Algorithms for Similarity Transforms*

Arne Storjohann
Institute of Scientific Computing
ETH Zurich, Switzerland
storjoha@inf.ethz.ch

Gilles Villard
CNRS
LMC-IMAG Grenoble, France
Gilles.Villard@imag.fr

Extended Abstract

1 Introduction

Let F be a field. Corresponding to any matrix $A \in \mathsf{F}^{n\times n}$ there exists an invertible U over F such that

$$U^{-1}AU = F = \begin{bmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \ddots & \\ & & & C_{f_l} \end{bmatrix} \in \mathsf{F}^{n\times n}.$$

F is the Frobenius canonical form of A, also called the rational canonical form. Each block C_{f_i} is the companion matrix of a monic $f_i \in F[x]$ and $f_i|f_{i+1}$ for $1 \le i \le l-1$. We give an $O(n^3)$ field operations algorithm that takes as input any $A \in \mathsf{F}^{n\times n}$ and recovers a similarity transform matrix U such that $U^{-1}AU = F$. This complexity bound improves by a factor of $O(n)$ on previous deterministic algorithms [1, 6, 7, 8].

The algorithm has two main stages. The first stage computes a transforming matrix $U \in \mathsf{F}^{n\times n}$ such that $U^{-1}AU = Z$ with Z in Zigzag form. The Zigzag form has an almost block diagonal shape and fewer than $2n$ nonzero entries. The cost of computing U and Z from A is $O(n^3)$ field operations using a modification of Gaussian elimination [10, 11]. We don't describe stage one further in this paper.

The second stage computes a transforming matrix $V \in \mathsf{F}^{n\times n}$ such that $V^{-1}ZV = F$ with F in Frobenius form. Then $(UV)^{-1}A(UV) = F$ so UV is a Frobenius transform matrix for A. The cost of computing V and F from Z is $O(n^2(\log n)^2)$ field operations. To achieve this complexity result matrix

*A version of this abstract was presented at the Rhine Workshop on Computer Algebra, Bregenz, Austria, 2000. This version incorporates some corrections. Arne Storjohann, U. Waterloo, May 2005.

multiplication must be avoided. Instead, we work over $\mathsf{F}[x]$ with the associated shifted-Popov form [3] and corresponding polycyclic basis vectors; this is explained in the next two sections.

2 Notation and Preliminaries

A block is a submatrix comprised of a contiguous sequence of rows and columns.

For $g = g_0 + g_1 x + \cdots + g_{d-1}x^{d-1} + x^d \in \mathsf{F}[x]$, let $C_g \in \mathsf{F}^{d\times d}$ denote the companion matrix of g. Recall that C_g has the shape

$$C_g = \begin{bmatrix} 0 & \cdots & 0 & -g_0 \\ 1 & \ddots & \vdots & \vdots \\ & \ddots & 0 & -g_{d-2} \\ & & 1 & -g_{d-1} \end{bmatrix} \in \mathsf{F}^{d\times d}. \tag{1}$$

When using C_g as a block label, we allow the special case $g = 1$ in which case C_g has zero rows and columns.

Let $b = b_0 + b_1 x + \cdots + b_d x^d \in \mathsf{F}[x]$. We use the label B_b to denote a block which has the shape

$$B_b = \begin{bmatrix} & b0 \\ & b1 \\ & \vdots \\ & b_d \\ & 0 \\ & \vdots \\ & 0 \end{bmatrix}.$$

More precisely, all entries zero except for entries in the last column row i equal to b_{i-1} for $1 \le i \le d+1$. The dimensions of a block labeled B_b will be conformal with adjacent blocks. Note that B_b may have zero columns and should have at least $1 + \deg b$ rows if $b \neq 0$.

Lemma 1. *Let $A \in \mathsf{F}^{n\times n}$ and $U \in \mathsf{F}^{n\times n}$ be nonsingular. Then*

$$U^{-1}AU = \begin{bmatrix} C_{c_1} & B_{b_{12}} & \cdots & B_{b_{1k}} \\ B_{b_{21}} & C_{c_2} & & B_{b_{2k}} \\ \vdots & & \ddots & \vdots \\ B_{b_{k1}} & B_{b_{k2}} & \cdots & C_{c_k} \end{bmatrix} \tag{2}$$

if and only if

$$U = [u_1|Au_1|\cdots|A^{d_1-1}u_1|\cdots|u_k|Au_k|\cdots|A^{d_k-1}u_k] \tag{3}$$

with $d_i = \deg c_i$ and $u_i \in \mathsf{F}^{n\times 1}$ for $1 \le i \le k$.

The list of vectors $[u_1, u_2, \ldots, u_k]$ is called a polycyclic basis for the matrix shown in (2). We associate the matrix shown in (2) to

$$M = \phi_x(U^{-1}AU) = \begin{bmatrix} c_1 & b_{12} & \cdots & b_{1k} \\ b_{21} & c_2 & & b_{2k} \\ \vdots & & \ddots & \vdots \\ b_{k1} & b_{k2} & \cdots & c_k \end{bmatrix} \in \mathsf{F}[x]^{k\times k}, \tag{4}$$

which is in *shifted-Popov form*: off-diagonal entries in each row have degree less than the monic diagonal entry.

We will start with a U such that the matrix shown in (2) has a particular structure: in Section 4 diagonal (6); in Section 5 Vee form (7); in Section 6 Zigzag form (8) [10].

In each case the goal is to transform (2) in place to get the right hand side in Frobenius form. The next section shows how we can accomplish this by transforming the associated shifted-Popov form over $\mathsf{F}[x]$, updating the polycyclic vectors $[u_1, u_2, \ldots, u_k]$ via matrix-vector multiplications involving A. At the end, an explicit transformation U is recovered using (3).

3 Module Isomorphism: Examples

We recall the material used in [12, §4] and give two examples. We are starting with matrices U, A and S such that

$$\overset{U^{-1}}{\begin{bmatrix} 3 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -2 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \overset{A}{\begin{bmatrix} -30 & 1 & 15 & -17 \\ 31 & 0 & -15 & 17 \\ -74 & 3 & 37 & -41 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \overset{U}{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 2 & 0 & 3 & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix}} = \overset{S}{\left[\begin{array}{ccc|c} 0 & 0 & 8 & -2 \\ 1 & 0 & -14 & 3 \\ 0 & 1 & 7 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]}.$$

To a nonsingular matrix M in $\in \mathsf{F}[x]^{k\times k}$ in shifted-Popov form (4) with diagonal entries of degrees d_i greater than one, we associate the matrix $S = \psi_c(M)$ in shifted-Popov form in $\mathsf{F}^{n\times n}$. We will also use that $M = \phi_x(S)$:

$$M = \left[\begin{array}{c|c} x^3 - 7\,x^2 + 14\,x - 8 & x^2 - 3\,x + 2 \\ \hline 0 & x - 1 \end{array}\right] \quad \begin{array}{c} \psi_c \\ \rightarrow \\ \leftarrow \\ \phi_x \end{array} \quad S = \left[\begin{array}{ccc|c} 0 & 0 & 8 & -2 \\ 1 & 0 & -14 & 3 \\ 0 & 1 & 7 & -1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right]$$

Let $[u_1, u_2, \ldots, u_k]$ be a polycyclic basis for S with respect to A, so that $S = U^{-1}AU$ with U as in (3).

$$u_1 = [\,1 \;\; 0 \;\; 2 \;\; 0\,], \quad u_2 = [\,1 \;\; 0 \;\; 3 \;\; 1\,],$$

Let $M' = PMQ$ be equivalent to M, also in shifted-Popov form, with degrees of diagonal entries δ_i. Then we know that $S' = \psi_c(M') = V^{-1}AV$ is given by

$$V = p_M \circ P^{-1} \circ p_{M'}^{-1}$$

where p_M and $p_{M'}$ are the coordinate functions with respect to the bases

$$\overline{(1,0)}, \overline{(x,0)}, \overline{(x^2,0)}, \overline{(1,0)} \quad \text{and} \quad \overline{(1,0)}, \overline{(x,0)}, \ldots, \overline{(x^{\delta_1-1},0)}, \ldots, \overline{(0,x^{\delta_2-1})}.$$

In other words, the polycyclic vectors $v_1, \ldots, v_k$ for S' may be computed by:

$$v_i = P^{-1}_{1,i}(A)u_1 + P^{-1}_{2,i}(A)u_2 + \ldots + P^{-1}_{k,i}(A)u_k. \tag{5}$$

On the example, let us transform M to get:

$$M'(x) = \begin{bmatrix} x-1 & 0 \\ 0 & x^3 - 7\,x^2 + 14\,x - 8 \end{bmatrix} = P(x)M(x)Q(x),$$

$$P^{-1}(x) = \begin{bmatrix} -\frac{3}{7}\,x + \frac{10}{21} + \frac{2}{21}\,x^2 & -x-1 \\ \frac{11}{21} - \frac{2}{21}\,x & 1 \end{bmatrix}.$$

This gives:

$$v_1 = P^{-1}_{1,1}(A)u_1 + P^{-1}_{2,1}(A)u_2 = [\tfrac{9}{7}, -\tfrac{5}{7}, \tfrac{67}{21}, \tfrac{3}{7}]^t,$$

$$v_2 = P^{-1}_{1,2}(A)u_1 + P^{-1}_{2,2}(A)u_2 = [0,-1,1,1]^t$$

and using the transformation $V = [v_1,\ v_2,\ Av_2,\ A^2v_2]$,

$$S' = V^{-1}AV = \psi_c(M') = \left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 8 \\ 0 & 1 & 0 & -14 \\ 0 & 0 & 1 & 7 \end{array}\right].$$

Given $P^{-1}(x)$, the cost of computing the new polycyclic basis vectors depends on the cost of a single matrix-vector product involving A, plus the number of matrix-vector products required. For example, if A is sparse, with only $O(n)$ nonzero entries, then a matrix-vector product costs only $O(n)$ field operations. The number of matrix-vector products depends of the degrees of entries in $P^{-1}(x)$.

Notice that if the number of nontrivial diagonal entries in M' is $k' < k$, then some of the v_i are zero and in fact do not have to be considered for A'. For instance, let $U = I$, M and $S = A = \psi_c(M)$ with $k = 4$ be:

$$\left[\begin{array}{c|c|c|c} x-1 & 0 & 1 & 2 \\ \hline 0 & x^2 - 3\,x + 2 & x-1 & x+3 \\ \hline 0 & 0 & x-1 & 4 \\ \hline 0 & 0 & 0 & x^2-5 \end{array}\right] \quad \begin{array}{c} \psi_c \\ \rightarrow \\ \leftarrow \\ \phi_x \end{array} \quad \left[\begin{array}{c|cc|c|cc} 1 & 0 & 0 & -1 & 0 & -2 \\ \hline 0 & 0 & -2 & 1 & 0 & -3 \\ 0 & 1 & 3 & -1 & 0 & -1 \\ \hline 0 & 0 & 0 & 1 & 0 & -4 \\ \hline 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

and transform M to obtain:

$$M'(x) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & x-1 & 0 & 4 \\ 0 & 0 & -4\,x^2 + x^3 + 5\,x - 2 & x^2 - 8\,x + 11 \\ 0 & 0 & 0 & x^2 - 5 \end{bmatrix} = P(x)M(x)Q(x),$$

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

Using $u_1 = e_1, u_2 = e_2, u_3 = e_4$ and $u_4 = e_5$ and noticing that $k' = 3 < 4 = k$, the new polycyclic vectors are:

$$\begin{aligned} &(v_1 = u_1 + (A-1)u_2 + (A-1)u_3 = 0)\,, \\ &v_2 = u_2 + (A-1)u_3 = [-1, 2, -1, 0, 0, 0]^t, \\ &v_3 = u_3 = [0,0,0,1,0,0]^t, \quad v_4 = u_4 = [0,0,0,0,1,0]^t. \end{aligned}$$

They lead to the transformation $U = [v_2,\ v_3,\ Av_3,\ A^2v_3,\ v_4,\ Av_4]$ and to

$$A' = U^{-1}AU = \psi_c(M') = \left[\begin{array}{c|ccc|cc} 1 & 0 & 0 & 0 & 0 & -4 \\ \hline 0 & 0 & 0 & 2 & 0 & -11 \\ 0 & 1 & 0 & -5 & 0 & 8 \\ 0 & 0 & 1 & 4 & 0 & -1 \\ \hline 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right].$$

4 From Diagonal Form

We start with shifted-Popov form that has the shape

$$D = \left[\begin{array}{c|cccc|c} * & & & & & \\ \hline b_* & a_1 & & & & b_* \\ b_* & & a_2 & & & b_* \\ \vdots & & & \ddots & & \vdots \\ b_* & & & & a_k & b_* \\ \hline & & & & & * \end{array}\right] \tag{6}$$

Let $[u_1, u_2, \ldots, u_k]$ be the n-dimensional polycyclic basis vectors with respect to $A \in \mathsf{F}^{n\times n}$ corresponding to the center block. We will modify only these vectors. Recall that a diagonal shifted-Popov form is in Smith form if each diagonal entry (except the last) divides the next.

Lemma 2. *New polycyclic vectors* $[v_1, v_2, \ldots, v_l]$ *can be computed from the initial* $[u_1, u_2, \ldots, u_k]$ *such that the corresponding shifted-Popov form has center block in Smith form. If a matrix-vector product involving* A *costs* $O(n)$ *field operations, then the cost of the transformation is* $O(nm \log m)$ *field operations where* $m = \deg a_1 + \deg a_2 + \cdots + \deg a_k$.

Proof. (Sketch) The blocks corresponding to $\{a_1, a_2, \ldots, a_k\}$ are split into smaller blocks with relatively prime characteristic polynomials. The splitting is accomplished using factor refinement [2] over $\mathsf{F}[x]$. The "splitting" of the corresponding cyclic vectors is accomplished using a binary tree paradigm. The depth of the tree is $O(\log m)$ and $O(m)$ matrix-vector products involving A are required at each level.

These smaller blocks are combined to get the Smith form. Combining the cyclic vectors requires $O(m)$ vector additions. □

We remark that factor refinement is used in a similar context in [5]. A complete factorization is used to recover the primary rational form in [4].

5 From Vee Form

We start with a shifted-Popov form that has the shape

$$V = \left[\begin{array}{c|ccccc|c} * & & & & & & \\ \hline b_* & a_1 & & & & b_1 & b_* \\ b_* & & a_2 & & & b_2 & b_* \\ \vdots & & & \ddots & & \vdots & \vdots \\ b_* & & & & a_{k-1} & b_{k-1} & b_* \\ b_* & & & & & a_k & b_* \\ \hline & & & & & & * \end{array}\right] \tag{7}$$

with $\mathrm{diag}(a_1, a_2, \ldots, a_{k-1})$ in Smith form. Let $[u_1, u_2, \ldots, u_k]$ be the n-dimensional polycyclic basis vectors with respect to $A \in \mathsf{F}^{n \times n}$ corresponding to the center block. We will modify only these vectors.

Lemma 3. *New polycyclic vectors* $[v_1, v_2, \ldots, v_l]$ *can be computed from the initial* $[u_1, u_2, \ldots, u_k]$ *such that the corresponding shifted-Popov form has center block in Smith form. If a matrix-vector product involving* A *costs* $O(n)$ *field operations, the cost of the transformation is* $O(nm)$ *field operations, where* $m = \deg a_1 + \deg a_2 + \cdots + \deg a_k$.

Proof. (Sketch) The center block of V has exactly the shape required to apply [9, Theorem 6]. The algorithm generalizes the proof of this latter theorem to include the computation of the new polycyclic vectors. These vectors actually satisfies a recurrence relation which allows to compute them, together with the Smith form of the center block, in time $O(nm)$. □

6 From Zigzag Form

We start with a shifted-Popov form that has the shape

$$Z = \left[\begin{array}{c|ccccccc|c} * & & & & & & & & \\ \hline b_* & c_1 & b_1 & & & & & & \\ & & c_2 & & & & & & \\ & & b_2 & c_3 & b_3 & & & & \\ & & & & c_4 & & & & \\ & & & & & \ddots & & & \\ & & & & & & c_{k-1} & & \\ & & & & & & b_{k-1} & c_k & b_* \\ \hline & & & & & & & & * \end{array}\right] \tag{8}$$

with each b_i in the center block either 0 or 1. The center block of Z is in Zigzag form [10]. Let $[u_1, u_2, \ldots, u_k]$ be the n-dimensional polycyclic basis vectors with respect to $A \in \mathsf{F}^{n\times n}$ corresponding to the center block. We will modify only these vectors

Lemma 4. *New polycyclic vectors $[v_1, v_2, \ldots, v_l]$ can be computed from the initial $[u_1, u_2, \ldots, u_k]$ such that the corresponding shifted-Popov form has center block in in Smith form. If a matrix-vector product involving A costs $O(n)$ field operations, the cost of the transformation is $O(nm(\log m)^2)$ field operations, where $m = \deg c_1 + \deg c_2 + \cdots + \deg c_k$.*

Proof. Note that k is odd. If $k = 1$ there is nothing to do. For $k \geq 3$ we apply a divide and conquer algorithm derived from [11]; we describe this now.

The input matrix can be partitioned in at least one of the following ways:

$$\left[\begin{array}{c|cccc|c|cccc|c}
* &&&&&&&&&& \\ \hline
b_* & c_* & b_* &&&&&&&& \\
&& c_* &&&&&&&& \\
&&& \ddots &&&&&&& \\
&&&& c_* & b_* &&&&& \\ \hline
&&&&& c_* &&&&& \\ \hline
&&&&& b_* & c_* & b_* &&& \\
&&&&&&& c_* &&& \\
&&&&&&&& \ddots && \\
&&&&&&&&& c_* & b_* \\ \hline
&&&&&&&&&& *
\end{array}\right] \quad \text{or} \quad \left[\begin{array}{c|cccc|ccc|cccc|c}
* &&&&&&&&&&&& \\ \hline
b_* & c_* & b_* &&&&&&&&&& \\
&& c_* &&&&&&&&&& \\
&&& \ddots &&&&&&&&& \\
&&&& c_* & b_* &&&&&&& \\ \hline
&&&&& c_* &&&&&&& \\
&&&&& b_* & c_* & b_* &&&&& \\
&&&&&&& c_* &&&&& \\ \hline
&&&&&&& b_* & c_* & b_* &&& \\
&&&&&&&&& c_* &&& \\
&&&&&&&&&& \ddots && \\
&&&&&&&&&&& c_* & b_* \\ \hline
&&&&&&&&&&&& *
\end{array}\right]$$

such that each of the second and fourth diagonal blocks satisfies at least one of the following conditions: the dimension of the block is one; the sum of degrees of diagonal entries is $\leq m/2$.

Divide and Conquer At a cost of (at most) two recursive calls to problems of half the size (in the parameter m) transform the second and fourth block to Smith form. The shifted-Popov form now has the shape

$$
\left[\begin{array}{c|cccc|c|cccc|c}
* & & & & & & & & & & \\
\hline
b_* & c_* & & & & b_* & & & & & \\
b_* & & c_* & & & b_* & & & & & \\
 & & & \ddots & & \vdots & & & & & \\
b_* & & & & c_* & b_* & & & & & \\
\hline
 & & & & & c_* & & & & & \\
\hline
 & & & & & b_* & c_* & & & & b_* \\
 & & & & & b_* & & c_* & & & b_* \\
 & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & *
\end{array}\right]
\quad \text{or} \quad
\left[\begin{array}{c|cccc|ccc|cccc|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & b_* & & & & & & & \\
b_* & & c_* & & & b_* & & & & & & & \\
\vdots & & & \ddots & & \vdots & & & & & & & \\
b_* & & & & c_* & b_* & & & & & & & \\
\hline
 & & & & & c_* & & & & & & & \\
 & & & & & b_* & c_* & b_* & & & & & \\
 & & & & & & & c_* & & & & & \\
\hline
 & & & & & & & b_* & c_* & & & & b_* \\
 & & & & & & & b_* & & c_* & & & b_* \\
 & & & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & & & *
\end{array}\right]
$$

depending on how the input matrix was partitioned.

Merge Assume for now that the matrix was partitioned with center block dimension three. Permute the first two diagonal entries in the center by switching two rows and columns (update the polycyclic basis accordingly by switching two vectors) to get

$$
\left[\begin{array}{c|cccc|ccc|cccc|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & b_* & & & & & & \\
b_* & & c_* & & & & b_* & & & & & & \\
\vdots & & & \ddots & & & \vdots & & & & & & \\
b_* & & & & c_* & & b_* & & & & & & \\
\hline
 & & & & & c_* & b_* & b_* & & & & & \\
 & & & & & & c_* & & & & & & \\
 & & & & & & & c_* & & & & & \\
\hline
 & & & & & & & b_* & c_* & & & & b_* \\
 & & & & & & & b_* & & c_* & & & b_* \\
 & & & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].
$$

Increase by one the index of the second horizontal and vertical partitioning lines:

$$
\left[\begin{array}{c|ccccc|cc|cccc|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & b_* & & & & & & \\
b_* & & c_* & & & & b_* & & & & & & \\
\vdots & & & \ddots & & & \vdots & & & & & & \\
b_* & & & & c_* & & b_* & & & & & & \\
 & & & & & c_* & b_* & b_* & & & & & \\
\hline
 & & & & & & c_* & & & & & & \\
 & & & & & & & c_* & & & & & \\
\hline
 & & & & & & & b_* & c_* & & & & b_* \\
 & & & & & & & b_* & & c_* & & & b_* \\
 & & & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].
$$

The second diagonal block is in Smith form except for the last entry; apply Lemma 3 to transform the block to Smith form. The fact that there are two columns to the right of the second diagonal block is no essential difficulty: the new entries in each of these columns can be computed separately. Increase by one the index of the second horizontal and vertical partitioning line:

$$
\left[\begin{array}{c|cccccc|c|cccc|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & b_* & b_* & & & & & \\
b_* & & c_* & & & & b_* & b_* & & & & & \\
\vdots & & & \ddots & & & \vdots & \vdots & & & & & \\
b_* & & & & c_* & & b_* & b_* & & & & & \\
b_* & & & & & c_* & b_* & b_* & & & & & \\
 & & & & & & c_* & b_* & & & & & \\
\hline
 & & & & & & & c_* & & & & & \\
\hline
 & & & & & & & b_* & c_* & & & & b_* \\
 & & & & & & & b_* & & c_* & & & b_* \\
 & & & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].
$$

Apply Lemma 2 to transform the second diagonal block to Smith form:

$$
\left[\begin{array}{c|cccccc|c|cccc|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & & b_* & & & & & \\
b_* & & c_* & & & & & b_* & & & & & \\
\vdots & & & \ddots & & & & \vdots & & & & & \\
b_* & & & & c_* & & & b_* & & & & & \\
b_* & & & & & c_* & & b_* & & & & & \\
b_* & & & & & & c_* & b_* & & & & & \\
\hline
 & & & & & & & c_* & & & & & \\
\hline
 & & & & & & & b_* & c_* & & & & b_* \\
 & & & & & & & b_* & & c_* & & & b_* \\
 & & & & & & & \vdots & & & \ddots & & \vdots \\
 & & & & & & & b_* & & & & c_* & b_* \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].
$$

If the initial partitioning of the input matrix had center block with dimension one, then the steps up until now did now need to be performed.

Permute the third and fourth diagonal blocks (update the polycyclic basis accordingly by permuting the vectors) so that

$$\left[\begin{array}{c|cccccc|cccc|c|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & & & & & & b_* & \\
b_* & & c_* & & & & & & & & & b_* & \\
\vdots & & & \ddots & & & & & & & & \vdots & \\
b_* & & & & c_* & & & & & & & b_* & \\
b_* & & & & & c_* & & & & & & b_* & \\
b_* & & & & & & c_* & & & & & b_* & \\
\hline
 & & & & & & & c_* & & & & b_* & b_* \\
 & & & & & & & & c_* & & & b_* & b_* \\
 & & & & & & & & & \ddots & & \vdots & \vdots \\
 & & & & & & & & & & c_* & b_* & b_* \\
\hline
 & & & & & & & & & & & c_* & \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].$$

Extract the second vertical and horizontal partitioning lines:

$$\left[\begin{array}{c|cccccccccc|c|c}
* & & & & & & & & & & & & \\
\hline
b_* & c_* & & & & & & & & & & b_* & \\
b_* & & c_* & & & & & & & & & b_* & \\
\vdots & & & \ddots & & & & & & & & \vdots & \\
b_* & & & & c_* & & & & & & & b_* & \\
b_* & & & & & c_* & & & & & & b_* & \\
b_* & & & & & & c_* & & & & & b_* & \\
 & & & & & & & c_* & & & & b_* & b_* \\
 & & & & & & & & c_* & & & b_* & b_* \\
 & & & & & & & & & \ddots & & \vdots & \vdots \\
 & & & & & & & & & & c_* & b_* & b_* \\
\hline
 & & & & & & & & & & & c_* & \\
\hline
 & & & & & & & & & & & & *
\end{array}\right].$$

Transform the second diagonal block of to Smith form using Lemma 2. As before, the fact that there are two columns to the right of the second diagonal block is no essential difficulty. Finally, extract the second vertical and horizontal partitioning lines and apply Lemma 3 to complete the transformation of the shifted-Popov form and polycyclic basis.

We have shown how to solve a problem of size (n, m) by solving (at most) two problems of size $(n, \lfloor m/2 \rfloor)$ and merging at cost $O(nm \log m)$ field operations. The claimed complexity result follows. $\square$

References

[1] D. Augot and P. Camion. Frobenius form and cyclic vectors. *C.-R.-Acad.-Sci.-Paris-Ser.-I-Math.*, 318(2):183–188, 1994.

[2] E. Bach and J. Shallit. *Algorithmic Number Theory*, volume 1 : Efficient Algorithms. MIT Press, 1996.

[3] B. Beckermann, G. Labahn, and G. Villard. Shifted normal forms of polynomial matrices. In S. Dooley, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '99*, pages 189—196. ACM Press, New York, 1999.

[4] M. Giesbrecht. *Nearly Optimal Algorithms for Canonical Matrix Forms.* PhD thesis, University of Toronto, 1993.

[5] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and its Applications*, 136:189–208, 1990.

[6] H. Lüneburg. *On Rational Normal Form of Endomorphisms: a Primer to Constructive Algebra*. Wissenschaftsverlag, Mannheim, 1987.

[7] P. Ozello. *Calcul Exact Des Formes De Jordan et de Frobenius d'une Matrice*. PhD thesis, Université Scientifique Technologique et Medicale de Grenoble, 1987.

[8] A. Steel. A new algorithm for the computation of canonical forms of matrices over fields. *Journal of Symbolic Computation*, 24:409—432, 1997.

[9] A. Storjohann. Computing Hermite and Smith normal forms of triangular integer matrices. *Linear Algebra and its Applications*, 282:25–45, 1998.

[10] A. Storjohann. An $O(n^3)$ algorithm for Frobenius normal form. In O. Gloor, editor, *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '98*, pages 101–104. ACM Press, New York, 1998.

[11] A. Storjohann. *Algorithms for Matrix Canonical Forms.* PhD thesis, Swiss Federal Institute of Technology, ETH–Zurich, 2000.

[12] G. Villard. Fast parallel algorithms for matrix reduction to normal forms. *Applicable Algebra in Engineering, Communication and Control*, 8:511—537, 1997.