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 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].

We begin with a $U \in \mathsf{F}^{n\times n}$ such that $U^{-1}AU = Z$ is in Zigzag form; a matrix with an almost block diagonal shape and fewer than $2n$ nonzero entries. The initial U and Z can be recovered in $O(n^3)$ field operations [11]. We then apply a sequence of tranformations inplace until we achieve $U^{-1}AU = F$ with F in Frobenius form. The transformation from Zigzag to Frobenius form is accomplished in $O(n^2 \log n)$ field opeartions.

To achieve this complexity result we need to avoid matrix multiplication. 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.

*31.10.99

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

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

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 all entries zero except for entries in the last column row i equal to b_i for $1 \le i \le d$. 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 $b \ne 0$.

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 $u_i \in \mathsf{F}^{n\times n}$ for $1 \le i \le n$.

The list of vectors $[u_1, u_2, \ldots, u_k]$ is called a polycyclic basis for 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*: offdiagonal 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 block diagonal (6); in Section 5 Vee form (7); in Section 6 Zigzag form (8) [11].

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 working only with the associated shifted-Popov form over $\mathsf{F}[x]$ and corresponding polycyclic vectors $[u_1, u_2, \ldots, u_k]$. 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. To an invertible 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 $A = \psi_c(M)$ in shifted-Popov form in $\mathsf{F}^{n\times n}$. We will also use that $M = \phi_x(A)$:

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

Let $u_1, \ldots, u_k$ be the polycyclic vectors associated to A such that A is given in the basis $u_1, Au_1, \ldots, A^{d_1-1}u_1, \ldots, u_k, \ldots, A^{d_k-1}u_k$,

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

For $M' = PMQ$ equivalent to M also in shifted-Popov form we know that $A' = \psi_c(M') = U^{-1}AU$ is given by :

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

In other words, the polycyclic vectors $v_1, \ldots, v_k$ for A' 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:

$$v_1 = P^{-1}_{1,1}(A)u_1 + P^{-1}_{2,1}(A)u_2 = [\tfrac{2}{3}, -\tfrac{5}{7}, \tfrac{4}{21}, \tfrac{3}{7}]^t,$$

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

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

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

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 M and $A = \psi_c(M)$ 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:

$$M'(x) = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & x-1 & 0 & 4 \\ 0 & 0 & -4\,x^2+x^3+5\,x-2 & x^2-8\,x+11 \\ 0 & 0 & 0 & x^2-5 \end{array}\right] = P(x)M(x)Q(x),$$

$$P^{-1}(x) = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ x-1 & 1 & 0 & 0 \\ x-1 & x-1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right].$$

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:

$$\begin{array}{l} (v_1 = u_1 + (A-1)u_2 + (A-1)u_3 = 0)\,, \\ v_2 = u_2 + (A-1)u_3 = [-1, 2, -1, 0, 0, 0]^t, \\ v3 = u_3 = [0, 0, 0, 1, 0, 0]^t, \quad v_4 = u_4 = [0, 0, 0, 0, 1, 0]^t. \end{array}$$

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 Block Diagonal Form

We start with shifted-Popov form that has the shape

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

Let $[u_1, u_2, \ldots, u_k]$ be the polycyclic basis vectors corresponding to the center block. We will modify only these vectors.

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 can be written as above but with center block in Smith form. 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 based on factor refinement [2]. Factor refinement is used in a similar context in [5]. In [4] a complete factorization is used to recover the primary rational form,

These smaller blocks are combined in a different order using a binary tree paradigm. The depth of the tree is $O(\log m)$ and $O(m)$ matrix-vector products involving D are required at each level. □

5 From Vee Form

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

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

with $\operatorname{diag}(a_1, a_2, \ldots, a_{k-1})$ in Smith form. Let $[u_1, u_2, \ldots, u_k]$ be the polycyclic basis vectors 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 can be written as above but with the center block in Smith form. 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 [10, 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 normal form of M, in time $O(nm)$. $\square$

6 From Zigzag Form

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

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

with each b_i in the center block either 0 or 1. The center block of Z is in Zigzag form [11]. Let $[u_1, u_2, \ldots, u_k]$ be the polycyclic basis vectors 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 can be written as above but with the center block in Smith form. 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) If $k = 1$ there is nothing to do. If $k = 2$ apply the algorithm of Lemma 3. For $k > 2$ we apply a divide and conquer algorithm from [9]; we describe this now.

Partition the matrix as

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

such that the sum of the degrees of the diagonal entries in each of the second and fourth diagonal block is $\leq n/2$. Note both the second and fourth block are in Zigzag form.

Divide and Conquer At a cost of two recursive calls to problems of half the size, transform the second and fourth block to Smith form. The shifted-Popov form now has the shape

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

Merge Either permute (in case $e = 0$) or combining (in case $e = 1$) the first two diagonal entries in the center block to get

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

The transformation on the shifted-Popov form is straightforward. The polycyclic basis is updated easily by either switching two vectors (in case $e = 0$) or extracting the vector corresponding to the second diagonal entries of the (unmodified) center block (in case $e = 1$).

Now use Lemma 2 and 3 to transform the second block to Smith form. Then permute the blocks (reorder the polycyclic basis) so that

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

Finally, apply Lemma 2 and 3 in succesion to the center block to complete the transformation of the shifted-Popov form and polycyclic basis. $\square$

References

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

[2] Eric Bach and Jeffrey 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 *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '99*, pages 189—196, 1999.

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

[5] Erich Kaltofen, M. S. Krishnamoorthy, and B. David 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] Allan Steel. A new algorithm for the computation of canonical forms of matrices over fields. *Journal of Symbolic Computation*, 24:409—432, 1997.

[9] Arne Storjohann. Phd Thesis, to appear.

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

[11] ———., An $O(n^3)$ algorithm for Frobenius normal form. In *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC '98*, 1998.

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