# EXACT COMPUTATION OF THE GREATEST COMMON DIVISOR OF TWO POLYNOMIAL MATRICES

By

M. MONESS* and B. LANTOS

Department of Process Control, Technical University Budapest

Received February 8, 1982
Presented by Prof. Dr. A. FRIGYES

## 1. Introduction

Computation of $G(s)$, the greatest common divisor GCD of two polynomial matrices $D(s)$ and $C(s)$ is of vital importance in the frequency domain approach to multivariable control systems. It is useful in the problem of nonsingular factorization of a polynomial matrix, minimal state-space realization of a rational function transfer matrix, relative primeness test of two polynomial matrices and so on.

The problem has been tackled by many authors and through different techniques. An indirect method is to find an irreducible representation by any known algorithm in this field and then return to find out the GCD (see, e.g., EMRE [3]). There are other techniques to find the GCD as a polynomial combination, i.e., $G(s)=P(s)\cdot C(s)+Q(s)\cdot D(s)$, (see, e.g., MCDUFFEE [8]), or to transform the composite matrix $[D'(s)\ C'(s)]'$ to its upper-right triangular form $[G'(s)\ 0']$ (see e.g., WOLOVICH [9]). The most significant method seems to be the extension of the well-known Sylvester's matrix of two scalar polynomials to the matrix case to form the so-called generalized Sylvester's matrix (see, e.g., ANDERSON [1] and BITMEAD [2]).

Neither of the methods mentioned above guarantee numerical stability. So it was suggested to use $p$-adic arithmetic to compute the GCD of two polynomial matrices by the generalized Sylvester's matrix method. Appendix A contains a brief discussion of $p$-adic arithmetic while the routines used to handle $p$-adic objects are listed in Appendix B. Definitions necessary to the GCD problem are given in chapter 2. Chapter 3 describes the algorithm and the main theory. An example is solved in chapter 4.

* Aspirant at the Department of Process Control, Technical University, Budapest.

## 2. Definitions

### *2.1 GCRD of two polynomial matrices*

A greatest common right divisor (GCRD), $G_R(s)$ of two polynomial matrices $D(s)$ and $C(s)$ with the same number of columns is defined as a polynomial matrix which is the right divisor of both $D(s)$ and $C(s)$ and at the same time the left multiple of any other common right divisor CRD, i.e.,

$$C(s)=\bar{C}(s)\cdot G_R(s)$$

$$D(s)=\bar{D}(s)\cdot G_R(s), \text{ and}$$

$$G_R(s)=M(s)\cdot \bar{G}(s)$$

where $\bar{G}(s)$ is any CRD of $D(s)$ and $C(s)$

Notes:

i — a greatest common left divisor (GCLD) of two polynomial matrices is defined, and may be obtained, by using duality;

ii — the GCDs are not unique and differ in a unimodulator factor.

iii — if the composite polynomial matrix $F(s)=\begin{bmatrix} D(s) \\ C(s) \end{bmatrix}$ is of full rank, then $G_R(s)$ will be non-singular.

### *2.2 The generalized Sylvester's matrix*

Two polynomial matrices — $D(s)$ and $C(s)$ — are relatively right prime (RRP) if and only if there exists an irreducible pair (with an unimodulator GCRD) of polynomial matrices $[B(s)\ A(s)]$ with $A(s)$ and $C(s)$ of the same determinant degree i.e., $\partial|A(s)|=\partial|C(s)|$ such that:

$$A(s)\cdot D(s)+B(s)\cdot C(s)=0\,. \tag{2.1}$$

Expressing $D(s)$ and $C(s)$ as

$$D(s)=\sum_{i=0}^{l} D_i s^{l-i}, \quad C(s)=\sum_{i=0}^{l} C_i s^{l-i} \tag{2.2}$$

if $K$ is the degree of $A(s)$ and $B(s)$ satisfying Eq. (2.1), then this equation will have the form

$$[A_0 \quad B_0 \quad A_1 \quad B_1 \quad \dots \quad A_K \quad B_K]\cdot S_K=0 \tag{2.3}$$

where

$$S_K \triangleq \begin{bmatrix} D_0 & D_1 & \dots & D_l & 0 & \dots & 0 \\ C_0 & C_1 & \dots & C_l & 0 & \dots & 0 \\ 0 & D_0 & \dots & D_{l-1} & D_l & \dots & 0 \\ 0 & C_0 & \dots & C_{l-1} & C_l & \dots & 0 \\ \\ 0 & 0 & \dots & D_{l-K} & D_{l-K+1} & \dots & D_l \\ 0 & 0 & \dots & C_{l-K} & C_{l-K+1} & \dots & C_l \end{bmatrix} \tag{2.4}$$

$S_K$ is called the generalized Sylvester's matrix of order $K$. Usually Eq. (2.1) is written in concise form as:

$$M(s) \cdot F(s) = 0 \tag{2.5a}$$

where

$$M(s) = [A(s) \quad B(s)], \tag{2.5b}$$

and

$$F(s) = [D'(s) \quad C'(s)]'. \tag{2.5c}$$

### 2.3 Observability index

If $S(A, B, C, D)$ is the state-space description of an $n$-states observable system, then the well-known $q$-order observability matrix $\mathcal{O}_q$ is defined as:

$$\mathcal{O}'_q \triangleq [C' \quad A'C' \quad \dots \quad A'^{q-1}C'], \quad q = 1, 2, \dots, n. \tag{2.6}$$

The observability index of such a system is defined as the least integer among the $q$-set which makes $\mathcal{O}_q$ of rank $n$.

If $H(s)$ is a $p \times m$ rational function transfer matrix, representing an irreducible realization of $S(A, B, C, D)$, i.e.,

$$H(s) = D(s) \cdot C^{-1}(s) \tag{2.7}$$

then the column degrees of $C(s)$, $v_i$ $i = 1, 2, \dots, m$ are called the dual dynamical indices. Moreover, if $H(s)$ is proper, these indices will coincide with the observability indices.

### 2.4 Echelon form

A scalar, rectangular matrix is said to be in a row (column) echelon form if its elements satisfy the following conditions:

i — the leading nonzero element of a row (column) is 1, unless the row (column) consists entirely of zeros;

ii — any column (row) containing nonzero leading element of a row (column) has zeros elsewhere below (to the right of) the leading element;

iii — for any two nonzero rows (columns) $i$ and $j$, if $i<j$ then the leading nonzero element of the $i^{th}$ row (column) appears to the left of (above) the $j^{th}$ one; and

iv — all the zero rows (columns) follow the nonzero ones.

## 3. The algorithm description and the main theory

Let us compute the GCRD of two polynomial matrices $D(s)$ and $C(s)$, of dimensions "$p\times m$" and "$m\times m$", respectively. If $q$ is the maximum degree of $D(s)$ and $C(s)$, then they can be expressed as:

$$D(s)=D_0s^q+D_1s^{q-1}+\ldots+D_{q-1}s+D_q \tag{3.1.a}$$

$$C(s)=C_0s^q+C_1s^{q-1}+\ldots+C_{q-1}s+C_q \tag{3.1.b}$$

The initial composite matrix, or the generalized Sylvester's matrix of order one, $\mathscr{F}^1$ as is defined:

$$\mathscr{F}^{(1)}=\begin{bmatrix} D_0 & D_1 & \ldots & D_{q-1} & D_q \\ C_0 & C_1 & \ldots & C_{q-1} & C_q \end{bmatrix}. \tag{3.2}$$

The following algorithm, using only scalar operations on $\mathscr{F}^1$, will be proven to give the GCRD, $G_R(s)$ of $C(s)$ and $D(s)$, and also to give some dynamical properties of the system described by the transfer function rational matrix

$$H(s)=D(s)C^{-1}(s). \tag{3.3}$$

*Algorithm steps:*

Step 1. Set $k=1$. Reduce $\mathscr{F}^{(1)}$ to the echelon form $\mathscr{E}^1$ by means of an "$m+p$" nonsingular scalar matrix $T^1(s)$. Calculate $l_1=$rank of $\mathscr{E}^{(1)}$. If $l_1<m$, there exists only the trivial solution, i.e., GCRD of infinite degree, and hence STOP, otherwise insert $\mathscr{C}\leftarrow\mathscr{E}^{(1)}$ and continue.

Step 2. Set $k=k+1$ and construct the $k^{th}$ block of the composite matrix $\mathscr{C}$ by introducing $\mathscr{E}^{(k-1)}$ (the "$k-1$"$^{th}$ block of $\mathscr{C}$) from the "$(k-1)(m+p)+$ $+1$"$^{th}$ row, through and up to the $k(m+p)^{th}$ row after shifting it to the right by $m(k-1)$ columns with respect to the initial block.

Step 3. Reduce the $k^{th}$ block of $\mathscr{C}$ into the echelon form $\mathscr{E}^{(k)}$ by using row operations from the first $(k-1)$ blocks so that each element under the pivoting ones is zero, and then by row operations within the $k^{th}$ block itself by means of an "$(m+p)k$" transformation matrix $T^{(k)}$ applied to $\mathscr{C}$. Calculate $l_k$ = rank of $\mathscr{C}$ and if $l_k - l_{k-1} = m$ go to the fourth step otherwise return to the second step.

Step 4. Set $v=k$. The first $m$ nonzero rows of the $v^{th}$ block, $\mathscr{E}^{(v)}$ give the scalar coefficients of $G_R(s)$ arranged from the highest power and downward. The dual dynamical indices may be obtained from $l$'s STOP.

*The main theory of the generalized Sylvester's matrix*

The previously described algorithm can be formulated in the following theorem:

*THEOREM* "The generalized resultant matrix algorithm gives the following information in its various steps:

i — The first 2"$m$", nonzero rows of $\mathscr{E}^{v}$ give the scalar coefficients of $G_R(s)$, starting from the highest power and downward,

ii — If $D(s)$ and $C(s)$ are any MFRD of an "$p \times m$" rational transfer matrix $H(s)$, then the $p$-dual dynamical indices of the system described by $H(s)$ are given by the relationship:

$$\gamma_i = 2l_i - (l_{i+1} + l_{i-1}), \quad i = 0, 1, \ldots, v$$

$$l_0 = 0 \text{ and } l_{-1} = -(m+p)$$

where $\gamma_i$ — number of dual dynamical indices of order $i$ or its equivalent:

$$l_k = (m+p)k - \sum_i (k - v_i) \qquad k = 2, 3, \ldots$$

$$\{i \mid 0 < i < k\}, \qquad i = 1, 2, \ldots, p$$

where $v_i$ — dual dynamical index of the $i^{th}$ row, and

iii — The determinant degree of $G_R(s)$, $\partial_g = n - \sum_{i=1}^{p} v_i$, where $n$ — determinant degree of $C(s)$."

*Proof:*

i — To prove the first part of the theory, it will be proven first that the independent-variable version $E^{v}(s)$ of the last scalar block $\mathscr{E}^{(v)}$ obtained by means of the algorithm is a unimodulator transformation from $F^{(1)}(s)$. It has only to be proven that $E^{(2)}(s)$ is related to $F^{(1)}(s)$ by a unimodulator matrix, since the transformation procedure from $\mathscr{E}^{(2)}$ to $\mathscr{E}^{(v)}$ is just a repetition. $F^{(1)}(s)$ can be written as follows:

$$F^{(1)}(s) \triangleq [D'(s)C'(s)]' =$$

$$= \mathscr{F}^{(1)} S^{(1)}(s) \tag{3.3}$$

where $\mathscr{F}^{(1)}$ is defined by Eq. (3.2) and $S^{(i)}(s)$ is defined as:

$$S^{(i)}(s) = \begin{bmatrix} s^{q+i-1} I_m & & \bigcirc \\ & \ddots & \\ & & sI_m & \\ \bigcirc & & & I_m \end{bmatrix} \tag{3.4}$$

Step 1 in the algorithm is the transformation of $\mathscr{F}^{(1)}$ into its echelon form $\mathscr{E}^{(1)}$ by an "$m+p$" non-singular scalar matrix $T^{(1)}$, i.e.,

$$T^{(1)} \cdot \mathscr{F}^{(1)} \cdot S^{(1)}(s) = T^{(1)} \cdot F^{(1)}(s) =$$

$$= \mathscr{E}^{(1)} \cdot S^{(1)}(s) =$$

$$\triangleq E^{(1)}(s), \tag{3.5}$$

and the general form of $\mathscr{E}^{(1)}$ is:

$$\mathscr{E}^{(1)} = \begin{bmatrix} A_0^{(1)} & A_1^{(1)} & A_2^{(1)} & \dots & A_{q-1}^{(1)} & A_q^{(1)} \\ 0 & B_0^{(1)} & B_1^{(1)} & \dots & B_{q-2}^{(1)} & B_{q-1}^{(1)} \end{bmatrix} \tag{3.6}$$

where $A$'s and $B$'s are in the echelon form. Since the right-shift step is equivalent to the multiplication by the independent variable, in our case $s$, then for $k=2$

$$F^{(2)}(s)=\begin{bmatrix} sE(s) \\ E^{(1)}(s)\end{bmatrix}= \tag{3.7.a}$$

$$=\begin{bmatrix} A_0^{(1)} & A_1^{(1)} & A_2^{(1)} & \dots & A_{q-1}^{(1)} & A_q^{(1)} & 0 \\ 0 & B_0^{(1)} & B_1^{(1)} & \dots & B_{q-2}^{(1)} & B_{q-1}^{(1)} & 0 \\ 0 & A_0^{(1)} & A_1^{(1)} & \dots & A_{q-2}^{(1)} & A_{q-1}^{(1)} & A_q^{(1)} \\ 0 & 0 & B_0^{(1)} & \dots & B_{q-3}^{(1)} & B_{q-2}^{(1)} & B_{q-1}^{(1)} \end{bmatrix} \cdot S^{(2)}(s)= \tag{3.7.b}$$

$$=\bar{\mathscr{C}}_2 \cdot S^{(2)}(s)\,. \tag{3.7.c}$$

The transformation of $\bar{\mathscr{C}}_2$ to a form having the first two properties of the echelon form definition can be realized by a $2(m+p)$ nonsingular scalar matrix $T^{(2)}$.

$$\mathscr{C}_2=T^{(2)}\bar{\mathscr{C}}_2 \tag{3.8}$$

The $T^{(2)}$ — construction, (step 3 in the algorithm) is done by two substeps. The first substep comprises the operations from the first block onto the second, while the second one those within the second block. It is obvious from the shape of $\bar{\mathscr{C}}_2$, (Eq. 3.7.b), that the first operations are from the matrices $B$'s of the first block onto the matrices $A$'s of the second one, i.e. the first subtransformation matrix has the form:

$$T_1^{(2)}=\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & Q_1 & I & 0 \\ 0 & 0 & 0 & I \end{bmatrix} \tag{3.9}$$

and this yields:

$$\mathscr{C}_2^{(2)}=\begin{bmatrix} A_0^{(1)} & A_1^{(1)} & A_2^{(1)} & A_3^{(1)} & \dots & A_{q-1}^{(1)} & A_q^{(1)} & 0 \\ 0 & B_0^{(1)} & B_1^{(1)} & B_2^{(1)} & \dots & B_{q-2}^{(1)} & B_{q-1}^{(1)} & 0 \\ 0 & \bar{A}_0^{(1)} & \bar{A}_1^{(1)} & \bar{A}_2^{(1)} & \dots & \bar{A}_{q-2}^{(1)} & \bar{A}_{q-1}^{(1)} & \bar{A}_q^{(1)} \\ 0 & 0 & B_0^{(1)} & B_1^{(1)} & \dots & B_{q-3}^{(1)} & B_{q-2}^{(1)} & B_{q-1}^{(1)} \end{bmatrix}. \tag{3.10}$$

Since the rows $B$'s of the 2nd block are either zero or linearly independent, the transformation of this block to a form having either linearly independent rows or zero rows (properties 1 and 2 of the echelon form) can be carried out by an elementary transformation from the rows $B$'s to the $\bar{A}$'s or within the rows $\bar{A}$'s themselves i.e., the second subtransformation matrix $T_2^{(2)}$ has the form:

$$T_2^{(2)} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & Q_2 & Q_3 \\ 0 & 0 & 0 & I \end{bmatrix} \tag{3.11}$$

from Eqs (3.9) and (3.11):

$$T^{(2)} = T_2^{(2)} \cdot T_1^{(2)} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & Q_2 Q_1 & Q_2 & Q_3 \\ 0 & 0 & 0 & I \end{bmatrix} \tag{3.12}$$

using the above equations, we have

$$T^{(2)} \cdot E^{(2)}(s) = \begin{bmatrix} E(s) \\ E_0^{(2)}(s) \end{bmatrix} = T^{(2)} \cdot \begin{bmatrix} sE^{(1)}(s) \\ E^{(1)}(s) \end{bmatrix} \tag{3.13}$$

where $E_0^{(2)}(s)$ has the echelon form with some row orders permuted. Or:

$$E_0^{(2)}(s) = U_2(s) E^{(1)}(s) \tag{3.14}$$

where

$$U_2(s) = \begin{bmatrix} Q_2 & s\,Q_2\,Q_1 + Q_3 \\ 0 & I \end{bmatrix}. \tag{3.15}$$

It is clear that $|U_2(s)| = |Q_2| \neq f(s)$, i.e., $U_2(s)$ is a unimodulator matrix. To transform $E_0^{(2)}(s)$ into the echelon form only a rearrangement of its rows, i.e., no polynomial but only scalar operations, are needed and hence $E^{(2)}(s)$ is related to $E^{(1)}(s)$ by a unimodulator matrix, needed to continue our proof. The last step,

$$E^{(v)}(s) = \begin{bmatrix} R(s) \\ 0 \end{bmatrix} = \tag{3.16.a}$$

$$= U_v(s) \cdot E^{(1)}(s) \tag{3.16.b}$$

where $U_v(s)$ is a unimodulator matrix of the form

$$U_v(s)=\begin{bmatrix} U_{1,1}(s) & U_{1,2}(s) \\ U_{2,1}(s) & U_{2,2}(s) \end{bmatrix}.$$

Writing Eq. (3.16.a) in the form

$$E^{(1)}(s)=U_v^{-1}(s)\cdot E(s)=$$

$$=\begin{bmatrix} \bar{U}_{1,1}(s) & \bar{U}_{1,2}(s) \\ \bar{U}_{2,1}(s) & \bar{U}_{2,2}(s) \end{bmatrix} \tag{3.17}$$

then:

$$C(s)=\bar{U}_{1,1}(s)\cdot R(s) \tag{3.18.a}$$

$$D(s)=\bar{U}_{2,1}(s)\cdot R(s) \tag{3.18.b}$$

thus, $R(s)$ is a CRD of $C(s)$ and $D(s)$. From Eq. (3.16.b)

$$R(s)=U_{1,1}(s)\cdot C(s)+U_{1,2}(s)\cdot D(s). \tag{3.19}$$

If $R_0(s)$ is a CRD, then

$$C(s)=C_0(s)\cdot R_0(s), \quad D(s)=D_0(s)\cdot R_0(s) \tag{3.20}$$

hence

$$R(s)=(U_{1,1}(s)\cdot C_0(s)+U_{1,2}(s)\cdot D_0(s))R_0(s)=$$

$$=\bar{R}(s)\cdot R_0(s) \tag{3.21}$$

i.e. $R(s)$ is a left multiple for every CRD and so it is a possible $G_R(s)$.

ii — The second part can be proved by making use of Forney's theorem [4]. In that theory the following statements are equivalent, regarding a $p\times q$ polynomial matrix $M(s)$ $(p\leqq q)$

(a) the GCD of the $p\times p$ minors of $M(s)$ is 1 and the highest degree is $v$,

(b) for any two polynomial vectors $y(s)$ and $x(s)$ of $q$ and $p$-tuples, respectively, expressed as $y(s)=x(s)\cdot M(s)$; $\deg y(s)=\max(\deg x^{(i)}(s)+v_i)$, where $v_i$ is the $i^{th}$ row index, and $1\leqq i\leqq p$, and

(c) the indices $v_i$ are such that for all $k\geqq 0$, $\dim V_k=\sum_{i|v_i<\kappa}(k-v_i)$, where $V_k$ is the set of all *n-tuples of polynomials with less than* $k$ degrees in the $n$-tuples vector space over the field of rational functions.

In our case $M(s)=[A(s)B(s)]$ and by definition of the Sylvester's matrix, $M(s)\cdot F(s)=0$. Under the constraint that $A(s)$ and $B(s)$ are irreducible pairs, statement (a) is satisfied and accordingly statements (b) and (c) are true. If the following sets are defined:

$$\mathcal{N}_k \equiv \{w \mid w\mathcal{F}^{(k)}=0, \text{ where } w \text{ is a } k(p+m) \text{ row vector}\}$$

$$U_k \equiv \{u(s) \mid u(s)\cdot F(s)=0 \text{ and } \partial u(s)<k\}$$

$$V_k \equiv \{v(s) \mid v(s)=x(s)\cdot M(s),\ \partial x^{(i)}(s)<(k-v_i)\}$$

and since $M(s)\cdot F(s)=0$, then statements (b) and (c) show that $V_k^{\perp}=U_k$ and $\mathcal{N}_k$ is isomorphic to $U_k$. From statement (c), dim $V_k=\sum_{i|v_i<\kappa}(k-v_i)$ which is equal to the dimension of $\mathcal{N}_k$, so

$$\dim V_k+\operatorname{rank}\mathcal{F}^{(k)}=k(m+p)$$

or its equivalent:

$$\operatorname{rank}\mathcal{F}^{(k)}=k(m+p)-\sum_{\{i|v_i<k\}}(k-v_i);\quad k=1,2,\ldots, \tag{3.22}$$

relationship between the increment changes in the ranks of the generalized Sylvester's matrix $\mathcal{F}^{(i)}$, and the number of indices of order $i$,

$$\gamma_i=2l_i-(l_{i+1}+l_{i-1}) \tag{3.23}$$

can be obtained by direct substitution into Eq. (3.22), (see, e.g., Bitmead [2]).

iii — The minimum degree $n_{\min}$ of a realized, proper system is known to be given by:

$$n_{\min}=\sum_{i=1}^{p}v_i \tag{3.24}$$

and since

$$C(s)=\bar{C}(s)\cdot G_R(s) \tag{3.25}$$

where $\bar{C}(s)$ is the irreducible version of $C(s)$; then:

$$|C(s)|=|\bar{C}(s)||G_R(s)| \tag{3.26}$$

or:

$$\begin{aligned}\partial g \triangleq G_R(s)&=\\ &=n-n_{\min}\end{aligned} \tag{3.27}$$

where $n=|C(s)|$.

## 4. Example

A numerical example will be solved to show the algorithm application, as well as the importance of using $p$-adic arithmetic to avoid numerical instability which arises in some problems.

Let us have the following two polynomial matrices:

$$D(s)=\begin{bmatrix} s^2+\frac{102}{101}s+\frac{1}{101} & s^2+\frac{203}{101}s+\frac{2}{101} \\ s^2+\frac{708}{101}s+\frac{7}{101} & s^2+\frac{304}{101}s+\frac{3}{101} \end{bmatrix};$$

$$C(s)=\begin{bmatrix} s^2+\frac{506}{101}s+\frac{5}{101} & 0 \\ 0 & s^2+11s+\frac{11}{101} \end{bmatrix}$$

and the computation of their GCRD polynomial matrix, $G_R(s)$ of the general form:

$$G_R(s)=\begin{bmatrix} a_{1,1}(s) & a_{1,2}(s) \\ a_{2,1}(s) & a_{2,2}(s) \end{bmatrix}$$

is needed for some design purposes.

Using the floating point arithmetics (simple and double precision), some small quantity $\varepsilon$ must be defined as zero. Since the span and the elements of the generalized Sylvester's matrix are variables, they cannot be estimated in advance. Table (4–1) shows the computed values of $G_R(s)$ and the two dynamical indices $v_1$ and $v_2$ for different values of $\varepsilon$.

It is evident from the Table that the results can be classified into groups, and each one gives certain results. So, some basis is needed to distinguish between the different results. By using $p$-adic arithmetic the following exact results are obtained for $p=5419$, $r=8$ (see Appendices A and B):

$$G_R(s)=\begin{bmatrix} s+1/101 & 0 \\ 0 & 1 \end{bmatrix}$$

$l_1=4,\quad l_2=7,\quad l_3=9,$
$v_1=1$ and $v_2=2$

Making use of these exact results, neither a big value of $\varepsilon$ (from $10^{-1}$ up to $10^{-3}$), nor a relatively small value of $\varepsilon$ (less than $10^{-8}$) is seen to give correct

**Table 4.1**

*A comparison between exact solution using p-adic and floating point arithmetic of different ε*

| $\varepsilon$ | $a_{1,1}(s)$ | $a_{1,2}(s)$ | $\nu_1$ |
|---|---|---|---|
| Exact | $s+1/101$ | 0 | 1 |
| $10^{-1}$ | 1.0000000000$E$ 00 * $S$ + 4.9504946917$E$-02<br>1.0000000000$D$ 00 * $S$ + 4.9504946917$D$-02 | 5.9237349778$E$-02 * $S$ + 0.0<br>5.9237386612$D$-02 * $S$ + 0.0 | 1 |
| $10^{-2}$ | 1.0000000000$E$ 00 * $S$ + 9.9009908736$E$-03<br>1.0000000000$D$ 00 * $S$ + 9.9009912343$D$-03 | 4.2275935411$E$-03 * + 0.0<br>4.2276014292$D$-03 * $S$ + 0.0 | 1 |
| $10^{-3}$ | 1.0000000000$E$ 00 * $S$ + 9.9009908736$E$-03<br>1.0000000000$D$ 00 * $S$ + 9.9009912343$D$-03 | 8.4561866166$E$-04 * $S$ + 0.0<br>8.4552044389$D$-04 * $S$ + 0.0 | 1 |
| $10^{-4}\rightarrow10^{-7}$ | 1.0000000000$E$ 00 * $S$ + 9.9009908736$E$-03<br>1.0000000000$D$ 00 * $S$ + 9.9009912343$D$-03 | 0.0 * $S$ + 0.0<br>3.2526065175$D$-19 * $S$ + 0.0 | 1 |
| $10^{-8}$ | 1.0000000000$E$ 00 * $S$ + 9.9009908736$E$-03<br>1.0000000000$D$ 00 * $S$ + 9.9009911523$D$-03 | 0.0 * $S$ + 0.0<br>3.7947676037$D$-19 * $S$ + 0.0 | 1 |
| $10^{-9}$ & $10^{-10}$ | 0.0 * $S$ + 1.0000000000$E$ 00<br>0.0 * $S$ + 1.0000000000$D$ 00 | 0.0 * $S$ + 0.0<br>−1.1368683772$D$-13 * $S$ + 0.0 | 2 |

Table 4.1 continued

| $\varepsilon$ | $a_{2,1}(s)$ | $a_{2,2}(s)$ | $\nu_2$ |
|---|---|---|---|
| Exact | 0 | 1 | 2 |
| $10^{-1}$ | 0.0 * S + −8.9108884335E-02 | 0.0 * S + 1.0000000000E 00 | 2 |
| | 0.0 * S + −8.9108906686D-02 | 1.332267296 D-15 * S + 1.0000000000D 00 | |
| $10^{-2}$ | 1.1175876895E-8 * S + 0.0 | 1.0000000000E 00 * S + 9.8858736455E-03 | 1 |
| | 1.6763806343D-08 * S + 0.0 | 1.0000000000D 00 * S + 9.8858747054D-03 | |
| $10^{-3} \rightarrow 10^{-7}$ | 1.1175876895E-08 * S + 0.0 | 0.0 * S + 1.0000000000E 00 | 2 |
| | 1.6763806343D-08 * S + 0.0 | 0.0 * S + 1.0000000000D 00 | |
| $10^{-8}$ | −1.0615373025E-09 * S + 0.0 | 0.0 * S + 1.0000000000E 00 | 2 |
| | −1.5923058423D-09 * S + 0.0 | 0.0 * S + 1.0000000000D 00 | |
| $10^{-9}$ & $10^{-10}$ | 0.0 * S + 1.0510270605E-11 | 0.0 * S + 1.0000000000E 00 | 2 |
| | 0.0 * S + 1.5765406056D-11 | 0.0 * S + 1.0000000000D 00 | |

results in the example. The results are only exact up to eight digits for a range of $\varepsilon$ between $10^{-4}$ and $10^{-8}$. It is also obvious that wrong bands of $\varepsilon$ may give wrong observability indices.

## 5. Conclusion

To compute the GCD of two polynomial matrices from their generalized Sylvester matrix, a complete theory with an easy proof is offered. In light of this proof a systematic algorithm has been constructed for the numerical use.

In converting this algorithm into a set of FORTRAN IV subroutines, the classical convergence problem arose, i.e., even if it is known that the algorithm has a numerically stable band, how can it be found? The use of some exact computation techniques is suggested to overcome this difficulty. Actually, the $p$-adic techniques have been successfully applied for the exact computation of many problems. This technique is hoped to be a useful basis for another study on the best numerical method for computing the GCD of two polynomial matrices.

Appendix A: *p-adic arithmetics.*

A $p$-adic arithmetic system is identified as residue arithmetic modulo $p^r$. In this system, choosing a certain prime $p$ and an even number $r$, any rational number $\alpha$, will be represented in $r$-digits having the value from "0" to "$p-1$". *The computation according to this method will be exact if numerator and denominator of the computed number will be within a prescribed bound given by* $p^{r/2}/\sqrt{2}$. For more details see KRISHNAMURTHY [5, 6]. In the example given to illustrate the computation of the GCRD we use the self denominator technique. On item will be here reproduced from [6] for convenience.

In the self-denominator technique, the $p$-adic representation of a rational number $\alpha = a/b$ is executed through $2(r+1)$ dimensional array rather than $(r+1)$ dimensional one. The first half of this array, M represents $a/b$, while the second half E, represents the denominator $b$. In each half the first $r$-digits give the mantissa, and the $(r+1)^{th}$ digit gives the exponent. The four basic arithmetic operations between any two $p$-adic numbers (M1, E1) and (M2, E2) can be abbreviated in this technique as follows:

$$(\mathrm{M1}, \mathrm{E1}) \circ (\mathrm{M2}, \mathrm{E2}) = (\mathrm{M3}, \mathrm{E3})$$

where

| | |
|---|---|
| $\mathrm{M3} = \mathrm{M1} \circ \mathrm{M2}$ | in all operations; |
| $\mathrm{E3} = \mathrm{lcm}\,(\mathrm{E1}, \mathrm{E2})$ | in addition and subtraction; |
| $\mathrm{E3} = \mathrm{E1} \cdot \mathrm{E2}$ | in multiplication; and |
| $\mathrm{E3} = \mathrm{E1}\,\lvert \mathrm{M2} \cdot \mathrm{E2} \rvert_p$ | in division |

where $|\cdot|_p$ is the absolute value in $p$-adic sense.

To recover the conventional number again from its $p$-adic code (M, E) the following two functions are defined:

$$\mathrm{VALUE(X)} = \begin{cases} \mathrm{X} & \mathrm{O} \le \mathrm{X} \le (p^r - 1)/2 \\ \mathrm{X} - p^r & \text{otherwise} \end{cases}$$

where X is an integer,

$$I(H) = \sum_{i=0}^{r-1} h_i \cdot p^i$$

where $H$ is an $(r+1)$-array representing a $p$-adic number and $h_i$ is the integer value in the $i$th position. Hence,

$$a = \mathrm{VALUE}(I(\mathrm{M} \cdot \mathrm{E}))$$

$$b = I(\mathrm{E})$$

Appendix B. *Subroutines' list*

In this appendix, the used subroutines are listed with the accomplished arguments

B1- CNVHAN(A,B,H,P,N)
gives the representation of A/B ($\mathrm{N} = r + 1$) in the $p$-adic form in the N-vector H

B2- CNVSD(A,B,HSD,P,N)
as B1 but HSD is of dimension 2N and gives the self-denominator representation.

B3- COMP(H1,HC,P,N)
HC is the $p$-adic complement of H1.

B4- ADD(H1,H2,HS,P,N)
HS is the $p$-adic sum of H1 and H2.

B5- SUB(H1,H2,HD,P,N)
HD is the $p$-adic difference of H2 from H1.

B6- MULT(H1,H2,HM,P,N)
HM is the $p$-adic product of H1 and H2.

B7- DIV(H1,H2,HQ,P,N)
HQ is the $p$-adic quotient of H1 and H2.

B8- GCD(H1,H2,HG,P,N)
HG is the gcd of two integers H1 and H2 (in $p$-adic).

B9- HABS (H1,H2,HA,P,N)
HA is the absolute value of H1 and H2 in $p$-adic sense.

B10- LCM(H1,H2,HL,P,N)
HL is the lcm of H1 and H2.

B11- ECHE(A,E,N1,N2,RANK,P,N)
E is the echelon form of a given $N1 \times N2 \times 2N$ single array A where N1 and N2 are the numbers of rows and columns of A.

## Summary

An algorithm is given to achieve numerical stability during the estimation of the GCD of two polynomial matrices. It has been found that the use of $p$-adic arithmetic will guarantee exact computation within prescribed bounds. A complete theory of this algorithm with proof is also given.

## References

1. Anderson, B. D. O.—Jury, E. I.: Generalized Bezoution and Sylvester Matrices in Multivariable Linear Control, IEEE AC-21, 1976, pp.: 551–556.
2. Bitmead, R. R. et al.: Greatest Common Divisors via Generalized Sylvester and Bezout Matrices, IEEE AC-23, 1978, pp: 1043–1047.
3. Emre, E.: Nonsingular Factors of Polynomial Matrices and (A, B)-Invariant Subspace, SIAM. JOU. CONT. and OPT., Vol. 18, 1980. pp: 288–296.
4. Forney, G. D.: Minimal Bases of Rational Vector Spaces with Application to Multivariable Linear Systems, SIAM. JOU. CONT. and OPT.,Vol. 13, 1975, pp.: 493–520.
5. Krishnamurthy, E. V. et al.: Finite Segment $p$-adic Number Systems with Application to Exact Computation, The Proceedings of the Indian Academy of Sciences Vol. 81, 1975, pp: 58–79.
6. Krishnamurthy, E. V. et al.: $p$-adic Arithmetic Procedures for Exact Matrix Computations, The Proceedings of the Indian Academy of Sciences Vol. 82, 1975. pp: 165–175.
7. Kung, S. Y. et al.: A Generalized Resultant Matrix for Polynomial Matrices, Proc. IEEE Conf. Decision and Control, 1976. pp: 892–895.
8. MacDuffee, C. C.: The Theory of Matrices, New York Chelsea, 1956.
9. Wolovich, W. A.: Linear Multivariable Systems, New York, Springer-Verlag, 1974.

M. Moness Assiut University, Faculty of Engineering, Electrical Engineering Department, Egypt
Dr. Béla Lantos H-1521 Budapest,