NEW PROOF FOR A BLIND EQUALIZATION RESULT: A MODULE THEORY APPROACH

Philippe Ciblat * **Alban Quadrat** **

* *Laboratoire de Télécommunications, Université catholique de Louvain, Louvain-la-Neuve, Belgium (ciblat@tele.ucl.ac.be)*
** *School of Mathematics, University of Leeds, Leeds, United Kingdom (quadrat@amsta.leeds.ac.uk)*

Abstract: In the blind equalization problem, one can recently observe that the sought unknown filter can be performed from the sole knowledge of second order statistics of the received signal. According to this fact, a powerful algorithm which is the so-called subspace method has been developed. The subspace method was previously described in rational spaces framework which seemed to be unappropriated. Indeed, the filter to identify is polynomial. In this paper, we show how the module theory over the polynomial ring $\mathbb{C}[z]$ and, in particular, the duality of modules can highlight the previous proof of the subspace method and lead to generalize its results.

Keywords: Blind equalization, Second order statistics, Subspace method, Polynomial matrices, Duality of modules, Module theory, MA process, Spectral factorization.

1. INTRODUCTION

In a wireless communication scheme, in order to retrieve the transmitted information, the receiver has to remove an Inter Symbol Interference arising from the propagation channel (Proakis, 1989). It is the so-called *equalization* problem. Obviously the channel is unknown and has to be identified. The so-called *blind identification* problem consists in estimating the disturbing channel from the sole knowledge of the received signal. (Tong *et al.*, 1991) has recently noticed that the channel could be estimated from the sole knowledge of its second order statistics. This problem is equivalent to determine the coefficients of a SIMO (Single Input/Multi Output) MA process from its power spectral density. This analysis led to introduce new algorithms. The most popular one is the *subspace method* (Moulines *et al.*, 1995). An extension to a MIMO (Multi Input/Multi Output) case is addressed in (Abed-Meraim *et al.*, 1997).

For a few years, the interest of the MA process has grown up in control theory again. Although the module theory (Bourbaki, 1980; Rotman, 1979) has been already used for analyzing the control systems (Kalman *et al.*, 1969), many results relying on module theory have been recently obtained in control theory (Oberst, 1990; Fliess, 1990; Pommaret and Quadrat, 1999). The module theory enables us to reformulate the problems in a more appropriate way and to highlight some well-known results. Furthermore, this new point of view leads to obtain some theorems which cannot be proved in another way (Pommaret and Quadrat, 1999).

In blind equalization problem, we wish to determine the components of a polynomial transfer function. Although the subspace method only deals with polynomial matrix operators, its analysis is based on the rational spaces associated with the rational functions. This rational spaces approach however leads to some interesting results (Abed-Meraim *et al.*, 1997). It is clear that the polynomial matrix set can strongly be linked with modules structure. Therefore, the module theory should be a more relevant framework.

In this paper, we analyze the subspace method by means of the module theory. The modules approach leads to highlight some well-known results and to generalize some others.

This paper is organized as follows. In Section 2, we review the blind identification problem. In Section 3, we briefly remind of the module theory. In Section 4, we address the subspace method. Finally, Section 5 is devoted to proofs.

2. REVIEW ON BLIND IDENTIFICATION

We consider a i.i.d. zero-mean unit-variance circular symbol sequence $\{s_n\}_{n\in\mathbb{Z}}$ containing the digital information to transmit. The sequence is assumed to be linearly modulated and to be shaped thanks to a Nyquist filter $g(t)$ at the baud rate $1/T_s$. Hence, the continuous-time transmitted signal $x_a(t)$ writes as follows

$$x_a(t) = \sum_{k\in\mathbb{Z}} s_k g_a(t - kT_s).$$

In a wireless communication system (see, e.g., GSM standard), the signal passes through a multi-path propagation channel. At the receiver, a single antenna is used. For sake of clarity, we only treat the noiseless case. Then, the continuous-time received signal $y_a(t)$ is as follows

$$y_a(t) = \sum_{n\in\mathbb{Z}} s_n h_a(t - nT_s)$$

with $h_a(t)$ depending on the shaping filter and on the propagation channel. Without restriction, $h_a(t)$ is assumed to be causal and time-limited.

At the receiver, we wish to retrieve the transmitted information, i.e., the symbol sequence. The convolution filter $h_a(t)$ spans an Inter-Symbol Interference (ISI) which disturbs the information retrieval. Removing ISI is thus necessary. Due to the unknown multi-path propagation channel, the mapping $t \mapsto h_a(t)$ is also unknown. Therefore, we may *identify* it (or one of its sampled versions). In most cases, the transmitter sends a training sequence which is a small symbol sequence known from the receiver. Sampling the continuous-time received signal corresponding to the transmitted training sequence at baud rate $1/T_s$ and then matching the obtained discrete-time signal with its theoretical closed-form expression enables us to estimate the filter accurately. Unfortunately, this method decreases the effective transmission rate. Moreover, in some contexts (e.g., military context), this approach fails because the training sequence is not available.

Therefore, several works focus on the channel identification from the sole data $y_a(t)$, i.e., without any deterministic knowledge on $\{s_n\}_{n\in\mathbb{Z}}$. This problem can be solved by exploiting either the high order statistics or the second order cyclic statistics of the received signal.

One avoids to use high order approaches because they have some numerical drawbacks. One can notice that the second order statistics of the continuous-time received signal is cyclostationary and not stationary. This means that the correlation mapping $(t_1, t_2) \mapsto r_{y_a}(t_1, t_2) = \mathbb{E}[y_a(t_1 + t_2)y_a^*(t_1)]$ is periodic in the variable t_1 with the period T (see (Proakis, 1989) and references therein). The notation $\mathbb{E}[.]$ stands for the mathematical expectation. More precisely, T_s is the cyclic period of $y_a(t)$. If the receiver samples the continuous-time received signal at the baud rate $1/T_s$, the discrete-time sampled signal becomes stationary. Then, it is well known that the filter estimation is not possible. In order to keep the cyclostationary property on the discrete-time sampled signal, (Tong *et al.*, 1991) proposes to oversample the continuous-time received signal at baud rate $1/T_e = q/T_s$ with q an integer strictly greater than 1. In such a case, $y(n) = y_a(nT_e)$ takes the following form

$$y(n) = [h(z)].v_n \tag{1}$$

where $h(z) = \sum_{l=0}^{L'} h_a(lT_e)z^{-k}$. L' is equal to the integer part of $L_a T_e$, where L_a is the length of the time support of $h_a(t)$. The notation $[.]$ stands for a convolution operator. $\{v_n\}_{n\in\mathbb{Z}}$ is the "pseudo-symbol" sequence obtained by inserting $(q-1)$ zero between two consecutive symbols s_n. In this way, the second order information is contained in the set of the following so-called cyclo-spectra $\{h(e^{2i\pi f})h(e^{2i\pi(f-k/q)})^*, k \in \{0, \cdots, q-1\}\}$. (Tong *et al.*, 1991) has proved that this set provided enough information to blindly identify the channel under the following condition on the filter : the polyphase components of $h(z)$ get no common zero.

The model (1) can be rewritten in the following form. We stacked the data in a q-variate process $\{Y(n)\}_{n\in\mathbb{Z}}$. Hence, $Y(n) = [y(qn), \cdots, y(qn+q-1)]^T$. The multivariate process $Y(n)$ is stationary. Moreover we obtain that

$$Y(n) = [H(z)].s_n$$

where $H(z) = \sum_{k=0}^{L} H_k z^{-k}$ is a causal FIR $q \times 1$ transfer function. L represents the nearest upper integer of L'/q. More precisely, we have

$$H(z) = [h_0(z), \cdots, h_{q-1}(z)]^T,$$

with $h_k(z)$ the k^{th} polyphase component of $h(z)$. This stationary SIMO model is equivalent to the previous cyclostationary SISO (Single Input/Single Output) model. The second order statistics of $Y(n)$ are described by the multivariate power spectral density

$$S_Y(e^{2i\pi f}) : f \mapsto H(e^{2i\pi f})H(e^{2i\pi f})^*. \tag{2}$$

It is well known that if $H(z)$ is minimum phase, then $S_Y(e^{2i\pi f})$ determines $H(z)$ perfectly. Fortunately, in the multivariate case, $H(z)$ is minimum phase if the previous assumption on $h(z)$ holds.

Several algorithms relying on oversampling approach have been introduced. Among them, the most popular one is the subspace method introduced by (Moulines *et al.*, 1995) because its theoretical performance is good and its computation complexity is low. Unfortunately, it is not widely used because the performance is poor in the band-limited case (Ciblat and Loubaton, 1998).

The previous scheme can be extended to the p-variate input case (with $1 < p < q$). The extension makes sense in a multi-user communication system. The model is modified as follows

$$Y(n) = [H(z)].S_n \qquad (3)$$

where $H(z)$ is henceforth a $q \times p$ transfer function and $S_n = [s_n^{(1)}, \cdots, s_n^{(p)}]^T$ is a p-variate process and each of its components $s_n^{(j)}$ represents a transmitted source. Without loss of generality, $\{S_n\}_{n \in \mathbb{Z}}$ is assumed to be a zero-mean, unit-variance and i.i.d. process. Recovering the different inputs from the received signal is the so-called *source separation* problem. We still wish to identify the polynomial matrix $H(z)$ only from the spectral density function of $Y(n)$ which has the same form than in (2). This problem is connected to the spectral factorization problem. Indeed, equation (3) represents a MA process. It is well known that $H(z)$ can be identified up to a $p \times p$ orthogonal matrix under certain might conditions (Rozanov, 1967). The above mentioned subspace algorithm tries to solve this factorization problem. In the case $p = 1$, the subspace method is powerful. Therefore, (Abed-Meraim *et al.*, 1997) has adapted it to the multi-input case. Unfortunately, in such a case, the subspace method fails (Abed-Meraim *et al.*, 1997). In this paper, even if the subspace method is not relevant in the case $p > 1$, we continue to consider this extended case in order to show the power of the module tools.

3. REVIEW ON MODULE THEORY

In the sequel, we shall note by $\mathbb{C}[z]$ the $\mathbb{C}$-algebra of polynomials ring in z^{-1} with coefficients in $\mathbb{C}$. Recall that $\mathbb{C}[z]$ is a commutative *integral domain* ($\forall\, a, b \in \mathbb{C}[z], a\, b = 0,\ a \neq 0 \Rightarrow b = 0$) as well as a *principal ideal domain*, i.e. any ideal I of $\mathbb{C}[z]$ has the form of $I = \mathbb{C}[z]\, a$ for a certain $a \in \mathbb{C}[z]$.

d denotes the $q \times p$ matrix with entries in $\mathbb{C}[z]$ ($0 < p \leq q$). We define the $\mathbb{C}[z]$-morphism $d.$ by

$$d. \ : \begin{cases} \mathbb{C}[z]^p & \longrightarrow \mathbb{C}[z]^q \\ y(z) = [y_1(z), \cdots, y_p(z)]^T & \longrightarrow d(z)\, y(z), \end{cases}$$

and the $\mathbb{C}[z]$-module (Malgrange, 1962)

$$\operatorname{coker}(d.) = \mathbb{C}[z]^q / \operatorname{im}(d.) = \mathbb{C}[z]^q / d(z)\, \mathbb{C}[z]^p.$$

The dual of $d.$ is the $\mathbb{C}[z]$-morphism $.d$ defined by:

$$.d \ : \begin{cases} \mathbb{C}[z]^p & \longleftarrow \mathbb{C}[z]^q \\ y(z)\, d(z) & \longleftarrow y(z) = [y_1(z), \cdots, y_q(z)]. \end{cases}$$

We denote

$$\operatorname{coker}(.d) = \mathbb{C}[z]^p / \operatorname{im}(.d) = \mathbb{C}[z]^p / \mathbb{C}[z]^p\, d(z)$$

We now recall certain concepts of useful homological algebra (Bourbaki, 1980; Rotman, 1979).

Definition 1. Let P_j and P_{j-1} be $\mathbb{C}[z]$-modules.

- A *complex* is a sequence of $\mathbb{C}[z]$-morphisms $d_j : P_j \to P_{j-1}$ such that:
  $$d_j \circ d_{j+1} = 0 \Leftrightarrow \operatorname{im} d_{j+1} \subset \ker\, d_j,\ \forall\, j \in \mathbb{Z}.$$
- A complex is *exact at* P_j if $\operatorname{im} d_{j+1} = \ker\, d_j$.
- A complex is *exact* if $\operatorname{im} d_{j+1} = \ker d_j, \forall j \in \mathbb{Z}$.
- Finally, a complex is usually denoted by:
  $$\ldots \xrightarrow{d_{j+1}} P_j \xrightarrow{d_j} P_{j-1} \xrightarrow{d_{j-1}} P_{j-2} \xrightarrow{d_{j-2}} \ldots$$

The following theorem provides a relationship between $\ker(d_j)$ and $\operatorname{coker}(d_j)$.

Theorem 1. Let i and π denote the canonical inclusion and surjection respectively. The following exact sequence is exact.

$$0 \longrightarrow \ker d_j \xrightarrow{i} P_j \xrightarrow{d_j} P_{j+1} \xrightarrow{\pi} \operatorname{coker} d_j \longrightarrow 0$$

We introduce usual properties of a module.

Definition 2. A finitely generated $\mathbb{C}[z]$-module M is

(1) *free* if $M \cong \mathbb{C}[z]^n$ for a certain $n \in \mathbb{Z}_+$,
(2) *torsion-free* if its *torsion-submodule*, namely
$$t(M) = \{m \in M \mid \exists\, 0 \neq a \in \mathbb{C}[z],\ a\, m = 0\},$$
is trivial, i.e. $t(M) = 0$. Any element $m \in t(M)$ is called a *torsion element* of M,
(3) *torsion* if $t(M) = M$.

The following theorem describes the link between the freeness and torsion notions.

Theorem 2. Let M be a $\mathbb{C}[z]$-module, then M is free iff it is torsion-free.

Recall that $\mathbb{C}(z)$ is called the *quotient field* of $\mathbb{C}[z]$. Let us note $S = \mathbb{C}[z] \setminus 0$. If M is a $\mathbb{C}[z]$-module, then we can define the $\mathbb{C}(z)$-vector space $S^{-1}M$ by : $S^{-1}M = \{m/s \mid m \in M,\ 0 \neq s \in \mathbb{C}[z]\}$.

Definition 3. The *rank* of a $\mathbb{C}[z]$-module M is defined by $\operatorname{rank}(M) = \dim_{\mathbb{C}(z)}(S^{-1}M)$.

One can obtain the following theorems.

Theorem 3. We consider the following exact sequence of $\mathbb{C}[z]$-modules

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0. \qquad (4)$$

Then the following sequence is exact :

$$0 \to S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P \to 0,$$

with $S^{-1}f(a \otimes m) = a\, f(m),\ \forall\, (a, m) \in \mathbb{C}(z) \times M$.

Corollary 1. Let (4) be an exact sequence of $\mathbb{C}[z]$-modules, then $\mathrm{rank}(N) = \mathrm{rank}(M) + \mathrm{rank}(P)$.

Let us finally denote by $\hom_{\mathbb{C}[z]}(M, \mathbb{C}[z])$ the $\mathbb{C}[z]$-module of $\mathbb{C}[z]$-morphism from M to $\mathbb{C}[z]$. $M^\star = \hom_{\mathbb{C}[z]}(M, \mathbb{C}[z])$ is called the dual module of M. We now provide a few propositions dealing with the dual module (Bourbaki, 1980; Rotman, 1979).

Proposition 1. We have the following assertions:

(1) M is a torsion $\mathbb{C}[z]$-module iff $\mathrm{rank}(M) = 0$.
(2) M is a torsion $\mathbb{C}[z]$-module iff $M^\star = 0$.

Proposition 2. Let N be a $\mathbb{C}[z]$-module. Let M be a submodule of N. The so-called orthogonal set of M is defined by $M^\perp = \{f \in N^\star | \forall m \in M, f(m) = 0\}$. Then, $M^\perp = (N/M)^\star$.

Proposition 3. Let M, N and P be $\mathbb{C}[z]$-modules. We consider the $\mathbb{C}[z]$-morphisms $.d_1 : M \to N$ and $.d_2 : N \to P$. If the sequence

$$0 \longrightarrow M \xrightarrow{.d_1} N \xrightarrow{.d_2} P \longrightarrow 0$$

is exact then, the following complex is also exact.

$$0 \longrightarrow P^\star \xrightarrow{d_2.} N^\star \xrightarrow{d_1.} M^\star$$

4. THE SUBSPACE METHOD

At first, we review the subspace method. The transfer function $H(z)$ to identify is a $q \times p$ polynomial matrix (with $p < q$). Let $H_j(z) = \sum_{l=0}^{L_j} H_{j,l} z^{-l}$ be a $q \times 1$ polynomial vector of degree L_j and $H(z) = [H_1, \cdots, H_p(z)]$. By definition, the degree of $H(z)$ is equal to $L = \sum_{j=1}^{p} L_j$ (Kailath, 1980). In practice, these degrees are unknown. We denote $\{\hat{L}_j\}_{j=1,\cdots,p}$ and $\hat{L} = \sum_{j=1}^{p} \hat{L}_j$ the estimated degrees. In fact, the model can be always overdetermined, i.e., we get $\hat{L}_j \geq L_j$ for each j and so $\hat{L} \geq L$. We introduce a few definitions (Abed-Meraim *et al.*, 1997).

Definition 4. A $q \times p$ polynomial matrix $F(z)$ is *full-rank* iff $\mathrm{rank}(F(z)) = p$ for each complex-valued number z, except at a finite number of points. It is *irreducible* iff $\mathrm{rank}(F(z)) = p$ for each complex-valued number z, including the infinity. $H(z)$ is said to be *column-reduced* iff $\mathrm{rank}([H_{1,L_1}, \cdots, H_{p,L_p}]) = p$.

In the sequel, $H(z)$ is assumed to be full-rank but not necessary irreducible and/or column-reduced. If $H(z)$ is full-rank, then it can be decomposed into the following way $H(z) = H''(z)R(z)$, where $H''(z)$ and $R(z)$ are a $q \times p$ irreducible polynomial matrix and a $p \times p$ full-rank polynomial matrix respectively. L'' and $\{L''_j\}_{j=1,\cdots,p}$ stand for the degree of $H''(z)$ and the degree of its column polynomial vectors respectively.

Let us inspect the subspace algorithm now (see (Moulines *et al.*, 1995; Abed-Meraim *et al.*, 1997) for more details). We consider the stacking vector

$$Y_N(n) = [Y(n)^T, \cdots, Y(n-N)^T]^T$$

and its correlation matrix

$$R_N(\mathbf{h}) = T_N(\mathbf{h}) T_N(\mathbf{h})^*,$$

where $T_N(\mathbf{h})$ is the $q(N+1) \times p(N + L_s + 1)$ Sylvester matrix associated with the polynomial $H(z) = \sum_{l=0}^{L_s} H_l z^{-l}$ where each H_l is a scalar-valued component matrix and $L_s = \sup_j\{L_j\}$. We consider the mapping $\Phi : H(z) \mapsto \mathbf{h}$ such as $\mathbf{h} = \mathrm{vec}(H_0, \cdots, H_{L_s})$. vec(.) is the operator reshaping any matrix into a column vector. Since $q(N+1) \geq p(N + L_s + 1)$, the matrix $R_N(\mathbf{h})$ is deficient rank and get a left kernel. We denote Π_N, the orthogonal projector on this kernel. The subspace method consists in looking for the filter $F(z)$ minimizing the mapping $\mathbf{f} \mapsto ||\Pi_N T_N(\mathbf{f})||^2$, whose behaviour is described by the following theorem proved in (Abed-Meraim *et al.*, 1997) by means of rational spaces.

Theorem 4. Assume that $H(z)$ is irreducible and column-reduced. ($H(z) = H''(z)$ thus holds)

Let $F(z) = [F_1(z), \cdots, F_p(z)]$ be a $q \times p$ full-rank polynomial matrix such as $\deg(F_1(z)) \leq \cdots \leq \deg(F_p(z))$ (this condition is necessary to avoid undetermined permutations).
This matrix solution $\Pi_N T_N(\mathbf{f}) = 0$ admits

- no solution if $\deg(F_j(z)) < L_j$, for each j.
- infinite number of solutions if $\deg(F_j(z)) \geq L_j$ for each j. In fact, $F(z) = H(z)R(z)$ with $R(z)$ a $p \times p$ full-rank polynomial matrix. If $\deg(F_j(z)) = L_j$ for each j, then $R(z)$ is reduced to a block triangular polynomial matrix with constant block diagonal matrices. Moreover, if $L = L_j$ for each j, $R(z)$ is reduced to a constant $p \times p$ invertible matrix.

The filter $H(z)$ has to satisfy some restrictive assumptions. Thanks to our new forthcoming proof based on module theory, we shall show that this theorem can be extended to a full-rank filter $H(z)$.

Corollary 2. We consider the Single Input case ($p = 1$). We assume that $H(z)$ is irreducible and column-reduced, i.e, its components have no common zero. Theorem 4 implies that if $F(z)$ is a $q \times 1$ polynomial matrix (with degree $\hat{L}$),

$$\Pi_N T_N(\mathbf{f}) = 0 \iff F(z) = H(z)r(z)$$

with $r(z)$ a $(\hat{L} - L)$ degree scalar polynomial.

In the Single Input case, if the degree is known (i.e., the subspace method seeks a filter $F(z)$ such as $\hat{L} = L$), then the filter $H(z)$ is obtained up to a constant. In contrast, in the Multi Input case, the subspace method is not relevant because the sought filter is undetermined up to an unknown matrix, whatever the degree constraints.

The subspace method is now rewritten in a more suitable form for the modules approach. We consider the correlation matrix $R_N(\mathbf{h})$ for a fixed N satisfying $N \geq \hat{L}$ (so $q(N+1) \geq p(N + L_s + 1)$). This matrix gets a left kernel, called noise subspace and denoted $\ker(R_N(\mathbf{h}))$. Let $\mathbf{g} = [\mathbf{g}_0, \cdots, \mathbf{g}_N]$ be a row vector (each of its blocks is of size $1 \times q$) belonging to $\mathrm{Ker}(R_N(\mathbf{h}))$. We get

$$\Pi_N T_N(\mathbf{h}) = 0 \iff G(z)H(z) = 0 \qquad (5)$$

with $G(z) = \sum_{k=0}^{N} \mathbf{g}_k z^{-k}$. We set

$$B_N = \{G(z) \in \mathbb{C}_N^{1\times q}[z] \mid G(z)H(z) = 0\}$$

where $\mathbb{C}_N^{p,q}[z]$ is the restriction of $\mathbb{C}^{p,q}[z]$ to the polynomial of degree strictly smaller than $(N+1)$. The subspace method is based on the sole knowledge of the noise subspace of $R_N(\mathbf{h})$, i.e., B_N. Indeed, according to Equation (5), the method tracks the $q \times p$ polynomial filtering matrix $F(z)$ belonging to the set C which is defined by

$$C=\{E(z) \in \mathbb{C}^{q\times p}[z] | \forall G(z) \in B_N, G(z)E(z) = 0\}.$$

Therefore, we now wish to describe C completely. In fact, such a description is given by Theorem 4, under some restrictive assumptions. We set

$$D=\{D(z) \in \mathbb{C}^{q\times 1}[z] | \forall G(z) \in B_N, G(z)D(z) = 0\}$$

which represents any column of the elements of C. Therefore, characterizing D is equivalent to characterizing C. We henceforth focus on the description of D. We set

$$B = \{G(z) \in \mathbb{C}^{1\times q}[z] \mid G(z)H(z) = 0\}.$$

Theorem 1 leads to the following exact sequence

$$0 \leftarrow \mathrm{coker}(.H) \leftarrow \mathbb{C}[z]^p \xleftarrow{.H} \mathbb{C}[z]^q \xleftarrow{i} \ker(.H) \leftarrow 0.$$

Let us notice that:

$$\ker(.H) = \{G(z) \in \mathbb{C}[z]^{1\times q} | G(z)H(z) = 0\} = B.$$

Thus, B is a submodule of the free $\mathbb{C}[z]$-module $\mathbb{C}[z]^q$. By Theorem 2, B is a torsion-free $\mathbb{C}[z]$-module. In contrast, as H is full-rank, $\mathrm{coker}(.H)$ is a torsion $\mathbb{C}[z]$-module. According to point 1 of Proposition 1, we get $\mathrm{rank}(\mathrm{coker}(.H)) = 0$. This result does not mean that $\mathrm{coker}(.H)$ is reduced to 0, but only that the torsion-free part of $\mathrm{coker}(.H)$ is reduced to 0. By Corollary 1, we get:

$$\mathrm{rank}(B) = q - p + \mathrm{rank}(\mathrm{coker}(.H)) = q - p.$$

Therefore, B is a free $\mathbb{C}[z]$-module of rank $q - p$. There exists a polynomial basis $\{g_j(z)\}_{j=1,\cdots,q-p}$. Their degrees $\{K_j\}_{j=1,\cdots,q-p}$ are the so-called *Kronecker indices* of B. There also exists an orthogonal set denoted $B^\perp$. It is a free module of rank p. Its Kronecker indices are $\{K_j^\perp\}_{j=1,\cdots,p}$. We assume that $N > \sum_{j=1}^{p} K_j^\perp$. According to the forthcoming theorem, this condition is not restrictive because it holds if $N > \hat{L}$. As $\sum_{j=1}^{q-p} K_j = \sum_{j=1}^{p} K_j^\perp$ (Abed-Meraim *et al.*, 1997), we get $N \geq \sup_{j=1,\cdots,q-p} K_j$. The polynomials $\{g_j(z)\}_{j=1,\cdots,q-p}$ thus belong to B_N.

Lemma 1. If $N \geq \sum_{j=1}^{p} K_j^\perp$, then $\mathrm{span}(B_N) = B$. span(.) stands for the space spanned by all the linear combinations of the considered set.

According to Lemma 1, $D = B^\perp$. Therefore B is completely determined by B_N. We set

$$B'' = \{G(z) \in \mathbb{C}^{1\times q}[z] \mid G(z)H''(z) = 0\}.$$

One can easily prove the following lemma.

Lemma 2. As $H(z)$ is full-rank, we get $B'' = B$.

It turns out that, $B''^\perp$ is equal to D. The characterization of $B''^\perp$, given by the characterization of D, is provided in the following theorem. The proof based on the modules approach is given in Section 5.

Theorem 5. If $N \geq \sum_{j=1}^{p} K_j^\perp$ and $H(z)$ full-rank, then $D = \{H''(z)r(z) \mid r(z) \in \mathbb{C}^{p\times 1}[z]\}$ and $C = \{H''(z)R(z) \mid R(z) \in \mathbb{C}^{p\times p}[z]\}$.

Our contribution has consisted in proving Theorem 4 in a different way. Because the assumptions on $H(z)$ are less strong, Theorem 5 is an extension of Theorem 4. One can restrict the sought space by constraining the matrix $R(z)$ to get a certain form (see Theorem 4) thanks to a knowledge on the degrees of $H(z)$.

5. PROOF OF THE MAIN THEOREM

We consider the $\mathbb{C}[z]$-morphism $H''.$ associated with the matrix $H''(z)$ and its dual $.H''$. Applying Theorem 1 on the morphism $.H''$ and noticing $B'' = \ker(.H'')$ lead to the following exact sequence

$$0 \to B'' \xrightarrow{i} \mathbb{C}[z]^q \xrightarrow{.H''} \mathbb{C}[z]^p \xrightarrow{\pi} \mathrm{coker}(.H'') \to 0$$

As B'' is a free $\mathbb{C}[z]$-module of rank $(q-p)$, there exists an isomorphism $\phi : B'' \to \mathbb{C}[z]^{q-p}$. The previous sequence can be simplified as follows

$$0 \to \mathbb{C}[z]^{q-p} \xrightarrow{.F} \mathbb{C}[z]^{q} \xrightarrow{.H''} \mathbb{C}[z]^{p} \xrightarrow{\pi} \mathrm{coker}(.H'') \to 0 \quad (6)$$

where $.F$ is a morphism corresponding to $i \circ \phi^{-1}$ in the canonical basis of $\mathbb{C}[z]^{q-p}$ and $\mathbb{C}[z]^{p}$. This obviously implies that $\ker(.H'') = \mathrm{im}(.F)$. Hence $B'' = \ker(.H'') = \mathrm{im}(.F)$. Thus, $B''^{\perp} = \mathrm{im}(.F)^{\perp}$. According to Proposition 2, we get

$$\mathrm{im}(.F)^{\perp} = (\mathbb{C}[z]^{q}/\mathrm{im}(.F))^{\star} = \mathrm{coker}(.F)^{\star}$$

It remains to inspect the orthogonal set of $\mathrm{im}(.F)$. According to the previous sequence, the complex $0 \to \mathbb{C}[z]^{q-p} \xrightarrow{.F} \mathbb{C}[z]^{q}$ is exact. It yields that $.F$ is an injective morphism, i.e., $\ker(.F) = 0$. Then, applying Theorem 1 on the morphism $.F$ leads to the following exact sequence

$$0 \to \mathbb{C}[z]^{q-p} \xrightarrow{.F} \mathbb{C}[z]^{q} \xrightarrow{\pi} \mathrm{coker}(.F) \to 0$$

Dualizing the previous sequence and using Proposition 3 lead to the following exact complex.

$$0 \longrightarrow \mathrm{coker}(.F)^{\star} \xrightarrow{i} \mathbb{C}[z]^{q} \xrightarrow{F.} \mathbb{C}[z]^{q-p}$$

The morphism i represents a canonical injection. Hence, $\mathrm{im}(i) = \mathrm{coker}.(F)^{\star}$. Thus we obtain that

$$\mathrm{im}(.F)^{\perp} = \mathrm{coker}(.F)^{\star} = \ker(F.)$$

Therefore, $B''^{\perp} = \ker(F.)$. So characterizing $\ker(F.)$ enables us to describe $B''^{\perp}$.

We introduce the well-known theorem extending Bezout identity (Bourbaki, 1980).

Proposition 4. Let $F(z)$ be a $q \times p$ polynomial matrix. The following assertions are equivalent :

(1) There exists $E(z) \in \mathbb{C}[z]^{p\times q}$ such that $E(z)F(z) = I_p$, with I_p the $p \times p$ identity matrix.
(2) $\mathrm{rank}(F(z)) = p$, $\forall\, z$, i.e, $F(z)$ is irreducible.

As $H''(z)$ is irreducible, there exists a $p \times q$ polynomial matrix $G(z)$ such that

$$G(z)H''(z) = I_p, \quad \forall z$$

We denote $G(z) = [g_1(z)^T, \cdots, g_p(z)^T]^T$, where $g_j(z)$ corresponds to a row of $G(z)$. It follows that,

$$g_j(z)H''(z) = e_j(z), \quad \forall z,$$

where $e_j(z) = [0_{1\times(j-1)}, 1, 0_{1\times(p-j)}]^T$ is an element of the canonical basis of $\mathbb{C}[z]^{p}$. We have proved that each element of the canonical basis of $\mathbb{C}[z]^{p}$ belonged to $\mathrm{im}(.H'')$. As $\mathrm{coker}(.H'') = \mathbb{C}[z]^{p}/\mathrm{im}(.H'')$, we get $\mathrm{coker}(.H'') = 0$. We can reduce the sequence (6) as follows

$$0 \longrightarrow \mathbb{C}[z]^{q-p} \xrightarrow{.F} \mathbb{C}[z]^{q} \xrightarrow{.H''} \mathbb{C}[z]^{p} \longrightarrow 0$$

Thanks to Proposition 3, dualizing the previous expression leads to the following exact complex

$$0 \longrightarrow \mathbb{C}[z]^{p} \xrightarrow{H''.} \mathbb{C}[z]^{q} \xrightarrow{F.} \mathbb{C}[z]^{q-p}.$$

Thus, we finally obtain $\ker(F.) = \mathrm{im}(H''.)$.

6. CONCLUSION

Introducing the module theory approach is relevant to study a Signal Processing problem. Indeed, the analysis of the subspace method can be performed powerfully. This leads to highlight known results and to generalize them. Beyond this new proof of the subspace method, we also wish to emphasize the fact that the module theory is not restricted to control theory.

7. REFERENCES

Abed-Meraim, K., Ph. Loubaton and E. Moulines (1997). A subspace algorithm for certain blind identification problems. *IEEE Trans. on Information Theory* **43**, 1–16.

Bourbaki (1980). *Algèbre homologique*. Masson.

Ciblat, Ph. and Ph. Loubaton (1998). Second order blind equalization : band-limited case. In: *ICASSP*. Vol. 6. Seattle (USA). pp. 3401–3404.

Fliess, M. (1990). Some basic structural properties of generalized linear systems. *Systems and Control Letters* **15**, 391–396.

Kailath, T. (1980). *Linear Systems*. Prentice-Hall.

Kalman, R.E., P.L. Falb and M.A. Arbib (1969). *Topics in Mathematical System Theory*. McGraw-Hill.

Malgrange, B. (1962). Systèmes à coefficients constants. In: *Séminaire Bourbaki*. Vol. 246. pp. 1–11.

Moulines, E., P. Duhamel, J.F. Cardoso and S. Mayrargue (1995). Subspace method for the blind equalization of multichannel FIR filters. *IEEE Trans. on Signal Processing* **43**, 516–526.

Oberst, U. (1990). Multidimensional constant linear systems. *Acta Applicandae Mathematica* **20**, 1–175.

Pommaret, J.F. and A. Quadrat (1999). Algebraic analysis of linear multidimensional control systems. *IMA Journal of Mathematical Control & Information* **16**, 275–297.

Proakis, J.G. (1989). *Digital Communications*. Mc Graw Hill.

Rotman, J.J. (1979). *An Introduction to Homological Algebra*. Academic Press.

Rozanov, Y. (1967). *Stationary Random Process*. Holden-Day. San Franscico (CA).

Tong, L., G. Xu and T. Kailath (1991). A new approach to blind identification and equalization of multipath channels. In: *ASILOMAR*. Pacific Grove (USA). pp. 856–860.