Parallel Processing Letters

FAST PARALLEL COMPUTATION OF THE JORDAN NORMAL FORM OF MATRICES

JEAN-LOUIS ROCH and GILLES VILLARD
Institut IMAG, Laboratoire LMC
46, Av. F. Viallet,
38031 Grenoble Cedex, France

Received (received date)
Revised (revised date)
Accepted by D. Bini

ABSTRACT

We establish that the problem of computing the Jordan normal form of a matrix over a field F is in $\mathcal{NC}^3_F$ for F being a field of characteristic zero or a finite field.

Keywords: Parallel algorithm, $\mathcal{NC}^3_F$, Jordan normal form, invariant factors.

1. Introduction

Computing normal forms of matrices is a basic problem in linear algebra. In particular the *Jordan form* is widely used for computing matrix functions and for solving differential equations. Since the computation of the Jordan form involves a set of rank decisions, its computation by means of numerical arithmetic is a difficult problem and the development of new algebraic methods is of great practical importance for ill-posed problems. The form is well known from a theoretical point of view [1] and sequential algorithms are known, but to find a fast parallel algorithm for its computation was still an open question (question 6.5 in [2]).

In the existing sequential algorithms for the Jordan form, two main approaches are used. The Jordan form of a matrix A whose coefficients are in a field F, is derived either from the *Frobenius form* of A or from the *Smith form* of $A - \lambda I$. The Smith form involves computations on polynomials; for this reason, the Frobenius form which is entirely computed within the field F is often prefered. But there is no relevant theoretical criterion to choose between the two approaches: they both consist in computing the *invariant factors* of A. In [3,4,5,6] the Jordan form is computed using the Frobenius form; concerning the Smith form, algorithms may be found in [7,8,9]. In all cases polynomial time solutions are proposed, but none of them is helpful in deriving the parallel complexity of the computation since they all consist of elimination processes requiring $O(n)$ steps.

From a parallel point of view, few algorithms are reported in the literature. Kaltofen, Krishnamoorthy and Saunders [7,8] give parallel algorithms to compute the Smith, the Frobenius, then the Jordan form, but their algorithms use random choices so the problems were only known to be in $\mathcal{RNC}$. In [6] Giesbrecht gives processor efficient probabilistic algorithms for the same problems. We refer to [10] for the definitions of the boolean complexity classes $\mathcal{NC}$ and $\mathcal{RNC}$ of problems deterministically and probabilistically solvable by boolean circuits. In analogy with these classes von zur Gathen [11] has defined the classes $\mathcal{NC}_F$ and $\mathcal{RNC}_F$ of problems solvable by arithmetic circuits over F.

After some basic reminders in section 2 we present, in section 3, a new exact algorithm in $\mathcal{NC}_F$ that avoids random choices for the computation of the Jordan normal form. Since our algorithm makes use of the squarefree decomposition of polynomials, we will assume that F is a field of characteristic zero or is a finite field.

Let A be a matrix of $F^{n\times n}$ having l distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_l$ with respective multiplicities in the characteristic polynomial $m_1, m_2, \ldots, m_l$. Our algorithm directly computes the number and the dimensions of the diagonal blocks in the Jordan form of A from the nullities (dimension of the kernels) of the successive powers

$$A - \lambda_i I, (A - \lambda_i I)^2, \ldots, (A - \lambda_i I)^{m_i},\ 1 \le i \le l.$$

It is shown that the problem of computing the form is in $\mathcal{NC}_F^3$. As an intermediate result we obtain that the problem of computing the invariant factors of A is in $\mathcal{NC}_F^2$.

2. Basic Concepts

In the following, F is a field of characteristic zero or a finite field and A is a matrix of dimension n whose entries are in F, having l distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_l$.

2.1. Jordan Normal Form

Any matrix A is similar to a unique (up to permutation) block-diagonal matrix J whose diagonal blocks are matrices of the form:

$$J_k(\lambda_i) = \begin{bmatrix} \lambda_i & 1 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & & 0 \\ 0 & 0 & \lambda_i & & \vdots \\ \vdots & & & & 1 \\ 0 & \ldots & \ldots & 0 & \lambda_i \end{bmatrix} \in F^{k\times k}$$

where λ_i is an eigenvalue of A; J_k is a $k \times k$ banded matrix, which is called a k-Jordan block associated with λ_i. We refer to [1] for the proof; J is the Jordan normal form of A. Two similar matrices have the same Jordan normal form.

When the field F is not algebraically closed, the eigenvalues of A lie in an algebraic extension of F. If these are given our algorithm will compute the Jordan

form. In general, since we do not know how to factor polynomials fast in parallel [2] we will compute a variant of the Jordan form consisting of blocks corresponding to *generalized eigenvalues*, *i.e.* to eigenvalues belonging to the same factors in a partial factorization of the characteristic polynomial of A [8,2]. This form is the *symbolic Jordan form*. It gives the structure of J using symbols that take the place of the eigenvalues.

2.2. Symbolic Jordan Normal Form

With any matrix A we may associate its symbolic Jordan form $\tilde{J}$. The structure of $\tilde{J}$ is the same as the structure of J with l distinct symbols $\tilde{\lambda_i}$ taking the place of the eigenvalues. Each symbol $\tilde{\lambda_i}$ is associated with a polynomial $\Lambda_i(\lambda)$ in $F[\lambda]$, with the understanding that Λ_i is a representation of λ_i, *i.e.* $\Lambda_i(\lambda_i) = 0$. We may assume that the Λ_i are monic squarefree factors of the characteristic polynomial of A.

Clearly, the symbolic Jordan form is not unique, since different choices are possible for the Λ_i. It coincides with the Jordan form if the eigenvalues are known, *i.e.* if the Λ_i are the linear factors $(\lambda - \lambda_i)$.

But the Λ_i need not be irreducible. Otherwise, polynomial factorization would be required. In the following, as in [8], we will consider the unique symbolic Jordan form corresponding to the Λ_i satisfying:

(i) If there exists a dimension k such that λ_i and λ_j do not have the same number of k-Jordan blocks, then Λ_i and Λ_j are relatively prime.
(ii) If for all integers k, $1 \leq k \leq n$, λ_i and λ_j have the same number of k-Jordan blocks, then $\Lambda_i = \Lambda_j$.

When the eigenvalues are not known, this unique matrix $\tilde{J}$ will be improperly called *the Jordan form* of A. The main fact is that it can be computed by polynomial gcd operations only and does not require polynomial factorization [8].

We conclude those reminders with another way to specify the symbolic Jordan form: defining a form with entries in F, thus avoiding the use of symbols.

2.3. Rational Jordan Form

The symbolic Jordan form gives rise to a block-diagonal normal form J_F in $F^{n\times n}$ similar to A, called *the rational Jordan form* of A. Each block of J_F corresponds to a set of eigenvalues of A, called a *generalized eigenvalue* of A, the set of the roots of a Λ_i.

More precisely, if the roots $\lambda_i^1, \lambda_i^2, \ldots, \lambda_i^d$ of a given Λ_i of degree d are associated with k-Jordan blocks $J_k(\lambda_i^1), J_k(\lambda_i^2), \ldots, J_k(\lambda_i^d)$ (from (i) and (ii) above we know they have the same Jordan blocks), then J_F has a diagonal block in "block-Jordan"

form:

$$J_k(C_{\Lambda_i}) = \begin{bmatrix} C_{\Lambda_i(\lambda)} & I & 0 & \dots & 0 \\ 0 & C_{\Lambda_i(\lambda)} & I & & \vdots \\ 0 & 0 & C_{\Lambda_i(\lambda)} & & \vdots \\ \vdots & & & & I \\ 0 & \dots & \dots & 0 & C_{\Lambda_i(\lambda)} \end{bmatrix} \in F^{kd \times kd},$$

where, if $\Lambda_i(\lambda) = \lambda^d + a_{d-1}\lambda^{d-1} + \ldots + a_0$, $C_{\Lambda_i(\lambda)}$ is the companion matrix

$$C_{\Lambda_i(\lambda)} = \begin{bmatrix} 0 & 0 & 0 & \dots & -a_0 \\ 1 & 0 & 0 & & -a_1 \\ 0 & 1 & 0 & & \vdots \\ \vdots & & & & -a_{d-2} \\ 0 & \dots & \dots & 1 & -a_{d-1} \end{bmatrix} \in F^{d \times d}.$$

As for the symbolic Jordan form, if the Λ_i are linear factors, J_F coincides with the usual Jordan form. Furthermore, if the Λ_i are irreducible over $F[\lambda]$, J_F is called *the primary rational normal form* of A [1].

Clearly, it makes no difference to consider either $\tilde{J}$ or J_F. From here, if the eigenvalues are not known, "Jordan form" will equally stand for "symbolic Jordan form" or for "rational Jordan form".

3. A Fast Parallel Algorithm

We now give a deterministic fast parallel algorithm for computing the Jordan form. We begin with a standard lemma giving a method of computing the number of Jordan blocks. From this lemma we will then develop the algorithm computing also the representations Λ_i of the eigenvalues.

Using the above notation, for any eigenvalue λ_i of A, let us consider the kernels of the successive powers of $A - \lambda_i I$. It is widely known that

$$\ker(A - \lambda_i I) \subset \ker(A - \lambda_i I)^2 \subset \ldots \subset \ker(A - \lambda_i I)^{\mu_i} = \ldots = \ker(A - \lambda_i I)^{m_i},$$

where μ_i and m_i are respectively the multiplicities of λ_i in the minimal polynomial μ_A and in the characteristic polynomial χ_A of A. For each i, $1 \leq i \leq l$, and k, $1 \leq k \leq n+1$ (or $1 \leq k \leq m_i$), let

$$d_i^{(k)} = \dim(\ker(A - \lambda_i I)^k).$$

Lemma 1 *If $d_i^{(k)}$ is the dimension of the kernel of $(A - \lambda_i I)^k$, then the number $\delta_i^{(k)}$ of blocks $J_k(\lambda_i)$ of dimension k associated with λ_i in the Jordan normal form of A is given by:*

$$\delta_i^{(k)} = 2d_i^{(k)} - d_i^{(k-1)} - d_i^{(k+1)}.$$

Proof. First notice that only the Jordan blocks associated with λ_i have an influence on the dimension of $\ker(A-\lambda_i I)^k$. For all h, $1 \leq h \leq n$, the matrices $J_h(\lambda_i)-\lambda_i I$ are nilpotent, so we have:

$$\dim\left(\ker\left(J_h(\lambda_i)-\lambda_i I\right)^k\right) = \begin{cases} k, & 1 \leq k \leq h, \\ h, & k \geq h, \end{cases}$$

then

$$\dim\left(\ker(J_h(\lambda_i)-\lambda_i I)^{k+1}\right) - \dim\left(\ker(J_h(\lambda_i)-\lambda_i I)^k\right) = \begin{cases} 1, & h > k, \\ 0, & h \leq k. \end{cases}$$

Now, $d_i^{(k+1)} - d_i^{(k)}$ is the number of Jordan blocks of dimension strictly greater than k associated with λ_i. The number of blocks of dimension k associated with λ_i is

$$\delta_i^{(k)} = [d_i^{(k)} - d_i^{(k-1)}] - [d_i^{(k+1)} - d_i^{(k)}] = 2d_i^{(k)} - d_i^{(k-1)} - d_i^{(k+1)},$$

which completes the proof. □

The problem consequently reduces to rank, or equivalently, to nullity computations. From [12] when F is a subfield of $\mathbf{R}$, and from [13] for an arbitrary field, we know that the problem of rank determination is in $\mathcal{NC}_F^2$: it can be read from the coefficients of a well chosen characteristic polynomial. We now extend those algorithms in order to compute both the nullities of the successive powers $(A-\lambda_i I)^k$ and the representations Λ_i of the λ_i.

We proceed in two main steps, computing at first, in lemma 2 below, a set of invariant polynomials of A. This set is analogous but slightly different from the set of the *invariant factors* [1] of A. It is related to an algebraic expression of the previous lemma which leads to the Jordan blocks given by dimensions. The second step, given by theorem 2, will consist in computing the target representations Λ_i from these invariant polynomials.

Lemma 2 *For F a field of characteristic zero or a finite field, let A be in $F^{n\times n}$ with l distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_l$, and let $\delta_i^{(k)}$ denote the number of Jordan blocks $J_k(\lambda_i)$ of dimension k associated with λ_i. The set of polynomials*

$$\mathcal{I}_A = \left\{ \Delta^{(k)} = \prod_{i=1}^{l} (\lambda - \lambda_i)^{\delta_i^{(k)}} \right\}_{1 \leq k \leq n}$$

is invariant up to similarity, it can be computed within $\mathcal{NC}_F^2$.

Proof. Given the Jordan form of A, $\mathcal{I}_A$ is unique. Conversely, the Jordan form is entirely determined from the the $\Delta^{(k)}$, therefore $\mathcal{I}_A$ is invariant up to similarity. We focus on its computation.

Let us recall at first the algorithm of Mulmuley [13] for the rank or the nullity of a matrix A over an arbitrary field. Consider the symmetric matrix

$$\tilde{A} = \begin{bmatrix} 0 & A \\ A^t & 0 \end{bmatrix}.$$

Let Z be a diagonal matrix in an indeterminate z such that $Z_{ii} = z^{i-1},\ 1 \leq i \leq 2n$. The highest degree d such that x^d divides the characteristic polynomial $\tilde{\chi}_A(x) = \det(xI - Z\tilde{A})$ is twice the nullity of A. Moreover, since for any matrices A_1, A_2, A_3 and A_4 of equal dimensions, we have the following identity on determinants:

$$\begin{vmatrix} A_1 & A_2 \\ A_3 & A_4 \end{vmatrix} = \begin{vmatrix} -A_1 & A_2 \\ A_3 & -A_4 \end{vmatrix},$$

we deduce that

$$\tilde{\chi}_A(x) = \det(xI - Z\tilde{A}) = \begin{vmatrix} xI & -Z_1 A \\ -Z_2 A^t & xI \end{vmatrix} = \begin{vmatrix} -xI & -Z_1 A \\ -Z_2 A^t & -xI \end{vmatrix} = \tilde{\chi}_A(-x).$$

In other words, $\tilde{\chi}_A(x)$ is of degree $2n$ and is an even function of x. Now, to compute the nullities of $(A - \lambda_i I)^k$, in the same way as Mulmuley's algorithm associates $\tilde{\chi}_A(x)$ with A, we associate the characteristic polynomials $\tilde{\chi}_i^{(k)}(x)$ with the powers $(A - \lambda_i I)^k$, and $\tilde{\chi}^{(k)}(x, \lambda)$ with $(A - \lambda I)^k$ viewing λ as an indeterminate. As for $\tilde{\chi}_A(x)$, these polynomials are of degree $2n$ in x and are even functions, so we can write:

$$\begin{array}{rcl} \tilde{\chi}_i^{(k)}(x) & = & \sum_{j=0}^{n} a_{i,j}^{(k)}\ x^{2j},\ 1 \leq i \leq l, \\ \tilde{\chi}^{(k)}(x, \lambda) & = & \sum_{j=0}^{n} a_j^{(k)}(\lambda)\ x^{2j}. \end{array}$$

Furthermore, since these polynomials are determinants, we know by homomorphism that:

$$\begin{array}{rcl} \tilde{\chi}^{(k)}(x, \lambda_i) & = & \tilde{\chi}_i^{(k)}(x),\ 1 \leq i \leq l, \\ a_j^{(k)}(\lambda_i) & = & a_{i,j}^{(k)},\ 0 \leq j \leq n,\ 1 \leq i \leq l. \end{array}$$

From the above definitions, the highest degree d such that x^d divides $\tilde{\chi}_i^{(k)}(x)$ is twice $d_i^{(k)}$:

$$d_i^{(k)} = \max_j \left\{ j \ / \ a_{i,h}^{(k)} = 0,\ 0 \leq h < j \right\} = \max_j \left\{ j \ / \ a_h^{(k)}(\lambda_i) = 0,\ 0 \leq h < j \right\}. \quad (1)$$

Using this characterization of the $d_i^{(k)}$ we may now develop the main point of the proof. To work with a squarefree polynomial instead of the characteristic polynomial χ_A of A, let $\chi(\lambda)$ be the greatest squarefree monic divisor of $\chi_A(\lambda)$, and define

$$q_j^{(k)}(\lambda) = \gcd\left(\chi(\lambda), a_0^{(k)}(\lambda), a_1^{(k)}(\lambda), \ldots, a_j^{(k)}(\lambda)\right),\ 0 \leq j \leq n-1,\ 1 \leq k \leq n+1.$$

By construction, the $q_j^{(k)}(\lambda)$ are products of distinct $(\lambda - \lambda_i)$. From identity (1), if $d_i^{(k)} = d$ then $(\lambda - \lambda_i)$ divides $a_0^{(k)}(\lambda), a_1^{(k)}(\lambda), \ldots$ and $a_{d-1}^{(k)}(\lambda)$, but not $a_d^{(k)}(\lambda)$. In the same way, $(\lambda - \lambda_i)$ divides $q_j^{(k)}(\lambda)$ for all j, $1 \leq j \leq d-1$, but not for higher values of j. Now consider the polynomials

$$Q^{(0)}(\lambda) = 1,\ Q^{(k)}(\lambda) = \prod_{j=0}^{n-1} q_j^{(k)}(\lambda),\ 1 \leq k \leq n+1.$$

We know that

$$Q^{(0)}(\lambda) = 1,\ Q^{(k)}(\lambda) = \prod_{i=1}^{l} (\lambda - \lambda_i)^{d_i^{(k)}},\ 1 \leq k \leq n+1.$$

These $Q^{(k)}(\lambda)$ yield the desired invariant polynomials since, applying lemma 1, it is easily verified that

$$\left(Q^{(k)}(\lambda)\right)^2 / \left(Q^{(k-1)}(\lambda) Q^{(k+1)}(\lambda)\right) = \Delta^{(k)}(\lambda),\ 1 \leq k \leq n.$$

It remains to establish that the computation can be done within $\mathcal{NC}_F^2$. Using the algorithm in [14] the problem of computing the characteristic polynomials χ_A and $\tilde{\chi}^{(k)}$ is in $\mathcal{NC}_F^2$. From χ_A, χ is computed within $\mathcal{NC}_F^2$ using the algorithm in [15] for the computation of the distinct power decomposition of polynomials (and [13] for the rank). The computation of the $q_i^{(k)}$ consists in calculating the gcd of the polynomials $a_j^{(k)}$ which are the coefficients of the previous polynomials $\tilde{\chi}^{(k)}$. These coefficients are of degree $O(n^2)$ in z and in λ. Using the algorithm for the gcd of many polynomials in [15] (and [13] for the rank) this is done within $\mathcal{NC}_F^2$. Obviously the computation of the $Q^{(k)}$ and of the $\Delta^{(k)}$ from the $q_i^{(k)}$ is done within $\mathcal{NC}_F^2$. □

Before computing the Jordan normal form, we may point out that lemma 2 leads to a first interesting result: the following theorem establishes that the problem of computing the invariant factors of A is in $\mathcal{NC}_F^2$. Obviously, this also gives an algorithm for *testing similarity of matrices*, however for this latter problem a simpler and more general solution may be found in [16].

Theorem 1 *For F a field of characteristic zero or a finite field and A in $F^{n\times n}$, the problem of computing the invariant factors of A, or equivalently, the Frobenius normal form of A is in $\mathcal{NC}_F^2$.*

Proof. Let us recall the definition of the invariant factors. We assume that each eigenvalue λ_i of A is associated with n_i Jordan blocks of dimension greater than or equal to 1, and for the sake of simplicity, we consider that λ_i is associated with $n - n_i$ blocks of dimension 0. Those blocks are numbered by decreasing dimensions, let $\gamma_{i,j}$ be the dimension of the j-th block associated with λ_i. The invariant factors of A are the n polynomials in $F[\lambda]$ given by:

$$s_j = \prod_{i=1}^{l} (\lambda - \lambda_i)^{\gamma_{i,j}},\ 1 \leq j \leq n.$$

We show that the invariant factors can be computed within $\mathcal{NC}_F^2$ from the invariant polynomials $\Delta^{(k)}$ of lemma 2. Let us define

$$\Gamma^{(d)} = \prod_{j=d}^{n} \Delta^{(j)},\ 1 \leq d \leq n.$$

For the $\delta_i^{(k)}$ blocks of dimension k associated with an eigenvalue λ_i, the factor $(\lambda - \lambda_i)$ appears to the power $\delta_i^{(k)}$ in the k polynomials $\Gamma^{(1)}$,$\Gamma^{(2)}$,...,$\Gamma^{(k)}$. Now it

suffices to compute the distinct power decompositions of the $\Gamma^{(d)}$, let:

$$\Gamma^{(d)} = I_{d,1} I_{d,2}^2 \ldots I_{d,n}^n, \ 1 \leq d \leq n,$$

where the $I_{d,i}$ are monic and $\gcd(I_{d,i}, I_{d,j}) = 1$ for $1 \leq i < j \leq n$ and $1 \leq d \leq n$. By construction, for any i, d and k, the factor $(\lambda - \lambda_i)$ appears in $I_{d,k}$ if and only if λ_i is associated with k blocks of dimension greater than or equal to d. In the same way, $(\lambda - \lambda_i)$ divides $\prod_{k \geq j} I_{d,k}$ if and only if λ_i is associated with at least j blocks of dimension greater than or equal to d. The j-th block corresponding to λ_i is then obtained by taking the product for all d *i.e.* the invariant factors are given by:

$$s_j = \prod_{1 \leq d \leq n} \prod_{k \geq j} I_{d,k}, \ 1 \leq j \leq n.$$

The complexity is dominated by the distinct power decompositions of the $\Gamma^{(d)}$: using the algorithm in [15] this problem is in $\mathcal{NC}_F^2$. The Frobenius form of A is the block-diagonal matrix whose blocks are the companion matrices associated to the invariant factors of A. □

In lemma 2 we have computed the structure of the Jordan form, it remains to compute representations $\Lambda_i(\lambda)$ of the eigenvalues satisfying the properties given in section 2.2. They will be the finest possible representations $\Lambda_i(\lambda)$ of the eigenvalues that can be found by gcd operations as described below, without complete polynomial factorization.

Theorem 2 *For F a field of characteristic zero or a finite field and A in $F^{n \times n}$, the problem of computing the symbolic Jordan normal form of A is in $\mathcal{NC}_F^3$.*

Proof. We use a result in [8]. The process makes use of the following definition. A *squarefree relatively prime basis of polynomials* $\{P_1, P_2, \ldots, P_n\}$ in $F[\lambda]$ consists of polynomials $\{I_1, I_2, \ldots, I_m\}$ in $F[\lambda]$ that satisfy:

- I_i is squarefree for $1 \leq i \leq m$.
- I_i and I_j are relatively prime for $1 \leq i < j \leq m$.
- There exist positive integers $e_{i,j}$ such that $P_j = \prod_{i=1}^m I_i^{e_{i,j}}$ for $1 \leq j \leq n$.

In a way analogous to the non-uniqueness of the representations of the eigenvalues, for a given set of polynomials, a squarefree relatively prime basis is not unique. But it is shown in [8] that the coarsest such basis (*i.e.* with a minimum number of elements), called *the standard basis*, is unique and can be computed by gcd operations only. Furthermore, the standard relatively prime basis of the invariant polynomials given by $\mathcal{I}_A$, is equal to the standard relatively prime basis of the invariant factors of A (both sets are invariant up to similarity) and consists of the desired representations $\Lambda_i(\lambda)$ of the eigenvalues [8] (without repetition).

In conclusion, the invariant polynomials of $\mathcal{I}_A$ can be computed within $\mathcal{NC}_F^2$, and from [8] the problem of computing their standard squarefree relatively prime basis is in $\mathcal{NC}_F^3$: this latter complexity dominates the whole computation of the Jordan form. □

The next result follows immediately, its proof is omitted.

Corollary 1 *For F a field of characteristic zero or a finite field, given A in $F^{n\times n}$ and given $\lambda_1,\ldots,\lambda_l \in F$ the l distinct eigenvalues of A, the problem of computing the Jordan normal form of A is in $\mathcal{NC}^2_F$.*

Since it appears to be quite huge, we will now spend only a few words on the processor demand of our algorithm. The steps that require the most processors are the computations of the n characteristic polynomials $\tilde{\chi}^{(k)}$ and of the n^2 polynomials $q_i^{(k)}$ (proof of lemma 2). The $\tilde{\chi}^{(k)}$ are characteristic polynomials of matrices which entries are polynomials in two variables λ and z. If $O(M(n))$ operations are sufficient to multiply two $n\times n$ matrices over F, each $\tilde{\chi}^{(k)}$ can be calculated with $O(n^3M(n))$ processors using the algorithm in [14]. The $q_i^{(k)}$ are the gcd of the polynomials $a_j^{(k)}$ which are of degree $O(n)$ in λ and $O(n^2)$ in z (the degree in λ can be reduced modulo $\chi(\lambda)$). Using the algorithm for the gcd of many polynomials in [15], each can be computed with $O(n^3M(n))$ processors.

Thus *the overall demand of our algorithm is $O(n^5M(n))$ processors.* The sequential deterministic algorithms in [3] and in [4] require $O(n^4)$ operations in F, and the cost of a deterministic version of the algorithm in [6] appears to be $O(nM(n)\log n)$. In parallel, the best known probabilistic algorithm is given in [6], it runs in time $(\log n)^{O(1)}$ on $O(M(n)(\log n)^{O(1)})$ processors. It is processor efficient since a demonstrated lower bound for the problem is $\Omega(M(n))$ operations in F.

4. Conclusion

We have provided a fast parallel algorithm for a crucial problem in linear algebra: the computation of the *Jordan normal form* of matrices. Moreover, a similarity matrix P for the Jordan form, *i.e.* $J = P^{-1}AP$, could also be obtained in $\mathcal{NC}^3_F$, and we have recently obtained a new algorithm which allows to compute a slightly different form which runs over any commutative field [17]. Those results have various applications especially in linear algebra [1,6,18].

Acknowledgements

We are grateful to Dominique Duval (University of Limoges) for useful discussions; in particular she suggested the use of the successive kernels.

References

1. F.R. Gantmacher, *Théorie des matrices* (Dunod, Paris, 1966).
2. J. von zur Gathen, Parallel arithmetic computations: a survey, in *Proc. 12th Int. Symp. Math. Found. Comput. Sci.*, Bratislava (Springer-Verlag LNCS 233, 1986) 93–112.
3. P. Ozello, Calcul exact des formes de Jordan et de Frobenius d'une matrice, Ph. D. Thesis, Université Scientifique et Médicale de Grenoble , 1987.
4. H. Lüneburg, *On rational form of endomorphims : a primer to constructive algebra* (Wissenschaftsverlag, Mannheim, 1987).

5. M.H. Mathieu and D. Ford, On p-adic computation of the rational form of a matrix, *J. Symbolic Computation* **10** (1990) 453–464.

6. M. Giesbrecht, Nearly optimal algorithms for canonical matrix forms , Ph. D. Thesis, Department of Computer Science, University of Toronto, 1993.

7. E. Kaltofen, M.S. Krishnamoorthy, and B.D. Saunders, Fast parallel computation of Hermite and Smith forms of polynomials matrices, *SIAM J. Alg. Disc. Meth.* **8** (4) (1987) 683–690.

8. E. Kaltofen, M.S. Krishnamoorthy, and B.D.Saunders, Parallel algorithms for matrix normal forms, *Lin. Alg. Appl.* **136** (1990) 189–208.

9. G. Villard, Computation of the Smith normal form of polynomial matrices, in *Proc. International Symposium on Symbolic and Algebraic Computation*, Kiev Ukraine (ACM Press, July 1993).

10. S.A. Cook, A taxonomy of problems with fast parallel algorithms, *Inf. Contr.* **64** (1985) 2–22.

11. J. von zur Gathen, Algebraic complexity theory, *Ann. Rev. Comp. Sc.* **3** (1988) 317–347.

12. O. Ibarra, S. Moran, and L.E. Rosier, A note on the parallel complexity of computing the rank of order n matrices, *Inf. Proc. Let.* **11** (1980) 162.

13. K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, *Combinatorica*, **7** (1) (1987) 101–104.

14. A. Borodin, S.A. Cook, and N. Pippenger, Parallel computation for well-endowed rings and space bounded probalistic machines, *Inf. Contr.* **58** (1983) 113–136.

15. J. von zur Gathen, Parallel algorithms for algebraic problems, *SIAM J. Comp.* **13** (1984) 802–824.

16. Y. Zalcstein and M. Garzon, An NC^2 algorithm for testing similarity of matrices, *Inf. Proc. Let.* **30** (1989) 253–254.

17. J.L. Roch and G. Villard, Calcul formel et parallélisme : étude de la forme normale de Jordan (In english), APACHE Report 7, IMAG Grenoble France, Fev. 94.

18. G. Villard, Calcul formel et parallélisme : étude de la forme normale de Smith (In english), APACHE Report 8, IMAG Grenoble France, Fev. 94.