# Computing the Rank and a Small Nullspace Basis of a Polynomial Matrix[*]

Arne Storjohann
School of Computer Science, U. Waterloo
Waterloo Ontario N2L 3G1 Canada
http://www.scg.uwaterloo.ca/~astorjoh

Gilles Villard
CNRS, LIP, École Normale Supérieure de Lyon
46, Allée d'Italie, 69364 Lyon Cedex 07, France
http://perso.ens-lyon.fr/gilles.villard

## ABSTRACT

We reduce the problem of computing the rank and a nullspace basis of a univariate polynomial matrix to polynomial matrix multiplication. For an input $n \times n$ matrix of degree $d$ over a field $\mathsf{K}$ we give a rank and nullspace algorithm using about the same number of operations as for multiplying two matrices of dimension $n$ and degree $d$. If the latter multiplication is done in $\mathsf{MM}(n,d) = O\tilde{~}(n^\omega d)$ operations, with $\omega$ the exponent of matrix multiplication over $\mathsf{K}$, then the algorithm uses $O\tilde{~}(\mathsf{MM}(n,d))$ operations in $\mathsf{K}$. For $m \times n$ matrices of rank $r$ and degree $d$, the cost expression is $O\tilde{~}(nmr^{\omega-2}d)$. The soft-O notation $O\tilde{~}$ indicates some missing logarithmic factors. The method is randomized with Las Vegas certification. We achieve our results in part through a combination of matrix Hensel high-order lifting and matrix minimal fraction reconstruction, and through the computation of minimal or small degree vectors in the nullspace seen as a $\mathsf{K}[x]$-module.

**Categories and Subject Descriptors:** I.1[**Symbolic and Algebraic Manipulation**]: Algorithms; F.2.1[**Analysis of Algorithms and Problem Complexity**]: Numerical Algorithms and Problems—*Computations on matrices*

**General Terms:** Algorithms

**Keywords:** linear algebra, polynomial matrix, matrix rank, nullspace basis, minimal polynomial basis

## 1. INTRODUCTION

Two $n \times n$ univariate polynomial matrices over a field $\mathsf{K}$, whose entries have degree $d$ at most, can be multiplied in $\mathsf{MM}(n,d) = O\tilde{~}(n^\omega d)$ operations in $\mathsf{K}$ [7, 9] where $\omega$ is the exponent of matrix multiplication over $\mathsf{K}$ [8, Chapter 15]. For $M \in \mathsf{K}[x]^{n\times n}$ of degree $d$ we propose an algorithm that uses about the same number of operations for computing the rank $r$ of $M$ over $\mathsf{K}(x)$, and $n-r$ linearly independent vectors $N_i$ in $\mathsf{K}[x]^n$ such that $N_iM = 0$, $1 \le i \le n-r$. The cost of the algorithm is $O\tilde{~}(\mathsf{MM}(n,d)) = O\tilde{~}(n^\omega d)$ operations in $\mathsf{K}$. If $M$ is $m \times n$ of rank $r$, a more precise and rank-sensitive expression of the cost is $O\tilde{~}(nmr^{\omega-2}d)$ (see Theorem 7.3). The soft-O notation $O\tilde{~}$ indicates missing logarithmic factors $\alpha(\log n)^\beta(\log d)^\gamma$ for three positive real constants $\alpha, \beta, \gamma$. We mention previous works on the subject in Section 2. Our main idea is to combine *matrix lifting* techniques [29, 30], minimal bases computation and *matrix fraction reconstruction* [1, 15, 16], together with a *degree/dimension compromise* for keeping the cost of the computation as low as possible. Within the target complexity, lifting used alone only allows to obtain few vectors of large degrees, while minimal bases used alone only leadx to an incomplete set of vectors of small degrees.

Our study extends the knowledge of the interaction between *matrix multiplication* and other *basic linear algebra problems* on matrices over $\mathsf{K}[x]$. The interaction is quite well known for linear algebra over an abstract field. For instance we refer to the survey [8, Chapter 16] for a list of problems on matrices in $\mathsf{K}^{n\times n}$ that can be solved in $O(n^\omega)$ or $O\tilde{~}(n^\omega)$ operations in $\mathsf{K}$. Only recent results give an analogous view (although incomplete) of the situation for polynomial matrices. It is known that the following problems can be solved with $O\tilde{~}(\mathsf{MM}(n,d))$ operations: *linear system solution*, *determinant*, *order d approximants*, *Smith normal form*, and, for a non-singular matrix, *column reduction* [15, 29, 30]. It is possible to compute the *inverse* of a generic matrix in essentially optimal time $O\tilde{~}(n^3d)$ [16]. We may also consider the problem of computing the *Frobenius normal form*, thus in particular the *characteristic polynomial*, of a square matrix. It does not seem to be known how to calculate the Frobenius form in time $O\tilde{~}(\mathsf{MM}(n,d))$. The best known estimate $O\tilde{~}(n^{2.7}d)$ is given in [21] (see also [18]) with $\omega = 2.376$ [11].

Hence, we augment the above list of problems solved in $O\tilde{~}(\mathsf{MM}(n,d))$ with the *certified computation of the rank* and a *nullspace basis*. This improvement is made possible by combining in a new way the key ideas of [15, 16, 29]. For the rank, the target complexity $O\tilde{~}(\mathsf{MM}(n,d))$ was only attainable by a Monte Carlo (non-certified) approach consisting in computing the rank of $M(x_0)$ for $x_0$ a random value in $\mathsf{K}$.

In obtaining a certified value of the rank and a nullspace basis within the target complexity, a difficulty is related to the output size. For $M \in \mathsf{K}[x]^{2n\times n}$ of degree $d$ and rank $n$, Gaussian elimination (fraction free or using evaluation/interpolation) leads to a basis of $n$ vectors of degrees $nd$ in $\mathsf{K}[x]^{2n}$ in the worst-case, hence to an output size in $\Theta(n^3d)$. A complexity in $O\tilde{~}(n^\omega d)$ must therefore rely on a different strategy.

[*] An extended version including proofs is available as the research report [31] (http://www.ens-lyon.fr/LIP/Pub).

*ISSAC'05,* July 24–27, 2005, Beijing, China.

We propose a sort of elimination scheme based on *minimal polynomial bases.* A minimal basis of the nullspace as $\mathsf{K}[x]$-module is a basis with lowest possible degrees (all necessary definitions are given in Section 3). For $M \in \mathsf{K}[x]^{2n\times n}$ as above, the total size of a minimal basis of the nullspace is in $O(n^2d)$ (see Theorem 3.3). However, it is not known how to reduce the problem of computing such a basis to that of polynomial matrix multiplication. In the same context, minimal bases have been already used for computing the inverse of a polynomial matrix in [16], but only the generic case has been solved. Indeed, for a generic $M \in \mathsf{K}[x]^{2n\times n}$, the degrees in a minimal basis of the nullspace are all equal to the input degree $d$, and somehow, a basis is easy to compute in $O\tilde{}(\mathsf{MM}(n,d))$ operations [16, Section 4]. In the general case, the vector degrees in a minimal basis may be unbalanced, they range between 0 to $nd$. Known methods whose cost is essentially driven by the highest degree do not seem to allow our objective (see Section 2).

Our solution presented in Section 7 is to slightly relax the problem, and to compute a small degree—rather than minimal—nullspace basis in a logarithmic number of steps. We rely on the fact that even in the unbalanced degree case, the sum of the degrees remains bounded by $nd$ (Theorem 3.3). Intuitively, at step $k$ for $1 \leq k \leq \log_2 n$, we compute about $n/2^k$ nullspace vectors of degrees less than $2^kd$. Algorithm $\mathsf{Nullspace_{2n}}$ (Section 7), for the whole nullspace, calls at most $\log_2 n$ times Algorithm Nullspace minimal vectors (Section 6), for nullspace vectors of bounded degree $\delta$, with increasing degree thresholds $\delta$. To keep the cost as low as possible, the degree increase requires to reduce the dimensions of involved matrices in the same proportion (see (14)). We refer to an analogous degree/dimension compromise in [30, Section 17] for computing the Smith normal form, and in [16, Section 2] for matrix inversion.

**Algorithm overview.** For a general view of the process, including *successive compressions* of the problem into smaller problems for reducing dimensions, consider

$$M = \begin{bmatrix} A \\ B \end{bmatrix} \in \mathsf{K}[x]^{m\times n} \tag{1}$$

with $A$ square and non-singular. The rows of the matrix $[BA^{-1} \; -I_{m-n}]$ give a basis of the nullspace of $M$. However, as noticed previously a direct calculation of $BA^{-1}$ would be too expensive. Now, note that if $[BA^{-1} \; -I_{m-n}] = S^{-1}N$, for $S$ and $N$ two appropriate polynomial matrices, then the rows of $S[BA^{-1} \; -I_{m-n}] = N$ are also in the nullspace. Considering polynomial matrices $N$ and $S$ instead of $[BA^{-1} \; -I_{m-n}]$ will take advantage of minimal bases properties, and allow us to manipulate smaller degrees.

For computing a nullspace basis we proceed the following way. We deal with a small number of submatrices of the initial input for reducing the problem to

$$M = \begin{bmatrix} A \\ B \end{bmatrix} \in \mathsf{K}[x]^{(n+p)\times n},\ 1 \leq p \leq n, \tag{2}$$

and introduce *compressing matrices* $P \in \mathsf{K}[x]^{n\times p}$. The successive choices of $p$ are guided by the compromise with the degree. For a given $p$, we start with a matrix lifting/fraction reconstruction phase. We compute an expansion of $H = BA^{-1}$ in $\mathsf{K}[[x]]^{p\times n}$ using [29, 30] to sufficiently high order $\eta$, and "compress" it to $H_p = BA^{-1}P \in \mathsf{K}[[x]]^{p\times p}$. A reconstruction phase [1, 15] (see also the comments about coprime factorization in Section 2) then gives

$$H_p = S^{-1}N_p = BA^{-1}P. \tag{3}$$

We prove that "good" choices of $P$ imply that $S$, denominator matrix for $H_p$, is also a denominator matrix for $H$ (Proposition 4.1) and that vectors in the nullspace of $M$ can be recovered (Proposition 5.4). Indeed, the computation of $S[H \; -I_{m-n}] \bmod x^{\delta+1}$ gives row vectors in the nullspace of degrees bounded by $\delta$ (Proposition 6.4).

From a candidate Monte Carlo value $r_0$ for the rank, in $\log_2 n$ steps of compression/uncompression (and choices of $\delta$ and $p$) combined with matrix lifting/matrix fraction reconstruction, we are able to compute candidate vectors for a nullspace basis. A final multiplication certifies that the rank is correct (i.e., $r_0 = r$) and that a nullspace has actually been computed (Section 7.2). Although for each degree threshold $\delta$ we compute a minimal basis for the nullspace of (2), the compression strategy unfortunately does not lead to a minimal basis for the whole nullspace of (1). However, we prove that small degree vectors are obtained (Proposition 7.1).

Our algorithms are randomized of Las Vegas kind—always correct, probably fast. Randomization is linked to the compression stages where the matrices $P$ are chosen at random. We also use random matrices $Q$ over $\mathsf{K}$ for linear independence preconditioning [10], or random evaluation points $x_0$ in $\mathsf{K}$. Our results are proven for symbolic points $x_0$ and matrices $P$ and $Q$. By evaluation [12, 34, 27], the same results hold with high probability for random $x_0$, $P$ and $Q$ if $\mathsf{K}$ has enough elements (Remark 7.4). The cost estimates might increase by poly-logarithmic factors in the case of small fields (with the introduction of an algebraic extension). We skip the details here, and refer for instance to the techniques used in [10, 19, 20] and to the references therein.

**Complexity estimates.** We study the cost of the algorithms by bounding the number of field operations in $\mathsf{K}$ on an algebraic random access machine. In [15] and [30], *ad hoc* cost functions have been defined for matrix polynomial problems that can be reduced recursively to matrix polynomial multiplication:

$$\mathsf{MM}'(n,d) = \sum_{i=0}^{\log_2 d} 2^i \mathsf{MM}(n, 2^{-i}d) \tag{4}$$

and

$$\overline{\mathsf{MM}}(n,d) = \sum_{i=0}^{\log_2 n} 4^i \mathsf{MM}(2^{-i}n, d) + n^2(\log n)\mathsf{B}(d) \tag{5}$$

where $\mathsf{B}(d)$ is the cost for solving the extended gcd problem for two polynomial in $\mathsf{K}[x]$ of degree bounded by $d$.

The two techniques we combine are lifting and matrix fraction reconstruction. Lifting for computing the expansion of $BA^{-1}$ to the order $\eta$ (see Step (c) in Section 6) has cost

$$O(\overline{\mathsf{MM}}(n,d) + \log(\eta/d)\lceil p\eta/nd\rceil \mathsf{MM}(n,d)) \tag{6}$$

operations in $\mathsf{K}$ [30, Proposition 15]. From the latter expansion of $BA^{-1}$ we will solve (3) (see Step (e) in Section 6) in

$$O(\mathsf{MM}'(p,\eta) + \eta\mathsf{MM}(p)) \tag{7}$$

operations in $\mathsf{K}$ [15, §2]. These rather technical complexity notations has been proposed for capturing the reduction to polynomial matrix multiplication. Both (6) and (7) concern algorithms that work in a logarithmic number of stages, with matrices whose dimensions and degrees are changing [15, 30].

We will keep both (6) and (7) in $O\tilde{~}(\mathsf{MM}(n,d))$ by retricting $p\eta$ to $O(nd)$ (degree/dimension compromise). For simplifying the cost results in this paper we consider either that $\mathsf{MM}(n,d) = O(n^\omega \mathsf{M}(d))$ [9], or, when the field $\mathsf{K}$ has at least $2d+1$ elements [6, 7], $\mathsf{MM}(n,d) = O(n^\omega d + n^2\mathsf{M}(d))$. Here $\mathsf{M}(d)$ is the number of operations in $\mathsf{K}$ required for multiplying two polynomials in $\mathsf{K}[x]$ of degree $d$. Hence, taking $\mathsf{M}(d) = O(d \log d \log\log d)$ [9], and $\mathsf{B}(d) = O(\mathsf{M}(d)\log d)$ [22, 26], we assume that

$$\begin{aligned} \mathsf{MM}'(n,d) &= O(\mathsf{MM}(n,d)\log d), \\ \overline{\mathsf{MM}}(n,d) &= O((\mathsf{MM}(n,d) + n^2\mathsf{B}(d))\log n). \end{aligned} \tag{8}$$

If the assumption (8) is not made then some of our cost results that use $\mathsf{MM}(n,d)$ are not valid. However, we state our algorithms in terms of polynomial matrix multiplication; precise complexity estimates in terms of the cost functions (4) and (5) could be derived with some extra care.

## 2. PREVIOUS WORKS

The rank and a basis for the nullspace of a matrix $M \in \mathsf{K}[x]^{m\times n}$ of degree $d$ and rank $r$ may be computed by fraction free Gaussian elimination in $O\tilde{~}(nmr^{\omega-1}d)$ operations in $\mathsf{K}$ [28, Chapter 2]. The same asymptotic estimate may also be obtained using evaluation/interpolation techniques such as Chinese remaindering [14, Section 5.5].

Therefore, compared to these classical approaches, we improve the cost by a factor $n$ in the worst-case ($2n \times n$ full column-rank matrix).

An elimination strategy specific to polynomial matrices is given in [24] that improves, asymptotically in the dimensions, on $O\tilde{~}(nmr^{\omega-1}d)$ , and computes the rank by a deterministic algorithm in $O(nmrd^2)$ operations in $\mathsf{K}$. But how to incorporate matrix multiplication, and generalize the approach to computing the nullspace, is not known.

An alternative to the *matrix over the polynomials* approach above is to *linearize* the problem. A first type of linearization is to consider a degree one matrix of larger dimension with the same structural invariants (see the definition of the Kronecker indices in Section 3) [4]. A degree one matrix is a *matrix pencil* and an important literature exists on the topic. A minimal nullspace basis of a pencil may be computed through the calculation of the *Kronecker canonical form.* To our knowledge, the best known complexity for computing the Kronecker form of an $m \times n$ pencil is $O(m^2n)$ [3, 23, 25]. Taking into account the dimension increase due to the linearization we may evaluate that computing a minimal basis of $M$ would cost $O((md)^2(nd)) = O(m^2nd^3)$. This approach is superior to ours concerning the quality of the output basis which is minimal. However, it is unclear how it can lead to the reduction to polynomial matrix multiplication that we establish. A second alternative and different linearization of the problem is to associate to $M$ a generalized *Sylvester matrix* (i.e., a block-Toeplitz matrix [5]) or another type of *resultant.* This has been heavily used for control theory problems and in linear algebra. A polynomial vector of degree $\delta$ in the nullspace of $M$ may be obtained from the nullspace of a block-Toeplitz of dimension about $n\delta$. This leads to costs too high by a factor of $n$ when the degrees in a minimal nullspace basis are unbalanced. We are not aware of an approach based on successive compression here that would allow to save a factor $n$ and to introduce polynomial matrix multiplication.

These two types of linearization correspond to two main approaches—*via* state-space realizations or resultants— for the problem of *coprime matrix fraction description* or *coprime factorization* [17, Chapter 6]. We see from (3) that we will use a solution to the latter problem a logarithmic number of times. If all matrices involved are of degree $d$, then we use the $\sigma$-basis algorithm of [1], and the corresponding reduction to polynomial matrix multiplication of [15]. A solution of the coprime factorization in case of unbalanced degree, in a way similar to the block-Toeplitz approach, is faced with the question of saving a factor $n$ in the cost. Known algorithms seem to have a cost driven only by the highest degree in the factorization, rather than by the sum of the involved degrees as we propose.

Our work is a derivation of an elimination scheme using minimal bases directly on polynomial matrices. Our compression/uncompression strategy can be compared to the techniques used for the staircase algorithm of [3, 25] for preserving a special structure. We somehow generalize the latter to the case of polynomial matrices for reducing the factorization problem with input $BA^{-1}$ to the polynomial matrix multiplication.

## 3. PRELIMINARIES

We give here some definitions and results about minimal bases [13] and matrix fraction descriptions that will be used in the rest of the paper. For a comprehensive treatment we refer to [17, Chapter 6]. For a matrix $M \in \mathsf{K}[x]^{m\times n}$ of rank $r$ and degree $d$, we call (left) nullspace the $\mathsf{K}(x)$-vector space of vectors $v \in \mathsf{K}(x)^m$ such that $vM = 0$. We will compute a basis of that space. The basis will be given by $m-r$ linearly independent polynomial vectors, and is related to the notion of minimal basis of the nullspace seen as a $\mathsf{K}[x]$-module.

Definition 3.1. *A basis $N_1, \ldots, N_{m-r} \in \mathsf{K}[x]^m$ with degrees $\delta_1 \le \ldots \le \delta_{m-r}$ of the nullspace of $M$ seen as a $\mathsf{K}[x]$-module is called a* minimal basis *if any other nullspace basis with degrees $\delta'_1 \le \ldots \le \delta'_{m-r}$ satisfies $\delta'_i \ge \delta_i$ for $1 \le i \le m-r$.*

In the rest of the text, *basis* will usually refer to the vector space while *minimal basis* will refer to the module. The degrees $\delta_1, \ldots, \delta_{m-r}$ are structural invariants of the nullspace. They are called the minimal indices of the nullspace basis. The minimal indices of a nullspace basis of $M$ are called the (left) *Kronecker indices* of $M$. A full row-rank polynomial matrix $N$ in $\mathsf{K}[x]^{l\times m}$ is called *row-reduced* if its leading row coefficient matrix has full rank $l$. It is called *irreducible* if its rank is full for all (finite) values of $x$ (i.e., $I_l$ is contained in the set of $\mathsf{K}[x]$-linear combinations of columns of $N$). These two definitions are used for characterizing minimal bases; we refer to [17, Theorem 6.5-10] for the proof of the following.

Theorem 3.2. *The rows of $N \in \mathsf{K}[x]^{(m-r)\times m}$, such that $NM = 0$, form a minimal basis of the nullspace of $M$ if and only if $N$ is row-reduced and irreducible.*

A key point for keeping the cost of the computation low is the *degree transfer* between $M$ and a minimal nullspace basis $N$. The McMillan degree of $M$ of rank $r$ is the maximum of the degrees of the determinants of $r \times r$ submatrices of $M$ [17, Exercise 6.5-9].

Theorem 3.3. *The Kronecker indices of $M \in \mathsf{K}[x]^{m\times n}$ of rank $r$ satisfy $\sum_{i=1}^{m-r} \delta_i \le$ McMillan-deg $M$.*

The reader may refer to [2, Theorem 5.1] for the latter bound. As discussed in the introduction, Gaussian elimination is far too pessimistic when it results in a nullspace basis with size in $\Theta(n^3 d)$. Theorem 3.3 shows that there exist minimal bases with size in $O(n^2 d)$ whose computation should be cheaper.

We will use minimal bases in relation with left or right *matrix fraction descriptions.* For $\mathcal{H} \in \mathsf{K}(x)^{l\times m}$, a left fraction description, i.e. a pair $(S,N)$ such that $\mathcal{H} = S^{-1}N$, with $S \in \mathsf{K}[x]^{l\times l}$ and $N \in \mathsf{K}[x]^{l\times m}$, is irreducible (or coprime), if any non-singular polynomial matrix and left common divisor $U$ of $S$ and $N$ ($S = US'$ and $N = UN'$ for polynomial matrices $S'$ and $N'$) is unimodular. We call (left) *denominator matrix* of $\mathcal{H}$ any non-singular polynomial matrix $S$ such that $S\mathcal{H}$ is a polynomial matrix $N$, i.e. such that $(S,N)$ is a (left) description of $\mathcal{H}$. Analogous definitions hold on the right.

Lemma 3.4. *The rows of $N = [\bar{N} \ -S]$, such that $\bar{N}M = 0$, with $S$ non-singular, form a basis for the nullspace of $M$ as a $\mathsf{K}[x]$-module if and only if $S^{-1}\bar{N}$ is irreducible.*

In Section 6 we will focus on computing only vectors of degrees bounded by a given $\delta$ in a nullspace minimal basis. We define their number $\kappa(= \kappa(\delta)) = \max\{1 \le i \le m - r \text{ s.t. } \delta_i \le \delta\}$ (the Kronecker indices are arranged in increasing order). Corresponding vectors are called $\kappa$ *first minimal vectors* in the nullspace.

# 4. MATRIX FRACTIONS AND NULLSPACE

We consider a matrix $M = [A^T \ B^T]^T \in \mathsf{K}[x]^{(n+p)\times n}$ of degree $d$ as in (2) with $A$ square $n \times n$ and invertible. Our study here and in next section focuses on the case $p \le n$ which is the heart of the method, and where all difficulties arise for establishing a cost sensitive to $p$ (see Remark 6.6).

The rows of $\mathcal{H} = [H \ -I_p] = [BA^{-1} \ -I_p]$ form a nullspace basis of $M$. Hence, for $N$ a minimal nullspace basis, there exists a transformation $S$ in $\mathsf{K}(x)^{p\times p}$ such that $S\mathcal{H} = N$. With the special shape of $\mathcal{H}$ we deduce that $S$ is a polynomial matrix in $\mathsf{K}[x]^{p\times p}$ whose columns are given by the last $p$ columns of $N$. This leads to the following left matrix fraction description of $\mathcal{H}$:

$$\mathcal{H} = [H \ -I_p] = [BA^{-1} \ -I_p] = S^{-1}[\bar{N} \ -S] = S^{-1}N. \quad (9)$$

The left fraction description $S^{-1}\bar{N}$ and $S^{-1}N$ must be irreducible by Lemma 3.4.

For reducing the cost of our approach we will introduce a (random) column compression $H_p$ of $H$ given by

$$H_p = HP = BA^{-1}P \in \mathsf{K}(x)^{p\times p} \quad (10)$$

with $P \in \mathsf{K}[x]^{n\times p}$.

In order to be appropriate for computing the nullspace of $M$, $H_p$ must keep certain invariants of $BA^{-1}$. Next proposition establishes that there exists a $P$ such that—on the left—the description $H_p = S^{-1}(\bar{N}P) = S^{-1}N_p$ *remains irreducible.* With the same $P$ the proposition also shows the existence—on the right—of a description whose *denominator matrix has relatively small degree.*

Proposition 4.1. *Let $A \in \mathsf{K}[x]^{n\times n}$ be non-singular of degree less than $d$ and determinantal degree $\nu$, and let $B \in \mathsf{K}[x]^{p\times n}$. Assume that $S \in \mathsf{K}[x]^{p\times p}$ is any denominator of a left irreducible fraction description of $BA^{-1}$. Then there exists a matrix $P$ of degree less than $d-1$ in $\mathsf{K}[x]^{n\times p}$ such that*

$$H_p = BA^{-1}P = CT^{-1} \quad (11a)$$
$$= S^{-1}N_p \in \mathsf{K}[x]^{p\times p} \quad (11b)$$

*where $CT^{-1}$ is a right irreducible description with $T \in \mathsf{K}[x]^{p\times p}$ of degree less than $\lceil \nu/p \rceil \le (n/p)d + 1$, and where $S^{-1}N_p$ is a left irreducible description.*

The proof of Proposition 4.1 [31] relies on the correspondence between the formalism of minimum generating polynomials introduced in [32, 33] and [21, Section 2], and matrix fraction denominators.

Remark 4.2. Proposition 4.1 establishes fraction properties for a symbolic $P$. As a consequence of [31, Lemma 4.1], and [32, Corollary 6.4] or [21, Section 2], the same properties hold for a random matrix $P$ unless it forms a zero of a fixed polynomial (for given $A$ and $B$) of degree $O(nd)$ in $O(nd)$ variables over $\mathsf{K}$.

# 5. COMPRESSED MINIMAL BASES

We will compute a small basis for the nullspace of the input matrix as a set of successive minimal bases of matrices like in (2). The latter minimal bases are computed in two main steps. We first compute an expansion of $H_p = BA^{-1}P$ and reconstruct a corresponding fraction (3) with denominator $S$. Then, if $P$ is such that $H_p$ satisfies (11b), we know that $S[BA^{-1} - I_p]$ is a polynomial matrix $N$, which by construction satisfies $NM = 0$.

In the spirit of the scalar polynomial case and of [1] for the matrix case, the reconstruction may be done via Padé approximation, and through the computation of particular bases of the nullspace of $[-I_p \ H_p^T]^T$. Indeed we have the equivalence between $S^{-1}N_p = H_p$ and $[N_p \ S]\cdot[-I_p \ H_p^T]^T = 0$. Hence the purpose of this section is to identify the bases of the nullspace of $[H_p^T \ -I_p]^T$ that actually lead to *minimal* bases $N$ for $M$.

Through a conditioning of $M$ let us first specify the location of the leading degree terms in the latter bases (see Theorem 3.3).

Lemma 5.1. *For $M$ as in (2) there exist a matrix $Q \in \mathsf{K}^{(n+p)\times(n+p)}$ such that the McMillan degree of the top $n \times n$ submatrix of $QM$ is equal to the McMillan degree of $QM$ (and of $M$). This implies that if $N$ is a minimal basis of the nullspace of $QM$, then $S = N_{\cdot,n+1..n+p}$ is row-reduced with row degrees the Kronecker indices $\delta_1,\ldots,\delta_p$.*

Remark 5.2. The property given by the multiplication by $Q$ in Lemma 5.1 will hold for a random $Q$ over $\mathsf{K}$ (compare to Remark 4.2).

In next sections, nullspace vectors $v^T$ for $M$ are easily obtained from nullspace vectors $w^T$ for $QM$, indeed $v^T = w^TQ$ satisfies $v^TM = w^TQM = 0$. This conditioning of $M$—and implicitly of $N$—will alllow us to compute $S$, and then deduce $N$, from a *shifted minimal basis* for the nullspace of $[-I_p \ H_p^T]^T$. Shifted bases are defined as usual minimal bases by changing the notion of degree. For $\bar{t}$ a fixed multi-index in $\mathbb{Z}^m$, the $\bar{t}$-degree of a vector $v$ in $\mathsf{K}[x]^m$ is

$$\bar{t}\text{-}\deg v = \max_{1\le i\le m}\{\deg v_i - \bar{t}_i\}. \quad (12)$$

Definition 5.3. *A basis of a $\mathsf{K}[x]$-submodule of $\mathsf{K}[x]^m$, given by the rows of a matrix $N$, is called $\bar{t}$-minimal if $N$ is row-reduced with respect to the $\bar{t}$-degree. Equivalently, $N \cdot x^{-\bar{t}}$ is row-reduced with respect to the usual degree (see [2, Definition 3.1]).*

For $\bar{t} = [0, \ldots, 0]$ the definition corresponds to the usual definition of minimal bases. The value $\bar{t} = [(d-1)_p, 0_p]$ below, where $(d-1)_p$ and $0_p$ respectively denote the values $d-1$ and 0 repeated $p$ times, is chosen from the degree $d-1$ of the compression matrix $P$ of Proposition 4.1. This value forces the row reduction in the last columns of the bases.

Proposition 5.4. *Let $M \in \mathsf{K}[x]^{(n+p)\times n}$ be of full rank such that the matrix $S$, formed by the last $p$ columns of a minimal basis $N$ for its nullspace, is row-reduced with row degrees the Kronecker indices $\delta_1, \ldots, \delta_p$. Assume that $P \in \mathsf{K}[x]^{n\times p}$ satisfies (11). Let $\bar{t} = [(d-1)_p, 0_p] \in \mathbb{N}^{2p}$. Then $[N_p\ S]$ is a $\bar{t}$-minimal basis for the nullspace of $[-I_p\ H_p^T]^T$ if and only if $N = S[BA^{-1}\ \ -I_p] = [\bar{N}\ \ -S]$ is a minimal basis for the nullspace of $M$.*

Most of the proof of Proposition 5.4 is technical for proving the minimality [31], the main argument comes from (11b) which allows to go from a basis to another. For compressing matrices $P$ which satisfy (11b), Proposition 5.4 establishes strong links between the nullspace of $[-I_p\ H_p^T]^T$ and the one of $M$. In particular, $[-I_p\ H_p^T]^T$ and $M$ have the same Kronecker indices. For any given $\delta$, there is a one-to-one correspondence between the vectors of $\bar{t}$-degree $\delta$ in the nullspace of $[-I_p\ H_p^T]^T$, and those of degree $\delta$ in the nullspace of $M$. This is seen from the "$S$" common part of the bases.

## 6. NULLSPACE MINIMAL VECTORS

We still consider a full column-rank matrix $M$ of degree $d$. Let $\delta$ be a fixed integer and $\kappa (= \kappa(\delta))$ be the number of vectors of degree less than $\delta$ in a minimal basis $N$ of the $\mathsf{K}[x]$-nullspace of $M$. In this section we study the cost for computing $\kappa$ such vectors.

Algorithm Nullspace minimal vectors below starts with lifting on a compressed matrix (Proposition 4.1). Then it partially (subject to the degree threshold) computes a denominator matrix $S$ through a partial $\bar{t}$-minimal basis computation. Using Proposition 5.4 the target nullspace vectors are finally obtained.

We prove the algorithm and its cost in the rest of the section. Step (a) is the conditioning seen in Section 5 to ensure the degree dominance of the last $p$ columns of $N$. Together with the randomized compression of Step (d) studied in Proposition 4.1 this will allow the computation of $S$ at Step (e). Step (b) is a randomized choice for working with a matrix $A$ non-singular at $x = 0$. The latter condition is required for computing at Step (c) the expansion of $BA^{-1}$ by lifting [29, 30]. Step (e) partly reconstructs a description $S^{-1}N_p$ from a truncated expansion of $H_p$. The computation is explained in Lemma 6.3 below, and the selection of small degree rows at Step (f) is justified. Our approach for the reconstruction is very close to the column reduction of [15, §3]. A degree less than $\delta$ in $S$ corresponds to a $\bar{t}$-degree (see (12)) less than $\delta$ in $[N_p\ S]$ (the compression using $P$ increases the degree in $N_p$ by $d-1$), and to a degree less than $\delta$ in $N$. Step (g) applies Proposition 5.4 for partly reconstructing the nullspace of $M$, and Steps (h) and (i) certify the outputs.

```
Algorithm Nullspace minimal vectors ($M$,$\delta$)
  Input:   $M \in \mathsf{K}[x]^{(n+p)\times n}$ of degree $d$,
           a degree threshold $\delta$,
           $M$ has full column-rank.
  Output:  $\kappa = \max\{1 \le i \le p \text{ s.t. } \delta_i \le \delta\}$ independent
           $N_i \in \mathsf{K}[x]^{n+p}$ of degree $\delta_i$ in the nullspace of $M$.
  (a)  $M := QM$ for a random $Q \in \mathsf{K}^{(n+p)\times(n+p)}$;
  (b)  $M := M(x + x_0)$ for $x_0$ random in $\mathsf{K}$;
       $A := M_{1..n,1..n}$;
       if $\det A(0) = 0$ then fail;  /* probably rank $M < n$ */
       $B := M_{n+1..n+p,1..n}$;
       $\eta := \delta + d + \lceil nd/p \rceil$;
  (c)  $H :=$ expansion of $BA^{-1} \bmod x^\eta$;
  (d)  $H_p := HP$ for $P$ random in $\mathsf{K}[x]^{n\times p}$, $\deg P \le d-1$;
       $\bar{t} = [(d-1)_p, 0_p] = [d-1, \ldots d-1, 0, \ldots, 0] \in \mathbb{N}^{2p}$;
  (e)  $L := [\mathcal{N}_p\ \mathcal{S}] :=$ a $\sigma$-basis with respect to
         $\bar{t}$ for $[-I_p\ \ H_p^T]^T$ of order $\eta$;
  (f)  $\kappa :=$ nb of rows of $[\mathcal{N}_p\ \ \mathcal{S}]$ of $\bar{t}$-degree at most $\delta$;
       select $\kappa$ rows $S_i$ of $\mathcal{S}$ by increasing degrees;
  (g)  $N_i := S_i[H\ \ -I_p] \bmod x^{\delta+1}$, $1 \le i \le \kappa$;
       $N_i(x) := N_i(x - x_0)Q$, $1 \le i \le \kappa$;
       $\lambda := \#\{N_i \text{ s.t. } N_iM = 0\}$;
  (h)  if $\lambda \ne \kappa$ then fail;            /* certification of $\kappa$ */
       $N^{(\delta)} :=$ the $\kappa \times (n+p)$ matrix formed by the $N_i$'s;
  (i)  if $N^{(\delta)}$ is not row-reduced then fail; /* minimality */
       else return $\kappa$ and $N_i$,  $1 \le i \le \kappa$.                □
```

The partial reconstruction of $N_p$ and $S$ (i.e., of a $\bar{t}$-minimal basis at Step (e), and of the denominator matrix at Step (f)) is done using a minimal *nullspace basis expansion*—or $\sigma$-*basis* [1]. We generalize [2, §4.2] and [15, §3] especially for the partial computation aspects.

Definition 6.1. *Let $G$ be in $\mathsf{K}[[x]]^{q\times p}$. Let $\bar{t}$ be a fixed multi-index in $\mathbb{Z}^q$. A $\sigma$-basis of (matrix-)order $d$ with respect to $\bar{t}$ for $G$ is a matrix polynomial $L$ in $\mathsf{K}[x]^{q\times q}$ such that:*

i) *$L(x)G(x) \equiv 0 \bmod x^d$;*

ii) *every $v \in \mathsf{K}[x]^q$ such that $v(x)G(x) = O(x^d)$ admits a unique decomposition $v^T = \sum_{i=1}^q \alpha_i L_i$ where, for $1 \le i \le q$, $L_i$ is the $i$th row of $L$, and $\alpha_i \in \mathsf{K}[x]$ is such that $\deg \alpha_i + \bar{t}\text{-}\deg L_i \le \bar{t}\text{-}\deg v$.*

The reader may notice that we have slightly adapted the notion of order of the original Definition 3.2 of [1] for a fully matrix point of view. We also use the notion of shifted degree (see [2]) equivalently to the notion of defect used in [1, Definition 3.1]. The following shows that a $\sigma$-basis to sufficiently high order contains a minimal basis.

Lemma 6.2. *Let us assume that a minimal nullspace basis of $G$ has $\kappa$ vectors of $\bar{t}$-degree at most $\delta$, and consider a $\sigma$-basis $L$ with respect to $\bar{t}$. For an approximation order greater than $\delta + 1$, at least $\kappa$ rows in $L$ have $\bar{t}$-degree at most $\delta$.*

Next lemma identify the situation where a $\sigma$-basis will give the exact information we need. We assume that we are in the situation of Proposition 5.4, in particular $S$ in the minimal bases has row degrees $\delta_1, \ldots, \delta_p$, the Kronecker indices of $M$ and of $[-I_p\ H_p^T]^T$. We fix a value $\delta$ and define $\kappa = \max\{1 \le i \le p \text{ s.t. } \delta_i \le \delta\}$, and $\bar{t} = [(d-1)_p, 0_p] \in \mathbb{N}^{2p}$.

LEMMA 6.3. *Let us assume we are in the situation of Proposition 5.4. Let $L$ be a $\sigma$-basis for $[-I_p\ H_p^T]^T$, with respect to $\bar{t}$, and of order of approximation at least $\eta = \delta + d + \lceil nd/p \rceil$. Then exactly $\kappa$ rows of $L$ have $\bar{t}$-degree at most $\delta$, are in the nullspace of $[-I_p\ H_p^T]^T$, and have $\bar{t}$-degrees $\delta_1, \ldots, \delta_\kappa$.*

Our proof of Lemma 6.3 is a modification of the one of [15, Lemma 3.7] for taking into account the degree threshold. We use (11a) for fixing the approximation order.

PROPOSITION 6.4. *Let $M \in \mathsf{K}[x]^{(n+p)\times n}$ be of full column-rank with Kronecker indices $\delta_1, \ldots, \delta_p$. Algorithm* Nullspace minimal vectors *with inputs $M$ and $\delta \in \mathbb{N}$ returns the quantity $\kappa = \max\{1 \leq i \leq p \text{ s.t. } \delta_i \leq \delta\}$, and $\kappa$ first minimal vectors of the nullspace of $M$. The algorithm is randomized, it either fails or returns correct values (Las Vegas fashion).*

For establishing Proposition 6.4 [31] we first verify that if the random choices of $x_0$, $Q$ and $P$ work as expected then the result is correct. This is obtained from Lemma 6.3 for the nullspace of $[-I_p\ H_p^T]^T$, and using the nullspace correspondence of Proposition 5.4 for the nullspace of $M$. Then, the certification of the outputs uses Lemma 6.2 and the test (h) for checking the value of $\kappa$. Using $\sigma$-bases properties we also show that the reduceness at Step (i) is equivalent to the minimality. Note that in any case, the computation of $\lambda$ ensures that the returned vectors are in the nullspace.

The algorithm may fail because the computed value $\kappa$ is too large. This will happen for bad choices of $P$, when the nullspace of the compressed matrix (see (11b)), and the approximating $\sigma$-basis (see (11a)), does not reflect the nullspace of $M$ correctly. Additionally, even for correct values of $\kappa$, the minimality may not be ensured without the test at Step (i). Indeed, a bad choice of $Q$, depending on $P$, may lead to a row reduction in the non-dominant part of the basis (see Lemma 5.1), and to a loss of minimality (see Proposition 5.4). In the latter case, a correctly computed value of $\kappa$ may lead to a smaller value $\lambda$ after the truncation (g) of a non-minimal vector.

The cost of Algorithm Nullspace minimal vectors is essentially given by (6) for the lifting and (7) for the $\sigma$-basis i.e the reconstruction phase. It may be stated for arbitrary values of $p$ and $\delta$ [31]. We rather give below a complexity estimate in the special case $p\delta/nd = O(1)$. The latter corresponds to the degree/dimension compromise that we will realize for the whole nullspace computation in Section 7. We also use (8) for simplifying the reduction to polynomial matrix multiplication.

COROLLARY 6.5. *Let $M \in \mathsf{K}[x]^{(n+p)\times n}$ be of full column-rank and degree $d$ with $1 \leq p \leq 2n$, and let $d \leq \delta \leq nd$. Minimal independent vectors in the nullspace of $M$, of degrees the Kronecker indices less than $\delta$, can be computed by a randomized Las Vegas (certified) algorithm in*

$$O(\mathsf{MM}(n,d)\log(nd) + n^2\mathsf{B}(d)\log n + n\mathsf{M}(nd)) \qquad (13)$$

*operations in $\mathsf{K}$ when $p\delta/nd = O(1)$.*

We see that computing minimal vectors in the nullspace at essentially the cost of multiplying two polynomial matrices relies on the *compromise between $p$ and $\delta$*. Many vectors of small degrees (large $p$ and small $\delta$) are computed using lifting to a limited order and large matrix reconstruction. Conversely, few vectors of large degrees (small $p$ and large $\delta$) are computed from a high-order lifting and reconstruction with matrices of small dimensions.

REMARK 6.6. The random compression $P$ is relevant for $p < n$. Everything we saw is valid for any $p$, however, when $p \geq n$, one may work directly with $H_p = H$ at Step (d).

# 7. NULLSPACE BASIS COMPUTATION

Corollary 6.5 which uses for (13) a compromise between $p$ and $\delta$, does not directly allow a low-cost computation of large degree vectors in a nullspace of large dimension. For the latter situation, and for computing a whole set of linearly independent vectors in the nullspace of a matrix $M$ in $\mathsf{K}[x]^{(n+q)\times n}$, we need to successively restrict ourselves to smaller nullspace dimensions (while increasing the degree). Here we take the notation $m = n + q$ for $M$ as in (1). We keep the notation $p$ for submatrices (2), and successive compressions, as in Sections 4-6 .

## 7.1 Full column-rank and $n < m \leq 2n$ case

Let $M \in \mathsf{K}[x]^{(n+q)\times n}$ with $1 \leq q \leq n$ be of degree $d$ and rank $n$. The way we restrict ourselves to smaller nullspaces is derived from the following observation. Let $C$ be in $\mathsf{K}^{(n+p)\times(n+q)}$ with $1 \leq p \leq q$. If $CM \in \mathsf{K}[x]^{(n+p)\times n}$ also has full column-rank, then let $\delta_1, \ldots, \delta_p$ be its Kronecker indices, and with the degree threshold $\delta = 2nd/p$ take $\kappa = \max\{1 \leq i \leq p \text{ s.t. } \delta_i \leq \delta\}$. Since $\sum_1^p \delta_i \leq nd$, at most $nd/\delta = p/2$, hence $\lfloor p/2 \rfloor$, vectors in a minimal basis of the nullspace of $CM$ may have degrees more than $\delta$, therefore $\kappa \geq \lceil p/2 \rceil$. From at least $p/2$ minimal vectors $D_1, \ldots, D_\kappa \in \mathsf{K}[x]^{n+p}$ of degrees at most $2nd/p$ in the nullspace of $CM$, we obtain $\kappa$ corresponding vectors $N_i = D_iC \in \mathsf{K}[x]^{n+q}$ in the nullspace of $M$.

Algorithm $\mathsf{Nullspace_{2n}}$, proven in Proposition 7.1 below, uses above observation a logarithmic number of times. For computing the whole nullspace, the algorithm generates a sequence of decreasing dimensions $p$ at Step (h). Following the observation, each time the algorithm passes through the "while loop" the dimension is divided by at least two, hence at most $O(\log_2 q)$ stages are necessary. This corresponds to $O(\log_2 q)$ calls to Nullspace minimal vectors with input $CM$ (for different matrices $C$). Each time the dimension is decreased, the degree threshold is increased in the same proportion at Step (b), we preserve the invariant

$$p\delta/(nd) = 2 \qquad (14)$$

that will be used for applying the cost estimate (13).

The proof of Proposition 7.1 [31] checks that $q$ vectors in the nullspace are actually computed. Their linear independency is ensured on the fly, and relies on the initial conditioning with $Q$ for working with a top $n \times n$ non-singular submatrix. The vectors for updating the nullspace are computed at Step (e) and Step (f) in the nullspace of $M_{\bar{I},1..n}$, with $\bar{I} = \{1, 2, \ldots, n, i_1, i_2, \ldots, i_p\}$. This is done through the construction of the *index selecting matrix* $C$ at Step (c) which selects the corresponding rows of $M$. The choice of the indices $\{i_1, i_2, \ldots, i_p\}$ at Step (a), complements the index choices at Step (g) that are kept in $I$ at Step (h) for previous stages, and will provide the linear independency by construction.

Another perhaps simpler strategy for ensuring independency could be based on randomization.

**Algorithm** $\mathsf{Nullspace}_{\mathsf{2n}}(M)$

```
  Input:   $M \in \mathsf{K}[x]^{(n+q)\times n}$ of degree $d$,
           $M$ has full column-rank and $1 \le q \le n$.
  Output:  $q$ "small" linearly independent polynomial
           vectors in the nullspace of $M$.
  $M := QM$ for a random $Q \in \mathsf{K}^{(n+q)\times(n+q)}$;
  if $\det M_{1..n,1..n}(x_0) = 0$ for $x_0$ random in $\mathsf{K}$ then fail;
  $I = \{\}$;
  $p := q$;
  while $\#I < q$
    (a)  $\{i_1, \ldots, i_p\} := \{n+1, \ldots, n+q\} \setminus I$;
    (b)  $\delta := 2nd/p$;
    (c)  construct $C \in \mathsf{K}^{(n+p)\times(n+q)}$ with
                $C_{i,i} := 1,\ 1 \le i \le n$,
                $C_{n+j,i_j} := 1,\ 1 \le j \le p$,
                and $C_{i,j} := 0$ otherwise;
    (d)  $\bar{M} := CM \in \mathsf{K}[x]^{(n+p)\times n}$;
    (e)  $\{\kappa, \{D_i, 1 \le i \le \kappa\}\} :=$
                Nullspace minimal vectors$(\bar{M}, \delta)$;
         $N_i^{(\delta)} = D_i C,\ 1 \le i \le \kappa$;
    (f)  $N^{(\delta)}$ := the matrix formed by the $N_i^{(\delta)}$'s;
    (g)  $J := \kappa$ column indices greater than $n+1$
                such that $N_{1..\kappa,J}$ is non-singular;
    (h)  $I := I \cup J$, $p := p - \kappa$;
    (i)  $N := [N^T \ \ (N^{(\delta)})^T]^T$;   /* nullspace update */
  $N := NQ$;
  return $N_i,\ 1 \le i \le q$.                                □
```

Each of the times the algorithm passes through the "while loop", the sum of the degrees of the computed vectors is bounded by the sum $nd$ of the Kronecker indices (these vectors are minimal for the nullspace of the submatrix $\bar{M}$). Hence the sum of the degrees in output is less than $nd\lceil \log_2 q \rceil$.

Proposition 7.1. *Let $M \in \mathsf{K}[x]^{(n+q)\times n}$ with $1 \le q \le n$ be of full column-rank. Algorithm $\mathsf{Nullspace}_{\mathsf{2n}}$ computes $q$ linearly independent polynomial vectors in the nullspace of $M$. If $M$ has degree $d$ then the sum of the degrees of the output vectors is less than $nd\lceil \log_2 q \rceil$. The algorithm is randomized, it either fails or returns correct values (Las Vegas fashion).*

The computed vectors $D_i$'s are minimal in the nullspace of $CM$ but the minimality is not preserved in general for the vectors $N_i$'s in the nullspace of $M$. The output basis for the nullspace as $\mathsf{K}(x)$-vector space may not be a basis for the $\mathsf{K}[x]$-module. However, Proposition 7.1 shows that if the sum of the Kronecker indices is $nd$ (the maximum possible), then the sum of the computed degrees is only within $\lceil \log_2 q \rceil$ times the optimum. We notice also that the vectors computed at the first stage are minimal vectors by Proposition 6.4 ($C = I_{n+q}$), hence the algorithm reaches the optimum for a generic matrix $M$ (the whole nullspace is computed with $p = q$). It would be interesting to study the loss of minimality compared to the Kronecker indices in the general case.

Corollary 7.2. *Let $M \in \mathsf{K}[x]^{(n+q)\times n}$ be of full column-rank and degree $d$ with $1 \le q \le n$, $q$ polynomial vectors whose degree sum is less than $nd\lceil \log_2 q \rceil$ can be computed in*

$$O((\mathsf{MM}(n,d)\log(nd) + n^2\mathsf{B}(d)\log n + n\mathsf{M}(nd))\log q) \quad (15)$$

*operations in $\mathsf{K}$ by a randomized Las Vegas (certified) algorithm.*

Since Algorithm Nullspace minimal vectors is called $O(\log q)$ times, and since $p\delta/nd = 2$, (15) is a consequence of (13).

## 7.2 General case

We now briefly give an idea of our method with a general matrix $M \in \mathsf{K}[x]^{m\times n}$ of degree $d$. The details will be found in [31, Section 7.2].

We compute the rank $r$ of $M$ and $m - r$ linearly independent and "small" polynomial vectors in the nullspace.

Our strategy first uses Monte Carlo (non-certified) randomized techniques for computing a value $r_0 \le r$, equal to $r$ with high probability (see Remark 7.4), and a full column-rank matrix $\tilde{M} \in \mathsf{K}[x]^{m\times r_0}$ of degree $d$ whose nullspace contains the nullspace of $M$. This requires, for Step (a) below, the computation of the rank of $M(x_0)$ for $x_0$ a random field value, and the multiplication $\tilde{M} = MR$ for a random $n \times r_0$ matrix $R$ over $\mathsf{K}$. We then apply the results of previous sections for computing $m - r_0$ candidate independent vectors in the nullspace of $\tilde{M}$. We finally test by multiplication whether these $m - r_0$ vectors are actually in the nullspace of $M$. A positive answer implies that $r \le r_0$, therefore certifies that $r = r_0$, and that a correct nullspace representation has been constructed.

For computing the candidate nullspace vectors, the case $m \le 2r_0$ has been treated in Section 7.1.

When $m \gg r_0$, the sum of the Kronecker indices is at most $r_0 d$, hence at most $r_0$ vectors may have degrees greater than $d$. We apply the technique of successive row indices selection of Section 7.1 for computing $m - 2r_0$ independent vectors of degrees less than $d$. We work successively with $s = \lceil (m - 2r_0)/r_0 \rceil$ submatrices $\tilde{M}^{(k)}$ of $\tilde{M}$ of size $3r_0 \times r_0$, hence having at least $r_0$ nullspace vectors of degree less than $d$. This requires $s$ calls to Algorithm Nullspace minimal vectors at Step (c). We terminate by computing $r_0$ vectors of possibly higher degrees using the case $m = 2r_0$, in one call to Algorithm $\mathsf{Nullspace}_{\mathsf{2n}}$ with input a $2r_0 \times r_0$ submatrix $\tilde{M}^{(s+1)}$ of $\tilde{M}$ at Step (d).

**Algorithm** Nullspace$(M)$

```
  Input:   $M \in \mathsf{K}[x]^{m\times n}$ of degree $d$.
  Output:  $r = \operatorname{rank} M$,
           $m - r$ "small" linearly independent polynomial
           vectors in the nullspace of $M$.
  (a)  Compute $r_0$ and $\tilde{M} \in \mathsf{K}[x]^{m\times r_0}$;
       if $m = r_0$ then return $m$ and $\{\}$;
  (b)  randomly ensure that the top $r_0 \times r_0$ submatrix
           of $\tilde{M}$ is non-singular or fail;
       $s := \lceil (m - 2r_0)/r_0 \rceil$;
  (c)  $\{N_i, 1 \le i \le m - 2r_0\} :=$
           Nullspace minimal vectors$(\tilde{M}^{(k)}, d)$ for $1 \le k \le s$;
  (d)  $\{N_i', 1 \le i \le \min\{m, 2r_0\} - r_0\} :=$
                                   $\mathsf{Nullspace}_{\mathsf{2n}}(\tilde{M}^{(s+1)})$;
       $N$ := the matrix formed by the $N_i$'s and the $N_i'$'s;
  (e)  if $NM \ne 0$ then fail;
       else return $r_0$ and $N_i,\ 1 \le i \le m - r_0$.          □
```

As in Section 7.1, the successive index selections for constructing the submatrices of $\tilde{M}$ lead to linearly independent nullspace vectors.

The proof of Theorem 7.3 [31] below takes into account (13) for the $s = O(m/r)$ calls to Nullspace minimal vectors, and (15) for the call to $\mathsf{Nullspace}_{\mathsf{2n}}$.

Theorem 7.3. *Let $M \in \mathsf{K}[x]^{m\times n}$ be of degree $d$. The rank $r$ of $M$ and $m-r$ linearly independent polynomial vectors in the nullspace of $M$ can be computed in*

$$O(nm\mathsf{MM}(r,d)/r^2 + (m/r + \log r)(\mathsf{MM}(r,d)\log(rd) + r^2\mathsf{B}(d)\log r + r\mathsf{M}(rd)))$$

*hence $O\tilde{~}(nmr^{\omega-2}d)$ operations in $\mathsf{K}$ by a randomized Las Vegas (certified) algorithm. The degree sum of the computed nullspace vectors is less than $rd\lceil\log_2 r\rceil + (m-2r)d$.*

For $m \le 2r$ we have already commented after Proposition 7.1 the quality of the degree sum bound $rd\lceil\log_2 r\rceil$. For $m \gg r$, since the sum of the Kronecker indices is no more than $rd$, we see that the bound we propose in Theorem 7.3 is within a factor asymptotically $m/r$ from the optimal.

Remark 7.4. We did not detail the probability analysis. Random values in $\mathsf{K}$ occur for: the choice of the compressing matrix $P$ for Proposition 4.1; the choice of $Q$ in Lemma 5.1 and as linear independence conditioning; a random shifting or evaluation point $x_0$ in all algorithms; the conditioning of $M$ into $\tilde{M}$ in Section 7.2. Our algorithms are deterministic if random values are replaced by symbolic variables. For a given input matrix $M$, the algorithm succeeds if the random values do not form a zero of a fixed polynomial over $\mathsf{K}$ of degree $O(nd)$ in the latter variables. The probability of success is at least $1 - cnd/|\mathsf{R}|$, for a positive real constant $c$, if the random values are chosen from a subset $\mathsf{R}$ of cardinal $|\mathsf{R}|$ of $\mathsf{K}$ [12, 34, 27] (see also our comments in Introduction).

## Concluding remarks

We compute a $\mathsf{K}(x)$-nullspace basis of an input matrix over $\mathsf{K}[x]$ as the union of few minimal $\mathsf{K}[x]$-basis of submatrices of the input matrix. It remains to compute a *minimal basis* with an analogous complexity estimate. A possible direction of work here is to ensure the irreducibility of the output basis either on the fly or *a posteriori*.

*Subsequent work* may also concern the applicability of our compression/uncompression scheme to other problems such as questions about matrix approximants or block structured matrices.

Computing a nullspace basis is added to the recent list of problems that can be solved in about the same number of operations as for multiplying two matrix polynomials. We hope that this will help in making progress for the *characteristic polynomial* [18, 21], and for (non-generic) *matrix inversion* [16].

## 8. REFERENCES

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

[2] B. Beckermann, G. Labahn, and G. Villard. Normal forms for general polynomial matrices. RR LIP 2002-1, Laboratoire LIP, ÉNS Lyon, France, 2002. To appear in *J. Symb. Comput.*

[3] T. Beelen and P.M. Van Dooren. An improved algorithm for the computation of Kronecker's canonical form of a singular pencil. *Lin. Alg. Appl.*, 105:9–65, 1988.

[4] T. Beelen and P.M. Van Dooren. A pencil approach for embedding a polynomial matrix into a unimodular matrix. *SIAM J. Matrix Anal. Appl.*, 9(1):77–89, Jan. 1988.

[5] R.R. Bitmead, S.Y. Kung, B.D.O. Anderson, and T. Kailath. Greatest common divisors via generalized Sylvester and Bezout matrices. *IEEE Trans. Aut. Control.*, 23(6):1043–1047, 1978.

[6] A. Bostan. *Algorithmique efficace pour des opérations de base en calcul formel.* PhD thesis, École Polytechnique, Palaiseau, France, Dec. 2003.

[7] A. Bostan and E. Schost. Polynomial evaluation and interpolation on special sets of points. To appear in *J. Complexity.*

[8] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory.* Volume 315, Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1997.

[9] D.G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28(7):693–701, 1991.

[10] L. Chen, W. Eberly, E. Kaltofen, B.D. Saunders, W.J. Turner, and G. Villard. Efficient matrix preconditioners for black box linear algebra. *Lin. Alg. Appl.*, 343-344:119–146, 2002.

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

[12] R. A. DeMillo and R. J. Lipton. A probabilistic remark on algebraic program testing. *Inf. Proc. Letters*, 7(4):193–195, 1978.

[13] G.D. Forney. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. Control*, 13:493–520, 1975.

[14] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, 1999.

[15] P. Giorgi, C.-P. Jeannerod, and G. Villard. On the complexity of polynomial matrix computations. In *Proc. ISSAC'03, Philadelphia, Pennsylvania, USA*, pages 135–142. ACM Press, August 2003.

[16] C.-P. Jeannerod and G. Villard. Essentially optimal computation of the inverse of generic polynomial matrices. *J. Complexity*, 21(1):72–86, 2005.

[17] T. Kailath. *Linear systems.* Prentice Hall, 1980.

[18] E. Kaltofen. On computing determinants without divisions. In *Proc. ISSAC'92, Berkeley, California USA*, pages 342–349. ACM Press, July 1992.

[19] E. Kaltofen, M.S. Krishnamoorthy, and B.D. Saunders. Parallel algorithms for matrix normal forms. *Lin. Alg. Appl.*, 136:189–208, 1990.

[20] E. Kaltofen and B.D. Saunders. On Wiedemann's method of solving sparse linear systems. In *Proc. AAECC-9*, LNCS 539, Springer Verlag, pages 29–38, 1991.

[21] E. Kaltofen and G. Villard. On the complexity of computing determinants. *Computational Complexity*, 13:91–130, 2004.

[22] D.E. Knuth. The analysis of algorithms. In *Proc. Int. Congr. Math., Nice, France*, volume 3, pages 269–274, 1970.

[23] P. Misra, P. Van Dooren, and A. Varga. Computation of structural invariants of generalized state-space systems. *Automatica*, 30:1921–1936, 1994.

[24] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symb. Comput.*, 35(4):377–401, 2003.

[25] C. Oară and P. Van Dooren. An improved algorithm for the computation of structural invariants of a system pencil and related geometric aspects. *Syst. Cont. Letters*, 30:38–48, 1997.

[26] A. Schönhage. Schnelle Berechnung von Kettenbruchenwicklungen. *Acta Informatica*, 1:139–144, 1971.

[27] J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27:701–717, 1980.

[28] A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Institut für Wissenschaftliches Rechnen, ETH-Zentrum, Zurich, Switzerland, November 2000.

[29] A. Storjohann. High-Order Lifting. In *Proc. ISSAC'02, Lille, France*, pages 246–254. ACM Press, July 2002.

[30] A. Storjohann. High-order lifting and integrality certification. *Journal of Symbolic Computation*, 36(3-4):613–648, 2003.

[31] A. Storjohann and G. Villard. Computing the rank and a small nullspace basis of a polynomial matrix. RR LIP 2005-3, Laboratoire LIP, ÉNS Lyon, France, 2005, http://www.ens-lyon.fr/LIP/Pub

[32] G. Villard. A study of Coppersmith's block Wiedemann algorithm using matrix polynomials, Feb. 1997. RR 975-I-M IMAG Grenoble, France.

[33] G. Villard. Further analysis of Coppersmith's block Wiedemann algorithm for the solution of sparse linear systems. In *Proc. ISSAC'97, Maui, Hawaii, USA*, pages 32–39. ACM Press, July 1997.

[34] R.E. Zippel. Probabilistic algorithms for sparse polynomials. In *Proc. EUROSAM*, LNCS 72, Springer Verlag, pages 216–226, 1979.