New Results in 2-D Systems Theory, Part I: 2-D Polynomial Matrices, Factorization, and Coprimeness

MARTIN MORF, MEMBER, IEEE, BERNARD C. LÉVY, STUDENT MEMBER, IEEE, AND SUN-YUAN KUNG, STUDENT MEMBER, IEEE

Abstract—During recent years, linear system theory has intensively been applied in estimation and control. At the same time, image processing has attracted increasing interest and attempts have been made to extend the techniques of systems theory to multidimensional problems, among others, by Bose, Attasi, Givone and Roesser, and Mitra.

Part I of our results is centered around polynomial descriptions of systems. The notion of minimality in connection with state space requires the concept of coprimeness of 2-D polynomial matrices. For this purpose, we have extended the existing 1-D results on greatest common right divisor (GCRD) extraction, Sylvester resultants, matrix fraction descriptions (MFD) to the 2-D case. In addition we have results that appear to be unique for multidimensional problems such as existence and uniqueness of so-called "primitive factorizations" and existence of general factorizations.

Part II will appear in a companion paper presenting results on a comparison between the different state space models that have been proposed, using what we consider to be proper definitions of state, controllability and observability and their relation to minimality of 2-D systems. We also present new implementations of 2-D transfer functions using a minimal number of dynamic elements.

Manuscript received August 24, 1976; revised December 3, 1976. This work was supported by the National Science Foundation under Contract NSF-ENG 75-18952, Air Force Office of Scientific Research, Air Force Systems Command, under Contract AF44-620-74-C-0068, and the Joint Services Electronics Program under Contract N00014-75-C-0601.

The authors are with the Information Systems Laboratory, Stanford University, Stanford, CA 94305.

I. INTRODUCTION

THE THEORY of 2-D systems has received increasing attention during recent years, the reason most probably being the wide range of applications in digital filtering, digital picture processing, seismic data processing and many other areas. These systems can be represented with two types of dynamical elements (say z^{-1} and ω^{-1}) and consequently there is a very close connection between the theory of 2-D systems and the theory of polynomials of 2 variables.

As in the 1-D case these systems can either be studied in the transform domain (for constant parameter models) or in the state space form. In the first case the polynomial aspect is most important and many significant results have already been

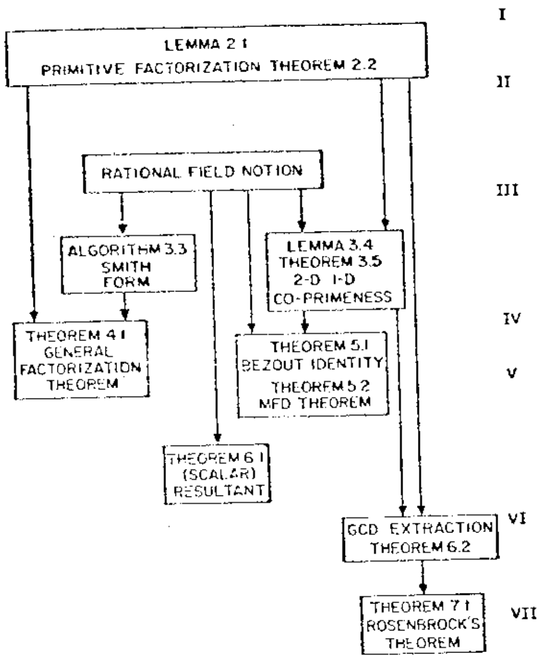

Fig. 1. Logical dependence of the proofs.

obtained particularly in the case of scalar (i.e., single input, single output) systems.

Indeed, the theory of polynomials of several variables goes back to Gauss and Hilbert and some accounts of this theory can be found in Bocher [1] or in Van Der Waerden [2]. And various applications to scalar 2-D systems are given by Bose [3], [4], or Bose and Jury [5].

In the state space approach, the notions of controllability, observability, minimality play an important part and some important results in this direction have been provided by Attasi [6], Fornasini–Marchesini [7], Givone–Roesser [8].

In the present paper, we have extended some of the results of scalar 2-D polynomials to the multivariable (i.e., 2-D polynomial matrix) case. Such an extension is known in the 1-D case (see MacDuffee [9]) and there is a very close relation between 1-D polynomial matrices and 1-D state space theory, a fact that has been studied in detail by Rosenbrock [10] or Wolovich [11].

In a subsequent paper, Part II, we shall study along similar lines the connections between 2-D polynomial matrices and 2-D state space notions.

The tools involved in the study of 2-D polynomial matrices generalize either some notions appearing in the theory of 2-D scalar polynomials or some tools already existing for 1-D polynomial matrices. The matrix primitive factorization presented in Section II or the rational field argument studied at the beginning of Section III belong clearly to the first category. Similarly the Hermite form and the Smith form of Section III or the general factorization algorithm of Section IV are notions obviously borrowed from 1-D theory.

As applications of these results we present in Section V the Bezout Identity and a study of the properties of MFD (matrix fraction description) of 2-D transfer functions. In Section VI an algorithm is given for the greatest common right divisor (GCRD) extraction of two polynomial matrices and in Section VII Rosenbrock's criterion of relative primeness of two polynomial matrices is extended to the 2-D case.

The logical dependence of the proofs and accordingly of the sections of this paper is presented in Fig. 1.

II. Primitive Factorization

Many significant results have long been obtained for scalar (i.e., single input, single output) 2-D systems. For matrix (multi-input, multi-output) 2-D problems, fewer results are known (see [15]). One possible reason is that there still exist many open problems in the scalar case that may have attracted (almost) all the attention of researchers in the field of 2-D systems. Another possibility is that 2-D matrix problems appear to be potentially much more difficult. Also, the "noncommutativity" of 2-D matrices causes no less trouble than its 1-D counterpart. Another (even more unexpected) aspect we wish to discuss now is the difficulties of the factorization problems associated with 2-D matrices.

In the following, we shall denote $F[z, \omega]$ the ring of polynomials in z and ω with coefficients in the field F. We shall also assume (except in part a) of Section VI and in Section VII) that the field F is algebraically closed.

Since any polynomial

$$a(z, \omega) = \sum_{i=0}^{n} a_i(\omega)\, z^i$$

(respectively, $\sum_{j=0}^{m} a_j(z)\,\omega^j$), we identify $F[z, \omega]$ with $F[\omega][z]$ (respectively, $F[z][\omega]$) the ring of polynomials in z with coefficients in $F[\omega]$ (respectively, the ring of polynomials in ω with coefficients in $F[z]$). These are subrings of $F(\omega)[z]$ and of $F(z)[\omega]$ which will also play an important part in our analysis.

In the theory of scalar 2-D polynomials, the notion of primitive factorization (see [1]) was of particular importance.

To be more precise, $a(z, \omega) = \bar{a}(\omega)\, a^*(z, \omega)$ is a primitive factorization of

$$a(z, \omega) = \sum_{i=0}^{n} a_i(\omega)\, z^i$$

in $F[\omega][z]$ if $\bar{a}(\omega)$ is the greatest divisor of $a(z, \omega)$ belonging to $F[\omega]$. $\bar{a}(\omega)$ is just the GCD of $[a_i(\omega),\ i = 1, 2, \cdots, r]$. Symmetrically, we could define the primitive factorization

$$a(z, \omega) = \breve{\alpha}(z)\, \alpha^*(z, \omega)$$

in $F[z][\omega]$. In the remainder of this section, we shall consider only primitive factorizations in $F[\omega][z]$.

Now, if we are interested in the primitive factorization in $F[\omega][z]$ of a polynomial matrix, say

$$A(z, \omega) = \sum_{i=0}^{n} A_i(\omega)\, z^i$$

it seems that as in the scalar case we need only to find $\bar{A}(\omega)$ the left GCD of $[A_1(\omega), A_2(\omega), \cdots, A_n(\omega)]$. Then

$$A(z, \omega) = \sum_{i=0}^{n} \bar{A}(\omega)\, A_i^*(\omega)\, z^i = \bar{A}(\omega)\, A^*(z, \omega).$$

Alternatively, we can also obtain a right factor by calculating the right GCD of

$$\begin{bmatrix} A_1(\omega) \\ A_2(\omega) \\ \vdots \\ A_n(\omega) \end{bmatrix}.$$

However, it is not that simple. As a counterexample, consider the following matrix

$$A(z,\omega)=\begin{bmatrix}\omega+z^2 & \omega+z^2+z\\ z^2-z & z^2-1\end{bmatrix}=\begin{bmatrix}1&1\\1&1\end{bmatrix}z^2+\begin{bmatrix}0&1\\-1&0\end{bmatrix}z+\begin{bmatrix}\omega&\omega\\0&-1\end{bmatrix}. \quad (2.1)$$

We can easily check that there exists no nontrivial right and/or left GCD of the $A_i(\omega)$'s, therefore, there does not seem to exist such a factorization. However, it can be verified that $|A(z,\omega)|=\omega(z-1)$, and this suggests strongly that there should exist a factor whose determinant is equal to ω.[1] Therefore, the following questions arise:

Do such factorizations always exist or not?
If yes, how can they be obtained?
If yes, is the factorization unique? Or unique in a certain sense?
Does there exist a more general factorization?

In fact, there are many more such questions and they all have motivated the present research. In this section, we provide answers to all the questions raised above. These results will turn out to be of fundamental importance in finding solutions to many of the problems raised in the later sections.

First, we need to define the term "primitive."

Definition: Let $A(z,\omega)$ be a $m\times n$ polynomial matrix, $(m\leqslant n)$ then $A(z,\omega)$ is said to be *primitive* in $F[\omega][z]$ iff $A(z,\omega_0)$ is of full rank for all fixed ω_0.

By full rank, we mean that there is an $m\times m$ submatrix whose determinant is not the zero element of $F(z)$.

It is clear that in the scalar case $a(z,\omega)$ is primitive if and only if $a_0(\omega), a_1(\omega),\cdots,a_n(\omega)$ have no nontrivial common factor. However, in the matrix case, this simple relation does not hold. Note that this definition of "primitive" in the scalar case is in fact the definition used by Bocher [1] and Bose [4], while our definition provides a natural generalization to the matrix case.

Our first observation is the following lemma.

Lemma 2.1: Let $R(z,\omega)$ be a given $m\times n$ full rank 2-D polynomial matrix with

$$R=AB=CD$$

for some $m\times m$ A, $m\times n$ B, $m\times p$ C, $p\times n$ D, where $p\leqslant n$. Also assume that $|A|\in F[\omega]$ and that D is primitive. Then

$$B=A^{-1}CD\equiv ED$$

where *E is a polynomial matrix.*

Proof: Suppose that E is a rational (nonpolynomial) matrix, then there is at least one row, say the first one, which is nonpolynomial. But since F has been assumed algebraically closed, this means that there exists some ω_0 and $g(\omega)$ such that

$$E_1=\left[\frac{e_{11}(z,\omega)}{g(\omega)(\omega-\omega_0)},\frac{e_{12}(z,\omega)}{g(\omega)(\omega-\omega_0)},\cdots,\frac{e_{1p}(z,\omega)}{g(\omega)(\omega-\omega_0)}\right].$$

With $e_{1i}, i=1,\cdots,p$ not all identically zero. Hence there exists a $p\times p$ unimodular matrix in z, say $V(z)$, such that

[1] At the end of this section we shall prove the existence of a matrix primitive factorization and apply it to the example above.

$$E_1(z,\omega)V(z)=\tilde{E}_1(z,\omega)=\left[\frac{\tilde{e}_{11}(z,\omega)}{g(\omega)(\omega-\omega_0)},\cdots,\frac{\tilde{e}_{1p}(z,\omega)}{g(\omega)(\omega-\omega_0)}\right]$$

with

$$\tilde{e}_{11}(z,\omega_0)\neq 0$$

and

$$\tilde{e}_{1i}(z,\omega_0)=0,\quad i=2,\cdots,p.$$

Now we have that

$$B=\underbrace{EV}\,\underbrace{V^{-1}D}\equiv\tilde{E}F.$$

Since V^{-1} is unimodular, $F=V^{-1}D$ is also primitive. Let $B_1(z,\omega)$ be the first row of $B(z,\omega)$ and $F_i(z,\omega)$ be the ith row of $F(z,\omega)$, then

$$B_1(z,\omega)=\sum_1^p\frac{\tilde{e}_{1i}(z,\omega)}{g(\omega)(\omega-\omega_0)}F_i(z,\omega)$$

or

$$(\omega-\omega_0)g(\omega)B_1(z,\omega)=\sum_1^p\tilde{e}_{1i}(z,\omega)F_i(z,\omega). \quad (2.2)$$

Now let $\omega=\omega_0$, Equation (2.1) becomes

$$0'=\tilde{e}_{11}(z,\omega_0)F_1(z,\omega_0)$$

i.e.,

$$F_1(z,\omega_0)=0'$$

which implies that $F_1(z,\omega)$ contains the factor $(\omega-\omega_0)$, therefore, contradicting the "primitive" assumption on $F(z,\omega)$ and therefore on $D(z,\omega)$. Thus we can conclude that $E(z,\omega)$ is in fact a polynomial. ∎

This lemma will be very useful in later sections as well as in our following major theorem.

Theorem 2.2—Primitive Factorization Theorem: Let $R(z,\omega)$ be a given $m\times n$ full rank 2-D polynomial matrix, where $m\leqslant n$, then there exist a unique $\bar{R}(z,\omega)$ (modulo a right unimodular matrix) and a unique $R^*(z,\omega)$ (modulo a left unimodular matrix) with

$$|\bar{R}(z,\omega)|=\bar{r}(\omega)$$

where $\bar{r}(\omega)$ is some polynomial in ω and $R^*(z,\omega)$ is primitive in $F[\omega][z]$ such that

$$R(z,\omega)=\bar{R}(z,\omega)R^*(z,\omega).$$

Proof:

i) Existence—we prove it by the following constructive algorithm (*Primitive Factorization Algorithm*).

I. Find all the roots ω_i, which make $R(z,\omega_i)$ not full rank.

II. Since $R(z,\omega_i)$ has not full rank, the (upper triangular) Hermite form of $R(z,\omega_i)$ has its last row identically equal to zero [11].

That is to say we can find a unimodular matrix $V_1(z)$ such that

$$V_1(z)R(z,\omega_1)=\begin{bmatrix}X\\ 0\,0\,0\,0\,0\,0\,0\end{bmatrix}$$

i.e.,

$$V_1(z)\,R(z,\omega)=\begin{bmatrix}1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & (\omega-\omega_1)\end{bmatrix}[\tilde{R}]$$

for some $\tilde{R}(z,\omega)$, or

$$R(z,\omega)=\underbrace{V_1^{-1}(z)\begin{bmatrix}1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & (\omega-\omega_1)\end{bmatrix}}\tilde{R}\equiv A_1\tilde{R}.$$

Continuing the same procedure on $\tilde{R}$, we will eventually obtain a final result of the form

$$R(z,\omega)=\underbrace{A_1\;A_2\;\cdots\;A_k}\;R^*\equiv\bar{R}R^*$$

with

$$|\bar{R}|=|A_1|\,|A_2|\cdots|A_k|=\prod_{i=1}(\omega-\omega_i)=\bar{r}(\omega)$$

and $R^*(z,\omega)$ is apparently primitive (otherwise the procedure could be still continued). Q.E.D.

ii) Uniqueness: assume

$$R=\bar{R}_1R_1^*=\bar{R}_2R_2^*$$

by Lemma 2.1, taking $p=m\leqslant n$, we have

$$E=\bar{R}_1^{-1}\bar{R}_2$$

is a polynomial, conversely, $E^{-1}=\bar{R}_2^{-1}\bar{R}_1$ is also a polynomial hence $\bar{R}_1$ and $\bar{R}_2$ are related by a unimodular matrix. Q.E.D. ∎

Remark 1: In the first step of the above primitive factorization algorithm, we need to find the roots ω_i. This can be done by first taking a nonsingular minor and calculating its determinant, say $\alpha(z,\omega)$. Then we can easily factor $\alpha(z,\omega)=\bar{\alpha}(\omega)\,\alpha^*(z,\omega)$, and obtain our candidate roots from the set of roots of $\bar{\alpha}(\omega)=0$. By checking each candidate root we can pick out those making $R(z,\omega)$ not full rank and obtain the complete set of ω_i's.

Remark 2: This theorem tells us that we can always obtain a primitive factorization but it will not be as easy as in the scalar case. Also this theorem is a very powerful tool in 2-D matrix system theory as appears in the logical dependence chart in Section I.

Remark 3: We may note that this algorithm might not be ultimately the best method of finding the primitive factorization, since it requires finding roots of polynomials. By using GCRD and GCLD and the ideas above, a more efficient algorithm may be developed.

Example: Let us reconsider the matrix in (2.1), i.e.,

$$R(z,\omega)=\begin{bmatrix}\omega+z^2 & \omega+z^2+z\\ z^2-z & z^2-1\end{bmatrix}.$$

First, we shall find a left factorization. Since $\omega=0$ is a root, the corresponding unimodular matrix is

$$V_1(z)=\begin{bmatrix}-1 & 1\\ z-1 & -z\end{bmatrix}$$

i.e.,

$$V_1(z)\,R(z,\omega)=\begin{bmatrix}-\omega-z & -\omega-z-1\\ \omega(z-1 & \omega(z-1)\end{bmatrix}$$

$$=\begin{bmatrix}1 & 0\\ 0 & \omega\end{bmatrix}\begin{bmatrix}-\omega-z & -\omega-z-1\\ z-1 & z-1\end{bmatrix}.$$

Thus we have the result

$$R(z,\omega)=V_1^{-1}(z)\begin{bmatrix}1 & 0\\ 0 & \omega\end{bmatrix}\begin{bmatrix}-\omega-z & -\omega-z-1\\ z-1 & z-1\end{bmatrix}$$

$$=\begin{bmatrix}-z & -\omega\\ -z+1 & -\omega\end{bmatrix}\begin{bmatrix}-\omega-z & -\omega-z-1\\ z-1 & z-1\end{bmatrix}\equiv C(z,\omega)\,D(z,\omega).$$

It is easy to verify that $|C|=\omega$, and hence we have obtained the desired factorization. Similarly the right factorization is given by

$$R(z,\omega)=\begin{bmatrix}-z & 1\\ -z+1 & 0\end{bmatrix}\begin{bmatrix}-z & -z-1\\ \omega & \omega\end{bmatrix}.$$ ∎

III. Notion of Rational Field

One powerful approach to tackle 2-D problems is to view a 2-D polynomial

$$a(z,\omega)=\sum_{i=1}^{n}a_i(\omega)\,z^i$$

of $F[\omega][z]$ as being an element of $F(\omega)[z]$, that is to say as a 1-D polynomial in z with coefficients in the field $F(\omega)$. The field $F(\omega)$ is chosen because it contains all $a_i(\omega)$'s.

With this approach, similar results to the ones of 1-D system theory can be obtained by natural extensions.

Algorithm 3.1–2-D Euclidean Algorithm in $F[\omega][z]$ (Scalar Case): Let us denote $\mathcal{A}(z)=a(z,\omega)$, $\mathcal{B}(z)=b(z,\omega)$ with the ω part implicitly represented by the coefficients of the powers of z. Then there exist $\mathcal{Q}(z)$, $\mathcal{R}(z)$ such that

$$\mathcal{A}(z)=\mathcal{Q}(z)\,\mathcal{B}(z)+\mathcal{R}(z) \tag{3.1}$$

where $\mathcal{R}(z)$ has $\delta_z\mathcal{R}(z)<\delta_z\mathcal{B}(z)\equiv m$, denoting by $\delta_z p(z)$ the degree in z of the polynomial $p(z)$. In addition, let

$$\mathcal{Q}(z)=\frac{q_0(\omega)}{p_0(\omega)}\,z^{n-m}+\cdots+\frac{q_{n-m}(\omega)}{p_{n-m}(\omega)}\,z^0.$$

In order to renormalize (3.1) back to 2-D polynomial representation we must multiply (3.1) by a polynomial $p(\omega)$, where

$$p(\omega)=\mathrm{LCM}\,(p_0,\cdots,p_i,\cdots,p_{n-m})$$

the least common multiple of all the p_i. It is clear that

$$\mathcal{Q}(z)=\frac{1}{p(\omega)}\cdot\sum_{0}^{n-m}\tilde{q}_iz^i\equiv\frac{1}{p(\omega)}\,k(z,\omega)$$

and (3.1), after translating back to the 2-D polynomial language, becomes

$$p(\omega)\,a(z,\omega)=k(z,\omega)\,b(z,\omega)+r(z,\omega)$$

where $r(z,\omega)=p(\omega)\cdot\mathcal{R}(z)$ is certainly a 2-D polynomial. Also note that $\delta_z r(z,\omega)<m$ and that $p(\omega)$ and $k(z,\omega)$ are coprime.

Symmetrically, a 2-D Euclidean division algorithm can also be defined in $F[z][\omega]$. Thus we can find $\rho(z)$, $l(z,\omega)$, and

$s(z, \omega)$ such that

$$\rho(z)\, a(z, \omega) = l(z, \omega)\, b(z, \omega) + s(z, \omega),$$

$$\delta_\omega s(z, \omega) < \delta_\omega b(z, \omega)$$

$\rho(z)$ and $l(z, \omega)$ being coprime.

Algorithm 3.2–Hermite form w.r.t. $F[\omega][z]$: We are now interested in finding the Hermite form for a 2-D *full rank* polynomial matrix, say $m \times n$ $M(z, \omega)$. Just as we work in the 1-D case (see [16]) over the real field, we can work here over $F(\omega)$, and find $\mathcal{U}_z$ a unimodular polynomial matrix in $F(\omega)[z]$ such that if $m \geqslant n$

$$\mathcal{U}_z M = \left[\begin{array}{ccc} x & & x \\ & \ddots & \\ \bigcirc & & x \\ \hline & \bigcirc & \end{array}\right] = \left[\begin{array}{c} \mathcal{H} \\ \hline \bigcirc \end{array}\right] \tag{3.2a}$$

or if $m \leqslant n$

$$\mathcal{U}_z M = \left[\begin{array}{ccc|c} x & & x & \\ & \ddots & & X \\ \bigcirc & & x & \end{array}\right] = [\mathcal{H} | \tilde{\mathcal{H}}] \tag{3.2b}$$

where $\mathcal{H}$, $\tilde{\mathcal{H}}$ are unique, and $\delta_z \mathcal{H}_{ii} > \delta_z \mathcal{H}_{ki}$, for $k \neq i$. The renormalization to 2-D polynomial matrix is straightforward. Let $p_i(\omega) = \mathrm{LCM}$ (denominators of $[\mathcal{U}_z]_{1,i}, i = 1, \cdots, m$) and premultiply (3.2) by $\mathrm{diag}\,(p_i(\omega))$, then we have the relation that if $m \geqslant n$

$$U_z M = \left[\begin{array}{ccc} x & & x \\ & \ddots & \\ \bigcirc & & x \\ \hline & \bigcirc & \end{array}\right] = \left[\begin{array}{c} H \\ \hline \bigcirc \end{array}\right] \tag{3.3a}$$

or if $m \leqslant n$

$$U_z M = \left[\begin{array}{ccc|c} x & & x & \\ & \ddots & & X \\ \bigcirc & & x & \end{array}\right] = [H | \tilde{H}] \tag{3.3b}$$

where $U_z, H, \tilde{H}$ are 2-D polynomial matrices. This completes the derivation of the Hermite form w.r.t. $F[\omega][z]$.

Algorithm 3.3–Smith Form w.r.t. $F[\omega][z]$: As in the 1-D case, we can use unimodular transformations in z on both sides to reduce any matrix, say $M(z, \omega)$, to a 1-D Smith form over $F(\omega)$ and then renormalize both unimodular matrices by two diagonal polynomial matrices in $F[\omega]$. Hence, the following result: *Given any polynomial matrix $M(z, \omega)$, there exist two polynomial matrices $U(z, \omega)$, $V(z, \omega)$ with $|U| = \alpha(\omega)$, $|V| = \beta(\omega)$, where $\alpha(\omega)$, $\beta(\omega) \in F[\omega]$, such that we can obtain the 2-D Smith form.* If $m \geqslant n$

$$UMV = \left[\begin{array}{ccc} S_{11} & & \\ & \ddots & \\ & & S_{nn} \\ \hline & \bigcirc & \end{array}\right] \tag{3.4a}$$

or if $m \leqslant n$

$$UMV = \left[\begin{array}{ccc|c} S_{11} & & \bigcirc & \\ & \ddots & & \bigcirc \\ \bigcirc & & S_{mm} & \end{array}\right] \tag{3.4b}$$

with $S_{ii} | S_{kk}$ if $i < k$, (where $a | b$ denotes "a divides b").

Remark: H and S, the Hermite and Smith forms of M over $F[\omega][z]$ are quite different from the Hermite and Smith forms of M over $F[z][\omega]$.

Indeed, in one case, we consider first $\mathcal{H}$ and $\mathcal{S}$ the Hermite and Smith forms of M over $F(\omega)[z]$ and then we renormalize with some polynomials in ω to make H and S equivalent to M over $F[z, \omega]$, in the other case we use $F(z)[\omega]$ as the intermediate ring of polynomials and renormalize with some polynomials in z.

These examples have illustrated the great convenience of using the 2-D language of $F[z, \omega]$ and the 1-D language of $F(\omega)[z]$ or $F(z)[\omega]$ interchangeably (this idea can be extended to N-D systems). Now let us discuss the question of irreducibility of a 2-D representation and see how it can be translated to the 1-D language. Consider a 2-D rational polynomial matrix $G(z, \omega)$, it can be written as

$$G = BA^{-1}. \tag{3.5}$$

If A and B are (right) coprime, that is A, B has no nontrivial right common factor, then (3.5) is a irreducible representation. We may note that an irreducible representation has potential applications in network realization, dynamic system analysis, etc. In order to relate 2-D coprimeness to 1-D coprimeness we will make use of Theorem 3.5. However, before this theorem, we have to prove the following lemma.

Lemma 3.4: Let

$$U \left[\begin{array}{c} A \\ \hline B \end{array}\right] = \left[\begin{array}{c} R \\ \hline 0 \end{array}\right]$$

where U, A, B, R are 2-D polynomial matrices, and $|U| \in F[\omega]$. If R has a primitive (left) factorization $R = \bar{R}R^*$ in $F[\omega][z]$ then R^* is a right common factor of A and B.

Proof:

$$\left[\begin{array}{c} A \\ \hline B \end{array}\right] = U^{-1} \left[\begin{array}{c} R \\ \hline 0 \end{array}\right] = \frac{1}{\alpha(\omega)}\, \tilde{U} \left[\begin{array}{c} R \\ \hline 0 \end{array}\right]$$

where $\alpha(\omega) = |U|$ and $\tilde{U} = \mathrm{adj}\,(U)$. This can also be written as

$$[\alpha(\omega)I] \left[\begin{array}{c} A \\ \hline B \end{array}\right] = \tilde{U} \left[\begin{array}{c} R \\ \hline 0 \end{array}\right] \equiv [\tilde{U}_1 | \tilde{U}_2] \left[\begin{array}{c} R \\ \hline 0 \end{array}\right] = \tilde{U}_1 \bar{R} R^*$$

with $\tilde{U}_1$ and $\tilde{U}_2$ defined in an obvious way. Now we can apply Lemma 2.1 where we assume $p = n$. Then, we have

$$\left[\begin{array}{c} A \\ \hline B \end{array}\right] = [\alpha(\omega)I]^{-1}\, \tilde{U}_1 \bar{R} R^* \equiv [E]\, R^* \tag{3.6}$$

with E a polynomial matrix. Now (3.6) implies that R^* is a right common factor of A and B. Q.E.D. ■

Theorem 3.5: $A(z, \omega)$, $B(z, \omega)$ are 2-D right coprime w.r.t. $F[z, \omega]$ iff

A, B are 1-D right coprime w.r.t. $F(\omega)[z]$

and

A, B are 1-D right coprime w.r.t. $F(z)[\omega]$.

Remark: By A and B 2-D right coprime w.r.t. $F[z, \omega]$, we mean that there is no right common factor, say R, such that:

$$A = \tilde{A}R \qquad B = \tilde{B}R$$

$\tilde{A}$, $\tilde{B}$, R have all their entries in $F[z, \omega]$ and $\delta_z|R| > 0$ or $\delta_\omega |R| > 0$.

Proof: Necessity: Assume A, B, 2-D coprime. Suppose A, B are not 1-D coprime w.r.t., say $F(\omega)[z]$. Then there exists $\mathfrak{U}$,

$$\mathfrak{U}\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} \mathfrak{R}(z) \\ 0 \end{bmatrix} \tag{3.7}$$

where $\mathfrak{U}$, $\mathfrak{R}$ are 1-D polynomial matrices with coefficients in $F(\omega)$, $|\mathfrak{U}| \in F(\omega)$ and $\delta_z |\mathfrak{R}(z)| > 0$. Renormalizing (3.7) we have 2-D polynomial matrices U and R such that $|U| \in F[\omega]$ and

$$U\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} R \\ 0 \end{bmatrix}.$$

Let $R = \bar{R}R^*$ be a primitive factorization of R in $F[\omega][z]$. Then by Lemma 3.4, R^* is a nontrivial (i.e., $\delta_z |R^*| > 0$) right common factor of A, B – a contradiction. Hence the "necessity" part is proven.

Sufficiency: Assume A, B 1-D coprime w.r.t. $F(\omega)[z]$ and 1-D coprime w.r.t. $F(z)[\omega]$. Suppose A, B are not 2-D coprime, i.e., A, B have a nontrivial common factor, say $E(z, \omega)$, then there are two cases.

i) $|E(z, \omega)|$ contains z, then $A(z, \omega)$, $B(z, \omega)$ are not 1-D coprime in $F(\omega)[z]$ since $E(z, \omega)$ is a nontrivial 1-D common factor.

ii) $|E(z, \omega)|$ does not contain z, hence it must contain ω, then $A(z, \omega)$, $B(z, \omega)$ are not 1-D coprime w.r.t. $F(z)[\omega]$.

Hence both cases reach contradictions and the proof is completed.

Some applications of this theorem will be discussed in Section V. Next we turn to the general factorization problem.

IV. The General Factorization Theorem

In Section II, we proved that an arbitrary square matrix $R(z, \omega)$ of size m has a primitive factorization w.r.t. $F[\omega][z]$, i.e., if

$$|R(z, \omega)| = \bar{r}(\omega)\, r^*(z, \omega)$$

where $r^*(z, \omega)$ is a primitive polynomial w.r.t. $F[\omega][z]$, then by the primitive factorization algorithm, we can factor $R(z, \omega)$ as

$$R(z, \omega) = \bar{R}(z, \omega)\, R^*(z, \omega)$$

with

$$|\bar{R}| = \bar{r} \qquad |R^*| = r^*.$$

In this section we shall extend this result to the case of an arbitrary factorization, i.e., if $|R| = \Pi_1^k r_i$, then we can factor $R = \Pi_1^k R_i$ with $|R_i| = r_i$. The first step is the following lemma.

Lemma 4.1: If

$$|R| = r_1 r_2$$

we can factor R as

$$R = R_1 R_2 \text{ with } |R_i| = r_i, \quad i = 1, 2.$$

Proof: Let

$$r_i(z, \omega) = \bar{r}_i(\omega)\, r_i^*(z, \omega)$$

where $r_i^*(z, \omega)$ is a primitive polynomial for $i = 1, 2$, then by the primitive (left) factorization algorithm R can be factored as

$$R = \bar{R}_1 \tilde{R} \tag{4.1}$$

with $|\bar{R}_1| = \bar{r}_1$. Now we can apply the Smith form algorithm to $\tilde{R}(z, \omega)$

$$U(z, \omega)\, \tilde{R}(z, \omega)\, V(z, \omega) = S(z, \omega) \tag{4.2}$$

where S is diagonal, U and V are unimodular in z, then

$$S = \bar{S} S_1^* S_2^* \tag{4.3}$$

with

$$|S_i^*| = r_i^*, \qquad \text{for } i = 1, 2$$

and $\bar{S}$ is unimodular in z.

Since $U\tilde{R}V = \bar{S}S_1^*S_2^*$, where U is unimodular in z and $S_1^*S_2^*$ is primitive, by Lemma 2.1 we have

$$\tilde{R}V = \Lambda S_1^* S_2^* \tag{4.4}$$

where Λ is a polynomial matrix. But ΛS_1^* is a left primitive factorization of $M_1 = \Lambda S_1^*$. There also exists a right primitive factorization

$$M_1 = R_1^* \Lambda_1 \tag{4.5}$$

with $|R_1^*| = |S_1^*| = r_1^*$, Λ_1 being unimodular in z. Similarly $M_2 = \Lambda_1 S_2^* = R_2^* \Lambda_2$ with $|R_2^*| = |S_2^*| = r_2^*$, Λ_2 being unimodular in z, hence

$$\tilde{R}V = R_1^* R_2^* \Lambda_2. \tag{4.6}$$

Recall that V is unimodular in z and $R_1^*R_2^*$ is primitive, then by Lemma 2.1

$$\tilde{R} = R_1^* R_2^* \bar{R}_2 \tag{4.7}$$

where $\bar{R}_2$ is a polynomial matrix. But this implies that $|\bar{R}_2| = \bar{r}_2$, therefore, we get the desired result that

$$R = \bar{R}_1 R_1^* R_2^* \bar{R}_2 = R_1 R_2 \qquad (R_1 = \bar{R}_1 R_1^*,\ R_2 = R_2^* \bar{R}_2) \tag{4.8}$$

with

$$|R_i| = r_i, \qquad i = 1, 2.$$

Q.E.D. ∎

The general factorization theorem is an immediate consequence of the lemma.

Theorem 4.2: If

$$|R(z, \omega)| = \prod_1^k r_i(z, \omega)$$

where the r_i's are arbitrary polynomials, then $R(z, \omega)$ can be factored such that

$$R(z, \omega) = \prod_1^k R_i(z, \omega)$$

with

$$|R_i| = r_i.$$

Remark 1: This factorization is in general not unique (even up to unimodular matrices in z and ω), since in the 1-D case

$$\begin{bmatrix}(z+1)^2 & 0\\ 0 & (z+1)\end{bmatrix}=\begin{bmatrix}z+1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}z+1 & 0\\ 0 & z+1\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & z+1\end{bmatrix}\begin{bmatrix}(z+1)^2 & 0\\ 0 & 1\end{bmatrix}$$

and

$$\begin{bmatrix}z+1 & 0\\ 0 & z+1\end{bmatrix}$$

is not equivalent to

$$\begin{bmatrix}(z+1)^2 & 0\\ 0 & 1\end{bmatrix}.$$

Remark 2: Lemma 4.1 enables us to give a short proof to Theorem 4.2, however, if one is really interested to carry out a general factorization, instead of going $k-1$ times through the steps of Lemma 4.1, which would involve using $k-1$ Smith form decompositions, it is possible to use only one Smith form as it is shown in the algorithm presented in Appendix I.

V. Matrix Fraction Description Theorem

In this section, we discuss how to exploit Theorem 3.4 to prove the 2-D Bezout identity and then obtain a 2-D matrix fraction description (MFD) theorem.

Theorem 5.1–Bezout Identity: Let $N_R(z,\omega)$, $D_R(z,\omega)$ ($N_L(z,\omega)$, $D_L(z,\omega)$) be two polynomial matrices being right (left) coprime, then there exists a polynomial matrix in ω, say, $E_R(\omega)$ ($E_L(\omega)$), and two 2-D polynomial matrices X_R, Y_R(X_L, Y_L), such that

$$X_RD_R+Y_RN_R=E_R \tag{5.1a}$$

$$(N_LY_L-D_LX_L=E_L) \tag{5.1b}$$

Proof: By theorem 3.4, we know that N_R, D_R are also right 1-D coprime w.r.t. $F(\omega)[z]$, hence there exists $\mathfrak{X}_R(z,\omega)$, $\mathfrak{Y}_R(z,\omega)$ being polynomial in z while having coefficients in $F(\omega)$ and

$$\mathfrak{X}_RD_R+\mathfrak{Y}_RN_R=I \tag{5.2}$$

by renormalizing (5.2), we can have, for some 2-D polynomial matrices X_R, Y_R

$$X_RD_R+Y_RN_R=E_R.$$

In a similar manner we can prove (5.1b). ∎

Using the Bezout identity, we can further prove the following theorem which is a generalized version of the MFD theorem in 1-D system (see [12]).

Theorem 5.2–MFD Theorem: Given a 2-D transfer function $G(z,\omega)$, and if

$$G=N_RD_R^{-1}=D_L^{-1}N_L$$

with N_R, D_R right coprime, and N_L, D_L left coprime, then

$$|D_R|=|D_L|$$

Proof: From (5.1a, b) and noting that $N_LD_R-D_LN_R=0$ we have

$$\begin{bmatrix}X_R & Y_R\\ N_L & -D_L\end{bmatrix}\begin{bmatrix}D_R & Y_L\\ N_R & X_L\end{bmatrix}\equiv UV=\left[\begin{array}{c|c}E_R & W\\ \hline 0 & E_L\end{array}\right]$$

where U, V are defined in an obvious way and $W=X_RY_L+Y_RX_L$, therefore,

$$|U||V|=|E_R||E_L|=e_R(\omega)\cdot e_L(\omega)$$

hence

$$|U|=\alpha(\omega)$$

and

$$|V|=\beta(\omega)$$

for some polynomial $\alpha(\omega)$ and $\beta(\omega)$. Now we have

$$U\begin{bmatrix}D_R & 0\\ N_R & I\end{bmatrix}=\begin{bmatrix}E_R & Y_R\\ 0 & -D_L\end{bmatrix}$$

taking determinants of both sides,

$$|U||D_R|=-|E_R(\omega)|\cdot|D_L|$$

or

$$\alpha(\omega)|D_R|=-e_R(\omega)|D_L|. \tag{5.3a}$$

By symmetry we can also obtain the relation

$$\overline{\alpha}(z)|D_R|=-\overline{e}_R(z)|D_L|. \tag{5.3b}$$

It is obvious that (5.3a, b) imply $|D_R|=|D_L|$.

Corollary: From the above theorem, by (5.3a) and the fact that $|D_L|=|D_R|$, we conclude that $|U|=e_R$, and similarly $|V|=e_L$. The following lemma is a generalization of a 1-D result (see [14]).

Lemma 5.3: Given 2-D polynomial matrices V, T, F and let $P=VT^{-1}F$. Now, if V and T are right coprime then P is a polynomial matrix if and only if $T^{-1}F$ is a polynomial matrix.

Proof: The "if" part is trivial. "Only if" part: Since V and T are coprime, then by Theorem 5.1, there exists X, Y such that

$$XT+YV=E(\omega)$$

Postmultiplying by $T^{-1}F$, we obtain

$$XF+YP=E(\omega)T^{-1}F \tag{5.4}$$

And since P is a polynomial matrix, $T^{-1}F=E^{-1}(\omega)(XF+YP)$ is a polynomial matrix in z with coefficients in $F(\omega)$.

By symmetry between z and $\omega T^{-1}F$ is also a polynomial matrix in ω with coefficients in $F(z)$.

Hence $T^{-1}F$ is a polynomial matrix in z and ω.

With this lemma, we are now ready to prove the following potentially very useful theorem.

Theorem 5.4: Let

$$N_RD_R^{-1}=D_L^{-1}N_L$$

both being irreducible, as well as $D_R^{-1}B$. Then

$$[D_L,N_LB]$$

are (left) coprime.

Proof: Assume D_L, N_LB are not coprime, therefore, $D_L^{-1}N_LB$ can be reduced:

$$D_L^{-1}(N_LB)=\tilde{N}\tilde{D}^{-1}$$

and

$$N_RD_R^{-1}B\tilde{D}=\tilde{N}$$

hence by Lemma 5.3

$$D_R^{-1}B\tilde{D}=K$$

where K is a polynomial matrix, then

$$D_R^{-1} B = K\tilde{D}^{-1} \tag{5.5}$$

However, $\tilde{D}$ has a determinantal degree less than the one of D_R, hence (5.5) contradicts the assumption that $D_R^{-1} B$ is irreducible. Q.E.D. ∎

Theorem 5.5: Let

$$VT^{-1}U = ND^{-1}$$

With T, U being left coprime and (T, V), (D, N) both being right coprime then

$$|T| = |D|$$

Proof: Let $T_L^{-1} V_L$ be an irreducible left MFD of VT^{-1}, then by Theorem 5.2,

$$|T_L| = |T|.$$

Also

$$VT^{-1}U = T_L^{-1} V_L U = ND^{-1}$$

and, by Theorem 5.4, T_L and $V_L U$ are left coprime, therefore, again by Theorem 5.2,

$$|T_L| = |D|.$$

This completes the proof. ∎

One application of the above theorem is to the problem of determining minimality of a state-space model implementation [10]. As in the 1-D case, a system is called minimal iff the transfer function is in an irreducible form, i.e., the order (n, m) of the system is equal to (p, q) where p and q are the dimensions of horizontal and vertical states, respectively. More details can be found in Part II of this paper.

VI. The GCRD Extraction Algorithm

Given two scalar 2-D polynomials or two 2-D matrix polynomials, here we are only interested in two types of questions as far as their relative primeness is concerned:

i) Are they left or right coprime?
ii) What is their (left-right) GCD?

In the scalar case Bose [3] has proposed a test to check if 2-D polynomials are relatively prime. We shall present an extension of the Sylvester test on the first part of this section that is closely connected with Bose's test.

In Section VII Rosenbrock's criterion for relative primeness of polynomial matrices is extended to the 2-D case.

In the problem of GCD extraction Bocher [1] or Bose [4] provide some ways of extracting the GCD of two scalar polynomials. In the second part of this section an algorithm will be presented for the extraction of the GCRD of two polynomial matrices. These results will be needed to properly answer questions i) and ii) presented above.

A. Sylvester's Test of Relative Primeness of Two 2-D Polynomials

Let $a(z, \omega)$ and $b(z, \omega)$ be two scalar 2-D polynomials with

$$\delta_z a = \bar{n},\ \delta_\omega a = n^*,\ \delta_z b = \bar{m},\ \delta_\omega b = m^*$$

$$a(z, \omega) = \sum_0^{\bar{n}} a_i(\omega) z^{\bar{n}-i},\quad b(z, \omega) = \sum_0^{\bar{m}} b_i(\omega) z^{\bar{m}-i}. \tag{6.1}$$

Since

$$\delta_\omega a = n^*,\ \delta_\omega a_i \leq n^*, \qquad \text{for } i = 1, \cdots, \bar{n}$$

(with strict equality for at least one of them). Hence

$$a_i(\omega) = \sum_0^{n^*} a_{ij}\,\omega^{n^*-j}. \tag{6.2}$$

Similarly

$$\delta_\omega b_i \leq m^*, \qquad \text{for } i = 1, \cdots, \bar{m}$$

with

$$b_i(\omega) = \sum_0^{m^*} b_{ij}\,\omega^{m^*-j}$$

Theorem 6.1: $a(z, \omega)$ and $b(z, \omega)$ are relatively prime iff $R^z(a, b)$ and $R^\omega(a, b)$ are full rank

$R^z(a, b)$

$$= \left[\begin{array}{cccccc}
\mathcal{A}_0^z & \mathcal{A}_1^z & \cdots & \mathcal{A}_{\bar n}^z & & \bigcirc \\
 & \ddots & \ddots & & \ddots & \\
\bigcirc & & \mathcal{A}_0^z & \mathcal{A}_1^z & \cdots & \mathcal{A}_{\bar n}^z \\
 & \mathcal{B}_0^z & \mathcal{B}_1^z & \cdots & & \mathcal{B}_{\bar m}^z \\
 & \ddots & & & \ddots & \\
\mathcal{B}_0^z & \mathcal{B}_1^z & \cdots & \mathcal{B}_{\bar m}^z & & \bigcirc
\end{array}\right]
\begin{array}{l}
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \bar m \\
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \bar n
\end{array} \tag{6.3}$$

with

$$\mathcal{A}_i^z = \underbrace{\left[\begin{array}{ccccccc}
a_{i0} & a_{ij} & a_{in^*} & & \bigcirc \\
 & \ddots & \ddots & \ddots & \\
\bigcirc & & a_{i0} & a_{ij} \cdots & a_{in^*}
\end{array}\right]}_{n^* + m^* + 1}
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} m^* + 1$$

$$\mathcal{B}_i^z = \underbrace{\left[\begin{array}{ccccc}
\bigcirc & b_{i0} & b_{ij} \cdots & b_{im^*} & \\
 & \ddots & \ddots & \ddots & \bigcirc \\
b_{i0} & b_{ij} & \cdots & b_{im^*} &
\end{array}\right]}_{n^* + m^* + 1}
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} n^* + 1$$

and $R^\omega(a, b) =$

$$\left[\begin{array}{cccccc}
\mathcal{A}_0^\omega & \mathcal{A}_1^\omega & \cdots & \mathcal{A}_{\bar n}^\omega & & \bigcirc \\
 & \ddots & \ddots & & \ddots & \\
\bigcirc & & \mathcal{A}_0^\omega & \mathcal{A}_1^\omega & \cdots & \mathcal{A}_{\bar n}^\omega \\
 & \mathcal{B}_0^\omega & \mathcal{B}_1^\omega & \cdots & & \mathcal{B}_{\bar m}^\omega \\
 & \ddots & & & \ddots & \\
\mathcal{B}_0^\omega & \mathcal{B}_1^\omega & \cdots & \mathcal{B}_{\bar m}^\omega & & \bigcirc
\end{array}\right]
\begin{array}{l}
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \bar m + 1 \\
\left.\begin{array}{c} \\ \\ \\ \end{array}\right\} \bar n + 1
\end{array}$$

with

$$\mathcal{A}_i^\omega = \underbrace{\left.\begin{bmatrix} a_{i0} & & a_{ij} & \cdots & a_{in^*} & & 0 \\ & \ddots & & \ddots & & \ddots & \\ 0 & & a_{i0} & & a_{ij} & \cdots & a_{in^*} \end{bmatrix}\right\} m^*}_{n^*+m^*}$$

$$\mathcal{B}_i^\omega = \underbrace{\left.\begin{bmatrix} & & b_{i0} & & b_{ij} & \cdots & b_{im^*} \\ & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & 0 \\ b_{i0} & & b_{ij} & \cdots & b_{im^*} & & \end{bmatrix}\right\} n^*}_{n^*+m^*}$$

$R^z(a,b)$ and $R^\omega(a,b)$ have a block Toeplitz of Toeplitz matrix structure, they are obtained from the same matrix $R(a,b)$ either by deleting the top and bottom block or by deleting the top (or bottom) line of each block. The block sizes and the number of blocks of these matrices are of particular importance.

Proof: If a and b are not relatively prime they have a common factor $q(z,\omega)$ such that either $\delta_z q \geq 1$ or $\delta_\omega q \geq 1$. In the first case

$$\begin{aligned} a(z,\omega) &= q(z,\omega)\,\tilde{a}(z,\omega), \qquad \delta_z\tilde{a} \leq \bar{n}-1 \\ b(z,\omega) &= q(z,\omega)\,\tilde{b}(z,\omega), \qquad \delta_z\tilde{b} \leq \bar{m}-1 \end{aligned} \tag{6.5}$$

where

$$\tilde{a}(z,\omega) = \sum_0^{\bar{n}-1} \tilde{a}_i(\omega)\, z^{\bar{n}-1-i}$$

and

$$\tilde{b}(z,\omega) = \sum_0^{\bar{m}-1} \tilde{b}_i(\omega)\, z^{\bar{m}-1-i}$$

with

$$\delta_\omega \tilde{a}_i \leq n^* \qquad \delta_\omega \tilde{b}_i \leq m^*.$$

But, then

$$\tilde{b}(z,\omega)\,a(z,\omega) - \tilde{a}(z,\omega)\,b(z,\omega) = 0$$

or

$$[\tilde{b}_0(\omega), \cdots, \tilde{b}_{\bar{m}-1}(\omega), -\tilde{a}_{\bar{n}-1}(\omega), \cdots, -\tilde{a}_0(\omega)]$$

$$\times \underbrace{\begin{bmatrix} \left.\begin{matrix} a_0(\omega) & & a_1(\omega) & \cdots & a_{\bar{n}}(\omega) & & \\ & \ddots & & \ddots & & \ddots & \\ & & a_0(\omega) & & a_1(\omega) & \cdots & a_{\bar{n}}(\omega) \end{matrix}\right\} \bar{m} \\ \left.\begin{matrix} & & b_0(\omega) & & b_1(\omega) & \cdots & b_{\bar{m}}(\omega) \\ & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & & \cdot^{\cdot^{\cdot}} & \\ b_0(\omega) & & b_1(\omega) & \cdots & b_{\bar{m}}(\omega) & & \end{matrix}\right\} \bar{n} \end{bmatrix}}_{\bar{n}+\bar{m}}$$

$$= [0, \cdots, 0]. \tag{6.6}$$

Hence

$$[\tilde{b}_0, \cdots, \tilde{b}_{\bar{m}-1}, -\tilde{a}_{\bar{n}-1}, \cdots, -\tilde{a}_0]\, R^z(a,b) = [0, \cdots, 0] \tag{6.7}$$

where

$$\tilde{b}_i = [\tilde{b}_{i0}, \cdots, \tilde{b}_{im^*}]$$

and

$$\tilde{a}_i = [\tilde{a}_{in^*}, \cdots, \tilde{a}_{i0}]$$

so that $R^z(a,b)$ is not full rank. Similarly if $\delta_\omega q \geq 1$ then $R^\omega(a,b)$ is not full rank. Reciprocally, if $R^z(a,b)$ is not full rank, equation (6.7) has a solution and it is easy to check that a and b have a common factor q with $\delta_\omega q \geq 1$.

B. GCD Extraction of Polynomial Matrices

The following theorem provides a constructive GCD algorithm and a complete proof of the extraction of GCD's of 2-D polynomial matrices.

Theorem 6.2—GCD Extraction Theorem: Given two 2-D polynomial matrices $A(z,\omega)$ and $B(z,\omega)$, we can obtain their GCD by the following three steps.

i) Use the primitive factorization algorithm w.r.t. $F[\omega][z]$ on the right side, i.e., find A^*, B^* and R_0 such that

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} A^* \\ B^* \end{bmatrix} R_0$$

with

$$\begin{bmatrix} A^* \\ B^* \end{bmatrix}$$

being primitive in $F[\omega][z]$

ii) Apply Algorithm 3.2 (2-D Hermite form),

$$U \begin{bmatrix} A^* \\ B^* \end{bmatrix} = \begin{bmatrix} R \\ 0 \end{bmatrix} \tag{6.8}$$

where $|U| = u(\omega)$ for some polynomial in ω and R is in Hermite form w.r.t. $F[\omega][z]$;

iii) Use the primitive factorization algorithm (on the left) of R,

$$R = \bar{R}R^* \tag{6.9}$$

now $D = R^*R_0$ is the GCRD of A and B.

Proof: The step i) is quite straightforward, hence all we need to show is that R^* is a GCRD of A^* and B^*. By Lemma 3.4, we have already shown that R^* is a CRD of A^*, B^*. Now we need only to prove R^* is divisible by any CRD of A^* and B^*. Assume D^* is any CRD of A^* and B^*, our goal is to prove that R^* and D^* are related by some polynomial matrix.

Since D^* is a CRD we have that

$$\begin{bmatrix} A^* \\ B^* \end{bmatrix} = \begin{bmatrix} \tilde{A} \\ \tilde{B} \end{bmatrix} D^*.$$

Let

$$U = \left[\begin{array}{c|c} U_1 & U_2 \\ \hline U_3 & U_4 \end{array}\right]$$

and using (6.8), we get

$$\begin{bmatrix} R \\ 0 \end{bmatrix} = U \begin{bmatrix} A^* \\ B^* \end{bmatrix} = U \begin{bmatrix} \tilde{A} \\ \tilde{B} \end{bmatrix} D^* = \begin{bmatrix} CD^* \\ 0 \end{bmatrix} \tag{6.10}$$

where

$$C = U_1 \tilde{A} + U_2 \tilde{B}.$$

Now by (6.9) and (6.10), we have

$$R = \breve{R} R^* = CD^*$$

and since the left factorization is a primitive factorization, by Lemma 2.1 we can conclude that

$$R^* = \breve{R}^{-1} CD^* = ED^*$$

where E is a polynomial, thus completing the proof. ∎

VII. A Criterion of Relative Primeness of 2-D Polynomial Matrices

In the 1-D case, a theorem of Rosenbrock's (see [10, pp. 71-72]) provides a criterion of relative primeness, we repeat it here for convenience.

Theorem 7.1-(Rosenbrock): $A(z)$ and $B(z)$ which are, respectively, $(n \times n)$ and $(m \times n)$ polynomial matrices are right coprime iff

$$\rho \begin{bmatrix} A(z) \\ B(z) \end{bmatrix} = n, \qquad \text{for all } z \in \mathcal{C}. \qquad ∎$$

Or equivalently for all $z_0 \in \mathcal{C}$ such that $|A(z_0)| = 0$, where the z_0 can be viewed as generic points as we shall see.

We shall derive a similar theorem in the 2-D case. However, the terminology is a little bit more involved and familiarity is assumed with some algebraic geometry notions, as presented for example in Hodge and Pedoe [13], and with the theory of polynomials of several variables (see Van Der Waerden [2, vol. 2, ch. 16]).

We assume that $A(z, \omega)$ and $B(z, \omega)$ are polynomial matrices of size $(n \times n)$ and $(m \times n)$. The coefficients are taken over the field F ($\mathcal{R}$ or $\mathcal{C}$) and we assume that $|A(z, \omega)| \not\equiv 0$ in $F[z, \omega]$.

Then, let Σ be a universal extension field of F (universal: all the extension fields that we shall consider will be contained in Σ (see [13])).

So that $|A(z, \omega)| = 0$ defines an algebraic curve V (i.e., an algebraic variety of dimension 1) in Σ^2.

Now if

$$|A(z, \omega)| = \prod_{i=1}^{k} a_i(z, \omega)$$

with the a_i's being irreducible polynomials over F, the a_i's generate the irreducible algebraic curves V_i in Σ^2 and

$$V = \bigcup_i V_i \tag{7.1}$$

this decomposition being unique. Then we can extend Rosenbrock's theorem as follows.

Theorem 7.2: $A(z, \omega)$ and $B(z, \omega)$ are right coprime iff

$$\rho \begin{bmatrix} A(\xi_1, \xi_2) \\ B(\xi_1, \xi_2) \end{bmatrix} = n \tag{7.2}$$

for any generic point (ξ_1, ξ_2) of any irreducible algebraic curve W of Σ^2 (or equivalently for any generic point (ξ_1, ξ_2) of V_i, V_i being one of the irreducible algebraic curves appearing in the decomposition 7.1).

Remark 1: This test applies to algebraic curves, i.e., algebraic varieties of dimension 1, but not to points, i.e., algebraic varieties of dimension 0. A natural extension for polynomial matrices $A(z_1, z_2, \cdots, z_n)$ and $B(z_1, z_2, \cdots, z_n)$ of n variables is that they are right coprime iff

$$\rho \begin{bmatrix} A(\xi_1, \xi_2, \cdots, \xi_n) \\ B(\xi_1, \xi_2, \cdots, \xi_n) \end{bmatrix} = n$$

for any generic point $(\xi_1, \xi_2, \cdots, \xi_n)$ of any irreducible algebraic variety of dimension $n - 1$ in Σ^n (or equivalently for any generic point $(\xi_1, \xi_2, \cdots, \xi_n)$ of V_i). So that in this case we do not consider the algebraic varieties of dimension lower than $n - 1$.

Remark 2: When $n = 1$ we obtain Rosenbrock's theorem. Indeed varieties of dimension 0 are finite sets of points. In this case:

If $F = \mathcal{C}$ the irreducible varieties are the isolated points $z_0 \in \mathcal{C}$.

If $F = \mathcal{R}$ the irreducible varieties are either isolated points $z_0 \in \mathcal{R}$ or conjugate points $(z_0, \bar{z}_0)$ of $\mathcal{C}$.

In both cases it is enough to take the universal field Σ as being $\mathcal{C}$ and any point of an irreducible variety is generic. So that we get back Rosenbrock's test.

Remark 3: The introduction of the universal field Σ is motivated by the following reasons: First it ensures that algebraic curves are really curves; i.e., in $\mathcal{R}^2$, $V = \{(z, \omega): z^2 + \omega^2 = 0\}$ is only the point $(0, 0)$ while in $\mathcal{C}^2$ we obtain the two lines $z + i\omega$, $z - i\omega$. Also since a generic point (ξ_1, ξ_2) of an irreducible algebraic curve is a point of F_*^2 where F_* is an extension field of F and since $F_* \subseteq \Sigma$ (Σ is universal), all the generic points that we shall consider are points in Σ^2.

Proof of the Theorem: Suppose that

$$\begin{bmatrix} A(z, \omega) \\ B(z, \omega) \end{bmatrix}$$

are not right coprime. Then

$$\begin{bmatrix} A(z, \omega) \\ B(z, \omega) \end{bmatrix} = \begin{bmatrix} \bar{A}(z, \omega) \\ \bar{B}(z, \omega) \end{bmatrix} D(z, \omega) \tag{7.3}$$

where $|D(z, \omega)|$ has at least one irreducible nontrivial factor $d_0(z, \omega)$ (nonconstant). However, since $|A| = |\bar{A}||D|$, d_0 is also one of the irreducible factors appearing in the decomposition of $|A|$, say a_{i_0} and its associated irreducible algebraic curve V_{i_0}.

Now, let (ξ_1, ξ_2) be a generic point of V_{i_0} (we know that we can find one since V_{i_0} is irreducible), with $\xi_i \in F_*$. Then

$$|D(\xi_1, \xi_2)| = 0 \text{ in } F_*$$

but this implies that

$$\rho \begin{bmatrix} A(\xi_1, \xi_2) \\ B(\xi_1, \xi_2) \end{bmatrix} < n$$

(the notion of rank is defined in the extension field F_*).

Conversely, assume that there is an irreducible algebraic curve W and (ξ_1, ξ_2) a generic point of this curve such that

$$\rho \begin{bmatrix} A(\xi_1, \xi_2) \\ B(\xi_1, \xi_2) \end{bmatrix} < n.$$

We assume also that the curve W is not a parallel to the z axis (i.e., of the type $W = \{\omega = \omega_0 \text{ fixed}, z \text{ arbitrary}\}$). Indeed if it was, it would not be a parallel to the ω axis and the following argument could be carried out by interchanging the roles of ω and z.

Now, using the Hermite form algorithm (Algorithm 3.2) w.r.t. $F[\omega][z]$

$$U(z,\omega)\begin{bmatrix} A(z,\omega) \\ B(z,\omega) \end{bmatrix} = \begin{bmatrix} D(z,\omega) \\ 0 \end{bmatrix} \tag{7.4}$$

and $|U(z,\omega)| = u(\omega)$. Now, let $u(\omega) = \Pi_i u_i(\omega)$ where the u_i's are irreducible polynomials and U the variety associated to $u(\omega): U = \cup_i U_i$ is a union of parallels to the z axis.

Now, $U(\xi_1, \xi_2)$ has full rank in F_*, otherwise since (ξ_1, ξ_2) is a generic point of W, $|U(\xi_1, \xi_2)| = 0$ implies that $|U(z,\omega)| = 0$ over W. This would imply that $W \subseteq U$, an impossibility since W is not a parallel to the z axis. Hence,

$$\rho\begin{bmatrix} A(\xi_1,\xi_2) \\ B(\xi_1,\xi_2) \end{bmatrix} = \rho\begin{bmatrix} D(\xi_1,\xi_2) \\ 0 \end{bmatrix} \text{ in } F_* \tag{7.5}$$

but if

$$\rho\begin{bmatrix} A(\xi_1,\xi_2) \\ B(\xi_1,\xi_2) \end{bmatrix} < n \text{ this implies that } |D(\xi_1,\xi_2)| = 0.$$

However, (ξ_1, ξ_2) is a generic point of W or equivalently $|D(z,\omega)| = 0$ over W. Therefore, since W is an irreducible algebraic curve, the ideal of the polynomials of $F[z,\omega]$ vanishing on W is a principal ideal. Indeed (see Van Der Waerden [2]) any $n-1$ dimensional prime ideal of $F[z_1, \cdots, z_n]$ is principal.

Let $g(z,\omega)$ be its generator, g is an irreducible primitive polynomial and is nonconstant. Then $g(z,\omega)$ divides $|D(z,\omega)|$, but this implies that if we consider the primitive factorization $D = \bar{D}D^*$ in $F[\omega][z]$ (i.e., $|\bar{D}(z,\omega)| = \bar{d}(\omega)$ and D^* is primitive) g must divide $|D^*|$. Hence the GCRD of A and B is nonunimodular and A and B are not right coprime. Q.E.D. ■

In order to get a better understanding of the previous ideas, let us consider an example that will provide some insight into the notion of generic points and illustrate Rosenbrock's test.

A. Example of Generic Points

Let V be the algebraic curve defined by $z^2 + \omega^2 - 1 = 0$, then $\xi = (z(\theta), \omega(\theta)) = (\cos\theta, \sin\theta)$ is a generic point. Its coordinates belong to the extension field

$$F_* = \left\{ \frac{p(\cos\theta, \sin\theta)}{q(\cos\theta, \sin\theta)} \right\}$$

(the field of ratios of trigonometric polynomials). Now if $p(z,\omega)$ is a 2-D polynomial such that $p(\cos\theta, \sin\theta) = 0$ in F_* then

$$p(z,\omega) = (z^2 + \omega^2 - 1)\,\tilde{p}(z,\omega).$$

Another generic point would be $\eta = (z, \sqrt{1-z^2})$ and its extension field is

$$F_* = \left\{ \frac{p_0(z) + \sqrt{1-z^2}\,p_1(z)}{q_0(z) + \sqrt{1-z^2}\,q_1(z)} \right\}$$

where $p_0, p_1, q_0, q_1 \in F[z]$.

B. Example of Rosenbrock's Test

Now, if

$$A(z,\omega) = \begin{bmatrix} z+1 & \omega \\ -\omega & z-1 \end{bmatrix}, \quad B(z,\omega) = [z - \omega^2 + 1 \quad \omega z]$$

let us prove that A and B are not right coprime. The determinant of $A(z,\omega)$ is given by $|A| = z^2 + \omega^2 - 1$, so that V is the only algebraic curve appearing in the decomposition of $|A|$. Therefore, we can write

$$\begin{bmatrix} A(\cos\theta, \sin\theta) \\ B(\cos\theta, \sin\theta) \end{bmatrix} = \begin{bmatrix} \cos\theta + 1 & \sin\theta \\ -\sin\theta & \cos\theta - 1 \\ \cos\theta(\cos\theta + 1) & \sin\theta\cos\theta \end{bmatrix}$$

but

$$\begin{bmatrix} A(\cos\theta, \sin\theta) \\ B(\cos\theta, \sin\theta) \end{bmatrix} \begin{bmatrix} \sin\theta \\ -(\cos\theta + 1) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

so that

$$\rho\begin{bmatrix} A(\cos\theta, \sin\theta) \\ B(\cos\theta, \sin\theta) \end{bmatrix} < 2$$

and from Theorem 7.2 we conclude that A and B are not coprime.

APPENDIX I

In the primitive factorization algorithm w.r.t. $F[\omega][z]$, we extracted the roots of $\bar{r}(\omega)$ one by one, therefore we can extend the result of Section II to the following trivial statement.

Lemma A.1: If $|R(z,\omega)| = \Pi_1^k \bar{r}_i(\omega)\, r^*(z,\omega)$ where r^* is a primitive polynomial w.r.t. $F[\omega][z]$, then $R(z,\omega)$ can be factored as follows

$$R(z,\omega) = \prod_1^k \bar{R}_i(z,\omega)\, R^*(z,\omega)$$

with

$$|\bar{R}_i| = \bar{r}_i \qquad |R^*| = r^*.$$

Proof: We extract the roots of $\bar{r}_1$ first, then the roots of $\bar{r}_2$ (one by one) and so on. The corresponding matrices are $\bar{R}_1, \bar{R}_2, \cdots, \bar{R}_k$, the residual matrix being R^*.

This result is just a special case of the general factorization theorem given earlier. We restate it here and give a different proof (more efficient algorithmically) using the approach of Lemma A.1.

Theorem A.2: If

$$|R| = \prod_1^k r_i \tag{A.1}$$

where the r_i's are arbitrary polynomials then R can be factored such that

$$R = \prod_1^k R_i, \quad |R_i| = r_i. \tag{A.2}$$

Proof: i) We assume first that R is a primitive polynomial matrix w.r.t. $F[\omega][z]$ so that $r = |R|$ is primitive and all the r_i's are primitive. Then $URV = S$ the Smith Form of R with $|U| = u(\omega)$, $|V| = v(\omega)$, S being diagonal. And $S = \bar{S}S^*$ is the primitive factorization of S and since S^* is primitive $|S^*| = |R| = \Pi_1^k r_i$. S^* being diagonal, it can be factored as

$$S^* = \prod_1^k S_i^*, \qquad |S_i^*| = r_i$$

So that

$$URV = \overline{S} \prod_1^k S_i^*$$

and by Lemma 2.1

$$RV = \Lambda \prod_1^k S_i^*$$

where Λ is a polynomial matrix. Now, if we set $\Lambda_0 = \Lambda$, and if Λ_{i-1} is unimodular in z, then

$$M_i = \Lambda_{i-1} S_i^* = R_i \Lambda_i, \quad i = 1, \cdots, k \tag{A.3}$$

are, respectively, the left and right primitive factorization of M_i, so that

$$|R_i| = |S_i^*| = r_i$$

and Λ_i is unimodular in z. Hence

$$RV = \left(\prod_1^k R_i\right) \Lambda_k$$

and by Lemma 2.1

$$R = \left(\prod_1^k R_i\right) W \tag{A.4}$$

W being a unimodular matrix in z and ω. This completes the proof in the case where R is primitive.

ii) If R is not primitive w.r.t. $F[\omega][z]$, let

$$r_i(z, \omega) = \overline{r}_i(\omega)\, r_i^*(z, \omega)$$

r_i^* being primitive, then

$$r = \overline{r}(\omega)\, r^*(z, \omega)$$

with

$$\overline{r} = \prod_1^k \overline{r}_i \qquad r^* = \prod_1^k r_i^*.$$

With Lemma A.1, we can factor R as

$$R = \prod_1^k \overline{R}_i R^*, \qquad |\overline{R}_i| = \overline{r}_i$$

R^* being primitive. Now, using the first part of the proof R^* can be factored as

$$R^* = \prod_1^k R_i^*, \qquad |R_i^*| = r_i^*.$$

So that

$$R = \left(\prod_1^k \overline{R}_i\right)\left(\prod_1^k R_i^*\right). \tag{A.5}$$

By interchanging left and right primitive factorization like in (A.3) we can interleave the $\overline{R}_i$ and R_i^* so that

$$R = \prod_1^k R_i, \qquad \text{with } |R_i| = r_i$$

thus completing the alternate proof of the general factorization theorem. Algorithmically this proof uses only one Smith form factorization and provides an alternative approach to the one given in Section IV.

References

[1] M. Bocher, *Introduction to Higher Algebra*. New York: Macmillan, 1907.

[2] B. L. Van Der Waerden, *Algebra*, 7th ed. (2 volumes). New York: Frederick Ungar Publishing Co., 1970.

[3] N. K. Bose, "A criterion to determine if two multivariable polynomials are relatively prime," *Proc. IEEE*, vol. 60, pp. 134–135, Jan. 1972.

[4] N. K. Bose, "An algorithm for GCF extraction from two multivariable polynomials," *Proc. IEEE*, vol. 64, no. 1, pp. 185–186, Jan. 1976.

[5] N. K. Bose and E. I. Jury, "Positivity and stability tests for multidimensional filters (discrete-continuous)," *IEEE Trans. Acoustics, Speech, and Signal Processing*, vol. ASSP-22, pp. 174–180, June 1974.

[6] S. Attasi, "Modélisation et Traitement des suites à deux indices," *Rapport IRIA*, Sept. 1975.

[7] E. Fornasini and G. Marchesini, "Algebraic realization theory of two dimensional filters," in *Variable Structure Systems*, A. Ruberti and R. Mohler, Eds. (Springer Lecture Notes in Economics and Mathematical Systems). New York: Springer Verlag, 1975.

[8] D. D. Givone and R. P. Roesser, "Minimization of multidimensional linear iterative circuits," *IEEE Trans. Comput.*, vol. C-22, pp. 673–678, July 1973.

[9] C. C. MacDuffee, *The Theory of Matrices*. New York: Chelsea, 1946.

[10] H. H. Rosenbrock, *State-Space and Multivariable Theory*. New York: Wiley, 1970.

[11] W. A. Wolovich, *Linear Multivariable Systems*. New York: Springer-Verlag, 1974.

[12] G. D. Forney, Jr., "Minimal bases of rational vector spaces with applications to multivariable linear systems," *SIAM J. Control*, vol. 13, pp. 493–520, May 1975.

[13] W. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, (3 volumes). Cambridge, England: Cambridge Univ. Press, 1947.

[14] W. A. Wolovich, "The application of state feedback invariants to exact model matching," in *Proc. 5th Ann. Princeton Conf. Information Sciences and Systems*, pp. 387–392, Mar. 1971.

[15] D. C. Youla, "The synthesis of networks containing lumped and distributed elements," in *Proc. Symp. Generalized Networks* (Polytechnic Institute of Brooklyn), 1966.

[16] F. R. Gantmakher, *Theory of Matrices*. New York: Chelsea Publishing Co., 1959.