
This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Noferini, Vanni; van Dooren, Paul

Revisiting the matrix polynomial greatest common divisor

Published in:
SIAM Journal on Matrix Analysis and Applications

DOI:
[10.1137/22M1531993](https://doi.org/10.1137/22M1531993)

Published: 01/01/2023

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Noferini, V., & van Dooren, P. (2023). Revisiting the matrix polynomial greatest common divisor. *SIAM Journal on Matrix Analysis and Applications*, 44(3), 1164-1188. <https://doi.org/10.1137/22M1531993>

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

REVISITING THE MATRIX POLYNOMIAL GREATEST COMMON DIVISOR*

VANNI NOFERINI[†] AND PAUL VAN DOOREN[‡]

Abstract. In this paper, we revisit the greatest common right divisor (GCRD) extraction from a set of polynomial matrices $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, with coefficients in a generic field \mathbb{F} and with common column dimension n . We give necessary and sufficient conditions for a matrix $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ to be a GCRD using the Smith normal form of the $m \times n$ compound matrix $P(\lambda)$ obtained by concatenating $P_i(\lambda)$ vertically, where $m = \sum_{i=1}^k m_i$. We also describe the complete set of degrees of freedom for the solution $G(\lambda)$, and we link it to the Smith form and Hermite form of $P(\lambda)$. We then give an algorithm for constructing a particular minimum size solution for this problem when $\mathbb{F} = \mathbb{C}$ or \mathbb{R} , using state-space techniques. This new method works directly on the coefficient matrices of $P(\lambda)$, using orthogonal transformations only. The method is based on the staircase algorithm, applied to a particular pencil derived from a generalized state-space model of $P(\lambda)$.

Key words. polynomial matrix, greatest common divisor, Hermite normal form, Smith normal form, generalized state-space, staircase algorithm

MSC codes. 15A22, 15A24, 65F45, 93-08, 93B52

DOI. 10.1137/22M1531993

1. Introduction. The notions of a common right divisor (CRD) and of a greatest common right divisor (GCRD) of a set of polynomial matrices is a natural extension of the analogous concepts for scalar polynomials. As commutativity is lost in the matrix case, one needs first to specify on which side (right or left) the common divisor should lie. The following definition of CRDs and GCRDs is classical [14, 16, 30]; while [14, 16] only consider the field of complex numbers \mathbb{C} , the same definition is in fact still valid when \mathbb{F} is any arbitrary field [30].

DEFINITION 1.1 (common right divisor and greatest common right divisor). *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices all having the same number of columns. We say that $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ is a common right divisor (CRD) of the set $\{P_i(\lambda)\}_{i=1}^k$ if it is a right divisor of each $P_i(\lambda)$, i.e., if there exist polynomial matrices $Q_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times p}$, $i = 1, \dots, k$, such that $P_i(\lambda) = Q_i(\lambda)D(\lambda)$ for all $i = 1, \dots, k$. Furthermore, $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is said to be a greatest common right divisor (GCRD) of the set $\{P_i(\lambda)\}_{i=1}^k$ if, for every CRD $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ of the same set, $D(\lambda)$ is a right divisor of $G(\lambda)$, i.e., there exist a polynomial matrix $Q(\lambda) \in \mathbb{F}[\lambda]^{\ell \times p}$ such that $G(\lambda) = Q(\lambda)D(\lambda)$.*

Even though Definition 1.1 applies to any nonempty set of polynomial matrices $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$ with the same number of columns n , the authors of [14, 16, 30]

*Received by the editors November 1, 2022; accepted for publication (in revised form) April 11, 2023; published electronically August 8, 2023.

<https://doi.org/10.1137/22M1531993>

Funding: The work of the first author was supported by Academy of Finland (Suomen Akatemian päätös) grant 331240. The work of the second author was supported by the Aalto Science Institute Visitor Programme.

[†]Department of Mathematics and Systems Analysis, Aalto University, FI-00076, Aalto, Finland (vanni.noferini@aalto.fi).

[‡]Department of Mathematical Engineering, Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium (vandooren.p@gmail.com).

immediately restrict their discussion of the problem by assuming (at least) that the compound matrix

$$(1.1) \quad P(\lambda) := \begin{bmatrix} P_1(\lambda) \\ \vdots \\ P_k(\lambda) \end{bmatrix} \in \mathbb{F}[\lambda]^{m \times n}, \quad m := \sum_{i=1}^k m_i,$$

has full normal rank n and the GCRD is square (and therefore $n \times n$) and nonsingular. This simplification is crucial in the design of several of the existing algorithms since they do not extend to the rank deficient case. Once a GCRD has been found, the polynomial factors $Q_i(\lambda)$ of Definition 1.1 are said to be *right coprime* [1], meaning that they only have common right divisors with a trivial Smith form (i.e., with elementary divisors 1). In the case where (1.1) has full normal rank, this in turn implies that the square CRDs of the coprime matrices $Q_i(\lambda)$ must be unimodular.

As mentioned above, there is obviously a dual problem of finding a greatest common left divisor (GCLD) for a set of polynomial matrices all having the same number of rows, but since it is obvious that the latter can be reduced to the GCRD extraction simply by transposing all the defining equations, we restrict ourselves in this paper to the right factor extraction. One of the main applications of GCRD and GCLD extraction (for $\mathbb{F} = \mathbb{C}$ or \mathbb{R}) is the reduction of polynomial system quadruples $\{A(\lambda), B(\lambda), C(\lambda), D(\lambda)\}$ to minimal quadruples. These polynomial quadruples were introduced by Rosenbrock [23] in linear system theory and have recently become of interest also in the context of nonlinear eigenvalue problems; see, e.g., [6, 8, 20] and the references therein. Such system quadruples are a minimal representation of the (rational) transfer function $R(\lambda) := C(\lambda)A(\lambda)^{-1}B(\lambda) + D(\lambda)$ provided the pairs $\{-A(\lambda), C(\lambda)\}$ and $\{-A(\lambda), B(\lambda)\}$ are right and left coprimes, respectively. In these system quadruples, $A(\lambda)$ is always assumed to be invertible over the field of fractions $\mathbb{F}(\lambda)$, implying that the compound matrices $\begin{bmatrix} -A(\lambda) \\ C(\lambda) \end{bmatrix}, \begin{bmatrix} -A(\lambda) & B(\lambda) \end{bmatrix}$ have automatically full column and row rank, respectively. If the system quadruple $\{A(\lambda), B(\lambda), C(\lambda), D(\lambda)\}$ is not minimal, one can obtain a minimal one by extracting a GCRD of the pair $\{-A(\lambda), C(\lambda)\}$, followed by the computation of a GCLD of the (updated) pair $\{-A(\lambda), B(\lambda)\}$ [4]. Other relevant applications, for which the compound matrix (1.1) may also be rank deficient, include nonsingular factorizations of polynomial matrices [9, 18] or coprimeness tests for polynomial matrices [18]. It is therefore not surprising that the GCRD and GCLD extraction problem has been extensively studied in the systems theory literature [16]. Furthermore, the problem of computing a GCRD (or GCLD) is also mathematically interesting per se and has been well studied in the matrix theory literature, with particular emphasis on its connection with Sylvester or Bézout resultant matrices [12, 13, 14, 17, 19]. Nevertheless, most of the numerical algorithms that we could find in the literature are designed for the full rank case only [3, 9, 14, 16, 24] and their extension to the rank deficient case is not discussed; the only exception seems to be [15]. We also mention that recently the related (but distinct) problem of computing an *approximate* GCRD has received attention [10], but again under the full rank assumption.

The present manuscript has two goals. On the one hand, we review and extend the theory of GCRDs, paying particular attention to the non-full rank case that apparently has received little to no attention in the existing literature. Our description is built on the Hermite and Smith normal forms and thus is similar in spirit (while making much weaker assumptions) to the approach of the control theory literature [16, 30] but significantly differs from the approach based on common restrictions described

in [14] and the references therein. On the other hand, for $\mathbb{F} = \mathbb{C}$ or \mathbb{R} , we propose a new algorithm for the computation of a GCRD that is based on generalized state-space realizations. The new algorithm is inspired by previous approaches based on state-space realizations [9, 24], but it differs from them in (a) using generalized state-space realizations, thus being able to accept as input any nonempty set of polynomial matrices with the same number of columns with no further restriction, and (b) relying on the staircase algorithm [25], which is numerically stable.

The organization of the paper is as follows. In section 2, we recall the theory of polynomial matrices with coefficients over any arbitrary field, needed to define correctly greatest common divisors and their connection to the Smith normal form and the Hermite normal form of $P(\lambda)$. We also develop a comprehensive list of properties that such greatest common right divisors must have and how any generic GCRD can be derived from a particular, minimal-size solution that we label a *compact GCRD*. We then restrict our attention to the case $\mathbb{F} = \mathbb{C}$ or \mathbb{R} , with the aim of developing a numerical algorithm. In section 3, we recall useful properties of state-space realizations and feedback and show that feedback can be interpreted as a factorization of a given transfer function. In section 4, we then extend these ideas to generalized state-space realizations of a general polynomial matrix $P(\lambda)$ and show how to use this to compute a compact GCRD of $P(\lambda)$. Section 5 then discusses numerical aspects of GCRD algorithms and gives numerical experiments illustrating our new algorithm. We end this paper with some concluding remarks in section 6.

2. Theory of greatest common right divisors. In this section, we review and extend the theory of GCRDs; some of the results that we give are to our knowledge new, while others appeared in the literature (see, e.g., [14, 16, 30] and the references therein) but sometimes under additional assumptions that we have relaxed or removed. In particular, we establish the existence of a GCRD of any nonempty set of polynomial matrices with the same number of columns, as well as its uniqueness up to fixing the number of rows and up to left multiplication by a unimodular matrix. We start with an obvious, but useful, lemma. It relies on Definition 1.1, given earlier.

LEMMA 2.1. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices, and suppose that $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$. Suppose, moreover, that $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. If $G(\lambda)$ is a right divisor of $D(\lambda)$, then $D(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$.*

Proof. By assumption there is a polynomial matrix $A(\lambda)$ such that $D(\lambda) = A(\lambda)G(\lambda)$. Let $C(\lambda)$ be any CRD of $\{P_i(\lambda)\}_{i=1}^k$; then, since $G(\lambda)$ is a GCRD of the same set, $G(\lambda) = Q(\lambda)C(\lambda)$ for some polynomial matrix $Q(\lambda)$. It follows that $D(\lambda) = A(\lambda)Q(\lambda)C(\lambda)$, showing that $C(\lambda)$ divides $D(\lambda)$ and hence that $D(\lambda)$ is a GCRD of the given set. \square

The next result provides a lower bound on the row size of a right CRD.

LEMMA 2.2. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices, and suppose that $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Then, $p \geq r$, where $r = \text{rank } P(\lambda)$ is the normal rank of the compound matrix (1.1).*

Proof. Since $D(\lambda)$ is a CRD of the given set, there must exist a polynomial matrix $N(\lambda) \in \mathbb{F}[\lambda]^{m \times p}$ such that $P(\lambda) = N(\lambda)D(\lambda)$. It follows that $r = \text{rank } P(\lambda) \leq \text{rank } D(\lambda) \leq p$. \square

Lemma 2.2 justifies the following definition.

DEFINITION 2.3. Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices, and suppose that their compound matrix (1.1) has rank r . Then, any GCRD (resp., CRD) $G(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is called a compact GCRD (resp., compact CRD) of the set $\{P_i(\lambda)\}_{i=1}^k$.

From now on, we will assume that $r \geq 1$. This is essentially no loss of generality, for if $r = 0$, then $P_i(\lambda)$ are all zero matrices, and the problem of extracting a GCRD is trivial: $G(\lambda)$ is a GCRD of theirs if and only if it is a zero matrix with the same number of columns as the $P_i(\lambda)$.

PROPOSITION 2.4. Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices, and suppose that their compound matrix $P(\lambda)$ as in (1.1) has rank $r \geq 1$. If $G(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is a compact GCRD of $\{P_i(\lambda)\}_{i=1}^k$, then $G(\lambda)$ has full row rank.

Proof. From the equation $P(\lambda) = N(\lambda)G(\lambda)$ we have $r \leq \text{rank } G(\lambda)$. □

In a sense, it is natural to restrict ourselves to compact GCRDs, because, as we will see below, any other GCRD can be constructed from them. However, it is conceivable that there are scenarios where the number ℓ of rows of a GCRD $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is strictly greater than r ; for instance, it may be natural to take $\ell = n$, thus studying square GCRDs, even if $n > r$. For this reason, we will also study the case $\ell > r$.

2.1. Background on normal forms of polynomial matrices. Recall that a square polynomial matrix is said to be regular if it is invertible over the field of fractions $\mathbb{F}(\lambda)$, that is, if its determinant is a nonzero polynomial; and it is said to be a unimodular matrix if it is invertible over the ring $\mathbb{F}[\lambda]$, that is, if its determinant is a nonzero constant. Moreover, a polynomial matrix $N(\lambda)$, not necessarily square, is called left (resp., right) invertible if there is a polynomial matrix $L(\lambda)$ such that $L(\lambda)N(\lambda) = I$ (resp., $N(\lambda)L(\lambda) = I$). More precisely, the previous property defines left (resp., right) invertibility over the ring $\mathbb{F}[\lambda]$. Occasionally, we will also refer to the weaker property of being left (resp., right) invertible over the field of fractions $\mathbb{F}(\lambda)$, which means that there is a possibly rational matrix $L(\lambda)$ such that $L(\lambda)N(\lambda) = I$ (resp., $N(\lambda)L(\lambda) = I$).

To further develop the theory of GCRDs, we will make extensive use of the Smith normal form and the Hermite normal form of a polynomial matrix. We recall them below.

THEOREM 2.5 (Smith normal form). For any polynomial matrix $P(\lambda) \in \mathbb{F}[\lambda]^{m \times n}$, there exist unimodular matrices $U(\lambda) \in \mathbb{F}[\lambda]^{m \times m}$ and $V(\lambda) \in \mathbb{F}[\lambda]^{n \times n}$ such that $P(\lambda) = U(\lambda)S(\lambda)V(\lambda)$ and

$$S(\lambda) := \left[\begin{array}{ccc|c} s_1(\lambda) & & & 0 \\ & \ddots & & \\ & & s_r(\lambda) & 0 \\ \hline & & 0 & 0 \end{array} \right] \in \mathbb{F}[\lambda]^{m \times n}$$

contains r monic polynomials $s_i(\lambda)$ on diagonal and zeros for the rest. The elements $s_i(\lambda)$ form a divisibility chain

$$s_1(\lambda) | s_2(\lambda) | \dots | s_r(\lambda),$$

and r is the normal rank of $P(\lambda)$. The matrix $S(\lambda)$ is called the Smith normal form of $P(\lambda)$ and is uniquely determined by $P(\lambda)$ [11, Theorem 1.14.1 and Normalization 1.14.4].

Occasionally in this paper we will use a *compact* Smith form as well. It is obtained by just deleting the last $n-r$ rows of $V(\lambda)$ and the last $m-r$ columns of $U(\lambda)$, as well as by keeping only the top-left $r \times r$ submatrix of $S(\lambda)$, thus yielding the decomposition $P(\lambda) = \hat{U}(\lambda)\hat{S}(\lambda)\hat{V}(\lambda)$, where $\hat{U}(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$ is left invertible, $\hat{S}(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ is square, regular, and in Smith normal form, and $\hat{V}(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is right invertible. When $r = n$, the right matrix $\hat{V}(\lambda) = V(\lambda)$ is still square and unimodular.

THEOREM 2.6 (Hermite normal form). *For any polynomial matrix $P(\lambda) \in \mathbb{F}[\lambda]^{m \times n}$, there exists a unimodular matrix $U(\lambda) \in \mathbb{F}[\lambda]^{m \times m}$ such that $P(\lambda) = U(\lambda)H(\lambda)$ and $H(\lambda) \in \mathbb{F}[\lambda]^{m \times n}$ satisfies the following properties:*

- *It is in row echelon form, and its zero rows (if any) are located below its nonzero rows (if any).*
- *The pivot (leftmost nonzero element) of each nonzero row is a monic polynomial, and it is located strictly to the right of the pivots of the rows above.*
- *All elements below a pivot are zero, and all the elements above a pivot are monic polynomials of degree strictly less than the pivot below.*
- *The number of its nonzero rows is r , the normal rank of $P(\lambda)$.*

The matrix $H(\lambda)$ is called the Hermite normal form of $P(\lambda)$ and is uniquely determined by $P(\lambda)$ [11, Theorem 1.12.7 and Corollary 1.12.11].

When $m > r$, the bottom $m-r$ rows of $H(\lambda)$ are necessarily zero and one can then rewrite the decomposition $P(\lambda) = U(\lambda)H(\lambda)$ in the *compact* form $P(\lambda) = \tilde{U}(\lambda)\tilde{H}(\lambda)$, where $\tilde{U}(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$ is obtained by just deleting the rightmost $m-r$ columns of $U(\lambda)$ (and is therefore left invertible), and $\tilde{H}(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is obtained by deleting the $m-r$ bottom rows of $H(\lambda)$, which are zero. Moreover, it follows from Theorem 2.6 that if $r = \text{rank } P(\lambda) = n$, then $\tilde{H}(\lambda)$ is square upper triangular and invertible.

2.2. Properties of greatest common right divisors. We are now ready to further develop our analysis of the problem of finding a GCRD of a set of polynomial matrices. First, we show that there is no loss of generality in restricting ourselves to the case where $m := \sum_{i=1}^k m_i \geq n$.

LEMMA 2.7. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i < n$. Moreover, let $\delta = n - m$ and define $P_{k+1}(\lambda) := 0_{\delta \times n}$. Then, $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$ if and only if it is a GCRD of $\{P_i(\lambda)\}_{i=1}^{k+1}$.*

Proof. Suppose first that $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^{k+1}$. Then, for $i = 1, \dots, k+1$ there are $Q_i(\lambda)$ such that $P_i(\lambda) = Q_i(\lambda)G(\lambda)$, implying that $G(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. If it was not a GCRD of the latter set, then such a set would admit another CRD $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ that is not a right divisor of $G(\lambda)$. In particular, $P_i(\lambda) = R_i(\lambda)D(\lambda)$ for all $i = 1, \dots, k$. But clearly $P_{k+1}(\lambda) = 0_{\delta \times p} \cdot D(\lambda)$, and hence $D(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^{k+1}$ contradicting that $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^{k+1}$.

Conversely, suppose that $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$. Then, for $i = 1, \dots, k$ there are $Q_i(\lambda)$ such that $P_i(\lambda) = Q_i(\lambda)G(\lambda)$, and obviously $P_{k+1}(\lambda) = 0_{\delta \times \ell} \cdot G(\lambda)$, thus showing that $G(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^{k+1}$. If we suppose for a contradiction that $G(\lambda)$ is not a GCRD of the latter set, then we could find a CRD $D(\lambda)$ of $\{P_i(\lambda)\}_{i=1}^{k+1}$ that is not a right divisor of $G(\lambda)$. But, following the argument above, then such $D(\lambda)$ would also be a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Hence, we easily reach the contradiction that $G(\lambda)$ cannot possibly be a GCRD of $\{P_i(\lambda)\}_{i=1}^k$ either. \square

Next, we characterize the right null space of a GCRD.

LEMMA 2.8. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i \geq n$, and define their compound*

matrix $P(\lambda)$ as in (1.1). If $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$, then $\ker G(\lambda) \subseteq \ker P(\lambda)$. If $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$, then $\ker G(\lambda) = \ker P(\lambda)$.

Proof. It is clear that $\ker G(\lambda) \subseteq \ker P(\lambda)$ whenever $G(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Indeed, due to the relation $P_i(\lambda) = Q_i(\lambda)G(\lambda)$ which is valid for all $i = 1, \dots, k$, we have that every vector $v(\lambda)$ in the null space of $G(\lambda)$ is also in the null space of $P_i(\lambda)$ for all i , and hence $v(\lambda)$ also belongs to the null space of $P(\lambda)$. Now suppose that $G(\lambda)$ is a GCRD and consider a compact Smith decomposition $P(\lambda) = \hat{U}(\lambda)\hat{S}(\lambda)\hat{V}(\lambda)$ where $\hat{U}(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$ is left invertible, $\hat{S}(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ is in Smith form, and $\hat{V}(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is right invertible. By construction, $\hat{S}(\lambda)\hat{V}(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$, and hence it is a right divisor of $G(\lambda)$. It follows that $\text{rank } G(\lambda) \leq \text{rank } \hat{S}(\lambda)\hat{V}(\lambda) = \text{rank } \hat{S}(\lambda) = \text{rank } P(\lambda)$. Hence, $\dim \ker G(\lambda) = \dim \ker P(\lambda)$ and therefore $\ker G(\lambda) = \ker P(\lambda)$. \square

We now state Theorem 2.9, one of the main results of this section, implying among other things the existence of a GCRD of any given nonempty set of polynomial matrices all with the same number of columns (thus far in our analysis we have merely assumed that a GCRD always exists, taking the risk to have been pondering about the empty set). For convenience of exposition, however, we will first prove Theorem 2.9 under the assumption that (1.1) has full column rank, i.e., $n = r$ using the notation above. Later, we will show how to remove this assumption.

THEOREM 2.9. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i \geq n$, and let $P(\lambda)$ be their compound matrix as in (1.1). Assume that $r = \text{rank } P(\lambda) \geq 1$. Then, the following are equivalent:*

1. $G(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is a compact GCRD of $\{P_i(\lambda)\}_{i=1}^k$.
2. There exists a left invertible polynomial matrix $N(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$ such that $P(\lambda) = N(\lambda)G(\lambda)$.
3. There exists a unimodular matrix $U(\lambda) \in \mathbb{F}[\lambda]^{m \times m}$ such that

$$P(\lambda) = U(\lambda) \begin{bmatrix} G(\lambda) \\ 0 \end{bmatrix}.$$

Moreover, any compact GCRD $G(\lambda)$ of $\{P_i(\lambda)\}_{i=1}^k$ can always be expressed as a (left) linear combination

$$G(\lambda) = \sum_{i=1}^k L_i(\lambda)P_i(\lambda)$$

for some polynomial matrices $L_i(\lambda) \in \mathbb{F}[\lambda]^{r \times m_i}$; equivalently, there is a polynomial matrix $L(\lambda) \in \mathbb{F}[\lambda]^{r \times m}$ such that $G(\lambda) = L(\lambda)P(\lambda)$.

Proof of Theorem 2.9 in the case where $r = n$.

- 1 \Rightarrow 2 Since $G(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$, there must exist matrices $N_i(\lambda)$ satisfying $P_i(\lambda) = N_i(\lambda)G(\lambda)$ for each i . Defining $N(\lambda) := \begin{bmatrix} N_1(\lambda) \\ \vdots \\ N_k(\lambda) \end{bmatrix}$, then by construction $P(\lambda) = N(\lambda)G(\lambda)$. Consider the compact Hermite decomposition $N(\lambda) = U(\lambda)H(\lambda)$ where $U(\lambda)$ is left invertible and $H(\lambda)$ is square upper triangular. It follows that $H(\lambda)G(\lambda)$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Hence, there exists some polynomial matrix $A(\lambda)$ such that $G(\lambda) = A(\lambda)H(\lambda)G(\lambda)$. However, by Lemma 2.8 and by the assumption that $P(\lambda)$ has full column rank, $\ker G(\lambda) = \{0\}$ and hence $A(\lambda)H(\lambda) = I$. It follows that $H(\lambda) = A(\lambda)^{-1}$ is unimodular and thus $N(\lambda)$ is left invertible.

- 2 ⇒ 3 By, e.g., [1, Theorem 3.3], since $N(\lambda)$ is left invertible, it has a trivial Smith form and hence it is completable to a unimodular matrix $U(\lambda)$. The sought implication follows immediately.
- 3 ⇒ 1 Partition

$$U(\lambda) = \begin{bmatrix} N_1(\lambda) & U_1(\lambda) \\ \vdots & \vdots \\ N_k(\lambda) & U_k(\lambda) \end{bmatrix}, \quad U(\lambda)^{-1} = \begin{bmatrix} L_1(\lambda) & \dots & L_k(\lambda) \\ V_1(\lambda) & \dots & V_k(\lambda) \end{bmatrix}$$

and define $N(\lambda) := \begin{bmatrix} N_1(\lambda) \\ \vdots \\ N_k(\lambda) \end{bmatrix}$ so that $P(\lambda) = N(\lambda)G(\lambda)$. In turn, this implies $P_i(\lambda) = N_i(\lambda)G(\lambda)$, and hence it is clear that $G(\lambda)$ is a CRD of the set $\{P_i(\lambda)\}_{i=1}^k$. On the other hand,

$$\begin{bmatrix} G(\lambda) \\ 0 \end{bmatrix} = U(\lambda)^{-1}P(\lambda) \Rightarrow G(\lambda) = \sum_{i=1}^k L_i(\lambda)P_i(\lambda).$$

Hence, it is clear that if $D(\lambda)$ is any CRD of $\{P_i(\lambda)\}_{i=1}^k$, then it must also be a right divisor of $G(\lambda)$. Therefore, $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$. Finally, we note that the proof above, and in particular the argument to show that condition 3 implies condition 1, also implies the last statement. □

Since a unimodular matrix $U(\lambda)$ and a square matrix $G(\lambda)$ satisfying condition 3 can always be found—for example via the compact Hermite form of $P(\lambda)$ or the Smith form of $P(\lambda)$ —the proof above establishes the existence of a GCRD in the case where the compound matrix (1.1) has full column rank. We now proceed to explore the case where the compound matrix does not have full column rank n . In particular, finding compact GCRDs in this case can be reduced to the full column rank case.

THEOREM 2.10. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i \geq n$, and let $P(\lambda)$ be their compound matrix as in (1.1). Suppose that $V(\lambda) \in \mathbb{F}[\lambda]^{n \times n}$ is a unimodular matrix such that $P(\lambda)V(\lambda) = \begin{bmatrix} Q(\lambda) & 0_{m \times (n-r)} \end{bmatrix}$, where*

$$Q(\lambda) = \begin{bmatrix} Q_1(\lambda) \\ \vdots \\ Q_k(\lambda) \end{bmatrix} \in \mathbb{F}[\lambda]^{m \times r}$$

with $Q_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times r}$, $i = 1, \dots, k$, and $r = \text{rank } P(\lambda) = \text{rank } Q(\lambda)$. Then, $D(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ is a compact GCRD of $\{Q_i(\lambda)\}_{i=1}^k$ if and only if $G(\lambda)$ is a compact GCRD of $\{P_i(\lambda)\}_{i=1}^k$, where

$$(2.1) \quad G(\lambda) = U(\lambda) \begin{bmatrix} D(\lambda) & 0 \end{bmatrix} V(\lambda)^{-1} \in \mathbb{F}[\lambda]^{r \times n},$$

and $U(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ is an arbitrary unimodular polynomial matrix.

Before proving Theorem 2.10, we note that the existence of a unimodular matrix $V(\lambda)$ and a full column rank polynomial matrix $Q(\lambda)$ with the sought properties is clear, for example, from the Smith form of $P(\lambda)$.

Proof of Theorem 2.10. Suppose first that $D(\lambda)$ is a compact GCRD of $\{Q_i(\lambda)\}_{i=1}^k$, and write (by Theorem 2.9) $Q(\lambda) = N(\lambda)D(\lambda)$ for some left invertible

$N(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$. Then, it is immediate that $P(\lambda) = N(\lambda) [D(\lambda) \ 0] V(\lambda)^{-1} = N(\lambda)U(\lambda)^{-1}G(\lambda)$, so $G(\lambda)$ is a compact CRD of $\{P_i(\lambda)\}_{i=1}^k$. Now let $A(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ be any other CRD of the same set, so that $P(\lambda) = M(\lambda)A(\lambda)$ for some (not necessarily left invertible) $M(\lambda) \in \mathbb{F}[\lambda]^{m \times p}$. If we let $L(\lambda) \in \mathbb{F}[\lambda]^{r \times m}$ be a left inverse of $N(\lambda)$, then $D(\lambda) = L(\lambda)Q(\lambda)$ and therefore

$$G(\lambda) = U(\lambda)L(\lambda) [Q(\lambda) \ 0_{m \times (n-r)}] V(\lambda)^{-1} = U(\lambda)L(\lambda)P(\lambda).$$

Hence, we have $G(\lambda) = U(\lambda)L(\lambda)M(\lambda)A(\lambda)$. This shows that $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$.

For the reverse implication, we first need to show that any compact GCRD $G(\lambda)$ of $\{P_i(\lambda)\}_{i=1}^k$ must have the form (2.1) for some polynomial matrix $D(\lambda)$ and some unimodular matrix $U(\lambda)$. By Lemma 2.8, $\ker G(\lambda) = \text{span} \left\{ V(\lambda) \begin{bmatrix} 0 \\ I_{n-r} \end{bmatrix} \right\}$. Hence, necessarily such a compact GCRD $G(\lambda)$ must have the form

$$G(\lambda) = [X(\lambda) \ 0] V(\lambda)^{-1}$$

for some appropriate polynomial matrix $X(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$. However, obviously, we can write $X(\lambda) = U(\lambda)D(\lambda)$ for some $r \times r$ unimodular matrix $U(\lambda)$ and some $r \times r$ polynomial matrix $D(\lambda)$ (just take $U(\lambda)$ arbitrarily and define $D(\lambda) := U(\lambda)^{-1}X(\lambda)$). Hence, we may assume that $G(\lambda)$ indeed has the form (2.1).

On the other hand, since $G(\lambda)$ is a compact GCRD of $\{P_i(\lambda)\}_{i=1}^k$, then $P(\lambda) = M(\lambda)G(\lambda)$ for some $M(\lambda) \in \mathbb{F}[\lambda]^{n \times r}$. It follows that $D(\lambda)$ is a CRD of $\{Q_i(\lambda)\}_{i=1}^k$, because (2.1) then implies $Q(\lambda) = M(\lambda)U(\lambda)D(\lambda)$. Now let $A(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ be any compact GCRD of $\{Q_i(\lambda)\}_{i=1}^k$ (the existence of $A(\lambda)$ is guaranteed by the proof of Theorem 2.9 for the case of a full column rank compound matrix since $Q(\lambda)$ has full column rank). By the first part of this proof, $H(\lambda) := [A(\lambda) \ 0] V(\lambda)^{-1} \in \mathbb{F}[\lambda]^{r \times n}$ is then a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Hence, there is a polynomial matrix $W(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ such that $G(\lambda) = W(\lambda)H(\lambda)$. Therefore, $D(\lambda) = U(\lambda)^{-1}W(\lambda)A(\lambda)$, which shows that $A(\lambda)$ is a right divisor of $D(\lambda)$, and hence $D(\lambda)$ is a GCRD of $\{Q_i(\lambda)\}_{i=1}^k$ by Lemma 2.1. \square

We are now ready to prove that Theorem 2.9 still holds even if we remove the assumption that the compound matrix $P(\lambda)$ has full column rank. By the comments that we have made above, establishing Theorem 2.9 in the most general case implies in particular that a compact GCRD exists for any given nonempty set of polynomial matrices all with the same number of columns.

Proof of Theorem 2.9 in the case where $\text{rank } P(\lambda) = r < n$. In our proof for the case $r = n$, we only used such an assumption in showing that condition 1 implies condition 2. Let us give another proof of the same implication but this time assuming that $P(\lambda)$ has rank $r < n$. Then, by Theorem 2.10, $G(\lambda)$ has the form $U(\lambda) [G_c(\lambda) \ 0] V(\lambda)^{-1}$ where $P(\lambda)V(\lambda) = [Q(\lambda) \ 0]$, $Q(\lambda)$ has full column rank r , and, by Theorem 2.9, $Q(\lambda) = N(\lambda)G_c(\lambda)$ for a left invertible $N(\lambda)$ and a compact square GCRD $G_c(\lambda)$. Then,

$$P(\lambda) = [Q(\lambda) \ 0] V(\lambda)^{-1} = N(\lambda) [G_c(\lambda) \ 0] V(\lambda)^{-1} = N(\lambda)U(\lambda)^{-1}G(\lambda),$$

which proves the statement since $N(\lambda)U(\lambda)^{-1}$ is by construction left invertible. \square

The next step is to show how to construct an arbitrary GCRD from a compact GCRD.

COROLLARY 2.11. *Let $\{P_i(\lambda)\}_{i=1}^k$, with $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i \geq n$, and define their*

compound matrix $P(\lambda)$ as in (1.1). If $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$, then $\text{rank } G(\lambda) = r = \text{rank } P(\lambda)$.

Proof. By Theorem 2.9, there exists a compact GCRD $G_c(\lambda)$ of the given set, and by Proposition 2.4, $\text{rank } G_c(\lambda) = r$. On the other hand, by Lemma 2.8, $\ker G(\lambda) = \ker G_c(\lambda)$. Thus, by the rank-nullity theorem, $\text{rank } G(\lambda) = n - \dim \ker G(\lambda) = n - \dim \ker G_c(\lambda) = r$. \square

THEOREM 2.12. *Let $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices such that $m := \sum_{i=1}^k m_i \geq n$, let $P(\lambda)$ be their compound matrix as in (1.1), and assume $r = \text{rank } P(\lambda) \geq 1$. Then, $G_c(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$ is a compact GCRD of $\{P_i(\lambda)\}_{i=1}^k$ if and only if $G(\lambda)$ is a GCRD of $\{P_i(\lambda)\}_{i=1}^k$, where*

$$(2.2) \quad G(\lambda) = Z(\lambda) \begin{bmatrix} G_c(\lambda) \\ 0 \end{bmatrix} \in \mathbb{F}[\lambda]^{\ell \times n}, \quad \ell \geq r,$$

and $Z(\lambda) \in \mathbb{F}[\lambda]^{\ell \times \ell}$ is an arbitrary unimodular matrix, Moreover, any GCRD $G(\lambda)$ of $\{P_i(\lambda)\}$ can always be expressed as a (left) linear combination

$$G(\lambda) = \sum_{i=1}^k L_i(\lambda) P_i(\lambda)$$

for some polynomial matrices $L_i(\lambda) \in \mathbb{F}[\lambda]^{\ell \times m_i}$; equivalently, there is a polynomial matrix $L(\lambda) \in \mathbb{F}[\lambda]^{\ell \times m}$ such that $G(\lambda) = L(\lambda)P(\lambda)$

Proof. Suppose first that $G_c(\lambda)$ is a compact GCRD of the given set. This implies that $P(\lambda) = N(\lambda)G_c(\lambda)$ for some $N(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$. Hence,

$$P(\lambda) = \begin{bmatrix} N(\lambda) & 0_{m \times (\ell-r)} \end{bmatrix} Z(\lambda)^{-1} G(\lambda),$$

and thus $G(\lambda)$ is a CRD of the same set. On the other hand, $G(\lambda) = Z_\ell(\lambda)G_c(\lambda)$, where $Z_\ell(\lambda) \in \mathbb{F}[\lambda]^{\ell \times r}$ contains the leftmost r columns of $Z(\lambda)$, and hence $G(\lambda)$ is a GCRD by Lemma 2.1.

For the reverse implication, let us first check that any GCRD $G(\lambda)$ must have the form (2.2). By the definition of GCRD, there are matrix polynomials $A(\lambda) \in \mathbb{F}[\lambda]^{r \times \ell}$, $B(\lambda) \in \mathbb{F}[\lambda]^{\ell \times r}$ such that $G_c(\lambda) = A(\lambda)G(\lambda)$ and $G(\lambda) = B(\lambda)G_c(\lambda)$. Hence, $G_c(\lambda) = A(\lambda)B(\lambda)G_c(\lambda)$; but $G_c(\lambda)$ has a right inverse over the field of fractions $\mathbb{F}(\lambda)$ by Proposition 2.4, and thus $A(\lambda)B(\lambda) = I_r$. It follows that $B(\lambda)$ is left invertible over the ring of polynomials $\mathbb{F}[\lambda]$, and hence by [1, Theorem 3.3] it holds that $B(\lambda) = Z(\lambda) \begin{bmatrix} I_r \\ 0 \end{bmatrix}$ for some unimodular $Z(\lambda) \in \mathbb{F}[\lambda]^{\ell \times \ell}$, as sought.

Suppose now that $G(\lambda)$ as in (2.2) is a GCRD of the given set. Then, $P(\lambda) = M(\lambda)G(\lambda)$ for some $M(\lambda) \in \mathbb{F}[\lambda]^{m \times \ell}$, implying $P(\lambda) = M(\lambda)Z_\ell(\lambda)G_c(\lambda)$, where $Z_\ell(\lambda) \in \mathbb{F}[\lambda]^{\ell \times r}$ contains the leftmost r columns of $Z(\lambda)$: this shows that $G_c(\lambda)$ is a compact CRD of $\{P_i(\lambda)\}_{i=1}^k$. By Theorem 2.9, there exists a compact GCRD of the same set, say, $D_c(\lambda) \in \mathbb{F}[\lambda]^{r \times n}$. Hence, by the first part of this proof, $D(\lambda) = \begin{bmatrix} D_c(\lambda) \\ 0_{(\ell-r) \times n} \end{bmatrix} \in \mathbb{F}[\lambda]^{\ell \times n}$ is a CRD of $\{P_i(\lambda)\}_{i=1}^k$. Thus, since $G(\lambda)$ is a GCRD, we have $G(\lambda) = X(\lambda)D(\lambda)$ for some $X(\lambda) \in \mathbb{F}[\lambda]^{\ell \times \ell}$. Hence,

$$G_c(\lambda) = \begin{bmatrix} I_r & 0 \end{bmatrix} Z(\lambda)^{-1} X(\lambda) \begin{bmatrix} I_r \\ 0 \end{bmatrix} D_c(\lambda),$$

proving that $G_c(\lambda)$ is a GCRD by Lemma 2.1.

It remains to prove the last part of the statement. Using Theorem 2.9, we know that any compact GCRD can be expressed as a left linear combination, say, $G_c(\lambda) =$

$\sum_{i=1}^k M_i(\lambda)P_i(\lambda)$. Therefore, if $G(\lambda)$ is a GCRD, then for some unimodular $Z(\lambda)$ and some compact GCRD $G_c(\lambda)$ it holds that

$$G(\lambda) = Z(\lambda) \begin{bmatrix} \sum_{i=1}^k M_i(\lambda)P_i(\lambda) \\ 0 \end{bmatrix} = \sum_{i=1}^k \left(Z(\lambda) \begin{bmatrix} M_i(\lambda) \\ 0 \end{bmatrix} \right) P_i(\lambda),$$

and the statement follows by defining $L_i(\lambda) := Z(\lambda) \begin{bmatrix} M_i(\lambda) \\ 0 \end{bmatrix}$. □

Remark 2.13. Note that, by applying simultaneously Theorems 2.10 and 2.12, we have that a generic GCRD of $\{P_i(\lambda)\}_{i=1}^k$, such that $P(\lambda)$ as in (1.1) has rank $r \geq 1$, must have the form

$$G(\lambda) = U(\lambda) \begin{bmatrix} D(\lambda) & 0 \\ 0 & 0 \end{bmatrix} V(\lambda)^{-1} \in \mathbb{F}[\lambda]^{\ell \times n},$$

where the following hold:

- $U(\lambda) \in \mathbb{F}[\lambda]^{\ell \times \ell}$ is an arbitrary unimodular matrix.
- $V(\lambda) \in \mathbb{F}[\lambda]^{n \times n}$ is a unimodular matrix such that $P(\lambda)V(\lambda) = \begin{bmatrix} Q(\lambda) & 0_{m \times (n-r)} \end{bmatrix}$, where $Q(\lambda) \in \mathbb{F}[\lambda]^{m \times r}$ has full column rank.
- $D(\lambda) \in \mathbb{F}[\lambda]^{r \times r}$ is a square and compact (and hence regular) GCRD of $\{Q_i(\lambda)\}_{i=1}^k$, defined as in Theorem 2.10.

Satisfying the properties above is, indeed, a sufficient and necessary condition for being a GCRD.

It is obvious by the definition of a GCRD that if $G(\lambda)$ is a GCRD of a given set of polynomial matrices $\{P_i(\lambda)\}$ and $U(\lambda)$ is a unimodular matrix, then $U(\lambda)G(\lambda)$ is also a GCRD for the same set. In fact, once we have fixed the number of rows of a GCRD, these are the only possible degrees of freedom in determining a GCRD, in the sense that a reverse implication holds. This fact was stated in the literature but only for the full column rank case; combining it with Theorem 2.12, it characterizes the set of all possible GCRDs.

THEOREM 2.14. *Let $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, be a nonempty set of polynomial matrices, and suppose that $G_1(\lambda), G_2(\lambda)$ are two GCRDs of this set such that $G_1(\lambda)$ and $G_2(\lambda)$ have the same number of rows. Then, $G_1(\lambda) = U(\lambda)G_2(\lambda)$ for some unimodular $U(\lambda)$.*

Proof. Note first that, by the definition of GCRD, there are polynomial matrices $A(\lambda), B(\lambda)$ such that $G_1(\lambda) = A(\lambda)G_2(\lambda)$ and $G_2(\lambda) = B(\lambda)G_1(\lambda)$. Suppose first that $G_1(\lambda)$ and $G_2(\lambda)$ are compact GCRDs. Then, by Lemma 2.8, $G_1(\lambda)$ is right invertible over the field of fractions $\mathbb{F}(\lambda)$. Hence, $G_1(\lambda) = A(\lambda)B(\lambda)G_1(\lambda)$ implies that $I = A(\lambda)B(\lambda)$ so that both $A(\lambda)$ and $B(\lambda)$ must be unimodular; in particular, taking $U(\lambda) := A(\lambda)$ proves the statement in this case.

If instead the two GCRDs are not compact, by Theorem 2.12 we have that $G_i(\lambda)$ must have the form

$$G_i(\lambda) = Z_i(\lambda) \begin{bmatrix} R_i(\lambda) \\ 0 \end{bmatrix}$$

for all $i = 1, 2$, where $Z_1(\lambda)$ and $Z_2(\lambda)$ and $V(\lambda)$ are unimodular, whereas $R_1(\lambda), R_2(\lambda)$ are compact GCRDs of the same set. By the first part of this proof, there exists a unimodular matrix $V(\lambda)$ such that $R_1(\lambda) = V(\lambda)R_2(\lambda)$. Thus,

$$G_1(\lambda) = Z_1(\lambda) \begin{bmatrix} V(\lambda) & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} R_2(\lambda) \\ 0 \end{bmatrix} = Z_1(\lambda) \begin{bmatrix} V(\lambda) & 0 \\ 0 & I \end{bmatrix} Z_2(\lambda)^{-1} G_2(\lambda),$$

which concludes the proof since $U(\lambda) := Z_1(\lambda)(V(\lambda) \oplus I)Z_2(\lambda)^{-1}$ is unimodular. \square

Remark 2.15. It follows from Theorem 2.9 that any compact GCRD satisfies $P(\lambda) = N(\lambda)G_c(\lambda)$, where $N(\lambda)$ is left invertible. Hence, any compact GCRD $G_c(\lambda)$ must contain all the finite eigenvalues of $P(\lambda)$ since the rank drops of $P(\lambda)$ must occur in the right factor $G_c(\lambda)$. Moreover, by Theorem 2.12, every GCRD $G(\lambda)$ is unimodularly left-equivalent to $\begin{bmatrix} G_c(\lambda) \\ 0 \end{bmatrix}$, where $G_c(\lambda)$ is a compact GCRD. Thus, more generally, any (not necessarily) compact GCRD $G(\lambda)$ must contain all the finite eigenvalues of $P(\lambda)$. In addition, Lemma 2.8 shows that $G(\lambda)$ must also contain all the right minimal indices of $P(\lambda)$. Any compact GCRD $G_c(\lambda)$ has the additional property to have full row rank r , and therefore it has no left minimal indices. Moreover, the additional degree of freedom of a left unimodular factor $U(\lambda)$ yields a compact GCRD $U(\lambda)G_c(\lambda)$ that can be made row proper and therefore has no zeros at infinity in the sense of McMillan (see [16]). (We note that a row proper polynomial matrix may still have infinite eigenvalues in the sense of Gohberg, Lancaster, and Rodman [14].)

Remark 2.16. Let $\mathbb{F} \subseteq \mathbb{K}$ be a field extension, and suppose that $D(\lambda) \in \mathbb{F}[\lambda]^{p \times n}$ is a CRD (resp., compact CRD) of a set of polynomial matrices $P_i(\lambda) \in \mathbb{F}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$. It is then obvious, by Definition 1.1 and by the invariance of the rank under field extensions, that $D(\lambda)$ is also a CRD (resp., compact CRD) of the same set of polynomial matrices, when seen as polynomial matrices in $\mathbb{K}[\lambda]^{m_i \times n}$. Moreover, it follows from Theorems 2.9 and 2.12 that if $G(\lambda) \in \mathbb{F}[\lambda]^{\ell \times n}$ is a GCRD (resp., compact GCRD) over $\mathbb{F}[\lambda]$, it is also a GCRD (resp., compact GCRD) over $\mathbb{K}[\lambda]$.

For example, let us consider the case $\mathbb{F} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$. The theory we developed shows that every nonempty set of real polynomial matrices $P_i(\lambda) \in \mathbb{R}[\lambda]^{m_i \times n}$, $i = 1, \dots, k$, has a real GCRD $G(\lambda) \in \mathbb{R}[\lambda]^{\ell \times n}$ for all $\ell \geq r$, where $r = \text{rank } P(\lambda)$ in (1.1); the observations above additionally show that such $G(\lambda)$ is also a complex GCRD, i.e., a GCRD for the same $P_i(\lambda)$ seen as complex polynomial matrices. Moreover, by Theorem 2.14, any other real GCRD with the same number of rows has the form $U(\lambda)G(\lambda)$ where $U(\lambda) \in \mathbb{R}[\lambda]^{\ell \times \ell}$ is a real unimodular matrix; and any other complex GCRD with the same number of rows has the form $V(\lambda)G(\lambda)$ where $V(\lambda) \in \mathbb{C}[\lambda]^{\ell \times \ell}$ is a complex unimodular matrix. As a consequence, if one has computed a complex non-real GCRD for a given set of real polynomial matrices, it is always possible to obtain a real GCRD for the same set by some appropriate left unimodular multiplication.

3. State-space realizations and feedback. In this section and the following ones, we restrict our attention to the case where the base field \mathbb{F} is the field of complex numbers \mathbb{C} , with the goal of developing and testing a novel numerical algorithm. The case $\mathbb{F} = \mathbb{R}$ is analogous, but one has to rely on the real staircase form; for simplicity of exposition, we just focus on the complex case.

Before describing the new algorithm for GCRD extraction of a polynomial matrix, we briefly recall the properties of (generalized and classical) state-space realizations and the effect of feedback on them. Since only proper transfer functions have a standard state-space realization, one either has to make use of a generalized state-space or pencil realization, or one has to perform a change of variables $\lambda = 1/\mu$ to then realize $P(1/\mu)$ in standard state-space form. In [9, 24], an approach to computing GCRDs based on state-space realization and feedback was described, but there an assumption was made that (1.1) has full rank. Those methods were based on the

notion of (A, B) -invariant subspaces [31], which required the use of state-space models. In this section, we first recall those ideas, using the method described in [24].

Our starting point is an expansion of the compound matrix (1.1) in the monomial basis $P(\lambda) =: P_0 + P_1\lambda + \dots + P_d\lambda^d$, where d is the degree of (1.1). A pencil realization of $P(\lambda)$ is a quintuple of matrices A, B, C, D, E such that the system matrix of $P(\lambda)$ is given by

$$S_\lambda(\lambda) := \left[\begin{array}{c|c} A - \lambda E & \lambda B \\ \hline C & D \end{array} \right], \quad P(\lambda) = C(\lambda E - A)^{-1}\lambda B + D.$$

Note that $P(\lambda)$ is the Schur complement of its system matrix $S_\lambda(\lambda)$ with respect to the (invertible) leading submatrix $A - \lambda E$. A classical solution for this is given by the companion-like form

$$(3.1) \quad S_\lambda(\lambda) = \left[\begin{array}{cccc|c} I_n & -\lambda I_n & & & \\ & I_n & -\lambda I_n & & \\ & & \ddots & \ddots & \\ & & & I_n & -\lambda I_n \\ \hline P_d & \dots & \dots & P_2 & P_1 & -\lambda I_n \\ & & & & & P_0 \end{array} \right].$$

The pencil realization (3.1) is also *irreducible* since neither the submatrix $\left[\begin{array}{c|c} A - \lambda E & \lambda B \end{array} \right]$ nor the submatrix $[A - \lambda E | \lambda B]$ has any finite Smith zeros [23, 29].

Remark 3.1. It is well known that there exist unimodular transformations $U(\lambda)$ and $V(\lambda)$ such that

$$U(\lambda)S_\lambda(\lambda)V(\lambda) = \left[\begin{array}{c|c} I_{dn} & \\ \hline & P(\lambda) \end{array} \right].$$

This shows clearly that the Smith zeros of $P(\lambda)$ are also those of $S_\lambda(\lambda)$ and that the pencil $S_\lambda(\lambda)$ has normal rank $dn + r$. In other words, $S_\lambda(\lambda)$ is a linearization of $P(\lambda)$ [14] and it can be used to compute the finite zeros of $P(\lambda)$ via the staircase algorithm, followed by the QZ algorithm.

If we use the change of variables $\lambda = 1/\mu$, then a standard state-space realization of

$$P(1/\mu) = P_0 + P_1/\mu + \dots + P_d/\mu^d$$

is given by the following system matrix:

$$(3.2) \quad S_\mu(\mu) := \left[\begin{array}{c|c} \mu I_{dn} - A & -B \\ \hline C & D \end{array} \right] := \left[\begin{array}{cccc|c} \mu I_n & -I_n & & & \\ & \mu I_n & -I_n & & \\ & & \ddots & \ddots & \\ & & & \mu I_n & -I_n \\ \hline P_d & \dots & \dots & P_2 & P_1 & -I_n \\ & & & & & P_0 \end{array} \right],$$

which is not observable if $\text{rank } P_d$ is smaller than n , but it is controllable. We will see that controllability suffices for our purpose. The relation $S_\lambda(\lambda) = (\lambda I_{dn} \oplus I_m)S_\mu(\mu)$ also shows that (3.1) and (3.2) have the same normal rank. If we assume that P_0 has

full column rank, then $P(\lambda)$ has full normal rank n , $P(\lambda)$ and $S_\lambda(\lambda)$ have no zeros at $\lambda=0$, and $P(1/\mu)$ and $S_\mu(\mu)$ have no zeros at $\mu=\infty$.

Theorem 3.2 below describes a decomposition that holds for the system matrix $S_\mu(\mu)$, under the assumption that P_0 has full rank n . This approach is essentially described in the papers [9, 24], but the present derivation avoids elaborate system theoretic concepts. The full rank assumption implies that the method proposed in [9, 24] can only be applied to the case where (1.1) has full column rank (up to a linear change of variables $\lambda \mapsto \lambda - \alpha$, this can be assumed to be equivalent to a full rank P_0). The main advantage of the standard state-space model for $P(1/\mu)$ is that it has only four matrices $\{A, B, C, D\}$ and that subsequent transformations of the model are simpler. It also shows that the construction of a particular feedback solves the GCRD extraction problem.

THEOREM 3.2. *Let P_0 have full column rank n , and let $\left[\begin{array}{c|c} \mu I_{dn} - A & -B \\ \hline C & D \end{array} \right]$ be as in (3.2). Then, there exist a unitary transformation $U \in \mathbb{C}^{dn \times dn}$ and a “feedback” matrix $F \in \mathbb{C}^{n \times dn}$ such that*

$$(3.3) \quad \left[\begin{array}{cc|c} \mu I_{d_f} - \hat{A}_{11} & -\tilde{A}_{12} & -B_1 \\ 0 & \mu I_{d_0} - \tilde{A}_{22} & -B_2 \\ \hline 0 & \tilde{C}_2 & D \end{array} \right] := \left[\begin{array}{c|c} U^* & 0 \\ \hline 0 & I_m \end{array} \right] S_\mu(\mu) \left[\begin{array}{c|c} U & 0 \\ \hline F & I_n \end{array} \right],$$

where \hat{A}_{11} is square and contains the d_f finite eigenvalues of the pencil $S_\mu(\mu)$, \tilde{A}_{22} is square and has its $d_0 = dn - d_f$ eigenvalues at 0, and the pair $(\tilde{A}_{22}, (I_m - P_0 P_0^\dagger) \tilde{C}_2)$ is observable.

Proof. The proof is constructive. Apply the feedback

$$\hat{F} := \left[\hat{F}_d \quad \dots \quad \hat{F}_1 \right] := -P_0^\dagger \left[P_d \quad \dots \quad P_1 \right] = -P_0^\dagger C$$

and define the matrices \hat{A} and \hat{C} as

$$\hat{A} := A + B\hat{F}, \quad \hat{C} := C + D\hat{F} = (I_m - P_0 P_0^\dagger) \left[P_d \quad \dots \quad P_1 \right] = (I_m - P_0 P_0^\dagger) C$$

to obtain the new system matrix

$$\left[\begin{array}{c|c} \mu I_{dn} - \hat{A} & -B \\ \hline \hat{C} & D \end{array} \right] := S_\mu(\mu) \left[\begin{array}{c|c} I_{dn} & 0 \\ \hline \hat{F} & I_n \end{array} \right].$$

Now compute the orthogonal state-space transformation U that displays the d_f unobservable modes of the pair (\hat{A}, \hat{C}) in a submatrix \hat{A}_{11} as follows [26]:

$$\left[\begin{array}{cc|c} \mu I_{d_f} - \hat{A}_{11} & -\hat{A}_{12} & -B_1 \\ 0 & \mu I_{d_0} - \hat{A}_{22} & -B_2 \\ \hline 0 & \hat{C}_2 & D \end{array} \right] := \left[\begin{array}{c|c} U^* & 0 \\ \hline 0 & I_m \end{array} \right] \left[\begin{array}{c|c} \mu I_{dn} - \hat{A} & -B \\ \hline \hat{C} & D \end{array} \right] \left[\begin{array}{c|c} U & 0 \\ \hline 0 & I_n \end{array} \right].$$

Finally, apply an additional feedback law \tilde{F}_2 to place all the eigenvalues of the subsystem (\hat{A}_{22}, B_2) at zero (which is known as deadbeat control [27]). This is possible since that subsystem inherits its controllability from that of the full system. The resulting matrix $\tilde{A}_{22} := \hat{A}_{22} + \tilde{B}_2 \tilde{F}_2$ is then nilpotent, and its index of nilpotency can be chosen to be minimal [27]:

$$\left[\begin{array}{cc|c} \mu I_{d_f} - \hat{A}_{11} & -\tilde{A}_{12} & -B_1 \\ 0 & \mu I_{d_0} - \hat{A}_{22} & -B_2 \\ \hline 0 & \tilde{C}_2 & D \end{array} \right] := \left[\begin{array}{cc|c} \mu I_{d_f} - \hat{A}_{11} & -\hat{A}_{12} & -B_1 \\ 0 & \mu I_{d_0} - \hat{A}_{22} & -B_2 \\ \hline 0 & \tilde{C}_2 & D \end{array} \right] \cdot \left[\begin{array}{cc|c} I_{d_f} & 0 & 0 \\ 0 & I_{d_0} & 0 \\ \hline 0 & \tilde{F}_2 & I_n \end{array} \right].$$

Combining the different steps and setting $F := \hat{F}U + [0, \tilde{F}_2]$ yields the desired result (3.3). \square

Notice that the deadbeat control part can be avoided, because before the feedback \hat{F} was applied, all eigenvalues of A were at $\mu = 0$. It suffices to only apply the part of the feedback that cancels the finite zeros and leaves the other eigenvalues unchanged. How this can be done is shown in [24].

COROLLARY 3.3. *Let the assumptions of Theorem 3.2 hold. Then, in the same notation of the statement of Theorem 3.2, $P(\lambda) = N(\lambda)G(\lambda)$ with*

$$N(\lambda) = D + \tilde{C}_2(I_{d_0} - \lambda\tilde{A}_{22})^{-1}\lambda B_2 \quad \text{and} \quad G(\lambda) = I_n - F(I_{dn} - \lambda A)^{-1}\lambda B$$

and the fact that $N(\lambda)$ is left invertible and $G(\lambda)$ is a GCRD for the blocks of the compound matrix $P(\lambda)$.

Proof. It follows from (3.2) and (3.3) that we also have

$$\left[\begin{array}{cc|c} I_{dn} - \lambda U^*AU & -\lambda U^*B \\ \hline CU & D \end{array} \right] \left[\begin{array}{c|c} I_{dn} & 0 \\ \hline F & I_n \end{array} \right] = \left[\begin{array}{cc|c} I_{d_f} - \lambda\hat{A}_{11} & -\lambda\tilde{A}_{12} & -\lambda B_1 \\ 0 & I_{d_0} - \lambda\hat{A}_{22} & -\lambda B_2 \\ \hline 0 & \tilde{C}_2 & D \end{array} \right].$$

The transfer function of the system quadruple on the right-hand side is

$$D + \tilde{C}_2(I_{d_0} - \lambda\tilde{A}_{22})^{-1}\lambda B_2$$

which is polynomial since \tilde{A}_{22} is nilpotent and has no finite zeros since there exists a unitary matrix V such that

$$\left[\begin{array}{c|c} I_{d_0} & 0 \\ \hline 0 & V \end{array} \right] \left[\begin{array}{cc|c} I_{d_0} - \lambda\tilde{A}_{22} & -\lambda B_2 \\ \hline (I_m - P_0P_0^\dagger)C & P_0 \end{array} \right] = \left[\begin{array}{cc|c} I_{d_0} - \lambda\tilde{A}_{22} & -\lambda B_2 \\ \hline \tilde{C}_V & 0 \\ 0 & \tilde{P}_0 \end{array} \right],$$

where \tilde{P}_0 is invertible, and $(\tilde{A}_{22}, \tilde{C}_V)$ is observable. Therefore, that pencil has no finite zeros. As shown in Lemma 4.6, the feedback operation can be written as the matrix factorization $P(\lambda) = N(\lambda)G(\lambda)$, where the polynomial matrices $P(\lambda)$ and $G(\lambda)$ are realized by the system matrices

$$\left[\begin{array}{cc|c} I_0 - \lambda\tilde{A}_{22} & -\lambda B_2 \\ \hline \tilde{C}_2 & D \end{array} \right] \quad \text{and} \quad \left[\begin{array}{cc|c} I_{dn} - \lambda A & -\lambda B \\ \hline -F & I_n \end{array} \right],$$

respectively. Moreover, the coefficients $G_i, i = 0, \dots, d$, and $N_i, i = 1, \dots, d$, of the polynomial expansions $G(\lambda) = \sum_{i=0}^d G_i\lambda^i$ and $N(\lambda) = \sum_{i=0}^d N_i\lambda^i$ are given by

$$G_0 = I_n, G_i = -F_i, i = 1, \dots, d, \quad N_0 = P_0, N_i = \tilde{C}_2\tilde{A}_{22}^{i-1}B_2, i = 1, \dots, d. \quad \square$$

4. Generalized state-space approach. In this section, we describe a novel variation of the approach of section 3, leading to a new algorithm. Let us consider a general $m \times n$ polynomial matrix $P(\lambda)$ of normal rank r and represent it as the transfer function of a generalized state-space model

$$(4.1) \quad S_P(\lambda) = \left[\begin{array}{c|c} \frac{A - \lambda E}{C} & \frac{B}{D} \end{array} \right] := \left[\begin{array}{cccc|cc} I_n & -\lambda I_n & & & & \\ & I_n & -\lambda I_n & & & \\ & & \ddots & \ddots & & \\ & & & I_n & -\lambda I_n & \\ \hline P_d & \dots & \dots & P_1 & P_0 & -I_n \\ & & & & & 0 \end{array} \right]$$

which has state-space dimension $(d + 1)n$ and is irreducible for all finite points. This pencil has normal column rank equal to $(d + 1)n + r$, and its finite zeros are the finite eigenvalues of the pencil $S_P(\lambda)$. Moreover, if $\Lambda(\lambda)$ is the Smith form of the matrix $P(\lambda)$, then the Smith form of $S_P(\lambda)$ defined in (4.1), and $S_\lambda(\lambda)$ given in (3.1), are, respectively,

$$I_{(d+1)n} \oplus \Lambda(\lambda) \quad \text{and} \quad I_{dn} \oplus \Lambda(\lambda).$$

It is also easy to see that the pencil $S_P(\lambda)$ is strictly equivalent to $I_n \oplus S_\lambda(\lambda)$, which implies that the left and right minimal indices and the finite and (nontrivial) infinite zeros of (3.1) and (4.1) are the same.

The following decomposition can then be obtained by running the staircase reduction on the $(dn + m) \times (dn + n)$ subpencil $S_\lambda(\lambda)$, given in (3.1), of the system matrix $S_P(\lambda)$.

THEOREM 4.1. *Let the $m \times n$ polynomial matrix $P(\lambda)$ have normal rank r ; then there exist unitary transformations $Q \in \mathbb{C}^{dn \times dn}$ and $Z \in \mathbb{C}^{(d+1)n \times (d+1)n}$ satisfying*

$$\begin{aligned} & \left[\begin{array}{c|c} Q^* & \\ \hline & I_m \end{array} \right] \left[\begin{array}{cccc|cc} I_n & -\lambda I_n & & & & \\ & I_n & -\lambda I_n & & & \\ & & \ddots & \ddots & & \\ & & & I_n & -\lambda I_n & \\ \hline P_d & \dots & \dots & P_1 & P_0 & \end{array} \right] Z \\ & = \left[\begin{array}{cccc|c} A_{11} - \lambda E_{11} & A_{12} - \lambda E_{12} & A_{13} - \lambda E_{13} & A_{14} - \lambda E_{14} & \\ 0 & A_{22} - \lambda E_{22} & A_{23} - \lambda E_{23} & A_{24} - \lambda E_{24} & \\ 0 & 0 & A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & \\ \hline 0 & 0 & 0 & C_4 & \end{array} \right], \end{aligned}$$

where the following hold:

- the pencil $A_{22} - \lambda E_{22}$ is regular and contains the finite zeros of $S_\lambda(\lambda)$;
- the pencil $A_{11} - \lambda E_{11}$ contains the $n - r$ right Kronecker blocks of $S_\lambda(\lambda)$;
- the pencil

$$\left[\begin{array}{cc|c} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & \\ \hline 0 & C_4 & \end{array} \right]$$

contains the infinite zeros and the $m - r$ left Kronecker blocks of $S_\lambda(\lambda)$;

- the submatrix C_4 has full column rank.

Proof. The staircase form, described in Lemma 4.7, precisely separates the right minimal indices and the finite zeros of a given pencil, from its remaining structural elements, which in our case are the infinite zeros and the left minimal indices of the pencil. It does so using a unitary equivalence transformation that separates the different groups of structural elements in a block upper triangular form. In a first stage, the right Kronecker blocks and finite zeros are separated from the infinite zeros and left Kronecker blocks. In a second stage, an updating unitary equivalence transformation separates further the right Kronecker blocks from the finite zeros, to generate a three-way decomposition, as described in Lemma 4.7. The first step of stage 1 is a row transformation compressing the rows of the coefficient of λ . But the coefficient of λ in the pencil $S_\lambda(\lambda)$ is already in row-compressed form since its top part is the submatrix I_{dn} . The next step then compresses the columns of the submatrix

$$[P_d \ \dots \ P_1 \ P_0]$$

to the right, to produce the matrix C_4 of full column rank n_4 . The algorithm then proceeds further with the leading subpencil of dimension $dn \times (dn - n_4)$ and applies a similar sequence of row and column compressions to subpencils of decreasing dimensions. The special block structure of the left transformation $Q^* \oplus I_m$ thus follows from the fact that the very first step of the staircase algorithm can be skipped here. \square

In Theorem 4.2 below, we analyze how the decomposition of Theorem 4.1 can be combined with feedback to yield a transfer function with the desired properties.

THEOREM 4.2. *Let the $m \times n$ polynomial matrix $P(\lambda)$ have normal rank r ; then there exist a feedback matrix F and unitary matrices Q and Z such that*

$$(4.2) \quad \left[\begin{array}{c|c} Q^* & \\ \hline I_n & I_m \end{array} \right] \left[\begin{array}{cccc|c} I_n & -\lambda I_n & & & \\ & I_n & -\lambda I_n & & \\ & & \ddots & \ddots & \\ & & & I_n & -\lambda I_n \\ \hline & & & & I_n & -I_n \\ P_d & \dots & \dots & P_1 & P_0 & 0 \end{array} \right] \left[\begin{array}{c|c} Z & \\ \hline FZ & I_n \end{array} \right]$$

$$= \left[\begin{array}{cccc|cc} A_{11} - \lambda E_{11} & A_{12} - \lambda E_{12} & A_{13} - \lambda E_{13} & A_{14} - \lambda E_{14} & 0 & 0 \\ 0 & A_{22} - \lambda E_{22} & A_{23} - \lambda E_{23} & A_{24} - \lambda E_{24} & 0 & 0 \\ 0 & 0 & A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & 0 & 0 \\ 0 & 0 & Z_3 & Z_4 & -I_r & 0 \\ Z_1 & 0 & 0 & 0 & 0 & -I_{n-r} \\ \hline 0 & 0 & 0 & C_4 & 0 & 0 \end{array} \right],$$

where $A_{22} - \lambda E_{22}$ is square, contains the finite zeros of $P(\lambda)$, and is unobservable in this realization, the pencil $\begin{bmatrix} A_{11} - \lambda E_{11} \\ Z_1 \end{bmatrix}$ is unimodular and unobservable in this realization, and the subpencil

$$(4.3) \quad \begin{bmatrix} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} \\ Z_3 & Z_4 \end{bmatrix}$$

is unimodular.

Proof. In order to obtain the decomposition (4.2), we first apply a feedback $F = [0 \ \dots \ 0 \ I_n]$, to eliminate the coupling term I_n in the last block row of $(A - \lambda E)$:

$$\left[\begin{array}{cccc|c} I_n & -\lambda I_n & & & \\ & & \ddots & & \\ & & & I_n & -\lambda I_n \\ & & & & 0 \\ \hline P_d & \dots & P_1 & P_0 & -I_n \\ & & & & 0 \end{array} \right] = \left[\begin{array}{cccc|c} I_n & -\lambda I_n & & & \\ & & \ddots & & \\ & & & I_n & -\lambda I_n \\ & & & & I_n \\ \hline P_d & \dots & P_1 & P_0 & -I_n \end{array} \right] \left[\begin{array}{c|c} I_{(d+1)n} & \\ \hline F & I_n \end{array} \right].$$

Then, we integrate in this decomposition the transformations Q and Z of Theorem 4.1. It follows from the construction of that theorem that the pencils $A_{11} - \lambda E_{11}$ and $[A_{33} - \lambda E_{33} \ A_{34} - \lambda E_{34}]$ have full row rank for all finite λ and that their leading coefficient has full row rank as well. By [21, Lemma 5.2], these pencils are then right invertible and, as a consequence [1, Theorem 3.3], they always have a unimodular embedding (4.3), realized by the matrices Z_1 and $[Z_3 \ Z_4]$, respectively. These matrices $Z_1, Z_3,$ and Z_4 are then placed in the bottom block row of $(A - \lambda E)$ by the updated feedback matrix

$$F = [0 \ 0 \ 0 \ I_n] - \begin{bmatrix} 0 & 0 & Z_3 & Z_4 \\ Z_1 & 0 & 0 & 0 \end{bmatrix} Z^T.$$

A construction for the embedding matrices Z_1 and $[Z_3 \ Z_4]$ is given, e.g., in [2]. \square

We now have all the ingredients to construct a factorization, as stated in the following theorem.

THEOREM 4.3. *The decomposition of Theorem 4.1 of the polynomial matrix $P(\lambda)$ of normal rank r , defined by its system matrix $S_P(\lambda)$ described in (4.1), yields the polynomial factorization $P(\lambda) = N_r(\lambda)G_c(\lambda)$, where $N_r(\lambda) \in \mathbb{C}[\lambda]^{m \times r}$ has full rank r for all finite λ and $G_c(\lambda) \in \mathbb{C}[\lambda]^{r \times n}$ contains all the finite zeros of $P(\lambda)$. Moreover, $N_r(\lambda)$ and $G_c(\lambda)$ are given by their system matrices*

$$(4.4) \quad S_{N_r}(\lambda) := \left[\begin{array}{cc|c} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & 0 \\ Z_3 & Z_4 & -I_r \\ \hline 0 & C_4 & 0 \end{array} \right], \quad S_{G_c}(\lambda) := \left[\begin{array}{c|c} A - \lambda E & B \\ \hline -[I_r, 0]F & [I_r, 0] \end{array} \right].$$

Proof. We obtain from the above feedback construction and from Lemma 4.6 the factorization $P(\lambda) = N(\lambda)G(\lambda)$, where the two factors are given by the system matrices

$$S_N(\lambda) := \left[\begin{array}{cc|cc} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & 0 & 0 \\ Z_3 & Z_4 & -I_r & 0 \\ \hline 0 & C_4 & 0 & 0 \end{array} \right], \quad S_G(\lambda) := \left[\begin{array}{c|c} A - \lambda E & B \\ \hline -F & I_n \end{array} \right].$$

The matrix $N(\lambda)$ is clearly zero in its last $n - r$ columns and can thus be written as $N(\lambda) = N_r(\lambda)[I_r \ 0]$. And this right factor $[I_r \ 0]$ can be absorbed in the product $G_c(\lambda) = [I_r \ 0]G(\lambda)$, where the system matrices of $N_r(\lambda)$ and $G_c(\lambda)$ are as in (4.4). The two factors are polynomial, because their system matrices have unimodular matrices as state-transition pencils. The constructed factor $N_r(\lambda)$ has full column rank r since its system matrix $S_{N_r}(\lambda)$ is strictly equivalent to the pencil

$$I_r \oplus \begin{bmatrix} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} \\ 0 & C_4 \end{bmatrix},$$

which has only left minimal indices and infinite zeros. \square

The computation of the coefficients N_i and G_i of the expansions $N_r(\lambda) = \sum_{i=0}^d N_i \lambda^i$ and $G_c(\lambda) = \sum_{i=0}^d G_i \lambda^i$ are now given in terms of the matrices

$$[\hat{F}_d \ \dots \ \hat{F}_1 \ \hat{F}_0] := \hat{F} := [I_r \ 0] F$$

and

$$\left[\begin{array}{c|c} \hat{A} - \lambda \hat{E} & -\hat{B} \\ \hline \hat{C} & 0 \end{array} \right] := \left[\begin{array}{cc|c} A_{33} - \lambda E_{33} & A_{34} - \lambda E_{34} & 0 \\ Z_3 & Z_4 & -I_r \\ \hline 0 & C_4 & 0 \end{array} \right]$$

as follows:

$$G_0 = I_n - \hat{F}_0, \ G_i = -\hat{F}_i, \ i = 1, \dots, d, \quad N_i = \hat{C}(\hat{A}^{-1}\hat{E})^i \hat{A}^{-1}\hat{B}, \ i = 0, \dots, d.$$

Remark 4.4. The generalized state-space approach has the disadvantage of requiring the computation of two large transformation matrices, but its main advantage is that the norm of the feedback matrix F can be chosen to be bounded. All calculations of the decomposition are completely based on orthogonal transformations in the real case and unitary transformations in the complex case. The final construction of the GCRD is directly obtained from the feedback matrix F . Typically, its submatrices Z_i are chosen to have orthonormal rows (see [2]), and it then follows that each row of the matrix $G_c(\lambda)$ has Frobenius norm 1. We point out that the construction of the factor $G_c(\lambda)$ only requires the product $[I_r \ 0] F$. This implies that the matrix Z_1 does not need to be computed and that the separation of the blocks $(A_{11} - \lambda E_{11})$ and $(A_{22} - \lambda E_{22})$ in stage 2 of the staircase algorithm does not need to be performed.

Remark 4.5. Note that we can construct from $N_r(\lambda)$ and $G_c(\lambda)$ also factorizations $P(\lambda) = N_\ell(\lambda)G_\ell(\lambda)$, where $N_\ell(\lambda) \in \mathbb{C}[\lambda]^{m \times \ell}$ and $G_\ell(\lambda) \in \mathbb{C}[\lambda]^{\ell \times n}$ for any $r < \ell \leq n$ by appending columns to N_0 that are linear independent from those of N_0 and appending zero rows to $G_c(\lambda)$.

4.1. Appendix to section 4: Technical results. We recall here some basic lemmata about system pencils.

LEMMA 4.6. *The following block transformation of the system matrix of $P(\lambda)$*

$$S_N(\lambda) = \left[\begin{array}{c|c} A + BF - \lambda E & B \\ \hline C + DF & D \end{array} \right] := S_P(\lambda) \left[\begin{array}{c|c} I & 0 \\ \hline F & I_n \end{array} \right]$$

extracts from the transfer function $P(\lambda) = N(\lambda)G(\lambda)$ a right factor $G(\lambda)$ defined by the system matrix

$$S_G(\lambda) = \left[\begin{array}{c|c} A - \lambda E & B \\ \hline -F & I_n \end{array} \right]$$

provided the pencil $(A + BF - \lambda E)$ is regular.

Proof. It is well known that the system matrix of a product can be obtained from a product of (expanded) system matrices (see [28]). Applying this to the system matrices $S_N(\lambda)$ and $S_G(\lambda)$, we obtain the system matrix for the product $N(\lambda)G(\lambda)$ as follows:

$$\left[\begin{array}{cc|c} A + BF - \lambda E & -BF & B \\ 0 & A - \lambda E & B \\ \hline C + DF & -DF & D \end{array} \right] = \left[\begin{array}{cc|c} A + BF - \lambda E & 0 & B \\ 0 & I & 0 \\ \hline C + DF & 0 & D \end{array} \right] \left[\begin{array}{cc|c} I & 0 & 0 \\ 0 & A - \lambda E & B \\ \hline 0 & -F & I_n \end{array} \right].$$

This is a valid Rosenbrock system quadruple provided the pencil $(A + BF - \lambda E)$ is regular. Using a trivial block row and block column transformation, we then find that the left system matrix is a strict system equivalent to

$$\left[\begin{array}{cc|c} A + BF - \lambda E & 0 & 0 \\ 0 & A - \lambda E & B \\ \hline C + DF & C & D \end{array} \right] \sim \left[\begin{array}{c|c} A - \lambda E & B \\ \hline C & D \end{array} \right]. \quad \square$$

We also recall basic properties of the staircase form of pencils used in the paper. For details of the proof, we refer the reader to [25], where a lower triangular version is given.

LEMMA 4.7 (staircase form). *Let $A - \lambda E \in \mathbb{C}[\lambda]^{m \times n}$ be a general $m \times n$ matrix pencil of normal rank r . Then there exist unitary transformations $Q \in \mathbb{C}^{m \times m}$ and $Z \in \mathbb{C}^{n \times n}$ such that*

$$Q^*(A - \lambda E)Z = \begin{bmatrix} A_{11} - \lambda E_{11} & A_{12} - \lambda E_{12} & A_{13} - \lambda E_{13} \\ 0 & A_{22} - \lambda E_{22} & A_{23} - \lambda E_{23} \\ 0 & 0 & A_{33} - \lambda E_{33} \end{bmatrix},$$

where $A_{11} - \lambda E_{11}$ contains the $n - r$ right Kronecker blocks of $A - \lambda E$, $A_{22} - \lambda E_{22}$ is regular and contains the finite zeros of $A - \lambda E$, and $A_{33} - \lambda E_{33}$ contains the infinite zeros and $m - r$ left Kronecker blocks of $A - \lambda E$.

5. Numerical aspects. Numerical algorithms for the computation of a GCRD of a polynomial matrix $P(\lambda)$ can be classified into four categories. The classical (algebraic) approach uses unimodular transformations to construct the Hermite form of the matrix $P(\lambda)$ (see [11]), from which the GCRD can be derived. The worst case complexity of this approach is significantly larger than for other methods, and it is easy to see that coefficient growth can be quite dramatic since numerical pivoting techniques are precluded. A positive aspect of this approach is that it also applies to matrices with deficient normal rank. A second class of methods is based on spectral divisors of the submatrices $P_i(\lambda)$ forming $P(\lambda)$ [14], but these methods apply only to square submatrices $P_i(\lambda)$ and also require the computation of their zeros. A third class of methods is related to resultant matrices [3, 15, 18, 32]; in particular, [15] shares two advantages with our new algorithm; that is, it allows for a rank deficient input, and it relies only on multiplication by unitary matrices. These matrices and their left null vectors can be used to characterize the left inverses of $P(\lambda)$ and from there also construct the GCRD. The methods using this approach perform a numerical elimination of linear dependent rows of the Sylvester matrix, but the elimination procedure and corresponding echelon form can be seen to make implicit use of unimodular transformations. This again precludes standard pivoting techniques that are important for numerical stability. Moreover, it is unclear how (or if) these methods can be adapted to the case where (1.1) is not full rank. A fourth class of methods is based on state-space realizations [9, 24], as explained in section 3.

The method proposed in this paper does not belong to any of these classes, but it is close to the fourth class. Our algorithm¹ uses a *generalized* state-space realization of the polynomial matrix, its staircase reduction to find its decoupling part and state feedback to implement the factorization defining a GCRD. Its complexity is that of the staircase algorithm, which is cubic in the state-space dimension (which is smaller than

¹A MATLAB implementation is freely available from GitHub at <https://github.com/VanDoorenPaul/Greatest-Common-Divisor>.

the size of the Sylvester matrix used in the third class of methods). This approach has the additional advantage that all rank decisions are based on orthogonal state-space transformations only, but it does not take away the inherent ill condition of the problem.

We now describe some numerical experiments that we performed to test the new algorithm. We first considered the example

$$P(\lambda) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 5 & 2 \\ -1 & -1 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 2 & 2 \\ 3 & 4 \\ 1 & 1 \end{bmatrix} \lambda + \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 2 & 0 \\ 1 & 1 \end{bmatrix} \lambda^2 + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \lambda^3,$$

drawn from [3], and for which the authors of [3] computed a compact GCRD

$$G(\lambda) = \begin{bmatrix} 5 & 2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix} \lambda.$$

Our algorithm uses only orthogonal transformations on the system matrix pencil of $P(\lambda)$. Therefore, if we normalize $P(\lambda)$ to have a norm equal to 1, all rank decisions will be on submatrices bounded in norm by 1. For this example, we obtained the computed factorization

$$N_r(\lambda) \approx \begin{bmatrix} 1.4633 & -0.9267 \\ 1.1785 & 0.7818 \\ 6.4620 & 0.4920 \\ -1.4633 & 0.9267 \end{bmatrix} + \begin{bmatrix} 1.1785 & 0.7818 \\ 2.6418 & -0.1449 \\ 1.4633 & -0.9267 \\ 2.6418 & -0.1449 \end{bmatrix} \lambda + \begin{bmatrix} 0.0000 & -0.0000 \\ 0.0000 & -0.0000 \\ 1.1785 & 0.7818 \\ 0.0000 & 0.0000 \end{bmatrix} \lambda^2,$$

$$G_c(\lambda) \approx \begin{bmatrix} 0.7641 & 0.3496 \\ 0.1274 & -0.5270 \end{bmatrix} + \begin{bmatrix} 0.3496 & 0.4144 \\ -0.5270 & 0.6544 \end{bmatrix} \lambda$$

and obtained a factorization residual norm $\|P(\lambda) - N_r(\lambda)G_c(\lambda)\|_F \approx 8.10^{-15}$. The tolerance for the rank decisions was chosen as $tol = 1000\epsilon_M$, where $\epsilon_M \approx 2.10^{-16}$ is the machine precision of the computer used. To check the roots of $G_c(\lambda)$, we compared the (monic) characteristic polynomials of $G_c(\lambda)$ and $G(\lambda)$ (the latter is $\lambda^2 + \lambda - 1$) and the error was approximately 2.10^{-15} .

As a second experiment, we constructed the input

$$(5.1) \quad P(\lambda, k) = Z \begin{bmatrix} \lambda^2 & 2\lambda \\ 0 & \lambda \\ \lambda & k\lambda + 1 \\ 0 & \lambda^2 \end{bmatrix} \in \mathbb{C}[\lambda]^{4 \times 2},$$

where $0 \leq k \in \mathbb{R}$ is a parameter, and $Z \in \mathbb{C}^{4 \times 4}$ is a complex unitary matrix, randomly generated by first taking X to be a realization of a 4×4 Gaussian random matrix and then computing Z as the unitary factor of the QR factorization of X . It is not difficult to show that, for all k, Z as above, any compact GCRDs of (5.1) must have the form $V(\lambda) \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ where $V(\lambda) \in \mathbb{C}[\lambda]^{2 \times 2}$ is unimodular; in particular, all these GCRDs are regular, have a defective eigenvalue at 1, and have a root polynomial [7, 22] at 0 equal to $[-1 \ \lambda]^T$. On the other hand, when $k \rightarrow +\infty$, the columns of the input become unbalanced: the Frobenius norm of the second column diverges, whereas the

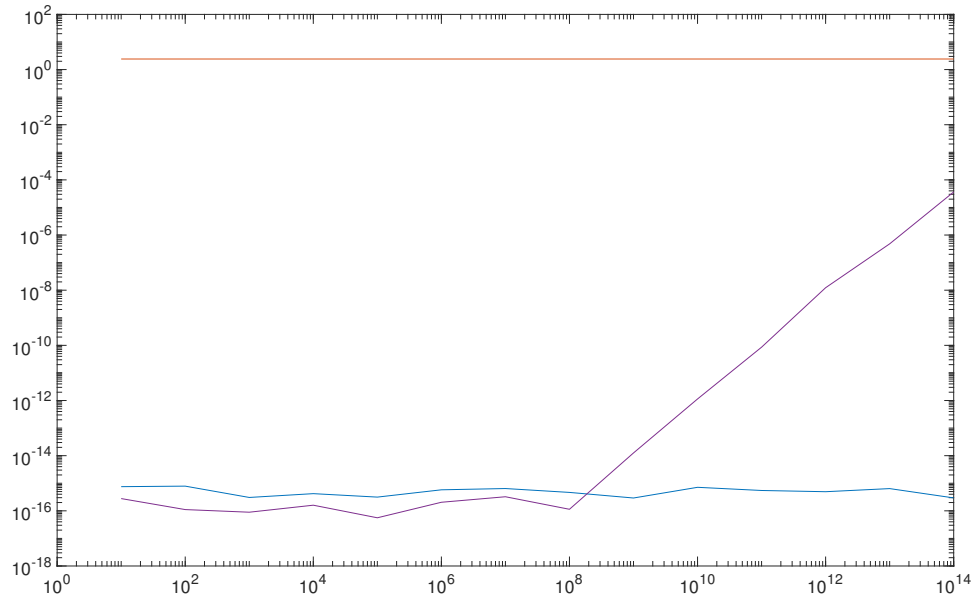


FIG. 1. In blue, residual $\rho_1(k)$ for the computed GCRD factorization of (5.1) for varying values of k . In red, condition number $\rho_2(k)$ of the computed compact GCRD of (5.1), evaluated at $\lambda = 1$, for the same values of k . In purple, norm $\rho_4(k)$ of the vector $G'_c(0, k)e_1 - G_c(0, k)e_2$ for the same values of k . (Color is available online only.)

Frobenius norm of the first column is independent of k and equal to $\sqrt{2}$. Hence, when k is large, one could expect numerical difficulties. For $k = 10, 10^2, \dots, 10^{14}$, we computed a GCRD factorization $P(\lambda, k) = N_r(\lambda, k)G_c(\lambda, k)$ and then four quantities: the factorization residual $\rho_1(k) = \|N_r(\lambda, k)G_c(\lambda, k) - P(\lambda, k)\|_F$, the quantity $\rho_2(k) = \kappa(G_c(1, k))$, where κ is the 2-norm condition number, and the norms $\rho_3(k) = \|G_c(0, k)e_1\|_2$ and $\rho_4(k) = \|G'_c(0, k)e_1 - G_c(0, k)e_2\|_2$. In particular, if $\rho_2(k)$ is not large, then $G_c(\lambda, k)$ is correctly computed to be regular; and if $\rho_3(k)$ and $\rho_4(k)$ are both small, then $[-1 \ \lambda]$ is indeed a root polynomial at 0 for $G_c(\lambda)$. In our computations, $\rho_3(k)$ was computed to be exactly zero to machine precision for all values of k ; Figure 1 provides a logarithmic plot of $\rho_1(k)$, $\rho_2(k)$, and $\rho_4(k)$.

Note that, for $\log_{10}(k) \geq 9$, the root polynomials at the eigenvalue 0 were not always accurately captured. Values of k for which $\rho_4(k)$ is large suggest that the largest partial multiplicity of 0 was computed to be 1 in lieu of the correct value of 2; but this behavior in the presence of a Jordan chain of length 2 is not surprising for an algorithm run in double precision.

The numerical tests discussed above are for small-sized and small-degree polynomial matrices. It should be noted that the problem of computing a GCRD is ill-posed. One way to see this is to observe, generically in the Euclidean topology, that almost all sets of input matrices only have right invertible (over $\mathbb{R}[\lambda]$) compact GCRDs. Recall [21, Lemma 5.2] that being right invertible over $\mathbb{R}[\lambda]$ is equivalent to having no finite eigenvalues and no left minimal indices. Thus, especially when the size or the degree of the input grows larger, even a backward stable method can be expected to incorrectly approximate finite eigenvalues in the computed GCRD. Indeed, all the numerical experiments that we could find in the literature for (both exact and approximate) GCRD computation are for polynomial matrices of very small, say $O(1)$,

TABLE 1

Norms of the factors $N_r(\lambda)$, $G_c(\lambda)$ and the residual matrix $Res(\lambda)$, and condition numbers of $G_c(\lambda)$ at the eigenvalues λ_i , $i = 1, \dots, 4$, for 10 randomly generated compound matrices $P(\lambda)$ as in (1.1) with $m = 1000$ rows, $n = 500$ columns, normal rank $r = 20$, degree 6, and 4 finite eigenvalues.

$\ N_r(\cdot)\ _2$	$\ G_c(\cdot)\ _2$	$\ Res(\cdot)\ _2$	$\kappa(G_c(\lambda_1))^{-1}$	$\kappa(G_c(\lambda_2))^{-1}$	$\kappa(G_c(\lambda_3))^{-1}$	$\kappa(G_c(\lambda_4))^{-1}$
1.0013e+00	4.4721e+00	2.9624e-15	1.7509e-15	1.7509e-15	2.7147e-15	2.7147e-15
1.0003e+00	4.4721e+00	3.7683e-15	1.6676e-16	3.3772e-16	3.3772e-16	4.1002e-15
9.9912e-01	4.4721e+00	3.2400e-15	3.0898e-16	1.0641e-15	4.1927e-15	4.1927e-15
9.9966e-01	4.4721e+00	4.4029e-15	2.5095e-16	1.9051e-15	1.3357e-15	1.3357e-15
9.9992e-01	4.4721e+00	3.0857e-15	3.3193e-16	9.9503e-16	9.9503e-16	2.1699e-15
1.0003e+00	4.4721e+00	3.8058e-15	7.0299e-16	1.1784e-15	1.1784e-15	5.3952e-15
1.0007e+00	4.4721e+00	4.6801e-15	2.1369e-16	2.1369e-16	6.9481e-16	6.9481e-16
1.0005e+00	4.4721e+00	4.0644e-15	1.4874e-16	8.0534e-16	9.3845e-16	9.3845e-16
9.9994e-01	4.4721e+00	3.3280e-15	3.0311e-16	3.0311e-16	7.7456e-16	2.4649e-15
1.0005e+00	4.4721e+00	6.4201e-15	6.5535e-16	6.4943e-16	4.9751e-15	7.6166e-15

size and degree. Nevertheless, in the next experiments we will test our code against higher values of the input size and of the input degree.

For our third experiment, we randomly generated 10 examples of the form $P(\lambda) = M(\lambda)S(\lambda)N(\lambda) \in \mathbb{R}[\lambda]^{1000 \times 500}$ of normal rank 20 where $M(\lambda) \in \mathbb{R}[\lambda]^{500 \times 20}$ and $N(\lambda) \in \mathbb{R}[\lambda]^{20 \times 500}$ are degree-1 polynomial matrices whose coefficients are realizations of Gaussian random matrices, and $S(\lambda) \in \mathbb{R}[\lambda]^{20 \times 20} = I_{19} \oplus p(\lambda)$, where $p(\lambda)$ is a scalar polynomial of degree 4 with coefficients that are realizations of normal random variables. Then, almost surely, the matrices $P(\lambda) \in \mathbb{R}[\lambda]^{1000 \times 500}$ are of degree 6 and have as finite Smith zeros the roots of the fourth degree polynomial $p(\lambda)$. Moreover, again with probability 1, by Remark 2.15 any compact GCRD $G_c(\lambda) \in \mathbb{R}[\lambda]^{20 \times 500}$ has 4 finite eigenvalues and 480 right minimal indices. For these larger size inputs, we set the tolerance for rank decisions at $tol = 10^4 \epsilon_M$. Table 1 yields, for these randomly generated examples, the norms of the computed factors $N_r(\lambda)$ and $G_c(\lambda)$ of $P(\lambda)$, the norm of the residual $Res(\lambda) := P(\lambda) - N_r(\lambda)G_c(\lambda)$, and the inverse condition numbers $\kappa(G_c(\lambda_i))^{-1} := \sigma_r(G_c(\lambda_i)) / \sigma_1(G_c(\lambda_i))$ of the matrices $G_c(\lambda_i)$ evaluated in the Smith zeros of λ_i of $P(\lambda)$.

It can be seen from Table 1 that in all of the 10 examples the algorithm found the correct normal rank $r = 20$ and a right factor $G_c(\lambda)$ that contains the four Smith zeros of $P(\lambda)$; the accuracy in the computation of the eigenvalues is remarkable and even somewhat surprising for an input of $O(10^3)$ size, given the remarks above on the ill-posedness of the problem. Moreover, the norms of the two factors $N_r(\lambda)$ and $G_c(\lambda)$ are very reasonable, which can be explained from the use of orthogonal transformations applied to the system matrix pencil. As pointed out in Remark 4.4, the Frobenius norm of $G_c(\lambda)$ is approximately the square root of its number of rows; note that $\sqrt{20} \simeq 4.4721$, so the algorithm has always computed the normal rank correctly. We conclude that, in the case of small input degree but relatively large input size, the experimental results are thus compatible with a backward stable algorithm, both for the compact GCRD extraction and for the computation of the factorization $P(\lambda) = N_r(\lambda)G_c(\lambda)$.

For our fourth experiment, we repeated a numerical test similar to the previous one but with different parameters, to test the behavior of algorithm for moderate-degree input. This time $P(\lambda) = M(\lambda)S(\lambda)N(\lambda) \in \mathbb{R}[\lambda]^{4 \times 3}$ is constructed by randomly generating degree-10 $M(\lambda) \in \mathbb{R}[\lambda]^{4 \times 2}$ and $N(\lambda) \in \mathbb{R}[\lambda]^{2 \times 3}$, and $S(\lambda) = 1 \oplus p(\lambda)$, where $p(\lambda)$ is a randomly generated scalar polynomial of degree 4. Hence, almost surely, $P(\lambda) \in \mathbb{R}[\lambda]^{4 \times 3}$ has degree 24 and normal rank 2. Therefore, almost surely,

TABLE 2

Norms of the factors $N_r(\lambda)$, $G_c(\lambda)$ and the residual matrix $Res(\lambda)$, and condition numbers of $G_c(\lambda)$ at the eigenvalues λ_i , $i = 1, \dots, 4$, for 10 randomly generated compound matrices $P(\lambda)$ as in (1.1) with $m = 4$ rows, $n = 3$ columns, normal rank $r = 2$, degree 24, and 4 finite eigenvalues.

$\ N_r(\cdot)\ _2$	$\ G_c(\cdot)\ _2$	$\ Res(\cdot)\ _2$	$\kappa(G_c(\lambda_1))^{-1}$	$\kappa(G_c(\lambda_2))^{-1}$	$\kappa(G_c(\lambda_3))^{-1}$	$\kappa(G_c(\lambda_4))^{-1}$
1.0300e+00	1.4142e+00	1.3774e-13	7.6420e-16	7.6420e-16	4.7405e-16	3.9246e-13
1.0052e+00	1.4142e+00	1.4404e-13	2.9781e-13	5.4190e-13	3.4446e-13	3.4446e-13
5.2905e+00	1.7321e+00	7.2512e-05	2.4736e-15	3.8403e-16	3.8403e-16	1.5077e-14
1.6320e+00	1.7321e+00	3.1000e-13	1.3971e-16	4.3847e-15	4.3847e-15	5.2610e-14
4.2221e+00	1.7321e+00	1.2369e-08	6.9758e-15	6.9758e-15	2.3524e-15	1.4909e-14
6.7245e+00	1.7321e+00	9.1725e-05	6.1401e-16	6.1401e-16	2.3190e-14	2.3190e-14
9.5240e-01	1.4142e+00	2.7136e-13	5.5111e-16	1.6181e-15	1.6181e-15	1.0418e-12
1.0000e+00	1.7321e+00	2.9692e-13	1.0000e+00	1.0000e+00	1.0000e+00	1.0000e+00
1.0000e+00	1.7321e+00	2.4253e-14	1.0000e+00	1.0000e+00	1.0000e+00	1.0000e+00
1.0295e+00	1.4142e+00	8.7189e-14	3.8456e-15	3.9381e-14	3.9381e-14	1.3311e-07

any compact GCRD $\mathbb{R}[\lambda]^{2 \times 3}$ has four eigenvalues and one right minimal index. The same residual tests as before have been computed and are reported in Table 2.

Table 2 shows that, when the input degree grows, computing a compact GCRD correctly becomes more challenging. For example, the factorization residual is not always small, indicating that, when the input degree is $\gg 1$, the algorithm is not backward stable for the computation of the factorization $P(\lambda) = N_r(\lambda)G_c(\lambda)$. The results are, however, still compatible with the algorithm being backward stable as a method to compute $G_c(\lambda)$ only, even though the analysis to explain this is delicate. First, recalling Remark 4.4 and noting that $\sqrt{2} \simeq 1.4142$ and $\sqrt{3} \simeq 1.7321$, it is clear that most of the time the algorithm has overestimated the normal rank of the input; occasionally, this has also led to a high factorization residual. It also becomes relatively common to inaccurately capture the finite eigenvalues that the GCRD should (in exact arithmetic) have, or even to miss them entirely. As mentioned above, these shortcomings are not an indication of backward instability of the method as an algorithm to compute a compact GCRD. Indeed, it is known [5] that polynomial matrices with full column rank and no eigenvalues are everywhere dense (in the Euclidean topology) in $\mathbb{R}[\lambda]_{24}^{4 \times 3}$, the vector space of 4×3 real polynomial matrices of degree at most 24. Hence, most small perturbation of the input are such that their compact GCRD is a 3×3 unimodular matrix. In fact, the lines of the previous table where the inverse condition number at the expected eigenvalues is 1 are caused by the fact that the algorithm computed $G_c(\lambda)$ to be a constant orthogonal matrix: by the discussion above, this is still compatible with backward stability, because there exist (infinitely many) polynomial matrices whose GCRD is a constant unitary matrix and that are arbitrarily close to the actual input. It is in some sense remarkable that, at least in some cases, the correct eigenvalues are not missed, even if the degree of the input is $\gg 1$.

Finally, we tested the effect of the tolerance with which the algorithm runs (which is a crucial parameter, in particular for the staircase algorithm): in Table 3, we report the same tests for the *same* inputs (row by row) as Table 2 but having re-run the algorithm with a tolerance increased by a factor 10.

It can be seen in Table 3 that the numerical estimations of the normal rank and of the finite eigenvalues often improve by increasing the tolerance; however, occasionally this comes at the expense of a higher factorization residual. How to set the tolerance a priori with respect to the known parameters (such as size and degree of an input) is generally a difficult problem and is left for future research.

TABLE 3

Norms of the factors $N_r(\lambda)$, $G_c(\lambda)$ and the residual matrix $Res(\lambda)$, and condition numbers of $G_c(\lambda)$ at the eigenvalues λ_i , $i = 1, \dots, 4$, for the same inputs as Table 2 but having run the algorithm with a tolerance 10 times higher. Results that have improved significantly after the increase in tolerance are in bold; those that have worsened significantly are in italic.

$\ N_r(\cdot)\ _2$	$\ G_c(\cdot)\ _2$	$\ Res(\cdot)\ _2$	$\kappa(G_c(\lambda_1))^{-1}$	$\kappa(G_c(\lambda_2))^{-1}$	$\kappa(G_c(\lambda_3))^{-1}$	$\kappa(G_c(\lambda_4))^{-1}$
1.0300e+00	1.4142e+00	1.3774e-13	7.6420e-16	7.6420e-16	4.7405e-16	3.9246e-13
1.0052e+00	1.4142e+00	1.4404e-13	2.9781e-13	5.4190e-13	3.4446e-13	3.4446e-13
1.1276e+00	1.4142e+00	4.9997e-12	1.2706e-13	6.3114e-13	6.3114e-13	4.2452e-12
9.1563e-01	1.7321e+00	5.2990e-12	5.8681e-16	3.0430e-15	3.0430e-15	1.5136e-13
4.2221e+00	1.7321e+00	1.2369e-08	6.9758e-15	6.9758e-15	2.3524e-15	1.4909e-14
1.0362e+00	1.4142e+00	7.6057e-13	1.4496e-14	1.4496e-14	1.4221e-12	1.4221e-12
9.5240e-01	1.4142e+00	2.7136e-13	5.5111e-16	1.6181e-15	1.6181e-15	1.0418e-12
7.6350e+01	1.7321e+00	3.8364e-06	6.4356e-17	1.7544e-14	5.7841e-14	5.7841e-14
9.9824e-01	1.4142e+00	5.7547e-12	6.7049e-15	1.9289e-11	3.5895e-11	3.5895e-11
1.0295e+00	1.4142e+00	8.7189e-14	3.8456e-15	3.9381e-14	3.9381e-14	1.3311e-07

6. Concluding remarks. In this paper, we revisited the problem of Greatest Common Right Divisor extraction in its most general form, where the given matrix $P(\lambda)$ does not need to have full column rank and where the GCRD need not be square. Along the way, we introduced the so-called compact GCRDs, which play a central role here since all other GCRDs can be derived from them. Moreover, we presented a novel algorithm that computes such a minimal-size GCRD. The compact factorization is expected to play an important role in other problems, such as the computation of a compact Smith-like decomposition $P(\lambda) = U_r(\lambda)S_r(\lambda)V_r(\lambda)$, where the middle factor $S_r(\lambda)$ is regular and is of dimension $r \times r$.

REFERENCES

- [1] A. AMPARAN, S. MARCAIDA, AND I. ZABALLA, *On coprime rational function matrices*, Linear Algebra Appl., 50 (2016), pp. 1–31.
- [2] T. BEELEN AND P. VAN DOOREN, *A pencil approach for embedding a polynomial matrix into a unimodular matrix*, SIAM J. Matrix Anal. Appl., 9 (1988), pp. 77–89, <https://doi.org/10.1137/0609006>.
- [3] R. BITMEAD, S. Y. KUNG, B. D. O. ANDERSON, AND T. KAILATH, *Greatest common divisors via generalized Sylvester and Bezout matrices*, IEEE Trans. Automat. Control, 23 (1978), pp. 1043–1046.
- [4] W. A. COPPEL, *Matrices of rational functions*, Bull. Austral. Math. Soc., 11 (1974), pp. 89–113.
- [5] A. DMYTRYSHYN AND F. M. DOPICO, *Generic complete eigenstructures for sets of matrix polynomials with bounded rank and degree*, Linear Algebra Appl., 535 (2017), pp. 213–230.
- [6] F. M. DOPICO, S. MARCAIDA, M. C. QUINTANA, AND P. VAN DOOREN, *Local linearizations of rational matrices with application to rational approximations of nonlinear eigenvalue problems*, Linear Algebra Appl., 604 (2020), pp. 441–475.
- [7] F. DOPICO AND V. NOFERINI, *Root polynomials and their role in the theory of matrix polynomials*, Linear Algebra Appl., 584 (2020), pp. 37–78.
- [8] F. M. DOPICO, M. C. QUINTANA, AND P. VAN DOOREN, *Strongly minimal self-conjugate linearizations for polynomial and rational matrices*, SIAM J. Matrix Anal. Appl., 43 (2022), pp. 1354–1381, <https://doi.org/10.1137/21M1453542>.
- [9] E. EMRE, *Nonsingular factors of polynomial matrices and (A, B)-invariant subspaces*, SIAM J. Control Optim., 18 (1980), pp. 288–296, <https://doi.org/10.1137/0318020>.
- [10] A. FAZZI, N. GUGLIELMI, AND I. MARKOVSKY, *Generalized algorithms for the approximate matrix polynomial GCD of reducing data uncertainties with application to MIMO system and control*, J. Comput. Appl. Math., 393 (2021), 113499.
- [11] S. FRIEDLAND, *Matrices—Algebra, Analysis and Applications*, World Scientific, Hackensack, NJ, 2016.

Downloaded 10/18/23 to 130.233.58.71 . Redistribution subject to SIAM license or copyright; see <https://pubs.siam.org/terms-privacy>

- [12] I. GOHBERG, M. A. KAASHOEK, L. LERER, AND L. RODMAN, *Common multiples and common divisors of matrix polynomials. I: Spectral method*, Indiana Univ. Math. J., 30 (1981), pp. 321–356.
- [13] I. GOHBERG, M. A. KAASHOEK, L. LERER, AND L. RODMAN, *Common multiples and common divisors of matrix polynomials. II: Vandermonde and resultant*, Linear Multilinear Algebra, 12 (1982), pp. 159–203.
- [14] I. GOHBERG, P. LANCASTER, AND L. RODMAN, *Matrix Polynomials*, Academic Press, New York, London, 1982.
- [15] D. HENRION AND M. SEBEK, *Reliable numerical methods for polynomial matrix triangularization*, IEEE Trans. Automat. Control, 44 (1999), pp. 497–508.
- [16] T. KAILATH, *Linear Systems*, Prentice-Hall, Englewood Cliffs, NJ, 1980.
- [17] L. LERER AND M. TISMENETSKY, *The Bezoutian and the eigenvalue-separation problem for matrix polynomials*, Integral Equations Operator Theory, 5 (1982), pp. 386–445.
- [18] M. MONESS AND B. LANTOS, *Exact computation of the greatest common divisor of two polynomial matrices*, Period. Polytech. Electr. Eng. (Arch.), 26 (1982), pp. 266–280.
- [19] Y. NAKATSUKASA, V. NOFERINI, AND A. TOWNSEND, *Vector spaces of linearizations for matrix polynomials: A bivariate polynomial approach*, SIAM J. Matrix Anal. Appl., 38 (2017), pp. 1–29, <https://doi.org/10.1137/15M1013286>.
- [20] V. NOFERINI, L. NYMAN, J. PÉREZ, AND M. C. QUINTANA, *Perturbation Theory of Transfer Function Matrices*, preprint, <https://arxiv.org/abs/2207.06791>.
- [21] V. NOFERINI AND P. VAN DOOREN, *On Computing Root Polynomials and Minimal Bases of Matrix Pencils*, preprint, <https://arxiv.org/abs/2110.15416>.
- [22] V. NOFERINI AND P. VAN DOOREN, *Root vectors of polynomial and rational matrices: Theory and computation*, Linear Algebra Appl., 656 (2023), pp. 510–540.
- [23] H. H. ROSENBROCK, *State-Space and Multivariable Theory*, John Wiley & Sons, New York, 1970.
- [24] L. M. SILVERMAN AND P. VAN DOOREN, *A system theoretic interpretation for GCD extraction*, IEEE Trans. Automat. Control, 26 (1981), pp. 1273–1276.
- [25] P. VAN DOOREN, *The computation of Kronecker’s canonical form of a singular pencil*, Linear Algebra Appl., 27 (1979), pp. 103–141.
- [26] P. VAN DOOREN, *The generalized eigenstructure problem in linear system theory*, IEEE Trans. Automat. Control, 26 (1981), pp. 111–129.
- [27] P. VAN DOOREN, *Deadbeat control, a special inverse eigenvalue problem*, BIT, 24 (1984), pp. 681–699.
- [28] P. VAN DOOREN, *Rational and polynomial matrix factorizations via recursive pole-zero cancellation*, Linear Algebra Appl., 137/138 (1990), pp. 663–697.
- [29] G. VERGHESE, P. VAN DOOREN, AND T. KAILATH, *Properties of the system matrix of a generalized state space system*, Internat. J. Control, 30 (1979), pp. 235–243.
- [30] W. A. WOLOVICH, *Linear Multivariable Systems*, Springer-Verlag, New York, 1974.
- [31] M. WONHAM, *Linear Multivariable Control: A Geometric Approach*, Springer-Verlag, New York, 1974.
- [32] J. C. ZÚÑIGA ANAYA AND D. HENRION, *An improved Toeplitz algorithm for polynomial matrix null-space computation*, Appl. Math. Comput., 207 (2009), pp. 256–272.