# LSP matrix decomposition revisited 

Claude-Pierre Jeannerod

## To cite this version:

Claude-Pierre Jeannerod. LSP matrix decomposition revisited. [Research Report] Laboratoire de l'informatique du parallélisme. 2006, 2+15p. hal-02102348

## HAL Id: hal-02102348 <br> https://hal-lara.archives-ouvertes.fr/hal-02102348

Submitted on 17 Apr 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Laboratoire de l'Informatique du Parallélisme 



École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON-UCBL n ${ }^{\circ} 5668$

## LSP Matrix Decomposition Revisited

Claude-Pierre Jeannerod

September, 2006

Research Report No 2006-28

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : lip@ens-lyon.fr

INRIA

# LSP Matrix Decomposition Revisited 

Claude-Pierre Jeannerod

September, 2006


#### Abstract

In this paper, we study the problem of computing an LSP-decomposition of a matrix over a field. This decomposition is an extension to arbitrary matrices of the well-known LUP-decomposition of full rowrank matrices. We present three different ways of computing an LSPdecomposition, that are both rank-sensitive and based on matrix multiplication. In each case, for an $m$ by $n$ input matrix of unknown rank $r$, the cost we obtain is in $O\left(m n r^{\omega-2}\right)$ for $\omega>2$. When $r$ is small, this improves the $O\left(n m^{\omega-1}\right)$ complexity bound of Ibarra, Moran and Hui.


Keywords: Matrix factorization, matrix multiplication, reduced echelon form, rank profile, algorithmic complexity

## Résumé

Cet article considère le problème du calcul d'une décomposition LSP d'une matrice à coefficients dans un corps. Cette décomposition est une extension aux matrices de rang quelconque de la décomposition LUP, classique pour les matrices de rang plein en lignes. On présente trois façons de calculer une décomposition LSP en fonction du rang et via le produit de matrices. Dans chaque cas, le coût obtenu pour une matrice $m \times n$ de rang $r$ (inconnu a priori) est en $O\left(m n r^{\omega-2}\right)$ avec $\omega>2$. Pour $r$ petit, cela améliore la borne de complexité en $O\left(n m^{\omega-1}\right)$ d'Ibarra, Moran et Hui.

Mots-clés: Factorisation de matrice, produit de matrices, forme échelonnée, profil de rang, complexité algorithmique

## 1 Introduction

Let $A$ be an $m$ by $n$ matrix over a field $k$. It is well known that if $A$ has full row rank then it has an LUP-decomposition: $A=L U P$ where $L \in k^{m \times m}$ is unit lower triangular, $U \in k^{m \times n}$ is upper triangular with nonzero elements on the main diagonal, and $P \in k^{n \times n}$ is a permutation matrix. Furthermore, Bunch and Hopcroft's algorithm [3, 1] computes an LUP-decomposition of $A$ in $O\left(n m^{\omega-1}\right)$ field operations (see for example the proof of [4, Theorem 16.5]). Here, a field operation is any of $\{+,-, \times$, divide by a nonzero, compare with zero $\}$ and $\omega$ is such that two $n$ by $n$ matrices over $k$ can multiplied in $O\left(n^{\omega}\right)$ field operations.

When $A$ has not full row rank, LUP-decomposition may not exist anymore and Ibarra, Moran and Hui [8] extended it to the so-called LSP-decomposition (assuming $m \leq n$ ): $A=$ $L S P$ where $L$ and $P$ are as before, but where $S$ is only semi-upper triangular, that is, deleting the zero rows of $S$ yields an upper triangular matrix whose entries on the main diagonal are nonzero.

LSP-decomposition is interesting because it reveals the rank $r$ of $A$ as the number of nonzero rows of $S$. Let $i_{1}<\cdots<i_{r}$ be the indices of those rows. Then another interesting property is that $\left(i_{1}, \ldots, i_{r}\right)$ is the row rank profile of $A$, that is, the lexicographically smallest subsequence $\left(h_{1}, \ldots, h_{r}\right)$ of $(1, \ldots, m)$ such that rows $h_{1}, \ldots, h_{r}$ have full rank. (The column rank profile is defined similarly by considering columns instead of rows.)

Following Bunch and Hopcroft's approach, Ibarra, Moran and Hui also reduced the problem of computing an LSP-decomposition to that of matrix multiplication: the algorithm they give in $[8, \S 2]$-which we shall call the IMH algorithm - is for $m \leq n$ and has cost $O\left(n m^{\omega-1}\right)$.

By definition, $S$ has $r$ nonzero rows and thus its size (that is, the number of field elements required to represent it) is only $O(r n)$. For $L$, the definition requires no more than a unit lower triangular shape. However, since rows $j \notin\left\{i_{1}, \ldots, i_{r}\right\}$ of $S$ are zero and since $L$ multiplies $S$, the values of $L_{j+1, j}, \ldots, L_{m, j}$ can be anything; by choosing them to be zero, we get a factor $L$ whose $j$ th column is $e_{j}$, the $j$ th unit vector of $k^{m}$. For example, if $A \in k^{4 \times 6}$ has row rank profile $(1,3)$ then

$$
S=\left[\begin{array}{llllll}
* & * & * & * & * & * \\
& * & * & * & * & *
\end{array}\right] \rightarrow L=\left[\begin{array}{llll}
1 & & & \\
* & 1 & & \\
* & & 1 & \\
* & & * & 1
\end{array}\right]=\left[\begin{array}{ll}
* & \\
* & \\
* & *
\end{array}\right]\left[\begin{array}{llll}
1 & & & \\
& & 1 &
\end{array}\right]+\left[\begin{array}{lllll}
1 & & & \\
& 1 & & \\
& & & 1 & \\
& & & & 1
\end{array}\right] .
$$

With no loss of generality, we can thus consider that $L$ has such a shape, with (vertical) stripes corresponding to the (horizontal) stripes of $S$, and we shall say that $L$ is striped according to $S$. Clearly, such an $L$ can now be represented in a more compact way as

$$
\begin{equation*}
L=M F^{T}+I_{m}, \quad M \in k^{m \times r}, \quad F=\left[e_{i_{1}}, \ldots, e_{i_{r}}\right] \in k^{m \times r} . \tag{1}
\end{equation*}
$$

Here $M$ is dense but strictly lower triangular and even in echelon form: for $1 \leq j \leq r$, $M_{i, j}=0$ if $i \leq i_{j}$. To sum up, $O((m+n) r)$ field elements are enough for representing an LSP-decomposition $L, S, P$ with $L$ striped according to $S$. Since such a decomposition has a size that depends on $r=\operatorname{rank}(A)$, how to compute it in a rank-sensitive manner?

Gaussian elimination with column pivoting would do that with $O(m n r)$ field operations, which is indeed rank-sensitive, but unlike IMH it does not reduce to matrix multiplication.

Following the approach of [11], we show in this paper that an LSP-decomposition with $L$ striped according to $S$ can be computed both in a rank-sensitive way and via matrix
multiplication. We give three different ways of doing this, each of them having cost $O\left(m n r^{\omega-2}\right)$ if $w>2$ and $O\left(m n \log _{2} r\right)$ if $\omega=2$.

A first way, which we present in Section 2, is to compute the so-called reduced column echelon form $C$ of $A$ with Storjohann's fast, rank-sensitive GaussJordan algorithm [11, §2.2]. In Section 2.1 we show that moving from $C$ to $L, S, P$ then essentially reduces to LUPdecomposition of a full row-rank $r$ by $n$ matrix plus some matrix multiplications, for an extra cost of $O\left((m+n) r^{\omega-1}\right)$. Since $r \leq \min \{m, n\}$, note that $(m+n) r^{\omega-1}=O\left(m n r^{\omega-2}\right)$ even if $\omega=2$. Conversely, we remark in Section 2.2 that moving from $L, S, P$ to $C$ can be done also with $O\left((m+n) r^{\omega-1}\right)$ field operations.

A second way, presented in Section 3, is to improve the IMH algorithm [8] itself. Our improvement is twofold: remove the assumption that $m \leq n$; modify the elimination step to have its cost decreased from $O\left(n m^{\omega-1}\right)$ to $O\left(m n r^{\omega-2}\right)$ for $\omega \geq 2$. The resulting algorithm LSP is described in Section 3.1 and, using the techniques of [11, §1.3], its complexity is analysed in Section 3.2.

The third approach is to directly compute an LQUP-decomposition of $A$ as defined in [8]: $Q$ is an $m$ by $m$ permutation matrix, $U=\left[V^{T} \mid 0\right]^{T}$ where $V \in k^{r \times r}$ is upper triangular and invertible, and $Q U=S$. As before, we can assume with no loss of generality that $L$ is striped according to $S$ and of the form (1). Then, because of the structure of $S$ and $V$,

$$
\begin{equation*}
Q=[F \mid G] \quad \text { for some } G \in k^{m \times(m-r)} \tag{2}
\end{equation*}
$$

Therefore, using $Q Q^{T}=I_{m}$,

$$
\begin{equation*}
A=L S P=L Q U P=([M \mid 0]+Q)\left[\frac{V}{0}\right] P \tag{3}
\end{equation*}
$$

In Section 4 we give an algorithm for computing an LQUP-decomposition of $A$ in the above compressed form $M, Q, V, P$; again, its cost is $O\left(m n r^{\omega-2}\right)$ if $w>2$ and $O\left(m n \log _{2} r\right)$ if $\omega=2$. The advantage of such a compressed form is that now $M$ and $V$ can be stored as the first $r$ columns and rows, respectively, of a single $m$ by $n$ matrix. Since recovering $L, S, P$ from $M, Q, V, P$ is easy, the latter form has been used in $[9,6,5]$ to obtain extremely efficient in-place implementations of LSP-decomposition for matrices over finite fields. However no rank-sensitive complexities appear in these works.

As shown in [8, 10], LSP-/LQUP-decomposition has several applications beyong the rank and rank profile. Among them are linear system solving, computing a nullspace basis and diagonalizing transforms and generalized inverses. We conclude in Section 5 by remarking how such application problems may benefit from our improved complexity results. This may be seen as an alternative to Storjohann's Gauss-Jordan canonical form approach [11, §2.2].

## 2 LSP-decomposition and reduced echelon forms

For every $A \in k^{m \times n}$ there exists an invertible $U \in k^{m \times m}$ such that $U A=R$ is the reduced row echelon form of $A$. That form $R$ is unique and also known as the Gauss-Jordan canonical form of $A$ [11]. As a row echelon form, $R$ displays the rank $r$ and the column rank profile $\left(j_{1}, \ldots, j_{r}\right)$ of $A$ : only the first $r$ rows of $R$ are nonzero and, for $1 \leq i \leq r$, the first nonzero entry in row $i$ is $R_{i, j_{i}}$. What makes $R$ reduced is the additional property that column $j_{i}$ is the $i$ th unit vector.

For example, if $A \in k^{5 \times 9}$ has rank 3 and column rank profile ( $2,5,7$ ) then its reduced row echelon form $R$ has the following shape:

$$
R=\left[\begin{array}{llllllll}
1 & * & * & & * & & * & * \\
& & & 1 & * & & * & * \\
& & & & & 1 & * & * \\
\hline & & & & & & &
\end{array}\right] .
$$

The reduced column echelon form of $A$ can be defined as the transpose of the reduced row echelon form of $A^{T}$. If we call it $C$ then $A V=C$ for some invertible matrix $V$ and

$$
C=[E+F \mid 0], \quad \text { with } F=\left[e_{i_{1}}, \ldots, e_{i_{r}}\right] \in k^{m \times r}
$$

and with $\left(i_{1}, \ldots, i_{r}\right)$ the row rank profile of $A$. Transposing the above $5 \times 9$ matrix example, we see that the first $r$ columns of $C$ simply consist of $F$ (which has the 1 's) superimposed on $E$ (which has the $*$ 's). This way of writing $C$ will be used in the next two subsections.

Given $A$, how fast can we compute $R$ or $C$ ? Gauss-Jordan elimination would do that in time $O(m n r)$. Another way is to use Storjohann's GaussJordan algorithm [11, p. 42] whose cost is $O\left(m n r^{\omega-2}\right)$ if $\omega>2$ and $O\left(m n \log _{2} r\right)$ if $\omega=2$. This recursive algorithm will produce in particular the rank $r$ as well as a transform $U$ such that $U A=R$. Then, moving from $U$ to $R$ is cheap because $U$ is in fact returned in the form

$$
U=U_{1} U_{2}, \quad \text { where } U_{1}=\left[\begin{array}{cc}
U_{11} & \\
U_{21} & I_{m-r}
\end{array}\right] \text { and } U_{2} \text { is an } m \times m \text { permutation matrix. }
$$

To get the $r$ nonzero rows of $R$, it suffices to multiply $U_{11}$ by the first $r$ rows of $U_{2} A$. The cost of this rectangular matrix product is at most $\lceil n / r\rceil \mathrm{MM}(r)$, which for $r \leq m$ is $O\left(m n r^{\omega-2}\right)$.

By transposing twice, we obtain the same upper bound on the cost of the reduced column echelon form.

### 2.1 From the reduced column echelon form to $L, S, P$ factors

Given the reduced column echelon form $C$, we already have the row rank profile ( $i_{1}, \ldots, i_{r}$ ) of $A$. To find some $L, S, P$ factors, let $C^{\prime}$ consist of rows $i_{1}, \ldots, i_{r}$ of $C$. Then $C^{\prime}=\left[I_{r} \mid 0\right]$ and thus

$$
C=(E+F) C^{\prime} .
$$

Since $A V=C$, we have in particular $A^{\prime} V=C^{\prime}$ where $A^{\prime}$ consists of the pivot rows $i_{1}, \ldots, i_{r}$ of $A$. Since $V$ is invertible, multiplying on the right by $V^{-1}$ leads further to $A=(E+F) A^{\prime}$. For example, if $A \in k^{9 \times 5}$ has rank 3 and row rank profile $(2,5,7)$ then

$$
A=(E+F) A^{\prime}=\left[\begin{array}{cccc}
1 & & \\
* & & \\
* & & \\
& 1 & \\
* & * & \\
* & * & * \\
* & * & *
\end{array}\right]\left[\begin{array}{ccccc}
* & * & * & * & * \\
* & * & * & * & * \\
* & * & * & * & *
\end{array}\right]
$$

Notice that such a factorization reveals an important property of the reduced column echelon form $C=[E+F \mid 0]$ : every row $i$ of $A$ is equal to a unique linear combination of earlier pivot
rows (that is, of rows $i_{1}, i_{2}, \ldots$ of $A$ such that $i_{1}, i_{2}, \ldots \leq i$ ) and, above all, the coefficients of this combination are exactly the entries of the $i$ th row of $E+F$.

Since $A^{\prime} \in k^{r \times n}$ has full row rank, it has an LUP-decomposition, say $A^{\prime}=L^{\prime} U^{\prime} P$. Let $S=F U^{\prime}$. Since $U^{\prime} \in k^{r \times n}$ is upper triangular, $S \in k^{m \times n}$ is semi-upper triangular. Therefore, using the fact that $F^{T} F=I_{r}$ we obtain the following factorization:

$$
A=L^{\prime \prime} S P, \quad \text { where } L^{\prime \prime}=(E+F) L^{\prime} F^{T} .
$$

The last step to modify $L^{\prime \prime}$ slightly in order to find a unit lower triangular factor $L$. Let $E^{\prime} \in k^{m \times r}$ be defined by

$$
E^{\prime}+F=(E+F) L^{\prime} .
$$

Since $L^{\prime}$ is unit lower triangular, $E^{\prime}+F$ has exactly the same echelon form as $E+F$. (However, notice that row $i_{j}$ of $E+F$ is not a unit vector but contains instead the $j$ th row of $L^{\prime}$.) It follows that $L^{\prime \prime}=E^{\prime} F^{T}+F F^{T}=$ (strictly lower triangular) + (diagonal) is lower triangular. To get a unit lower triangular factor, simply replace $L^{\prime \prime}$ with

$$
\begin{equation*}
L=E^{\prime} F^{T}+I_{m} . \tag{4}
\end{equation*}
$$

The rows $i_{1}, \ldots, i_{r}$ of $S$ being zero, we have indeed $A=L S P$, which is now an LSPdecomposition of $A$. Furthermore, $L$ in (4) is striped according to $S$.

The above move from $C$ to $L, S, P$ requires LUP-decomposition of an $r \times n$ matrix as well as computing the product $(E+F) L^{\prime}$ where $E+F$ is $m \times r$ and $L^{\prime}$ is $r \times r$. The latter costs at most $\lceil m / r\rceil \mathrm{MM}(r) \in O\left(m r^{\omega-1}\right)$ and the former can be done in time $O\left(n r^{\omega-1}\right)$ with the Bunch and Hopcroft algorithm [3]. Hence a total of $O\left((m+n) r^{\omega-1}\right)$, which is in $O\left(m n r^{\omega-2}\right)$ for $r \leq \min \{m, n\}$. We thus have shown the following result:

Theorem 2.1 An LSP-decomposition of $A \in k^{m \times n}$ of (unknown) rank $r$ can be computed in time $O\left(m n r^{\omega-2}\right)$ by calling Storjohann's reduced row echelon form algorithm and then the Bunch and Hopcroft LUP-decomposition algorithm. If $\omega=2$, the cost becomes $O\left(m n \log _{2} r\right)$.

### 2.2 From $L, S, P$ factors to the reduced column echelon form

Conversely, what if some $L, S, P$ factors of $A$ are given? First, deducing from $S$ the row rank profile ( $i_{1}, \ldots, i_{r}$ ) of $A$ and taking $F=\left[e_{i_{1}}, \ldots, e_{i_{r}}\right] \in k^{m \times r}$, an $L Q U P$-decomposition follows easily: augment $F$ with $m-r$ columns into a permutation matrix $Q=[F \mid G] \in k^{m \times m}$ and let $V=F^{T} S$; then $V$ is upper triangular with nonzero elements on the main diagonal, and

$$
A=L Q U P, \quad U=\left[\frac{V}{0}\right] .
$$

A second step is to move further to the reduced column echelon form of $A$; this can be done fast with as claimed below.

Theorem 2.2 Given $A=L S P \in k^{m \times n}$, one can deduce the reduced column echelon form of A together with a transformation matrix in $O\left((m+n) r^{\omega-1}\right)$ operations.

Proof. With no loss of generality, assume that $L$ is striped according to $S$. Then, by (3) we have $A=(M+F) V P$. Let $N \in k^{r \times r}$ consist of rows $i_{1}, \ldots, i_{r}$ of $M+F$. Then $N$ is unit
lower triangular and, writing $A^{\prime}$ for the submatrix of $A$ that consists of rows $i_{1}, \ldots, i_{r}$, we get $A^{\prime}=N V P$ and thus

$$
A=(M+F) N^{-1} A^{\prime}
$$

Now let $D \in k^{m \times r}$ be defined by $D+F=(M+F) N^{-1}$. It is not hard to see that the $m$ by $n$ matrix $[D+F \mid 0]$ is in reduced column echelon form; if we show that $A=[D+F \mid 0] W$ for some invertible matrix $W$ then, by uniqueness, $[D+F \mid 0]$ must be the reduced column echelon form of $A$. To show that, let

$$
W=W_{1} W_{2}, \quad W_{1}=\left[\begin{array}{cc}
W_{11} & W_{12} \\
& I_{n-r}
\end{array}\right], \quad\left[\begin{array}{ll}
W_{11} & W_{12}
\end{array}\right]=A^{\prime} P^{T}, \quad W_{2}=P^{T}
$$

Since $V=N^{-1} A^{\prime} P^{T}$ has nonzero elements on the main diagonal, $W_{1}$ is invertible and so is $W$. On the other hand, using $(D+F) A^{\prime}=A$, we obtain $A=[D+F \mid 0] W$. Therefore $[D+F \mid 0]$ is indeed the reduced column echelon form of $A$ and a transformation matrix is $W^{-1}$.

Since $D+F=(M+F) N^{-1}$ is $m \times r$ and $N$ is $r \times r$, one can obtain $D$ with $O\left(m r^{\omega-1}\right)$ field operations; since [ $W_{11} \mid W_{12}$ ] is $r \times n$ and $W_{11}$ is $r \times r$, one can obtain $W^{-1}$ with $O\left(n r^{\omega-1}\right)$ field operations.

## 3 A rank-sensitive version of the IMH algorithm

We now present another approach to computing $A=L S P$, which is a rank-sensitive extension of algorithm IMH (Ibarra, Mora and Hui [8]; see also [2, p. 103] for a description). The principle of IMH is as follows: cut $A$ into horizontal slices $A_{1}$ and $A_{2}$ with roughly the same number of rows; compute $A_{1}=L_{1} S_{1} P_{1}$ recursively; perform on $A_{2} P_{1}^{T}$ an elimination step similar to that of block-Gaussian elimination; compute $B_{2}=L_{2} S_{2} P_{2}$ recursively with $B_{2}$ the lower-right block produced by elimination. This principle is depicted below on a $6 \times 4$ matrix with row rank profile $(1,3,5,6)$; there, $\bar{*}$ means a nonzero entry:

$$
A=\underbrace{\left[\begin{array}{llll}
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & *
\end{array}\right]}_{=:\left[\begin{array}{lll}
A_{1} \\
A_{2}
\end{array}\right]} \rightarrow\left[\begin{array}{llll}
\bar{*} & * & * & * \\
& \bar{*} & * & * \\
* & * & * & * \\
* & * & * & * \\
* & * & * & *
\end{array}\right] \rightarrow \underbrace{\left[\begin{array}{lllll}
\bar{*} & * & * & * \\
& \bar{*} & * & * \\
& * & * \\
& * & * \\
& & *
\end{array}\right]}_{=:\left[\begin{array}{lllll}
S_{11} & S_{12} \\
& & B_{2}
\end{array}\right]} \rightarrow\left[\begin{array}{ll|ll}
\bar{*} & * & * & * \\
& \bar{*} & * & * \\
\hline & & \bar{*} & \\
& & & \\
& &
\end{array}\right]=S .
$$

Factor $S$ is obtained by stacking [ $S_{11} S_{12} P_{2}^{T}$ ] over [ $0 S_{2}$ ], with $\left[S_{11} S_{12}\right]=S_{1}$. Factors $L$ and $P$ record respectively the row operations and column interchanges needed for moving from $A$ to $S$. For example, after the elimination step, we have an intermediate factorization of the form

$$
\left[\begin{array}{l}
A_{1}  \tag{5}\\
A_{2}
\end{array}\right]=\left[\begin{array}{cc}
L_{1} & \\
L_{21} & I_{m_{2}}
\end{array}\right]\left[\begin{array}{cc}
S_{11} & S_{12} \\
& B_{2}
\end{array}\right] P_{1} .
$$

Now let $r_{1}$ be the rank of $A_{1}$. Then $r_{1}$ is also the number of nonzero rows of $S_{1}$, and $S_{11}$ consists of the first $r_{1}$ columns of $S_{1}$.

Our algorithm improves on algorithm IMH in two ways. In [8] it is always assumed that $m \leq n$, which implies $r_{1}<n$. Unlike algorithm IMH, the algorithm we describe in Section 3.1
works for arbitrary input dimensions $m \times n$ and the situation where $r_{1}=n$ may occur. In that case, $B_{2}$ is an empty matrix and the second recursive call is not needed. Hence an explicit test to detect that $r_{1}=n$ and then exit early. Second, algorithm IMH computes $L_{21}$ and $B_{2}$ in $O\left(m^{\omega-1} n\right)$ field operations. We show in Section 3.2 that our algorithm computes them in $O\left(m n r^{\omega-2}\right)$ with $r$ the rank of $A$.

### 3.1 Algorithm description

We present here a rank-sensitive version of the IMH algorithm along with a correctness proof. The algorithm is written in Maple-like pseudo code. Note that $m \leq n$ is not assumed.

```
Algorithm LSP( \(A\) )
Input: \(A \in k^{m \times n}\).
Output: an LSP-decomposition of \(A\).
if \(A=0\) then
    \(L, S, P:=I_{m}, 0_{m \times n}, I_{n} ;\)
else if \(m=1\) then
    \(j:=\) the index of the first nonzero entry of \(A\);
    \(P:=\) the permutation matrix that interchanges \(A_{1,1}\) and \(A_{1, j}\);
    \(L, S:=I_{1}, A P ;\)
else
    \(m_{1}, m_{2}:=\lfloor m / 2\rfloor,\lceil m / 2\rceil ;\)
    \(L_{1}, S_{1}, P_{1}:=\operatorname{LSP}\left(A_{1}\right)\) with \(A_{1}\) the first \(m_{1}\) rows of \(A\);
    \(r_{1}:=\) the number of nonzero rows of \(S_{1}\);
    if \(r_{1}=0\) then
        \(L_{2}, S_{2}, P_{2}:=\operatorname{LSP}\left(A_{2}\right)\) with \(A_{2}\) the last \(m_{2}\) rows of \(A\);
        \(L, S, P:=\left[\begin{array}{ll}I_{m_{1}} & \\ & L_{2}\end{array}\right],\left[\begin{array}{l} \\ S_{2}\end{array}\right], P_{2} ;\)
    else
        \(S_{11}:=\) the first \(r_{1}\) columns of \(S_{1}\);
        \(Q_{1}:=\) the first \(r_{1}\) rows of a permutation matrix \(Q\) such that \(Q S_{11}=\left[\begin{array}{ll}U^{T} & 0\end{array}\right]^{T}\)
                with \(U\) upper triangular and nonsingular;
            \(T_{2}:=A_{2} P_{1}^{T}\) with \(A_{2}\) the last \(m_{2}\) rows of \(A\);
            \(L_{21}:=\left(T_{21} U^{-1}\right) Q_{1}\) with \(T_{21}\) the first \(r_{1}\) columns of \(T_{2}\);
            if \(r_{1}=n\) then
            \(L, S, P:=\left[\begin{array}{cc}L_{1} & \\ L_{21} & I_{m_{2}}\end{array}\right],\left[\begin{array}{l}S_{1} \\ \end{array}\right], P_{1} ;\)
            else
                \(B_{2}:=T_{22}-\left(L_{21} Q_{1}^{T}\right)\left(Q_{1} S_{12}\right)\) with \(S_{12}, T_{22}\) the last \(n-r_{1}\) columns of \(S_{1}, T_{2}\);
            \(L_{2}, S_{2}, P_{2}:=\operatorname{LSP}\left(B_{2}\right) ;\)
            \(L, S, P:=\left[\begin{array}{cc}L_{1} & \\ L_{21} & L_{2}\end{array}\right],\left[\begin{array}{cc}S_{11} & S_{12} P_{2}^{T} \\ & S_{2}\end{array}\right],\left[\begin{array}{cc}I_{r_{1}} & \\ & P_{2}\end{array}\right] P_{1} ;\)
        fi;
    fi;
f;
return \(L, S, P\);
```

If $A=0$ then correctness of Algorithm LSP is clear. If $A \neq 0$, we proceed by induction on $m$. If $m=1$ then $P^{2}=I_{n}$ and $A=\left(I_{1}\right)(A P)(P)$ is an LSP-decomposition of $A$. Assume now that $m>1$. From $m_{1}=\lfloor m / 2\rfloor$ and $m_{2}=\lceil m / 2\rceil$, it follows that

$$
m_{1} \leq m_{2}<m
$$

Hence by induction we have the LSP-decomposition $A_{1}=L_{1} S_{1} P_{1}$; similarly, $L_{2}, S_{2}, P_{2}$ is an LSP-decomposition of $A_{2}$ when $r_{1}=0$ and of $B_{2}$ when $0<r_{1}<n$. Therefore, for each of the three cases " $r_{1}=0$ ", " $r_{1}=n$ " and " $0<r_{1}<n$ ", the matrices $L, S, P$ computed by the algorithm have the desired shape ( $L$ is unit lower triangular, $S$ is semi-upper triangular and $P$ is a permutation matrix). It remains to show that the product $L S P$ indeed equals $A$. To do that let us consider each case separately, using $r_{1}=\operatorname{rank}\left(A_{1}\right)$ and $U^{-1} Q_{1} S_{11}=I_{r_{1}}$.

1. If $r_{1}=0$ then $A_{1}=0$ and $A_{2}=L_{2} S_{2} P_{2}$, which leads to

$$
A=\left[\begin{array}{l} 
\\
A_{2}
\end{array}\right]=\left[\begin{array}{ll}
I_{m_{1}} & \\
& L_{2}
\end{array}\right]\left[\begin{array}{l} 
\\
S_{2}
\end{array}\right] P_{2}=L S P
$$

2. If $r_{1}=n$ then $S_{11}=S_{1}$ and $T_{2}=T_{21}$. Hence $U^{-1} Q_{1} S_{1}=I_{r_{1}}$ and $A_{2}=T_{21} P_{1}$. Since $L_{21}=T_{21} U^{-1} Q_{1}$, it follows that $L_{21} S_{1} P_{1}=A_{2}$. Using $A_{1}=L_{1} S_{1} P_{1}$ we arrive at

$$
A=\left[\begin{array}{l}
A_{1} \\
A_{2}
\end{array}\right]=\left[\begin{array}{cc}
L_{1} & \\
L_{21} & I_{m_{2}}
\end{array}\right]\left[\begin{array}{l}
S_{1} \\
\end{array}\right] P_{1}=L S P
$$

3. If $0<r_{1}<n$ then $L_{21} Q_{1}^{T}$ consists of the first $r_{1}$ columns of $L_{21} Q^{T}$ and $Q_{1} S_{12}$ consists of the first $r_{1}$ rows of $Q S_{12}$. Since by definition of $Q$ and $S_{1}$ all other rows of $Q S_{12}$ are zero, $\left(L_{21} Q_{1}^{T}\right)\left(Q_{1} S_{12}\right)=\left(L_{21} Q^{T}\right)\left(Q S_{12}\right)=L_{21} S_{12}$. Therefore $T_{22}=L_{21} S_{12}+B_{2}$. In addition, $U^{-1} Q_{1} S_{11}=I_{r_{1}}$ gives $T_{21}=L_{21} S_{11}$. Since $T_{2} P_{1}=\left[T_{21} T_{22}\right] P_{1}=A_{2}$ and $L_{1}\left[S_{11} S_{12}\right] P_{1}=A_{1}$ we get the intermediate factorization (5). Then $B_{2}=L_{2} S_{2} P_{2}$ gives

$$
A=\left[\begin{array}{cc}
L_{1} & \\
L_{21} & L_{2}
\end{array}\right]\left[\begin{array}{cc}
S_{11} & S_{12} P_{2}^{T} \\
& S_{2}
\end{array}\right]\left[\begin{array}{ll}
I_{r_{1}} & \\
& P_{2}
\end{array}\right] P_{1}=L S P .
$$

To sum up, the output $L, S, P$ satisfies $A=L S P$ for each case and correctness follows.
Notice that so far we have used only the fact that $m_{1}+m_{2}=m$ with $m_{1}, m_{2}<m$. The values $m_{1}=\lfloor m / 2\rfloor$ and $m_{2}=\lceil m / 2\rceil$ will be used in the next subsection for bounding the complexity of the algorithm.

### 3.2 Complexity analysis

First let us verify that the unit lower triangular factor $L$ computed by Algorithm LSP has the expected sparsity structure.

Property 3.1 The factor L computed by Algorithm LSP is striped according to $S$.
Proof. For $A=0$ this is clear since $L-I_{m}$ is zero. For $A$ nonzero, let us proceed by induction on $m$, the case $m=1$ being clear too. Assume $m>1$ and recall that $m_{1}=\lfloor m / 2\rfloor \leq$ $m_{2}=\lceil m / 2\rceil<m$. If $r_{1}=0$ then $\left(i_{1}, \ldots, i_{r}\right)=\left(m_{1}+i_{1}^{\prime \prime}, \ldots, m_{1}+i_{r}^{\prime \prime}\right)$ with $\left(i_{j}^{\prime \prime}\right)$ the row rank profile of $A_{2}$, and the assertion follows by induction. If $r_{1}>0$ then the row rank profile of $A_{1}$
is $\left(i_{1}, \ldots, i_{r_{1}}\right)$; hence by induction only those columns of $L_{1}-I_{m_{1}}$ can be nonzero. Now, the $j$ th column of $Q_{1}$ is zero for all $j \notin\left\{i_{1}, \ldots, i_{r_{1}}\right\}$, for otherwise $U$ would have a zero row (a contradiction). It follows that only columns $i_{1}, \ldots, i_{r_{1}}$ of $L_{21}$ can be nonzero. If $r_{1}=n$ then we are done. If $r_{1}<n$ then let $\left(i_{j}^{\prime \prime}\right)$ be the row rank profile of $B_{2}$. Since from (5) one has $r_{2}:=\operatorname{rank}\left(B_{2}\right)=r-r_{1}$ and $i_{r_{1}+j}=m_{1}+i_{j}^{\prime \prime}$ for $1 \leq j \leq r_{2}$, the claim follows by induction.

Therefore $L$ requires only $O(m r)$ field elements compared to $m(m-1) / 2$ for general $m \times m$ unit lower triangular matrices. Now let us bound the cost of the elimination step, that is, of computing $L_{21}$ and $B_{2}$.
Lemma 3.2 Computing $L_{21}$ and $B_{2}$ can be done with $O\left(m n r^{\omega-2}\right)$ field operations.
Proof. For $L_{21}=\left(T_{21} U^{-1}\right) Q_{1}$, the invertible matrix $U$ is $r_{1} \times r_{1}$ and $T_{21}$ is $m_{2} \times r_{1}$. In addition, $r_{1}=\operatorname{rank}\left(A_{1}\right)$ implies $r_{1} \leq m_{2}$. Hence $T_{21} U^{-1}$ can be computed in time $O\left(m_{2} r_{1}^{\omega-1}\right)$. For $B_{2}$, let $C_{21}=L_{21} Q_{1}^{T}$ and $R_{12}=Q_{1} S_{12}$. Then $C_{21}$ is $m_{2} \times r_{1}$ and $R_{12}$ is $r_{1} \times\left(n-r_{1}\right)$. We have already seen that $r_{1} \leq m_{2}$. Now, if $r_{1} \leq n-r_{1}$ then one can compute in $C_{21} R_{12}$ in time $O\left(m_{2}\left(n-r_{1}\right) r_{1}^{\omega-2}\right)$; else simply multiply $C_{21}$ by $R_{12}$ padded first with $2 r_{1}-n$ zero columns, and that in time $O\left(m_{2} r_{1}^{\omega-1}\right)$. Adding $T_{22}$ has cost $O\left(m_{2}\left(n-r_{1}\right)\right)$. Conclusion follows for both $L_{21}$ and $B_{2}$ from $m_{2} \leq m$ and $r_{1} \leq r \leq n$.

Using this lemma, let us now estimate $T(m, n, r)$, the number of field operations required by Algorithm LSP for input $A \in k^{m \times n}$ of (unknown) rank $r$. Following [11] we count a comparison with zero as a field operation. Then, when $r=0$ (that is, $A=0$ ) or $m=1$, we have $T(m, n, r)=O(m n)$. Otherwise, recall that $r_{1}$ is the rank of $A_{1}$ and let $r_{2}$ be the rank of $B_{2}$; then, by Lemma 3.2

$$
T(m, n, r)= \begin{cases}T\left(m_{1}, n, 0\right)+T\left(m_{2}, n, r\right)+O(m n) & \text { if } r_{1}=0 \\ T\left(m_{1}, n, r_{1}\right)+O\left(m n r^{\omega-2}\right) & \text { if } r_{1}=n \\ T\left(m_{1}, n, r_{1}\right)+T\left(m_{2}, n-r_{1}, r_{2}\right)+O\left(m n r^{\omega-2}\right) & \text { if } 0<r_{1}<n\end{cases}
$$

Hence $T(m, n, r)$ is upper bounded by a function $f_{n}(m, r)$ such that

$$
f_{n}(m, r)= \begin{cases}O(m n) & \text { if } m=1 \text { or } r=0, \\ f_{n}\left(\lfloor m / 2\rfloor, r_{1}\right)+f_{n}\left(\lceil m / 2\rceil, r_{2}\right)+O\left(m n r^{\omega-2}\right) & \text { otherwise }\end{cases}
$$

for some $r_{1}, r_{2} \geq 0$ with $r=r_{1}+r_{2}$. By [11, §1.3] one has $f_{n}(m, r)=O\left(m n r^{\omega-2}\right)$ if $\omega>2$ and $f_{n}(m, r)=O\left(m n \log _{2} r\right)$ if $\omega=2$. Thus we have shown the following:
Theorem 3.3 Let $A \in k^{m \times n}$ of (unknown) rank $r$. Algorithm LSP computes an LSPdecomposition of $A$ in time $O\left(m n r^{\omega-2}\right)$ if $\omega>2$. If $\omega=2$, the cost becomes $O\left(m n \log _{2} r\right)$.

One could modify easily Algorithm LSP so that it returns not only some factors $L, S, P$ but also the rank and the row rank profile of $A$. For applications (see Section 5), one might need $L^{-1}$ rather than $L$; modifying Algorithm LSP accordingly and obtaining the same complexity bound as in Theorem 3.3 is not hard neither. Here it is interesting to note that if $L$ is striped according to $S$ then its inverse $L^{-1}$ is too. To check this, simply observe that if $j \notin\left\{i_{1}, \ldots, i_{r}\right\}$ then $e_{j}$ is the $j$ th column of both $L$ and $I_{m}$. Therefore the $j$ th column of $L^{-1}$ is $L^{-1} e_{j}=e_{j}$, which means that $L^{-1}$ is striped according to $S$.

As already observed in [8], once we have an LSP-decomposition of $A$, an LQUP-decomposition can be deduced immediately. In the next section, we modify Algorithm LSP so as to compute directly an LQUP-decomposition.

## 4 A rank-sensitive LQUP-decomposition algorithm

Instead of computing $L, S, P$ recursively, one can work directly with a corresponding LQUPdecomposition in compressed form. Using the same divide-and-conquer approach as in Section 3, the goal is now to compute matrices $M, Q, V, P$ as in (1), (2), (3).

Recall that $M \in k^{m \times r}$ is in echelon form ( $M_{i, j}=0$ for $i \leq i_{j}$ ), that the first $r$ columns of $Q$ are $F$, and that $V \in k^{r \times r}$ is upper triangular and invertible. Furthermore, an LSPdecomposition of $A$ with $L$ striped according $S$ follows from

$$
A=([M \mid 0]+Q)\left[\frac{V}{0}\right] P
$$

by taking

$$
L=[M \mid 0] Q^{T}+I_{m} \quad \text { and } \quad S=Q\left[\frac{V}{0}\right] .
$$

Theorem 4.1 Algorithm LQUP is correct. Its cost is $O\left(m n r^{\omega-2}\right)$ if $\omega>2$ and $O\left(m n \log _{2} r\right)$ if $\omega=2$.

Proof. The proof is similar to that of Theorem 3.3: for correctness, we can proceed by induction on $m$ and, for $m>1$, study separately three cases " $r_{1}=0$ ", " $r_{1}=n$ " and " $0<r_{1}<n$." (Some details about each case are provided in Appendix A.) As for the complexity bound, it is obtained in exactly the same way as in Section 3.2.

In the algorithm below, by "matrix $m \times 0$ " we mean a matrix with $m$ empty rows.

```
Algorithm LQUP \((A)\)
Input: \(A \in k^{m \times n}\).
Output: an LQUP-decomposition of \(A\) in compressed form \(M, Q, V, P\) and its rank \(r\).
if \(A=0\) then
    \(M, Q, V, P, r:=\) matrix \(m \times 0, I_{m}\), matrix \(0 \times n, I_{n}, 0 ;\)
else if \(m=1\) then
    \(j:=\) the index of the first nonzero entry of \(A\);
    \(P:=\) the permutation matrix that interchanges \(A_{1,1}\) and \(A_{1, j}\);
    \(M, Q, V, r:=0_{1 \times 1}, I_{1}, A P, 1 ;\)
else
    \(m_{1}, m_{2}:=\lfloor m / 2\rfloor,\lceil m / 2\rceil ;\)
    \(M_{1}, Q_{1}, V_{1}, P_{1}, r_{1}:=\operatorname{LQUP}\left(A_{1}\right)\) with \(A_{1}\) the first \(m_{1}\) rows of \(A\);
    if \(r_{1}=0\) then
        \(M_{2}, Q_{2}, V_{2}, P_{2}, r_{2}:=\operatorname{LQUP}\left(A_{2}\right)\) with \(A_{2}\) the last \(m_{2}\) rows of \(A\);
        \(M, Q, V, P, r:=\left[\begin{array}{ll}M_{2}\end{array}\right],\left[\begin{array}{ll}I_{m_{1}} \\ Q_{2} & \end{array}\right], V_{2}, P_{2}, r_{2} ;\)
    else
        \(V_{11}:=\) the first \(r_{1}\) columns of \(V_{1}\);
        \(T_{2}:=A_{2} P_{1}^{T}\) with \(A_{2}\) the last \(m_{2}\) rows of \(A\);
        \(M_{21}:=T_{21} V_{11}^{-1}\) with \(T_{21}\) the first \(r_{1}\) columns of \(T_{2}\);
        if \(r_{1}=n\) then
            \(M, Q, V, P, r:=\left[\begin{array}{c}M_{1} \\ M_{21}\end{array}\right],\left[\begin{array}{cc}Q_{1} & \\ & I_{m_{2}}\end{array}\right], V_{11}, P_{1}, r_{1} ;\)
        else
            \(B_{2}:=T_{22}-M_{21} V_{12}\) with \(V_{12}, T_{22}\) the last \(n-r_{1}\) columns of \(V_{1}, T_{2}\);
            \(M_{2}, Q_{2}, V_{2}, P_{2}, r_{2}:=\operatorname{LQUP}\left(B_{2}\right)\);
            \(M, V, P, r:=\left[\begin{array}{cc}M_{1} & \\ M_{21} & M_{2}\end{array}\right],\left[\begin{array}{cc}V_{11} & V_{12} P_{2}^{T} \\ & V_{2}\end{array}\right],\left[\begin{array}{cc}I_{r_{1}} & \\ & P_{2}\end{array}\right] P_{1}, r_{1}+r_{2} ;\)
            \(Q:=\left[\begin{array}{l|l|l|l}Q_{11} & & Q_{12} & \\ \hline & Q_{21} & & Q_{22}\end{array}\right]\) with \(Q_{i}=\left[Q_{i 1} \mid Q_{i 2}\right]\) and \(Q_{i 1}\) having \(r_{i}\) columns;
        f;
    fi;
fi;
return \(M, Q, V, P, r\);
```


## 5 Some applications of LSP-/LQUP-decomposition

In $[8, \S 4]$ and $[10, \S 4]$, several applications of an LSP- or LQUP-decomposition are given: solve the linear system $A x=b$ or detect that it has no solution; find a submatrix of $A$ whose column and row ranks are both equal to $r$, and, more generally, reorder the rows and columns of $A$ to obtain a matrix with generic rank profile; compute left and right nullspace bases of $A$; diagonalize $A$, that is, compute an $m$ by $m$ nonsingular matrix $X$ and an $n$ by nonsingular matrix $Y$ such that $X A Y=\operatorname{diag}\left(I_{r}, 0\right)$; compute various generalized inverses (generalized, reflexive generalized [8, p.54] and, when $k$ is the field of complex numbers, Moore-Penrose [7, p.257]).

A consequence of the algorithms of the previous sections is that the complexity of such application problems is now bounded by $O\left(n m r^{\omega-2}\right)$ or $O\left(m n \log _{2} r\right)$ instead of $O\left(n m^{\omega-1}\right)$.

We give some details below.
Generic rank profile. Partition $V$ in (3) as $V=\left[V_{1} \mid V_{2}\right]$ with $V_{1} \in k^{r \times r}$. Then

$$
Q^{T} A P^{T}=\left[\frac{F^{T} M+I_{r}}{G^{T} M}\right]\left[V_{1} \mid V_{2}\right] .
$$

Since $F^{T} M+I_{r}$ is unit lower triangular and $V_{1}$ is upper triangular and nonsingular, the first $r$ principal minors of the product $\left(F^{T} M+I_{r}\right) V_{1}$ are nonsingular. Hence $Q^{T} A P^{T}$ has generic rank profile.

Linear system solving. Here the classic process is as follows. Given $A \in k^{m \times n}$ and $b \in k^{n}$, first compute an LSP-decomposition of $A$; then compute the vector $c=L^{-1} b$; conclude that $A x=b$ has no solution, otherwise solve $S y=c$ for $y$ and return $x=P^{T} y$.

Due to the semi-upper triangular shape of $S$, solving $S y=c$ has cost $O\left(r^{\omega}\right)$. In order to bound the cost of solving $L c=b$, observe that

$$
L=[M \mid 0] Q^{T}+I_{m}
$$

leads to

$$
Q^{T} L Q=Q^{T}[M \mid 0]+I_{m} .
$$

Now, $W:=Q^{T} L Q$ has the shape

$$
W=\left[\begin{array}{ll}
W_{1} & \\
W_{2} & I_{m-r}
\end{array}\right], \quad \text { with } W_{1} \in k^{r \times r} \text { invertible. }
$$

Therefore, by inverting $W$, one can compute $L^{-1} b=Q\left(W^{-1}\left(Q^{T} b\right)\right)$ with $O\left(m r^{\omega-1}\right)$ field operations. In conclusion, when $A=L S P$ is given, one can solve $A x=b$ or decide that no solution exists with $O\left(m r^{\omega-1}\right)$ extra operations.

Left and right nullspace bases. With $V_{1}, V_{2}, W_{1}, W_{2}$ as above, it is not hard to verify that bases of the left and right nullspaces of $A$ are given by, respectively,

$$
\left[\begin{array}{ll}
-W_{2} W_{1}^{-1} & I_{m-r}
\end{array}\right] Q^{T} \quad \text { and } \quad P^{T}\left[\begin{array}{c}
-V_{1}^{-1} V_{2} \\
I_{n-r}
\end{array}\right] .
$$

Given $A=L Q U P$, computing those two bases costs $O\left((m+n) r^{\omega-1}\right)$ field operations.
Diagonalizing transforms. Some transforms $X \in k^{m \times m}$ and $Y \in k^{n \times n}$ such that $X A Y=$ $\operatorname{diag}\left(I_{r}, 0\right)$ are (see [8, p.53])

$$
X=Q^{-1} L^{-1} \quad \text { and } \quad Y=P^{T}\left[\begin{array}{cc}
V_{1}^{-1} & -V_{1}^{-1} V_{2} \\
& I_{n-r}
\end{array}\right]
$$

Hence, given $A=L Q U P$, one can compute them at an extra cost of $O\left((m+n) r^{\omega-1}\right)$.
Generalized inverses. From the proof of [8, Theorem 3.3], an arbitrary generalized inverse and an arbitrary reflexive inverse can both be deduced from the above $X, Y, L, Q, V$ via some matrix multiplications having cost $O\left(m n r^{\omega-2}\right)$. From the proof of [8, Theorem 3.4] one can see that, given $A=L Q U P$, the cost of the Moore-Penrose inverse is dominated by the cost of multiplying an $n \times r$ matrix by an $r \times m$ matrix, which is $O\left(m n r^{\omega-2}\right)$ too.

## References

[1] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974.
[2] D. Bini and V.Y. Pan. Polynomial and Matrix Computations, Volume 1: Fundamental Algorithms. Birkhäuser, Boston, 1994.
[3] J. Bunch and J. Hopcroft. Triangular factorization and inversion by fast matrix multiplication. Mathematics of Computation, 28(125):231-236, 1974.
[4] B. Bürgisser, C. Clausen, and M.A. Shokrollahi. Algebraic Complexity Theory, volume 315 of Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1997.
[5] J.-G. Dumas, T. Gautier, P. Giorgi, and C. Pernet. Dense linear algebra over finite fields: the FFLAS and FFPACK packages. Technical Report cs.SC/0601133, arXiv, 2006.
[6] J.-G. Dumas, P. Giorgi, and C. Pernet. FFPACK: Finite Field Linear Algebra Package. In J. Gutierrez, editor, Proc. International Symposium on Symbolic and Algebraic Computation, Santander, Spain, pages 119-126. ACM Press, 2004.
[7] G.H. Golub and C.F. Van Loan. Matrix Computations. The Johns Hopkins University Press, third edition, 1996.
[8] O.H. Ibarra, S. Moran, and R. Hui. A generalization of the fast LUP matrix decomposition algorithm and applications. Journal of Algorithms, 3:45-56, 1982.
[9] C. Pernet. Calcul du polynôme caractéristique sur des corps finis. Master's thesis, Université Joseph Fourier, 2003.
[10] C. Pernet. Algèbre linéaire exacte efficace: le calcul du polynôme caractéristique. PhD thesis, Université Joseph Fourier, 2006.
[11] A. Storjohann. Algorithms for Matrix Canonical Forms. PhD thesis, Swiss Federal Institute of Technology, ETH-Zurich, 2000.

## A Some details for the correctness proof of Algorithm LQUP

## A. 1 Case where $r_{1}=0$

In this case $r=r_{2}$ and

$$
A=\left[\frac{0}{A_{2}}\right],
$$

which implies

$$
A P_{2}^{T}=\left[\begin{array}{c}
0 \\
\hline L_{2} Q_{2} U_{2}
\end{array}\right]=\left[\begin{array}{l|l}
I_{m_{1}} & \\
\hline & L_{2} Q_{2}
\end{array}\right]\left[\begin{array}{c}
0 \\
\hline U_{2}
\end{array}\right], \quad L_{2} Q_{2}=\left[M_{2} \mid 0\right]+Q_{2}, \quad U_{2}=\left[\begin{array}{c}
V_{2} \\
\hline 0
\end{array}\right] .
$$

Hence

$$
A=[\begin{array}{l|l} 
& I_{m_{1}} \\
\hline\left[M_{2} \mid 0\right]+Q_{2} &
\end{array}\left[\begin{array}{c}
U_{2} \\
\hline 0
\end{array}\right]=(\underbrace{\left[\begin{array}{c|c}
0 & 0_{m_{1} \times\left(m-r_{2}\right)} \\
\hline M_{2} & 0
\end{array}\right]}_{=:[M \mid 0]}+\underbrace{\left[\begin{array}{c|c} 
& I_{m_{1}} \\
\hline Q_{2} &
\end{array}\right]}_{=: Q}\left[\left[\begin{array}{c}
V_{2} \\
0
\end{array}\right] P_{2}\right.
$$

and $V:=V_{2}$ and $P:=P_{2}$. The first $r$ columns of $Q$ are $\left[\frac{0}{Q_{2}}\right]=\left[e_{i_{1}^{\prime}+m_{1}}, \ldots, e_{i_{r}^{\prime}+m_{1}}\right]$ where, by induction, $\left(i_{j}^{\prime}\right)$ is the row rank profile of $A_{2}$. Conclusion follows from the fact that when $r_{1}=0$ one has $i_{j}=i_{j}^{\prime}+m_{1}$ for $1 \leq j \leq r$. Similarly, $M$ is of the desired shape because $M_{2}$ is, by induction.

## A. 2 Case where $r_{1}>0$

In this case

$$
A=\left[\frac{A_{1}}{A_{2}}\right]=\left[\frac{L_{1} Q_{1} U_{1}}{T_{2}}\right] P_{1}, \quad L_{1} Q_{1}=\left[M_{1} \mid 0\right]+Q_{1}, \quad U_{1}=\left[\begin{array}{c}
V_{1} \\
0
\end{array}\right]
$$

Therefore, with $V_{1}=\left[\begin{array}{ll}V_{11} & V_{12}\end{array}\right]$ and $T_{2}=\left[\begin{array}{ll}T_{21} & T_{22}\end{array}\right]$,

$$
\begin{aligned}
A P_{1}^{T} & =\left[\begin{array}{l|l}
{\left[M_{1} \mid 0\right]+Q_{1}} & \\
\hline & I_{m_{2}}
\end{array}\right]\left[\begin{array}{cc}
V_{11} & V_{12} \\
0 & 0 \\
\hline T_{21} & T_{22}
\end{array}\right] \\
& =\left[\begin{array}{ll|l}
{\left[M_{1} \mid 0\right]+Q_{1}} & \\
\hline & I_{m_{2}}
\end{array}\right]\left[\begin{array}{cc}
I_{r_{1}} & \\
\hline I_{m_{1}-r_{1}} & \\
\hline M_{21} & I_{m_{2}}
\end{array}\right]\left[\begin{array}{cc}
V_{11} & V_{12} \\
0 & 0 \\
\hline 0 & B_{2}
\end{array}\right]
\end{aligned}
$$

where $M_{21}=T_{21} V_{11}^{-1}$ and $B_{2}=T_{22}-M_{21} V_{12}$.

## A.2.1 Case where $r_{1}=n$

In this case $r=r_{1}=n$ and thus

$$
\left.\begin{array}{rl}
A & =\left[\begin{array}{l|l}
{\left[M_{1} \mid 0\right]+Q_{1}} & \\
\hline & I_{m_{2}}
\end{array}\right]\left[\begin{array}{ll}
I_{n} & \\
& I_{m_{1}-n}
\end{array}\right. \\
\hline M_{21} & I_{m_{2}}
\end{array}\right]\left[\begin{array}{c}
V_{11} \\
0 \\
0
\end{array}\right] P_{1} .
$$

In addition the first $r$ columns of $Q$ are the first $r_{1}$ columns of $\left[\frac{Q_{1}}{0}\right]$, that is, by induction, $\left[e_{i_{1}^{\prime}}^{\prime}, \ldots, e_{i_{r_{1}}^{\prime}}\right]$ where $\left(i_{j}^{\prime}\right)$ is the row rank profile of $A_{1}$. Since $r_{1}=n,\left(i_{j}^{\prime}\right)$ is also the row rank profile $\left(i_{j}\right)$ of $A$ and thus the first $r$ columns of $Q$ are $\left[e_{i_{1}}, \ldots, e_{i_{r}}\right]$ as wanted. Also, since by induction $M_{1}$ has the correct echelon shape, the same holds for $M$.

## A.2. 2 Case where $0<r_{1}<n$

Since $B_{2}=\left(\left[M_{2} \mid 0\right]+Q_{2}\right)\left[\frac{V_{2}}{0}\right] P_{2}$ we have

$$
A P_{1}^{T}=\left(\left[\begin{array}{cc|c}
M_{1} & 0 & \\
\hline M_{21} & 0 & M_{2}
\end{array}\right]+\left[\begin{array}{l|l}
Q_{1} & \\
\hline & Q_{2}
\end{array}\right]\right)\left[\begin{array}{cc}
V_{11} & V_{12} P_{2}^{T} \\
0 & 0 \\
\hline & V_{2} \\
& 0
\end{array}\right]\left[\begin{array}{lll}
I_{r_{1}} & \\
\hline & P_{2}
\end{array}\right]
$$

Hence

$$
\begin{aligned}
& A=\left(\left[\begin{array}{l|l|l|l}
M_{1} & 0 & & \\
\hline M_{21} & 0 & M_{2} & 0
\end{array}\right]+\left[\begin{array}{l|l|l|l}
Q_{11} & Q_{12} & & \\
\hline & & Q_{21} & Q_{22}
\end{array}\right]\right)\left[\begin{array}{l|l|l|l}
I_{r_{1}} & & & \\
\hline & & I_{m_{1}-r_{1}} & \\
\hline & I_{r_{2}} & & \\
\hline & & & I_{m_{2}-r_{2}}
\end{array}\right] \\
& \times \underbrace{\left[\begin{array}{cc}
V_{11} & V_{12} P_{2}^{T} \\
& V_{2} \\
\hline 0 & 0 \\
0
\end{array}\right]}_{=:\left[\begin{array}{l}
V \\
0
\end{array}\right]} \underbrace{\left[\begin{array}{c|c}
I_{r_{1}} & \\
\hline & P_{2}
\end{array}\right] P_{1}}_{=: P} . \\
& =(\underbrace{\left[\begin{array}{cc|c}
M_{1} & 0 & 0 \\
M_{21} & M_{2} & 0
\end{array}\right]}_{=:[M \mid 0]}+\underbrace{\left[\begin{array}{l|l|l|l}
Q_{11} & & Q_{12} & \\
\hline & Q_{21} & & Q_{22}
\end{array}\right]}_{=: Q})\left[\begin{array}{l}
V \\
\hline 0
\end{array}\right] P .
\end{aligned}
$$

Now, $r=r_{1}+r_{2}$ and the first $r$ columns of $Q$ are $\left[\begin{array}{l|l}Q_{11} & \\ \hline & Q_{21}\end{array}\right]$, that is, by induction,

$$
\left[e_{i_{1}^{\prime}}, \ldots, e_{i_{r_{1}}^{\prime}} \mid e_{i_{1}^{\prime \prime}+m_{1}}, \ldots, e_{i_{r_{2}}^{\prime \prime}+m_{1}}\right]
$$

where $\left(i_{j}^{\prime}\right)$ is the row rank profile of $A_{1}$ and $\left(i_{j}^{\prime \prime}\right)$ is the row rank profile of $B_{2}$. Since the row rank profile $\left(i_{j}\right)$ of $A$ satisfies $i_{j}=i_{j}^{\prime}$ for $1 \leq j \leq r_{1}$ and $i_{j}=i_{j}^{\prime \prime}+m_{1}$ for $r_{1}<j \leq r$, we conclude that he first $r$ columns of $Q$ are $\left[e_{i_{1}}, \ldots, e_{i_{r}}\right]$ as wanted. Also, $M=\left[\begin{array}{cc}M_{1} & \\ M_{21} & M_{2}\end{array}\right]$ has the desired shape, because that is true, by induction, for both $M_{1}$ and $M_{2}$ and because of the above relationship between $\left(i_{j}\right),\left(i_{j}^{\prime}\right)$ and $\left(i_{j}^{\prime \prime}\right)$.

