AAECC **8**, 511–537 (1997)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Fast Parallel Algorithms for Matrix Reduction to Normal Forms

Gilles Villard

LMC-IMAG, B.P. 53, F-38041 Grenoble Cedex 9, France (e-mail: gilles.villard@imag.fr.)

Received: February 29, 1996; revised version: August 29, 1997

Abstract. We investigate fast parallel algorithms to compute normal forms of matrices and the corresponding transformations. Given a matrix B in $\mathscr{M}_{n,n}(K)$, where K is an arbitrary commutative field, we establish that computing a similarity transformation P such that $F = P^{-1}BP$ is in Frobenius normal form can be done in $\mathscr{N}\mathscr{C}_K^2$. Using a reduction to this first problem, a similar fact is then proved for the Smith normal form $S(x)$ of a polynomial matrix $A(x)$ in $\mathscr{M}_{n,m}(K[x])$; to compute unimodular matrices $U(x)$ and $V(x)$ such that $S(x) = U(x)A(x)V(x)$ can be done in $\mathscr{N}\mathscr{C}_K^2$. We get that over concrete fields such as the rationals, these problems are in $\mathscr{N}\mathscr{C}^2$.

Using our previous results we have thus established that the problems of computing transformations over a field extension for the Jordan normal form, and transformations over the input field for the Frobenius and the Smith normal form are all in $\mathscr{N}\mathscr{C}_K^2$. As a corollary we establish a polynomial-time sequential algorithm to compute transformations for the Smith form over $K[x]$.

Keywords: Parallel algorithm, $\mathscr{N}\mathscr{C}_K^2$, Matrix normal forms, Unimodular matrices, Similarity matrices.

1 Introduction

The classical problem of computing canonical form of matrices is widely addressed in the literature and has many applications in various areas. In this paper we deal with the Frobenius and the Jordan normal forms of matrices over a commutative field K, and with the Smith normal form over a ring $K[x]$ of univariate polynomials.

For theoretical aspects about the existence and the computation of the normal forms, the reader may refer to [20, 6]. The forms are well understood if considered as giving informations about a module decomposition [14]. From a practical point of view, fast sequential and parallel algorithms are known to compute the normal forms themselves. The problems of computing the Frobenius and the Smith form are in class $\mathscr{P}$ (sequential polynomial-time problems) and in classes

$\mathcal{NC}$ and $\mathcal{NC}_K$. We refer to [4] for the definitions of the boolean parallel complexity class $\mathcal{NC}$ and to [8] for the arithmetic parallel complexity class $\mathcal{NC}_K$. A computational problem with input size n is in $\mathcal{NC}$ (*resp.* $\mathcal{NC}_K$) under the boolean (*resp.* arithmetic over K) model of parallel computation, if for a non-negative integer k, this problem can be solved by using $O(\log^k n)$ parallel boolean (*resp.* arithmetic) steps and a polynomial number $n^{O(1)}$ of processors.

A number of problems concerning computation of the transformation matrices have until now not been overcome. Efficient probabilistic solutions have been given but no deterministic algorithm was known to compute a transformation for the Frobenius form in $\mathcal{NC}_K$. The same question was also open for the Smith form: how to compute unimodular transformations fast and deterministically in parallel? How to obtain transformations over $K[x]$ even for small fields? Our new results will strongly rely on previous results in [25, 29] that will be referred to often throughout this paper.

We will first focus on the problem of computing a transformation for the Frobenius form. We propose a reduction of this problem to the one of computing a transformation for the Jordan normal form and we use known solutions for this latter problem. This will establish a fast parallel deterministic algorithm.

Next we will compute transformations over $K[x]$ for the Smith normal form. We will see that the problem is somehow equivalent to the one of computing a transformation for the Frobenius form (see §4.2 and §5.2). Indeed, we compute unimodular transformations from similarity transformations for an associated Frobenius form and conversely. This will give a fast parallel and a polynomial-time sequential solution.

1.1 The Smith and Frobenius Normal Forms

The normal forms we deal with are from the following two theorems of Smith and Frobenius. In the following the identity matrix of dimension n will be denoted by I_n or by I if the dimension can be deduced from the context.

Definition 1.1 *A square matrix of polynomials in $K[x]$ is said to be unimodular if its determinant is a non-zero element in K. It is easily seen that a matrix is unimodular if and only if it has an inverse over $K[x]$.*

Theorem 1.2 *If $A(x)$ is a $n \times m$ matrix of polynomials of rank r, there exist unimodular matrices $U(x)$ of dimension n and $V(x)$ of dimension m such that the only non-zero entries of $S(x) = U(x)A(x)V(x)$ are the first r diagonal entries $s_{i,i}(x)$ for $1 \leqq i \leqq r$, these latter are monic and $s_{i,i}(x)$ is a factor of $s_{i+1,i+1}(x)$ for $1 \leqq i < r$. The diagonal form satisfying these conditions is unique.*

We call this unique form $S(x)$ the Smith normal form of $A(x)$. Further, σ polynomials among the $s_{i,i}(x)$ are not units in $K[x]$, say for $r - \sigma + 1 \leqq i \leqq r$, we will call them the non-trivial invariant factors of $A(x)$ and denote them by $s_1(x), \ldots, s_\sigma(x)$. The square diagonal submatrix of $S(x)$ consisting of the σ non-trivial invariant factors will be denoted by $S_\sigma(x)$.

Theorem 1.3 *If B is a $n \times n$ matrix with entries in K, B is similar to a matrix F ($F = P^{-1}BP$ with P over K) which is block-companion, the polynomials associated to the companion blocks are the non-trivial invariant factors of $xI - B$.*

This unique form F is called the Frobenius normal form of B.

1.2 Previous Algorithms and Limitations

We overview the known methods and algorithms before introducing our new approach.

The first polynomial-time algorithms to compute the *Frobenius form* has been independently proposed in [19] and in [24]. They are polynomial-time in the dimension of the matrix, and also in the coefficient lengths for concrete fields such as the field of the field of the rationals Q or GF_q, the finite field with q elements. These algorithms consist in elimination processes and are consequently highly sequential. They can be adjusted to compute an associated transformation matrix over K even for small fields [21, 10]. The n steps of the elimination process can be avoided by randomization to give Monte-Carlo or Las Vegas algorithms. The key idea used in [23, 12] is that a random construction of a transformation matrix leads with high probability to the form. This approach is proven to be reliable and efficient in [12], where corresponding sequential and fast parallel (processor efficient) probabilistic algorithms are given.

Algorithms to compute the *Smith normal form* has been first proposed for matrices of integers. Computing the diagonalization by repeated triangularizations of the matrix and of its transpose has led to the first polynomial-time algorithms in [5, 18]. Using intermediate banded and bidiagonal matrices instead of triangular ones, better complexity results are given in [27]. The same type of diagonalization has been proposed for polynomial matrices [17]; this bounds the degrees of the polynomials involved during the calculations, but seems to be inadequate to bound the coefficients of those polynomials in particular over the rational polynomials.

The first polynomial-time algorithm to compute the Smith form over $Q[x]$ appeared in [15], it is based on the Chinese remainder algorithm. Subsequently it has been established in [30] that the form and associated unimodular transformations can be computed over any ring $K[x]$, with coefficient lengths remaining polynomially bounded over $Q[x]$. The algorithm deterministically computes a conditioning of the matrix so that in one triangularization, the diagonal form is obtained. The same idea has been applied in [28] over the integers to reduce the problem to the extended gcd problem, and to compute very small transformation matrices.

A drawback of this latter method over the polynomials is that a field extension is needed if K has less than $2d \min\{n, m\} + 1$ elements, where d is the degree of the polynomials in input, and consequently the unimodular transformations are not obtained over $K[x]$ but involve elements of the extension. As for the computation of the Frobenius form, randomization can remove the sequential iterations (successive triangularizations). This has been used in [15, 16, 26, 11]. The key idea is equivalent to the one used for the Frobenius form: after a random transformation of the input matrix only one triangularization is sufficient with high probability (randomized construction of the previously seen conditioning). This gives a probabilistic parallel solution for the problem and speeds the sequential methods themselves.

All the above algorithms are sequential elimination processes that can be randomized to give fast sequential and parallel solutions. A different approach has been only recently used for algorithmic purposes. It is based on the following theorem about characteristic subspaces of a matrix [6].

Theorem 1.4 *Let B a $n \times n$ matrix with entries in K and let $\chi(x)$ be its characteristic polynomial. If $\chi_1(x)$ and $\chi_2(x)$ are relatively prime such that $\chi(x) = \chi_1(x)\chi_2(x)$ then*

$$K^n = \ker \chi_1(B) \oplus \ker \chi_2(B).$$

If $e_1, e_2, \ldots, e_{n_1}$ and $f_1, f_2, \ldots, f_{n_2}$ are bases for $\ker \chi_1(B)$ *and* $\ker \chi_2(B)$, *let P be the $n \times n$ matrix which columns are the e_i's and the f_i's in this order, then*

$$P^{-1}BP = \begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix}$$

is block-diagonal, the blocks B_1 and B_2 are of dimension n_1 and n_2.

This fact shows us that provided a factorization of the characteristic polynomial is known, B can be brought into a corresponding special form. This approach is used in [1] for sequential algorithms over finite fields, using an irreducible decomposition of the characteristic polynomial. Avoiding the factorization step, it can also be used to develop fast algorithms which work over any fields. See [13] for sequential and [25, 29] for parallel aspects. Introducing the linear factors $x - \lambda_i$, $1 \leqq i \leqq l$, of $\chi(x)$ and using an arithmetic on algebraic numbers, the Jordan, the Frobenius and the Smith normal forms can be computed fast in parallel in a deterministic way. But it was still an open question, even with this approach, to compute transformation matrices over K for the Frobenius and the Smith form.

1.3 A New Approach

To answer the raised questions about the computation of transformation matrices over an arbitrary field K both sequentially and in parallel, we propose new reductions between problems. The paper is organized as follows: we begin at §2 with basic reminders about the Hermite normal form (echelon form of the input matrix) and the Jordan normal form which will be needed as intermediate forms. In addition, for computing the Smith form, two applications of the Hermite form will allow us to focus on square non-singular matrices for the rest of the paper. In §3 we present an algorithm for computing transformations for the Frobenius form. We reduce the problem to the computation of transformation matrices for the Jordan form. This establishes that the problem *REDUCTION TO FROBENIUS FORM OVER K* (the normal form and a similarity transformation) is in $\mathcal{NC}_K^2$. Then in §4 and §5, considering K^n as a $K[x]$-module, we show how the problems of computing transformations for the Frobenius form over K and transformations for the Smith form over $K[x]$ can be viewed as equivalent. We solve the former from the latter and *vice versa*. From these results we derive an algorithm in §6 and show that the problem *REDUCTION TO SMITH FORM OVER* $K[x]$ (the normal form and unimodular transformations) is in $\mathcal{NC}_K^2$. This will also establish, as a corollary, a sequential polynomial-time algorithm which is independent of K.

2 Hermite and Jordan Normal Form: Technical Results

Two intermediate forms will play an important role: the Hermite normal form — to compute the Smith normal form — and the Jordan normal form — to compute the Frobenius normal form.

2.1 Hermite Normal Form Computation

Definition 2.1 Two matrices $A(x)$ and $A'(x)$ of polynomials are said to be right (resp. left) equivalent if there exist a unimodular matrix $V(x)$ (resp. $U(x)$) such that $A(x) = A'(x)V(x)$ (resp. $A(x) = U(x)A'(x)$). If $A(x) = U(x)A'(x)V(x)$ then $A(x)$ and $A'(x)$ are said to be equivalent.

The Hermite normal form has been originally developed for square matrices [20], it is triangular and unique if the matrix is non-singular. We are going to follow a treatment found in [16] giving the canonical form for right or left equivalence of arbitrary matrices over a principal ideal domain. For arbitrary rectangle matrices, only an echelon form can be obtained, which we will also call the Hermite normal form.

Definition 2.2 A matrix $H(x)$ of rank r is in (right) Hermite normal form if:

– r non-zero columns precede zero columns,

– the tailing non-zero element in each column is monic and of row index strictly lower than the row indexes of the tailing elements of the following columns,

– in each row which contains the tailing non-zero element of some column, the entries following that entry are of lower degree.

With such a definition, each matrix in $\mathscr{M}_{n,m}(K[x])$ is right equivalent to a unique matrix in (right) Hermite normal form; associated unimodular transformations are not unique. If $H(x)$ is square and non-singular it is upper-triangular. Fast parallel algorithms to compute the form are given in [15, 31].

Theorem 2.3 *The* (*right*) *Hermite normal form* $H(x)$ *of a polynomial matrix* $A(x)$ *and a unimodular matrix* $R(x)$ *such that* $A(x) = H(x)R(x)$ *can be computed in* $\mathscr{N}C_K^2$. *Over the rationals or finite fields* GF_q *this can be done in* $\mathscr{N}C^2$.

Transposing everything in the above, we can define a left Hermite normal form with similar properties. With the following corollary we will restrict ourselves to the case of non-singular square matrices.

Corollary 2.4 *Each matrix* $A(x)$ *in* $\mathscr{M}_{n,m}(K[x])$ *is equivalent to a matrix*

$$\begin{bmatrix} I & 0 & 0 \\ 0 & H_\tau(x) & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.1}$$

where $H_\tau(x)$ *is a square non-singular matrix of dimension* τ *in* (*right*) *Hermite normal form and which diagonal entries are at least of degrees* 1. *One can compute form* (2.1) *and associated left and right unimodular multipliers in* $\mathscr{N}C_K^2$ ($\mathscr{N}C^2$ *over* Q *and* GF_q).

Proof. Let r be the rank of $A(x)$. Applying theorem 2.3 twice we compute the left Hermite normal form $L(x)$ of $A(x)$ and the (right) Hermite normal form of $L(x)$ to obtain:

$$A(x) = U_1(x)\begin{bmatrix} H_r(x) & 0 \\ 0 & 0 \end{bmatrix} V_1(x)$$

where $H_r(x)$ is square of rank r in (right) Hermite normal form. Further, $H_r(x)$ has non-zero diagonal entries with say $r - \tau$ unit ones and in each row which contains a unit element on the diagonal, all the other entries are zero. By elementary row operations every entries above a unit diagonal one can be zeroed. Then by row and column permutations we can construct an identity submatrix with the $r - \tau$ unit diagonal entries, the other entries give $H_\tau(x)$ and the form (2.1) is obtained. □

In the rest of the paper — unless it is specified — only the (right) Hermite normal form is considered, which we will simply call the Hermite normal form.

2.2 Jordan Normal Form Computation

We now consider the parallel construction of the Jordan normal form of a matrix B in $\mathcal{M}_{n,n}(K)$.

Definition 2.5 *Each matrix B in $\mathcal{M}_{n,n}(K)$ is similar to a unique (up to permutation) block-diagonal matrix J whose blocks are banded matrices $\mathcal{J}_k(\lambda_i)$ in $\mathcal{M}_{k,k}(K)$ of the form:*

$$\begin{bmatrix} \lambda_i & 1 & 0 & \cdots \\ 0 & \lambda_i & \ddots & 0 \\ \vdots & & \ddots & 1 \\ 0 & \cdots & 0 & \lambda_i \end{bmatrix}$$

where λ_i, $1 \leqq i \leqq 1$, is an eigenvalue of B. This form is called the Jordan form of B.

In general, the exact Jordan normal form cannot be computed, as this involves finding all roots of the characteristic polynomial. Fortunately, it is well known that most of the informations given by the form can be computed over an arbitrary field. Especially, from [25] we know that a symbolic form can be computed fast in parallel. More precisely, we can compute a symbolic Jordan form in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l])$: this form gives the structure of J with indeterminates $\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l$ that take the place of the distinct eigenvalues. Each indeterminate $\tilde{\lambda}_i$ is associated with a polynomial $\Lambda_i(x)$ in $K[x]$, with the understanding that Λ_i is a representation of the corresponding eigenvalue λ_i, *i.e.* $\Lambda_i(\lambda_i) = 0$; $\Lambda_i(x)$ is a *generalized eigenvalue*. The Λ_i's are divisors of the characteristic polynomial of B. Clearly, this symbolic form is not unique, different choices are possible for the Λ_i's. Following [16, 25] we only need to distinguish between eigenvalues having Jordan blocks with different structures. We are going to consider symbolic Jordan forms corresponding to Λ_i's such that: if there is a dimension k such that λ_i and λ_j do not have the same number of Jordan blocks of dimension k then Λ_i and Λ_j are relatively prime, otherwise the representations are the same.

Theorem 2.6 *The problem of computing a symbolic Jordan form in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l])$ of a matrix B in $\mathcal{M}_{n,n}(K)$, is in $\mathcal{NC}^2_K$. Over the rationals or finite fields GF_q the problem is in $\mathcal{NC}^2$. The indeterminates are associated to generalized eigenvalues, $\Lambda_i(x)$, that are equal if and only if the corresponding eigenvalues have the same Jordan structure and are relatively prime otherwise. Further, the multiplicity of each root of $\Lambda_i(x)$ is at least the dimension of the smallest corresponding Jordan block.*

Proof. Up to the time complexity, this is theorem 7 of [25]. As shown there, the property on the $\Lambda_i(x)$'s is satisfied by computing a gcd-free basis. Using the algorithm in [9] this is done in $O(\log^2 n)$ arithmetic or boolean steps using polynomially many processors. □

3 A Transformation for the Frobenius Form

From the previous theorem concerning the symbolic Jordan form, we are going to develop an algorithm to compute a transformation P for the Frobenius form. At this point, we may emphasize that it seems hard to compute P over K fast in parallel directly, *i.e.* without using the Jordan form, for an arbitrary field. Even though this is probably easy if K is such that polynomial factorization is in $\mathcal{NC}_K$. We will need the following result of [29] to compute the form itself.

Theorem 3.1 *The problem of computing the Frobenius normal form F in $\mathcal{M}_{n,n}(K)$ of a matrix B in $\mathcal{M}_{n,n}(K)$ is in $\mathcal{NC}_K^2$. Over the rationals or finite fields GF_q the problem is in $\mathcal{NC}^2$.*

Let us give an idea of our method. Using at first a classical construction [6, 32], we obtain a transformation matrix involving the eigenvalues (indeterminates representing them), then a transformation over the input field is computed. For the former matrix, we begin by computing a transformation L for the symbolic Jordan normal form of B (lemma 3.4 and lemma 3.5), $J = L^{-1}BL$, then we consider a transformation M from the symbolic Jordan form to the Frobenius form (Lemma 3.6), $F = M^{-1}JM$, and finally we will take $P = LM$. We will have to ensure that P can be obtained over K. This will rely on the particular structure of L and on that of M.

The matrix L is computed *conformable to J i.e.* the structure of L and the way the $\tilde{\lambda}_i$ appear match the structure of J [13, 24]. Each Jordan block of dimension k of J is associated to k columns in L, the corresponding vectors form a so called *Jordan chain of length* k [6]. Note that a matrix is conformable to its symbolic Jordan normal form, if and only if it is conformable to its "true" Jordan normal form.

Definition 3.2 Let L in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l])$ be a transformation from B to its symbolic Jordan normal form, L is said to be conformable to J if:

– to each block $\mathcal{J}_k(\tilde{\lambda}_i)$ composed of the columns indexed, for a fixed j_0, from $j_0 + 1$ to $j_0 + k$ in J correspond the columns indexed from $j_0 + 1$ to $j_0 + k$ in L; the corresponding k column vectors form a Jordan chain of length k;

– these columns of L depends only on $\tilde{\lambda}_i$: their entries are elements of $K[\tilde{\lambda}_i]$;

– if two indeterminates $\tilde{\lambda}_{i_1}$ and $\tilde{\lambda}_{i_2}$ are associated to the same generalized eigenvalue $\Lambda_i(x)$, the entries in the columns of L corresponding to the blocks $\mathcal{J}_k(\tilde{\lambda}_{i_1})$ and the entries in the columns corresponding to $\mathcal{J}_k(\tilde{\lambda}_{i_2})$ are polynomials with the same coefficients.

Example 3.3 Let B and its Jordan normal form be

$$B = \begin{bmatrix} 11/4 & 7/4 & 5/4 \\ -1/2 & 1/2 & -3/2 \\ -3/4 & -7/4 & 3/4 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1-\sqrt{2} & 0 \\ 0 & 0 & 1+\sqrt{2} \end{bmatrix}.$$

The three distinct eigenvalues are simple and are thus associated to the same generalized eigenvalue $\Lambda(x)$. Further, since the dimension of the matrix is 3, $\Lambda(x)$ must be the characteristic polynomial $x^3 - 4x^2 + 3x + 2$. A matrix L conformable to J must have its three columns identical up to the indeterminates. For instance:

$$J = \begin{bmatrix} \tilde{\lambda}_1 & 0 & 0 \\ 0 & \tilde{\lambda}_2 & 0 \\ 0 & 0 & \tilde{\lambda}_3 \end{bmatrix},$$

$$L(\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3) = \begin{bmatrix} \tilde{\lambda}_1^2 - 5/4\tilde{\lambda}_1 - 9/4 & \tilde{\lambda}_2^2 - 5/4\tilde{\lambda}_2 - 9/4 & \tilde{\lambda}_3^2 - 5/4\tilde{\lambda}_3 - 9/4 \\ -1/2\tilde{\lambda}_1 + 3/2 & -1/2\tilde{\lambda}_2 + 3/2 & -1/2\tilde{\lambda}_3 + 3/2 \\ -3/4\tilde{\lambda}_1 + 5/4 & -3/4\tilde{\lambda}_2 + 5/4 & -3/4\tilde{\lambda}_3 + 5/4 \end{bmatrix}.$$

Obviously, one could obtain here a simpler matrix L. Anyway, this will not be possible in the general case since decomposition into primes and even square-free factorization of polynomials, may not be available over the ground field K. □

As a corollary of theorem 2.6, using nullspace computations over algebraic numbers [25, 9], an associated transformation matrix $L(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l)$ in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l])$ can also be computed. The following classical results are derived from [6]. Let $B^*(x)$ denote the reduced adjoint matrix of $x - B$:

$$(x - B)^{-1} = B^*(x)/\psi(x)$$

where $\psi(x)$ is the minimum polynomial of B. To construct the Jordan chains giving the columns of L, one can take, up to constants $1/k!$, certain linear combinations of the column vectors of the successive derivatives of $B^*(x)$. To ensure the algorithm works over any field, as done in [7] for the square-free decomposition, we define:

$$(x^n)^{[k]} = C_n^k x^{n-k}, \quad n, k \geqq 0.$$

By linearity, this gives a mapping $K[x] \to K[x]$ such that for any polynomial $a(x)$,

$$(a(x))^{[k]} = \frac{1}{k!}\frac{d^k a}{dx^k}, \quad k! \neq 0. \tag{3.1}$$

Lemma 3.4 *For each B in $\mathcal{M}_{n,n}(K)$ a transformation matrix $L(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l)$ for the symbolic Jordan form, conformable to J, can be computed in $\mathcal{NC}_K^2$. Over the rationals or finite fields the problem is in $\mathcal{NC}^2$.*

Proof. We refer to [6] for this construction. Let $[j_1, j_2, \ldots, j_k]$ be k consecutive columns of a Jordan block $\mathcal{J}_k(\lambda_i)$ of dimension k of J. The corresponding columns $[l_1, l_2, \ldots, l_k]$ of L constitute a Jordan chain of length k associated to λ_i:

$$(B - \lambda_i I)l_1 = 0, \quad (B - \lambda_i I)l_i = l_{i-1}, \quad 2 \leqq i \leqq k. \tag{3.2}$$

We first focus on the computation of the Jordan chains of length k for any given k and λ_i, thus working over the algebraic extension $K(\lambda_i)$. Then we will see that symbolically the transformation matrix can be computed as announced.

If the successive transforms of the adjoint $B^*(x)$, using (3.1) entry-wise, are denoted by $B^{[k]}$:

$$B^{[k]}(x) = (B^*(x))^{[k]}, \quad k \geqq 0 \tag{3.3}$$

we know [6] that

$$(B - \lambda_i I)B^{[0]}(\lambda_i) = 0, \quad (B - \lambda_i I)B^{[i]}(\lambda_i) = B^{[i-1]}(\lambda_i), \quad 2 \leqq i \leqq k. \tag{3.4}$$

We denote by κ the length of the longest Jordan chain associated to λ_i.

We first assume $k < \kappa$, $k = \kappa$ will be a particular case of this general situation. Let r_{k+1} be the rank of $B^{[\kappa-k-1]}(\lambda_i)$ and let $N_k(\lambda_i)$ be an invertible matrix such that the first r_{k+1} columns of $B^{[\kappa-k-1]}(\lambda_i)N_k(\lambda_i)$ are linearly independent and the others are null. From (3.4) the last $n - r_{k+1}$ columns of $B^{[\kappa-k]}(\lambda_i)N_k(\lambda_i)$ are eigenvectors. They belong to chains of lengths greater than k [6]. Now, we isolate the one belonging to chains of length k exactly. If r_k denotes the rank of $B^{[\kappa-k]}$, they are $r_k - 2r_{k+1}$ such eigenvectors. They are found by computing a maximal linearly independent set of vectors in the span of the last $n - r_{k+1}$ column ones of $B^{[\kappa-k]}(\lambda_i)N_k(\lambda_i)$ and linearly independent with respect to the first r_k columns of $B^{[\kappa-k-1]}(\lambda_i)N_k(\lambda_i)$. We assume that this is done by computing a transformation matrix $\tilde{N}_k(\lambda_i) = N_k(\lambda_i)M_k(\lambda_i)$ such that the columns $r_{k+1}+1, \ldots, r_k - r_{k+1}$ of $B^{[\kappa-k]}(\lambda_i)\tilde{N}_k(\lambda_i)$ satisfy this property. Once these $n_k = r_k - 2r_{k+1}$ eigenvectors belonging to the chains of length k are obtained, the chains themselves are easily derived. Indeed, let l_1 be one of these vectors, being the column c_1 of $B^{[\kappa-k]}(\lambda_i)\tilde{N}_k(\lambda_i)$, then the remaining vectors $[l_2, \ldots, l_k]$ of the associated chain (given by (3.2)) are the c_1-th columns of $B^{[\kappa-k]}(\lambda_i)\tilde{N}_k(\lambda_i)$, $k - 1 \leqq j \leqq 1$. The set of the chains constructed this way for all lengths k, $1 \leqq k \leqq n$ and all eigenvalues λ_i, $1 \leqq i \leqq l$, give the columns of a transformation matrix from B to its Jordan form [6]. For $k = \kappa$, the computation is a particular case of the above construction. The eigenvectors are directly found to form a maximal linearly independent set of columns of $B^{[0]}(x) = (B^*(x))^{[0]} = B^*(x)$. We compute them using $\tilde{N}_\kappa(x)$ such that the first r_k columns of $B^{[0]}(x)N_\kappa(x)$ are linearly independent. The rest of the chain is deduced as before.

We now perform the computation symbolically. The Jordan chains are going to be given by polynomials with equal coefficients for all the roots of a given generalized eigenvalue $\Lambda_i(x)$. Chains can be constructed for all k and i simultaneously, so we can restrict ourselves to a given k and a given $\Lambda_i(x)$. By definition of the $\Lambda_i(x)$'s, all their roots are eigenvalues with the same Jordan structure, the ranks r_{k+1} and r_k are also independent of the choice of the eigenvalue represented by $\Lambda_i(x)$. We may thus directly apply a parallel arithmetic on algebraic numbers as introduced in [25]. The eigenvalues are represented as polynomials in $K[x]/(\Lambda_i(x))$. The matrices $B^{[k]}(x)$ given by (3.3) are computed in parallel modulo $\Lambda_i(x)$. Then we apply proposition 4 in [25] (for maximal linearly independent set of columns and nullspace computation over algebraic numbers) to compute $N_k(x)$ and $M_k(x)$, with the understanding that $\tilde{N}_k(x)$ is a suitable matrix for all the roots of $\Lambda_i(x)$. The $r_k - 2r_{k+1}$ target eigenvectors are read off $B^{[k]}(x)\tilde{N}_k(x)$. For the rest of the chains, we simply pick up the corresponding columns in $B^{[\kappa-j]}(x)\tilde{N}_k(x)$, $k - 1 \leqq j \leqq 1$. Substituting the symbol x by the symbols of the symbolic eigenvalues $\tilde{\lambda}_j$ which representation is Λ_i we get the associated blocks of columns in $L(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l)$. For all the roots of a given generalized eigenvalue, the entries of the vectors of the associated chains are polynomials with the same coefficients since this true by construction [25] for the matrices $N_k(x)$ and $M_k(x)$. The matrix $L(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l)$ has been computed conformable to the Jordan form. Finally, the announced complexity is valid since it holds for matrix product, for a maximal linearly independent set of columns and for the nullspace [25]. □

We give a complement to this lemma that will be useful to show that the target transformation $P = LM$ will be actually computed over K (Theorem 3.7). This will be proven using Newton's identities [14] over any fields. The only complication requiring some extra care will concern computations over fields of characteristic p, $p > 0$.

Lemma 3.5 *Let K be a field of characteristic p, $p > 0$. Let B and L be as in lemma 3.4 and assume $\Lambda_i(x)$ to be a generalized eigenvalue representing eigenvalues associated to Jordan blocks $\mathscr{J}_{kp^\alpha}(\lambda_j)$ ($k \geqq 1$ and $\alpha \geqq 0$) which dimensions are only multiples of p^α. In particular we assume that $\Lambda_i(x)$ is a polynomial in x^{p^α}* i.e. *can be written as $\bar{\Lambda}_i(x^{p^\alpha})$. Then, the entries in $L(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l)$ of the ends of the chains (last vectors of the Jordan chains) associated to $\Lambda_i(x)$, are polynomials in x^{p^α}.*

Proof. This is a direct consequence of the previous proof. Let us compute the last vectors of the chains of length kp^α; again, the longest chains with $kp^\alpha = k_m p^\alpha = \kappa$ will be particular cases. The ends of chain are columns of

$$E_k = B^{[\kappa - 1]}(x) N_{kp^\alpha}(x) M_{kp^\alpha}(x).$$

It is sufficient to prove the claim of the lemma respectively for the three matrices of the above right-hand term.

First consider $B^{[\kappa-1]}(x)$. We view it as a matrix polynomial (of degree $d - 1$ if the minimum polynomial $\psi(x)$ is of degree d):

$$\begin{aligned} B^{[\kappa-1]}(x) = (B^*(x))^{[\kappa-1]} &= (x^{d-1})^{[\kappa-1]} + B_{d-2}(x^{d-2})^{[\kappa-1]} + \ldots + B_{\kappa-1} \\ &= C_{d-1}^{\kappa-1}\, x^{d-\kappa} + C_{d-2}^{\kappa-1} B_{d-2} x^{d-\kappa-1} + \ldots + B_{\kappa-1}\,. \end{aligned} \tag{3.5}$$

But since K is of characteristic p, $C_j^{\kappa-1} = C_j^{k_m p^\alpha - 1}$ is equal to zero if $j \neq k' p^\alpha - 1$ for some integer k'. If $j = k' p^\alpha - 1$ then $j - (\kappa - 1) = (k' - k_m)p^\alpha$ and only such powers may appear in (3.5).

Now, concerning $M_{kp^\alpha}(x)$. We very briefly describe the procedures in [3, 25] to compute a maximal linearly independent set of columns. Over an abstract field, for a set of columns $B = (B_1, \ldots, B_n)$, a maximal set is constructed by taking the columns j such that rank $(B_1, \ldots, B_{j-1}) <$ rank $(B_1, \ldots, B_j)$. Over algebraic numbers, this implies some extra work to ensure that the corresponding transformation matrix $M_{kp^\alpha}(x)$ is independent of the root of Λ_i (and further that L is conformable to J). Indeed, even if the rank of B is the same for all the roots, the choice of the columns may depend on them. We refer to [25] for a satisfying solution that consists in weighting the columns by suitable factors of the generalized eigenvalue. These latter factors can be chosen polynomials in x^{p^α} as Λ_i is. This yields a matrix $M_{kp^\alpha}(x)$ that satisfies the claimed property.

Finally, for $N_{kp^\alpha}(x)$. The nullspace of a matrix can be obtained [3] by computing a maximal linearly independent set of columns, then a maximal linearly independent set of rows and by inverting the corresponding submatrix. As indicated in Lemma 3.4, to compute a chain of length kp^α, this operation is done on $B^{[\kappa - kp^\alpha - 1]}(x)$ ($k < k_m$). For the same reason than for matrix (3.5) only p^α-th powers of x appear in $B^{[\kappa - kp^\alpha - 1]}(x)$. The property is preserved by matrix inversion and is true for $N_{kp^\alpha}(x)$. For the longest chains, we just take $\tilde{N}_\kappa(x) = M_\kappa(x)$ and the property also holds. □

From [32, 24] we now compute a transformation between a companion matrix and its Jordan normal form. This will be applied to sub-blocks of the companion blocks of the target Frobenius form.

Lemma 3.6 *Let C_χ be a $n \times n$ companion matrix with characteristic polynomial $\chi(x)$. If $\chi(x)$ is a q-th power of a square-free polynomial of degree l (C_χ has l distinct eigenvalues with the same multiplicity) then the Jordan form of C_χ is*

$$J = \mathrm{diag}(\mathscr{J}_q(\lambda_1), \mathscr{J}_q(\lambda_2), \ldots, \ldots, \mathscr{J}_q(\lambda_l)).$$

A transformation matrix M in $\mathscr{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_l])$ from J to C_χ is the $n \times n$ matrix

$$(M_q(\tilde{\lambda}_i))_{i=1}^{l}$$

where

$$M_q(x) = \begin{bmatrix} 0 & \cdots & 0 & 1 & \cdots & C_{q-1}^{n-2} x^{n-q-1} & C_{q-1}^{n-1} x^{n-q} \\ \vdots & & & & & & \\ 0 & 1 & 2x & 3x^2 & \cdots & C_1^{n-2} x^{n-3} & C_1^{n-1} x^{n-2} \\ 1 & x & x^2 & x^3 & \cdots & x^{n-2} & x^{n-1} \end{bmatrix} \in M_{q,n}(K[x]). \tag{3.6}$$

We now prove the main fact of this section by first reducing the general case to the situation of Lemma 3.6, where the Frobenius form is given by a unique invariant factor, power of a square-free polynomial.

Theorem 3.7 *Let K be a commutative field. The problem of computing the Frobenius normal form F of a matrix B in $\mathscr{M}_{n,n}(K)$ and a similarity transformation P in $\mathscr{M}_{n,n}(K)$ such that $F = P^{-1}BP$ is in $\mathscr{N}C_K^2$. Over the rationals or finite fields GF_q the problem is in $\mathscr{N}C^2$.*

Proof. The set of the invariant factors of $xI - B$, *i.e.* the Frobenius form of B, is pre-computed using Theorem 3.1. If F has σ companion blocks, let the Jordan blocks of J be numbered by increasing dimensions, considering that some blocks are of dimension 0 to have exactly σ blocks for each eigenvalue λ_i, $1 \leqq i \leqq l$. We denote these blocks by $\mathscr{J}^{(j)}(\lambda_i)$, $1 \leqq i \leqq l$ and $1 \leqq j \leqq \sigma$. For any fixed j, $1 \leqq j \leqq \sigma$, the companion block C_{s_j} of F associated to the j-th non-trivial invariant factor $s_j(x)$ is constructed from the blocks $\mathscr{J}^{(j)}(\lambda_i)$, $1 \leqq i \leqq l$. Thus each block C_{s_j} is computed independently of the others from J; in addition, by Lemma 3.4, the transformation matrix L can be split into blocks of columns corresponding to each $\mathscr{J}^{(j)}(\lambda_i)$ and C_{s_j}. Consequently, we can restrict ourselves to the computation of one of the blocks of F, let this block be the j_0-th one and be denoted by C_s with characteristic polynomial $s(x) = s_{j_0}(x)$ the j_0-th non-trivial invariant factor. By definition, each distinct eigenvalue of B is associated with a unique Jordan block in C_s.

To use the particular structure of conformable matrices we split $s(x)$ with respect to the generalized eigenvalues $\Lambda_i(x)$'s computed by Theorem 2.6. This leads us to compute a block-companion matrix $\bar{F}$ more refined than the Frobenius form. Each block of $\bar{F}$ will involve eigenvalues belonging to the same generalized eigenvalues and thus leading to the same dimension of Jordan block in C_s as required to apply Lemma 3.6. From a transformation for $\bar{F}$, a transformation for F will be easily computed. If there is d distinct $\Lambda_i(x)$ we split $s(x)$ in d factors:

$$s(x) = \chi_1(x)\chi_2(x)\ldots\chi_d(x)$$

where

$$\chi_i(x) = \gcd(s(x), \Lambda_i^n(x)), \quad 1 \leqq i \leqq d. \tag{3.7}$$

All the roots of $\chi_i(x)$, $1 \leqq i \leqq d$, are eigenvalues of B with the same Jordan structure. In addition, from identity (3.7), if it is non-trivial then $\chi_i(x)$ has the same roots as $\Lambda_i(x)$ all with multiplicity the dimension, say q, of the corresponding Jordan blocks:

$$\chi_i(x) = \prod_j (x - \lambda_j^{(i)})^q$$

the product being taken on the roots $\lambda_j^{(i)}$ of $\chi_i(x)$. If we compute a transformation from B to the block-diagonal matrix $\bar{F}$ composed of the companion blocks associated to the $\chi_i(\lambda)$

$$\bar{F} = \operatorname{diag}(C_{\chi_1}, \ldots, C_{\chi_d})$$

a transformation matrix for F is readily obtained: as a cyclic vector it suffices to take the sum of the cyclic vectors giving the blocks C_{χ_i}. Since L can be split into blocks of columns corresponding to each C_{χ_i} (Lemma 3.4), we can finally restrict ourselves to the case where F is a companion block associated to a $\chi_i(x)$. From now on, we may thus assume that F is a companion matrix of dimension n and that its characteristic polynomial is a polynomial $\chi(x)$ which roots have the same multiplicity q. Let $l' = n/q$ denote the number of distinct eigenvalues of F. The current generalized eigenvalue is $\Lambda_i(x)$.

We apply Lemma 3.4 and Lemma 3.6 to compute transformation matrices L and M in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{l'}])$. A symbolic transformation $\tilde{P}$ from B to F is

$$\tilde{P} = LM = [L_q(\tilde{\lambda}_1) | \ldots | L_q(\tilde{\lambda}_{l'})] \left[\begin{array}{c} M_q(\tilde{\lambda}_1) \\ \hline \ldots \\ \hline M_q(\tilde{\lambda}_{l'}) \end{array}\right] \tag{3.8}$$

where the $n \times q$ matrix $L_q(x)$ is formed by a Jordan chain of length q and where the $q \times n$ matrix $M_q(x)$ is given by identity (3.6). This construction gives a matrix $\tilde{P}$ in $\mathcal{M}_{n,n}(K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{l'}])$, it remains to deduce a matrix P in $\mathcal{M}_{n,n}(K)$. Actually, substituting the symbols in $\tilde{P}$ by the eigenvalues leads to such a matrix P in $\mathcal{M}_{n,n}(K)$. Indeed, the entries of $\tilde{P}$ are polynomials of $K[\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{l'}]$; simplifying them using $\chi(x)$ ($\chi(\tilde{\lambda}_i) = 0$) and using (3.8) we get homogeneous polynomials of the form

$$\begin{aligned} \tilde{P}_{ij} = p_{ij}^{(0)} + p_{ij}^{(1)}(\tilde{\lambda}_1 + \ldots + \tilde{\lambda}_{l'}) + p_{ij}^{(2)}(\tilde{\lambda}_1^2 + \ldots + \tilde{\lambda}_{l'}^2) \\ + \ldots + p_{ij}^{(n-1)}(\tilde{\lambda}_1^{n-1} + \ldots + \tilde{\lambda}_{l'}^{n-1}) \end{aligned} \tag{3.9}$$

where the $p_{ij}^{(k)}$'s are constants in K. The indeterminates $\tilde{\lambda}_i$ stands for the eigenvalues λ_i, consequently in the algebraic closure of K, the matrix P with entries

$$\begin{aligned} P_{ij} = p_{ij}^{(0)} + p_{ij}^{(1)}(\lambda_1 + \ldots + \lambda_{l'}) + p_{ij}^{(2)}(\lambda_1^2 + \ldots + \lambda_{l'}^2) \\ + \ldots + p_{ij}^{(n-1)}(\lambda_1^{n-1} + \ldots + \lambda_{l'}^{n-1}) \end{aligned} \tag{3.10}$$

is a transformation matrix for the Frobenius form. We denote by Σ_k the power sums of the distinct eigenvalues: $\Sigma_k = \lambda_1^k + \ldots + \lambda_{l'}^k$, $1 \leqq k \leqq n - 1$.

Different cases arise depending on q. Firstly, if $q \neq 0$ in K — either K is of characteristic $p = 0$ or $\gcd(q, p) = 1$ — then the Σ_k's are elements of K. They can be computed as $\Sigma_k = \bar{\Sigma}_k / q$ where the $\bar{\Sigma}_k$'s are the power sums of the zeros of $\chi(x)$ (themselves obtained by Newton's identities [14]). And, as claimed, P is a matrix in $\mathscr{M}_{n,n}(K)$:

$$P_{ij} = p_{ij}^{(0)} + p_{ij}^{(1)} \Sigma_1 + \ldots + p_{ij}^{(n-1)} \Sigma_{n-1} \in K. \tag{3.11}$$

If the division by q is not allowed, we will employ Lemma 3.5. Indeed, we can restrict ourselves to $\tilde{P}_1 = {}^t[\tilde{P}_{11}, \tilde{P}_{21}, \ldots, \tilde{P}_{n1}]$, the first column vector of $\tilde{P}$: we know the j-th column vector is computed from the first as $\tilde{P}_j = B^{j-1}\tilde{P}_1$, since we build a transformation for a companion block. Now, from the particular form of M (Lemma 3.6), $\tilde{P}_1$ is the sum of the ends of Jordan chains of length q. It is thus sufficient to prove that the entries of this sum can be computed as elements of K. We show that only selected power sums appear and that we can bypass the problem of the division by q.

Let $q = rp^{\beta}$ and β be maximal *i.e.* $\gcd(r, p) = 1$. If the assumption of Lemma 3.5 on $\Lambda^i(x)$ is true with $\alpha = \beta$, only multiples of p^{β} appear as exponents in relations (3.9) and (3.10) for the $\tilde{P}_{i1}$'s. The involved power sums are the $\Sigma_{kp^{\beta}}$'s. Analogously to the regular case ($q \neq 0$), we first compute power sums $\tilde{\Sigma}_{kp^{\beta}}$ with multiplicity r from

$$\chi_{p^{\beta}}(x) = \chi(x^{1/p^{\beta}}), \tag{3.12}$$

and the $\Sigma_{kp^{\beta}}$'s are derived by division by r. Now, if the assumption on $\Lambda_i(x)$ in Lemma 3.5 is not true. For some other invariant factor $\bar{s}(x)$ involving the same eigenvalues than $\chi(x)$ — but with a lower multiplicity $\bar{q}$ — we are led to the previous situation. We have $\bar{q} = \bar{r}p^{\bar{\beta}}$, with $\bar{\beta}$ such that $\gcd(\bar{r}, p) = 1$, and we can take $\alpha = \bar{\beta}$. Thus with $\bar{s}(x)$ and

$$\bar{\chi}(x) = \gcd(\bar{s}(x), \Lambda_i^n(x)),$$

the involved power sums can be computed as done above using relation (3.12), and used as in (3.11) to show that the sums of the ends of chain and thus P have entries in K.

To conclude the proof we have to verify that computations can be done fast in parallel. We first get the generalized eigenvalues $\Lambda_i(x)$'s, the invariant factors of $B - xI$ from Theorems 2.6 and 3.1. Then using (3.7) we simultaneously compute the $\chi_i(x)$ and solve the problem for each corresponding companion blocks. The transformation $\tilde{P}$ is obtained using Lemmata 3.4 and 3.6. It remains to compute the power sums. In the regular case, the sums with multiplicities are computed by Newton's identities as shown in [2]. For the general case, one can first search for an exponent $\bar{\beta}$ to apply Lemma 3.5. This can clearly be done in $O(\log n)$ polynomial divisions between the $\chi_i(x)$'s having the same roots but with different multiplicities. For concrete fields such as the rationals or finite fields, the problem is in $\mathscr{N}C^2$ since the algorithm is a fixed number of solutions of problems in $\mathscr{N}C^2$.

□

Example 3.8 We take the data of example 3.3 and follow the proof above. We have seen that the unique generalized eigenvalue, $\chi(x) = \chi_1(x) = x^3 - 4x^2 + 3x + 2$, is the characteristic polynomial of B. The Frobenius normal form F will be a companion block of dimension 3. A transformation matrix L for the Jordan form has been given in example 3.3. For M, using Lemma 3.6 we take:

$$\begin{bmatrix} 1 & \tilde{\lambda}_1 & \tilde{\lambda}_1^2 \\ 1 & \tilde{\lambda}_2 & \tilde{\lambda}_2^2 \\ 1 & \tilde{\lambda}_3 & \tilde{\lambda}_3^2 \end{bmatrix}.$$

Thus — after simplification using $\chi(x)$ — a transformation for F is:

$$P = LM = \begin{bmatrix} \Sigma_2 - 5/4\Sigma_1 - 27/4 & 11/4\Sigma_2 - 21/4\Sigma_1 - 6 & 23/4\Sigma_2 - 41/4\Sigma_1 - 33/2 \\ -1/2\Sigma_1 + 9/2 & -1/2\Sigma_2 + 3/2\Sigma_1 & -1/2\Sigma_2 + 3/2\Sigma_1 + 3 \\ -3/4\Sigma_1 + 15/4 & -3/4\Sigma_2 + 5/4\Sigma_1 & -7/4\Sigma_2 + 9/4\Sigma_1 + 9/2 \end{bmatrix}$$

where $\Sigma_1 = \lambda_1 + \lambda_2 + \lambda_3 = 4$ and $\Sigma_2 = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 = 10$. Consequently,

$$P = \begin{bmatrix} -7/4 & 1/2 & 0 \\ 5/2 & 1 & 4 \\ 3/4 & -5/2 & -4 \end{bmatrix}$$

is such that

$$F = P^{-1}BP = \begin{bmatrix} 0 & 0 & -2 \\ 1 & 0 & -3 \\ 0 & 1 & 4 \end{bmatrix}$$

is the Frobenius normal form of B. □

4 $K[x]$-Modules for the Smith and the Frobenius Forms

This section is intended to point out the correspondence between transformations for the Frobenius normal form of a constant matrix and transformations for the Smith normal form of a polynomial matrix. This will lead, at §5, to a reduction of the latter problem to the former and, at §6, to an algorithm based on this reduction and on Theorem 3.7.

Our approach is an extension of the one in [22] for computing normal forms of matrices. In [22], following the classical approach [14], the author computes transformations for the Frobenius normal form of a constant matrix, from transformations for the Smith normal form of an associated polynomial matrix. The algorithm is based on a similar correspondence to the one between the Frobenius form of a matrix B and the Smith form of $xI - B$ (Theorem 1.3). This section is intended to recall these basic facts. Then we will show that the converse approach also is valid, even if it is less usual, to compute transformations for the Smith form from transformations for the Frobenius one.

4.1 K^n as $K[x]$-module

The following presentation is derived from standard results in ([14], §3.10), the proofs are omitted. Let B be a matrix in $\mathscr{M}_{n,n}(K)$. We make K^n with basis (u_i),

$1 \leqq i \leqq n$, a $K[x]$-module by defining the action of x on a vector $v \in K^n$ as:

$$xv = Bv.$$

If we call N_0 the submodule of $K[x]^n$ generated by the columns of $xI - B$, N_0 is the kernel of p_0:

$$\begin{cases} p_0\colon\ K[x]^n \to K^n \\ p_0({}^t[g_1, g_2, \ldots, g_n]) = g_1u_1 + g_1u_2 + \ldots + g_nu_n \end{cases}$$

and K^n is isomorphic to $K[x]^n/N_0$. The following diagram commutes:

$$\begin{tikzcd} K[x]^n/N_0 \arrow[r, "p_0"] \arrow[d, "x"] & K^n \arrow[d, "B"] \\ K[x]^n/N_0 \arrow[r, "p_0"] & K^n \end{tikzcd}$$

Now we consider a matrix $H(x)$ equivalent to $xI - B$ with $H(x) = U_0(x)(xI - B)V_0(x)$ where $U_0(x)$ and $V_0(x)$ are invertible in $\mathscr{M}_{n,n}(K[x])$. We may assume (corollary 2.4) that $H(x)$ has the block-diagonal form:

$$\begin{bmatrix} I_{n-\tau} & \\ & H_\tau(x) \end{bmatrix} \tag{4.1}$$

where $I_{n-\tau}$ is the identity matrix of dimension $n - \tau$ and $H_\tau(x)$ is in Hermite normal form of rank τ, with diagonal entries of degrees $d_1, \ldots, d_\tau$ at least 1. As previously, if N is the submodule of $K[x]^\tau$ generated by the columns of $H_\tau(x)$, since $H(x)$ and $xI - B$ are equivalent, N is isomorphic to N_0 and we can make K^n isomorphic to $K[x]^\tau/N$. To construct a corresponding commuting diagram we choose as the natural K-basis of $K[x]^\tau/N$:

$$\overline{(1, 0, \ldots, 0)}, \overline{(x, 0, \ldots, 0)}, \ldots, \overline{(x^{d_1-1}, 0, \ldots, 0)}, \ldots$$
$$\ldots, \overline{(0, 0, \ldots, 1)}, \overline{(0, 0, \ldots, x)}, \ldots, \overline{(0, 0, \ldots, x^{d_\tau - 1})}, \tag{4.2}$$

and we denote by p the coordinate function with respect to this basis. We have:

$$\begin{tikzcd} K[x]^\tau/N \arrow[r, "p"] \arrow[d, "x"] & K^n \arrow[d, "C"] \\ K[x]^\tau/N \arrow[r, "p"] & K^n \end{tikzcd} \tag{4.3}$$

where, by construction, C is in *polycyclic* or *shift-Hessenberg* form. More precisely, C is block upper triangular with τ diagonal blocks. If the entries of $H_\tau(x)$ are denoted by:

$$h_{i,j}(x) = a_{i,0}^{(j)} + a_{i,1}^{(j)}x + \ldots + a_{i,d_i-1}^{(j)}x^{d_i-1}, \quad 1 \leqq i < j \leqq \tau$$
$$h_{i,i}(x) = a_{i,0}^{(i)} + a_{i,1}^{(i)}x + \ldots + a_{i,d_i-1}^{(i)}x^{d_i-1} + x^{d_i}, \quad 1 \leqq i \leqq \tau,$$

the diagonal blocks $C_{i,i}$ of C are the companion blocks associated to the $h_{i,i}(x)$; the upper diagonal blocks $C_{i,j}$ have non-zero entries only in their last column which is equal to ${}^t[-a_{i,0}^{(j)}, -a_{i,1}^{(j)}, \ldots, -a_{i,d_i-1}^{(j)}]$.

We can do the same thing for the submatrix $S_\sigma(x)$ of the Smith normal form of $xI - B$ formed by the σ non-trivial invariant factors,

$$S(x) = \begin{bmatrix} I & 0 \\ 0 & S_\sigma(x) \end{bmatrix}$$

the associated polycyclic form is the Frobenius normal form F of B. If we let N' be the submodule of $K[x]^\sigma$ generated by the columns of $S_\sigma(x)$, the diagram (4.3) becomes:

$$\begin{tikzcd} K[x]^\sigma/N' \arrow[r, "p'"] \arrow[d, "x"] & K^n \arrow[d, "F"] \\ K[x]^\sigma/N' \arrow[r, "p'"] & K^n \end{tikzcd} \tag{4.4}$$

where p' denotes the coordinate function according to the natural K-basis of $K[x]^\sigma/N'$:

$$\begin{aligned} &\overline{(1,0,\dots,0)}, \overline{(x,0,\dots,0)}, \dots, \overline{(x^{\delta_1-1},0,\dots,0)}, \dots \\ &\dots, \overline{(0,0,\dots,1)}, \overline{(0,0,\dots,x)}, \dots, \overline{(0,0,\dots,x^{\delta_\sigma-1})}, \end{aligned} \tag{4.5}$$

where the δ_i's are the degrees of the non-trivial invariant factors $s_i(x)$, $1 \leqq i \leqq \sigma$. We summarize in the following Lemma.

Lemma 4.1 *Let $H_\tau(x)$ be a matrix in $\mathscr{M}_{\tau,\tau}(K[x])$ of full rank which determinant is of degree n. We assume $H_\tau(x)$ to be in Hermite normal form with diagonal entries of degrees at least 1. Let $S(x)$ be its Smith normal form, $S(x) = U(x)H_\tau(x)V(x)$, and $S_\sigma(x)$ be the submatrix of $S(x)$ given by the σ non-trivial invariant factors. The columns of $H_\tau(x)$ and of $S_\sigma(x)$ generate the submodules N and N' of $K[x]^\tau$ and $K[x]^\sigma$. To $H_\tau(x)$ and $S_\sigma(x)$ we respectively associate matrices C and F in $\mathscr{M}_{n,n}(K)$: C has polycyclic form and F has Frobenius form. Then the following $K[x]$-module isomorphism diagram commutes*:

$$\begin{tikzcd} K[x]^\tau/N \arrow[r, "\phi_u"] \arrow[d, "p"] & K[x]^\sigma/N' \arrow[d, "p'"] \\ K^n \arrow[r, "p-1"] & K^n \end{tikzcd} \tag{4.6}$$

where ϕ_u is the restriction of the isomorphism associated to $U(x)$ and P is invertible in $\mathscr{M}_{n,n}(K)$ and satisfies *$F = P^{-1}CP$. The isomorphisms p and p' are the coordinate functions with respect to the bases*

$$\overline{(1,0,\dots,0)}, \overline{(x,0,\dots,0)}, \dots, \overline{(x^{d_1-1},0,\dots,0)}, \dots, \overline{(0,0,\dots,x^{d_\tau-1})}$$

$$\overline{(1,0,\dots,0)}, \overline{(x,0,\dots,0)}, \dots, \overline{(x^{\delta_1-1},0,\dots,0)}, \dots, \overline{(0,0,\dots,x^{\delta_\sigma-1})}$$

of $K[x]^\tau/N$ and $K[x]^\sigma/N'$.

Proof. Combining diagrams (4.3), diagram (4.4) and $S(x) = U(x)H_\tau(x)V(x)$ leads to the diagram (4.6) with p and p'. Taking $P = p \circ \phi_u^{-1} \circ p'^{-1}$, we have:

$$P(xu) = xP(u),\ u \in K^n, \text{ i.e. } PFu = CPu,$$

and,

$$F = P^{-1}CP$$

as announced. □

We notice that only $U(x)$ plays a role in the above construction, $H_\tau(x)$ and $S(x)$ can be considered up to a unimodular matrix $V(x)$. We also remark that from P only ϕ_u, the restriction of the isomorphism associated to $U(x)$ from $K[x]^\tau/N$ to $K[x]^\sigma/N'$, can be directly computed. We will need a "completion phase" to recover a satisfying matrix $U(x)$ from ϕ_u (see §5). Now we assume the assumptions of Lemma 4.1 are satisfied. We first look at the information given by diagram (4.6) about the relations between the matrices P^{-1} and $U(x)$ and we compute P^{-1} from $U(x)$.

4.2 From $U(x)$ to a transformation for the Frobenius normal form

To compute the columns of P^{-1} from $U(x)$, let us take K^n with the canonical basis rewritten as

$$(c_1^{(0)}, \ldots, c_1^{(d_1-1)}, \ldots, c_\tau^{(0)}, \ldots, c_\tau^{(d_\tau-1)})$$

and let

$$(e_1^{(0)}, \ldots, e_1^{(d_1-1)}, \ldots, e_\tau^{(0)}, \ldots, e_\tau^{(d_\tau-1)})$$

denotes the basis (4.2). For i, $1 \leqq i \leqq \tau$, and $j, 0 \leqq j \leqq d_i - 1$, we have:

$$\begin{aligned} P^{-1}c_i^{(j)} &= (p' \circ \phi_u \circ p^{-1})c_i^{(j)} = (p' \circ \phi_u)e_i^{(j)} = (p' \circ \phi_u)(x^j e_i^{(0)}) \\ &= x^j(p' \circ \phi_u)e_i^{(0)} = x^j p' U_i(x) = x^j \bar{U}_i = F^j \bar{U}_i \end{aligned}$$

where $U_i(x)$ is given by the vector $U^{(i)}(x)$ formed by the last σ entries of the i-th column of $U(x)$, and $\bar{U}_i$ is the image of $U_i(x)$ under p'. More precisely, as a representative $U_i(x)$ of the class $\{U^{(i)}(x) + N'\}$, one can take the unique element of the class for which the degree of the numerator of each entry of $S_\sigma^{-1}(x)\, U_i(x)$ is less than the degree of the denominator polynomial. It can be computed by finding the polynomial matrix $Q(x)$ such that:

$$U^{(i)}(x) = S_\sigma(x)Q(x) + U_i(x). \tag{4.7}$$

It can be easily seen that this consists in reducing each entry of $U^{(i)}(x)$ modulo the entry of $S_\sigma(x)$ with the same row index. Since $\sigma \leqq \tau$, invariant factors are non-constant: only the last σ rows of $U(x)$ are involved in computing P^{-1} (the others are zeroed by the reduction modulo $S_\sigma(x)$).

From the above identities and applying p' column-wise, we express P^{-1} by:

$$P^{-1} = p'\left([U^{(1)}(x), \ldots, x^{d_1-1}U^{(1)}(x), \ldots, U^{(\tau)}(x), \ldots] \bmod \begin{bmatrix} s_1(x) & & \\ & \ldots & \\ & & s_\sigma(x) \end{bmatrix} \right).$$

Equivalently, let the entries of the last σ columns of $U^{-1}(x)$ be denoted by $u_i^{(j)}(x)$, $1 \leqq j \leqq \sigma$ and $1 \leqq i \leqq \tau$, then from [14] we know that σ cyclic vectors P_j to build

P are given by:

$$P_j = u_1^{(j)}(x)c_1^{(0)} + \ldots + u_\tau^{(j)}(x)c_\tau^{(0)}, \quad 1 \leqq j \leqq \sigma. \tag{4.8}$$

These relations can be easily used to compute a transformation P for the Frobenius form, once a transformation $U(x)$ for the Smith form is known. This has been used in [22].

Example 4.2 Let $S_2(x)$ ($\tau = \sigma = 2$) the Smith normal form of $H_2(x)$ be given by:

$$\begin{aligned} S_2(x) &= U(x)H_2(x)V(x) \\ &= \begin{bmatrix} 1 & 0 \\ 2x - x^2 & 1 \end{bmatrix} \begin{bmatrix} x^2 - 1 & x + 1 \\ 0 & x^2 - x - 2 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ x & x - 1 \end{bmatrix} \\ &= \begin{bmatrix} x + 1 & 0 \\ 0 & (x-2)(x^2-1) \end{bmatrix}. \end{aligned}$$

To $H_2(x)$ we associate the matrix C in polycyclic form:

$$C = \begin{bmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Looking at the degrees of the diagonal entries of $C(x)$, for K-basis of $K[x]^\tau/N$ we take $(1,0)$, $(x,0)$, $(0,1)$, $(0,x)$. A transformation P^{-1} is constructed from the columns $U^{(1)}(x)$, $xU^{(1)}(x)$, $U^{(2)}(x)$ et $xU^{(2)}(x)$ reduced modulo the columns of $S(x)$:

$$P^{-1} = p'\left(\left[\begin{array}{cc|cc} 1 & x & 0 & 0 \\ \hline 2x - x^2 & 2x^2 - x^3 & 1 & x \end{array} \right] \bmod \begin{bmatrix} x+1 & \\ & x^3 - 2x^2 - x + 2 \end{bmatrix} \right)$$

thus,

$$U(x) = \left[\begin{array}{c|c} 1 & 0 \\ \hline 2x - x^2 & 1 \end{array} \right] \leftrightarrow P^{-1} = \left[\begin{array}{cc|cc} 1 & -1 & 0 & 0 \\ \hline 0 & 2 & 1 & 0 \\ 2 & -1 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{array} \right].$$

The Frobenius form F of C satisfies:

$$F = P^{-1} \begin{bmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix} P = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}.$$

The matrix P^{-1} is completely determined by the choice of $U(x)$. □

5 Transformations for the Smith Normal Form

We still assume that matrices are as in Lemma 4.1. Now, the problem is to compute a transformation $U(x)$ for the Smith form from a transformation P for the Frobenius form. As underlined previously, only ϕ_u, the restriction of the isomorphism associated to $U(x)$ from $K[x]^\tau/N$ to $K[x]^\sigma/N'$ is known. This will readily give us matrices $\bar{U}_{\sigma,\tau}(x)$ and $M_{\sigma,\tau}(x)$ in $\mathscr{M}_{\sigma,\tau}(K[x])$ such that

$$\bar{U}_{\sigma,\tau}(x)H_\tau(x) = S_\sigma(x)M_{\sigma,\tau}(x).$$

Then, $\bar{U}_{\sigma,\tau}(x)$ will be completed and modified to give a unimodular matrix $U(x)$.

5.1 Partial Construction

As seen above (identity (4.7)), we choose as representatives for the elements of $K[x]^\tau/N$ (resp. $K[x]^\sigma/N'$), elements of $K[x]^\tau$ (resp. $K[x]^\sigma$) taken modulo $H_\tau(x)$ (resp. modulo $S_\sigma(x)$). Let $(e_1, \ldots, e_\tau)$ and $(f_1, \ldots, f_\sigma)$ denote the constant vectors of the bases (4.2) and (4.5), they are minimal sets of generators of $K[x]^\tau/N$ and $K[x]^\sigma/N'$. Using diagram (4.6) and $\phi_u = p'^{-1} \circ P^{-1} \circ p$ we compute the matrix

$$\bar{U}_{\sigma,\tau}(x) = [\phi_u(e_1), \ldots, \phi_u(e_\tau)] \in \mathscr{M}_{\sigma,\tau}(K[x]). \tag{5.1}$$

With the chosen representation of the elements of $K[x]^\tau/N$, $\bar{U}_{\sigma,\tau}(x)$ is well defined. Since ϕ_u is an isomorphism and since the σ vectors $(f_1, \ldots, f_\sigma)$ generates $K[x]^\sigma/N'$, the rank of $\bar{U}_{\sigma,\tau}(x)$ is σ. By construction, any column of $H_\tau(x)$ is sent, under the homomorphism associated to $\bar{U}_{\sigma,\tau}(x)$: $K[x]^\tau \to K[x]^\sigma$, into the module generated by the columns of $S_\sigma(x)$. Thus there exists a matrix $M_{\sigma,\tau}(x)$ in $\mathscr{M}_{\sigma,\tau}(K[x])$ such that

$$\bar{U}_{\sigma,\tau}(x)H_\tau(x) = S_\sigma(x)M_{\sigma,\tau}(x). \tag{5.2}$$

If $\sigma = \tau$ and $\bar{U}_{\sigma,\tau}(x)$ is unimodular, we have $S(x) = S_\sigma(x)$, obviously we can take $U(x) = \bar{U}_{\sigma,\tau}(x)$. And $V(x) = M_{\tau,\tau}^{-1}(x)$ is a satisfying right multiplier.

Unfortunately, when $\sigma = \tau$, $\bar{U}_{\sigma,\tau}(x)$ may be non-unimodular and further, the generic case is $\sigma < \tau$. We show below that $\bar{U}_{\sigma,\tau}(x)$ satisfies conditions allowing it to be modified and completed to a correct transformation matrix. The matrices $\bar{U}_{\sigma,\tau}(x)$ and $S_\sigma(x)$ are left coprime.

5.2 Completion to a Unimodular Matrix

In the following, $\bar{U}_{\sigma,\tau}(x)$ has been computing by (5.1). The next proposition will be proven using two additional Lemmata.

Proposition 5.1 *If $\bar{U}_{\sigma,\tau}(x)$ is defined as in* (5.1), *then it satisfies* (5.2):

$$\bar{U}_{\sigma,\tau}(x)H_\tau(x) = S_\sigma(x)M_{\sigma,\tau}(x);$$

$\bar{U}_{\sigma,\tau}(x)$ can be completed and modified to give unimodular matrices $U(x)$ and $V(x)$ such that

$$U(x)H_\tau(x)V(x) = S(x)$$

is the Smith normal form of $H(x)$.

The first Lemma is a trivial construction.

Lemma 5.2 *Let $\bar{U}_{\sigma,\tau}(x)$ be a matrix of rank σ in $\mathscr{M}_{\sigma,\tau}(K[x])$, with $0 \leqq \sigma \leqq \tau$. Let $[\bar{H}_{\sigma,\sigma}(x), 0]$ be its Hermite normal form. Then there exists a bordering matrix $\bar{B}_{\tau-\sigma,\sigma}(x)$ in $\mathscr{M}_{\tau-\sigma,\tau}(K[x])$ such that the Hermite normal form of*

$$\bar{U}(x) = \begin{bmatrix} \bar{B}_{\tau-\sigma,\sigma}(x) \\ \bar{U}_{\sigma,\tau}(x) \end{bmatrix}$$

is

$$\begin{bmatrix} I_{\tau-\sigma} & 0 \\ 0 & \bar{H}_{\sigma,\sigma}(x) \end{bmatrix}.$$

In particular, if $\bar{H}_{\sigma,\sigma}(x) = I_\sigma$, $\bar{U}_{\sigma,\tau}(x)$ has been completed to a unimodular matrix $U(x) = \bar{U}(x)$.

Proof. Let $R(x)$ be a unimodular transformation in $\mathscr{M}_{\tau,\tau}(K[x])$ such that

$$\bar{U}_{\sigma,\tau}(x) = [0, \bar{H}_{\sigma,\sigma}(x)]R(x).$$

We can take

$$\begin{bmatrix} \bar{B}_{\tau-\sigma,\sigma}(x) \\ \bar{U}_{\sigma,\tau}(x) \end{bmatrix} = \begin{bmatrix} I_{\tau-\sigma} & 0 \\ 0 & \bar{H}_{\sigma,\sigma}(x) \end{bmatrix} R.$$

by construction, $\bar{B}_{\tau-\sigma,\sigma}$ satisfies the Lemma. □

The second Lemma gives a *skew Bezout identity*. The two considered left coprime matrices are actually *internally coprime* following the terminology of [33].

Lemma 5.3 *We consider matrices in $\mathscr{M}_{\tau,\tau}(K[x])$. Let $\bar{U}(x)$ and $S(x)$ be two left coprime non-singular matrices, $S(x)$ is assumed to be in Smith normal form, then there exist a diagonal matrix $T(x)$ and a matrix $W(x)$ such that*

$$U(x) = T(x)\bar{U}(x) + S(x)W(x) \tag{5.3}$$

is unimodular.

Proof. Since the matrices $\bar{U}(x)$ and $S(x)$ are left coprime, there exist [20] two matrices $X(x)$ and $Y(x)$ such that:

$$\bar{U}(x)X(x) + S(x)Y(x) = I_\tau. \tag{5.4}$$

We are going to prove the result in two steps. Firstly, we use the fact that the above Bezout identity (5.4) on matrix polynomials can be rewritten on well chosen scalar polynomials. Next, the Bezout coefficients obtained from these latter identities on polynomials will give target matrices $T(x)$ and $W(x)$. We compute the Hermite normal form $H_u(x)$ of $\bar{U}(x)$:

$$\bar{U}(x) = H_u(x)R(x).$$

Let $h_1(x), \dots, h_\tau(x)$ be the diagonal entries of $H_u(x)$, the $s_{1,1}(x), \dots, s_{\tau,\tau}(x)$ are the invariant factors, (5.4) may be rewritten as:

$$\begin{bmatrix} h_1 & \times & \times & \times \\ 0 & h_2 & \times & \times \\ \vdots & & \ddots & \times \\ 0 & \cdots & 0 & h_\tau \end{bmatrix} RX = \begin{bmatrix} 1 - s_{1,1}y_{1,1} & -s_{1,1}y_{1,2} & \cdots & -s_{1,1}y_{1,\tau} \\ -s_{2,2}y_{2,1} & 1 - s_{2,2}y_{2,2} & \cdots & -s_{2,2}y_{2,\tau} \\ & & \ddots & \\ -s_{\tau,\tau}y_{\tau,1} & -s_{\tau,\tau}y_{\tau,2} & \cdots & 1 - s_{\tau,\tau}y_{\tau,\tau} \end{bmatrix}.$$

For all i, $1 \leqq i \leqq \tau$, let us consider the minor computed with the last $\tau - i + 1$ rows and columns of the right-hand side matrix:

$$\begin{bmatrix} h_i & \times & \times & \times \\ 0 & h_{i+1} & \times & \times \\ \vdots & & \ddots & \times \\ 0 & \cdots & 0 & h_\tau \end{bmatrix}$$

$$\tilde{r}_i = \begin{bmatrix} 1 - s_{i,i}y_{i,i} & -s_{i,i}y_{i,i+1} & \cdots & -s_{i,i}y_{i,\tau} \\ -s_{i+1,i+1}y_{i+1,i} & 1 - s_{i+1,i+1}y_{i+1,i+1} & \cdots & -s_{i+1,i+1}y_{i+1,\tau} \\ & & \ddots & \\ -s_{\tau,\tau}y_{\tau,i} & -s_{\tau,\tau}y_{\tau,i+1} & \cdots & 1 - s_{\tau,\tau}y_{\tau,\tau} \end{bmatrix}.$$

where $\tilde{r}_i$ denotes the minor computed with the last $\tau - i + 1$ rows and columns of RX. Since $s_{i,i}(x)$ is a factor of $s_{j,j}(x)$ for $i \leqq j \leqq \tau$, there exist polynomials $\tilde{y}_i(x)$ such that:

$$h_i(x)(h_{i+1}(x) \dots h_\tau(x)\tilde{r}_i(x)) = 1 - s_{i,i}(x)\tilde{y}_i(x), \quad 1 \leqq i \leqq \tau,$$

this is simply a Bezout identity showing that $h_i(x)$ and $s_{i,i}(x)$ are relatively prime. Taking $t_i(x) = h_{i+1}(x) \dots h_\tau(x)\tilde{r}_i(x)$, as announced we get the translation of (5.4) on scalar polynomials:

$$h_i(x)t_i(x) + s_{i,i}(x)\tilde{y}_i(x) = 1, \quad 1 \leqq i \leqq \tau. \tag{5.5}$$

We now construct the matrices $T(x)$ and $W(x)$, clearly this can be done with any Bezout coefficients satisfying (5.5); $T(x)$ is the diagonal matrix defined by:

$$T(x) = \operatorname{diag}(t_1(x), \dots, t_\tau(x))$$

and $W(x)$ is:

$$W(x) = \tilde{Y}(x)R(x)$$

where $\tilde{Y}(x) = \operatorname{diag}(\tilde{y}_1(x), \dots, \tilde{y}_\tau(x))$. It remains to check that $U(x) = T(x)\bar{U}(x) + S(x)W(x)$, is unimodular. We have:

$$U(x) = (T(x)H_u(x) + S(x)\tilde{Y}(x))R(x)$$

the matrix $T(x)H_u(x) + S(x)\tilde{Y}(x)$ is triangular with diagonal identity, since $R(x)$ is unimodular so is $U(x)$. □

We are now ready to prove the proposition.

Proof of Proposition 5.1 A matrix $U(x)$ is constructed by applying Lemma 5.2 and Lemma 5.3 with $U_{\sigma,\tau}(x)$. We essentially need to show that it satisfies a left coprimeness criterion with $S(x)$.

As for the construction of $\bar{U}_{\sigma,\tau}(x)$, using diagram (4.6) and $\phi_u^{-1} = p^{-1} \circ P \circ p'$ we compute the matrix

$$\bar{U}_{\tau,\sigma}^{(-1)}(x) = [\phi_u^{-1}(f_1), \ldots, \phi_u^{-1}(f_\sigma)] \in \mathscr{M}_{\tau,\sigma}(K[x]).$$

Since ϕ_u is an isomorphism, we know that:

$$\pi(\bar{U}_{\sigma,\tau}(x)\bar{U}_{\tau,\sigma}^{(-1)}(x)) = I_\sigma$$

where $\pi: K[x]^\sigma \to K[x]^\sigma$ is applied column-wise and associates to a vector the representative of the corresponding class in $K[x]^\sigma/N'$, *i.e.* π reduces modulo $S_\sigma(x)$. Consequently — see (4.7) — there exists a matrix $Y_\sigma(x)$ in $\mathscr{M}_{\sigma,\sigma}(K[x])$ such that:

$$\bar{U}_{\sigma,\tau}(x)\bar{U}_{\tau,\sigma}^{(-1)}(x) + S_\sigma(x)Y_\sigma(x) = I_\sigma.$$

Following Lemma 5.2 we consider:

$$[0, \bar{H}_{\sigma,\sigma}(x)]R(x)\bar{U}_{\tau,\sigma}^{(-1)}(x) + S_\sigma(x)Y_\sigma(x) = I_\sigma$$

where $\bar{H}_{\sigma,\sigma}(x)$ and $S_\sigma(x)$ are left coprime. This coprimeness remains true for the matrices diag $(I_{\tau-\sigma}, \bar{H}_{\sigma,\sigma}(x))$ and $S(x) = \text{diag}(I_{\tau-\sigma}, S_\sigma(x))$. Thus $\bar{U}(x)$ constructed by Lemma 5.2 and $S(x)$ are left coprime. To finish we can apply Lemma 5.3 to $\bar{U}(x)$, we get

$$U(x) = T(x)\bar{U}(x) + S(x)W(x).$$

It remains to prove that $U(x)$ is a transformation matrix for the Smith form. From

$$\bar{U}_{\sigma,\tau}(x)H_\tau(x) = S_\sigma(x)M_{\sigma,\tau}(x)$$

it can be easily deduced that there exist $M(x)$ such that

$$\bar{U}H_\tau(x) = S(x)M(x).$$

Now for $U(x)$,

$$\begin{aligned} U(x)H_\tau(x) &= T(x)\bar{U}(x)H_\tau(x) + S(x)W(x)H_\tau(x) \\ &= T(x)S(x)M(x) + S(x)W(x)H_\tau(x) \end{aligned}$$

and using that $T(x)$ and $S(x)$ commute since they are diagonal we obtain:

$$\begin{aligned} U(x)H_\tau(x) &= S(x)(T(x)M(x) + W(x)H_\tau(x)) \\ &= S(x)M'(x). \end{aligned}$$

It is obvious that $M'(x)$ must be unimodular so we can take $V(x) = (M'(x))^{-1}$. □

Example 5.4 Let

$$H_2(x) = \begin{bmatrix} x^2 - 1 & 1 \\ 0 & x^2 - x - 2 \end{bmatrix}, \quad S_1(x) = [(x^2 - x - 2)(x^2 - 1)].$$

A transformation matrix P for the Frobenius form of the constant matrix C associated to $H_2(x)$ is given by:

$$F = P^{-1}CP = \left[\begin{array}{cc|cc} -6 & 2 & -3 & 0 \\ -1 & -5 & 1 & -3 \\ 4 & -4 & 0 & 1 \\ -1 & 3 & 0 & 0 \end{array}\right] \begin{bmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\times \begin{bmatrix} \frac{3}{32} & \frac{9}{32} & \frac{27}{32} & \frac{49}{32} \\ \frac{0}{32} & \frac{3}{32} & \frac{9}{32} & \frac{27}{32} \\ \frac{-1}{2} & \frac{-1}{2} & \frac{-3}{2} & \frac{-5}{2} \\ \frac{-1}{4} & \frac{-3}{4} & \frac{-5}{4} & \frac{-11}{4} \end{bmatrix}.$$

Here, $\tau = 2$ and $\sigma = 1$. Following (5.1) we get:

$$\bar{U}_{1,2}(x) = [-6 - x + 4x^2 - x^3 \;\; x - 3].$$

Notice that $\bar{U}_{1,2}(x)$ cannot be directly completed to a unimodular matrix since the greatest divisor of its entries is $x - 3 \neq 1$. As explained in Lemma 5.2 to complete $\bar{U}_{1,2}(x)$ and in Lemma 5.3 to modify it, we compute a unimodular matrix $R(x)$ for the Hermite normal form of $\bar{U}_{1,2}(x)$:

$$\bar{U}_{1,2}(x) = [0 \;\; \bar{H}_{1,1}]\,R(x) = [0 \;\; x - 3] \quad \begin{bmatrix} x - x^2 & 1 \\ x - x^2 + 2 & 1 \end{bmatrix}$$

$x - 3$ is relatively prime to $s_{2,2}(x)$, if $t_2(x)$ and $\tilde{y}_2(x)$ are corresponding Bezout coefficients, this leads to

$$U(x) = \left(\begin{bmatrix} 1 & 0 \\ 0 & t_2(x) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & x - 3 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & s_{2,2}(x) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \tilde{y}_2(x) \end{bmatrix} \right) R(x)$$

so in fact we can take $U(x) = R(x)$. The Hermite normal form of $U(x)H_2(x)$ is

$$S(x) = \begin{bmatrix} 1 & 0 \\ 0 & (x^2 - x - 2)(x^2 - 1) \end{bmatrix}$$

that is the Smith normal form of $H_2(x)$ (here $V(x) = I$). □

6 Reduction to Smith Normal Form: The Complexity

We know that a reduction (F, P^{-1}) to the Frobenius form over K is readily computed from a reduction $(S(x), U(x))$ to the Smith form over $K[x]$. Indeed, the transformation P^{-1} is computed by reducing $U(x)$ modulo $S(x)$ (see §4.2). Conversely, from §5, in addition to P^{-1}, we have used matrix Bezout identities (reductions to Hermite normal form) to obtain relation (5.3) for the "lifting" of $U(x)$.

The two problems — computing the Frobenius form and computing the Smith form — have the same parallel time complexity. In particular, next Theorem concerning the Smith form of polynomial matrices is "equivalent" to Theorem 3.7 concerning the Frobenius form of scalar matrices by virtue of above remarks.

Theorem 6.1 *Let K be a commutative field. The problem of computing the Smith normal form $S(x)$ of a matrix $A(x)$ of degree d in $\mathcal{M}_{n,m}(K[x])$, and unimodular transformations $U(x)$ in $\mathcal{M}_{n,n}(K[x])$ and $V(x)$ in $\mathcal{M}_{m,m}(K[x])$ such that $S(x) = U(x)A(x)V(x)$, is in $\mathcal{NC}^2_K$. Over the rationals or finite fields GF_q the problem is in $\mathcal{NC}^2$.*

Proof. We simply associate to $A(x)$ a constant matrix B which Frobenius form F gives $S(x)$ and from a transformation P for F (Theorem 3.7) we compute a transformation $U(x)$ (Proposition 5.1).

We first determine the dimension v of an appropriate matrix B. Let us remind that if N_A in the module generated by the columns of $A(x)$, this dimension is the dimension of $K[x]^n/N_A$ as K-vector space. Applying corollary 2.4 we bring $A(x)$ into form (2.1):

$$\begin{bmatrix} I & 0 & 0 \\ 0 & H_\tau(x) & 0 \\ 0 & 0 & 0 \end{bmatrix} = U_1(x)A(x)V_1(x).$$

It is now sufficient to deal with the regular matrix $H_\tau(x)$. If $S_\tau(x)$ is its Smith form with $S_\tau(x) = U_2(x)H_\tau(x)V_2(x)$, we have

$$S(x) = \begin{bmatrix} I & 0 & 0 \\ 0 & S_\tau(x) & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} I & 0 & 0 \\ 0 & U_2(x) & 0 \\ 0 & 0 & I \end{bmatrix} U_1(x)A(x)V_1(x) \begin{bmatrix} I & 0 & 0 \\ 0 & V_2(x) & 0 \\ 0 & 0 & I \end{bmatrix}.$$

We are led to the same matrix form than in (4.1), we choose for B the polycyclic form associated to $H_\tau(x)$ by Lemma 4.1. In particular, the dimension v is the degree of the determinant of $H_\tau(x)$ which is also the determinant of $S_\tau(x)$. If $A(x)$ is of rank r, v is the degree of the greatest common divisor of the $r \times r$ non-zero minors of $A(x)$.

Once B is known, applying Theorem 3.7, we compute a transformation P and its inverse. Also F and $S(x)$ are known. Then a matrix $\bar{U}_{\sigma,\tau}$, residue modulo $S(x)$ of $U_2(x)$, is constructed by identity (5.1) and finally unimodular matrices $U_2(x)$ and $V_2(x)$ — and further, $U(x)$ and $V(x)$ — are given by Proposition 5.1.

Computations can clearly be done in $\mathcal{NC}^2_K$. The problem reduces to the Frobenius normal form computation of the matrix which dimension v is lower than $d \min(n, m)$. The only cost that has not been given yet, is the cost of the lifting of the residue matrix to get $U(x)$ at Proposition 5.1. This consists in computing the Hermite normal form $H_u(x)$ of $\bar{U}_{\sigma,\tau}$ (in $\mathcal{NC}^2_K$ from [15, 31]) and to compute Bezout identities between the diagonal entries of $H_u(x)$ and the diagonal entries of $S(x)$ (using the algorithm in [3]). By reduction to a fixed number of problems in $\mathcal{NC}^2$ the problem is in $\mathcal{NC}^2$ for concrete fields. □

Example 6.2 We calculate a reduction to the Smith form of

$$A(x) = \begin{bmatrix} 1 & 0 & -2 & x \\ 3 & x^2 - 1 & -5 & 4x - x^3 \\ 3x^2 - 2x - 6 & 0 & 3x - 5x^2 + 10 & 3x^3 - 2x^2 - 6x \\ x + 3 & x^2 - 1 & -2x - 5 & x^2 - x^3 + 4x \end{bmatrix}.$$

By two Hermite normal form reductions (on the left and on the right) we get $H(x) = U_1(x)A(x)V_1(x)$ in form (2.1):

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x^2-1 & 1 & 0 \\ 0 & 0 & x^2-x-2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1-x^2 & -x & 0 & x \\ 0 & 1 & 0 & 0 \\ -x & 0 & 1 & 0 \\ -x & -1 & 0 & 1 \end{bmatrix}$$

$$\times A(x) \begin{bmatrix} 2x-5 & 0 & 2 & -x \\ -2x & 1 & 0 & x \\ -3 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 \end{bmatrix}.$$

Here the K-vector space for B is of dimension $v = 4$, the 2×2 polynomial regular submatrix $H_2(x)$ of $H(x)$ is the matrix we have considered at Example 5.4. □

As an obvious corollary we obtain a polynomial-time sequential algorithm to compute transformations for the Smith form. Since it is valid over any field K, this result slightly improves the old ones (see §1.2).

Corollary 6.3 *For any commutative field K, the proposed algorithm for computing the Smith normal form of a polynomial matrix $A(x)$ and associated unimodular transformations $U(x)$ and $V(x)$ over $K[x]$, runs in a polynomial number of operations in K. Over $Q[x]$ it runs in a polynomial number of bit operations.*

Remark 6.4. The same improvement could have been obtained using polynomials over K, instead of elements in a field extension, to run the algorithm of [30].

Conclusion

We have shown that normal forms of matrices and associated transformation matrices over the input field, can be computed fast in parallel. The main difficulty was to avoid, in the outputs, the field extensions used during intermediate stages.

This is to some extent a result for a rather "unrealistic" model of computation: we have not considered processor counts and communication costs. But this will be the basis for future works in these directions. In particular it seems that field extensions should be completely avoided to reach processor-efficiency.

Acknowledgements: Thanks go to referee 1 for text improvements and grammar corrections.

References

1. Augot, D., Camion, P.: The minimal polynomials, characteristic subspaces, normal bases and the Frobenius form. Technical Report 2006, INRIA France 1993
2. Bini, D., Pan, V.: Polynomial and matrix computations. Basel: Birkhäuser 1994
3. Borodin, A., von zur Gathen, J., Hopcroft, J.: Fast parallel matrix and gcd computations. Inf. Control **52**, 241–256 (1982)

4. Cook, S. A.: A taxonomy of problems with fast parallel algorithms. Inf. Control **64**, 2–22 (1985)
5. Frumkin, M. A.: Polynomial time algorithms in the Theory of linear diophantine equations. In Fundamentals of Computation Theory, pp. 386–392. LNCS 56, Berlin, Heidelberg New York: Springer 1977
6. Gantmacher, F. R.: Theorie des matrices. Paris, France, Dunod 1966
7. von zur Gathen, J.: Parallel algorithms for algebraic problems. SIAM J. Comp. **13**(4), 802–824 (1984)
8. von zur Gathen, J.: Parallel arithmatic computations: a survey. In Proc. 12th Int. Symp. Math. Found. Comput. Sci., pp. 93–112. LNCS 233, Berlin, Heidelberg, New York: Springer 1986
9. Gautier, T., Roch, J. L.: Fast parallel Algebraic Numbers Computations. In Second International Symposium on Parallel Symbolic Computation (PASCO'97), Maui, Hawaii, USA, July 1997
10. Giesbrecht, M.: Nearly optimal algorithms for canonical matrix forms. PhD thesis, Department of Computer Science, University of Toronto (1993)
11. Giesbrecht, M.: Fast computation of the Smith normal form of an integer matrix. In International Symposium on Symbolic and Algebraic Computation, Montreal, Canada, pp. 110–118. ACM Press 1995
12. Giesbrecht, M.: Nearly optimal algorithms for canonical matrix forms. SIAM Journal on Computing, **24**, 948–969 (1995)
13. Gómez-Díaz, T.: Quelques applications de l'e[valuation dynamique. PhD thesis, Université de Limoges, France (1994)
14. Jacobson, N.: Basic Algebra I. W. H. Freeman and Company 1974
15. Kaltofen, E., Krishnamoorthy, M. S., Saunders, B. D.: Fast parallel computation of Hermite and Smith forms of polynomials matrices. SIAM J. Alg. Disc. Meth. **8**, 683–690 (1987)
16. Kaltofen, E., Krishnamoorthy, M. S., Saunders, B. D.: Parallel algorithms for matrix normal forms. Linear Algebra and its Applications **136**, 189–208 (1990)
17. Kannan, R.: Solving systems of linear equations over polynomials. Theoret. Comput. Sci. **39**, 69–88 (1985)
18. Kannan, R., Bachem, A.: Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. SIAM J. Comput. **8**, 499–507 (1979)
19. Lüneburg, H.: On rational form of endomorphims: a primer to constructive algebra. Mannheim: Wissenschaftsverlag 1987
20. MacDuffee, C. C.: The Theory of matrices. New York: Chelsea 1956
21. Martin, K., Olazábal, J. M.: An algorithm to compute the change basis for the rational form of K-endomorphisms. Extracta Mathematicae **6**, 89–91 (1992)
22. Mulders, T.: Computation of normal forms for matrices. In Algoritmen In De Algebra, A Seminar on Algebraic Algorithms. University of Nijmegen, 1993
23. Ozello, P.: A probalistic algorithm to compute the Frobenius form of a matrix. Technical Report RR 653M, IMAG, Grenoble, France (1987)
24. Ozello, P.: Calcul exact des formes de Jordan et de Frobenius d'une matrice. PhD thesis, Université Scientifique et Médicale de Grenoble, France (1987)
25. Roch, J. L., Villard, G.: Parallel computations with algebraic numbers, a case study: Jordan normal form of matrices. In Parallel Architectures and Languages Europe 94, Athens Greece LNCS 817, Berlin Heidelberg New York: Springer 1994
26. Storjohann, A.: Computation of Hermite and Smith normal forms of matrices. Master's thesis, University of Waterloo, Canada (1994)
27. Storjohann, A.: Near optimal algorithms for computing smith normal forms of integer matrices. In International Symposium on Symbolic and Algebraic Computation, Zurich, Switzerland, pp 267–274, ACM Press 1996
28. Storjohann, A.: A solution to the extended gcd problem with application. In International Symposium on Symbolic and Algebraic Computation, Maui, Hawaii, USA, pp. 109–116, ACM Press 1997
29. Villard, G.: Fast parallel computation of the Smith normal form of polynomial matrices. In International Symposium on Symbolic and Algebraic Computation, Oxford, UK, pp. 312–317, ACM Press 1994
30. Villard, G.: Generalized subresultants for computing the Smith normal form of polynomial matrices. Journal of Symbolic Computation, **20**, 269–286 (1995)

31. Villard, G.: Computing Popov and Hermite forms of polynomial matrices. In International Symposium on Symbolic and Algebraic Computation, Zurich, Suisse, pp. 250–258. ACM Press 1996
32. Wilkinson, J. H.: The algebraic eigenvalue problem. Oxford University Press 1965
33. Wolovich, W.: Skew prime polynomial matrices. IEEE Trans. Automat. Control, AC-**23**, 880–887 (1978)