Algorithms Seminar 2000–2001,
F. Chyzak (ed.), INRIA, (2002), pp. 95–98.

Available online at the URL
http://algo.inria.fr/seminars/.

Transformations Exhibiting the Rank for Skew Laurent Polynomial Matrices

Manuel Bronstein
Projet CAFÉ, INRIA (France)

June 11, 2001

Summary by Alin Bostan

Abstract

This talk presents an algorithm to perform transformations exhibiting the rank (TER) on a large class of matrices with entries in skew polynomial rings. This algorithm only uses elementary linear algebra operations and has various applications in solving very general linear functional systems.

1. Motivation

The question of finding polynomial solutions for linear functional systems is of particular interest in treating various problems in differential and difference algebra, as well as in combinatorics. It appears as a basic subtask in algorithms for finding all rational solutions of differential and (q-)difference equations, for computing liouvillian solutions of differential equations and (q-)hypergeometric solutions of (q-)difference equations. It also applies in factoring linear differential and difference operators, or in designing effective Gröbner basis algorithms in multivariate Ore algebras, which in turn are used in generalization of Gosper's algorithm for indefinite hypergeometric summation and Zeilberger's "creative telescoping" algorithm for definite summation and integration.

The traditional computer algebra approach to solving functional systems is via an elimination method like the cyclic-vector method, which converts the system to scalar equations (this procedure is called *uncoupling*). The major problem of this approach is the increase in size of the coefficients of equations.

The algorithm described in the next section offers a direct alternative for transforming a linear system of recurrences into an equivalent one of a *simpler form*, well-suited for the purpose of computing solutions with finite support of such a system. This gives a useful tool for constructing polynomial solutions of very general linear functional systems; see Sections 4.1 and 4.2 below.

The main advantage of this approach is that it does not require preliminary uncoupling of linear systems, but only performs elementary linear algebra operations on the original matrix.

2. Description of the Algorithm

The existence of canonical forms for matrices over various types of rings, such as principal ideal domains, has been known since the middle of the last century; their computation has important applications in both theoretical and practical areas of mathematics, science, and engineering.

Suppose that we consider matrices over a ring for which the notion of *rank* makes sense. A method for obtaining canonical forms of a matrix is performing *elementary operations* on its rows. Here, by elementary operation we mean permuting two rows, adding a multiple of a row to another row, and multiplying a row by a nonzero element of the base ring. Such a finite sequence of elementary row

operations on a matrix A can be represented by a matrix E. It will be called a *TER* (*transformation exhibiting the rank*) if it has the additional property that the rank of A equals the number of nonzero rows of the matrix EA.

In the commutative case, Gaussian elimination is the classical example of a TER, but it is a very greedy one, because of the exponential growth of the intermediate expressions; see [5]. The *Popov form* from linear control theory [8, 9] and the *reduced matrix form* [10, 11] are two other examples.

In [6] Mulders and Storjohann gave a simple algorithm that computes a simplified, non-canonical version of the Popov form, called the *weak Popov form* of a polynomial matrix. The algorithm performs only *delicate* elementary transformations which avoid intermediate expression swell. As a by-product, fast algorithms are obtained for computing the rank, the determinant, the Hermite form, the triangular factorization, and also the Popov form.

In the following, we describe an algorithm that computes a TER in a non-commutative setting.

Let R be an integral domain and σ an automorphism of R. Localizing the skew polynomial ring $R[X;\sigma]$ at the set of powers of X, we obtain the *skew Laurent polynomial ring*

$$S = R[X, X^{-1}; \sigma],$$

with the commutation rules $X \cdot r = \sigma(r) \cdot X$, for all r in R (and therefore $X^{-1} \cdot r = \sigma^{-1}(r) \cdot X^{-1}$). It is a left Ore domain, in the sense that any nonzero elements of S have a nonzero common left multiple in S. This implies that for any S-module M, the rank of M, denoted by $\mathrm{rk}(M)$ is a well-defined notion; see [4]. If A is a matrix with entries in S, we will call the *rank of* A the rank of the S-module generated by the rows of the matrix A.

We detail an algorithm which computes a TER of a $n \times m$ matrix A with entries in the skew Laurent polynomial ring $S = R[X, X^{-1}; \sigma]$. If we write

$$A = A_t X^t + A_{t-1} X^{t-1} + \cdots + A_{s+1} X^{s+1} + A_s X^s,$$

where $s \leq t$ are integers, A_i are matrices with entries in R, the leading matrix A_t and the trailing matrix A_s are nonzero, we are interested in finding a TER E such that the trailing matrix (respectively the leading matrix) of EA be nonsingular.

Remark that a straightforward application of the algorithm given in [6] does not do the job, even in the commutative case. The algorithm hereafter is essentially the algorithm proposed in [2] for the particular case of recurrence polynomials and improves the EG-elimination method [1].

The algorithm consists in iterating the following two basic steps, as long as the first operation can be performed:

1. look for a nonzero $v \in R^n$ in the left kernel of the trailing (respectively leading) matrix of A, i.e., such that $v^T A_s = 0$ [respectively $v^T A_t = 0$] and such that v_i is zero whenever the ith row of A is zero;
2. choose i_0 in the set of indices i such that the maximal degree in X of the polynomials of the ith row of A be maximal [respectively, its valuation be minimal] and replace this row by $X^{-1} v^T A$ [respectively by $X v^T A$].

Remark that $\sum_i \deg({}_iA)$ decreases after each iteration, where ${}_iA$ denotes the ith row of A, so the above algorithm terminates after at most $n(t - s + 1)$ iterations.

Let N denote the number of iterations necessary for the previous algorithm to terminate and $A^{(p)}$ the matrix obtained from $A = A^{(0)}$ after p iterations. Then it can easily be seen that the number r of nonzero rows in the matrix $A^{(N)}$ equals its rank, as any linear nontrivial dependency over S of these nonzero rows would imply a linear nontrivial dependency over R of the corresponding rows of its trailing matrix.

On the other hand, the ranks of the matrices $A^{(p)}$ do not change all along the algorithm. This is implied by the formula $\mathrm{rank}A^{(p)} = \mathrm{rank}A^{(p+1)} + \mathrm{rank}\left(\mathcal{M}^{(p)}/\mathcal{M}^{(p+1)}\right)$, where $\mathcal{M}^{(p)}$ denotes the S-module generated by the rows of the matrix $A^{(p)}$, and by the fact that $\mathcal{M}^{(p)}/\mathcal{M}^{(p+1)}$ is a torsion module, therefore of rank zero.

This shows that the previous algorithm provides a TER for A.

3. Complexity

The previous algorithm only needs to compute nonzero elements of the kernels of matrices with entries in R. When R is a polynomial ring over some field K of characteristic 0, which is the case for differential and (q-)difference equations, one can use modular and probabilistic methods (like [7]) to find elements of the kernel. Their worst-case complexity is $O(n^3d^2)$ operations in K, where d is a bound on the degrees of the entries of A. Since the algorithm loops at most $n(t-s+1)$ times, its complexity is $O\big((t-s)n^4d^2\big)$. Refinements are possible; see [2].

4. Applications

4.1. **Desingularisation of recurrences.** As mentioned in the first section, linear systems of recurrences with variable coefficients are of interest in combinatorics and numeric computation. In addition, as shown in [3], they give a useful tool for constructing solutions of very general linear functional equations.

Consider the system $A_t(n)Y_{n+t} + \cdots + A_{s+1}(n)Y_{n+s+1} + A_s(n)Y_{n+s} = 0$, where A_i are $m \times m$ matrices with entries in the polynomial ring $K[n]$. This system is equivalent to $AY = 0$, where $A = A_tE^t + \cdots + A_sE^s$ is now viewed as a matrix with entries in $K[n][E, E^{-1}; \sigma]$, σ being the shift automorphism of $K[n]$.

If either the leading matrix A_t or the trailing matrix A_s is nonsingular, its determinant is a nonzero polynomial in $K[n]$ and the finite set of its integer roots gives the singularities of the recurrence and the possible degrees of polynomial solutions of the initial system. If the matrices A_s and A_t are singular, one faces the necessity to transform such a recurrence system into an equivalent one, with nonsingular leading (or trailing matrix). The following method is taken from [2]. If $\mathrm{rank}A = m > \mathrm{rank}A_t$, then applying the previous algorithm to the matrix A yields a new matrix

$$A^* = A^*_t E^t + \cdots + A^*_{s'} E^{s'}$$

such that $\mathrm{rank}A^*_t = m$.

4.2. **Solutions with finite support.** As already mentioned, the question of finding polynomial solutions of linear functional systems may be reduced to the problem of finding solutions with finite support $(Y_0, Y_1, \ldots, Y_N, 0, \ldots)$ of the previous recurrence system; see [3]. In [2] a similar method to that of Section 4.1 was given, in order to find constraints on the set of the possible values of the bound N for the support of such a solution.

If $\mathrm{rank}A = m = \mathrm{rank}A_s$ then we can find a finite set of candidates for N, given by the relation $\delta(N-s) = 0$ for $\delta(n) = \det A_s$. If $\mathrm{rank}A = m > \mathrm{rank}A_s$, then applying the previous TER to the matrix A gives a matrix $A^* = A^*_{t'}E^{t'} + \cdots + A^*_sE^s$ where $\mathrm{rank}A^*_s = m$ and $(\det A^*_s)(N-s) = 0$.

4.3. **Hensel lifting for singular linear systems.** Let A be a nonsingular matrix with entries in $K[X]$, where K is a field. We consider the problem of recovering a $v \in K(X)$ such that $Av = b$, or determine that no such v exists.

X-adic lifting works by computing a vector series $w = w_0 + w_1X + w_2X^2 + \cdots$, with each $w_i \in K^n$ and such that

$$A(w_0 + w_1X + w_2X^2 + \cdots) = b.$$

A rational solution v of the system $Av = b$ is then reconstructed from the truncated series solution $w \pmod{X^l}$ using Padé approximation. In general, we can compute the series solution w, by undetermined coefficients method, only when A is nonsingular modulo X.

In the case $A(0)$ is singular, one can manage by applying the previous TER to the extended matrix $[\,A \mid b\,]$ to transform the system $AY = b$ into an equivalent one $A^*Y = b^*$, with $A^*(0)$ nonsingular. A similar idea already appeared in [7].

4.4. **Solving linear differential systems.** We now consider the problem of solving a linear differential system $Y' = B(x)Y$ where B is a $m \times m$ matrix with entries in $K[x]$. By solving such a system we mean finding its formal power solutions. The system may be written in the compressed form $AY = 0$, where A is a matrix with entries in $K[X][D; d/dx]$.

Using the isomorphism of K-algebras:

$$\mathcal{R} : K[x, x^{-1}][D; d/dx] \longrightarrow K[n][E, E^{-1}; \sigma]$$

given by $\mathcal{R}x = E^{-1}$ and $\mathcal{R}D = (n+1)E$, we remark that there is a bijective correspondence between formal power solutions $Y = \sum_{n\geq 0} Y_n x^n$ of the linear differential system $AY = 0$ and sequences $Y = (Y_n)_{n\geq 0}$, solutions of the recurrence system $\mathcal{R}(A)(Y) = 0$. This reduces the problem of finding (polynomial) solutions of the differential system $AY = 0$ to finding solutions (with finite support) of the recurrence system $\mathcal{R}(A)(Y) = 0$.

Bibliography

[1] Abramov (Sergei A.). – EG-eliminations. *Journal of Difference Equations and Applications*, vol. 5, n° 4-5, 1999, pp. 393–433.

[2] Abramov (Sergei A.) and Bronstein (Manuel). – On solutions of linear functional systems. In Mourrain (Bernard) (editor), *ISSAC'01 (July 22-25, 2001. London, Ontario, Canada)*. pp. 1–6. – ACM Press, 2001. Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation.

[3] Abramov (Sergei A.), Bronstein (Manuel), and Petkovšek (Marko). – On polynomial solutions of linear operator equations. In Levelt (A. H. M.) (editor), *Symbolic and Algebraic Computation*. pp. 290–296. – ACM Press, New York, 1995. Proceedings of ISSAC'95, July 1995, Montreal, Canada.

[4] Cohn (P. M.). – *Free rings and their relations*. – Academic Press Inc., London, 1985, second edition, *London Mathematical Society Monograph*, vol. 19, xxii+588p.

[5] Fang (X. G.) and Havas (G.). – On the worst-case complexity of integer Gaussian elimination. In Küchlin (Wolfgang W.) (editor), *ISSAC'97 (July 21-23, 1997. Maui, Hawaii, USA)*. pp. 28–31. – ACM Press, New York, 1997. Conference proceedings.

[6] Mulders (Thom) and Storjohann (Arne). – *On lattice reduction for polynomial matrices*. – Technical Report n° 356, ETH Zürich, Institute of Scientific Computing, December 2000. 26 pages.

[7] Mulders (Thom) and Storjohann (Arne). – Rational solutions of singular linear systems. In Traverso (Carlo) (editor), *ISSAC'00 (August 6-9, 2000. St Andrews, Scotland)*. pp. 242–249. – ACM Press, 2000. Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation.

[8] Popov (V. M.). – Invariant description of linear, time-invariant controllable systems. *SIAM J. Control*, vol. 10, 1972, pp. 252–264.

[9] Villard (G.). – Computing Popov form and Hermite forms of polynomial matrices. In Lakshman (Y. N.) (editor), *ISSAC'96 (July 24-26, 1996. Zurich, Switzerland)*. pp. 250–258. – ACM Press, New York, 1996. Conference proceedings.

[10] von zur Gathen (Joachim). – Hensel and Newton methods in valuation rings. *Mathematics of Computation*, vol. 42, n° 166, 1984, pp. 637–661.

[11] von zur Gathen (Joachim) and Gerhard (Jürgen). – *Modern computer algebra*. – Cambridge University Press, New York, 1999, xiv+753p.