On the fraction-free computation of column-reduced matrix polynomials via FFFG

Bernhard Beckermann* and George Labahn†

January 9, 2002

Abstract

By generalizing former considerations, we show that we can modify our FFFG algorithm for computing a Matrix GCD into an algorithm which computes a column-reduced Matrix GCD or more generally a column-reduced form of a Matrix polynomial. When the matrix polynomial has coefficients from an integer domain, the result is a new algorithm for determining a column reduced form using only fraction-free arithmetic while at the same time keeping coefficient growth to a minimum. Such domains are typical when working in computer algebra systems. The algorithm has been implemented and is in the new MatrixPolynomialAlgebra package that will be available in the next release of the Maple computer algebra system.

Key words: Column reduction, Matrix polynomials, Fraction-free arithmetic.
Subject Classifications: AMS(MOS): 65D05, 41A21.

In [2] we have given a new algorithm for computing a left-hand GCD of two matrix polynomials $\mathbf{A}(z), \mathbf{B}(z)$ with coefficients over some integer domain $\mathbb{D}$ in a fraction–free manner provided that $\mathbf{G}(z) = [\mathbf{A}(z), \mathbf{B}(z)] \in \mathbb{D}[z]^{m\times n}$ has full rank r. If $\mathbf{G}(z)$ has total degree N then the idea used was to apply the algorithm FFFG to $\mathbf{F}(z) = z^N \cdot \mathbf{G}(1/z)$ and the multi-index $\vec{n} = (N, ..., N)$, producing a sequence of so-called Mahler systems $\mathbf{M}_\sigma(z) \in \mathbb{D}[z]^{n\times n}$ for increasing orders $\sigma = 0, 1, ...$ together with corresponding closest normal points $\vec{\nu}^\sigma$ and residuals $\mathbf{R}_\sigma(z) \in \mathbb{D}[z]^{m\times n}$ satisfying

$$\mathbf{F}(z)\mathbf{M}_{m\sigma}(z) = z^\sigma \mathbf{R}_{m\sigma}(z) \tag{1}$$

*Laboratoire d'Analyse Numérique et d'Optimisation, Université des Sciences et Technologies de Lille, 59655 Villeneuve d'Ascq Cedex, France, e–mail: bbecker@ano.univ-lille1.fr

†Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, N2L3G1. e–mail: glabahn@scg.uwaterloo.ca

and a similar order relation for orders being not a multiple of m. In addition, these Mahler systems are in Popov normal form, that is they satisfied

$$z^{-\vec{\nu}^{\sigma}} \cdot \mathbf{M}_{\sigma}(z) = c \cdot \mathbf{I}_m + \mathcal{O}(z^{-1})_{z\to\infty}, \quad \mathbf{M}_{\sigma}(z) \cdot z^{-\vec{\nu}^{\sigma}} = T + \mathcal{O}(z^{-1})_{z\to\infty} \quad (2)$$

with $c \in \mathbb{D}$ and $T \in \mathbb{D}^{n\times n}$ being upper triangular. Notice that (2) implies that $\mathbf{U}_{\sigma}(z) := \mathbf{M}_{\sigma}(1/z) z^{\vec{\nu}^{\sigma}}$ is unimodular. The cost to reach a Mahler system with multi-index $\vec{\nu}$ via the FFFG algorithm is then $\mathcal{O}(n \cdot ||\vec{\nu}||^4 ||\mathbf{G}(z)||^2)$ bit operations using classical arithmetic, where $||\mathbf{G}(z)||$ bounds the size of the coefficients of $\mathbf{G}(z)$ (cf. [2, Theorem 6.3]). Algorithm FFFG has been introduced in [2] as an fraction-free counterpart of a method presented in [1].

In the application of FFFG described in [2, Section 8], we stopped the iterations at the order $\sigma = \sigma^*$ such that, for the first time, $\mathbf{R}_{\sigma}(z)$ contains $n - r = n - m$ zero columns. In this case, because of the unimodularity of $\mathbf{U}_{\sigma}(z)$, a left GCD is given by the m non-zero columns of $\mathbf{F}(z)\mathbf{U}_{\sigma}(z)$. Finally, for σ^* we established in [2, Theorem 8.1(b)] the upper bounds

$$\begin{aligned} |\vec{\nu}^{\sigma^*}| &\leq \sigma^* \leq \sigma' := m \cdot (N + N^* + 1) \\ &\leq m \cdot (N + N^{\#} + 1) \leq m \cdot ((m+1)N + 1), \end{aligned} \quad (3)$$

where N^* is the largest of the minimal indices of $\mathbf{G}(z)$ and $N^{\#} = \text{MM-deg}\, \mathbf{G}(z)$ the McMillan degree of $\mathbf{G}(z)$.

In the present note we want to show that the FFFG algorithm may also be extended to allow one to compute, in a fraction–free manner, a column-reduced form of a general matrix polynomial $\mathbf{G}(z) \in \mathbb{D}[z]^{m\times n}$ of arbitrary rank r (and thus for instance a column-reduced Matrix GCLD). To our knowledge, such a fraction-free algorithm is new.

Our approach to determine a column reduced form is to alter the stopping criterion. We claim that if $\sigma^{**} = m\sigma$ is the first order index which is divisible by m and which verifies

$$\textit{rank}\, \mathbf{R}_{m\sigma}(0) + \text{ number of zero columns of } \mathbf{R}_{m\sigma}(z) = m$$

then the corresponding reversed counterpart $\mathbf{U}_{m\sigma}(z) := \mathbf{M}_{m\sigma}(1/z) z^{\vec{\nu}^{m\sigma}}$ of the resulting Mahler system is a unimodular multiplier with $\mathbf{G}(z)\mathbf{U}_{m\sigma}(z)$ being column reduced (i.e., containing only $r = \textit{rank}\, \mathbf{G}(z)$ columns different from zero which are column reduced). Indeed, by construction, $\mathbf{U}_{m\sigma}(z)$ is unimodular, and

$$\mathbf{G}(z)\mathbf{U}_{m\sigma}(z) = \mathbf{R}_{m\sigma}(1/z) z^{N-\sigma} z^{\vec{\nu}^{m\sigma}},$$

with the right-hand side being clearly a column-reduced matrix polynomial (with leading coefficient matrix $\mathbf{R}_{m\sigma}(0)$).

It remains to show that an order index σ^{**} satisfying the stopping criterion exists. Indeed, we not only show the existence of a stopping criterion but also establish the following upper bound for the corresponding closest normal index

$$
\begin{aligned}
|\vec{\nu}^{\sigma^{**}}| &\leq \max\{r(N^*+1)+N^{\#}, (r-1)\cdot(rN-N^{\#})\} && (4)\\
&\leq r((r+1)N+1). && (5)
\end{aligned}
$$

In the full column rank case (where $r = n$) the above formulas remain valid with $N^* = -\infty$.

Denote by $\vec{\beta}$ (a vector of length $n-r$) the minimal indices for the nullspace of $\mathbf{G}(z)$. Note that these equal the minimal indices of $\mathbf{F}(z)$, and that $N^* = \max_j \vec{\beta}_j$. It is well-known that $\mathbf{G}(z)$ has the invariant $\vec{\alpha}$ of length r being (up to permutation) the unique vector of column degrees of a column reduced matrix $\mathbf{T}(z) = \mathbf{G}(z)\mathbf{U}(z)$ with $\mathbf{U}(z)$ unimodular. Degree bounds for the columns $\mathbf{U}^j(z)$ of a particular so-called minimal multiplier $\mathbf{U}(z)$ were the subject of [4], (see also [3] for the full column rank case). Denoting by J the set of indices of the $n-r$ zero columns of $\mathbf{T}(z)$, it is shown that there exists a multiplier with

$$k \in J: \quad \mathit{deg}\, \mathbf{U}^k(z) \leq \vec{\beta}_k$$

by [4, Remark 3.7] and

$$k \notin J: \quad \mathit{deg}\, \mathbf{U}^k(z) \leq \max\{N^*-1, \vec{\alpha}_k + (r-1)N - \text{MM-deg}\, \mathbf{G}(z)\}$$

by [4, Theorem 5.1(a)] (with $\vec{a} = \vec{0} = \vec{b}$ and the estimate $\vec{\gamma} \leq N\vec{e}$), where we recall from [4, Theorem 5.1(b)] that

$$N^{\#} = \text{MM-deg}\, \mathbf{G}(z) = \sum_j \vec{\alpha}_j + \sum_\ell \vec{\beta}_\ell.$$

Define

$$\ell = \max\{0, N^* + 1 - (r-1)N + N^{\#}\},$$

and the vector $\vec{\nu}$ by

$$\vec{\nu}_k = \begin{cases} \vec{\beta}_k, & \text{if } k \in J, \\ \ell + \vec{\alpha}_k + (r-1)N - N^{\#}, & \text{if } k \notin J. \end{cases}$$

We notice that, on a component basis, $\vec{\nu}^{J^c} \geq \vec{\alpha} + (N^*+1)\vec{e} \geq (N^*+1)\vec{e}$, showing that the column degree of $\mathbf{U}(z)$ is bounded above by $\vec{\nu}$. Moreover, the quantity $\mathbf{M}(z) := \mathbf{U}(1/z)z^{\vec{\nu}}$ is in $\mathbb{D}[z]^{n\times n}$, with

$$\mathbf{F}(z)\mathbf{M}(z) = \mathbf{R}(z)\cdot z^{\sigma}, \quad \mathbf{R}(z) = \mathbf{T}(1/z)z^{\vec{\alpha}} \in \mathbb{D}[z]^{m\times n},$$

where $\sigma = N + \ell + (r-1)N - N^{\#}$. We notice that $\mathbf{R}(z)$ satisfies the stopping criterion, namely, order $m\sigma = \sigma''$ divisible by m, and

$$\mathit{rank}\, \mathbf{R}(0) + \text{ number of zero columns of } \mathbf{R}(z) = m,$$

since the columns of $\mathbf{R}(0)$ with indices in J^c coincide with the leading coefficient columns of the column-reduced matrix $\mathbf{T}(z)_{J^c}$. Since the columns of the Mahler system $\mathbf{M}_{m\sigma}(z)$ form a (column-reduced) basis of the set of vectors of order $m\sigma$, we know from [2, Theorem 7.3(a)] that there exists a $\mathbf{P}(z) \in \mathbb{Q}[z]^{n\times n}$ with

$$\mathbf{M}_{m\sigma}(z) \cdot \mathbf{P}(z) = \mathbf{M}(z).$$

By the predictable degree property [5] (see also [2, Theorem 7.3(a)]),

$$deg\,\mathbf{P}(z)_{j,k} \leq \vec{\nu}_k - \vec{\nu}_j^{m\sigma}.$$

On the other hand, along with $\mathbf{M}(z)$, $\mathbf{P}(z)$ is also nonsingular, showing that there is a permutation Π with

$$\vec{\nu}_k \geq \vec{\nu}^{m\sigma}_{\Pi(k)}, \quad k = 1, ..., n.$$

In particular, we have for $k \in J$

$$\begin{aligned} &deg\,\mathbf{R}_{m\sigma}(z)_{\Pi(k)} \leq -\sigma + deg\,\mathbf{F}(z) \cdot \mathbf{M}_{m\sigma}(z)_{\Pi(k)} \\ &\leq -\sigma + N + \vec{\nu}^{m\sigma}_{\Pi(k)} \leq -\sigma + N + \vec{\nu}_k \\ &\leq -\sigma + N + N^* = -\ell - (r-1)N + N^{\#} + N^* < 0 \end{aligned}$$

by construction of ℓ, showing that $\mathbf{R}_{m\sigma}(z)_{\Pi(k)}$ vanishes. Consequently, $\mathbf{R}_{m\sigma}(z)$ contains as many zero columns as $\mathbf{R}(z)$, namely $n - r$. Furthermore, by construction

$$\mathbf{R}_{m\sigma}(0) \cdot \mathbf{P}(0) = \mathbf{R}(0)$$

where we recall that $\mathbf{R}(0)$ has rank r, and $\mathbf{R}_{m\sigma}(0)$ contains at most r columns different from zero. It follows that also $\mathbf{R}_{m\sigma}(0)$ has rank r, in other words, the stopping criterion is reached for the order $\sigma'' = m\sigma$, or already for some order $\sigma^{**} \leq \sigma''$. By construction, $|\vec{\nu}^{\sigma^{**}}| \leq |\vec{\nu}^{\sigma''}|$, and hence

$$|\vec{\nu}^{\sigma^{**}}| \leq |\vec{\nu}^{m\sigma}| \leq |\vec{\nu}| = \begin{cases} r(N^*+1) + N^{\#}, & \text{if } \ell \geq 0, \\ (r-1)\cdot(rN - N^{\#}), & \text{if } \ell = 0, \end{cases}$$

as claimed in (4). Assertion (5) now follows by using the trivial estimates $N^* \leq N^{\#} \leq rN$, and $N^{\#} \geq 0$. We finally notice that for the corresponding order we have the estimate

$$\sigma^{**} \leq m\sigma \leq m \cdot \left\{ \begin{array}{ll} r(N + N^* + 1) & \text{if } \ell \geq 0, \\ rN - N^{\#}, & \text{if } \ell = 0, \end{array} \right\} \leq m \cdot ((m+1)N + 1),$$

the right hand side coinciding with the worst case bound of [2, Section 8] mentioned in (3).

References

[1] B. BECKERMANN & G. LABAHN, *A uniform approach for the fast, reliable computation of Matrix-type Padé approximants*, SIAM J. Matrix Anal. Appl. **15** (1994) 804-823.

[2] B. Beckermann and G. Labahn, Fraction-free Computation of Matrix Gcd's and Rational Interpolants, *SIAM J. Matrix Anal. Appl.*, **22**:1 (2000) 114-144.

[3] B. BECKERMANN, G. LABAHN & G. VILLARD, *Shifted Normal Forms of Polynomial Matrices*, Proceedings of ISSAC'99, Vancouver, ACM Press, (1999) 189-196.

[4] B. BECKERMANN, G. LABAHN & G. VILLARD, *Normal Forms of General Polynomial Matrices*, Manuscript (2001).

[5] T. KAILATH, *Linear systems*, Prentice–Hall (1980).