Fast computation of shifted Popov forms of polynomial matrices via systems of modular polynomial equations

Vincent Neiger

Fast Computation of Shifted Popov Forms of Polynomial Matrices via Systems of Modular Polynomial Equations

Vincent Neiger
ENS de Lyon
Laboratoire LIP, CNRS, Inria, UCBL, U. Lyon
vincent.neiger@ens-lyon.fr

ABSTRACT

We give a Las Vegas algorithm which computes the shifted Popov form of an $m \times m$ nonsingular polynomial matrix of degree d in expected $\widetilde{\mathcal{O}}(m^\omega d)$ field operations, where ω is the exponent of matrix multiplication and $\widetilde{\mathcal{O}}(\cdot)$ indicates that logarithmic factors are omitted. This is the first algorithm in $\widetilde{\mathcal{O}}(m^\omega d)$ for shifted row reduction with arbitrary shifts.

Using partial linearization, we reduce the problem to the case $d \leqslant \lceil \sigma/m \rceil$ where σ is the generic determinant bound, with σ/m bounded from above by both the average row degree and the average column degree of the matrix. The cost above becomes $\widetilde{\mathcal{O}}(m^\omega \lceil \sigma/m \rceil)$, improving upon the cost of the fastest previously known algorithm for row reduction, which is deterministic.

Our algorithm first builds a system of modular equations whose solution set is the row space of the input matrix, and then finds the basis in shifted Popov form of this set. We give a deterministic algorithm for this second step supporting arbitrary moduli in $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ field operations, where m is the number of unknowns and σ is the sum of the degrees of the moduli. This extends previous results with the same cost bound in the specific cases of order basis computation and M-Padé approximation, in which the moduli are products of known linear factors.

Keywords

Shifted Popov form; polynomial matrices; row reduction; Hermite form; system of modular equations.

1. INTRODUCTION

In this paper, we consider two problems of linear algebra over the ring $\mathbb{K}[X]$ of univariate polynomials, for some field $\mathbb{K}$: computing the shifted Popov form of a matrix, and solving systems of modular equations.

1.1 Shifted Popov form

A polynomial matrix $\mathbf{P}$ is row reduced [22, Section 6.3.2] if its rows have some type of minimal degree (we give precise definitions below). Besides, if $\mathbf{P}$ satisfies an additional normalization property, then it is said to be in Popov form [22, Section 6.7.2]. Given a matrix $\mathbf{A}$, the efficient computation of a (row) reduced form of $\mathbf{A}$ and of the Popov form of $\mathbf{A}$ has received a lot of attention recently [14, 28, 16].

In many applications one rather considers the degrees of the rows of $\mathbf{P}$ shifted by some integers which specify degree weights on the columns of $\mathbf{P}$, for example in list-decoding algorithms [2, 7], robust Private Information Retrieval [12], and more generally in polynomial versions of the Coppersmith method [9, 10]. A well-known specific shifted Popov form is the Hermite form; there has been recent progress on its fast computation [17, 15, 35]. The case of an arbitrary shift has been studied in [6].

For a *shift* $\mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{Z}^n$, the $\mathbf{s}$-*degree* of $\mathbf{p} = [p_1, \ldots, p_n] \in \mathbb{K}[X]^{1\times n}$ is $\max_{1\leqslant j\leqslant n}(\deg(p_j) + s_j)$; the $\mathbf{s}$-*row degree* of $\mathbf{P} \in \mathbb{K}[X]^{m\times n}$ is $\mathrm{rdeg}_{\mathbf{s}}(\mathbf{P}) = (d_1, \ldots, d_m)$ with d_i the $\mathbf{s}$-degree of the i-th row of $\mathbf{P}$. Then, the $\mathbf{s}$-*leading matrix* of $\mathbf{P} = [p_{i,j}]_{ij}$ is the matrix $\mathrm{lm}_{\mathbf{s}}(\mathbf{P}) \in \mathbb{K}^{m\times n}$ whose entry (i, j) is the coefficient of degree $d_i - s_j$ of $p_{i,j}$.

Now, we assume that $m \leqslant n$ and $\mathbf{P}$ has full rank. Then, $\mathbf{P}$ is said to be $\mathbf{s}$-*reduced* [22, 6] if $\mathrm{lm}_{\mathbf{s}}(\mathbf{P})$ has full rank. For a full rank $\mathbf{A} \in \mathbb{K}[X]^{m\times n}$, an $\mathbf{s}$-*reduced form of* $\mathbf{A}$ is an $\mathbf{s}$-reduced matrix $\mathbf{P}$ whose row space is the same as that of $\mathbf{A}$; by row space we mean the $\mathbb{K}[X]$-module generated by the rows of the matrix. Equivalently, $\mathbf{P}$ is left-unimodularly equivalent to $\mathbf{A}$ and the tuple $\mathrm{rdeg}_{\mathbf{s}}(\mathbf{P})$ sorted in nondecreasing order is lexicographically minimal among the $\mathbf{s}$-row degrees of all matrices left-unimodularly equivalent to $\mathbf{A}$.

Specific $\mathbf{s}$-reduced matrices are those in $\mathbf{s}$-*Popov form* [22, 5, 6], as defined below. One interesting property is that the $\mathbf{s}$-Popov form is canonical: there is a unique $\mathbf{s}$-reduced form of $\mathbf{A}$ which is in $\mathbf{s}$-Popov form, called the $\mathbf{s}$-*Popov form of* $\mathbf{A}$.

Definition 1.1 (Pivot). *Let $\mathbf{p} = [p_j]_j \in \mathbb{K}[X]^{1\times n}$ be nonzero and let $\mathbf{s} \in \mathbb{Z}^n$. The* $\mathbf{s}$-pivot index *of $\mathbf{p}$ is the largest index j such that $\mathrm{rdeg}_{\mathbf{s}}(\mathbf{p}) = \deg(p_j) + s_j$. Then we call p_j and $\deg(p_j)$ the* $\mathbf{s}$-pivot entry *and the* $\mathbf{s}$-pivot degree *of* $\mathbf{p}$.

We remark that adding a constant to the entries of $\mathbf{s}$ does not change the notion of $\mathbf{s}$-pivot. For example, we will sometimes assume $\min(\mathbf{s}) = 0$ without loss of generality.

Definition 1.2 (Shifted Popov form). *Let $m \leqslant n$, let $\mathbf{P} \in \mathbb{K}[X]^{m\times n}$ be full rank, and let $\mathbf{s} \in \mathbb{Z}^n$. Then, $\mathbf{P}$ is said to be in* $\mathbf{s}$-Popov form *if the $\mathbf{s}$-pivot indices of its rows are strictly increasing, the corresponding $\mathbf{s}$-pivot entries are monic, and in each column of $\mathbf{P}$ which contains a pivot the nonpivot entries have degree less than the pivot entry.*

In this case, the $\mathbf{s}$-pivot degree *of $\mathbf{P}$ is $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_m) \in \mathbb{N}^m$, with δ_i the $\mathbf{s}$-pivot degree of the i-th row of $\mathbf{P}$.*

ISSAC'16, July 19–22, 2016, Waterloo, ON, Canada.
ACM ISBN. DOI: http://dx.doi.org/10.1145/2930889.2930936

Here, although we will encounter Popov forms of rectangular matrices in intermediate nullspace computations, our main focus is on computing shifted Popov forms of *square nonsingular matrices*. For the general case, studied in [6], a fast solution would require further developments. A square matrix in $\mathbf{s}$-Popov form has its $\mathbf{s}$-pivot entries on the diagonal, and its $\mathbf{s}$-pivot degree is the tuple of degrees of its diagonal entries and coincides with its column degree.

> PROBLEM 1 (SHIFTED POPOV NORMAL FORM).
> Input: *the base field* $\mathbb{K}$, *a nonsingular matrix* $\mathbf{A} \in \mathbb{K}[X]^{m\times m}$, *a shift* $\mathbf{s} \in \mathbb{Z}^m$.
> Output: *the* $\mathbf{s}$-*Popov form of* $\mathbf{A}$.

Two well-known specific cases are the Popov form [27, 22] for the *uniform* shift $\mathbf{s} = \mathbf{0}$, and the Hermite form [19, 22] for the shift $\mathbf{h} = (0, \delta, 2\delta, \ldots, (m-1)\delta) \in \mathbb{N}^m$ with $\delta = m \deg(\mathbf{A})$ [6, Lemma 2.6]. For a broader perspective on shifted reduced forms, we refer the reader to [6].

For such problems involving $m \times m$ matrices of degree d, one often wishes to obtain a cost bound similar to that of polynomial matrix multiplication in the same dimensions: $\widetilde{\mathcal{O}}(m^\omega d)$ operations in $\mathbb{K}$. Here, ω is so that we can multiply $m \times m$ matrices over a commutative ring in $\mathcal{O}(m^\omega)$ operations in that ring, the best known bound being $\omega < 2.38$ [11, 25]. For example, one can compute $\mathbf{0}$-reduced [14, 16], $\mathbf{0}$-Popov [28], and Hermite [15, 35] forms of $m\times m$ nonsingular matrices of degree d in $\widetilde{\mathcal{O}}(m^\omega d)$ field operations.

Nevertheless, d may be significantly larger than the average degree of the entries of the matrix, in which case the cost $\widetilde{\mathcal{O}}(m^\omega d)$ seems unsatisfactory. Recently, for the computation of order bases [30, 34], nullspace bases [36], interpolation bases [20, 21], and matrix inversion [37], fast algorithms do take into account some types of average degrees of the matrices rather than their degree. Here, in particular, we achieve a similar improvement for the computation of shifted Popov forms of a matrix.

Given $\mathbf{A} = [a_{i,j}]_{ij} \in \mathbb{K}[X]^{m\times m}$, we denote by $\sigma(\mathbf{A})$ the *generic bound for* $\deg(\det(\mathbf{A}))$ [16, Section 6], that is,

$$\sigma(\mathbf{A}) = \max_{\pi \in S_m} \sum_{1\leqslant i\leqslant m} \overline{\deg}(a_{i,\pi_i}) \qquad (1)$$

where S_m is the set of permutations of $\{1, \ldots, m\}$, and $\overline{\deg}(p)$ is defined over $\mathbb{K}[X]$ as $\overline{\deg}(0) = 0$ and $\overline{\deg}(p) = \deg(p)$ for $p \neq 0$. We have $\deg(\det(\mathbf{A})) \leqslant \sigma(\mathbf{A}) \leqslant m \deg(\mathbf{A})$, and $\sigma(\mathbf{A}) \leqslant \min(|\mathrm{rdeg}(\mathbf{A})|, |\mathrm{cdeg}(\mathbf{A})|)$ with $|\mathrm{rdeg}(\mathbf{A})|$ and $|\mathrm{cdeg}(\mathbf{A})|$ the sums of the row and column degrees of $\mathbf{A}$. We note that $\sigma(\mathbf{A})$ can be substantially smaller than $|\mathrm{rdeg}(\mathbf{A})|$ and $|\mathrm{cdeg}(\mathbf{A})|$, for example if $\mathbf{A}$ has one row and one column of uniformly large degree and other entries of low degree.

THEOREM 1.3. *There is a Las Vegas randomized algorithm which solves Problem 1 in expected* $\widetilde{\mathcal{O}}(m^\omega \lceil\sigma(\mathbf{A})/m\rceil) \subseteq \widetilde{\mathcal{O}}(m^\omega \deg(\mathbf{A}))$ *field operations.*

The ceiling function indicates that the cost is $\widetilde{\mathcal{O}}(m^\omega)$ when $\sigma(\mathbf{A})$ is small compared to m, in which case $\mathbf{A}$ has mostly constant entries. Here we are mainly interested in the case $m \in \mathcal{O}(\sigma(\mathbf{A}))$: the cost bound may be written $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma(\mathbf{A}))$ and is both in $\widetilde{\mathcal{O}}(m^{\omega-1}|\mathrm{rdeg}(\mathbf{A})|)$ and $\widetilde{\mathcal{O}}(m^{\omega-1}|\mathrm{cdeg}(\mathbf{A})|)$.

Previous work on fast algorithms related to Problem 1 is summarized in Table 1. The fastest known algorithm for the

Ref.	Problem	Cost bound	
[18]	Hermite form	$\widetilde{\mathcal{O}}(m^4 d)$	
[31]	Hermite form	$\widetilde{\mathcal{O}}(m^{\omega+1} d)$	
[33]	Popov & Hermite forms	$\widetilde{\mathcal{O}}(m^{\omega+1} d + (md)^\omega)$	
[1, 2]	weak Popov form	$\widetilde{\mathcal{O}}(m^{\omega+1} d)$	
[26]	Popov & Hermite forms	$\mathcal{O}(m^3 d^2)$	
[14]	$\mathbf{0}$-reduction	$\widetilde{\mathcal{O}}(m^\omega d)$	$\star$
[28]	Popov form of $\mathbf{0}$-reduced	$\widetilde{\mathcal{O}}(m^\omega d)$	
[17]	Hermite form	$\widetilde{\mathcal{O}}(m^\omega d)$	$\star$
[16]	$\mathbf{0}$-reduction	$\widetilde{\mathcal{O}}(m^\omega d)$	
[35]	Hermite form	$\widetilde{\mathcal{O}}(m^\omega d)$	
[16]+[28]	$\mathbf{s}$-Popov form for any $\mathbf{s}$	$\widetilde{\mathcal{O}}(m^\omega (d+\mu))$	
Here	$\mathbf{s}$-Popov form for any $\mathbf{s}$	$\widetilde{\mathcal{O}}(m^\omega \lceil\sigma(\mathbf{A})/m\rceil)$	$\star$

Table 1: Fast algorithms for shifted reduction problems ($d = \deg(\mathbf{A})$; $\star$ = probabilistic; $\mu = \max(\mathbf{s}) - \min(\mathbf{s})$)**.**

$\mathbf{0}$-Popov form is deterministic and has cost $\widetilde{\mathcal{O}}(m^\omega d)$ with $d = \deg(\mathbf{A})$; it first computes a $\mathbf{0}$-reduced form of $\mathbf{A}$ [16], and then its $\mathbf{0}$-Popov form via normalization [28]. Obtaining the Hermite form in $\widetilde{\mathcal{O}}(m^\omega d)$ was first achieved by a probabilistic algorithm in [15], and then deterministically in [35].

For an arbitrary $\mathbf{s}$, the algorithm in [6] is fraction-free and uses a number of operations that is, depending on $\mathbf{s}$, at least quintic in m and quadratic in $\deg(\mathbf{A})$.

When $\mathbf{s}$ is not uniform there is a folklore solution based on the fact that $\mathbf{Q}$ is in $\mathbf{s}$-Popov form if and only if $\mathbf{QD}$ is in $\mathbf{0}$-Popov form, with $\mathbf{D} = \mathrm{diag}(X^{s_1}, \ldots, X^{s_m})$ and assuming $\mathbf{s} \geqslant 0$. Then, this solution computes the $\mathbf{0}$-Popov form $\mathbf{P}$ of $\mathbf{AD}$ using [16, 28] and returns $\mathbf{PD}^{-1}$. This approach uses $\widetilde{\mathcal{O}}(m^\omega(d+\mu))$ operations where $\mu = \max(\mathbf{s}) - \min(\mathbf{s})$, which is not satisfactory when μ is large. For example, its cost for computing the Hermite form is $\widetilde{\mathcal{O}}(m^{\omega+2} d)$. This is the worst case since one can assume without loss of generality that $\mu \in \mathcal{O}(m \deg(\det(\mathbf{A}))) \subseteq \mathcal{O}(m^2 d)$ [21, Appendix A].

Here we obtain, to the best of our knowledge, the best known cost bound $\widetilde{\mathcal{O}}(m^\omega \lceil\sigma(\mathbf{A})/m\rceil) \subseteq \widetilde{\mathcal{O}}(m^\omega d)$ for an arbitrary shift $\mathbf{s}$. This removes the dependency in μ, which means in some cases a speedup by a factor m^2. Besides, this is also an improvement for both specific cases $\mathbf{s} = \mathbf{0}$ and $\mathbf{s} = \mathbf{h}$ when $\mathbf{A}$ has unbalanced degrees.

One of the main difficulties in row reduction algorithms is to control the size of the manipulated matrices, that is, the number of coefficients from $\mathbb{K}$ needed for their dense representation. A major issue when dealing with arbitrary shifts is that the size of an $\mathbf{s}$-reduced form of $\mathbf{A}$ may be beyond our target cost. This is a further motivation for focusing on the computation of the $\mathbf{s}$-Popov form of $\mathbf{A}$: by definition, the sum of its column degrees is $\deg(\det(\mathbf{A}))$, and therefore its size is at most $m^2 + m \deg(\det(\mathbf{A}))$, independently of $\mathbf{s}$.

Consider for example $\mathbf{A} = \left[\begin{smallmatrix} \mathbf{B}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{B}_2 \end{smallmatrix}\right]$ for any $\mathbf{0}$-reduced $\mathbf{B}_1$ and $\mathbf{B}_2$ in $\mathbb{K}[X]^{m\times m}$. Then, taking $\mathbf{s} = (0, \ldots, 0, d, \ldots, d)$ with $d > 0$, $\left[\begin{smallmatrix} \mathbf{B}_1 & \mathbf{0} \\ \mathbf{C} & \mathbf{B}_2 \end{smallmatrix}\right]$ is an $\mathbf{s}$-reduced form of $\mathbf{A}$ for any $\mathbf{C} \in \mathbb{K}[X]^{m\times m}$ with $\deg(\mathbf{C}) \leqslant d$; for some $\mathbf{C}$ it has size $\Theta(m^2 d)$, with d arbitrary large independently of $\deg(\mathbf{A})$.

Furthermore, the size of the unimodular transformation leading from $\mathbf{A}$ to $\mathbf{P}$ may be beyond the target cost, which is why fast algorithms for $\mathbf{0}$-reduction and Hermite form do not directly perform unimodular transformations on $\mathbf{A}$ to reduce the degrees of its entries. Instead, they proceed in two steps: first, they work on $\mathbf{A}$ to find some equations which describe its row space, and then they find a basis of solutions to these equations in $\mathbf{0}$-reduced form or Hermite form. We will follow a similar two-step strategy for an arbitrary shift.

It seems that some new ingredient is needed, since for both $\mathbf{s} = \mathbf{0}$ and $\mathbf{s} = \mathbf{h}$ the fastest algorithms use shift-specific properties at some point of the process: namely, the facts that a $\mathbf{0}$-reduced form of $\mathbf{A}$ has degree at most $\deg(\mathbf{A})$ and that the Hermite form of $\mathbf{A}$ is triangular.

As in [17], we first compute the Smith form $\mathbf{S}$ of $\mathbf{A}$ and partial information on a right unimodular transformation $\mathbf{V}$; this is where the probabilistic aspect comes from. This gives a description of the row space of $\mathbf{A}$ as the set of row vectors $\mathbf{p} \in \mathbb{K}[X]^{1\times m}$ such that $\mathbf{pV} = \mathbf{qS}$ for some $\mathbf{q} \in \mathbb{K}[X]^{1\times m}$. Since $\mathbf{S}$ is diagonal, this can be seen as a system of modular equations: the second step is the fast computation of a basis of solutions in $\mathbf{s}$-Popov form, which is our new ingredient.

1.2 Systems of modular equations

Hereafter, $\mathbb{K}[X]_{\neq 0}$ denotes the set of nonzero polynomials. We fix some moduli $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \in \mathbb{K}[X]^n_{\neq 0}$, and for $\mathbf{A}, \mathbf{B} \in \mathbb{K}[X]^{m\times n}$ we write $\mathbf{A} = \mathbf{B} \bmod \mathfrak{M}$ if there exists $\mathbf{Q} \in \mathbb{K}[X]^{m\times n}$ such that $\mathbf{A} = \mathbf{B} + \mathbf{Q}\,\mathrm{diag}(\mathfrak{M})$. Given $\mathbf{F} \in \mathbb{K}[X]^{m\times n}$ specifying the equations, we call *solution for* $(\mathfrak{M}, \mathbf{F})$ any $\mathbf{p} \in \mathbb{K}[X]^{1\times m}$ such that $\mathbf{pF} = 0 \bmod \mathfrak{M}$.

The set of all such $\mathbf{p}$ is a $\mathbb{K}[X]$-submodule of $\mathbb{K}[X]^{1\times m}$ which contains $\mathrm{lcm}(\mathfrak{m}_1, \ldots, \mathfrak{m}_n)\mathbb{K}[X]^{1\times m}$, and is thus free of rank m [24, p. 146]. Then, we represent any basis of this module as the rows of a matrix $\mathbf{P} \in \mathbb{K}[X]^{m\times m}$, called a *solution basis for* $(\mathfrak{M}, \mathbf{F})$. Here, for example for the application to Problem 1, we are interested in such bases that are $\mathbf{s}$-reduced, in which case $\mathbf{P}$ is said to be an $\mathbf{s}$-*minimal solution basis for* $(\mathfrak{M}, \mathbf{F})$. The unique such basis which is in $\mathbf{s}$-Popov form is called the $\mathbf{s}$-*Popov solution basis for* $(\mathfrak{M}, \mathbf{F})$.

> PROBLEM 2 (MINIMAL SOLUTION BASIS).
> Input: *the base field* $\mathbb{K}$, *moduli* $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \in \mathbb{K}[X]^n_{\neq 0}$, *a matrix* $\mathbf{F} \in \mathbb{K}[X]^{m\times n}$ *such that* $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$, *a shift* $\mathbf{s} \in \mathbb{Z}^m$.
> Output: *an* $\mathbf{s}$-*minimal solution basis for* $(\mathfrak{M}, \mathbf{F})$.

Well-known specific cases of this problem are *Hermite-Padé approximation* with a single equation modulo some power of X, and *M-Padé approximation* [3, 32] with moduli that are products of known linear factors. Moreover, an $\mathbf{s}$-*order basis for* $\mathbf{F}$ *and* $(\sigma_1, \ldots, \sigma_n)$ [34] is an $\mathbf{s}$-minimal solution basis for $(\mathfrak{M}, \mathbf{F})$ with $\mathfrak{M} = (X^{\sigma_1}, \ldots, X^{\sigma_n})$.

An overview of fast algorithms for Problem 2 is given in Table 2. For M-Padé approximation, and thus in particular for order basis computation, there is an algorithm to compute the $\mathbf{s}$-Popov solution basis using $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ operations, with $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$ [21]. Here, for $n \in \mathcal{O}(m)$, we extend this result to arbitrary moduli.

THEOREM 1.4. *Assuming* $n \in \mathcal{O}(m)$*, there is a deterministic algorithm which solves Problem 2 using* $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ *field operations, with* $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$*, and returns the* $\mathbf{s}$*-Popov solution basis for* $(\mathfrak{M}, \mathbf{F})$.

We note that Problem 2 is a minimal interpolation basis problem [5, 20] when the so-called *multiplication matrix* $\mathbf{M}$ is block diagonal with companion blocks. Indeed, $\mathbf{p}$ is a solution for $(\mathfrak{M}, \mathbf{F})$ if and only if $\mathbf{p}$ is an *interpolant for* $(\mathbf{E}, \mathbf{M})$ [20, Definition 1.1], where $\mathbf{E} \in \mathbb{K}^{m\times\sigma}$ is the concatenation of the coefficient vectors of the columns of $\mathbf{F}$ and $\mathbf{M} \in \mathbb{K}^{\sigma\times\sigma}$ is $\mathrm{diag}(\mathbf{M}_1, \ldots, \mathbf{M}_n)$ with $\mathbf{M}_j$ the companion matrix associated with $\mathfrak{m}_j$. In this context, the multiplication $\mathbf{p} \cdot \mathbf{E}$ defined by $\mathbf{M}$ as in [5, 20] precisely corresponds to $\mathbf{pF} \bmod \mathfrak{M}$.

In particular, Theorem 1.4 follows from [20, Theorem 1.4] when $\sigma \in \mathcal{O}(m)$. If some of the moduli have small degree, we use this result for base cases of our recursive algorithm.

Ref.	Cost bound	Moduli	Particularities
[3, 32]	$\mathcal{O}(m^2\sigma^2)$	split	
[4]	$\mathcal{O}(m\sigma^2)$	$\mathfrak{m}_j = X^{\sigma/n}$	partial basis
[4]	$\widetilde{\mathcal{O}}(m^\omega\sigma)$	$\mathfrak{m}_j = X^{\sigma/n}$	
[14]	$\widetilde{\mathcal{O}}(m^\omega\sigma/n)$	$\mathfrak{m}_j = X^{\sigma/n}$	
[30]	$\widetilde{\mathcal{O}}(m^\omega\lceil\sigma/m\rceil)$	$\mathfrak{m}_j = X^{\sigma/n}$	partial basis, $\lvert\mathbf{s}\rvert \leqslant \sigma$
[34]	$\widetilde{\mathcal{O}}(m^\omega\lceil\sigma/m\rceil)$	$\mathfrak{m}_j = X^{\sigma/n}$	$\lvert\mathbf{s}\rvert \leqslant \sigma$
[8]	$\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$, probabilistic	any	returns a single small degree solution
[20]	$\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$	split	$\lvert\mathbf{s}\rvert \leqslant \sigma$
[20]	$\widetilde{\mathcal{O}}(m\sigma^{\omega-1})$	any	$\mathbf{s}$-Popov, $\sigma \in \mathcal{O}(m)$
[21]	$\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$	split	$\mathbf{s}$-Popov
Here	$\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$	any	$\mathbf{s}$-Popov

Table 2: Fast algorithms for Problem 2 ($n \in \mathcal{O}(m)$; *partial basis* = returns small degree rows of an $\mathbf{s}$-minimal solution basis; *split* = product of known linear factors)**.**

In the case of M-Padé approximation, knowing the moduli as products of linear factors leads to rewriting the problem as a minimal interpolation basis computation with $\mathbf{M}$ in Jordan form [5, 20]. Since $\mathbf{M}$ is upper triangular, one can then rely on recurrence relations to solve the problem iteratively [3, 32, 4, 5]. The fast algorithms in [4, 14, 34, 20, 21], beyond the techniques used to achieve efficiency, are essentially divide-and-conquer versions of this iterative solution and are thus based on the same recurrence relations.

However, for arbitrary moduli the matrix $\mathbf{M}$ is not triangular and there is no such recurrence in general. Then, a natural idea is to relate solution bases to nullspace bases: Problem 2 asks to find $\mathbf{P}$ such that there is some quotient $\mathbf{Q}$ with $[\mathbf{P}|\mathbf{Q}]\mathbf{N} = \mathbf{0}$ for $\mathbf{N} = [\mathbf{F}^\mathsf{T}| - \mathrm{diag}(\mathfrak{M})]^\mathsf{T}$. More precisely, $[\mathbf{P}|\mathbf{Q}]$ can be obtained as a $\mathbf{u}$-minimal nullspace basis of $\mathbf{N}$ for the shift $\mathbf{u} = (\mathbf{s} - \min(\mathbf{s}), \mathbf{0}) \in \mathbb{N}^{m+n}$.

Using recent ingredients from [17, 21] outlined in the next paragraphs, the main remaining difficulty is to deal with this nullspace problem when $n = 1$. Here, we give a $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ algorithm to solve it using its specific properties: $\mathbf{N}$ is the column $[\mathbf{F}^\mathsf{T}|\mathfrak{m}_1]^\mathsf{T}$ with $\deg(\mathbf{F}) < \deg(\mathfrak{m}_1) = \sigma$, and the last entry of $\mathbf{u}$ is $\min(\mathbf{u})$. First, when $\max(\mathbf{u}) \in \mathcal{O}(\sigma)$ we show that $[\mathbf{P}|\mathbf{Q}]$ can be efficiently obtained as a submatrix of the $\mathbf{u}$-Popov order basis for $\mathbf{N}$ and order $\mathcal{O}(\sigma)$. Then, when $\max(\mathbf{u})$ is large compared to σ and assuming $\mathbf{u}$ is sorted non-decreasingly, $\mathbf{P}$ has a lower block triangular shape. We show how this shape can be revealed, along with the $\mathbf{s}$-pivot degree of $\mathbf{P}$, using a divide-and-conquer approach which splits $\mathbf{u}$ into two shifts of amplitude about $\max(\mathbf{u})/2$.

Then, for $n \geqslant 1$ we use a divide-and-conquer approach on n which is classical in such contexts: two solution bases $\mathbf{P}^{(1)}$ and $\mathbf{P}^{(2)}$ are computed recursively in shifted Popov form and are multiplied together to obtain the $\mathbf{s}$-minimal solution basis $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$ for $(\mathfrak{M}, \mathbf{F})$. However this product is usually not in $\mathbf{s}$-Popov form and may have size beyond our target cost. Thus, as in [21], instead of computing $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$, we use $\mathbf{P}^{(2)}$ and $\mathbf{P}^{(1)}$ to deduce the $\mathbf{s}$-pivot degree of $\mathbf{P}$.

In both recursions above, we focus on finding the $\mathbf{s}$-pivot degree of $\mathbf{P}$. Using ideas and results from [17, 21], we show that this knowledge about the degrees in $\mathbf{P}$ allows us to complete the computation of $\mathbf{P}$ within the target cost.

2. FAST COMPUTATION OF THE SHIFTED POPOV SOLUTION BASIS

Hereafter, we call $\mathbf{s}$-*minimal degree of* $(\mathfrak{M}, \mathbf{F})$ the $\mathbf{s}$-pivot degree $\boldsymbol{\delta}$ of the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$; $\boldsymbol{\delta}$ coincides with the column degree of this basis. A central result for the cost analysis is that $|\boldsymbol{\delta}| = \delta_1 + \cdots + \delta_m$ is at most $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$. This is classical for M-Padé approximation [32, Theorem 4.1] and holds for minimal interpolation bases in general (see for example [20, Lemma 7.17]).

2.1 Solution bases from nullspace bases and fast algorithm for known minimal degree

This subsection summarizes and slightly extends results from [17, Section 3]. We first show that the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$ is the principal $m \times m$ submatrix of the $\mathbf{u}$-Popov nullspace basis of $[\mathbf{F}^\mathsf{T} | \operatorname{diag}(\mathfrak{M})]^\mathsf{T}$ for some $\mathbf{u} \in \mathbb{Z}^{m+n}$.

Lemma 2.1. *Let $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \in \mathbb{K}[X]^n_{\neq 0}$, $\mathbf{s} \in \mathbb{Z}^m$, $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$ with $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$, $\mathbf{P} \in \mathbb{K}[X]^{m \times m}$, and $\mathbf{w} \in \mathbb{Z}^n$ be such that $\max(\mathbf{w}) \leqslant \min(\mathbf{s})$. Then, $\mathbf{P}$ is the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$ if and only if $[\mathbf{P}|\mathbf{Q}]$ is the $\mathbf{u}$-Popov nullspace basis of $[\mathbf{F}^\mathsf{T} | \operatorname{diag}(\mathfrak{M})]^\mathsf{T}$ for some $\mathbf{Q} \in \mathbb{K}[X]^{m \times n}$ and $\mathbf{u} = (\mathbf{s}, \mathbf{w}) \in \mathbb{Z}^{m+n}$. In this case, $\deg(\mathbf{Q}) < \deg(\mathbf{P})$ and $[\mathbf{P}|\mathbf{Q}]$ has $\mathbf{s}$-pivot index $(1, 2, \ldots, m)$.*

Proof. Let $\mathbf{N} = [\mathbf{F}^\mathsf{T} | \operatorname{diag}(\mathfrak{M})]^\mathsf{T}$. It is easily verified that $\mathbf{P}$ is a solution basis for $(\mathfrak{M}, \mathbf{F})$ if and only if there is some $\mathbf{Q} \in \mathbb{K}[X]^{m \times n}$ such that $[\mathbf{P}|\mathbf{Q}]$ is a nullspace basis of $\mathbf{N}$.

Now, having $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$ implies that any $[\mathbf{p}|\mathbf{q}] \in \mathbb{K}[X]^{1 \times (m+n)}$ in the nullspace of $\mathbf{N}$ satisfies $\deg(\mathbf{q}) < \deg(\mathbf{p})$, and since $\max(\mathbf{w}) \leqslant \min(\mathbf{s})$ we get $\operatorname{rdeg}_\mathbf{w}(\mathbf{q}) < \operatorname{rdeg}_\mathbf{s}(\mathbf{p})$. In particular, for any matrix $[\mathbf{P}|\mathbf{Q}] \in \mathbb{K}[X]^{m \times (m+n)}$ such that $[\mathbf{P}|\mathbf{Q}]\mathbf{N} = 0$, we have $\operatorname{lm}_\mathbf{u}([\mathbf{P}|\mathbf{Q}]) = [\operatorname{lm}_\mathbf{s}(\mathbf{P})|\mathbf{0}]$. This implies that $\mathbf{P}$ is in $\mathbf{s}$-Popov form if and only if $[\mathbf{P}|\mathbf{Q}]$ is in $\mathbf{u}$-Popov form with $\mathbf{s}$-pivot index $(1, \ldots, m)$. ☐

We now show that, when we have *a priori* knowledge about the $\mathbf{s}$-pivot entries of a $\mathbf{s}$-Popov nullspace basis, it can be computed efficiently via an $\mathbf{s}$-Popov order basis.

Lemma 2.2. *Let $\mathbf{s} \in \mathbb{Z}^{m+n}$ and let $\mathbf{N} \in \mathbb{K}[X]^{(m+n) \times n}$ be of full rank. Let $\mathbf{B} \in \mathbb{K}[X]^{m \times (m+n)}$ be the $\mathbf{s}$-Popov nullspace basis for $\mathbf{N}$, $(\pi_1, \ldots, \pi_m)$ be its $\mathbf{s}$-pivot index, $(\delta_1, \ldots, \delta_m)$ be its $\mathbf{s}$-pivot degree, and $\delta \geqslant \deg(\mathbf{B})$ be a degree bound. Then, let $\mathbf{u} = (u_1, \ldots, u_{m+n}) \in \mathbb{Z}^{m+n}_{\leqslant 0}$ with*

$$u_j = \begin{cases} -\delta - 1 & \text{if } j \notin \{\pi_1, \ldots, \pi_m\}, \\ -\delta_i & \text{if } j = \pi_i. \end{cases}$$

Writing $(\sigma_1, \ldots, \sigma_n)$ for the column degree of $\mathbf{N}$, let $\tau_j = \sigma_j + \delta + 1$ for $1 \leqslant j \leqslant n$ and let $\mathbf{A}$ be the $\mathbf{u}$-Popov order basis for $\mathbf{N}$ and $(\tau_1, \ldots, \tau_n)$. Then, $\mathbf{B}$ is the submatrix of $\mathbf{A}$ formed by its rows at indices $\{\pi_1, \ldots, \pi_m\}$.

Proof. First, $\mathbf{B}$ is in $\mathbf{u}$-Popov form with $\operatorname{rdeg}_\mathbf{u}(\mathbf{B}) = \mathbf{0}$. Define $\mathbf{C} \in \mathbb{K}[X]^{(m+n) \times (m+n)}$ whose i-th row is $\mathbf{B}_{j,*}$ if $i = \pi_j$ and $\mathbf{A}_{i,*}$ if $i \notin \{\pi_1, \ldots, \pi_m\}$: we want to prove $\mathbf{C} = \mathbf{A}$.

Let $\mathbf{p} = [p_j]_j \in \mathbb{K}[X]^{1 \times (m+n)}$ be a row of $\mathbf{A}$, and assume $\operatorname{rdeg}_\mathbf{u}(\mathbf{p}) < 0$. This means $\deg(p_j) < -u_j$ for all j, so that $\deg(\mathbf{p}) < \max(-\mathbf{u}) = \delta + 1$. Then, for all $1 \leqslant j \leqslant n$ we have $\deg(\mathbf{p}\mathbf{N}_{*,j}) < \sigma_j + \delta + 1 = \tau_j$, and from $\mathbf{p}\mathbf{N}_{*,j} = 0 \bmod X^{\tau_j}$ we obtain $\mathbf{p}\mathbf{N}_{*,j} = 0$, which is absurd by minimality of $\mathbf{B}$. As a result, $\operatorname{rdeg}_\mathbf{u}(\mathbf{A}) \geqslant \mathbf{0} = \operatorname{rdeg}_\mathbf{u}(\mathbf{B})$ componentwise.

Besides, $\mathbf{CF} = 0 \bmod (X^{\tau_1}, \ldots, X^{\tau_n})$ and since $\mathbf{C}$ has its $\mathbf{u}$-pivot entries on the diagonal, it is $\mathbf{u}$-reduced: by minimality of $\mathbf{A}$, we obtain $\operatorname{rdeg}_\mathbf{u}(\mathbf{A}) = \operatorname{rdeg}_\mathbf{u}(\mathbf{C})$. Then, it is easily verified that $\mathbf{C}$ is in $\mathbf{u}$-Popov form, hence $\mathbf{C} = \mathbf{A}$. ☐

In particular, computing the $\mathbf{s}$-Popov nullspace basis $\mathbf{B}$, when its $\mathbf{s}$-pivot index, its $\mathbf{s}$-pivot degree, and $\delta \geqslant \deg(\mathbf{B})$ are known, can be done in $\widetilde{\mathcal{O}}(m^{\omega-1}(\sigma + n\delta))$ with $\sigma = \sigma_1 + \cdots + \sigma_n$ using the order basis algorithm in [21].

As for Problem 2, with Lemma 2.1 this gives an algorithm for computing $\mathbf{P}$ *and* the quotients $\mathbf{Q} = -\mathbf{PF}/\operatorname{diag}(\mathfrak{M})$ when we know *a priori* the $\mathbf{s}$-minimal degree $\boldsymbol{\delta}$ of $(\mathfrak{M}, \mathbf{F})$. Here, we would choose $\delta = \max(\boldsymbol{\delta}) \geqslant \deg([\mathbf{P}|\mathbf{Q}])$: in some cases $\delta = \Theta(\sigma)$ and this has cost bound $\widetilde{\mathcal{O}}(m^{\omega-1}(\sigma + n\sigma))$, which exceeds our target $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$. An issue is that $\mathbf{Q}$ has size $\mathcal{O}(mn\sigma)$ when $\mathbf{P}$ has columns of large degree; yet here we are not interested in $\mathbf{Q}$. This can be solved using partial linearization to expand the columns of large degree in $\mathbf{P}$ into more columns of smaller degree as in the next result, which holds in general for interpolation bases [21, Lemma 4.2].

Lemma 2.3. *Let $\mathfrak{M} \in \mathbb{K}[X]^n_{\neq 0}$ with entries having degrees $(\sigma_1, \ldots, \sigma_n)$. Let $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$ and $\mathbf{s} \in \mathbb{Z}^m$. Furthermore, let $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_m)$ denote the $\mathbf{s}$-minimal degree of $(\mathfrak{M}, \mathbf{F})$.*

Writing $\sigma = \sigma_1 + \cdots + \sigma_n$, let $\delta = \lceil \sigma/m \rceil \geqslant 1$, and for $i \in \{1, \ldots, m\}$ write $\delta_i = (\alpha_i - 1)\delta + \beta_i$ with $\alpha_i \geqslant 1$ and $0 \leqslant \beta_i < \delta$, and let $\widetilde{m} = \alpha_1 + \cdots + \alpha_m$. Define $\widetilde{\boldsymbol{\delta}} \in \mathbb{N}^{\widetilde{m}}$ as

$$\widetilde{\boldsymbol{\delta}} = (\underbrace{\delta, \ldots, \delta, \beta_1}_{\alpha_1}, \ldots, \underbrace{\delta, \ldots, \delta, \beta_m}_{\alpha_m}) \qquad (2)$$

and the expansion-compression matrix $\mathcal{E} \in \mathbb{K}[X]^{\widetilde{m} \times m}$ as

$$\mathcal{E} = \begin{bmatrix} 1 & & \\ X^{\delta} & & \\ \vdots & & \\ X^{(\alpha_1 - 1)\delta} & & \\ & \ddots & \\ & & 1 \\ & & X^{\delta} \\ & & \vdots \\ & & X^{(\alpha_m - 1)\delta} \end{bmatrix}. \qquad (3)$$

Let $\mathbf{d} = -\widetilde{\boldsymbol{\delta}} \in \mathbb{Z}^{\widetilde{m}}$ and $\mathbf{P} \in \mathbb{K}[X]^{\widetilde{m} \times \widetilde{m}}$ be the $\mathbf{d}$-Popov solution basis for $(\mathfrak{M}, \mathcal{E}\mathbf{F} \bmod \mathfrak{M})$. Then, $\mathbf{P}$ has $\mathbf{d}$-pivot degree $\widetilde{\boldsymbol{\delta}}$ and the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$ is the submatrix of $\mathbf{P}\mathcal{E}$ formed by its rows at indices $\{\alpha_1 + \cdots + \alpha_i, 1 \leqslant i \leqslant m\}$.

This leads to Algorithm 1, which solves Problem 2 efficiently when the $\mathbf{s}$-minimal degree $\boldsymbol{\delta}$ is known *a priori.*

Algorithm 1 (KnownDegPolModSys).

Input: polynomials $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \in \mathbb{K}[X]^n_{\neq 0}$, a matrix $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$ with $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$, a shift $\mathbf{s} \in \mathbb{Z}^m$, $\boldsymbol{\delta} = (\delta_1, \ldots, \delta_m)$ the $\mathbf{s}$-minimal degree of $(\mathfrak{M}, \mathbf{F})$.

Output: the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$.

1. $\delta \leftarrow \lceil (\deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n))/m \rceil$, $\alpha_i \leftarrow \lfloor \delta_i/\delta \rfloor + 1$ for $1 \leqslant i \leqslant m$, $\widetilde{m} \leftarrow \alpha_1 + \cdots + \alpha_m$, $\widetilde{\boldsymbol{\delta}}$ as in (2), $\mathcal{E}$ as in (3), $\widetilde{\mathbf{F}} \leftarrow \mathcal{E}\mathbf{F} \bmod \mathfrak{M}$
2. $\mathbf{u} \leftarrow (-\widetilde{\boldsymbol{\delta}}, -\delta - 1, \ldots, -\delta - 1) \in \mathbb{Z}^{\widetilde{m}+n}$ $\boldsymbol{\tau} \leftarrow (\deg(\mathfrak{m}_j) + \delta + 1)_{1 \leqslant j \leqslant n}$
3. $\widetilde{\mathbf{P}} \leftarrow$ the $\mathbf{u}$-Popov order basis for $[\widetilde{\mathbf{F}}^\mathsf{T} | \operatorname{diag}(\mathfrak{M})]^\mathsf{T}$ and $\boldsymbol{\tau}$ $\mathbf{P} \leftarrow$ the principal $\widetilde{m} \times \widetilde{m}$ submatrix of $\widetilde{\mathbf{P}}$
4. Return the submatrix of $\mathbf{P}\mathcal{E}$ formed by the rows at indices $\alpha_1 + \cdots + \alpha_i$ for $1 \leqslant i \leqslant m$

Proposition 2.4. *Algorithm* KnownDegPolModSys *is correct. Writing $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n)$ and assuming $\sigma \geqslant m \geqslant n$, it uses $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ operations in $\mathbb{K}$.*

Proof. By Lemmas 2.3 and 2.1, since $\min(-\widetilde{\boldsymbol{\delta}}) > -\delta - 1$ and $\mathbf{u} = (-\widetilde{\boldsymbol{\delta}}, -\delta - 1, \ldots, -\delta - 1)$, the $-\boldsymbol{\delta}$-Popov solution basis for $(\mathfrak{M}, \widetilde{\mathbf{F}})$ is the principal $\widetilde{m} \times \widetilde{m}$ submatrix of the $\mathbf{u}$-Popov nullspace basis $\mathbf{B}$ for $[\widetilde{\mathbf{F}}^\mathsf{T} | \operatorname{diag}(\mathfrak{M})]^\mathsf{T}$, and $\mathbf{B}$ has $\mathbf{u}$-pivot index $\{1, \ldots, \widetilde{m}\}$, $\mathbf{u}$-pivot degree $\widetilde{\boldsymbol{\delta}}$, and $\deg(\mathbf{B}) \leqslant \delta$. Then, by Lemma 2.2, $\mathbf{B}$ is formed by the first $\widetilde{m}$ rows of $\widetilde{\mathbf{P}}$ at Step **3**, hence $\mathbf{P}$ is the $\mathbf{d}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$. The correctness then follows from Lemma 2.3.

Since $|\boldsymbol{\delta}| \leqslant \sigma$, $\mathcal{E}$ has $\widetilde{m} \leqslant 2m$ rows and $\mathcal{E}\mathbf{F} \bmod \mathfrak{M}$ can be computed in $\widetilde{\mathcal{O}}(m\sigma)$ operations using fast polynomial division [13]. The cost bound of Step **3** follows from [21, Theorem 1.4] since $\tau_1 + \cdots + \tau_n = \sigma + n(1 + \lceil \sigma/m \rceil) \in \mathcal{O}(\sigma)$. $\square$

2.2 The case of one equation

We now present our main new ingredients, focusing on the case $n = 1$. First, we show that when the shift $\mathbf{s}$ has a small *amplitude* $\operatorname{amp}(\mathbf{s}) = \max(\mathbf{s}) - \min(\mathbf{s})$, one can solve Problem 2 via an order basis computation at small order.

LEMMA 2.5. *Let $\mathfrak{m} \in \mathbb{K}[X]_{\neq 0}$, $\mathbf{s} \in \mathbb{Z}^m$, and $\mathbf{F} \in \mathbb{K}[X]^{m \times 1}$ with $\deg(\mathbf{F}) < \deg(\mathfrak{m}) = \sigma$. Then, for any $\tau \geqslant \operatorname{amp}(\mathbf{s}) + 2\sigma$, the $\mathbf{s}$-Popov solution basis for $(\mathfrak{m}, \mathbf{F})$ is the principal $m \times m$ submatrix of the $\mathbf{u}$-Popov order basis for $[\mathbf{F}^\mathsf{T} | \mathfrak{m}]^\mathsf{T}$ and τ, with $\mathbf{u} = (\mathbf{s}, \min(\mathbf{s})) \in \mathbb{Z}^{m+1}$.*

PROOF. Let $\mathbf{A} = \left[\begin{smallmatrix} \mathbf{P} & \mathbf{q} \\ \mathbf{p} & q \end{smallmatrix}\right]$ denote the $\mathbf{u}$-Popov order basis for $[\mathbf{F}^\mathsf{T} | \mathfrak{m}]^\mathsf{T}$ and τ, where $\mathbf{P} \in \mathbb{K}[X]^{m \times m}$ and $q \in \mathbb{K}[X]$. Consider $\mathbf{B} = [\bar{\mathbf{P}} | \bar{\mathbf{q}}]$ the $\mathbf{u}$-Popov nullspace basis of $[\mathbf{F}^\mathsf{T} | \mathfrak{m}]^\mathsf{T}$: thanks to Lemma 2.1, it is enough to prove that $\mathbf{B} = [\mathbf{P} | \mathbf{q}]$.

First, we have $\operatorname{rdeg}(\mathbf{p}) \leqslant \deg(q)$ by choice of $\mathbf{u}$, so that $q\mathfrak{m} \neq 0$ implies $\deg(\mathbf{p}\mathbf{F} + q\mathfrak{m}) = \deg(q) + \sigma$. Since $\mathbf{p}\mathbf{F} + q\mathfrak{m} = 0 \bmod X^\tau$, this gives $\deg(q) + \sigma \geqslant \tau$. This also shows that the $\mathbf{u}$-pivot entries of $\mathbf{B}$ are located in $\bar{\mathbf{P}}$.

Then, since the sum of the $\mathbf{u}$-pivot degrees of $\mathbf{A}$ is at most τ, the sum of the $\mathbf{s}$-pivot degrees of $\mathbf{P}$ is at most σ; with $[\mathbf{P} | \mathbf{q}]$ in $\mathbf{u}$-Popov form, this gives $\deg(\mathbf{q}) < \sigma + \operatorname{amp}(\mathbf{s}) \leqslant \tau - \sigma$. We obtain $\deg(\mathbf{P}\mathbf{F} + \mathbf{q}\mathfrak{m}) < \tau$, so that $\mathbf{P}\mathbf{F} + \mathbf{q}\mathfrak{m} = 0$. Thus, the minimality of $\mathbf{B}$ and $\mathbf{A}$ gives the conclusion. $\square$

When $\operatorname{amp}(\mathbf{s}) \in \mathcal{O}(\sigma)$, this gives a fast solution to our problem. In what follows, we present a divide-and-conquer approach on $\operatorname{amp}(\mathbf{s})$, with base case $\operatorname{amp}(\mathbf{s}) \in \mathcal{O}(\sigma)$.

We first give an overview, assuming $\mathbf{s}$ is non-decreasing. A key ingredient is that when $\operatorname{amp}(\mathbf{s})$ is large compared to σ, then $\mathbf{P}$ has a lower block triangular shape, since it is in $\mathbf{s}$-Popov form with sum of $\mathbf{s}$-pivot degrees $|\boldsymbol{\delta}| \leqslant \sigma$. Typically, if $s_{i+1} - s_i \geqslant \sigma$ for some i then $\mathbf{P} = \left[\begin{smallmatrix} \mathbf{P}^{(1)} & \mathbf{0} \\ * & \mathbf{P}^{(2)} \end{smallmatrix}\right]$ with $\mathbf{P}^{(1)} \in \mathbb{K}[X]^{i \times i}$. Even though the block sizes are unknown in general, we show that they can be revealed efficiently along with $\boldsymbol{\delta}$ by a divide-and-conquer algorithm, as follows.

First, we use a recursive call with the first j entries $\mathbf{s}^{(0)}$ of $\mathbf{s}$ and $\mathbf{F}^{(0)}$ of $\mathbf{F}$, where j is such that $\operatorname{amp}(\mathbf{s}^{(0)})$ is about half of $\operatorname{amp}(\mathbf{s})$. This reveals the first $i \leqslant j$ entries $\boldsymbol{\delta}^{(1)}$ of $\boldsymbol{\delta}$ and the first i rows $[\mathbf{P}^{(1)} | \mathbf{0}]$ of $\mathbf{P}$, with $\mathbf{P}^{(1)} \in \mathbb{K}[X]^{i \times i}$. A central point is that $\operatorname{amp}(\mathbf{s}^{(2)})$ is about half of $\operatorname{amp}(\mathbf{s})$ as well, where $\mathbf{s}^{(2)}$ is the tail of $\mathbf{s}$ starting at the entry $i + 1$.

Then, knowing the degrees $\boldsymbol{\delta}^{(1)}$ allows us to set up an order basis computation that yields a *residual*, that is, a column $\mathbf{G} \in \mathbb{K}[X]^{(m-i) \times 1}$ and a modulus $\mathfrak{n}$ such that we can continue the computation of $\mathbf{P}$ using a second recursive call, which consists in computing the $\mathbf{s}^{(2)}$-Popov solution basis for $(\mathfrak{n}, \mathbf{G})$. From these two calls we obtain $\boldsymbol{\delta}$, and then we recover $\mathbf{P}$ using Algorithm 1.

Now we present the details. We fix $\mathbf{F} \in \mathbb{K}[X]^{m \times 1}$, $\mathfrak{m} \in \mathbb{K}[X]_{\neq 0}$ with $\sigma = \deg(\mathfrak{m}) > \deg(\mathbf{F})$, $\mathbf{s} \in \mathbb{Z}^m$, $\mathbf{P}$ the $\mathbf{s}$-Popov solution basis for $(\mathfrak{m}, \mathbf{F})$, and $\boldsymbol{\delta}$ its $\mathbf{s}$-pivot degree. In what follows, $\boldsymbol{\pi}^{\mathbf{s}} = (\pi_1, \ldots, \pi_m)$ is any permutation of $\{1, \ldots, m\}$ such that $(s_{\pi_1}, \ldots, s_{\pi_m})$ is non-decreasing.

Then, for $\mathbf{t} = (t_1, \ldots, t_m) \in \mathbb{Z}^m$ we write $\mathbf{t}_{[i:j]}$ for the subtuple of $\mathbf{t}$ formed by its entries at indices $\{\pi_i, \ldots, \pi_j\}$, and for a matrix $\mathbf{M} \in \mathbb{K}[X]^{m \times m}$ we write $\mathbf{M}_{[i:j,k:l]}$ for the submatrix of $\mathbf{M}$ formed by its rows at indices $\{\pi_i, \pi_{i+1}, \ldots, \pi_j\}$ and columns at indices $\{\pi_k, \pi_{k+1}, \ldots, \pi_l\}$. The main ideas in this subsection can be understood by focusing on the case of a non-decreasing $\mathbf{s}$, taking $\pi_i = i$ for all i: then we have $\mathbf{t}_{[i:j]} = (t_i, t_{i+1}, \ldots, t_j)$ and $\mathbf{M}_{[i:j,k:l]} = (\mathbf{M}_{u,v})_{i \leqslant u \leqslant j, k \leqslant v \leqslant l}$.

We now introduce the notion of splitting index, which will help us to locate zero blocks in $\mathbf{P}$.

DEFINITION 2.6 (SPLITTING INDEX). *Let $\mathbf{d} \in \mathbb{N}^m$, $\mathbf{t} \in \mathbb{Z}^m$ and $\boldsymbol{\pi}^{\mathbf{t}} = (\mu_i)_i$. Then, $i \in \{1, \ldots, m-1\}$ is a* splitting index *for $(\mathbf{d}, \mathbf{t})$ if $d_{\mu_j} + t_{\mu_j} - t_{\mu_{i+1}} < 0$ for all $j \in \{1, \ldots, i\}$.*

In particular, if i is a splitting index for $(\boldsymbol{\delta}, \mathbf{s})$, then we have $[\mathbf{P}_{[:i,:i]} | \mathbf{P}_{[:i,i+1:]}] = [\mathbf{P}_{[:i,:i]} | \mathbf{0}]$. Our algorithm first looks for such a splitting index, and then uses $\mathbf{P}_{[:i,i+1:]} = \mathbf{0}$ to split the problem into two subproblems of dimensions i and $m - i$.

To find a splitting index, we rely on the following property: if $(\mathbf{d}, \mathbf{t})$ does not admit a splitting index, then $|\mathbf{d}| > \operatorname{amp}(\mathbf{t})$. This allows us to partition $\mathbf{s}$ into ℓ subtuples which all contain a splitting index, as follows.

Given $\alpha \in \mathbb{Z}_{>0}$ we let $\ell = 1 + \lfloor \operatorname{amp}(\mathbf{s})/\alpha \rfloor$ and we consider the subtuples $\mathbf{s}_1, \ldots, \mathbf{s}_\ell$ of $\mathbf{s}$ where $\mathbf{s}_k$ consists of the entries of $\mathbf{s}$ in $\{\min(\mathbf{s}) + (k-1)\alpha, \ldots, \min(\mathbf{s}) + k\alpha - 1\}$; this gives a subroutine $\textsc{Partition}(\mathbf{s}, \alpha) = (\mathbf{s}_1, \ldots, \mathbf{s}_\ell)$. Now we take $\alpha \geqslant 2\sigma$ and we assume $s_{\pi_{i+1}} - s_{\pi_i} \leqslant \sigma$ for $1 \leqslant i < m$ without loss of generality [21, Appendix A]. Then, for $1 \leqslant k < \ell$, since $|\boldsymbol{\delta}| \leqslant \sigma$ and $\operatorname{amp}(\mathbf{t}) \geqslant \sigma$ with $\mathbf{t} = (\mathbf{s}_k, \min(\mathbf{s}_{k+1}))$, by the above remark $\mathbf{s}_k$ contains a splitting index for $(\boldsymbol{\delta}, \mathbf{s})$.

Still, we do not know in advance which entries of $\mathbf{s}_k$ correspond to splitting indices for $(\boldsymbol{\delta}, \mathbf{s})$. Thus we recursively compute the $\mathbf{s}$-Popov solution basis $\mathbf{P}^{(0)}$ for $\mathbf{s}_1, \ldots, \mathbf{s}_{\ell/2}$, and we are now going to prove that this gives us a splitting index which divides the computation into two subproblems, the first of which has been already solved by computing $\mathbf{P}^{(0)}$.

LEMMA 2.7. *Let $j \in \{2, \ldots, m\}$, $\mathbf{s}^{(0)} = \mathbf{s}_{[:j]}$, $\mathbf{P}^{(0)}$ be the $\mathbf{s}^{(0)}$-Popov solution basis for $(\mathfrak{m}, \mathbf{F}_{[:j]})$, and $\boldsymbol{\delta}^{(0)}$ be its $\mathbf{s}^{(0)}$-pivot degree. Suppose that there is a splitting index $i \leqslant j$ for $(\boldsymbol{\delta}^{(0)}, \mathbf{s}^{(0)})$. Let $\mathbf{P}^{(1)} \in \mathbb{K}[X]^{i \times i}$ be the $\mathbf{s}^{(1)}$-Popov solution basis for $(\mathfrak{m}, \mathbf{F}_{[:i]})$ with $\mathbf{s}^{(1)} = \mathbf{s}_{[:i]}$, and let $\boldsymbol{\delta}^{(1)}$ be its $\mathbf{s}^{(1)}$-pivot degree. Then i is a splitting index for $(\boldsymbol{\delta}, \mathbf{s})$ and $\mathbf{P}_{[:i,:i]} = \mathbf{P}^{(1)} = \mathbf{P}^{(0)}_{[:i,:i]}$, hence $\boldsymbol{\delta}_{[:i]} = \boldsymbol{\delta}^{(1)} = \boldsymbol{\delta}^{(0)}_{[:i]}$ (where $\mathbf{P}^{(0)}$ and $\boldsymbol{\delta}^{(0)}$ are indexed by $\{\pi_1, \ldots, \pi_j\}$ sorted increasingly).*

PROOF. Since i is a splitting index for $(\boldsymbol{\delta}^{(0)}, \mathbf{s}^{(0)})$ we have $[\mathbf{P}^{(0)}_{[:i,:i]} | \mathbf{P}^{(0)}_{[:i,i+1:]}] = [\mathbf{Q} | \mathbf{0}]$ for some $\mathbf{Q} \in \mathbb{K}[X]^{i \times i}$. Now, for any $\mathbf{B} \in \mathbb{K}[X]^{m \times m}$ with $[\mathbf{B}_{[:i,:i]} | \mathbf{B}_{[:i,i+1:]}] = [\mathbf{P}^{(1)} | \mathbf{0}]$, $\mathbf{B}_{[:i,:]}$ is in $\mathbf{s}$-Popov form with its rows being solutions for $(\mathfrak{M}, \mathbf{F})$. Then, by minimality of $\mathbf{P}$, $\mathbf{P}_{[:i,:]}$ has $\mathbf{s}$-pivot degree at most $\boldsymbol{\delta}^{(1)}$ componentwise, so that i is also a splitting index for $(\boldsymbol{\delta}, \mathbf{s})$, and in particular $[\mathbf{P}_{[:i,:i]} | \mathbf{P}_{[:i,i+1:]}] = [\mathbf{R} | \mathbf{0}]$ for some $\mathbf{R} \in \mathbb{K}[X]^{i \times i}$. It remains to prove that $\mathbf{Q} = \mathbf{R} = \mathbf{P}^{(1)}$.

Since $\mathbf{R}\mathbf{F}_{[:i]} = 0 \bmod \mathfrak{m}$ and $\mathbf{R} = \mathbf{P}_{[:i,:i]}$ is in $\mathbf{s}^{(1)}$-Popov form, proving that all solutions $\mathbf{p} \in \mathbb{K}[X]^{1 \times i}$ for $(\mathfrak{m}, \mathbf{F}_{[:i]})$ are in the row space of $\mathbf{R}$ is enough to obtain $\mathbf{R} = \mathbf{P}^{(1)}$. Since $\mathbf{q} \in \mathbb{K}[X]^{1 \times m}$ defined by $[\mathbf{q}_{[:i]} | \mathbf{q}_{[i+1:]}] = [\mathbf{p} | \mathbf{0}]$ is a solution for $(\mathfrak{m}, \mathbf{F})$, $\mathbf{q} = \boldsymbol{\lambda}\mathbf{P}$ for some $\boldsymbol{\lambda} \in \mathbb{K}[X]^{1 \times m}$. Now $\mathbf{P}$ is nonsingular, thus $\mathbf{P}_{[:i,i+1:]} = \mathbf{0}$ implies that $[\boldsymbol{\lambda}_{[:i]} | \boldsymbol{\lambda}_{[i+1:]}] =$

$[\boldsymbol{\mu}|\mathbf{0}]$ with $\boldsymbol{\mu} \in \mathbb{K}[X]^{1\times i}$, hence $\mathbf{p} = \mathbf{q}_{[:i]} = \boldsymbol{\lambda}_{[:i]}\mathbf{P}_{[:i,:i]} + \boldsymbol{\lambda}_{[i+1:]}\mathbf{P}_{[i+1:,:i]} = \boldsymbol{\mu}\mathbf{Q}$. Similar arguments give $\mathbf{Q} = \mathbf{P}^{(1)}$. □

The next two lemmas show that knowing $\boldsymbol{\delta}^{(1)}$, which is $\boldsymbol{\delta}_{[:i]}$, allows us to compute a so-called *residual* $(\mathfrak{n}, \mathbf{G})$ from which we can complete the computation of $\boldsymbol{\delta}$ and $\mathbf{P}$.

Lemma 2.8. *Let* $\mathbf{s}^{(2)} = \mathbf{s}_{[i+1:]}$, $\mathbf{d} = -\boldsymbol{\delta}^{(1)} + \min(\mathbf{s}^{(2)}) - 2\sigma \in \mathbb{Z}^i$, $\mathbf{v} \in \mathbb{Z}^m$ *be such that* $[\mathbf{v}_{[:i]}|\mathbf{v}_{[i+1:]}] = [\mathbf{d}|\mathbf{s}^{(2)}]$, *and* $\mathbf{u} = (\mathbf{v}, \min(\mathbf{d})) \in \mathbb{Z}^{m+1}$. *Let* $\left[\begin{smallmatrix}\mathbf{A} & \mathbf{q}\\ \mathbf{p} & q\end{smallmatrix}\right]$ *be the* $\mathbf{u}$*-Popov order basis for* $[\mathbf{F}^\mathsf{T}|\mathfrak{m}]^\mathsf{T}$ *and* 2σ, *where* $\mathbf{A} \in \mathbb{K}[X]^{m\times m}$ *and* $q \in \mathbb{K}[X]$. *Then we have* $\deg(q) \geqslant \sigma$, $\mathbf{A}_{[:i,i+1:]} = \mathbf{0}$, $\mathbf{p}_{[i+1:]} = \mathbf{0}$, *and* $[\mathbf{A}_{[:i,:i]}|\mathbf{q}_{[:i]}] = [\mathbf{P}^{(1)}|\mathbf{q}^{(1)}]$ *with* $\mathbf{q}^{(1)} = -\mathbf{P}^{(1)}\mathbf{F}_{[:i]}/\mathfrak{m}$.

Proof. Since $\mathbf{u} = (\mathbf{v}, \min(\mathbf{v}))$ we have $\deg(\mathbf{p}) \leqslant \deg(q)$, and since $\deg(\mathbf{F}) < \deg(\mathfrak{m})$ the degree of $\mathbf{pF}+q\mathfrak{m}$ is $\deg(q)+\sigma$; then $\mathbf{pF}+q\mathfrak{m} = 0 \bmod X^{2\sigma}$ implies $\deg(q)+\sigma \geqslant 2\sigma$. Now, since $\mathbf{A}$ is in $\mathbf{v}$-Popov form and $\deg(\mathbf{A}) \leqslant 2\sigma - \deg(q) < 2\sigma$, from $\min(\mathbf{s}^{(2)}) \geqslant \max(\mathbf{d})+2\sigma$ we get $\mathbf{A}_{[:i,i+1:]} = \mathbf{0}$. Besides, $\mathbf{p}_{[i+1:]} = \mathbf{0}$ since either $\deg(q) < 2\sigma$ and then $\min(\mathbf{s}^{(2)}) > \min(\mathbf{d})+\deg(q)$, or $\mathbf{A}$ is the identity matrix and then $\mathbf{p} = \mathbf{0}$.

Furthermore, by Lemma 2.1 $[\mathbf{P}^{(1)}|\mathbf{q}^{(1)}]$ is the $(\mathbf{d}, \min(\mathbf{d}))$-Popov nullspace basis for $[\mathbf{F}_{[:i]}^\mathsf{T}|\mathfrak{m}]^\mathsf{T}$, with $(\mathbf{d}, \min(\mathbf{d}))$-pivot index $\{1, \ldots, i\}$, $(\mathbf{d}, \min(\mathbf{d}))$-pivot degree $\boldsymbol{\delta}^{(1)}$ and degree at most $\max(\boldsymbol{\delta}^{(1)})$. Then, as in the proof of Lemma 2.2, one can show that $[\mathbf{A}_{[:i,:i]}|\mathbf{q}_{[:i]}] = [\mathbf{P}^{(1)}|\mathbf{q}^{(1)}]$. □

Thus, up to row and column permutations this order basis is $\left[\begin{smallmatrix}\mathbf{P}^{(1)} & \mathbf{0} & \mathbf{q}^{(1)}\\ * & \mathbf{P}^{(2)} & *\\ * & \mathbf{0} & q\end{smallmatrix}\right]$ with $\mathbf{P}^{(2)} = \mathbf{A}_{[i+1:,i+1:]} \in \mathbb{K}[X]^{(m-i)\times(m-i)}$ in $\mathbf{s}^{(2)}$-Popov form; let $\boldsymbol{\delta}^{(2)}$ denote its $\mathbf{s}^{(2)}$-pivot degree.

Lemma 2.9. *Let* $\mathfrak{n} = X^{-2\sigma}(\mathbf{p}_{[i+1:]}\mathbf{F}_{[i+1:]} + q\mathfrak{m}) \in \mathbb{K}[X]$ *and* $\mathbf{G} = X^{-2\sigma}(\mathbf{A}_{[i+1:,:]}\mathbf{F} + \mathbf{q}_{[i+1:]}\mathfrak{m}) \in \mathbb{K}[X]^{(m-i)\times 1}$. *Then,* $\deg(\mathbf{G}) < \deg(\mathfrak{n}) \leqslant \sigma - |\boldsymbol{\delta}^{(1)}| - |\boldsymbol{\delta}^{(2)}|$. *Let* $\mathbf{P}^{(3)}$ *be the* $\mathbf{t}$*-Popov solution basis for* $(\mathfrak{n}, \mathbf{G})$ *with* $\mathbf{t} = \mathrm{rdeg}_{\mathbf{s}^{(2)}}(\mathbf{P}^{(2)})$ *and* $\boldsymbol{\delta}^{(3)}$ *be its* $\mathbf{t}$*-pivot degree. Then,* $(\boldsymbol{\delta}_{[:i]}, \boldsymbol{\delta}_{[i+1:]}) = (\boldsymbol{\delta}^{(1)}, \boldsymbol{\delta}^{(2)} + \boldsymbol{\delta}^{(3)})$.

Proof. The sum $|\boldsymbol{\delta}^{(1)}| + |\boldsymbol{\delta}^{(2)}| + \deg(q)$ of the $\mathbf{u}$-pivot degrees of $\left[\begin{smallmatrix}\mathbf{A} & \mathbf{q}\\ \mathbf{p} & q\end{smallmatrix}\right]$ is at most the order 2σ. Thus, we have $\deg(\mathfrak{n}) = \deg(q) - \sigma \leqslant \sigma - |\boldsymbol{\delta}^{(1)}| - |\boldsymbol{\delta}^{(2)}|$, $\deg(\mathbf{A}_{[i+1:,:i]}) < |\boldsymbol{\delta}^{(1)}| \leqslant \sigma$, $\deg(\mathbf{A}_{[i+1:,i+1:]}) \leqslant |\boldsymbol{\delta}^{(2)}| \leqslant \sigma$, and $\deg(\mathbf{q}_{[i+1:]}) < \deg(q)$. This implies $\deg(\mathbf{G}) < \deg(q) - \sigma = \deg(\mathfrak{n})$.

Let $\mathbf{q}^{(3)} = -\mathbf{P}^{(3)}\mathbf{G}/\mathfrak{n}$ and $t = \mathrm{rdeg}_{\mathbf{u}}([\mathbf{p}|q]) = \deg(q) + \min(\mathbf{d}) \leqslant \min(\mathbf{s}^{(2)}) \leqslant \min(\mathbf{t})$. By Lemma 2.1, $[\mathbf{P}^{(3)}|\mathbf{q}^{(3)}]$ is the $(\mathbf{t}, t)$-Popov nullspace basis for $[\mathbf{G}^\mathsf{T}|\mathfrak{n}]^\mathsf{T}$. Defining $\mathbf{B} \in \mathbb{K}[X]^{m\times m}$ and $\mathbf{c} \in \mathbb{K}[X]^{m\times 1}$ by $\left[\begin{smallmatrix}\mathbf{B}_{[:i,:i]} & \mathbf{B}_{[:i,i+1:]} & \mathbf{c}_{[:i]}\\ \mathbf{B}_{[i+1:,:i]} & \mathbf{B}_{[i+1:,i+1:]} & \mathbf{c}_{[i+1:]}\end{smallmatrix}\right] = \left[\begin{smallmatrix}\mathbf{I} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{P}^{(3)} & \mathbf{q}^{(3)}\end{smallmatrix}\right]$, then $\left[\begin{smallmatrix}\mathbf{B} & \mathbf{c}\end{smallmatrix}\right]\left[\begin{smallmatrix}\mathbf{A} & \mathbf{q}\\ \mathbf{p} & q\end{smallmatrix}\right]$ is a $\mathbf{u}$-minimal nullspace basis of $[\mathbf{F}^\mathsf{T}|\mathfrak{m}]^\mathsf{T}$ [36, Theorem 3.9]. Thus Lemma 2.1 implies that $\bar{\mathbf{P}} = \left[\begin{smallmatrix}\mathbf{B} & \mathbf{c}\end{smallmatrix}\right]\left[\begin{smallmatrix}\mathbf{A}\\ \mathbf{p}\end{smallmatrix}\right]$ is a $\mathbf{v}$-minimal solution basis for $(\mathfrak{m}, \mathbf{F})$.

It is easily checked that $\mathbf{P}$ is in $\mathbf{v}$-Popov form, so that the $\mathbf{v}$-Popov form of $\bar{\mathbf{P}}$ is $\mathbf{P}$ and its $\mathbf{v}$-pivot degree is $\boldsymbol{\delta}$. Besides $\left[\begin{smallmatrix}\bar{\mathbf{P}}_{[:i,:i]} & \bar{\mathbf{P}}_{[:i,i+1:]}\\ \bar{\mathbf{P}}_{[i+1:,:i]} & \bar{\mathbf{P}}_{[i+1:,i+1:]}\end{smallmatrix}\right] = \left[\begin{smallmatrix}\mathbf{P}^{(1)} & \mathbf{0}\\ \mathbf{P}^{(3)}\mathbf{A}_{2,1}+\mathbf{q}^{(3)}\mathbf{A}_{3,1} & \mathbf{P}^{(3)}\mathbf{P}^{(2)}\end{smallmatrix}\right]$, so that $(\boldsymbol{\delta}_{[:i]}, \boldsymbol{\delta}_{[i+1:]}) = (\boldsymbol{\delta}^{(1)}, \boldsymbol{\delta}^{(2)} + \boldsymbol{\delta}^{(3)})$ [21, Section 3]. □

This results in Algorithm 2. It takes as input α which dictates the amplitude of the subtuples that partition $\mathbf{s}$; as mentioned above, the initial call can be made with $\alpha = 2\sigma$.

Proposition 2.10. *Algorithm* PolModSysOne *is correct and uses* $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ *operations in* $\mathbb{K}$.

Proof. The correctness follows from the results in this subsection. By [21, Theorem 1.4], each leaf of the recursion at Step **1.a** in dimension m uses $\widetilde{\mathcal{O}}(m^{\omega-1}\alpha)$ operations.

Algorithm 2 (PolModSysOne).

Input: a polynomial $\mathfrak{m} \in \mathbb{K}[X]_{\neq 0}$ of degree σ, a column $\mathbf{F} \in \mathbb{K}[X]^{m\times 1}$ with $\deg(\mathbf{F}) < \deg(\mathfrak{m})$, a shift $\mathbf{s} \in \mathbb{Z}^m$, a parameter $\alpha \in \mathbb{Z}_{>0}$ with $\alpha \geqslant 2\sigma$.

Output: the $\mathbf{s}$-Popov solution basis for $(\mathfrak{m}, \mathbf{F})$ and the $\mathbf{s}$-minimal degree $\boldsymbol{\delta}$ of $(\mathfrak{m}, \mathbf{F})$.

1. If $\mathrm{amp}(\mathbf{s}) \leqslant 2\alpha$:
  - **a.** $\mathbf{A} \leftarrow$ the $(\mathbf{s}, \min(\mathbf{s}))$-Popov order basis for $[\mathbf{F}^\mathsf{T}|\mathfrak{m}]^\mathsf{T}$ and $2\alpha + 2\sigma$; return the principal $m\times m$ submatrix of $\mathbf{A}$ and the degrees of its diagonal entries

2. Else: /* $\ell = 1 + \lfloor \mathrm{amp}(\mathbf{s})/\alpha \rfloor \geqslant 3$ */
  - **a.** $(\mathbf{s}_1, \ldots, \mathbf{s}_\ell) \leftarrow$ Partition$(\mathbf{s}, \alpha)$,
    $j \leftarrow$ sum of the lengths of $\mathbf{s}_1, \ldots, \mathbf{s}_{\lceil \ell/2\rceil}$, $\mathbf{s}^{(0)} \leftarrow \mathbf{s}_{[:j]}$,
    $(\mathbf{P}^{(0)}, \boldsymbol{\delta}^{(0)}) \leftarrow$ PolModSysOne$(\mathfrak{m}, \mathbf{F}_{[:j]}, \mathbf{s}^{(0)}, \alpha)$
  - **b.** $i \leftarrow$ the largest splitting index for $(\boldsymbol{\delta}^{(0)}, \mathbf{s}^{(0)})$, $\boldsymbol{\delta}^{(1)} \leftarrow \boldsymbol{\delta}^{(0)}_{[:i]}$, $\mathbf{s}^{(2)} \leftarrow \mathbf{s}_{[i+1:]}$, $\mathbf{d} = -\boldsymbol{\delta}^{(1)} + \min(\mathbf{s}^{(2)}) - 2\sigma$, $\mathbf{v} \in \mathbb{Z}^m$ with $[\mathbf{v}_{[:i]}|\mathbf{v}_{[i+1:]}] \leftarrow [\mathbf{d}|\mathbf{s}^{(2)}]$, $\mathbf{u} = (\mathbf{v}, \min(\mathbf{d}))$
  - **c.** $\left[\begin{smallmatrix}\mathbf{A} & \mathbf{q}\\ \mathbf{p} & q\end{smallmatrix}\right] \leftarrow \mathbf{u}$-Popov order basis for $[\mathbf{F}^\mathsf{T}|\mathfrak{m}]^\mathsf{T}$ and 2σ,
    $\boldsymbol{\delta}^{(2)} \leftarrow$ the $\mathbf{s}^{(2)}$-pivot degree of $\mathbf{A}_{[i+1:,i+1:]}$
    $\mathbf{G} \leftarrow X^{-2\sigma}(\mathbf{A}_{[i+1:,:]}\mathbf{F} + \mathbf{q}_{[i+1:]}\mathfrak{m})$,
    $\mathfrak{n} \leftarrow X^{-2\sigma}(\mathbf{p}_{[i+1:]}\mathbf{F}_{[i+1:]} + q\mathfrak{m})$.
  - **d.** $\mathbf{t} \leftarrow \mathbf{s}^{(2)} + \boldsymbol{\delta}^{(2)} = \mathrm{rdeg}_{\mathbf{s}^{(2)}}(\mathbf{A}_{[i+1:,i+1:]})$,
    $(\mathbf{P}^{(3)}, \boldsymbol{\delta}^{(3)}) \leftarrow$ PolModSysOne$(\mathfrak{n}, \mathbf{G}, \mathbf{t}, \alpha)$
  - **e.** $\boldsymbol{\delta} \in \mathbb{N}^m$ with $(\boldsymbol{\delta}_{[:i]}, \boldsymbol{\delta}_{[i+1:]}) \leftarrow (\boldsymbol{\delta}^{(1)}, \boldsymbol{\delta}^{(2)} + \boldsymbol{\delta}^{(3)})$
    $\mathbf{P} \leftarrow$ KnownDegPolModSys$(\mathfrak{m}, \mathbf{F}, \mathbf{s}, \boldsymbol{\delta})$
  - **f.** Return $(\mathbf{P}, \boldsymbol{\delta})$

Running the algorithm with initial input $\alpha = 2\sigma$, the recursive tree has depth $\mathcal{O}(\log(\ell)) = \mathcal{O}(\log(1 + \mathrm{amp}(\mathbf{s})/2\sigma))$, with $\mathrm{amp}(\mathbf{s})/2\sigma \in \mathcal{O}(m^2)$ [21, Appendix A]. All recursive calls are for a modulus of degree $\sigma < \alpha$. The order basis computation at Step **2.c** uses $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ operations; the computation of $\mathbf{G}$ and $\mathfrak{n}$ at Step **2.c** can be done in time $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ using partial linearization as in Lemma 2.11 below; Step **2.e** uses $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ operations by Proposition 2.4.

On a given level of the tree, the sum of the dimensions of the column vector in input of each sub-problem is in $\mathcal{O}(m)$. Since $a^{\omega-1} + b^{\omega-1} \leqslant (a+b)^{\omega-1}$ for all $a, b > 0$, each level of the tree uses a total of $\widetilde{\mathcal{O}}(m^{\omega-1}\alpha)$ operations. □

2.3 Fast divide-and-conquer algorithm

Now that we have an efficient algorithm for $n = 1$, our main algorithm uses a divide-and-conquer approach on n. Similarly to [21, Algorithm 1], from the two bases obtained recursively we first deduce the $\mathbf{s}$-minimal degree $\boldsymbol{\delta}$, and then we use this knowledge to compute $\mathbf{P}$ with Algorithm 1. When $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n) \in \mathcal{O}(m)$, we rely on the algorithm LinearizationMIB in [20, Algorithm 9].

The computation of the so-called *residual* at Step **3.c** can be done efficiently using partial linearization, as follows.

Lemma 2.11. *Let* $\mathfrak{M} = (\mathfrak{m}_j)_j \in \mathbb{K}[X]^n_{\neq 0}$, $\mathbf{P} \in \mathbb{K}[X]^{m\times m}$, $\mathbf{F} \in \mathbb{K}[X]^{m\times n}$ *with* $m \geqslant n$ *and* $\deg(\mathbf{F}_{*,j}) < \sigma_j = \deg(\mathfrak{m}_j)$, *and let* $\sigma \geqslant m$ *such that* $\sigma \geqslant \sigma_1 + \cdots + \sigma_n$ *and* $|\mathrm{cdeg}(\mathbf{P})| \leqslant \sigma$. *Then* $\mathbf{PF} \bmod \mathfrak{M}$ *can be computed in* $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ *operations.*

Proof. Using notation from Lemma 2.3, we let $\widetilde{\mathbf{P}} \in \mathbb{K}[X]^{m\times\widetilde{m}}$ such that $\mathbf{P} = \widetilde{\mathbf{P}}\mathcal{E}$ and $\deg(\widetilde{\mathbf{P}}) < \lceil |\mathrm{cdeg}(\mathbf{P})|/m \rceil$. As above, $\widetilde{\mathbf{F}} = \mathcal{E}\mathbf{F} \bmod \mathfrak{M}$ can be computed in time $\widetilde{\mathcal{O}}(m\sigma)$. Here we want to compute $\mathbf{PF} \bmod \mathfrak{M} = \widetilde{\mathbf{P}}\,\widetilde{\mathbf{F}} \bmod \mathfrak{M}$.

Algorithm 3 (PolModSys).
Input: polynomials $\mathfrak{M} = (\mathfrak{m}_1, \ldots, \mathfrak{m}_n) \in \mathbb{K}[X]^n_{\neq 0}$, a matrix $\mathbf{F} \in \mathbb{K}[X]^{m \times n}$ with $\deg(\mathbf{F}_{*,j}) < \deg(\mathfrak{m}_j)$, a shift $\mathbf{s} \in \mathbb{Z}^m$.
Output: the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$ and the $\mathbf{s}$-minimal degree $\boldsymbol{\delta}$ of $(\mathfrak{M}, \mathbf{F})$.

1. If $\sigma = \deg(\mathfrak{m}_1) + \cdots + \deg(\mathfrak{m}_n) \leqslant m$:
  a. Build $\mathbf{E} \in \mathbb{K}^{m \times \sigma}$ and $\mathbf{M} \in \mathbb{K}^{\sigma \times \sigma}$ as in Section 1.2
  b. Return LinearizationMIB$(\mathbf{E}, \mathbf{M}, \mathbf{s}, 2^{\lceil \log_2(\sigma) \rceil})$
2. Else if $n = 1$: Return PolModSysOne$(\mathfrak{m}_1, \mathbf{F}, \mathbf{s}, 2\sigma)$
3. Else:
  a. $\mathfrak{M}^{(1)}, \mathbf{F}^{(1)} \leftarrow (\mathfrak{m}_1, \ldots, \mathfrak{m}_{\lfloor n/2 \rfloor}), \mathbf{F}_{*,1 \ldots \lfloor n/2 \rfloor}$
  $\mathfrak{M}^{(2)}, \mathbf{F}^{(2)} \leftarrow (\mathfrak{m}_{\lfloor n/2 \rfloor + 1}, \ldots, \mathfrak{m}_n), \mathbf{F}_{*,\lfloor n/2 \rfloor + 1 \ldots n}$
  b. $\mathbf{P}^{(1)}, \boldsymbol{\delta}^{(1)} \leftarrow$ PolModSys$(\mathfrak{M}^{(1)}, \mathbf{F}^{(1)}, \mathbf{s})$
  c. $\mathbf{R} \leftarrow \mathbf{P}^{(1)} \mathbf{F}^{(2)} \bmod \mathfrak{M}^{(2)}$
  d. $\mathbf{P}^{(2)}, \boldsymbol{\delta}^{(2)} \leftarrow$ PolModSys$(\mathfrak{M}^{(2)}, \mathbf{R}, \mathrm{rdeg}_{\mathbf{s}}(\mathbf{P}^{(1)}))$
  e. $\mathbf{P} \leftarrow$ KnownDegPolModSys$(\mathfrak{M}, \mathbf{F}, \mathbf{s}, \boldsymbol{\delta}^{(1)} + \boldsymbol{\delta}^{(2)})$
  f. Return $(\mathbf{P}, \boldsymbol{\delta}^{(1)} + \boldsymbol{\delta}^{(2)})$

We have $\deg(\widetilde{\mathbf{P}}) \leqslant \lceil \sigma/m \rceil \leqslant 2\sigma/m$. Since $|\mathrm{cdeg}(\widetilde{\mathbf{F}})| < \sigma$ and $n \leqslant m \leqslant \widetilde{m} \leqslant 2m$, $\widetilde{\mathbf{F}}$ can be partially linearized into $\mathcal{O}(m)$ columns of degree $\mathcal{O}(\sigma/m)$. Then, $\widetilde{\mathbf{P}}\,\widetilde{\mathbf{F}}$ is computed in $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ operations. The j-th column of $\widetilde{\mathbf{P}}\,\widetilde{\mathbf{F}}$ has $\widetilde{m} \leqslant 2m$ rows and degree less than $\sigma_j + 2\sigma/m$: it can be reduced modulo $\mathfrak{m}_j$ in $\widetilde{\mathcal{O}}(\sigma + m\sigma_j)$ operations [13, Chapter 9]; summing over $1 \leqslant j \leqslant n$ with $n \leqslant m$, this is in $\widetilde{\mathcal{O}}(m\sigma)$. □

Proof of Theorem 1.4. The correctness and the cost $\widetilde{\mathcal{O}}(m^{\omega-1}\sigma)$ for Steps **1** and **2** of Algorithm 3 follow from [20, Theorem 1.4] and Proposition 2.10. With the costs of Steps **3.c** and **3.e** given in Proposition 2.4 and Lemma 2.11, we obtain the announced cost bound.

Now, using notation in Step **3**, suppose $\mathbf{P}^{(1)}$ and $\mathbf{P}^{(2)}$ are the $\mathbf{s}$- and $\mathrm{rdeg}_{\mathbf{s}}(\mathbf{P}^{(1)})$-Popov solution bases for $(\mathfrak{M}^{(1)}, \mathbf{F}^{(1)})$ and $(\mathfrak{M}^{(2)}, \mathbf{R})$. Then $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$ is a solution basis for $(\mathfrak{M}, \mathbf{F})$: if $\mathbf{p}$ is a solution for $(\mathfrak{M}, \mathbf{F})$, it is one for $(\mathfrak{M}^{(1)}, \mathbf{F}^{(1)})$ and thus $\mathbf{p} = \boldsymbol{\lambda}\mathbf{P}^{(1)}$ for some $\boldsymbol{\lambda}$, and it is one for $(\mathfrak{M}^{(2)}, \mathbf{F}^{(2)})$ so that $\mathbf{p}\mathbf{F}^{(2)} = \boldsymbol{\lambda}\mathbf{P}^{(1)}\mathbf{F}^{(2)} = \boldsymbol{\lambda}\mathbf{R} = \mathbf{0} \bmod \mathfrak{M}^{(2)}$ and thus $\boldsymbol{\lambda} = \boldsymbol{\mu}\mathbf{P}^{(2)}$ for some $\boldsymbol{\mu}$; then $\mathbf{p} = \boldsymbol{\mu}\mathbf{P}^{(2)}\mathbf{P}^{(1)}$.

Then $\mathbf{P}^{(2)}\mathbf{P}^{(1)}$ is an $\mathbf{s}$-minimal solution basis for $(\mathfrak{M}, \mathbf{F})$ and its $\mathbf{s}$-Popov form has $\mathbf{s}$-pivot degree $\boldsymbol{\delta}^{(1)} + \boldsymbol{\delta}^{(2)}$ [21, Section 3]. The correctness follows from Proposition 2.4. □

3. FAST COMPUTATION OF THE SHIFTED POPOV FORM OF A MATRIX

3.1 Fast shifted Popov form algorithm

Our fast method for computing the $\mathbf{s}$-Popov form of a nonsingular $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ uses two steps, as follows.

1. Compute the Smith form of $\mathbf{A}$, giving the moduli $\mathfrak{M}$, and a corresponding right unimodular transformation, giving the equations $\mathbf{F}$, so that $\mathbf{A}$ is a solution basis for $(\mathfrak{M}, \mathbf{F})$.
2. Find the $\mathbf{s}$-Popov solution basis for $(\mathfrak{M}, \mathbf{F})$.

We first show the correctness of this approach.

Lemma 3.1. *Let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular and $\mathbf{S} = \mathbf{UAV}$ be the Smith form of $\mathbf{A}$ with $\mathbf{U}$ and $\mathbf{V}$ unimodular. Let $\mathfrak{M} \in \mathbb{K}[X]^m_{\neq 0}$ and $\mathbf{F} \in \mathbb{K}[X]^{m \times m}$ be such that $\mathbf{S} = \mathrm{diag}(\mathfrak{M})$ and $\mathbf{F} = \mathbf{V} \bmod \mathfrak{M}$. Then $\mathbf{A}$ is a solution basis for $(\mathfrak{M}, \mathbf{F})$.*

Proof. Let $\mathbf{p} \in \mathbb{K}[X]^{1 \times m}$. If $\mathbf{p}$ is in the row space of $\mathbf{A}$ then $\mathbf{p}$ is a solution for $(\mathfrak{M}, \mathbf{F})$ since $\mathbf{AV} = \mathbf{U}^{-1}\mathbf{S}$ with $\mathbf{U}^{-1}$ over $\mathbb{K}[X]$. Now if $\mathbf{pF} = 0 \bmod \mathfrak{M}$, then $\mathbf{pV} = \mathbf{qS}$ for some $\mathbf{q}$ and $\mathbf{p} = \mathbf{qUA}$ is in the row space of $\mathbf{A}$. □

Concerning the cost of Step **1**, such $\mathfrak{M}$ and $\mathbf{F}$ can be obtained in expected $\widetilde{\mathcal{O}}(m^\omega \deg(\mathbf{A}))$ operations, by computing

1.a $\mathbf{R}$ a row reduced form of $\mathbf{A}$ [16, Theorem 18],
1.b $\mathrm{diag}(\mathfrak{M})$ the Smith form of $\mathbf{R}$ [29, Algorithm 12],
1.c $(*, \mathbf{F})$ a reduced Smith transform for $\mathbf{R}$ [15, Figure 3.2];

as in [15, Figure 6.1], Steps **1.b** and **1.c** should be performed in conjunction with the preconditioning techniques detailed in [23]. One may take for $\mathfrak{M}$ only the nontrivial Smith factors, and for $\mathbf{F}$ only the nonzero columns of the transform.

The product of the moduli in $\mathfrak{M}$ is $\det(\mathbf{A})$ so that the sum of their degrees is $\deg(\det(\mathbf{A}))$. Then, according to Theorem 1.4, Step **2** of the algorithm outlined above costs $\widetilde{\mathcal{O}}(m^{\omega-1} \deg(\det(\mathbf{A})))$ operations. Thus this algorithm solves Problem 1 in expected $\widetilde{\mathcal{O}}(m^\omega \deg(\mathbf{A}))$ field operations.

3.2 Reducing to almost uniform degrees

In this subsection, we use the partial linearization techniques from [16, Section 6] to prove the following result.

Proposition 3.2. *Let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular and let $\mathbf{s} \in \mathbb{Z}^m$. With no field operation, one can build a nonsingular $\widetilde{\mathbf{A}} \in \mathbb{K}[X]^{\widetilde{m} \times \widetilde{m}}$ and a shift $\mathbf{u} \in \mathbb{Z}^{\widetilde{m}}$ such that $\widetilde{m} \leqslant 3m$, $\deg(\widetilde{\mathbf{A}}) \leqslant \lceil \sigma(\mathbf{A})/m \rceil$, and the $\mathbf{s}$-Popov form of $\mathbf{A}$ is the principal $m \times m$ submatrix of the $\mathbf{u}$-Popov form of $\widetilde{\mathbf{A}}$.*

With the algorithm in the previous subsection, this implies Theorem 1.3. In the specific case of Hermite form computation, for which there is a deterministic algorithm with cost bound $\widetilde{\mathcal{O}}(m^\omega \deg(\mathbf{A}))$ [35], one can verify that this leads to a *deterministic* algorithm using $\widetilde{\mathcal{O}}(m^\omega \lceil \sigma(\mathbf{A})/m \rceil)$ operations. (However, for $\mathbf{s} = \mathbf{0}$ this does not give a $\widetilde{\mathcal{O}}(m^\omega \lceil \sigma(\mathbf{A})/m \rceil)$ *deterministic* algorithm for the Popov form using [16, 28], since the corresponding $\mathbf{u}$ is $(\mathbf{0}, t, \ldots, t)$ with $t \geqslant \deg(\mathbf{A})$.)

Definition 3.3 (Column partial linearization). *Let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ and $\boldsymbol{\delta} = (\delta_i)_i \in \mathbb{N}^m$. Then let $\delta = 1 + \lfloor (\delta_1 + \cdots + \delta_m)/m \rfloor$, let $\alpha_i \geqslant 1$ and $0 \leqslant \beta_i < \delta$ be such that $\delta_i = (\alpha_i - 1)\delta + \beta_i$ for $1 \leqslant i \leqslant m$, let $\widetilde{m} = \alpha_1 + \cdots + \alpha_m$, and let $\mathcal{E} = [\mathbf{I} | \mathbf{E}^\mathsf{T}]^\mathsf{T} \in \mathbb{K}[X]^{\widetilde{m} \times m}$ be the expansion-compression matrix with $\mathbf{I}$ the identity matrix and*

$$\mathbf{E} = \begin{bmatrix} X^\delta & & \\ \vdots & & \\ X^{(\alpha_1 - 1)\delta} & & \\ & \ddots & \\ & & X^\delta \\ & & \vdots \\ & & X^{(\alpha_m - 1)\delta} \end{bmatrix}. \tag{4}$$

The column partial linearization $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A}) \in \mathbb{K}[X]^{\widetilde{m} \times \widetilde{m}}$ of $\mathbf{A}$ is defined as follows:

- *the first m rows of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ form the unique matrix $\widetilde{\mathbf{A}} \in \mathbb{K}[X]^{m \times \widetilde{m}}$ such that $\mathbf{A} = \widetilde{\mathbf{A}}\mathcal{E}$ and $\widetilde{\mathbf{A}}$ has all columns of degree less than δ except possibly those at indices $m + (\alpha_1 - 1) + \cdots + (\alpha_i - 1)$ for $1 \leqslant i \leqslant m$,*
- *for $1 \leqslant i \leqslant m$, the row $m + (\alpha_1 - 1) + \cdots + (\alpha_{i-1} - 1) + 1$ of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ is $[0, \ldots, 0, -X^\delta, 0, \ldots, 0, 1, 0, \ldots, 0]$ where $-X^\delta$ is at index i and 1 is on the diagonal,*

- *for $1 \leqslant i \leqslant m$ and $2 \leqslant j \leqslant \alpha_i - 1$, the row $m + (\alpha_1 - 1) + \cdots + (\alpha_{i-1} - 1) + j$ of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ is $[0, \ldots, 0, -X^{\delta}, 1, 0, \ldots, 0]$ where 1 is on the diagonal.*

Defining the *row partial linearization* $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$ of $\mathbf{A}$ similarly, both linearizations are related by $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A}) = \mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A}^{\mathsf{T}})^{\mathsf{T}}$.

Now we show that for a well-chosen $\mathbf{u}$, one can directly read the $\mathbf{s}$-Popov form of $\mathbf{A}$ as a submatrix of the $\mathbf{u}$-Popov form of $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$ (resp. $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$).

LEMMA 3.4. *Let $\mathbf{A} \in \mathbb{K}[X]^{m \times m}$ be nonsingular, $\mathbf{s} \in \mathbb{Z}^m$, $\mathbf{P}$ be the $\mathbf{s}$-Popov form of $\mathbf{A}$, and $\boldsymbol{\delta} \in \mathbb{N}^m$. We have that:*

(i) if $\widetilde{m}$ is the dimension of $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$ and $\mathbf{u} = (\mathbf{s}, t, \ldots, t)$ is in $\mathbb{Z}^{\widetilde{m}}$ with $t \geqslant \max(\mathbf{s}) + \deg(\mathbf{P})$, then the $\mathbf{u}$-Popov form of $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$ is $\begin{bmatrix} \mathbf{P} & \mathbf{0} \\ * & \mathbf{I} \end{bmatrix}$;

(ii) if $\widetilde{m}$ is the dimension of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$, $\mathbf{E}$ is as in (4), and $\mathbf{u} = (\mathbf{s}, \mathbf{t}) \in \mathbb{Z}^{\widetilde{m}}$ for any $\mathbf{t} \in \mathbb{Z}^{\widetilde{m}-m}$, then the $\mathbf{u}$-Popov form of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A}) \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{E} & \mathbf{I} \end{bmatrix}$ is $\begin{bmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{bmatrix}$;

(iii) if $\widetilde{m}$ is the dimension of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ and $\mathbf{u} = (\mathbf{s}, t, \ldots, t)$ is in $\mathbb{Z}^{\widetilde{m}}$ with $t \geqslant \max(\mathbf{s}) + \deg(\mathbf{P})$, then the $\mathbf{u}$-Popov form of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ is $\begin{bmatrix} \mathbf{P} & \mathbf{0} \\ * & \mathbf{I} \end{bmatrix}$.

PROOF. *(i)* $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$ is left-unimodularly equivalent to $\left[\begin{smallmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{B} & \mathbf{I} \end{smallmatrix}\right]$ for some $\mathbf{B} \in \mathbb{K}[X]^{(\widetilde{m}-m) \times m}$ [16, Theorem 10 (i)]. Then, let $\mathbf{R}$ be the remainder of $\mathbf{B}$ modulo $\mathbf{P}$, that is, the unique matrix in $\mathbb{K}[X]^{(\widetilde{m}-m) \times m}$ which has column degree bounded by the column degree of $\mathbf{P}$ componentwise and such that $\mathbf{R} = \mathbf{B} + \mathbf{Q}\mathbf{P}$ for some matrix $\mathbf{Q}$ (see for example [22, Theorem 6.3-15], noting that $\mathbf{P}$ is $\mathbf{0}$-column reduced).

Let $\mathbf{W}$ denote the unimodular matrix such that $\mathbf{P} = \mathbf{W}\mathbf{A}$. Then, $\left[\begin{smallmatrix} \mathbf{W} & \mathbf{0} \\ \mathbf{Q}\mathbf{W} & \mathbf{I} \end{smallmatrix}\right]\left[\begin{smallmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{B} & \mathbf{I} \end{smallmatrix}\right] = \left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{R} & \mathbf{I} \end{smallmatrix}\right]$ is left-unimodularly equivalent to $\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A})$. Besides, since $\deg(\mathbf{R}) < \deg(\mathbf{P})$, we have that $\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{R} & \mathbf{I} \end{smallmatrix}\right]$ is in $\mathbf{u}$-Popov form by choice of t.

(ii) The matrix $\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{smallmatrix}\right]$ is obviously in $\mathbf{u}$-Popov form: it remains to prove that it is left-unimodularly equivalent to $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})\left[\begin{smallmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{E} & \mathbf{I} \end{smallmatrix}\right]$. Let $\mathbf{T}$ denote the trailing principal submatrix $\mathbf{T} = \mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})_{m+1\ldots\widetilde{m}, m+1\ldots\widetilde{m}}$, and let $\mathbf{W}$ be the unimodular matrix such that $\mathbf{W}\mathbf{P} = \mathbf{A}$. Then, $\mathbf{T}$ is unit lower triangular, thus unimodular, and by construction of $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$, for some matrix $\mathbf{B}$ we have $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})\left[\begin{smallmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{E} & \mathbf{I} \end{smallmatrix}\right] = \left[\begin{smallmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{T} \end{smallmatrix}\right] = \left[\begin{smallmatrix} \mathbf{W} & \mathbf{B} \\ \mathbf{0} & \mathbf{T} \end{smallmatrix}\right]\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{smallmatrix}\right]$.

(iii) From *(ii)*, $\mathcal{L}^{\mathrm{c}}_{\boldsymbol{\delta}}(\mathbf{A})$ is left-unimodularly equivalent to $\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{smallmatrix}\right]\left[\begin{smallmatrix} \mathbf{I} & \mathbf{0} \\ -\mathbf{E} & \mathbf{I} \end{smallmatrix}\right] = \left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ -\mathbf{E} & \mathbf{I} \end{smallmatrix}\right]$. Using arguments in the proof of *(i)* above, by choice of t the $\mathbf{u}$-Popov form of $\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ -\mathbf{E} & \mathbf{I} \end{smallmatrix}\right]$ is $\left[\begin{smallmatrix} \mathbf{P} & \mathbf{0} \\ \mathbf{R} & \mathbf{I} \end{smallmatrix}\right]$ with $\mathbf{R}$ the remainder of $-\mathbf{E}$ modulo $\mathbf{P}$. □

In the usual case where $\deg(\mathbf{P})$ is not known *a priori*, one may choose t using the inequality $\deg(\mathbf{P}) \leqslant \deg(\det(\mathbf{P})) = \deg(\det(\mathbf{A})) \leqslant m \deg(\mathbf{A})$.

This result implies Proposition 3.2 thanks to the following remark from [16]. Let π_1, π_2 be permutation matrices such that $\mathbf{B} = \pi_1 \mathbf{A} \pi_2 = [b_{i,j}]_{ij}$ satisfies $\deg(b_{i,i}) \geqslant \deg(b_{j,k})$ for all $j, k \geqslant i$ and $1 \leqslant i \leqslant m$. Defining $\mathbf{d} = (d_i)_i \in \mathbb{N}^m$ by $d_i = \overline{\deg}(b_{i,i}) = \begin{cases} \deg(b_{i,i}) & \text{if } b_{i,i} \neq 0 \\ 0 & \text{otherwise} \end{cases}$, we have $d_1 + \cdots + d_m \leqslant \sigma(\mathbf{A})$ by definition of $\sigma(\mathbf{A})$ in (1). Let $\boldsymbol{\delta} = \pi_1^{-1}\mathbf{d}$, where $\mathbf{d}$ is seen as a column vector, and $\boldsymbol{\gamma} = \mathrm{cdeg}(\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A}))$. Then the matrix $\widetilde{\mathbf{A}} = \mathcal{L}^{\mathrm{c}}_{\boldsymbol{\gamma}}(\mathcal{L}^{\mathrm{r}}_{\boldsymbol{\delta}}(\mathbf{A}))$ is $\widetilde{m} \times \widetilde{m}$ with $\widetilde{m} < 3m$, and we have $\deg(\widetilde{\mathbf{A}}) \leqslant \lceil \sigma(\mathbf{A})/m \rceil$ [16, Corollary 3]. Lemma 3.4 further shows that the $\mathbf{s}$-Popov form of $\mathbf{A}$ is the principal $m \times m$ submatrix of the $\mathbf{u}$-Popov form of $\widetilde{\mathbf{A}}$, for the shift $\mathbf{u} = (\mathbf{s}, t, \ldots, t) \in \mathbb{Z}^{\widetilde{m}}$ with $t = \max(\mathbf{s}) + m\deg(\mathbf{A})$.

Acknowledgements. The author sincerely thanks the anonymous reviewers for their careful reading and detailed comments, which were very helpful for preparing the final version of this paper. He also thanks C.-P. Jeannerod, G. Labahn, É. Schost, A. Storjohann, and G. Villard for their interesting and useful comments. The author gratefully acknowledges financial support provided through the international mobility grants *Explo'ra Doc from Région Rhône-Alpes*, *PALSE*, and *Mitacs Globalink - Inria*.

4. REFERENCES

[1] M. Alekhnovich. Linear Diophantine equations over polynomials and soft decoding of Reed-Solomon codes. In *FOCS'02*, pages 439–448. IEEE, 2002.

[2] M. Alekhnovich. Linear Diophantine equations over polynomials and soft decoding of Reed-Solomon codes. *IEEE Trans. Inf. Theory*, 51(7):2257–2265, July 2005.

[3] B. Beckermann. A reliable method for computing M-Padé approximants on arbitrary staircases. *J. Comput. Appl. Math.*, 40(1):19–42, 1992.

[4] B. Beckermann and G. Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. *SIAM J. Matrix Anal. Appl.*, 15(3):804–823, July 1994.

[5] B. Beckermann and G. Labahn. Fraction-free computation of matrix rational interpolants and matrix gcds. *SIAM J. Matrix Anal. Appl.*, 22(1):114–144, 2000.

[6] B. Beckermann, G. Labahn, and G. Villard. Normal forms for general polynomial matrices. *J. Symbolic Comput.*, 41(6):708–737, 2006.

[7] P. Busse. *Multivariate List Decoding of Evaluation Codes with a Gröbner Basis Perspective*. PhD thesis, University of Kentucky, 2008.

[8] M. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster algorithms for multivariate interpolation with multiplicities and simultaneous polynomial approximations. *IEEE Trans. Inf. Theory*, 61(5):2370–2387, 2015.

[9] H. Cohn and N. Heninger. Approximate common divisors via lattices. In *Tenth Algorithmic Number Theory Symposium*, pages 271–293. Mathematical Sciences Publishers (MSP), 2012-2013.

[10] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *Advances in Mathematics of Communications*, 9(3):311–339, 2015.

[11] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Comput.*, 9(3):251–280, 1990.

[12] C. Devet, I. Goldberg, and N. Heninger. Optimally robust private information retrieval. Cryptology ePrint Archive, Report 2012/083, 2012.

[13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra (third edition)*. Cambridge University Press, 2013.

[14] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *ISSAC'03*, pages 135–142. ACM, 2003.

[15] S. Gupta. Hermite forms of polynomial matrices. Master's thesis, University of Waterloo, 2011.

[16] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $K[x]$. *J. Symbolic Comput.*, 47(4):422–453, 2012.

[17] S. Gupta and A. Storjohann. Computing Hermite forms of polynomial matrices. ISSAC'11, pages 155–162. ACM, 2011.

[18] J. L. Hafner and K. McCurley. Asymptotically fast triangularization of matrices over rings. *SIAM Journal on Computing*, 20(6):1068–1083, 1991.

[19] C. Hermite. Sur l'introduction des variables continues dans la théorie des nombres. *Journal für die reine und angewandte Mathematik*, 41:191–216, 1851.

[20] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Computing minimal interpolation bases. HAL Open archive - https://hal.inria.fr/hal-01241781, 2015.

[21] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Fast computation of minimal interpolation bases in Popov form for arbitrary shifts. HAL Open archive - https://hal.inria.fr/hal-01265983, 2016.

[22] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

[23] E. Kaltofen, M.S. Krishnamoorthy, and D. Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra Appl.*, 136:189–208, 1990.

[24] S. Lang. *Algebra (Revised Third Edition)*. Springer-Verlag New-York Inc., 2002.

[25] F. Le Gall. Powers of tensors and fast matrix multiplication. In *ISSAC'14*, pages 296–303. ACM, 2014.

[26] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comput.*, 35:377–401, 2003.

[27] V. M. Popov. Invariant description of linear, time-invariant controllable systems. *SIAM Journal on Control*, 10(2):252–264, 1972.

[28] S. Sarkar and A. Storjohann. Normalization of row reduced matrices. In *ISSAC'11*, pages 297–304. ACM, 2011.

[29] A. Storjohann. High-order lifting and integrality certification. *J. Symbolic Comput.*, 36(3-4):613–648, 2003.

[30] A. Storjohann. Notes on computing minimal approximant bases. In *Dagstuhl Seminar Proceedings*, 2006.

[31] A. Storjohann and G. Labahn. Asymptotically fast computation of Hermite normal forms of integer matrices. ISSAC'96, pages 259–266. ACM, 1996.

[32] M. Van Barel and A. Bultheel. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numer. Algorithms*, 3:451–462, 1992.

[33] G. Villard. Computing Popov and Hermite forms of polynomial matrices. ISSAC'96, pages 250–258. ACM, 1996.

[34] W. Zhou and G. Labahn. Efficient algorithms for order basis computation. *J. Symbolic Comput.*, 47(7):793–819, 2012.

[35] W. Zhou and G. Labahn. A fast, deterministic algorithm for computing a Hermite normal form of a polynomial matrix. arXiv e-Print archive - http://arxiv.org/abs/1602.02049, 2016.

[36] W. Zhou, G. Labahn, and A. Storjohann. Computing minimal nullspace bases. In *ISSAC'12*, pages 366–373. ACM, 2012.

[37] W. Zhou, G. Labahn, and A. Storjohann. A deterministic algorithm for inverting a polynomial matrix. *J. Complexity*, 31(2):162–173, 2015.