Output-sensitive Modular Algorithms for Polynomial Matrix Normal Forms

Howard Cheng
Dept. of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Canada
cheng@cs.uleth.ca

George Labahn
Symbolic Computation Group
School of Computer Science
University of Waterloo
Waterloo, Canada
glabahn@scg.math.uwaterloo.ca

1 Introduction

We give modular algorithms to compute a row-reduced form and a weak Popov form of a polynomial matrix, improving on existing fraction-free algorithms. In each case we define lucky homomorphisms, determine the appropriate normalization, as well as bound the number of homomorphic images required. The algorithms have the advantage that they are output-sensitive, that is, the number of homomorphic images required depends on the size of the output. Furthermore, there is no need to verify the result by trial division or multiplication. Our algorithms can be used to compute normalized one-sided greatest common divisors and least common multiples of polynomial matrices along with irreducible matrix-fraction descriptions of matrix rational functions.

Let $\mathbb{D}$ be an integral domain and $\mathbf{F}(z) \in \mathbb{D}[z]^{m\times n}$ be polynomial matrix of degree N. We wish to compute polynomial matrices $\mathbf{U}(z)$ and $\mathbf{T}(z)$ such that

$$\mathbf{U}(z) \cdot \mathbf{F}(z) = \mathbf{T}(z) \tag{1}$$

with $\mathbf{U}(z)$ unimodular and $\mathbf{T}(z)$ row-reduced or in weak Popov form. Roughly speaking, we want the leading row coefficient of $\mathbf{T}(z)$ to be of the same rank as $\mathbf{F}(z)$ in the case of row-reduced form, or triangular in the case of weak Popov form [6, 7].

We are interested in the modular computation of row-reduced and weak Popov forms for polynomial matrices, as well as the associated transformation matrix. There are traditionally three major issues that must be addressed: the problem of "unlucky" homomorphisms, the number of images required for the reconstruction of the result, and the normalization of the result to ensure a unique answer. Although these issues are well understood in the case of polynomial GCD computations, they are nontrivial in our case. The problem of computing these normal forms and their transformation matrices can be viewed as one of determining a basis for a particular module. The difficulties in devising a modular algorithm to compute a basis for a module or a vector space is well known. The lack of uniqueness, definitions of lucky homomorphisms, and appropriate normalizations are all far from obvious in any basis computation. We overcome these difficulties by reducing the problem to a linear algebra problem.

2 Summary of Main Results

We study the linear systems solved by the Fast Fraction-free Gaussian (FFFG) elimination algorithm and use them as a basis for our modular algorithms [1]. The definition and detection of unlucky homomorphisms are addressed by examining the "computation paths" taken under the homormophisms, which reveal the singularities of the principal leading minors in the corresponding coefficient matrix. A bound on the size of the coefficients in the output, and hence a bound on the number of homomorphic images required, is obtained by applying Hadamard's bound to the solutions of linear systems.

Our algorithms reconstruct the final results incrementally with each additional homormophic image. By studying the norms of the results, we can prove that the reconstructed results are correct if they have not changed for a sufficient number of steps. This is done without the need to verify the results by trial division or multiplication.

Theorem 1 *Suppose $\mathbb{D} = \mathbb{Z}$ and the primes are ordered such that $p_1 < p_2 < \cdots$, and that*

$$\sum_{i=1}^{m} \sum_{k=0}^{N} \left| F_{i,j}^{(k)} \right| \leq p_1 \cdots p_\tau$$

for all $j = 1, \ldots, m$. Suppose that $\widetilde{\mathbf{U}}(z)$ and $\widetilde{\mathbf{T}}(z)$ are the reconstructed results in the modular algorithm and have not changed for τ additional primes. Then $\widetilde{\mathbf{U}}(z)$ and $\widetilde{\mathbf{T}}(z)$ give a solution to (1).

If $\mathbb{D} = \mathbb{Z}[x]$, then $\widetilde{\mathbf{M}}(z)$ and $\widetilde{\mathbf{R}}(z)$ give a solution to (1) if $\deg_x \mathbf{F}(z)_{i,j} \leq \tau$ for all i, j. □

It should be noted that $\tau = 1$ in many practical cases.

We also present complexity analysis and experimental results showing that the modular algorithm performs better than the fraction-free algorithm by an order of magnitude.

References

[1] B. Beckermann and G. Labahn. Fraction-free computation of matrix rational interpolants and matrix GCDs. *SIAM J. Matrix Anal. and Appl.*, 22(1):114–144, 2000.

[2] B. Beckermann and G. Labahn. On the fraction-free computation of column-reduced matrix polynomials via FFFG. Technical Report ANO436, Laboratoire ANO, University of Lille, 2001. Available at `http://ano.univ-lille1.fr/pub/2001/ano436.ps.Z`.

[3] W. S. Brown. On Euclid's algorithm and the computation of polynomial greatest common divisors. *Journal of the ACM*, 18(4):478–504, October 1971.

[4] S. Cabay. Exact solution of linear equations. In *Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation*, pages 392–398, 1971.

[5] H. Cheng. *Algorithms for Normal Forms for Matrices of Polynomials and Ore Polynomials*. PhD thesis, University of Waterloo, 2003.

[6] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

[7] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *Journal of Symbolic Computation*, 35(4):377–401, 2003.