Early Termination in Parametric Linear System Solving and Rational Function Vector Recovery with Error Correction

Erich L. Kaltofen
Dept. of Mathematics, NCSU
Raleigh, NC, USA
kaltofen@ncsu.edu

Clément Pernet
Univ. Grenoble Alpes
Grenoble, France
clement.pernet@univ-grenoble-alpes.fr

Arne Storjohann
Univ. of Waterloo
Waterloo, Ontario, Canada
astorjoh@uwaterloo.ca

Cleveland Waddell
Dept. of Mathematics, NCSU
Raleigh, NC, USA
cawaddel@ncsu.edu

ABSTRACT

Consider solving a black box linear system, $A(u)x = b(u)$, where the entries are polynomials in u over a field K, and $A(u)$ is full rank. The solution, $x = \frac{1}{g(u)}f(u)$, where g is always the least common monic denominator, can be found by evaluating the system at distinct points $\xi_\ell \in \mathsf{K}$. The solution can be recovered even if some evaluations are erroneous. In [Boyer and Kaltofen, Proc. SNC 2014] the problem is solved with an algorithm that generalizes Welch/Berlekamp decoding of an algebraic Reed-Solomon code. Their algorithm requires the sum of a degree bound for the numerators plus a degree bound for the denominator of the solution. It is possible that the degree bounds input to their algorithm grossly overestimate the actual degrees. We describe an algorithm that given the same inputs uses possibly fewer evaluations to compute the solution.

We introduce a second count for the number of evaluations required to recover the solution based on work by Stanley Cabay. The Cabay count includes bounds for the highest degree polynomial in the coefficient matrix and right side vector, but does not require solution degree bounds. Instead our algorithm iterates until the Cabay termination criterion is reached. At this point our algorithm returns the solution. Assuming we have the actual degrees for all necessary input parameters, we give the criterion that determines when the Cabay count is fewer than the generalized Welch/Berlekamp count.

Incorporating our two counts we develop a combined early termination algorithm. We then specialize the algorithm in [Boyer and Kaltofen, Proc. SNC 2014] for parametric linear system solving to the recovery of a vector of rational functions, $\frac{1}{g(u)}f(u)$, from its evaluations. Thus, if the rational function vector is the solution to a full rank linear system our early termination strategy applies and we may recover it from fewer evaluations than generalized Welch/Berlekamp decoding. If we allow evaluations at poles (roots of g) there are examples where the Cabay count is not sufficient to recover the rational function vector from just its evaluations. This problem is solved if in addition to indicating that an evaluation point is a pole, the black box gives information about the numerators of the solution at the evaluation point.

ISSAC '17, July 25-28, 2017, Kaiserslautern, Germany

ACM ISBN 978-1-4503-5064-8/17/07…$15.00
https://doi.org/10.1145/3087604.3087645

1 INTRODUCTION

Consistent linear systems of the form $A(u)x = b(u)$, where $A(u) \in \mathsf{K}[u]^{m\times n}$ and full rank, $b(u) \in \mathsf{K}[u]^m$, $m \geq n$, and K is a field, have as their solution rational functions $x_i = f^{[i]}(u)/g^{[i]}(u)$, $1 \leq i \leq n$. In particular there is a solution $\frac{1}{g(u)}f(u)$,[1] where $g(u)$ is the monic, least common denominator, that is

$$\mathrm{GCD}(f, g) \stackrel{\text{def}}{=} \mathrm{GCD}(\mathrm{GCD}_i(f^{[i]}), g) = 1.$$

The solution of such a system can be determined by evaluating the system at distinct points $\xi_\ell \in \mathsf{K}$ and interpolating the evaluated solution [7]. The solution can be found even if some evaluations are erroneous. The matrices of the systems we consider have full column rank, so their solution in the form $\frac{1}{g(u)}f(u)$ is unique. Note that for full rank matrices with univariate polynomial entries there are finitely many $\xi_\ell \in \mathsf{K}$ that may cause the evaluated matrix to be rank deficient. If for each evaluation that causes the matrix with scalar entries to be rank deficient an extra evaluation is included, then techniques from algebraic error correcting codes can be used to compute the solution [2, 4–6, 9]. Furthermore in [2] it is shown that for non-erroneous evaluation points, ξ_ℓ, it is not necessary to have $A(\xi_\ell)$ and $b(\xi_\ell)$ in order to interpolate the solution. Rather it is enough to have a scalar matrix $\hat{A}^{[\ell]}$ and right side vector $\hat{b}^{[\ell]}$ that have the evaluated solution $\frac{1}{g(\xi_\ell)}f(\xi_\ell)$ as a solution.

Consider the following model. Suppose there exists an oracle, which we will refer to as the black box. If we supply the black box with a value, ξ_ℓ, from the field K the black box returns to us $\hat{A}^{[\ell]}$ and $\hat{b}^{[\ell]}$ with entries from the field K. The scalar matrix, $\hat{A}^{[\ell]}$, and right side vector, $\hat{b}^{[\ell]}$, which are returned may not be $A(\xi_\ell)$ and $b(\xi_\ell)$. Nevertheless, if we query the black box L times we assume that $\leq E$ times we get $\hat{A}^{[\lambda]}$ and $\hat{b}^{[\lambda]}$ such that $\hat{A}^{[\lambda]}f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]}$. Such evaluations are considered to be erroneous. Furthermore we assume that fewer than R times the black box returns $\hat{A}^{[\ell]}$ and $\hat{b}^{[\ell]}$ such that $\hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$ but $\mathrm{rank}(\hat{A}^{[\ell]}) < n$. The objective is to find the solution $x = \frac{1}{g(u)}f(u)$ of the system $A(u)x = b(u)$ from as few queries of the black box as possible.

The count for the number of ξ_ℓ

$$L \geq L_{\mathrm{BK}} \stackrel{\text{def}}{=} d_f + d_g + R + 2E + 1 \tag{1}$$

[1] We write $\frac{1}{g}f$ if f is a vector of polynomials and $\frac{1}{g}$ a rational function scalar.

is employed by [2] to recover the solution $\frac{1}{g(u)}f(u)$. The input parameters must satisfy the following specifications:

$$d_f \geq \deg(f) \stackrel{\text{def}}{=} \max_{1\leq i\leq m}\{\deg(f^{[i]})\}, \quad d_g \geq \deg(g), \tag{2}$$

$$E \geq \left|\{\,\lambda \mid \hat{A}^{[\lambda]}f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]} \text{ for } 0\leq\lambda\leq L-1\,\}\right|,^{2} \tag{3}$$

$$R \geq \left|\{\,\ell \mid \hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]} \text{ and } \operatorname{rank}(\hat{A}^{[\ell]}) < n \text{ for } 0\leq\ell\leq L-1\,\}\right|. \tag{4}$$

Here $|\cdot|$ denotes the cardinality of a set. The bounds E and R can be derived from an error and singularity rate; see below. If $n = m = 1$ and $\hat{A}^{[\ell]} = I_1$ and $\hat{b}^{[\ell]} = \frac{1}{g(\xi_\ell)}f(\xi_\ell)$ the algorithm is Welch/Berlekamp decoding of an algebraic (rational function) Reed-Solomon code [12]. We prove that for the vector rational function case if the input bounds in (2, 3, 4) are exact then the bound L_{BK} is tight; see Lemma 3.2.

If the bounds d_f and d_g on input significantly overestimate the degrees, by early termination we can reduce the number of required evaluations to

$$L^*_{\text{BK}} \stackrel{\text{def}}{=} \max\{d_f+\deg(g), d_g+\deg(f)\} + 2E^* + R^* + 1, \tag{5}$$

where

$$E^* \geq \left|\{\,\lambda \mid \hat{A}^{[\lambda]}f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]} \text{ for } 0\leq\lambda\leq L^*_{\text{BK}}-1\,\}\right|, \tag{6}$$

$$R^* \geq \left|\{\,\ell \mid \hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]} \text{ and } \operatorname{rank}(\hat{A}^{[\ell]}) < n \text{ for } 0\leq\ell\leq L^*_{\text{BK}}-1\,\}\right|. \tag{7}$$

The number of evaluations L^*_{BK} in (5) is determined iteratively, without $\deg(f)$ and $\deg(g)$ as input, but has to meet the conditions (6, 7) for the number of erroneous and rank-deficient systems at evaluation points ξ_ℓ. One can use the estimate $E^* = E$ and $R^* = R$ from (3,4) before, but we will show in Algorithm 2.2 below how to dynamically adjust E^* and R^* from an error and singularity rate associated with the black box for $\hat{A}^{[\ell]}, \hat{b}^{[\ell]}$, as is originally suggested in [6, Remark 1.1].

Following Stanely Cabay's [3] early termination strategy (see also [8]), we can derive a second count of number of evaluations. The new input parameters are specified as follows:

$$\left.\begin{aligned} d_A &\geq \deg(A) \stackrel{\text{def}}{=} \max_{1\leq i\leq m,1\leq j\leq n}\{\deg(a_{i,j})\},\\ d_b &\geq \deg(b) \stackrel{\text{def}}{=} \max_{1\leq i\leq m}\{\deg(b_i)\}. \end{aligned}\right\} \tag{8}$$

Because in our algorithms we do not reconstruct A and b, for the bounds d_A and d_b we can use that pair $(A(u), b(u))$ with $A(u)f(u) = g(u)b(u)$ with a minimum $\deg(A)$. We derive a second evaluations count,

$$L^*_{\text{CAB}} = \max\{d_A+\deg(f), d_b+\deg(g)\} + 2E^* + R^* + 1, \tag{9}$$

for recovering the solution. Here E^* and R^* bound from above the corresponding counts for erroneous and singular systems in (3, 4) with L^*_{CAB} replacing L^*_{BK}. We prove that if all input parameter bounds are exact and $\deg(g) > \deg(A)$ then $L^*_{\text{CAB}} < L^*_{\text{BK}}$.

Next we combine the L^*_{BK} count and the L^*_{CAB} count into a general early termination strategy. This algorithm computes the solution using as few evaluations as possible when it is unclear how the $\deg(g)$ compares to the $\deg(A)$.

We also show that rational function vector recovery with errors is a special case of the algorithm in [2] for parametric linear system solving with errors. If we consider $\hat{b}^{[\ell]} = \frac{1}{g(\xi_\ell)}f(\xi_\ell)$ and $\hat{A}^{[\ell]} = I_n$ then we can recover the rational function vector $\frac{1}{g(u)}f(u)$ from its evaluations, when some evaluations are erroneous, using the [2] algorithm. Thus we can apply our early termination algorithms to the problem of rational function vector recovery with errors. There is just one caveat; for rational functions $\frac{1}{g(u)}f(u)$ where the $\deg(g) > \deg(A)$ we need more information at poles (when ξ_ℓ is a root of g). There are examples where it is not enough to just indicate that an evaluation point is a pole when attempting early termination. If we are to recover the rational function vector when some evaluations are poles then we need the black box to provide information about the numerators of the solution. We discuss in detail the additional information we require from the black box when it indicates that an evaluation is a pole.

[2]Note that the condition (3) on the error bound E rules out inconsistent systems.

2 EARLY TERMINATION

We describe and prove an early termination algorithm for the exact vector of function solving algorithm in [2]. Their algorithm solves a system of linear equations

$$A(u)\,x = b(u) \tag{10}$$

where $A(u) \in \mathsf{K}[u]^{m\times n}, b(u) \in \mathsf{K}[u]^m, m \geq n$ and K is a field. The system is assumed to have a unique solution

$$x = \begin{bmatrix} \vdots \\ \frac{1}{g(u)}f^{[i]}(u) \\ \vdots \end{bmatrix} \in \mathsf{K}(u)^n, \quad g \neq 0, \tag{11}$$

where g is the monic least common denominator. If for all $i, f^{[i]} = 0$ then g is set to 1. The solution vector x is computed by:

1. Selecting $L = d_f + d_g + R + 1$ distinct elements $\xi_\ell \in \mathsf{K}$ where
   a. $0 \leq \ell \leq L-1$ and $\xi_{\ell_1} \neq \xi_{\ell_2}$ for $\ell_1 \neq \ell_2$.
   b. $d_f \geq \deg(f)$.
   c. $d_g \geq \deg(g)$.
   d. $R \geq \left|\{\ell \mid \operatorname{rank}(A(\xi_\ell)) < n = \operatorname{rank}(A(u))\}\right|$.
2. Solving the homogeneous linear system

$$A(\xi_\ell)\begin{bmatrix} \vdots \\ \Phi^{[i]}(\xi_\ell) \\ \vdots \end{bmatrix} - \Psi(\xi_\ell)b(\xi_\ell) = 0, \tag{12}$$

where for all $i, \deg(\Phi^{[i]}) \leq d_f$ and $\deg(\Psi) \leq d_g$. The system (12) is linear in the coefficients of $\Phi^{[i]}(u)$ and $\Psi(u)$. There are $n(d_f+1)+d_g+1$ unknown coefficients for $\Phi^{[i]}$ and Ψ and mL equations.

Theorem 2.1. [2] *We suppose that for* $\geq d_f + d_g + 1$ *of the* ξ_ℓ *we have* $\operatorname{rank}(A(\xi_\ell)) = \operatorname{rank}(A(u)) = n$. *Let* $\Psi_{\min}$ *be the denominator component of a solution of* (12) *with* $\Psi_{\min} \neq 0$ *and scaled to have leading coefficient* 1 *in* u, *and of minimal degree of all such solutions, and let* $\Phi^{[i]}_{\min}$ *be the corresponding numerator components of that solution. Then for all* i *we have* $\Phi^{[i]}_{\min} = f^{[i]}$ *and* $\Psi_{\min} = g$.

The linear system (12) uses evaluations of $A(u)$ and $b(u)$ to solve for $x = \frac{1}{g}f$. The authors in [2] show that it is not necessary to have the evaluations of $A(u)$ and $b(u)$ in order to solve (10). Rather it is enough, for each ξ_ℓ, to have a scalar matrix $\hat{A}^{[\ell]} \in \mathsf{K}^{m\times n}$ and right side vector $\hat{b}^{[\ell]} \in \mathsf{K}^m$ such that $\hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$. They also show that the solution can be computed even if some of the scalar matrices $\hat{A}^{[\ell]}$ and/or right side vectors $\hat{b}^{[\ell]}$ are erroneous. That is for some $0 \leq \lambda \leq L-1$,

$$\hat{A}^{[\lambda]}f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]}. \tag{13}$$

The solution is computed by:

1. Selecting $L \geq L_{\text{BK}} = d_f + d_g + R + 2E + 1$ distinct elements $\xi_\ell \in \mathsf{K}$ where

a. $R \geq \left|\{\ell \mid \text{rank}(A(\xi_\ell)) < n \text{ and } \hat{A}^{[\ell]} f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}, 0 \leq \ell \leq L-1\}\right|$, that is (4).
b. $E \geq \left|\{\lambda \mid \hat{A}^{[\lambda]} f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]}, 0 \leq \lambda \leq L-1\}\right|$, that is (3).

2. Solving the homogeneous linear system

$$\hat{A}^{[\ell]} \begin{bmatrix} \vdots \\ \Phi^{[i]}(\xi_\ell) \\ \vdots \end{bmatrix} - \Psi(\xi_\ell)\hat{b}^{[\ell]} = 0,\ 1 \leq i \leq m, 0 \leq \ell \leq L-1, \quad (14)$$

where for all $i, \deg(\Phi^{[i]}) \leq d_f + E$ and $\deg(\Psi) \leq d_g + E$. The system (14) is linear in the coefficients of $\Phi^{[i]}(u)$ and $\Psi(u)$. There are $n(d_f + E + 1) + d_g + E + 1$ unknown coefficients of $\Phi^{[i]}(u)$ and $\Psi(u)$ and mL_{BK} equations.

Theorem 2.2. [2] *We suppose that for $\leq E$ of the ξ_ℓ we have $\hat{A}^{[\ell]} f(\xi_\ell) \neq g(\xi_\ell)\hat{b}^{[\ell]}$ and for $\geq d_f + d_g + E + 1$ of the ξ_ℓ we have $\text{rank}(\hat{A}^{[\ell]}) = n$ and $\hat{A}^{[\ell]} f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$. Let $\Psi_{\min}$ be the denominator component of a solution of (14) with $\Psi_{\min} \neq 0$ and scaled to have leading coefficient 1 in u, and of minimal degree of all such solutions, and let $\Phi^{[i]}_{\min}$ be the corresponding numerator components of that solution. Furthermore, let $\Lambda(u) = \prod_{\mu \text{ subj. to } (13)}(u - \xi_{\lambda_\mu})$ be an error locator polynomial. Then for all i we have $\Phi^{[i]}_{\min} = \Lambda f^{[i]}$ and $\Psi_{\min} = \Lambda g$.*

Remark 2.1. We assume we have a black box that we can probe with ξ_ℓ's. For each ξ_ℓ the black box returns $\hat{A}^{[\ell]}$ and $\hat{b}^{[\ell]}$. The scalar matrix $\hat{A}^{[\ell]}$ and scalar right-side vector $\hat{b}^{[\ell]}$ may not be $A(\xi_\ell)$ nor $b(\xi_\ell)$ respectively, but we are guaranteed that fewer than E are subject to condition (13). By Theorem 2.2, we can find the solution $x = \frac{1}{g} f$ as well as an error locator polynomial $\Lambda(u)$ that has as its roots the ξ_λ's that satisfy inequation (13). □

In the black box model it is not possible to determine degree bounds for the solution a-priori. Thus it is possible that the degree bounds d_f and d_g are much larger than $\max_{1 \leq i \leq n} \deg(f^{[i]})$ and $\deg(g)$ respectively. We describe next an algorithm that either finds the solution or determines that we need more evaluations. This allows us to design Algorithm 2.2, that computes the solution with possibly fewer evaluations than is required by the L_{BK} bound.

Algorithm 2.1: Compute $\frac{1}{g} f$ and Λ or determine degree bounds are too small.

Input: $d_f \geq \deg(f), d_g \geq \deg(g), 0 \leq d_f^* \leq d_f, 0 \leq d_g^* \leq d_g$,
$R^* \geq \left|\{\ell \mid \hat{A}^{[\ell]} f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]} \text{ and } \text{rank}(\hat{A}^{[\ell]}) < n \text{ for } 0 \leq \ell \leq L^*_{\text{BK}} - 1\}\right|$,
$E^* \geq \left|\{\lambda \mid \hat{A}^{[\lambda]} f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]} \text{ for } 0 \leq \lambda \leq L^*_{\text{BK}} - 1\}\right|$,
with L^*_{BK} from Step 1 below,
a stream $(\hat{A}^{[\ell]}, \hat{b}^{[\ell]})$, $\ell = 0, 1, \ldots$ which is static on multiple calls and extensible in length on demand.
Output: $\frac{1}{g} f$ and Λ or "$\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$."

1: $L^*_{\text{BK}} \leftarrow \max\{d_f + d_g^*, d_g + d_f^*\} + R^* + 2E^* + 1$
2: Determine the null space of

$$\hat{A}^{[\ell]} \Phi^*(\xi_\ell) - \Psi^*(\xi_\ell)\hat{b}^{[\ell]} = 0, \quad \ell = 0, 1, \ldots, L^*_{\text{BK}} - 1, \quad (15)$$

where $\deg(\Phi^*) \leq d_f^* + E^*, \deg(\Psi^*) \leq d_g^* + E^*$
3: **if** only trivial solution **then**
return "$\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$"; **end if**
4: Compute a basis, B, for the null space.
5: Compute the column echelon form for B, CEF(B).
Retrieve the last column,

$$\text{CEF}(B)_{*,r} \leftarrow \begin{bmatrix} \overrightarrow{\Psi^*_{\min}} \\ \overrightarrow{\Phi^*[1]_{\min}} \\ \vdots \\ \overrightarrow{\Phi^*[m]_{\min}} \end{bmatrix}, \text{ which has } \Psi^*_{\min} \neq 0.$$

Here $\vec{\cdot}$ are coefficient vectors.
6: $\Lambda^* \leftarrow \text{GCD}(\Phi^*_{\min}, \Psi^*_{\min})$; $k^* \leftarrow \deg(\Lambda^*)$.
7: $(f^*, g^*) \leftarrow (\frac{1}{\Lambda^*}\Phi^*_{\min}, \Psi^*_{\min}/\Lambda^*)$.
8: **if** $\deg(f^*) > d_f^*$ or $\deg(g^*) > d_g^*$ or $k^* > E^*$ **then**
return "$\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$"; **end if**
9: **return** $f \leftarrow f^*, g \leftarrow g^*, \Lambda \leftarrow \Lambda^*$; **end if**

Observe that Algorithm 2.1 is similar to the algorithm implied by Theorem 2.2. The main difference is that it uses the $L^*_{\text{BK}} \leq L_{\text{BK}}$ count. Recall that Theorem 2.2 requires $\geq L_{\text{BK}}$ evaluations to find the solution. We use the results of Theorem 2.2 to prove the correctness of our algorithm. That is our algorithm either determines that we just computed an interpolant of the evaluation points or that we have indeed found the solution. Recall that we assume there exists a unique solution to equation (10).

In Step 2 we compute a solution similar to (14). The difference being that we use the starred bounds. Observe that if $\deg(f) \leq d_f^*$ and $\deg(g) \leq d_g^*$ and we were to substitute $d_f = d_f^*$, $d_g = d_g^*$ in L_{BK}, then with $L^*_{\text{BK}} \geq d_f^* + d_g^* + 2E^* + R^*$ by Theorem 2.2 we are guaranteed to find the solution $(\Lambda f, \Lambda g)$. So if B indicates there is only the trivial solution then it must be the case that $\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$.

In Step 5 we compute a non-zero polynomial Ψ^* of minimal degree ($\Psi^*_{\min} \neq 0$). We claim that the last column of CEF(B) contains $\Psi^*_{\min}$. The fact that the degree of $\Psi^*_{\min}$ is minimum is clear from the form of the CEF(B). To see why $\Psi^*_{\min} \neq 0$, assume that $\Psi^*_{\min} = 0$. Then for all ξ_ℓ, $\hat{A}^{[\ell]}\Phi^*_{\min}(\xi_\ell) = \Psi^*_{\min}(\xi_\ell)\hat{b}^{[\ell]} = 0^m$. On $\geq \max\{d_f + d_g^*, d_g + d_f^*\} + E^* + 1$ evaluations $\text{rank}(\hat{A}^{[\ell]}) = n$, that is $\Phi^*_{\min}(\xi_\ell) = 0$, which implies by $\deg(\Phi^*_{\min}) \leq d_f^* + E^*$ that $\Phi^*_{\min} = 0$. This cannot be since CEF(B) is a basis for the solution space of equation (15) and thus cannot contain the zero vector. Hence $\Psi^*_{\min} \neq 0$.

In Step 7 we define $\frac{1}{g^*} f^* = \frac{1}{\Psi^*_{\min}}\Phi^*_{\min}$. We think of $\frac{1}{g^*} f^*$ as our candidate solution. Next in Step 8 we check if the candidate solution agrees with our starred bounds. We know from Theorem 2.2 that if $d_f^* \geq \deg(f)$ and $d_g^* \geq \deg(g)$ the bounds for the minimal solutions must be satisfied, so if they fail at least one bound is wrong.

Finally, we claim that if Algorithm 2.1 returns at Step 9 then we have computed the solution $\frac{1}{g} f$. Of the L^*_{BK} points ξ_ℓ at Step 9 we discard $\leq R^*$ "good" rank drops and $\leq E^*$ erroneous points for the solution (f, g) and $\leq k^* = \deg(\Lambda^*) \leq E^*$ points ξ_ℓ that have $\Lambda^*(\xi_\ell) = 0$. The remaining $\geq \max\{d_f + d_g^*, d_g + d_f^*\} + 1$ distinct ξ_ℓ satisfy

1. $\text{rank}(\hat{A}^{[\ell]}) = n$,
2. $\hat{A}^{[\ell]} f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$,
3. $\hat{A}^{[\ell]} f^*(\xi_\ell) = g^*(\xi_\ell)\hat{b}^{[\ell]}$, because

$$\hat{A}^{[\ell]}\Phi^*_{\min}(\xi_\ell) = \hat{A}^{[\ell]}\Lambda^*(\xi_\ell) f^*(\xi_\ell) = \Psi^*_{\min}(\xi_\ell)\hat{b}^{[\ell]} = \Lambda^*(\xi_\ell) g^*(\xi_\ell)\hat{b}^{[\ell]},$$

and $\Lambda^*(\xi_\ell) \neq 0$.

From Items 2 and 3 we get $\hat{A}^{[\ell]}(g(\xi_\ell) f^*(\xi_\ell) - g^*(\xi_\ell) f(\xi_\ell)) = 0$ which by Item 1 yields $g(\xi_\ell) f^*(\xi_\ell) - g^*(\xi_\ell) f(\xi_\ell) = 0$, that for at

least $\max\{d_f+d_g^*, d_g+d_f^*\}+1$ distinct ξ_ℓ. The vector $(gf^*-g^*f)(u)$ has polynomials of degree $\le \max\{d_f+d_g^*, d_f^*+d_g\}$ and is therefore equal 0, which proves $\frac{1}{g^*}f^* = \frac{1}{g}f$.

We observe that $d_f^* \le d_f$ and $d_g^* \le d_g$ implies that $L_{\text{BK}}^* \le L_{\text{BK}}$. Now Algorithm 2.1 guarantees that with L_{BK}^* many evaluations we either compute the solution $\frac{1}{g}f$ or we determine that $\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$. Thus L_{BK}^* count can be used in an early termination strategy. We give the details in the following algorithm.

Algorithm 2.2: Early Termination Strategy.

Input: $d_f \ge \deg(f)$, $d_g \ge \deg(g)$,
$\rho_E < 1/2$, a rational number with denominator q_E,
// the error rate.
$\rho_R < 1-2\rho_E$, a rational number with denominator q_R,
// the rank drop rate, see Remark 2.2.
// $q_E = q_R = \infty$ is permissible but may require
// more evaluations.
Output: $\frac{1}{g}f$ and Λ.

1: $d_f^* \leftarrow 0$; $d_g^* \leftarrow 0$.
2: $D \leftarrow \max\{d_f+d_g^*, d_g+d_f^*\}+1$.
3: $E^* \leftarrow \lfloor \bar{E}^* \rfloor$; $R^* \leftarrow \lfloor \bar{R}^* \rfloor$ with

$$\bar{E}^* = \frac{1}{1-2\rho_E-\rho_R}\Big(\rho_E\big(D+1-\frac{1}{q_R}\big)+(1-\rho_R)\big(1-\frac{1}{q_E}\big)\Big). \tag{16}$$

$$\bar{R}^* = \frac{1}{1-2\rho_E-\rho_R}\Big(\rho_R\big(D+2-\frac{2}{q_E}\big)+(1-2\rho_E)\big(1-\frac{1}{q_R}\big)\Big). \tag{17}$$

4: **if** Algorithm 2.1$(d_f, d_g, d_f^*, d_g^*, E^*, R^*)$ returns at Step 9
then return $\frac{1}{g}f$; **end if**
5: **while(true)** $D \leftarrow D+1$.
// returns below for $D = \max\{d_f+\deg(g), d_g+\deg(f)\}+1$
6: Reassign E^*, R^* as in Step 3 using the updated D in (16,17).
7: **forall** (d_f^*, d_g^*) **with** $D = \max\{d_f+d_g^*, d_g+d_f^*\}+1$ **do**
8: **if** Algorithm 2.1$(d_f, d_g, d_f^*, d_g^*, E^*, R^*)$
returns at Step 9 **then return** (f, g, Λ); **end if**
end for end while

Remark 2.2. Algorithm 2.2 saves evaluations is two ways. The first way we save evaluations is by probabilistic computation of E^* and R^* based on the size of D rather than using fixed bounds. Like [5] we view evaluations as probing a black box, thus we can also relate the error rate of the black box to E^*. Also given the number of evaluation and a strategy for choosing the evaluation points one may have a rate at which the problem drops rank. Such a rate for the rank drop can then be related to R^*. If there is no such rate then R from the L_{BK} count can always be substituted for R^* without affecting Algorithm 2.2.

We make the following assumption on the input error rates:

Assumption 2.1. *Suppose that for $L \ge L_E^{\min}$ the number of erroneous evaluations, k_E, **always** satisfies $k_E \le \lceil \rho_E L \rceil$, and also for $L \ge L_R^{\min}$: $k_R \le \lceil \rho_R L \rceil$ evaluations give rise to valid but rank deficient systems.*

Here $L_E^{\min}$ and $L_R^{\min}$ are sufficiently large numbers of evaluations for which the assumptions on k_E and k_R are sensible. Let $L_{\min} = \max\{L_E^{\min}, L_R^{\min}\}$, then $L_{\min}$ is a minimum on the number of evaluations our algorithm can work with. Assumption 2.1 differs from the rate assumptions in [5, Remark 1.1] and [6, Remark 1.1, Lemma 3.1] in that there we suppose $k_E \le \lfloor \rho_E L \rfloor$, which implies no error for $L < 1/\rho_E$. Our assumption here allows 1 error. Note that for $\rho_R = 0$, $q_R = \infty$ and $\rho_E = 1/q_E$ we get $\bar{E}^* = D/(q_E-2) + q_E/(q_E-2)$ whereas in [5, 6] we have $\bar{E}^* = D/(q_E-2)$. In [6, Remark 1.1] the assumptions are probabilistically validated by adjusting the error rate upwards and bounding the probability of failure via Chernoff bounds.

We now show that Assumption 2.1 and the computation of E^* and R^* in (16, 17) guarantee the input specifications for Algorithm 2.1. We have

$$\begin{aligned}\bar{L}^* &= D + 2\big(\rho_E\bar{L}^* + 1 - \frac{1}{q_E}\big) + \rho_R\bar{L}^* + 1 - \frac{1}{q_R} \\ &= \frac{1}{1-2\rho_E-\rho_R}\big(D + 3 - \frac{2}{q_E} - \frac{1}{q_R}\big)\end{aligned}$$

and for $\bar{E}^*, \bar{R}^*$ in (16,17) we have

$$\bar{E}^* = \rho_E\bar{L}^* + 1 - \frac{1}{q_E},\ \bar{R}^* = \rho_R\bar{L}^* + 1 - \frac{1}{q_R},\ \bar{L}^* = D + 2\bar{E}^* + \bar{R}^*.$$

Therefore we have

$$\begin{aligned}k_E^* &\le \lceil \rho_E L_{\text{BK}}^* \rceil = \lceil \rho_E(D + 2E^* + R^*) \rceil \\ &\le \rho_E(D + 2E^* + R^*) + 1 - \frac{1}{q_E} \\ &\le \rho_E(D + 2\bar{E}^* + \bar{R}^*) + 1 - \frac{1}{q_E} \\ &= \rho_E\bar{L}^* + 1 - \frac{1}{q_E} = \bar{E}^*,\end{aligned}$$

which implies by the integrality of k_E^* that $k_E^* \le \lfloor \bar{E}^* \rfloor = E^*$, as is required by Algorithm 2.1. Similarly, one proves $k_R^* \le R^*$.

We discuss now the second way Algorithm 2.2 saves evaluations. The algorithm initializes d_f^* and d_g^* to zero. Thus $L_{\text{BK}}^* \le L_{\text{BK}}$. The fewest number of evaluations we can use in Algorithm 2.1 is $D + R^* + E^*$ where $D = \max\{d_f, d_g\}+1$. Note this is the first bound used by Algorithm 2.2. We assume that $D \ge L$, we can always adjust d_f and/or d_g so that $D \ge L$. If L_{BK}^* has too few evaluations to return the solution, D is incremented by 1 and R^* and E^* are adjusted if needed. The algorithm then tries all possible combinations of d_f^* and d_g^* such that $D = \max\{d_f+d_g^*, d_g+d_f^*\}+1$. Thus we find the solution while incrementing D as slowly as possible. □

3 CABAY EARLY TERMINATION

We now describe the count L_{CAB}^* that incorporates degree bounds for the system being solved. The count is based on work in [3] (see also [8]). In Theorem 3.1, given exact values for degree parameters, we give the criteria and proof for when $L_{\text{CAB}}^* < L_{\text{BK}}^*$.

Consider another count L_{CAB}^*,

$$L_{\text{CAB}}^* = \max\{d_A + d_f^*, d_b + d_g^*\} + R^* + 2E^* + 1,$$

where $d_A \ge \deg(A)$ and $d_b \ge \deg(b)$. See (8) for the definitions of $\deg(A)$ and $\deg(b)$. Similar to Algorithm 2.1 we present next an algorithm that uses the L_{CAB}^* bound and either determines one of the starred bounds is too small or returns the solution.

Algorithm 3.1: Cabay Early Termination

Input: $d_A \ge \deg(A)$, $d_b \ge \deg(b)$,
d_f^*, d_g^*, with $0 \le d_f^* \le \deg(f)$, $0 \le d_g^* \le \deg(g)$
// same as in Algorithm 2.1
$R^* \ge \big|\{\ell \mid \hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$
and $\operatorname{rank}(\hat{A}^{[\ell]}) < n$ for $0 \le \ell \le L_{\text{CAB}}^* - 1\}\big|$,
$E^* \ge \big|\{\lambda \mid \hat{A}^{[\lambda]}f(\xi_\lambda) \ne g(\xi_\lambda)\hat{b}^{[\lambda]}$ for $0 \le \lambda \le L_{\text{CAB}}^* - 1\}\big|$,
Output: $\frac{1}{g}f$ and Λ or "$\deg(f) > d_f^*$ and/or $\deg(g) > d_g^*$".

1: $L^*_{\text{CAB}} \leftarrow \max\{d_A + d^*_f, d_b + d^*_g\} + R^* + 2E^* + 1$.
2: Determine the null space of the system
$$\hat{A}^{[\ell]}\Phi^*(\xi_\ell) - \Psi^*(\xi_\ell)\hat{b}^{[\ell]} = 0,\ \ell = 0, 1, \ldots, L^*_{\text{CAB}} - 1, \quad (18)$$
where $\deg(\Phi^*) \le d^*_f + E^*, \deg(\Psi^*) \le d^*_g + E^*$.
3: **if** only the trivial solution **then**
4: **return** $\deg(f) > d^*_f$ and/or $\deg(g) > d^*_g$; **end if**
5: Compute a basis, B, for the null space
6: Compute the column echelon form for B, CEF(B). See Step 7 in Algorithm 2.1.
7: $\Lambda^* \leftarrow \text{GCD}(\Phi^*_{\min}, \Psi^*_{\min})$; $k^* \leftarrow \deg(\Lambda^*)$.
8: $(f^*, g^*) \leftarrow (\frac{1}{\Lambda^*}\Phi^*_{\min}, \Psi^*_{\min}/\Lambda^*)$.
9: **return** $f \leftarrow f^*$, $g \leftarrow g^*$, and $\Lambda \leftarrow \Lambda^*$.

In Step 2 we again compute a similar object to (14) using our new starred degree bounds . We now justify Steps 3 and 4. We prove that if the computation in Step 2 produces only the trivial solution then $\deg(f) > d^*_f$ and/or $\deg(g) > d^*_g$. Assume $\deg(f) \le d^*_f$ and $\deg(g) \le d^*_g$. Then $(\Phi^*, \Psi^*) = (\Lambda f, \Lambda g)$ solves (18). Thus equation (18) cannot only contain the trivial solution. This implies that if (18) has only the trivial solution then $\deg(f) > d^*_f$ and/or $\deg(g) > d^*_g$.

We now justify Step 9. We prove that $\frac{1}{g^*}f^*$ is the solution of our system. Furthermore, the $\text{GCD}(\Phi^*_{\min}, \Psi^*_{\min})$ is the error locator polynomial. If we are at Step 9 of our algorithm then we have that on at least $\max\{d_A + d^*_f, d^*_g + d_b\} + E^* + 1$ evaluations $\hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$ and $\text{rank}(\hat{A}^{[\ell]}) = n$. The latter implies that $g(\xi_\ell) \neq 0$, for otherwise $f(\xi_\ell) = 0$ and $\frac{1}{g}f$ would not be reduced. For those ℓ we have computed Φ^* and Ψ^* such that $\hat{A}^{[\ell]}\Phi^*(\xi_\ell) = \Psi^*(\xi_\ell)\hat{b}^{[\ell]}$.

We show first that $\hat{A}^{[\ell]}\Phi^*(\xi_\ell) = \Psi^*(\xi_\ell)\hat{b}^{[\ell]}$ implies $A(\xi_\ell) \times \Phi^*(\xi_\ell) = \Psi^*(\xi_\ell)b(\xi_\ell)$. If $\Psi(\xi_\ell) = 0$ then $\Phi(\xi_\ell) = 0$ because $\hat{A}^{[\ell]}$ has linearly independent columns. If on the other hand $\Psi(\xi_\ell) \neq 0$ we get $\Phi^*(\xi_\ell)/\Psi^*(\xi_\ell) = f(\xi_\ell)/g(\xi_\ell)$ since the solution is unique. Now $A(\xi_\ell)(f(\xi_\ell)/g(\xi_\ell)) = A(\xi_\ell)(\Phi^*(\xi_\ell)/\Psi^*(\xi_\ell)) = b(\xi_\ell)$. So the computed Φ^* and Ψ^* must satisfy $A(\xi_\ell)\Phi^*(\xi_\ell) = \Psi^*(\xi_\ell)b(\xi_\ell)$.

Since $A(u)\Phi^*(u) - \Psi^*(u)b(u)$ is a polynomial vector of degree $\le \max\{d_A + d^*_f, d_b + d^*_g\} + E^*$ it is uniquely determined by $\max\{d_A + d^*_f, d_b + d^*_g\} + E^* + 1$ distinct evaluation points so we have $A(u)\Phi^*(u) = \Psi^*(u)b(u)$. So $\frac{1}{g}f = \frac{1}{\Psi^*_{\min}}\Phi^*_{\min} = \frac{1}{g^*}f^*$. This implies there is a polynomial $\Lambda^*(u)$ with $\Lambda^* f = \Phi^*_{\min}$ and $\Lambda^* g = \Psi^*_{\min}$. For each λ we have $\hat{A}^{[\lambda]}f(\xi_\lambda) \neq g(\xi_\lambda)\hat{b}^{[\lambda]}$ and $\hat{A}^{[\lambda]}(\Lambda^* f)(\xi_\lambda) = \hat{A}^{[\lambda]}\Phi^*_{\min}(\xi_\lambda) = \Psi^*_{\min}(\xi_\lambda)\hat{b}^{[\lambda]} = (\Lambda^* g)(\xi_\lambda)\hat{b}^{[\lambda]}$ which implies $\Lambda^*(\xi_\lambda) = 0$. Thus $\Lambda = \Lambda^*$.

Remark 3.1. Any non-zero solution computed in Step 5 of the previous algorithm has the property $\frac{1}{g}f = \frac{1}{\Psi^*}\Phi^*$. Nevertheless, only the pair $(\Phi^*_{\min}, \Psi^*_{\min}) = (\Lambda f, \Lambda g)$. So if there is no need to compute the error locator polynomial then Step 6 is unnecessary.

Remark 3.2. If we implement Algorithm 2.2 replacing Algorithm 2.1 with Algorithm 3.1 then we then get an early termination strategy for Cabay Termination. □

Remark 3.3. The matrix $A(u)$ having full rank implies by Cramer's rule that we can set $d_f = (n-1)d_A + d_b$ and $d_g = nd_A$. So $L_{\text{CAB}} \ge nd_A + d_b + R + 2E + 1 = d_f + d_g/n + R + 2E + 1$ in comparison to Theorem 2.2, which has $L_{\text{BK}} \ge d_f + d_g + R + 2E + 1$. In Theorem 3.1 we generalize when L_{CAB} is better than L_{BK}. □

Theorem 3.1. *If all bounds are exact then $L_{\text{CAB}} < L_{\text{BK}}$ if and only if* $\deg(g) > \deg(A)$.

Proof. $Af = gb$ implies $\deg(Af) = \deg(gb) = \deg(g) + \deg(b)$. Since some terms can cancel due to the matrix vector multiplication, Af, we have $\deg(Af) \le \deg(A) + \deg(f)$. This implies that $\deg(g) + \deg(b) \le \deg(A) + \deg(f)$.
Assume $\deg(g) + \deg(b) < \deg(A) + \deg(f)$. Then $L_{\text{CAB}} = \deg(f) + \deg(A) + R + 2E + 1 < L_{\text{BK}} = \deg(f) + \deg(g) + R + 2E + 1$if and only if $\deg(g) > \deg(A)$.
Now assume $\deg(g) + \deg(b) = \deg(A) + \deg(f)$, then there are two cases.
Case 1: $L_{\text{CAB}} = \deg(f) + \deg(A) + R + 2E + 1$.
Case 2: $L_{\text{CAB}} = \deg(g) + \deg(b) + R + 2E + 1$.
We have already dealt with case 1. Consider case 2, $L_{\text{CAB}} = \deg(g) + \deg(b) + R + 2E + 1 < L_{\text{BK}} = \deg(f) + \deg(g) + R + 2E + 1$ if and only if $\deg(b) < \deg(f)$. This implies $\deg(g) > \deg(A)$ since we assumed that $\deg(g) + \deg(b) = \deg(A) + \deg(f)$. □

Remark 3.4. If $n = m = 1$ then the Cramer rule bound in Remark 3.3 yields, in the exact case, $L_{\text{CAB}} = L_{\text{BK}}$. In fact the linear system $A(u)x = b(u)$ is actually of the form $a(u)x = b(u)$ where $a(u), b(u) \in K[u]$. This implies $x = b(u)/a(u) = f/g$ which implies $a(u) = h(u)g(u)$ and $b(u) = h(u)f(u)$, where $h(u) \in K[u]$. Thus if we use the exact degrees for our bounds we get $L_{\text{BK}} \le L_{\text{CAB}}$, since in this case $\deg(g) \le \deg(A)$. Furthermore, if one uses fewer than $L = \deg(f) + \deg(g) + 2k + 1$ evaluations then one loses the guarantee of a unique solution. In Lemma 3.2 below, given only $L = \deg(f) + \deg(g) + 2k$ we construct a second solution. □

Lemma 3.2. *Let $n = m = 1$ and K a field. For all $f, g \in \mathsf{K}[u]$ with $\deg(g) \ge 1$ and $\text{GCD}(f, g) = 1$ and for all $\xi_0, \ldots, \xi_{L-1}$ with $L = \deg(f) + \deg(g) + 2k$, $\xi_\ell \neq 0, \xi_{\ell_1} \neq \xi_{\ell_2}$ for $\ell_1 \neq \ell_2, 0 \le \ell, \ell_1, \ell_2 \le L - 1$ and $g(\xi_\ell) \neq 0$ for all ℓ with $0 \le \ell \le \deg(f) + \deg(g) - 1$ and for all $k \ge 0$ we have: if $|\mathsf{K}| \ge 2(\deg(f) + \deg(g) + k) + 1$ then there exist $\bar{f}, \bar{g} \in \mathsf{K}[u]$ and there exist $\hat{a}^{[\ell]}, \hat{b}^{[\ell]} \in \mathsf{K}$ for all ℓ with $0 \le \ell \le L - 1$ such that*

1. *$f/g \neq \bar{f}/\bar{g}$, $\text{GCD}(\bar{f}, \bar{g}) = 1$, $\deg(f) = \deg(\bar{f})$ and $\deg(g) = \deg(\bar{g})$.*
2. *$\bar{g}(\xi_\ell) \neq 0$ for all ℓ with $0 \le \ell \le \deg(f) + \deg(g) - 1$.*
3. *$\hat{a}^{[\ell]} \neq 0$ for all ℓ with $0 \le \ell \le \deg(f) + \deg(g) - 1$,*
4. *$\hat{a}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$ for all ℓ with $0 \le \ell \le \deg(f) + \deg(g) + k - 1$,*
$\hat{a}^{[\ell]}\bar{f}(\xi_\ell) = \bar{g}(\xi_\ell)\hat{b}^{[\ell]}$ for all ℓ with $0 \le \ell \le \deg(f) + \deg(g) - 1$ or $\deg(f) + \deg(g) + k \le \ell \le L - 1$.
5. *$\hat{a}^{[\ell_1]}f(\xi_{\ell_1}) \neq g(\xi_{\ell_1})\hat{b}^{[\ell_1]}$ for all ℓ_1 with $\deg(f) + \deg(g) + k \le \ell_1 \le L - 1$ and*
$\hat{a}^{[\ell_2]}\bar{f}(\xi_{\ell_2}) \neq \bar{g}(\xi_{\ell_2})\hat{b}^{[\ell_2]}$ for all ℓ_2 with $\deg(f) + \deg(g) \le \ell_2 \le \deg(f) + \deg(g) + k - 1$.

Proof. Recall the system we solve is given by equation (14) and we solve $\hat{a}^{[\ell]}\Phi(\xi_\ell) = \Psi(\xi_\ell)\hat{b}^{[\ell]}$. Let
$$\Phi(u) = y_d u^d + y_{d-1}u^{d-1} + \ldots + y_0 \text{ and}$$
$$\Psi(u) = u^e + z_{e-1}u^{e-1} + \ldots + z_0,$$
where $d = \deg(f) + k$ and $e = \deg(g) + k$. For all ℓ such that $0 \le \ell \le \deg(f) + \deg(g) - 1$ let $\hat{a}^{[\ell]} = g(\xi_\ell)$ and $\hat{b}^{[\ell]} = f(\xi_\ell)$. Assume first $k = 0$, i.e., there are no errors. We set up and solve the non-homogeneous linear system
$$\hat{a}^{[\ell]}\Phi(\xi_\ell) - \Psi^*(\xi_\ell)\hat{b}^{[\ell]} = \hat{b}^{[\ell]}\xi^e_\ell, \quad (19)$$
where $\Psi^* = z_{e-1}u^{e-1} + z_{e-2}u^{e-2} + \ldots + z_0$.
Let $B\begin{bmatrix} y \\ z^* \end{bmatrix} = v$ be the matrix representation of our system in (19).
We have for the right side vector v that $v \neq 0$ since $\hat{b}^{[\ell]} = f(\xi_\ell)$

cannot be zero for all $0 \le \ell \le \deg(f)+\deg(g)-1$ since $\deg(g) \ge 1$ and $\xi_\ell \ne 0$ for all $0 \le \ell \le L-1$. Our system then has L equations and $L+1$ unknowns, so $B \in \mathsf{K}^{L\times(L+1)}$. By construction $\begin{bmatrix} f \\ g^* \end{bmatrix}$ is a solution to our system. Since our system is underdetermined there must be other solutions

$$\begin{bmatrix} \bar{f}_c \\ \bar{g}_c^* \end{bmatrix} = \begin{bmatrix} f \\ g^* \end{bmatrix} + cw$$

where $w \ne 0$ is in the null space of B and $c \ne 0$. Let $p = \mathrm{res}_u(f + cw_f, g + cw_{g^*}), p$ is a polynomial in $c, p \ne 0$ since $p(0) \ne 0$. Note $\deg(p) \le \deg(f)+\deg(g)$ and $|\mathsf{K}| \ge 2(\deg(f)+\deg(g)+k)+1$. Thus there must be $c_1 \in \mathsf{K}$ such that $c_1 \ne 0, p(c_1) \ne 0$ and $\mathrm{lc}(f) \ne -\mathrm{lc}(c_1 w_f)$. Consider $\bar{f} = \bar{f}_{c_1}$ and $\bar{g} = \bar{g}_{c_1}$. Then by construction $\deg(f) = \deg(\bar{f})$ and $\deg(g) = \deg(\bar{g})$. Also since $p(c_1) \ne 0$ we have that $\mathrm{GCD}(\bar{f}, \bar{g}) = 1$.

Next we show that $f/g \ne \bar{f}/\bar{g}$. We show first that $\begin{bmatrix} f \\ g^* \end{bmatrix}$ and $\begin{bmatrix} \bar{f} \\ \bar{g}^* \end{bmatrix}$ are linearly independent. Assume $\begin{bmatrix} f \\ g^* \end{bmatrix}$ and $\begin{bmatrix} \bar{f} \\ \bar{g}^* \end{bmatrix}$ are linearly dependent, then there exits $\alpha \ne 0$ such that $\alpha \begin{bmatrix} f \\ g^* \end{bmatrix} = \begin{bmatrix} \bar{f} \\ \bar{g}^* \end{bmatrix}$, which implies $\alpha \begin{bmatrix} f \\ g^* \end{bmatrix} = \begin{bmatrix} f \\ g^* \end{bmatrix} + c_1 w$, which further implies $(\alpha-1)\begin{bmatrix} f \\ g^* \end{bmatrix} = c_1 w, \alpha \ne 1$ since $c_1 \ne 0$ and $w \ne 0$. So $\frac{\alpha-1}{c_1}\begin{bmatrix} f \\ g^* \end{bmatrix} = w$, but $0 \ne \frac{\alpha-1}{c_1} v = \frac{\alpha-1}{c_1} B\begin{bmatrix} f \\ g^* \end{bmatrix} = Bw = 0$, which is a contradiction. Thus $\begin{bmatrix} f \\ g^* \end{bmatrix}$ and $\begin{bmatrix} \bar{f} \\ \bar{g}^* \end{bmatrix}$ are linearly independent, which implies that $\begin{bmatrix} f \\ g \end{bmatrix}, \begin{bmatrix} \bar{f} \\ \bar{g} \end{bmatrix}$ are linearly independent. Which further implies that $f/g \ne \bar{f}/\bar{g}$.

To see why $\bar{g}(\xi_\ell) \ne 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$, assume $\bar{g}(\xi_\ell) = 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$. Since $\mathrm{GCD}(\bar{f}, \bar{g}) = 1$ and $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) = \bar{g}(\xi_\ell)\hat{b}^{[\ell]}$ then $\bar{g}(\xi_\ell) = 0$ implies that $\hat{a}^{[\ell]} = 0$. This is a contradiction since $\hat{a}^{[\ell]} = g(\xi_\ell) \ne 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$. Thus $\bar{g}(\xi_\ell) \ne 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$.

Now assume $k > 0$. By construction for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$ we have $\hat{a}^{[\ell]}f(\xi_\ell) - g(\xi_\ell)\hat{b}^{[\ell]} = 0$ and $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) - \bar{g}(\xi_\ell)\hat{b}^{[\ell]} = 0$. Thus $\hat{a}^{[\ell]}(\bar{g}(\xi_\ell)f(\xi_\ell) - g(\xi_\ell)\bar{f}(\xi_\ell)) = 0$. Since $\hat{a}^{[\ell]} \ne 0$ it must be that $\bar{g}(\xi_\ell)f(\xi_\ell) - g(\xi_\ell)\bar{f}(\xi_\ell) = 0$. Since $f/g \ne \bar{f}/\bar{g}$, and $\mathrm{GCD}(f,g) = \mathrm{GCD}(\bar{f}, \bar{g}) = 1$ then $\bar{g}f - g\bar{f} \in \mathsf{K}[u]$ is not identically zero. Since $\deg(f) = \deg(\bar{f})$ and $\deg(g) = \deg(\bar{g})$ and $(\bar{g}f - g\bar{f})(\xi_\ell) = 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$ we must have that $\deg(\bar{g}f - g\bar{f}) = \deg(f)+\deg(g)$. Observe that ξ_ℓ for $0 \le \ell \le \deg(f)+\deg(g)-1$ are $\deg(f)+\deg(g)$ distinct roots of $(\bar{g}f - g\bar{f})(u)$, so $(\bar{g}f - g\bar{f})(u)$ can have no other roots. Let $\hat{a}^{[\ell]} = g(\xi_\ell)$ and $\hat{b}^{[\ell]} = f(\xi_\ell)$ for all ℓ with $\deg(f)+\deg(g) \le \ell \le \deg(f)+\deg(g)+k-1$. Then for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)+k-1$ we have $\hat{a}^{[\ell]} = g(\xi_\ell)$ and $\hat{b}^{[\ell]} = f(\xi_\ell)$ and therefore $\hat{a}^{[\ell]}f(\xi_\ell) - g(\xi_\ell)\hat{b}^{[\ell]} = 0$. By construction $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) - \bar{g}(\xi_\ell)\hat{b}^{[\ell]} = 0$ for all ℓ with $0 \le \ell \le \deg(f)+\deg(g)-1$. Let $\hat{a}^{[\ell]} = \bar{g}(\xi_\ell)$ and $\hat{b}^{[\ell]} = \bar{f}(\xi_\ell)$ for all ℓ with $\deg(f)+\deg(g)+k \le \ell \le L-1$ then have we have $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) - \bar{g}(\xi_\ell)\hat{b}^{[\ell]} = 0$ for all ℓ with $\deg(f)+\deg(g)+k \le \ell \le L-1$.

Assume there exist ξ_ℓ for some ℓ with $\deg(f)+\deg(g) \le \ell \le \deg(f)+\deg(g)+k-1$ such that $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) - \bar{g}(\xi_\ell)\hat{b}^{[\ell]} = 0$. Then $(\bar{g}f - g\bar{f})(\xi_\ell) = 0$ for that ξ_ℓ. Which is a contradiction since we have already shown that if ξ_ℓ is a root of $(\bar{g}f - g\bar{f})(u)$ then $\ell < \deg(f)+\deg(g)$. Thus for all ℓ with $\deg(f)+\deg(g) \le \ell \le \deg(f)+\deg(g)+k-1$ we must have $\hat{a}^{[\ell]}\bar{f}(\xi_\ell) \ne \bar{g}(\xi_\ell)\hat{b}^{[\ell]}$. A similar argument shows that for all ℓ with $\deg(f)+\deg(g)+k \le \ell \le L-1$ we have $\hat{a}^{[\ell]}f(\xi_\ell) \ne g(\xi_\ell)\hat{b}^{[\ell]}$. Thus $\hat{a}^{[\ell_1]}f(\xi_{\ell_1}) \ne g(\xi_{\ell_1})\hat{b}^{[\ell_1]}$ for all ℓ_1 with $\deg(f)+\deg(g)+k \le \ell_1 \le L-1$ and $\hat{a}^{[\ell_2]}\bar{f}(\xi_{\ell_2}) \ne \bar{g}(\xi_{\ell_2})\hat{b}^{[\ell_2]}$ for all ℓ_2 with $\deg(f)+\deg(g) \le \ell_2 \le \deg(f)+\deg(g)+k-1$. □

We now show that if the solution $\frac{1}{g}f$ is such that $f^{[i_1]} = f^{[i_2]} \ne 0$ for all $1 \le i_1 < i_2 \le n$ then $\deg(g) \le \deg(A)$. Thus, by Theorem 3.1, if our parameters are exact we have that $L_{\mathrm{BK}} \le L_{\mathrm{CAB}}$.

Lemma 3.3. *If A is full rank, and the vector f has the property that $f^{[i_1]} = f^{[i_2]} \ne 0$ for all $1 \le i_1 < i_2 \le n$, and $Af = gb$ then $b \ne 0^m$.*

Proof. A full rank implies $\mathrm{rank}(A(u)) = n$. Assume $b = 0^m$, this implies $f^{[1]}\sum_{j=1}^{n} a_{i,j} = 0, i = 1, \ldots, m$. Since $f \ne 0$ this is equivalent to $\sum_{j=1}^{n} A_j = 0$, which implies the columns of A are linearly dependent. Thus A is not full rank, which is a contradiction. □

Corollary 3.4. *If A is full rank and $f^{[i_1]} = f^{[i_2]} \ne 0$ for all $1 \le i_1 < i_2 \le n$ then $\deg(g) \le \deg(A)$, thus by Theorem 3.1 in the exact case $L_{\mathrm{BK}} \le L_{\mathrm{CAB}}$.*

Proof. Let A full rank and $A(\frac{1}{g}f) = b, g \ne 0$. This implies $Af = gb$, which further implies $f^{[1]}\sum_j a_{i,j} = gb_i$ for all i. We know by Lemma 3.3 that $b_i \ne 0$ for all i. Recall that if $\frac{1}{g}f$ is the solution to $Ax = b$ then $\mathrm{GCD}(f,g) = 1$. Thus $f^{[1]}\sum_j a_{i,j} = gb_i$ implies g divides $\sum_j a_{i,j}$ for all i. For those i such that $b_i \ne 0$, $\deg(g) \le \deg\left(\sum a_{i,j}\right) \le \max_{1\le i\le m, 1\le j\le n} \deg(a_{i,j}) = \deg(A)$. Thus $\deg(g) \le \deg(A)$. □

We now have two counts that we can use to solve the problem we describe in Remark 2.1. Theorem 3.1 tells us that whenever $\deg(g) > \deg(A)$ then the L_{CAB} count uses fewer evaluations than the L_{BK} count if all parameter values are exact. Lemma 3.2 shows however, that if $n = m = 1$ we cannot do better than the L_{BK} count. Lemma 3.3 and Corollary 3.4 tell us that if the solution $\frac{1}{g}f$ is such that $f^{[i_1]} = f^{[i_2]}$ for all $1 \le i_1 < i_2 \le n$ then it must be the case that the $\deg(A) > \deg(g)$. In the following section we combine the two counts to get a general early termination strategy. Such a termination strategy would be useful when little is known about the degree of the system and/or solution, since in such cases it is likely that the bounds one chooses are much larger than the actual value of the parameters.

4 COMBINED EARLY TERMINATION

We now describe an algorithm that combines the early termination strategy for the L_{BK} count with early termination strategy for the L_{CAB} count. This strategy can be implemented when we are unsure how the $\deg(g)$ compares to the $\deg(A)$ and we suspect that our degree bounds significantly overestimates the actual values of their respective parameters.

Algorithm 4.1: Early Termination with L^*_{BK} and L^*_{CAB}

Input: $d_f \ge \deg(f), d_g \ge \deg(g), d_A \ge \deg(A), d_b \ge \deg(b)$
$\rho_E < 1/2$, a rational number with denominator q_E,
// the error rate
$\rho_R < 1 - 2\rho_E$, a rational number with denominator q_R,
// the rank drop rate, see Remark 2.2.

Output: f, g, and Λ.

1: $d_f^* \leftarrow 0; d_g^* \leftarrow 0$.
2: $D \leftarrow \min\left\{\max\{d_f + d_g^*, d_g + d_f^*\}, \max\{d_A + d_f^*, d_b + d_g^*\}\right\} + 1$.
3: $E^* \leftarrow \lfloor \bar{E}^* \rfloor; R^* \leftarrow \lfloor \bar{R}^* \rfloor$ where $\bar{E}^*$ and $\bar{R}^*$ are as defined in equations (16) and (17) respectively.
4: **if** $\max\{d_f + d_g^*, d_g + d_f^*\} \le \max\{d_A + d_f^*, d_b + d_g^*\}$ **then**
5: **if** Algorithm 2.1$(d_f, d_g, d_f^*, d_g^*, E^*, R^*)$ returns at Step 9 **then return** (f, g, Λ); **end if**
else
6: **if** Algorithm 3.1$(d_A, d_b, d_f^*, d_g^*, E^*, R^*)$ returns at Step 9 **then return** (f, g, Λ); **end if**
end if
7: **while(true)** $D \leftarrow D + 1$.
8: Reassign E^*, R^* as in Step 3 using the updated D in equations (16) and (17) respectively.
9: **forall** (d_f^*, d_g^*) **with** $D = \min\left\{\max\{d_f + d_g^*, d_g + d_f^*\}, \max\{d_A + d_f^*, d_b + d_g^*\}\right\} + 1$ **do**
10: **if** $D = \max\{d_f + d_g^*, d_g + d_f^*\}$ **then**
11: **if** Algorithm 2.1$(d_f, d_g, d_f^*, d_g^*, E^*, R^*)$ returns at Step 9 **then return** (f, g, Λ); **end if**
else
12: **if** Algorithm 3.1$(d_A, d_b, d_f^*, d_g^*, E^*, R^*)$ returns at Step 9 **then return** (f, g, Λ); **end if**
end if; **end for**; **end while**

Remark 4.1. The justification for Algorithm 4.1 follows from the justification for Algorithm 2.2. If values for d_A and d_b are not known they can be set to infinity and Algorithm 4.1 becomes Algorithm 2.2. Similarly if values for d_f and d_g are not known they can be set to infinity and Algorithm 4.1 is the Cabay early termination algorithm.

5 RATIONAL VECTOR RECOVERY

Suppose that there is a vector of rational functions $\frac{1}{g}f$ we wish to recover, and assume that this vector of rational functions is the unique solution to a system of linear equations

$$A(u)\,x = b(u), \quad A(u) \in \mathsf{K}[u]^{m\times n}, b(u) \in \mathsf{K}[u]^m,$$

where K is a field. See (10).
Let

$$\gamma_i^{[\ell]} = \begin{cases} f^{[i]}(\xi_\ell)/g(\xi_\ell) & \text{if } g(\xi_\ell) \neq 0 \\ \infty & \text{if } g(\xi_\ell) = 0. \end{cases}$$

We further assume that we have a black box that takes $\xi_\ell \in \mathsf{K}$ as inputs and returns vectors $\beta_i^{[\ell]}$ such that $\beta_i^{[\ell]} = \gamma_i^{[\ell]}$ for $\ell \notin \{\lambda_1, \ldots, \lambda_k\}$ and all $1 \le i \le n$ and $\beta_i^{[\ell]} \neq \gamma_i^{[\ell]}$ for $\ell \in \{\lambda_1, \ldots, \lambda_k\}$ on at least one i, $1 \le i \le n$. The remaining $m - n$ entries of the vector is filled with zeros. We show that using the model in [2] as defined in Section 2, one can recover the rational vector $\frac{1}{g}f$. Recall that in the model $\hat{A}^{[\ell]}$ and $\hat{b}^{[\ell]}$ do not necessarily equal $A(\xi_\ell)$ or $b(\xi_\ell)$ respectively. We only need on sufficiently many evaluations to have $\hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$, and $\operatorname{rank}(\hat{A}^{[\ell]}) = n$.
Thus if we let

$$\hat{A}^{[\ell]} = \begin{bmatrix} I_n \\ 0 \ldots 0 \\ \vdots \ddots \vdots \\ 0 \ldots 0 \end{bmatrix} \quad \text{and} \quad \hat{b}^{[\ell]} = \begin{bmatrix} \beta_1^{[\ell]} \\ \vdots \\ \beta_n^{[\ell]} \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{20}$$

for all ξ_ℓ such that $g(\xi_\ell) \neq 0$, and

$$\hat{A}^{[\ell]} = 0^{m\times n} \quad \text{and} \quad \hat{b}^{[\ell]} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{21}$$

whenever $g(\xi_\ell) = 0$ we can recover the vector of rational functions. We shall call the ξ_ℓ's such that $g(\xi_\ell) = 0$ the poles of the rational function. If none of our black box evaluations indicate that we have evaluated at a pole then $\hat{A}^{[\ell]}$ is always full rank. We know that we can recover the rational vector with $L = d_f + d_g + 2E + R + 1$ and $L = \max\{d_f + d_A, d_g + d_b\} + 2E + R + 1$ evaluations respectively. Note $R = 0$ since $\operatorname{rank}(\hat{A}^{[\ell]}) = n$ for all $0 \le \ell \le L - 1$. Now there must be a matrix $A(u)$ of minimal degree for which the vector $\frac{1}{g}f$ is the solution of the system $A(u)x = b(u)$. We have proved in Theorem 3.1 that in the cases where the $\deg(g) > \deg(A)$, $L = \max\{\deg(f) + \deg(A), \deg(g) + \deg(b)\} + 2k + 1 < L = \deg(f) + \deg(g) + 2k + 1$ so we can achieve Cabay early termination.

Suppose that on some evaluations of ξ_ℓ's the black box indicates, by the value ∞, that we have encountered a pole. We show that the count $L = d_f + d_g + 2E + 1$ evaluations suffices to recover the rational function vector. Ideally, we would like to say that this follows directly from Theorem 2.2, however we cannot guarantee that we have $\operatorname{rank}(\hat{A}^{[\ell]}) = n$ on $\ge d_f + d_g + E + 1$ many points for which $\hat{A}^{[\ell]}f(\xi_\ell) = g(\xi_\ell)\hat{b}^{[\ell]}$, one of the assumptions of Theorem 2.2. This full rank assumption is used in the proof of Theorem 2.2 only to establish that the vector of field elements $\Psi(\xi_\ell)f(\xi_\ell) - g(\xi_\ell)\Phi(\xi_\ell) = 0$. Thus if we can establish that the vector of field elements $\Psi(\xi_\ell)f(\xi_\ell) - g(\xi_\ell)\Phi(\xi_\ell) = 0$ without using the fact that the $\operatorname{rank}(\hat{A}^{[\ell]}) = n$ on $\ge d_f + d_g + E + 1$ many points we would establish our claim as all other assumptions of Theorem 2.2 remain the same.

Proof. There are two possibilities on non-erroneous evaluations of ξ_ℓ, that is $\ell \notin \{\lambda_1, \ldots, \lambda_k\}$:

1. $g(\xi_\ell) = 0$ which implies $\Psi(\xi_\ell) = 0$. See (21).
2. $g(\xi_\ell) \neq 0$ which implies $\Phi(\xi_\ell) = \Psi(\xi_\ell)\frac{1}{g(\xi_\ell)}f(\xi_\ell)$.

Recall that we solve equation (14). Note that in both cases we indeed have the vector of field elements $\Psi(\xi_\ell)f(\xi_\ell) - g(\xi_\ell)\Phi(\xi_\ell) = 0$. Thus our claim is established. □

Remark 5.1. The system formed by using $\hat{A}^{[\ell]}$ and $\hat{b}^{[\ell]}$ as described in (20) and (21) above is overdetermined. We show in Lemma 3.2 that without additional information about the errors we can always construct a second solution that has the same characteristics as the actual solution. Nevertheless, given appropriate assumptions about the error locations one can reduce the number of necessary equations. For instance, in decoding interleaved Reed-Solomon codes it is assumed that the errors occur in bursts, that is errors occur in blocks [1, 11]. In a forthcoming paper we will give the analysis for a semi-deterministic scenario, that is where the actual errors do not need to be random field elements. Note that Theorem 3.1 describes a second scenario where the number of evaluations is less for interleaved codes, namely when the vector

encodes a rational function that is the solution to a parametric linear system (see also [10]). □

5.1 Cabay Early Termination with poles

Suppose $\deg(g) > \deg(A)$ and that on evaluation at some ξ_ℓ's, $\ell \notin \{\lambda_1, \ldots, \lambda_k\}$, the black box indicates that $g(\xi_\ell)$ is a pole. There are examples where $L_{\mathrm{CAB}} = \max\{d_f + d_A, d_g + d_b\} + 2E + 1$ evaluations are not sufficient to recover the rational function vector using our current model for rational vector recovery. To prove that L_{CAB} was sufficient to recover the rational function vector $\frac{1}{g}f$ we needed the $\mathrm{rank}(\hat{A}^{[\ell]}) = n$ for all ξ_ℓ, $\ell \notin \{\lambda_1, \ldots, \lambda_k\}$. We needed this to establish that $A(\xi_\ell)\Phi(\xi_\ell) = \Psi(\xi_\ell)b(\xi_\ell)$ and the pair $(\Lambda f, \Lambda g)$ is a solution to our linear system, where $\Lambda(u)$ is the error locator polynomial. However in our rational vector recovery model we set $\hat{A}^{[\ell]} = 0$ whenever $g(\xi_\ell) = 0$ for all ℓ, see (21). Note that in the current rational vector recovery model when $g(\xi_\ell) = 0$ we set $\Psi(\xi_\ell) = 0$ and lose all information about $\Phi(\xi_\ell)$, see (21). Consequently we may not be able to recover $\frac{1}{g}f$ as we may not have enough information about f. To remedy the lack of information we adjust our black box output to gain some information about f at poles. Let

$$\gamma_i^{[\ell]} = \begin{cases} \frac{1}{g(\xi_\ell)} f(\xi_\ell) & \text{if } g(\xi_\ell) \neq 0 \\ \left.\begin{array}{l} w^{[1]}, \ldots, w^{[r_\ell]}, \text{ a basis for the} \\ \text{null space of } A(\xi_\ell), \\ \textbf{\textit{or}} \\ c_\ell f(\xi_\ell), \text{ a non-zero scalar multiple} \\ \text{of the evaluated numerator vector,} \\ \text{both with an indication that } g(\xi_\ell) = 0 \end{array}\right\} & \text{if } g(\xi_\ell) = 0 \end{cases}$$

be what the black box returns. We show that if at the poles we add the equations $\Phi(\xi_\ell) = \Theta_{\ell,1} w^{[1]} + \ldots + \Theta_{\ell,r_\ell} w^{[r_\ell]}$, or $\Phi(\xi_\ell) = \Theta_\ell c_\ell f(\xi_\ell), c_\ell \neq 0$, to the set of equations produced by the original rational vector recovery model then we can recover $\frac{1}{g}f$ with $L_{\mathrm{CAB}} = \max\{d_f + d_A, d_g + d_b\} + 2E + 1$ evaluations, where $\Theta_j \in \mathsf{K}$ for all j are new unknowns.

Theorem 5.1. *Suppose that for* $\geq \max\{d_f + d_A, d_g + d_b\} + E + 1$, ξ_ℓ *we have* $\beta_i^{[\ell]} = \gamma_i^{[\ell]}$ *for all* i. *If we add*

$$\Psi(\xi_\ell) = 0 \quad \textit{and} \tag{22}$$

$$\Phi(\xi_\ell) = \Theta_{\ell,1} w^{[1]} + \ldots + \Theta_{\ell,r_\ell} w^{[r_\ell]} \textit{ or} \tag{23}$$

$$\Phi(\xi_\ell) = \Theta_\ell c_\ell f(\xi_\ell), c_\ell \neq 0. \tag{24}$$

to the system we solve, whenever $\gamma_i^{[\ell]} = \infty$ *for all* i, $1 \leq i \leq m$, *and if* $\Phi \in \mathsf{K}[u]^n, \Psi \in \mathsf{K}[u]$, *and* $\Theta_{\ell,1}, \ldots, \Theta_{\ell,r_\ell} \in \mathsf{K}$, *or* $\Theta_\ell \in \mathsf{K}$ *is a solution of the system, then for the pair* (Φ, Ψ) *that we compute we have* $A(\xi_\ell)\Phi(\xi_\ell) = \Psi(\xi_\ell)b(\xi_\ell)$, *and* $(\Lambda f, \Lambda g)$ *solve* (22), *and* (23) *or* (24).

Proof. Note that the black box can return $w^{[1]}, \ldots, w^{[r_\ell]}$ for some poles and $c_\ell f(\xi_\ell), c_\ell \neq 0$ for others. If $g(\xi_\ell) = 0$ then we add two sets of equations, (22), and (23) or (24). Clearly $\Psi(\xi_\ell)b(\xi_\ell) = 0^m$, and for (23) we have

$$\begin{aligned} A(\xi_\ell)\Phi(\xi_\ell) &= A(\xi_\ell)(\Theta_{\ell,1} w^{[1]} + \ldots + \Theta_{\ell,r_\ell} w^{[r_\ell]}) \\ &= \Theta_{\ell,1} A(\xi_\ell) w^{[1]} + \ldots + \Theta_{\ell,r_\ell} A(\xi_\ell) w^{[r_\ell]} = 0^m, \end{aligned}$$

or for (24) we have

$$\begin{aligned} A(\xi_\ell)\Phi(\xi_\ell) &= A(\xi_\ell)(\Theta_\ell c_\ell f(\xi_\ell)) \\ &= \Theta_\ell c_\ell A(\xi_\ell) f(\xi_\ell) = g(\xi_\ell) b(\xi_\ell) = 0^m. \end{aligned}$$

Thus we indeed have $A(\xi_\ell)\Phi(\xi_\ell) = \Psi(\xi_\ell)b(\xi_\ell)$ whenever $g(\xi_\ell) = 0$. Consider $\Lambda(\xi_\ell)A(\xi_\ell)f(\xi_\ell) = \Lambda(\xi_\ell)g(\xi_\ell)b(\xi_\ell) = 0^m$. We always have $A(\xi_\ell)f(\xi_\ell) = g(\xi_\ell)b(\xi_\ell) = 0^m$ when $g(\xi_\ell) = 0$. This implies that $f(\xi_\ell)$ must be in the null space of $A(\xi_\ell)$. Thus $f(\xi_\ell) = \sum_j d_{\ell,j} w^{[j]}, d_{\ell,j} \in \mathsf{K}$. So if at a pole we add equation (23), then $\Lambda(\xi_\ell)f(\xi_\ell) = \Lambda(\xi_\ell)\sum_j d_{\ell,j} w^{[j]}$, so $\Theta_{\ell,j} = \Lambda(\xi_\ell) d_{\ell,j}$ implies that $\Lambda(\xi_\ell)f(\xi_\ell)$ solves (23). If we add (24) at a pole, observe that $\Lambda(\xi_\ell)f(\xi_\ell) = \Theta_\ell c_\ell f(\xi_\ell)$ implies $\Theta_\ell = \Lambda(\xi_\ell)/c_\ell$. So $\Lambda(\xi_\ell)f(\xi_\ell)$ solves (24). Clearly $\Lambda(\xi_\ell)g(\xi_\ell)$ is a solution to (22). □

ACKNOWLEDGMENTS

This research was supported in part by the National Science Foundation under Grant CCF-1421128 (Kaltofen and Waddell) and by the Natural Sciences and Engineering Research Council of Canada Grant RGPIN 50503-10412 (Storjohann).

Note added February 21, 2020: Added in Lemma 3.2 the Item 3, which excludes the trivial values $(\hat{a}^{[\ell]}, \hat{b}^{[\ell]}) = (0, 0)$ for $0 \leq \ell \leq \deg(f) + \deg(g) - 1$.

REFERENCES

[1] Daniel Bleichenbacher, Aggelos Kiayias, and Moti Yung. 2003. Decoding of interleaved Reed Solomon codes over noisy data. In *International Colloquium on Automata, Languages, and Programming*. Springer, 97–108.

[2] Brice B. Boyer and Erich L. Kaltofen. 2014. Numerical Linear System Solving With Parametric Entries By Error Correction. In *SNC'14 Proc. 2014 Internat. Workshop on Symbolic-Numeric Comput.*, Jan Verschelde and Stephen M. Watt (Eds.). Association for Computing Machinery, New York, N. Y., 33–38. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/14/BoKa14.pdf.

[3] Stanley Cabay. 1971. Exact Solution of Linear Equations. In *Proceedings of the Second ACM Symposium on Symbolic and Algebraic Manipulation (SYMSAC '71)*. ACM, New York, NY, USA, 392–398. https://doi.org/10.1145/800204.806310

[4] Erich Kaltofen and Clément Pernet. 2013. Cauchy Interpolation with Errors in the Values. Submitted manuscript, 13 pages. (Dec. 2013).

[5] Erich Kaltofen and Zhengfeng Yang. 2013. Sparse multivariate function recovery from values with noise and outlier errors. In *ISSAC 2013 Proc. 38th Internat. Symp. Symbolic Algebraic Comput.*, Manuel Kauers (Ed.). Association for Computing Machinery, New York, N. Y., 219–226. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/13/KaYa13.pdf.

[6] Erich L. Kaltofen and Zhengfeng Yang. 2014. Sparse Multivariate Function Recovery With a High Error Rate in Evaluations. In *ISSAC 2014 Proc. 39th Internat. Symp. Symbolic Algebraic Comput.*, Katsusuke Nabeshima (Ed.). Association for Computing Machinery, New York, N. Y., 280–287. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/14/KaYa14.pdf.

[7] M. T. McClellan. 1973. The exact solution of systems of linear equations with polynomial coefficients. *J. ACM* 20 (1973), 563–588.

[8] Zach Olesh and Arne Storjohann. 2007. The vector rational function reconstruction problems. In *Proc. Waterloo Workshop on Computer Algebra: devoted to the 60th birthday of Sergei Abramov (WWCA)*. 137–149.

[9] V. Olshevsky and M. Amin Shokrollahi. 2003. A Displacement Approach to Decoding Algebraic Codes. In *Algorithms for Structured Matrices: Theory and Applications*. American Mathematical Society, Providence, Rhode Island, USA, 265–292. Contemporary Math., vol. 323. URL: http://www.math.uconn.edu/~olshevsky/papers/shokrollahi_f.pdf.

[10] Clément Pernet. 2014. *High Performance Algebraic Reliable Computing*. Habilitation Thesis. Univ. Joseph Fourier (Grenoble 1).

[11] Georg Schmidt, Vladimir Sidorenko, and Martin Bossert. 2006. Collaborative Decoding of Interleaved Reed-Solomon Codes and Concatenated Code Designs. *CoRR* abs/cs/0610074 (2006). http://arxiv.org/abs/cs/0610074

[12] L. R. Welch and E. R. Berlekamp. 1986. Error Correction of Algebraic Block Codes. US Patent 4,633470. (1986). See http://patft.uspto.gov/.