On the relevance of some primeness properties in the analysis of nD finite support behaviors

Ettore Fornasini and Maria Elena Valcher*
Dip. Elettronica ed Informatica - Univ. di Padova
via Gradenigo 6a, 35131 Padova, ITALY

Abstract **Finite support nD output behaviors are discussed and various connections with primeness notions of nD FIR transfer functions are investigated.**

1. Introduction

Polynomial matrices in one variable constitute a fundamental tool for analysing the trajectories a linear 1D system generates. As a matter of fact, virtually any notion of Willems behavior theory [1] mirrors into an algebraic property of some 1D polynomial matrix and most results are couched in polynomial terms.
Quite recently P.Rocha and J.C. Willems [2] resorted to polynomial matrices in two variables for investigating 2D behaviors. As expected, the richer structure a family of trajectories on $\mathbf{Z} \times \mathbf{Z}$ is endowed with constitutes the natural counterpart of the higher complexity that 2D polynomial rings and matrices exhibit in comparison with their 1D analogs.

Somehow unexpectedly, however, the transition from 2D to nD still deserves a conspicuous interest. Actually, when $n \geq 3$, new phaenomena arise (as pointed out by D.Youla in [3]) involving the primeness definitions of polynomial matrices. This constitutes an important warning that nD behaviors should admit a a finer description based on new internal features, which make their appearance only when $n > 2$.

In this comunication we provide a preliminary report on some researches aiming to relate the structure of nD systems with the algebra of nD polynomial matrices used in their description. For sake of simplicity, we confine ourselves to nD systems with finite impulse response,and concentrate our analysis on their output trajectories.
This viewpoint is commonly adopted in convolutional coding theory, where the interest is in the code produced by an encoder rather than in the machinery underlying its generation. It turns out to be of great relevance also in fault detection problems, whenever the output trajectories are the only information we possess to check whether a system behaves correctly. It is easy to realize that many questions connected with the existence and the realizability of residual generators or decoders (and, in general, of inverse systems) can be answered only if we are provided with enough information on the output trajectories and the way they are produced by input-output maps.

In a 1D context the polynomial matrix algebra one applies for solving the aforementioned problems is rather simple and provides efficient algorithms, (based on elementary transformations), that allow for a complete analysis of the system dynamics. The algebra of nD polynomial matrices is much more difficult. As previously mentioned, there are several primeness notions (zero-primeness, p-primeness, minor-primeness and factor-primeness [4]), each of them implying the following one, without beeing implied by it. Moreover, up to now no algebraic algorithm is available to check factor-primeness, which makes this property rather elusive. Last but not least, the complexity of the presently available algorithms represents a serious drawback when trying to get an intuition on possible solutions to the open problems.

The paper is organized as follows. In the next section we translate very natural requirements on a set of nD finite support output trajectories into primeness conditions on the polynomial transfer functions. In section 3 we restrict our attention to some purely algebraic aspects, and compare factor and minor primeness. As the two properties are different for $n > 2$, several results we are accustomed to use in 1D and 2D theory do not hold anymore, and rather pathological situations may arise, as shown by simple examples.
For sake of brevity, no proof will be given. The interested reader is referred to [5].

2. nD finite support behaviors

Let $\mathbf{F}$ be a field. In the sequel, we will set z for the n-tuple $(z_1, z_2, ..., z_n)$ and z_i^c for the $(n-1)$-tuple $(z_1, z_2, ..., z_{i-1}, z_{i+1}, ..., z_n)$, so that $\mathbf{F}[z, z^{-1}]$ and $\mathbf{F}[z_i^c, (z_i^{-1})^c]$ are shorthand notations for the Laurent polynomials rings in the indeterminates $z_1, ..., z_n$ and $z_1, ..., z_{i-1}, z_{i+1}, ..., z_n$, respectively. Therefore, a com-

*Manuscript received January 25, 1994

pact support signal on $\mathbf{Z}^n$, with values in $\mathbf{F}^p$, is uniquely described by an element of $\mathbf{F}[z, z^{-1}]^p$.

An nD (*modular*) behavior $\mathcal{B}$ with p components is a subset of $\mathbf{F}[z, z^{-1}]^p$ which is closed under both the linear combinations over $\mathbf{F}$ and the shifts along the coordinates axes. Therefore, (modular) behaviors can be identified with the $\mathbf{F}[z, z^{-1}]$-submodules of the module $\mathbf{F}[z, z^{-1}]^p$ and are finitely generated, since $\mathbf{F}[z, z^{-1}]$ is a Noetherian ring.

Every ordered set of generators $(\mathbf{g}_1, \mathbf{g}_2, ..., \mathbf{g}_m)$ of $\mathcal{B}$ corresponds to a particular input-output map

$$\mathbf{u} \mapsto [\ \mathbf{g}_1 | \mathbf{g}_2 | ... | \mathbf{g}_m\ ]\, \mathbf{u} = G\mathbf{u}, \tag{2.1}$$

which amounts to say that $\mathcal{B}$ can be represented as the image module $\mathrm{Im}G := \{\mathbf{y} : \mathbf{y} = G\mathbf{u}, \mathbf{u} \in \mathbf{F}[z, z^{-1}]^m\}$.

It is easy to realize that two arbitrary sets of generators give raise to matrices having the same rank over $\mathbf{F}(z)$. So it's meaningful to define the *rank* of $\mathcal{B}$ as the rank of anyone of its representations.

In general, the map (2.1) is not an injection, namely different input sequences possibly produce the same output signal. Clearly a modular behavior $\mathcal{B}$ can be viewed as the image of an injective input-output map, acting on the set of compact support sequences which take value in $\mathbf{F}^r$, if and only if $\mathcal{B}$ possesses r linearly independent generators (a *basis*). In this case $\mathcal{B}$ is a free module and can be represented as the image of a full column rank polynomial matrix.

An useful classification of full column rank polynomial matrices which obviously reflects into the associated free modular behavior, is based on some primeness notions, we shall often refer to in the sequel.

Definition A matrix $G \in \mathbf{F}[z, z^{-1}]^{p \times m}$ is

- *unimodular* if $p = m$ and $\det G$ is a unit in $\mathbf{F}[z, z^{-1}]$;
- *left minor prime* (ℓMP) if $p \geq m$ and its maximal order minors have no common factor;
- *left zero prime* (ℓZP) if $p \geq m$ and the ideal generated by its maximal order minors is the ring $\mathbf{F}[z, z^{-1}]$ itself.

If $\mathcal{B}$ is free, and a set of linearly independent generators is available, a parametrization of all finite sets of generators of $\mathcal{B}$ can be given.

Proposition 1 Let $\mathcal{B} \subseteq \mathbf{F}[z, z^{-1}]^p$ be a free module of rank r, G_1 a $p \times r$ polynomial matrix whose columns are a basis of $\mathcal{B}$, and G_2 a $p \times m$ polynomial matrix.
$\mathcal{B} = \mathrm{Im}G_2$ if and only if there exists an ℓZP matrix $T \in \mathbf{F}[z, z^{-1}]^{r \times r}$, such that $G_2 = G_1 T$.
In particular, if $r = m$, T is unimodular.

If $\mathcal{B}$ is not free, and $\mathcal{L}$ is any free submodule of $\mathcal{B}$, there exists a free maximal submodule $\mathcal{M}$ satisfying the inclusions $\mathcal{L} \subseteq \mathcal{M} \subset \mathcal{B}$, as it can be seen by applying the Zorn Lemma.

Consequently, $\mathcal{B}$ includes more than one free maximal submodule. Actually, if $\mathcal{M}_1$ is such a module, there exists a vector $\mathbf{v}$ in $\mathcal{B} \setminus \mathcal{M}_1$ and hence a maximal free submodule $\mathcal{M}_2 \neq \mathcal{M}_1$ satisfying $\langle \mathbf{v} \rangle \subseteq \mathcal{M}_2 \subset \mathcal{B}$.

The structure of the maximal submodules of $\mathcal{B}$ is clarified by the following proposition.

Proposition 2 Let $\mathcal{B} = \mathrm{Im}G$ be a submodule of $\mathbf{F}[z, z^{-1}]^p$ and let $\bar{G} \in \mathbf{F}[z, z^{-1}]^{p \times r}$ be a full column rank matrix. $\mathrm{Im}\bar{G}$ is a maximal free submodule of $\mathcal{B}$ if and only if the polynomial equation $G = \bar{G}T$, in the unknown matrix T, has polynomial matrix solutions, and all of them have no nonunimodular right factor (i.e. are right *factor prime*, rFP).

Recognizing in $\mathbf{F}[z, z^{-1}]^p$ the sequences of $\mathcal{B}$ constitutes a problem somehow complementary to that of generating the behavior $\mathcal{B}$, via a 1-1 input-output map. This situation, that tipically arises in fault detection and convolutional encoding, can be managed by resorting to a linear filter (residual generator, syndrome decoder) that produces an identically zero output signal if and only if the input signal belongs to $\mathcal{B}$. From a mathematical point of view, this requires to find a set of sequences endowed with the property that the convolution with the elements of $\mathcal{B}$ (and those only) gives zero.

Such a set obviously exists, as, for instance, the algebraic dual $\mathcal{B}^*$ of $\mathcal{B}$ always satisfies the abovementioned conditions. When resorting to $\mathcal{B}^*$, however, we have to use also infinite support sequences, which are not convenient from an algorithmic point of view. So it's natural to look for conditions guaranteeing that an unambiguous decision concerning a trajectory can be taken by using only parity checks represented by compact support sequences.

Given $\mathcal{B} \subseteq \mathbf{F}[z, z^{-1}]^p$, a compact support parity check is a row vector $\mathbf{v}^T = [v_1 v_2 ... v_p]$ with entries in $\mathbf{F}[z, z^{-1}]$ such that $\mathbf{v}^T\mathbf{y} = 0, \forall \mathbf{y} \in \mathcal{B}$. If G is any $p \times m$ polynomial matrix whose columns generate $\mathcal{B}$, the set of all the compact support parity checks (in algebraic terms, the module of the syzygies corresponding to the row module of G) will be denoted by $\mathcal{B}^\perp$. $\mathcal{B}^\perp$ is generated by the rows of a matrix $H^T \in \mathbf{F}[z, z^{-1}]^{q \times p}$, that is

$$\mathcal{B}^\perp = \{\mathbf{w}^T H^T, \mathbf{w} \in \mathbf{F}[z, z^{-1}]^q\}.$$

Condition $\mathbf{v}^T\mathbf{y} = 0$, $\forall \mathbf{v} \in \mathcal{B}^\perp$ does not necessarily guarantee that $\mathbf{y}$ belongs to $\mathcal{B}$. In general, the module

$$\mathcal{B}^{\perp\perp} := \{\mathbf{y} \in \mathbf{F}[z, z^{-1}]^p : \mathbf{v}^T\mathbf{y} = 0, \forall\ \mathbf{v} \in \mathcal{B}^\perp\}$$

properly includes $\mathcal{B}$, and can be characterized as the set of all polynomial vectors that can be obtained by combining the columns of G, over the field of rational functions $\mathbf{F}(z)$.

If $\mathcal{B}$ has rank r, $\mathcal{B}^{\perp\perp}$ has the same rank and is the maximal submodule of $\mathbf{F}[z, z^{-1}]^p$ of rank r that includes

$\mathcal{B}$. Thus $\mathcal{B} = \mathcal{B}^{\perp\perp}$ if and only if

$$\mathcal{B} \equiv \{G\mathbf{u} : \mathbf{u} \in \mathbf{F}(z)^m, G\mathbf{u} \in \mathbf{F}[z, z^{-1}]^p\}.$$

We consider now some conditions on the polynomial matrices G, whose columns generate the module $\mathcal{B}$, which guarantee that the equality $\mathcal{B} = \mathcal{B}^{\perp\perp}$ holds. In the following discussion it will be quite useful to the refer to the characterizations of minor primeness provided by Lemma 3 below.

Lemma 3 Let $G \in \mathbf{F}[z, z^{-1}]^{p\times r}$ be a full column rank matrix. The following facts are equivalent:
i) G is right minor prime;
ii) for $i = 1, 2, ..., n$ there exist matrices $H_i \in \mathbf{F}[z, z^{-1}]^{r\times p}$ and polynomials $\psi_i \in \mathbf{F}[z_i^c, (z_i^{-1})^c]$ such that

$$H_i G = \psi_i I_r;$$

iii) for every $\mathbf{u} \in \mathbf{F}(z)^r$, $G\mathbf{u} \in \mathbf{F}[z, z^{-1}]^p$ implies $\mathbf{u} \in \mathbf{F}[z, z^{-1}]^r$;
iv) for every $\mathbf{u} \in \mathbf{F}[z, z^{-1}]^r$ rFP, also $G\mathbf{u}$ is rFP;
v) for $i = 1, 2, ..., n$ there exist matrices $C_i \in \mathbf{F}[z, z^{-1}]^{p\times(p-r)}$ and polynomials $c_i \in \mathbf{F}[z_i^c, (z_i^{-1})^c]$ such that

$$\det[\ G \mid C_i\ ] = c_i;$$

vi) ImG is a submodule of $\mathbf{F}[z, z^{-1}]^p$, maximal among the submodules of rank r.

Proposition 4 Let $\mathcal{B} \subseteq \mathbf{F}[z, z^{-1}]^p$ be a submodule of rank r. The following facts are equivalent:
i) $\mathbf{y} \in \mathcal{B} \Leftrightarrow \mathbf{v}^T\mathbf{y} = 0,\ \forall\ \mathbf{v} \in \mathcal{B}^{\perp}$;
ii) there exists a polynomial matrix H^T, with p columns, such that $\mathcal{B} = \ker H^T := \{\mathbf{y} \in \mathbf{F}[z, z^{-1}]^p : H^T\mathbf{y} = 0\}$;
iii) $\mathcal{B} = $ ImG, G right minor prime.

Unfortunately, when $\mathcal{B}$ is not a free module, the equality $\mathcal{B} = \mathcal{B}^{\perp\perp}$ cannot be easily reduced to a condition on the families of its generators, namely on the matrices G such that $\mathcal{B} = $ ImG.

Proposition 5 Let $\mathcal{B} = $ ImG be a rank r submodule of $\mathbf{F}[z, z^{-1}]^p$. Then
i) if $G = \bar{G}T$, with $\bar{G}$ right minor prime and T left zero prime, then $\mathcal{B} = \mathcal{B}^{\perp\perp}$;
ii) if $\mathcal{B} = \mathcal{B}^{\perp\perp}$, then the g.c.d. of the $r \times r$ minors of G is a unit.

None of the conditions of the above proposition is equivalent to the equality $\mathcal{B} = \mathcal{B}^{\perp\perp}$. Actually, if a matrix G can be factorized as follows

$$G = \bar{G}T,$$

where $\bar{G} \in \mathbf{F}[z, z^{-1}]^{p\times r}$ is rMP and $T \in \mathbf{F}[z, z^{-1}]^{r\times m}$ is ℓMP but not ℓZP, clearly the g.c.d. of the $r \times r$ minors of G is a unit. On the other hand, there is an index ν, $1 \leq \nu \leq m$ such that the ν-th column of every rigth inverse of T is not polynomial. Actually, suppose that for every i there exists a right inverse T_i^{-1} whose i-th column is polynomial. Then the matrix

$$T^{-1} := [\, T_1^{-1}\mathbf{e}_1 \quad \cdots \quad T_m^{-1}\mathbf{e}_m\,],$$

where $\mathbf{e}_i$ denotes the i-th vector of the canonical basis of $\mathbf{F}^m$, would be a polynomial inverse of T, and hence T would be ℓZP, a contradiction. As a consequence, the equation

$$\mathbf{e}_\nu = T\mathbf{x} \tag{2.2}$$

has solution in $\mathbf{F}(z)^m$, but not in $\mathbf{F}[z, z^{-1}]^m$. The vector $\mathbf{y} := G\mathbf{x} = \bar{G}T\mathbf{x} = \bar{G}\mathbf{e}_\nu$ is polynomial, but does not belong to the module of G, otherwise a polynomial vector $\mathbf{p}$ could be found so that $\mathbf{y} = G\mathbf{p} = \bar{G}(T\mathbf{p})$.
For the injectivity property of $\bar{G}$, this would mean that $\mathbf{e}_\nu = T\mathbf{p}$ so that (2.2) would have a polynomial solution. As far as *i)* is concerned, it can be proved [5] that the columns of matrix

$$G = \begin{bmatrix} (z_1+1)(z_2+1) & 0 \\ 0 & z_2+1 \\ z_3+2 & z_1+1 \end{bmatrix}$$

generate a module $\mathcal{B}$ that coincides with $\mathcal{B}^{\perp\perp}$, and yet G cannot be factorized as $G = \bar{G}T$, where $\bar{G}$ is rMP and T is ℓZP.

3. Minor primeness vs factor primeness

As we have seen in the previous section, when the behavior $\mathcal{B}$ is a free module, the system output allows for a reconstruction of the (unique) input signal that has produced it. The rank r of the behavior $\mathcal{B}$ somehow represents a complexity index of $\mathcal{B}$, as there exist r independent trajectories, while every $r+1$-tuple of trajectories $(\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_{r+1})$ satisfies an autoregressive equation

$$p_1\mathbf{y}_1 + p_2\mathbf{y}_2 + ... + p_{r+1}\mathbf{y}_{r+1} = 0,$$

where not every $p_i \in \mathbf{F}[z, z^{-1}]$ is zero. Every minimal set of generators of $\mathcal{B}$ (a basis) is made up of r generators, that can be juxtaposed in a full column rank matrix G.
Particularly interesting among the free modules of rank r are those that can be described by a right minor prime matrix. They can be identified with the maximal elements in the class of free modules of rank r, and correspond to sets of trajectories that cannot be included in larger sets without either modifying the complexity or losing the injectivity property of the input-output map that produces it.
It's worthwhile to underline that factor prime matrices with more than two indeterminates are not necessarily minor prime, as shown by the following example.

Example 1 The 3×2 matrix

$$\bar{G} = \begin{bmatrix} (z_1+1)(z_2+1) & 0 \\ 0 & z_2+1 \\ z_3+2 & z_1+1 \end{bmatrix} = [\ \bar{g}_1 \mid \bar{g}_2\ ]$$

has no right factor, except for the unimodular ones [5], and hence is factor prime. However it is not minor prime as the g.c.d. of the maximal order minors is z_2+1.

Given a free module $\bar{\mathcal{B}}$ of rank r, which is maximal with respect to these properties, the module $\bar{\mathcal{B}}^{\perp\perp}$ is maximal in the class of (not necessarily free) modules of rank r that include $\bar{\mathcal{B}}$, and coincides with $\bar{\mathcal{B}}$ if and only if $\bar{\mathcal{B}}$ is the image of a minor prime matrix.

Example 2 As the matrix $\bar{G}$ in Example 1 is not rMP, the module $\bar{\mathcal{B}}$ generated by its columns is not maximal among the (not necessarily free) modules of rank r. Actually, the module generated by the vectors $\bar{g}_1$, $\bar{g}_2$ and $\bar{g}_3 := [\ (z_1+1)^2 \quad -(z_3+2) \quad 0\ ]^T$, properly includes $\bar{\mathcal{B}}$ and has rank 2. Consequently $\bar{\mathcal{B}}^{\perp\perp} \neq \bar{\mathcal{B}}$.

Generally, when the number n of the indeterminates is greater than 2, a free nD behavior $\mathcal{B}$ of rank r needs not to be included in a unique maximal free module of the same rank. If G is a full column rank matrix such that $\mathcal{B} = \mathrm{Im}G$, this corresponds to the fact that in the factorization

$$G = \bar{G}T,$$

where $\bar{G}$ is rFP and T is a polynomial square matrix, $\bar{G}$ is not essentially unique, (i.e. unique up to a unimodular right factor).

Example 3 The module $\mathcal{B}$ generated by the columns of

$$G = \begin{bmatrix} (z_1+1)(z_2+1)^2 & -(z_1+1)^2(z_2+1) \\ 0 & (z_2+1)(z_1+1) \\ (z_2+1)(z_3+2) & 0 \end{bmatrix}$$

is a free module of rank 2. The matrix G admits the factorizations $G = \bar{G}_1 T_1 = \bar{G}_2 T_2$, where

$$\bar{G}_1 = \begin{bmatrix} (z_1+1)(z_2+1) & 0 \\ 0 & z_2+1 \\ z_3+2 & z_1+1 \end{bmatrix}$$

$$\bar{G}_2 = \begin{bmatrix} (z_1+1)(z_2+1) & -(z_1+1)^2 \\ 0 & (z_1+1) \\ (z_3+2) & 0 \end{bmatrix}$$

$$T_1 = \begin{bmatrix} z_2+1 & -(z_1+1) \\ 0 & z_3+2 \end{bmatrix} \quad T_2 = \begin{bmatrix} z_2+1 & 0 \\ 0 & z_2+1 \end{bmatrix}.$$

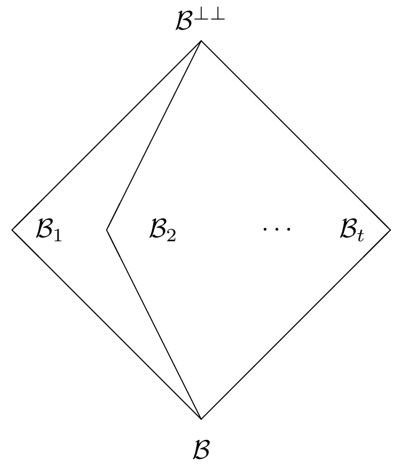
Since the rFP matrices $\bar{G}_1$ and $\bar{G}_2$ do not differ by a unimodular right factor, $\mathcal{B}$ is included in two different maximal free modules of rank 2, i.e. $\bar{\mathcal{B}}_1 = \mathrm{Im}\bar{G}_1$ and $\bar{\mathcal{B}}_2 = \mathrm{Im}\bar{G}_2$.

Interestingly enough, given a $p \times r$ matrix $\bar{G}$, which is rFP but not rMP, we can always guarantee the existence of another rFP matrix $\hat{G}$ such that the equation

$$\bar{G}T_1 = \hat{G}T_2$$

is fulfilled by a pair of $r \times r$ nonsingular polynomial matrices T_1 and T_2. Yet, no pair of unimodular matrices satisfies the above equation. Consequently, every free module $\bar{\mathcal{B}}$ generated by the columns of a factor but not minor prime matrix includes a free submodule $\mathcal{B}$ of the same rank with the property that the free maximal submodules of the same rank which include $\mathcal{B}$ are not uniquely determined [5].

The situation is summarized as follows: given a free module $\mathcal{B}$ of rank r there exist maximal free modules of rank r $\mathcal{B}_i$, $i \in \mathcal{I}$ which include $\mathcal{B}$ and in general $|\mathcal{I}|$ is greater than one. All of them are included in a unique maximal (not necessarily free) module of rank r, namely $\mathcal{B}^{\perp\perp}$.



If anyone of these modules, say $\mathcal{B}_1$, coincides with $\mathcal{B}^{\perp\perp}$, which happens if and only if $\mathcal{B}_1$ is the image of a rMP matrix, then $\mathcal{B}^{\perp\perp} = \mathcal{B}_i$ for all $i \in \mathcal{I}$.

References

1. J.C.Willems *Models for Dynamics*, Dynamics Reported, vol.2, Wiley and Teubner, pp. 171-269, 1989
2. P.Rocha, J.C.Willems *Controllability of 2D systems*, IEEE Trans. Aut. Contr., vol. AC 36, pp.413-23, 1991
3. D.C.Youla, G.Gnavi *Notes on n-dimensional system theory*, IEEE Trans. Circ. and Sys., vol.CAS 26, pp.105-11, 1979
4. S.Zampieri *Modellizzazione di sequenze di dati multidimensionali*, Ph.D. Thesis, Univ.of Padova, Italy, 1993
5. E.Fornasini, M.E.Valcher *On the autoregressive structure of nD behaviors*, submitted for publication