared to the early termination techniques of [9], we decrease the number of evaluation points. In return, our algorithm may fail for a small fraction of errors; we give an estimation of the success probability of our algorithm in presence of random errors.

To sum up, our contribution consists in proposing an early termination strategy which, benefits from the IRS decoding approach, is sensitive to the real number of errors, and also considers an error bound which is linearly dependent on the number of evaluations. To the best of our knowledge, the dependency on the real number of errors is original in the literature.

The paper is organized as follows: in Section 2 we recall the scenario of PLSwE with results revisited from literature, in Section 3 we present a new bound on the number of evaluation points needed for PLSwE solving in presence of random errors and finally in Section 4 we introduce an early termination algorithm that succeeds for almost all errors.

2 POLYNOMIAL LINEAR SYSTEM SOLVING WITH ERRORS

Let $\mathbb{F}_q$ be a finite field of order q. Consider a polynomial linear system (PLS),

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

where $A \in \mathbb{F}_q[x]^{n\times n}$ is nonsingular and $\boldsymbol{b} \in \mathbb{F}_q[x]^n$. This system admits only one solution $\boldsymbol{y} = \frac{\boldsymbol{v}}{d} \in \mathbb{F}_q(x)^n$, *i.e.* a vector of rational functions with the same denominator. We assume that $\gcd(\gcd_i(v_i), d) = 1$ and that d is monic.

Evaluation-interpolation [13] is a classic technique for solving PLS. It consists in: evaluating A and $\boldsymbol{b}$ at L distinct evaluation points α_j; pointwise solving $\boldsymbol{y}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$; and interpolating $\boldsymbol{y} \in \mathbb{F}_q(x)^n$ given the evaluated solutions $\boldsymbol{y}_j = \boldsymbol{y}(\alpha_j)$ and the degree bounds N, D such that $N > \deg(\boldsymbol{v}) := \max_{1\le i\le n}(\deg(v_i))$ and $D > \deg(d)$. In this work, we suppose that the evaluated matrices $A(\alpha_j)$ are still full rank. Notice that this implies that $d(\alpha_j) \neq 0$. Otherwise by $A(\alpha_j)\boldsymbol{v}(\alpha_j) = d(\alpha_j)\boldsymbol{b}(\alpha_j)$ then $\boldsymbol{v}(\alpha_j) = 0$, contradicting $\gcd(\boldsymbol{v}(x), d(x)) = 1$. In [9], the authors also handle the rank drops of the evaluated matrices $A(\alpha_j)$ in their scenario. We are confident that with our techniques we could also handle this case, and we leave it to future work.

We now introduce the number of evaluation points

$$\mathcal{L} := \min(\underbrace{N + D - 1}_{\mathcal{L}_{RFR}}, \underbrace{\max(\deg(A) + N, \deg(\boldsymbol{b}) + D)}_{\mathcal{L}_{PLS}}), \tag{2}$$

where $\deg(A) := \max_{1\le i,j\le n}(\deg(a_{i,j}(x)))$. Recall that $\mathcal{L}_{RFR}$ is the minimum number of evaluation points needed to uniquely interpolate a vector of rational functions (*i.e. vector Cauchy interpolation*) [6, Section 5.7]. On the other hand, $\mathcal{L}_{PLS}$ is the minimum number of evaluation points needed to uniquely recover a rational function which is a solution of a PLS [5]. Note that $\mathcal{L}_{PLS}$ and $\mathcal{L}_{RFR}$ can be compared when the bounds N, D are tight: if $N = \deg(\boldsymbol{v}) + 1$ and $D = \deg(d) + 1$, then $(\mathcal{L}_{PLS} < \mathcal{L}_{RFR}) \Leftrightarrow (\deg(d) > \deg(A))$ [9, Theorem 3.1].

Error model. In this work, as in [3, 9], we adapt the evaluation-interpolation technique in order to handle a scenario where errors occur. More specifically, we assume that some errors could be introduced before the interpolation step, *i.e.* $\boldsymbol{y}_j \neq \boldsymbol{y}(\alpha_j)$ for some j. We can then write $\boldsymbol{y}_j = (\boldsymbol{v}/d)(\alpha_j) + \boldsymbol{e}_j$ for some $\boldsymbol{e}_j \in \mathbb{F}_q^n$. Denoting $E := \{j \mid \boldsymbol{y}_j \neq \boldsymbol{y}(\alpha_j)\}$ the *error support*, we get that $\boldsymbol{e}_j \neq \boldsymbol{0}$ for any $j \in E$.

In this work, we focus on the following problem,

Definition 2.1 (Polynomial linear system solving with errors (PLSwE)). Under the framework of this section, the PLSwE problem consists in recovering the solution $\boldsymbol{y}(x) = \frac{\boldsymbol{v}(x)}{d(x)}$ of a PLS (1), given

- L distinct evaluation points α_j in $\mathbb{F}_q$,
- the matrix $Y \in \mathbb{F}_q^{n\times L}$ whose columns are the vectors $\boldsymbol{y}_j$,
- the degrees $\deg(A)$, $\deg(\boldsymbol{b})$ and the degree bounds N, D such that $N > \deg(\boldsymbol{v})$, $D > \deg(d)$ and $1 \le N, D \le L$,
- an error bound $\tau \ge |E| = |\{j \mid \boldsymbol{y}_j \neq \boldsymbol{y}(\alpha_j)\}|$.

Application to distributed computations. The evaluation interpolation technique can be easily parallelized by considering a set of L computing nodes and a master node. In this model, the master node sends $\alpha_j, A(x), \boldsymbol{b}(x)$ to each computing node which returns $\boldsymbol{y}_j$. We consider the computing nodes as black boxes as in [3], meaning that we are not supposed to know how they compute the $\boldsymbol{y}_j$'s. The master node must then solve a PLSwE to output the solution $\boldsymbol{y}(x)$ of the PLS.

Resolution method for PLSwE and previous results. In order to solve PLSwE, we study the set $\mathcal{S}_{Y,N+\tau,D+\tau}$ of solutions $(\boldsymbol{\varphi}, \psi) = (\varphi_1, \dots, \varphi_n, \psi) \in \mathbb{F}_q[x]^{n+1}$ of the *key equations*

$$\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j),\ \deg(\varphi_i) < N + \tau,\ \deg(\psi) < D + \tau \qquad (3)$$

for any $1 \le i \le n$ and $1 \le j \le L$. This approach comes from [3, 7, 9] and it is the generalization of the Welch-Berlekamp method [1] for decoding Reed-Solomon codes. Note that the key equations (3) are the vector generalization of the classic computer algebra problem of the *Cauchy interpolation* [6, Section 5.7]. In this framework, it is crucial to determine the smallest number of evaluation points L needed to guarantee the *uniqueness* of a solution of these key equations, where uniqueness is defined as follows. We say that $\mathcal{S}_{Y,N+\tau,D+\tau}$ has a *unique solution* if $\mathcal{S}_{Y,N+\tau,D+\tau} \neq \{(\boldsymbol{0}, 0)\}$ and for all $(\boldsymbol{\varphi}, \psi), (\boldsymbol{\varphi}', \psi') \in \mathcal{S}_{Y,N+\tau,D+\tau} \setminus \{(\boldsymbol{0}, 0)\}$, we have equality $\boldsymbol{\varphi}/\psi = \boldsymbol{\varphi}'/\psi'$ of the corresponding rational functions.

Let $\Lambda := \prod_{j \in E}(x - \alpha_j)$ be the *error locator polynomial*, *i.e.* the monic polynomial whose roots are the erroneous evaluation points. If $\boldsymbol{y}(x) = \boldsymbol{v}(x)/d(x)$ is the solution of (1) then $(\Lambda\boldsymbol{v}, \Lambda d) \in \mathcal{S}_{Y,N+\tau,D+\tau}$. Indeed, $\Lambda(\alpha_j)(v_i(\alpha_j) - y_{i,j}d(\alpha_j)) = 0$ for any $1 \le i \le n$ and $1 \le j \le L$. Moreover, $\deg(\Lambda\boldsymbol{v}) < N + \tau, \deg(\Lambda d) < D + \tau$.

If the degree bounds and the error bound are not tight, we get also other solutions, *i.e.* $\mathcal{S}_{Y,N+\tau,D+\tau} \supseteq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$, where

$$\delta_{N+\tau,D+\tau} := \min(N+\tau-(\deg(\boldsymbol{v})+|E|), D+\tau-(\deg(d)+|E|)). \quad (4)$$

Note that $\delta_{N+\tau,D+\tau}$ is defined so that $\deg(x^i\Lambda\boldsymbol{v}) < N + \tau$ and $\deg(x^i\Lambda d) < D + \tau$ for $i < \delta_{N+\tau,D+\tau}$. Finally, note that $\mathcal{S}_{Y,N+\tau,D+\tau}$ has unique solution when $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$.

In [3, 9] is provided the minimum number of points which guarantees the uniqueness of the solution. The following proposition is a restatement of this result using definitions and notations of this paper. We later prove this result in a more general context (see Proposition 4.1).

Proposition 2.2. *Under the setting of Definition 2.1, if $L \ge L_{KPSW} := \mathcal{L}+2\tau$, then $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$.*

We now recall how the solution set can be computed.

Remark 2.3. Let $\mathcal{V}_{m,p} = (\alpha_i^{j-1})_{\substack{1 \le i \le m \\ 1 \le j \le p}}$ and let D_i be the diagonal matrix whose diagonal elements are $\boldsymbol{y}_i$. The coefficient matrix of the homogeneous linear system related to (3) is

$$M_{Y,N+\tau,D+\tau} = \left(\begin{array}{ccc|c} \mathcal{V}_{L,N+\tau} & & & -D_1\mathcal{V}_{L,D+\tau} \\ & \ddots & & \vdots \\ & & \mathcal{V}_{L,N+\tau} & -D_n\mathcal{V}_{L,D+\tau} \end{array}\right)$$

and $\mathcal{S}_{Y,N+\tau,D+\tau} = \ker(M_{Y,N+\tau,D+\tau})$.

If $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle$, remark that the minimal degree solution $(\boldsymbol{\varphi}_{min}, \psi_{min})$ of $\mathcal{S}_{Y,N+\tau,D+\tau}$ with ψ_{min} monic is $(\Lambda\boldsymbol{v}, \Lambda d)$. This minimal monic solution can be obtained by computing a column echelon form of $M_{Y,N+\tau,D+\tau}$ [3, 9] or a basis of the $\mathbb{F}_q[x]$-module generated by $\mathcal{S}_{Y,N+\tau,D+\tau}$ using *e.g.* [15, 16].

We denote by $\texttt{FindSolution}(Y, N + \tau, D + \tau)$ the algorithm that computes $(\boldsymbol{v}, d)$ from $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle$ using one of the above methods. Note that we can recover $(\boldsymbol{v}, d)$ from $(\Lambda\boldsymbol{v}, \Lambda d)$ by dividing by $\Lambda = \gcd(\Lambda\boldsymbol{v}, \Lambda d)$.

3 NEW BOUND FOR PLSWE

In this section, we combine the advantages of IRS decoding techniques from [7] with the number of evaluations of [9] which exploits the linear algebra setting.

We briefly recall that an IRS codeword is the multipoint evaluation of a vector of polynomials of bounded degrees. In [7] we have remarked that if $\boldsymbol{y}(x) \in \mathbb{F}_q[x]^n$ (*i.e.* $D = 1$), PLSwE reduces to the interpolation of a vector of polynomials with errors, *i.e.* exactly the problem of decoding IRS codewords. A naive method to decode IRS codes would be to apply componentwise the decoding techniques of classic Reed-Solomon codes. In this way we can correct up to the *unique decoding radius* $\tau_0 := \lfloor \frac{L-N}{2} \rfloor$. Indeed, from a coding theory point of view, Proposition 2.2 tells us that we can uniquely decode IRS codewords when $L \ge N + 2\tau$, *i.e.* up to $\tau_0 \ge |E|$. But, the interleaved structure of IRS codes allows to correct beyond the unique decoding radius, or equivalently with fewer evaluations [2, 4, 17–19]. In return, IRS decoding may fail to correct a small fraction of errors, provided that errors are uniformly distributed.

In [7] we have generalized IRS decoding to the rational function case of PLSwE, and we have shown that we can reconstruct the solution with $L_{GLZ19} := N + \deg(d) - 1 + |E| + \left\lceil \frac{|E|}{n} \right\rceil$ evaluation points for almost all errors. However, we have assumed to know exactly the actual degree of the denominator d and the actual number of errors $|E|$.

In this section we present two main contributions. Our first contribution (see Theorem 3.1) consists in relaxing these constraints, only requiring upper bounds on these parameters. Our second contribution is the introduction of another number of evaluations which takes into account $\deg(A), \deg(\boldsymbol{b})$ of the PLS (1) as in [5, 9].

Theorem 3.1. *Under the setting of Definition 2.1, let $L \ge L_{GLZ} := \mathcal{L}+\tau+\lceil\tau/n\rceil$ and fix an error support $E \subseteq \{1, \dots, L\}$ such that $|E| \le \tau$. Consider the random matrix $Y \in \mathbb{F}_q^{n \times L}$ whose columns $\boldsymbol{y}_j \in \mathbb{F}_q^n$ are such that $\boldsymbol{y}_j = \boldsymbol{y}(\alpha_j) = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ if $j \notin E$, and $\boldsymbol{y}_j$ is uniformly distributed if $j \in E$. Then $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$ with probability at least $1 - \frac{D+\tau}{q}$ (for $\delta_{N+\tau,D+\tau}$ defined as in (4)).*

Proof. The proof is based on the following two steps:

(1) show that there exists a draw W of Y for which the corresponding solution space $\mathcal{S}_{W,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle$. We only need to prove the inclusion $\subseteq$ since the other one is always true;

(2) derive a bound on the probability of the event $\mathcal{S}_{Y,N+\tau,D+\tau} \neq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle$.

(1) Consider a partition of the error support E, *i.e.* $E = \cup_{i=1}^n I_i$, such that for any $1 \le i \le n$, $|I_i| \le \lceil |E|/n \rceil$. Such a partition exists since $n\lceil |E|/n \rceil \ge |E|$. For any $j \in E$, we denote by i_j the unique index such that $j \in I_{i_j}$.

First assume that $L_{GLZ} = N + D - 1 + \tau + \left\lceil \frac{\tau}{n} \right\rceil$. Construct a matrix W whose columns $\boldsymbol{w}_j$ satisfy $\boldsymbol{w}_j = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ if $j \notin E$, or $\boldsymbol{v}(\alpha_j) -$

$d(\alpha_j)\boldsymbol{w}_j = \boldsymbol{\varepsilon}_{i_j}$ when $j \in E$ (where $\boldsymbol{\varepsilon}_i$ is the ith element of the canonical basis of $\mathbb{F}_q^n$). Consider $(\boldsymbol{\varphi}, \psi) \in \mathcal{S}_{W,N+\tau,D+\tau}$. Our goal is to prove that $\psi(x)\boldsymbol{v}(x) - d(x)\boldsymbol{\varphi}(x) = \boldsymbol{0}$. Combining $\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{w}_j\psi(\alpha_j)$ and the equations defining $\boldsymbol{w}_j$, we get $(\psi\boldsymbol{v} - d\boldsymbol{\varphi})(\alpha_j) = \boldsymbol{0}$ if $j \notin E$, or $(\psi\boldsymbol{v} - d\boldsymbol{\varphi})(\alpha_j) = \psi(\alpha_j)\boldsymbol{\varepsilon}_{i_j}$ if $j \in E$. Fix $1 \le i \le n$ and consider the ith vector component $(\psi v_i - d\varphi_i)$ of $(\psi\boldsymbol{v} - d\boldsymbol{\varphi})$. Note that $\deg(\psi v_i - d\varphi_i) < N + D + \tau - 1$. We also have $(\psi v_i - d\varphi_i)(\alpha_j) = 0$ for $j \notin I_i$. So this polynomial has at least $L - |I_i|$ roots. Since $L - |I_i| \ge L - \lceil |E|/n \rceil \ge L_{GLZ} - \lceil \tau/n \rceil$ and $L_{GLZ} \ge N + D - 1 + \tau + \lceil \tau/n \rceil$, we get at least $L - |I_i| \ge N + D + \tau - 1$ roots. Therefore, $(\psi v_i - d\varphi_i)$ has more roots than its degree, so that $(\psi v_i - d\varphi_i) = 0$ and $\psi(x)\boldsymbol{v}(x) - d(x)\boldsymbol{\varphi}(x) = \boldsymbol{0}$.

Now assume that $L_{GLZ} = \max(\deg(A) + N, \deg(\boldsymbol{b}) + D) + \left\lceil \frac{\tau}{n} \right\rceil + \tau$. Construct a matrix W so that $\boldsymbol{w}_j = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)} = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$ if $j \notin E$, or $A(\alpha_j)\boldsymbol{w}_j - \boldsymbol{b}(\alpha_j) = \boldsymbol{\varepsilon}_{i_j}$ when $j \in E$ (recall $A(\alpha_j)$ is invertible by assumption). Consider $(\boldsymbol{\varphi}, \psi) \in \mathcal{S}_{W,N+\tau,D+\tau}$. Our goal is to prove that $\boldsymbol{p}(x) = \boldsymbol{0}$ where $\boldsymbol{p}(x) := A(x)\boldsymbol{\varphi}(x) - \psi(x)\boldsymbol{b}(x) = \boldsymbol{0}$. Combining $\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{w}_j\psi(\alpha_j)$ and the equations defining $\boldsymbol{w}_j$, we get $(A\boldsymbol{\varphi} - \boldsymbol{b}\psi)(\alpha_j) = \boldsymbol{0}$ if $j \notin E$, or $(A\boldsymbol{\varphi} - \boldsymbol{b}\psi)(\alpha_j) = \psi(\alpha_j)\boldsymbol{\varepsilon}_{i_j}$ if $j \in E$.

Fix $1 \le i \le n$, then $p_i(\alpha_j) = 0$ for $j \notin I_i$, where p_i is the ith vector component of $\boldsymbol{p}$. Note that $\deg(p_i(x)) < \max(\deg(A) + N, \deg(\boldsymbol{b}) + D) + \tau$. On the other hand p_i has at least $L - |I_i| \ge L_{GLZ} - \lceil \tau/n \rceil = \max(\deg(A) + N, \deg(\boldsymbol{b}) + D) + \tau$ roots. So we can conclude that $\boldsymbol{p}(x) = A(x)\boldsymbol{\varphi}(x) - \psi(x)\boldsymbol{b}(x) = \boldsymbol{0}$. Since $A(x)\boldsymbol{v}(x) = d(x)\boldsymbol{b}(x)$, we get $A(x)(\boldsymbol{\varphi}(x)d(x) - \psi(x)\boldsymbol{v}(x)) = \boldsymbol{0}$ and finally $\boldsymbol{\varphi}(x)d(x) - \psi(x)\boldsymbol{v}(x) = \boldsymbol{0}$.

Therefore, in both cases we have $\boldsymbol{\varphi}(x)d(x) - \psi(x)\boldsymbol{v}(x) = \boldsymbol{0}$. Now, $\gcd(\gcd_i(v_i), d) = 1$ by assumption, so there exists $R \in \mathbb{F}_q[x]$ such that $(\boldsymbol{\varphi}, \psi) = (R\boldsymbol{v}, Rd)$. By the key equations (3) we get $\boldsymbol{0} = \boldsymbol{\varphi}(\alpha_j) - \psi(\alpha_j)\boldsymbol{w}_j = R(\alpha_j)[\boldsymbol{v}(\alpha_j) - \boldsymbol{w}_j d(\alpha_j)]$ for all j. By construction, $\boldsymbol{v}(\alpha_j) - \boldsymbol{w}_j d(\alpha_j) \neq \boldsymbol{0}$ when $j \in E$, so $R(\alpha_j) = 0$. Therefore, there exists $R' \in \mathbb{F}_q[x]$ such that $R = \Lambda R'$, hence $(\boldsymbol{\varphi}, \psi) = (R'\Lambda\boldsymbol{v}, R'\Lambda d)$. The degree constraints on $(\boldsymbol{\varphi}, \psi)$ imply $\deg R' < \delta_{N+\tau,D+\tau}$, *i.e.* $(\boldsymbol{\varphi}, \psi) \in \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$. Finally, we get $\mathcal{S}_{W,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$ for a draw W of the matrix Y.

(2) We now conclude the proof by bounding the probability of the event $\mathcal{S}_{Y,N+\tau,D+\tau} \neq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle$. For a generic instance of Y recall that $\langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}} \subseteq \mathcal{S}_{Y,N+\tau,D+\tau} = \ker(M_{Y,N+\tau,D+\tau})$, so that $\dim(\ker(M_{Y,N+\tau,D+\tau})) \ge \delta_{N+\tau,D+\tau}$ (see Remark 2.3). We have $\operatorname{rank}(M_{Y,N+\tau,D+\tau}) \le n(N+\tau) + D + \tau - \delta_{N+\tau,D+\tau} =: \rho$ by the Rank-Nullity Theorem. On the other hand, as proved above, there exists a draw $\boldsymbol{w}_j$ of $\boldsymbol{y}_j$, for $j \in E$, such that $\operatorname{rank}(M_{W,N+\tau,D+\tau}) = \rho$. This means that there exists a nonzero ρ-minor in $M_{W,N+\tau,D+\tau}$. We consider the same nonzero ρ-minor in $M_{Y,N+\tau,D+\tau}$ as a multivariate polynomial C whose indeterminates are $(y_{i,j})_{1 \le i \le n, j \in E}$. We remark that we show the existence of a draw $\boldsymbol{w}_j$ of $\boldsymbol{y}_j$, for $j \in E$, such that $C(\boldsymbol{w}_j)$ is nonzero. Hence, the polynomial C is nonzero. For any matrix Y such that $(\boldsymbol{y}_j)_{j \in E}$ is not a root of C, then $\mathcal{S}_{Y,N+\tau,D+\tau} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$. Note that the total degree of the polynomial C is at most $D+\tau$, since only the last $D+\tau$ columns of the matrix $M_{Y,N+\tau,D+\tau}$ contain the variables $(y_{i,j})_{1 \le i \le n, j \in E}$ (see Remark 2.3).

Finally, by the Schwartz-Zippel Lemma, the polynomial C cannot vanish in more than a $(D+\tau)/q$-fraction of its domain. Therefore, the probability of $\mathcal{S}_{Y,N+\tau,D+\tau} \neq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{N+\tau,D+\tau}}$ is at most $(D+\tau)/q$. □

4 EARLY TERMINATION STRATEGY

In this section, we present the early termination strategies, review the literature about the subject [9] and contribute by including the advantages of IRS decoding as in [7].

The bounds L_{KPSW} and L_{GLZ} on the number of evaluations L introduced so far (see Proposition 2.2 and Theorem 3.1) depend on the upper bounds N, D and τ. Therefore, if N, D, τ overestimate the degrees $\deg(\boldsymbol{v})$, $\deg(d)$ and the number of errors $|E|$, the evaluation count L_{KPSW} (resp. L_{GLZ}) would be too large compared to the number we really need, *i.e.* replacing $N \longleftarrow \deg(\boldsymbol{v})+1$, $D \longleftarrow \deg(d)+1$, $\tau \longleftarrow |E|$ in L_{KPSW} (resp. L_{GLZ}).

An approach to overcome this problem consists in the introduction of an *early termination* strategy whose goal is to decrease the number of evaluations needed to recover a solution without knowing the actual degrees of the solution and the number of errors. The strategy proposed in [9] consists in incrementing L and introducing a stop criterion that interrupts the computations if L corresponds to the actual degrees and to the actual number of errors. Whereas [9] tried to guess a bound on the degrees of $(\boldsymbol{v}, d)$ but not on the number of errors, we introduce the parameters (ν, ϑ) that represent attempts to bound the degrees $(\deg(\boldsymbol{v}) + |E|, \deg(d) + |E|)$ of the minimal solution $(\Lambda\boldsymbol{v}, \Lambda d)$.

Let $\mathcal{S}_{Y,\nu,\vartheta}$ be the set of solutions $(\boldsymbol{\varphi}, \psi)$ of the key equations

$$\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j),\ \deg(\varphi_i) < \nu,\ \deg(\psi) < \vartheta.$$

Recall that $\mathcal{S}_{Y,\nu,\vartheta} \supseteq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{\nu,\vartheta}}$ where

$$\delta_{\nu,\vartheta} = \min(\nu - (\deg(\boldsymbol{v}) + |E|), \vartheta - (\deg(d) + |E|)).$$

By convention, if $\delta_{\nu,\vartheta} \le 0$ we set $\langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{\nu,\vartheta}} = \{(\boldsymbol{0}, 0)\}$. Notice that $\delta_{\nu,\vartheta} > 0$ *iff* ($\nu > \deg(\Lambda\boldsymbol{v})$ and $\vartheta > \deg(\Lambda d)$). Therefore, if ν, ϑ do not upper bound the degrees of $(\Lambda\boldsymbol{v}, \Lambda d)$ then $\delta_{\nu,\vartheta} \le 0$.

As in Proposition 2.2 and Theorem 3.1, we prove that $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0 \le i < \delta_{\nu,\vartheta}}$ if we have enough evaluations (see Proposition 4.1 and Theorem 4.2). This gives us a criterion `Check` to detect if ν, ϑ are correct upper bounds on the degrees of $(\Lambda\boldsymbol{v}, \Lambda d)$: ($\nu > \deg(\Lambda\boldsymbol{v})$ and $\vartheta > \deg(\Lambda d)$) *iff* $\delta_{\nu,\vartheta} > 0$ *iff* $\mathcal{S}_{Y,\nu,\vartheta} \neq \{(\boldsymbol{0}, 0)\}$. More specifically, let `Check`(Y, ν, ϑ) be the function that returns the Boolean $\mathcal{S}_{Y,\nu,\vartheta}$!= $\{(\boldsymbol{0}, 0)\}$. If `Check` equals `true`, then we can call `FindSolution`(Y, ν, ϑ) to recover $(\boldsymbol{v}, d)$ from $\mathcal{S}_{Y,\nu,\vartheta}$ (see Remark 2.3).

We can now sketch our early termination strategy. For a number of evaluations L that is iteratively incremented, we compute different `Check`(Y, ν, ϑ) to see if there exists ν, ϑ which upper bound $\deg(\Lambda\boldsymbol{v}, \Lambda d)$. As soon as the criterion is satisfied, we can output the solution $(\boldsymbol{v}, d)$ using `FindSolution`(Y, ν, ϑ).

Recall that in the early termination strategy, the number of evaluations L grows, and that our techniques require an error bound τ to work. Thus, a natural question is to understand how we can determine an error bound τ, even though the number of errors increases along with the number of evaluations. A first possible approach is to fix an error bound τ which is related to the largest number of evaluations: our early termination strategy stops when $L = L_{KPSW}$ (resp. L_{GLZ}) in the worst case, and we can set τ *w.r.t.* this number of evaluations (as we would have done in Sections 2, 3). The second approach, coming from [9–11], considers an error bound τ which (linearly) depends on the number of evaluations L. In this second setup, we are able to save some more evaluations compared to the fixed error bound approach.

Another significant difference from [9] consists in the reduction of the number of evaluations which guarantees to uniquely recover the solution in presence of random errors, based on the IRS decoding technique as in [7].

The remainder of the section is organized as follows. In Section 4.1, we first revisit the stop criterion of [9] and we introduce sensitivity on the number of errors. Then we contribute by reducing the number of evaluations in presence of random errors. In Section 4.2 we introduce early termination strategies for fixed error bounds, in both scenarios of any error as in [9] or of random errors as in [7]. Finally, in Section 4.3, we turn to linear error bounds which we integrate in both these scenarios.

4.1 Uniqueness results

For any error. The uniqueness of solutions $\mathcal{S}_{Y,\nu,\vartheta}$ is based on the following Proposition 4.1, which revisits [9] and requires to extend the definition of $\mathcal{L}$ (see (2))

$$\mathcal{L}(\nu,\vartheta) := \min\begin{pmatrix}\max(N-1+\vartheta, D-1+\nu)\\ \max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta)\end{pmatrix}.$$

Notice that $\mathcal{L}(N,D) = \mathcal{L}$.

Proposition 4.1. *Under the setting of Definition 2.1, if $L \geq L'_{KPSW}$ with $L'_{KPSW}(\nu,\vartheta,\tau) := \mathcal{L}(\nu,\vartheta)+\tau$ then $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$.*

We remark that Proposition 2.2 is a special case of Proposition 4.1 for $\nu = N+\tau, \vartheta = D+\tau$ (in which case $\delta_{\nu,\vartheta} > 0$). Indeed, $L'_{KPSW}(N+\tau, D+\tau, \tau) = \mathcal{L}(N+\tau, D+\tau)+\tau = \mathcal{L}+2\tau = L_{KPSW}$. Remark that $L'_{KPSW}(\nu,\vartheta,\tau)$ is non-decreasing in both ν and ϑ, and that $L'_{KPSW}(\nu+i,\vartheta+i,\tau) = L'_{KPSW}(\nu,\vartheta,\tau)+i$ for any $i \in \mathbb{Z}$.

Proof. We now prove that $\mathcal{S}_{Y,\nu,\vartheta} \subset \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$, the other inclusion being straightforward. From now on, we fix $(\boldsymbol{\varphi},\psi) \in \mathcal{S}_{Y,\nu,\vartheta}$. Let us show that $\boldsymbol{v}\psi - d\boldsymbol{\varphi} = \boldsymbol{0}$.

Assume that $L \geq \max(D-1+\nu, N-1+\vartheta)+\tau$. Combining for all j the equalities $\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{y}_j\psi(\alpha_j)$ and $(\Lambda\boldsymbol{v})(\alpha_j) = \boldsymbol{y}_j(\Lambda d)(\alpha_j)$, we get $(\Lambda(\boldsymbol{v}\psi - d\boldsymbol{\varphi}))(\alpha_j) = 0$. Now, we must have $\Lambda(\boldsymbol{v}\psi - d\boldsymbol{\varphi}) = \boldsymbol{0}$ since it has at least L roots and degree $< |E|+\max(\deg(\boldsymbol{v})+\vartheta, \deg(d)+\nu) \leq L$ by assumption. Finally, $\Lambda \neq 0$ so $\boldsymbol{v}\psi - d\boldsymbol{\varphi} = \boldsymbol{0}$.

On the other hand, assume $L \geq \max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta)+\tau$. For all j, we have $\Lambda(\alpha_j)(A(\alpha_j)\boldsymbol{y}_j - \boldsymbol{b}(\alpha_j)) = \boldsymbol{0}$. Combining this equation with $\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{y}_j\psi(\alpha_j)$ we get $(\Lambda(A\boldsymbol{\varphi} - \psi\boldsymbol{b}))(\alpha_j) = 0$. Now, notice that $(\Lambda(A\boldsymbol{\varphi} - \psi\boldsymbol{b}))$ has at least L roots and degree $< |E|+\max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta) \leq L$ by assumption. So $A\boldsymbol{\varphi} = \psi\boldsymbol{b}$. Combined with $A\boldsymbol{v} = d\boldsymbol{b}$, we get $A(\boldsymbol{\varphi}d - \boldsymbol{v}\psi) = \boldsymbol{0}$. Since A is full rank, we obtain $\boldsymbol{\varphi}d - \boldsymbol{v}\psi = \boldsymbol{0}$.

Since $\boldsymbol{\varphi}d - \boldsymbol{v}\psi = \boldsymbol{0}$ and $\gcd(\gcd_i(v_i), d) = 1$ then there exists $P \in \mathbb{F}_q[x]$ such that $(\boldsymbol{\varphi},\psi) = (P\boldsymbol{v}, Pd)$. The key equations $\boldsymbol{\varphi}(\alpha_j) = \boldsymbol{y}_j\psi(\alpha_j)$ yield $P(\alpha_j)(\boldsymbol{v}(\alpha_j) - \boldsymbol{y}_j d(\alpha_j)) = \boldsymbol{0}$ and so $P(\alpha_j) = 0$ for $j \in E$. This means that $\exists P' \in \mathbb{F}_q[x], P = \Lambda P'$. Finally, $(\boldsymbol{\varphi},\psi) = P'(\Lambda\boldsymbol{v}, \Lambda d)$ and the degree constraints on $(\boldsymbol{\varphi},\psi)$ imply $\deg P' < \delta_{\nu,\vartheta}$ which concludes our proof. □

For random errors. In the context of random errors, we can further reduce the number of evaluations of Proposition 4.1 required to get a unique solution in $\mathcal{S}_{Y,\nu,\vartheta}$.

Theorem 4.2. *Under the setting of Definition 2.1, let $L \geq L'_{GLZ}$ where $L'_{GLZ}(\nu,\vartheta,\tau) := \mathcal{L}(\nu,\vartheta) + \lceil\tau/n\rceil$, and fix an error support $E \subseteq \{1,\ldots,L\}$ such that $|E| \leq \tau$. Consider the random matrix Y whose columns $\boldsymbol{y}_j \in \mathbb{F}_q^n$ are such that $\boldsymbol{y}_j = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ if $j \notin E$, and $\boldsymbol{y}_j$ is uniformly distributed if $j \in E$.*

Then $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$ with probability $\geq 1 - \frac{\vartheta}{q}$.

Note that Theorem 3.1 is a special case of Theorem 4.2 for $\nu = N+\tau, \vartheta = D+\tau$ (in which case $\delta_{\nu,\vartheta} > 0$). Indeed, $L'_{GLZ}(N+\tau, D+\tau, \tau) = L_{GLZ}$.

Proof. The proof is similar to the proof of Theorem 3.1. We slightly adapt the first part to prove that there exists a draw W of Y for which $\mathcal{S}_{W,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$. As in Proposition 4.1, we only need to prove the inclusion $\subseteq$. We still consider the partition $E = \cup_{i=1}^{n} I_i$ such that $|I_i| \leq \lceil|E|/n\rceil$ for all i. Recall that for any $j \in E$, we denote by i_j the unique index such that $j \in I_{i_j}$.

We first assume that $\mathcal{L}(\nu,\vartheta) = \max(N-1+\vartheta, D-1+\nu)$. Construct a matrix W (as in the proof of Theorem 3.1) whose columns $\boldsymbol{w}_j$ satisfy $\boldsymbol{v}(\alpha_j) - d(\alpha_j)\boldsymbol{w}_j = \boldsymbol{0}$ if $j \notin E$, and $\boldsymbol{v}(\alpha_j) - d(\alpha_j)\boldsymbol{w}_j = \boldsymbol{\varepsilon}_{i_j}$ if $j \in E$. Let $(\boldsymbol{\varphi},\psi) \in \mathcal{S}_{W,\nu,\vartheta}$ and denote $\boldsymbol{p} := \psi\boldsymbol{v} - d\boldsymbol{\varphi}$, and p_i its ith component. We adapt the proof that gives $\boldsymbol{p}(x) = \boldsymbol{0}$.

We deduce as before that $\boldsymbol{p}(\alpha_j) = 0$ for $j \notin E$, and $\boldsymbol{p}(\alpha_j) = \psi(\alpha_j)\boldsymbol{\varepsilon}_{i_j}$ for $j \in E$. Fix $1 \leq i \leq n$, then for any $j \notin I_i$, $p_i(\alpha_j) = 0$. Now, notice that p_i has degree $\leq \max(\vartheta+N-1, D-1+\nu)-1$ and its number of roots is $L - |I_i| \geq L - \lceil|E|/n\rceil \geq L'_{GLZ} - \lceil|\tau|/n\rceil = \max(\nu+D-1, \vartheta+N-1)$ and so it is the zero polynomial.

Now assume that $\mathcal{L}(\nu,\vartheta) = \max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta)$. Construct a matrix W such that $A(\alpha_j)\boldsymbol{w}_j - \boldsymbol{b}(\alpha_j) = \boldsymbol{0}$ if $j \notin E$, and $A(\alpha_j)\boldsymbol{w}_j - \boldsymbol{b}(\alpha_j) = \boldsymbol{\varepsilon}_{i_j}$ if $j \in E$. Let $(\boldsymbol{\varphi},\psi) \in \mathcal{S}_{W,\nu,\vartheta}$ and denote $\boldsymbol{p} := A\boldsymbol{\varphi} - \boldsymbol{b}\psi$. Let us show that $\boldsymbol{p}(x) = \boldsymbol{0}$. As before, $p_i(\alpha_j) = 0$ for any $j \notin I_i$. Notice that $\deg(p_i) < \max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta)$ and that the number of roots is at least $L - |I_i| \geq \max(\deg(A)+\nu, \deg(\boldsymbol{b})+\vartheta)$ and so $p_i = 0$. Therefore, $A(x)\boldsymbol{\varphi}(x) = \boldsymbol{b}(x)\psi(x)$, but since $\boldsymbol{y}(x) = \frac{\boldsymbol{v}(x)}{d(x)}$ is the only solution of the linear system, we get $\psi\boldsymbol{v} - d\boldsymbol{\varphi} = \boldsymbol{0}$ also in this case.

The conclusion of the first part is the same as before, except that the new degree constraints lead to $\delta_{\nu,\vartheta}$ instead of $\delta_{N+\tau,D+\tau}$.

For the second part, now only the last ϑ columns of the matrix $M_{Y,\nu,\vartheta}$ contains the variables $(y_{i,j})_{1\leq i\leq n, j\in E}$. So the probability that $\mathcal{S}_{Y,\nu,\vartheta} \neq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$ is $\leq \vartheta/q$ using the Schwartz-Zippel Lemma. □

4.2 Fixed error bound

We are now ready to introduce our Early Termination Algorithm 1 for PLSwE in the context of a fixed error bound τ. Note that in Algorithm 1 the number of evaluations varies, which could affect the number of errors. Therefore, we denote $|E(L)| := |\{1 \leq j \leq L \mid \boldsymbol{e}_j \neq 0\}|$ instead of $|E|$ to stress out the dependency on L. So our assumption on the fixed error bound τ is that $|E(L)| \leq \tau$ for each value of L during the execution of Algorithm 1. As explained before, we can choose such an error bound τ because the number of

Algorithm 1: Early Termination algorithm for PLSwE in the context of a fixed error bound τ.

```
Input:
    (1) a fixed error bound $\tau$
    (2) degrees $\deg(A), \deg(\boldsymbol{b})$ and degree bounds $N, D$
    (3) an evaluations count $L'(\nu, \vartheta, \tau) \in \{L'_{KPSW}, L'_{GLZ}\}$
    (4) a stream of vectors $Y = (\boldsymbol{y}_j)_{j=1,2,\dots}$ extensible on demand
Output: $(\boldsymbol{v}, d)$ the solution of PLSwE
1 $L \leftarrow L'(1, 1, \tau)$ ; Extend $Y$ to $L$ vectors;
2 while true do
3     foreach $\nu, \vartheta$ such that $L'(\nu, \vartheta, \tau) = L$ do
4         if Check$(Y, \nu, \vartheta)$ then
5             return FindSolution$(Y, \nu, \vartheta)$;
6     $L \leftarrow L + 1$; Extend $Y$ to $L$ vectors;
```

evaluations L does not exceed the evaluations counts L_{KPSW}, L_{GLZ} considered in Sections 2 and 3.

Remark also that we need to consider $\deg(A), \deg(\boldsymbol{b}), N, D$ as inputs of Algorithm 1 since they are implicitly used in $L'(\nu, \vartheta, \tau)$ which is either the evaluation count $L'_{KPSW}(\nu, \vartheta, \tau)$ of Proposition 4.1 or $L'_{GLZ}(\nu, \vartheta, \tau)$ of Theorem 4.2.

Optimizing Algorithm 1. Notice that Check and FindSolution perform the same computation, *i.e.* compute a basis of $\mathcal{S}_{Y,\nu,\vartheta}$, and should be merged in practice.

Remark 4.3. We can optimize the steps 2 and 3 of Algorithm 1 by only testing, for each L, two specific (ν, ϑ) instead of all those giving L. The goal is to make early termination algorithms have a smaller failure probability, and incidentally to make them faster.

We want to find which (ν, ϑ) maximizes $\delta_{\nu,\vartheta}$ among those such that $L'(\nu, \vartheta, \tau) = L$ when L is fixed. We will consider the equivalent problem of maximizing $\delta_{\nu,\vartheta}$ for all (ν, ϑ) such that $\mathcal{L}(\nu, \vartheta) = \lambda$, for a fixed λ. The two candidates are $(\nu_1, \vartheta_1) = (\lambda - (D-1), \lambda - (N-1))$ and $(\nu_2, \vartheta_2) = (\lambda - \deg(A), \lambda - \deg(\boldsymbol{b}))$. Define the ordering $(\nu_1, \vartheta_1) \le (\nu_2, \vartheta_2) \Leftrightarrow (\nu_1 \le \nu_2$ and $\vartheta_1 \le \vartheta_2)$, so that $(\nu_1, \vartheta_1) \le (\nu_2, \vartheta_2)$ implies $\delta_{\nu_1,\vartheta_1} \le \delta_{\nu_2,\vartheta_2}$.

We now show that for any (ν, ϑ) such that $\lambda = \mathcal{L}(\nu, \vartheta)$, we have $(\nu, \vartheta) \le (\nu_1, \vartheta_1)$ or $(\nu, \vartheta) \le (\nu_2, \vartheta_2)$. Indeed, either $\lambda = \mathcal{L}(\nu, \vartheta) = \max(D - 1 + \nu, N - 1 + \vartheta)$ and $(\nu, \vartheta) \le (\nu_1, \vartheta_1)$, or $\lambda = \mathcal{L}(\nu, \vartheta) = \max(\deg(A) + \nu, \deg(\boldsymbol{b}) + \vartheta)$ and $(\nu, \vartheta) \le (\nu_2, \vartheta_2)$.

Remark that if $(D-1, N-1) \le (\deg(A), \deg(\boldsymbol{b}))$ then we should only try (ν_1, ϑ_1) because $(\nu_1, \vartheta_1) \ge (\nu_2, \vartheta_2)$ and $\mathcal{L}(\nu_1, \vartheta_1) = \lambda$ (but possibly $\mathcal{L}(\nu_2, \vartheta_2) \ne \lambda$). Similarly, if $(D-1, N-1) \ge (\deg(A), \deg(\boldsymbol{b}))$ then we should only try (ν_2, ϑ_2). However, if $(D-1, N-1)$ and $(\deg(A), \deg(\boldsymbol{b}))$ are not comparable, we should try both candidates because they are not comparable, and they both lead to $\mathcal{L}(\nu_1, \vartheta_1) = \mathcal{L}(\nu_2, \vartheta_2) = \lambda$. □

Termination. We now analyze the termination of Algorithm 1, and show that it stops exactly when the number of correct evaluations $C(L) := L - |E(L)|$ reaches $L'(\deg(\boldsymbol{v}), \deg(d), \tau) + 1$.

Proposition 4.4. *Algorithm 1 terminates, and when it stops, $L \le L^s$, where $L^s := min\{L \mid C(L) \ge L'(\deg(\boldsymbol{v}), \deg(d), \tau) + 1\}$.*

More precisely, Algorithm 1 terminates with L^s evaluations, except in the case of random errors $L' = L'_{GLZ}$ where Algorithm 1 could stop with $L < L^s$ evaluations with bounded probability (see Proposition 4.6).

Proof. We start by showing that L^s is well-defined. Since $C(L)$ verifies $C(0) = 0$, $\lim_{L \to +\infty} C(L) = +\infty$, $C(L) \le C(L+1) \le C(L)+1$, it must be surjective onto $\mathbb{N}$. As a consequence, $C(L)$ will eventually reach $L'(\deg(\boldsymbol{v}), \deg(d), \tau) + 1$, so that L^s is well-defined. We get additionally that $C(L^s) = L'(\deg(\boldsymbol{v}), \deg(d), \tau) + 1$.

For the parameters $\nu = \deg(\boldsymbol{v}) + |E(L^s)| + 1$ and $\vartheta = \deg(d) + |E(L^s)| + 1$, the number of evaluations $L = L'(\nu, \vartheta, \tau)$ equals to L^s and the algorithm stops (because $\delta_{\nu,\vartheta} > 0$ always implies $\mathcal{S}_{Y,\nu,\vartheta} \ne \{(\boldsymbol{0}, 0)\}$).

Assume now that Check always output a correct answer, *i.e.* that it correctly tells if $\delta_{\nu,\vartheta} > 0$ or not. We prove by contraposition that if $L < L^s$ then the algorithm does not stop, *i.e.* $\delta_{\nu,\vartheta} \le 0$ for all ν, ϑ such that $L = L'(\nu, \vartheta, \tau)$. Indeed if there exists ν, ϑ such that $\delta_{\nu,\vartheta} > 0$, then $\deg(\boldsymbol{v}) + |E(L)| < \nu$ and $\deg(d) + |E(L)| < \vartheta$ for $L = L'(\nu, \vartheta, \tau)$. As $L'(\nu, \vartheta, \tau)$ is non-decreasing in each variable ν, ϑ, we obtain $L \ge L'(\deg(\boldsymbol{v}), \deg(d), \tau) + |E(L)| + 1$ and so $L \ge L^s$.

We refer to the proof of Proposition 4.6 for the probability that Check outputs an incorrect answer during the execution of Algorithm 1. □

Remark 4.5. Our early termination strategy requires $L^s = L'_{KPSW}(\deg(\boldsymbol{v}), \deg(d), \tau) + |E(L^s)| + 1$ evaluations whereas [9, Equations 5 and 9] needs $L'_{KPSW}(\deg(\boldsymbol{v}), \deg(d), \tau) + \tau + 1$ evaluations. So we save some evaluations in Algorithm 1 due to a dependency on the real number of errors $|E(L^s)|$ (instead of τ). To the best of our knowledge, this dependency is original in the literature. □

Correctness. The correctness of Algorithm 1 is related to the correctness of Check and FindSolution. Recall that Check(Y, ν, ϑ) outputs the Boolean $\delta_{\nu,\vartheta} > 0$ by computing $\mathcal{S}_{Y,\nu,\vartheta}$!= $\{(\boldsymbol{0}, 0)\}$.

We know that $(\delta_{\nu,\vartheta} > 0)$ *iff* $(\langle x^i \Lambda \boldsymbol{v}, x^i \Lambda d \rangle_{0 \le i < \delta_{\nu,\vartheta}} \ne 0)$. So Check$(Y, \nu, \vartheta)$ is correct when $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i \Lambda \boldsymbol{v}, x^i \Lambda d \rangle_{0 \le i < \delta_{\nu,\vartheta}}$. By Proposition 4.4, if $L' = L'_{KPSW}$ then Check(Y, ν, ϑ) is correct and so FindSolution(Y, ν, ϑ) returns $(\boldsymbol{v}, d)$.

On the other hand, if $L' = L'_{GLZ}$, the correctness of Algorithm 1 depends on the draw of random error. Indeed, by Theorem 4.2, we have $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i \Lambda \boldsymbol{v}, x^i \Lambda d \rangle_{0 \le i < \delta_{\nu,\vartheta}}$ with probability $\ge 1 - \vartheta/q$, in which case Check is correct and FindSolution outputs $(\boldsymbol{v}, d)$.

Recall that FindSolution was defined only in the case $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i \Lambda \boldsymbol{v}, x^i \Lambda d \rangle$ (see Remark 2.3). Nevertheless, it could happen with probability $\le \vartheta/q$ that FindSolution is called, *i.e.* Check(Y, ν, ϑ) is true, but $\mathcal{S}_{Y,\nu,\vartheta} \ne \langle x^i \Lambda \boldsymbol{v}, x^i \Lambda d \rangle_{0 \le i < \delta_{\nu,\vartheta}}$. In order to handle this situation, we modify FindSolution to output a failure message if the minimal degree solution $(\boldsymbol{\varphi}_{min}, \psi_{min})$ of $\mathcal{S}_{Y,\nu,\vartheta}$ does not span all solutions (see Remark 2.3).

Recall that we try at most 2 affectations of parameters (ν_1, ϑ_1) and (ν_2, ϑ_2) for each number of evaluations L (see Remark 4.3). In the following proposition, we denote by (ν_1^s, ϑ_1^s), (ν_2^s, ϑ_2^s) the candidate parameters corresponding to L^s.

Proposition 4.6. *Algorithm 1 is correct, except when $L' = L'_{GLZ}$ with probability $\leq \frac{2\max(\vartheta_1^s,\vartheta_2^s)(\deg(\Lambda\boldsymbol{v},\Lambda d)+1)}{q}$.*

Proof. If all calls to `Check` and `FindSolution` output a correct answer during the execution of Algorithm 1, then Algorithm 1 returns the solution $(\boldsymbol{v}, d)$. We have previously remarked that `Check` and `FindSolution` could output an incorrect answer only if $\mathcal{S}_{Y,\nu,\vartheta} \neq \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$ for a choice of parameters (ν, ϑ) at line 3. The probability of this later event is related to the number of loops of the **foreach** at line 3, which we now study. The number of evaluations starts from $L'(1, 1, \tau)$ and ends at $L^s = L'(\deg(\boldsymbol{v}), \deg(d), \tau) + |E(L^s)| + 1$: there are at most $\max(\deg(\boldsymbol{v}), \deg(d)) + |E(L^s)| + 1 = \deg(\Lambda\boldsymbol{v}, \Lambda d) + 1$ different evaluation counts. Moreover, for each number of evaluations L, we try at most 2 affectations of parameters (ν_1, ϑ_1) and (ν_2, ϑ_2). Now any attempt (ν, ϑ) could fail with probability $\leq \vartheta/q$. This latter probability is always $\leq \max(\vartheta_1^s, \vartheta_2^s)/q$ for all attempts of ϑ during the execution of Algorithm 1. Combining all these results, we can conclude that the probability that Algorithm 1 would return an incorrect answer is at most $\frac{2\max(\vartheta_1^s,\vartheta_2^s)(\deg(\Lambda\boldsymbol{v},\Lambda d)+1)}{q}$. □

In the special case $\deg(A\boldsymbol{v}) = \deg(A) + \deg(\boldsymbol{v})$, we can prove that $\max(\vartheta_1^s, \vartheta_2^s) \leq D + E(L^s)$ as a bonus. Indeed, we have $\max(\vartheta_1^s, \vartheta_2^s) = \mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) + E(L^s) + 1 - \min(N-1, \deg(\boldsymbol{b}))$. First, if $N - 1 \leq \deg(\boldsymbol{b})$, then we have that $\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) \leq \max(D-1+\deg(\boldsymbol{v}), N-1+\deg(d)) \leq N+D-2$, and so $\max(\vartheta_1^s, \vartheta_2^s) \leq D + E(L^s)$. Otherwise, $N - 1 \geq \deg(\boldsymbol{b})$, and $\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) \leq \max(\deg(A) + \deg(\boldsymbol{v}), \deg(\boldsymbol{b}) + \deg(d)) = \deg(\boldsymbol{b}) + \deg(d)$ since $A\boldsymbol{v} = \boldsymbol{b}d$ and $\deg(A) + \deg(\boldsymbol{v}) = \deg(A\boldsymbol{v}) = \deg(\boldsymbol{b}d) = \deg(\boldsymbol{b}) + \deg(d)$. Therefore, also in this case we get the bound $\max(\vartheta_1^s, \vartheta_2^s) \leq \deg(d) + 1 + E(L^s) \leq D + E(L^s)$.

4.3 Linear error bound

Up until now, our early termination schemes consider fixed error bounds τ when L varies. This error bound τ has to be valid for the largest possible number of evaluations L that Algorithm 1 could reach. It would be interesting to have an error bound τ that grows along with the number of evaluations. In this case, the bound would be tighter than a fixed error bound when L is an intermediate number of evaluations. For this aim, in this section, we consider a linear error bound which depends on a given *error rate* ρ_E.

Assumption 4.7. For any number of evaluations L, the number of errors $|E(L)|$ is bounded by $|E(L)| \leq \rho_E L$ where $0 \leq \rho_E < 1/2$.

This assumption comes from [9–11], where they also consider the variant $|E(L)| \leq \lceil \rho_E L \rceil$. For the sake of simplicity, we restrict ourselves to Assumption 4.7. However, we are confident that our results can be adapted to the alternative linear error bound, and we leave it to future work.

Uniqueness results. We start by adapting Proposition 4.1 to the special case of linear error bound. This proposition is our adaptation of [9] where we add sensitivity to the real number of errors.

Proposition 4.8. *Consider $L = \left\lfloor \frac{\mathcal{L}(\nu,\vartheta)+1}{1-\rho_E} \right\rfloor$ evaluation points and the error bound $\tau = \lfloor \rho_E L \rfloor$. Under the setting of Definition 2.1 and Assumption 4.7, we have $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$.*

Intuitively, Proposition 4.8 is obtained from Proposition 4.1 by setting $\tau = \rho_E L$ in $L = L'_{KPSW}(\nu, \vartheta, \tau) = \mathcal{L}(\nu, \vartheta) + \tau$, thus obtaining $L = \mathcal{L}(\nu, \vartheta)/(1 - \rho_E)$. However, L is an integer, so we have to consider the count of Proposition 4.8. We postpone the proof after Proposition 4.9 in order to prove both results at the same time.

As before, we can lower the number of evaluation points by considering randomly distributed errors. Theorem 4.2 can be adapted to the context of a linear error bound.

Proposition 4.9. *Assume that we are in the setting of Definition 2.1, with the additional Assumption 4.7 and consider an error support E and a random matrix Y as in Theorem 4.2.*

Using $L = \left\lfloor \frac{\mathcal{L}(\nu,\vartheta)+1}{1-\rho_E/n} \right\rfloor$ evaluations and error bound $\tau = \lfloor \rho_E L \rfloor$, we have $\mathcal{S}_{Y,\nu,\vartheta} = \langle x^i\Lambda\boldsymbol{v}, x^i\Lambda d\rangle_{0\leq i<\delta_{\nu,\vartheta}}$ with probability at least $1 - \frac{\vartheta}{q}$.

Proof of Propositions 4.8 and 4.9. We prove simultaneously both propositions by considering $\left\lfloor \frac{\mathcal{L}(\nu,\vartheta)+1}{1-\rho_E/m} \right\rfloor$, which specializes to the number of evaluations of Proposition 4.8 when $m = 1$, and to the one of Proposition 4.9 when $m = n$.

Let $m \in \mathbb{N}^*$ and denote $\bar{L}^*(\nu, \vartheta) = \frac{\mathcal{L}(\nu,\vartheta)+1}{1-\rho_E/m}$, so that $L^*(\nu, \vartheta) = \left\lfloor \bar{L}^*(\nu, \vartheta) \right\rfloor$ is the number of evaluations, and $\tau^*(\nu, \vartheta) = \lfloor \rho_E L^*(\nu, \vartheta) \rfloor$ is the error bound.

Our goal is to show that we are under the hypotheses of Proposition 4.1 ($m = 1$) or Theorem 4.2 ($m = n$), *i.e.* that $\mathcal{L}(\nu, \vartheta) + \lceil \tau^*(\nu, \vartheta)/m \rceil \leq L^*(\nu, \vartheta)$ and $|E(L^*(\nu, \vartheta))| \leq \tau^*(\nu, \vartheta)$.

First $|E(L^*(\nu, \vartheta))| \leq \rho_E L^*(\nu, \vartheta)$ using Assumption 4.7. Since $|E(L^*(\nu, \vartheta))| \in \mathbb{N}$, we get $|E(L^*(\nu, \vartheta))| \leq \lfloor \rho_E L^*(\nu, \vartheta) \rfloor = \tau^*(\nu, \vartheta)$. Then

$$\begin{aligned}
\mathcal{L}(\nu, \vartheta) + \lceil \tau^*(\nu, \vartheta)/m \rceil &\leq \mathcal{L}(\nu, \vartheta) + \tau^*(\nu, \vartheta)/m + 1 \\
&\leq \mathcal{L}(\nu, \vartheta) + \rho_E/m L^*(\nu, \vartheta) + 1 \\
&\leq \mathcal{L}(\nu, \vartheta) + \rho_E/m \bar{L}^*(\nu, \vartheta) + 1 = \bar{L}^*(\nu, \vartheta).
\end{aligned}$$

Finally $\mathcal{L}(\nu, \vartheta) + \lceil \tau^*(\nu, \vartheta)/m \rceil \leq \left\lfloor \bar{L}^*(\nu, \vartheta) \right\rfloor = L^*(\nu, \vartheta)$. □

Early termination algorithm. We can use the evaluation counts of Propositions 4.8 and 4.9 to detect if (ν, ϑ) are good estimations, and eventually return the solution $(\boldsymbol{v}, d)$ of the PLS. We formalize this idea in Algorithm 2. It remains to prove its correctness and termination.

In the context of [9], the correctness of Algorithm 2 is a consequence of Proposition 4.8. Its termination is studied in the following proposition.

Proposition 4.10. *We have the following results:*

1. *Algorithm 2 stops with at most L^s evaluations where*
$$L^s = min\left\{ L \;\middle|\; L \geq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) + |E(L)| + 2}{1 - \rho_E} \right\rfloor \right\}. \quad (5)$$
2. *We can bound $L^s \leq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-2\rho_E} \right\rfloor$.*
3. *If for some reason fewer errors are made, i.e. $|E(L)| \leq \rho'_E L$ with $\rho'_E < \rho_E$, then $L^s \leq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-\rho'_E-\rho_E} \right\rfloor$.*

The inequality given in Item 2 relates the performance of our early termination algorithm to the literature. Indeed, the right-hand bound can be derived from [9, Algorithm 2.2] with $\rho_R = 0$ (no rank drops) and $q_R = q_E = +\infty$ (for simplicity).

Algorithm 2: Early Termination algorithm for PLSwE in the context of a linear error bound.

```
Input:
    (1) an error rate $\rho_E$
    (2) degrees $\deg(A), \deg(\boldsymbol{b})$ and degree bounds $N, D$
    (3) a stream of vectors $Y = (\boldsymbol{y}_j)_{j=1,2,\ldots}$ extensible on demand
Output: $(\boldsymbol{v}, d)$ the solution of PLSwE.
$L^{num} \leftarrow \mathcal{L}(1,1) + 1$;
while true do
    $L \leftarrow \left\lfloor \frac{L^{num}}{1-\rho_E} \right\rfloor$ (any error) or $\left\lfloor \frac{L^{num}}{1-\rho_E/n} \right\rfloor$ (random error);
    Extend $Y$ to $L$ vectors;
    foreach $\nu, \vartheta$ such that $\mathcal{L}(\nu, \vartheta) + 1 = L^{num}$ do
        if Check$(Y, \nu, \vartheta)$ then
            return FindSolution$(Y, \nu, \vartheta)$;
    $L^{num} \leftarrow L^{num} + 1$; Extend $Y$ to $L$ vectors;
```

Note that ρ_E and ρ'_E don't play the same role: ρ_E must be known in advance (it is an input of the algorithm) and be related to a linear error bound that is always true. If Assumption 4.7 is not true, then the correctness of Algorithm 2 may be lost. On the other hand, ρ'_E is used to demonstrate that our early termination technique is sensitive to the real number of errors (in addition to real degrees of $\boldsymbol{v}, d$), *i.e.* that it can stop earlier if fewer errors than expected are made.

In the context of random errors, we can lower the number of evaluations L^s when Algorithm 2 stops.

Proposition 4.11. *In the context of random errors, we have:*

1. *Algorithm 2 stops with at most L^s evaluations, where*
$$L^s = min\left\{L \,\middle|\, L \geq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) + |E(L)| + 2}{1 - \rho_E/n} \right\rfloor\right\}. \quad (6)$$
2. *We can bound $L^s \leq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-(1+1/n)\rho_E} \right\rfloor$.*
3. *If $|E(L)| \leq \rho'_E L$, then $L^s \leq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-\rho'_E-\rho_E/n} \right\rfloor$.*
4. *Finally, the output of Algorithm 2 is correct with probability $\geq 1 - \frac{2\max(\vartheta_1^s,\vartheta_2^s)(\deg(\Lambda\boldsymbol{v},\Lambda d)+1)}{q}$ (see Proposition 4.6).*

Proof of Propositions 4.10 and 4.11. We keep the notations of the proof of Proposition 4.8, *e.g.* $m \in \mathbb{N}^*$ must be replaced by $m = 1$ for Proposition 4.10, and by $m = n$ for Proposition 4.11.

(1) We need to prove that Algorithm 2 stops. Consider $f(L) := L - \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+\rho_E L+2}{1-\rho_E/m}$, which is strictly increasing because $1 > \rho_E/(1-\rho_E/m)$ (since $0 \leq \rho_E < 1/2$).

Let $g(L) = L - \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+|E(L)|+2}{1-\rho_E/m}$. We have $g(L) \geq f(L)$ so $\lim_{L\to+\infty} g(L) = +\infty$. Rewrite $L^s = min\{L | \lceil g(L) \rceil \geq 0\}$ (using $-\lfloor x \rfloor = \lceil -x \rceil$) to deduce that L^s exists. Moreover $-1 < g(L^s) \leq g(L^s - 1) + 1 \leq 0$, so $\lceil g(L^s) \rceil = 0$ and
$$L^s = \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) + |E(L^s)| + 2}{1 - \rho_E/m} \right\rfloor.$$
Put it differently, we have that $L^s = L^*(\nu^s, \vartheta^s)$ for $\nu^s = \deg(\boldsymbol{v}) + |E(L^s)|+1$, $\vartheta^s = \deg(d)+|E(L^s)|+1$ (see the proof of Proposition 4.9). So $\delta_{\nu^s,\vartheta^s} > 0$ and Algorithm 2 would stop with $L \leq L^s$ evaluations.

(2) Now let $\bar{L}' = \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-(1+1/m)\rho_E}$ and $L' = \lfloor \bar{L}' \rfloor$. $\bar{L}'$ is defined so that $0 = f(\bar{L}')$. Since $f(L^s) \leq g(L^s) = 0 = f(\bar{L}')$ and f is strictly increasing, we have $L^s \leq \bar{L}'$, thus $L^s \leq \lfloor \bar{L}' \rfloor = L'$.

(3) If one execution of PLSwE satisfies $|E(L)| \leq \rho'_E L$ for $\rho'_E < \rho_E$, we can prove that $L^s \leq \left\lfloor \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+2}{1-\rho'_E-\rho_E/m} \right\rfloor$ by adapting the previous proof with $\overline{f}(L) := L - \frac{\mathcal{L}(\deg(\boldsymbol{v}),\deg(d))+\rho'_E L+2}{1-\rho_E/m}$. Indeed $\bar{f}$ is still strictly increasing and verifies $g(L) \geq \bar{f}(L)$.

The statement of correctness for random errors can be proved similarly to Proposition 4.6. The only difference is that we need to consider L^{num} (see Algorithm 2) instead of L to count the number of loops. The numerator L^{num} of number of evaluations L starts from $\mathcal{L}(1,1)+1$ and ends at $\mathcal{L}(\deg(\boldsymbol{v}), \deg(d)) + |E(L^s)| + 2$: there are at most $\max(\deg(\boldsymbol{v}), \deg(d)) + |E(L^s)| + 1 = \deg(\Lambda\boldsymbol{v}, \Lambda d) + 1$ different values for L^{num}. □

REFERENCES

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

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

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

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

[5] S. Cabay. 1971. Exact Solution of Linear Equations. In *Proceedings of SYMSAC'71* (Los Angeles, California, USA). Association for Computing Machinery, New York, NY, USA.

[6] J. von zur Gathen and J. Gerhard. 2013. *Modern Computer Algebra* (3rd ed.). Cambridge University Press.

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

[8] E. Guerrini, R. Lebreton, and I. Zappatore. 2020. On the Uniqueness of Simultaneous Rational Function Reconstruction. In *Proceedings of ISSAC'20* (Kalamata, Messinia, Greece).

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

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

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

[12] M. Khonji, C. Pernet, J.-L. Roch, T. Roche, and T. Stalinski. 2010. Output-Sensitive Decoding for Redundant Residue Systems. In *Proceedings of ISSAC'10.*

[13] M. T. McClellan. 1977. The Exact Solution of Linear Equations with Rational Function Coefficients. *ACM Trans. Math. Softw.* 3, 1 (1977).

[14] M. Monagan. 2004. Maximal Quotient Rational Reconstruction: An Almost Optimal Algorithm for Rational Reconstruction. In *Proceedings of ISSAC'04.*

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

[16] J. Rosenkilde and A. Storjohann. 2016. Algorithms for Simultaneous Padé Approximations. In *Proceedings of ISSAC'2016.*

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

[18] G. Schmidt, V. Sidorenko, and M. Bossert. 2010. Syndrome Decoding of Reed–Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis. *IEEE Transactions on Information Theory* 56, 10 (2010).

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

[20] C.E. Shannon. 1948. A mathematical theory of communication. *Bell Syst. Tech. J.* 27, 3 (1948).