32th Asilomar Conference, California, Nov 1–4, 1998, pp.1569–1573

CLOSED-FORM BLIND CHANNEL IDENTIFICATION WITH MSK INPUTS

Pierre COMON[a], *Olivier GRELLIER*[a], *and Bernard MOURRAIN*[b]

(a) I3S, 2000 route des Lucioles, Sophia-Antipolis F-06410, France
(b) INRIA, 2004 route des Lucioles, Sophia-Antipolis F-06565, France

ABSTRACT

Blind equalization of non minimum phase FIR channels requires prior identification, for stability reasons. We present a novel algorithm able to identify a channel in presence of an unknown MSK modulated input (which can be viewed as an approximation of the GMSK modulation used in GSM mobile systems), by resorting only to output second order moments. Blind identification is made possible because the input is not circular. It is shown that this approach leads to a system of L quadrics in L unknowns, if L denotes the number of taps of the unknown FIR channel. This system is then solved with the help of an original algorithm based on resultant techniques. Performances in terms of Bit Error Rates are eventually reported.

1. INTRODUCTION

The growing computational power of digital signal processors makes it possible to process the data block-wise instead of fully recursively. This has the advantage of allowing a better use of the information contained in limited data records, which may be especially attractive in non stationary environments. For this reason, closed-form solutions to blind and semi-blind identification and equalization problems are being sought.

In a companion paper [4] [7], the FIR equalization problem has been investigated. Its limitation is that the channel cannot be well compensated when it is Single Input Single Output (SISO) FIR. In such a situation, it is necessary to identify the FIR channel before seeking to invert it, in a stabilized manner[2].

The problem of system *blind identification* has been addressed for a long time, with the help of second-order statistics [17] [11] or higher orders [16] [15], rarely dedicated to communications inputs [6] [3].

In this paper, a novel closed-form block blind identification algorithm is proposed, that is applicable to SISO, SIMO or MIMO systems. The principle is based on the knowledge of the desired source distribution, assumed to be discrete. A special attention is given to the case of Minimum Shift Keying Modulation (MSK), since it is known to linearly approximate the GMSK modulation utilized in the widely spread GSM standard [2] [9]. In the latter case, the algorithm is based on second order statistics of the observations. But the principle applies to other discrete modulations, with or without memory, *e.g.* PSK$-n$. This distinguishes the present contribution compared to previously published algorithms; see for instance [15] and references therein.

2. BLIND SISO IDENTIFICATION

2.1. Notation

Vectors are boldfaced and matrices are capitalized. The taps of a Finite Impulse Response (FIR) filter $h(\cdot)$ of length L will be stored in a column vector of size L, as $\mathbf{h}^{\mathrm{t}} = [h(0) \dots h(L-1)]$. A finite portion of length L of a time sequence will be stored in a column vector and denoted as:

$$\mathbf{y}(n; L)^{\mathrm{t}} = [y(n), y(n-1), \cdots y(n-L+1)].$$

The set of polynomials in the variables $h_1, \dots, h_l$ with coefficients in $\mathbb{C}$ will be denoted by $\mathcal{R} = \mathbb{C}[h_1, \dots, h_l] = \mathbb{C}[\mathbf{h}]$. For any polynomial $f_1, \dots, f_m \in \mathcal{R}$, the ideal $\mathcal{I} = (f_1, \dots, f_m)$ generated by these polynomials is the set of polynomials $\sum_{i=1}^{m} f_i q_i$, $q_i \in \mathcal{R}$.

2.2. Modeling

Assume P independent complex symbol sequences are wished to be transmitted through a communication channel. Denote $x_j(n)$ the symbol sequence of source j, $1 \le j \le P$, and $H_{ij}(m)$ the impulse response linking source j to antenna element i (which includes the channel), $1 \le i \le K$, assuming local stationarity of the channel. Also denote L the length of the channel (that can theoretically be infinite). Then the signal observed at the $K-$element receiver takes the following compact form:

$$\mathbf{y}(n) = \sum_{m=0}^{L-1} H(m)\, \mathbf{x}(n-m) + \mathbf{v}(n) \qquad (1)$$

[1] This work has been supported in part by the CNRS Telecommunications program No. TL97104.

[2] Equalizing a channel with a stable AR filter is equivalent to identify a minimum phase MA channel. Here, the phase is not assumed to be minimal.

where matrices $H(m)$ are $K \times P$, and $\mathbf{v}(n)$ stands for background and modeling noise.

2.3. Principle

In order to fix the ideas, assume first that sources are MSK modulated. This means in particular that, conditionally to $\mathbf{x}(0)$, sources are cyclostationary:

$$\mathrm{E}\{x_i(n)x_j(n-m)\,|\mathbf{x}(0)\} = \delta(i-j)\delta(m)(-1)^n x_i(0)^2 \tag{2}$$

where $\delta = 1$ at the origin and is null elsewhere. In absence of noise, the second-order moments of the observed sequences can thus be easily calculated:

$$\mathrm{E}\{y_p(n)y_q(n-\ell)\,|\mathbf{x}(0)\} = \sum_{m=0}^{L-1}\sum_{i=1}^{P} H_{pi}(m)H_{qi}(m-\ell)\,(-1)^{n-m}x_i^2(0). \tag{3}$$

Considering the fact that the filters $H_{ij}(m)$ can be identified only up to $P \times P$ constant post-multiplicative diagonal factor, the constants $x_i(0)^2$ can be dropped (that is, pulled inside the above unknown diagonal factor). The consequence is that we have at disposal a set of polynomial equations that the filter H should satisfy, in absence of noise. For instance, in the SISO case, we have for $L = 3$:

$$\begin{aligned}(-1)^n\mathrm{E}\{y(n)^2\} &= h_0^2 - h_1^2 + h_2^2 \\ (-1)^n\mathrm{E}\{y(n)y(n-1)\} &= h_0h_1 - h_1h_2 \\ (-1)^n\mathrm{E}\{y(n)y(n-2)\} &= h_0h_2\end{aligned} \tag{4}$$

On the other hand, for stationary second-order white sources, *e.g.* BPSK-modulated, moments of $\mathbf{y}(n)$ take a simpler expression:

$$\mathrm{E}\{y_p(n)y_q(n-\ell)\} = \sum_{m=0}^{L-1}\sum_{i=1}^{P} H_{pi}(m)H_{qi}(m-\ell)\,\mathrm{E}\{x_i^2(m)\},$$

and a similar system of equations can be obtained along the same lines. For $n-$PSK modulations, the degree of the polynomial system needs to be increased, but the principle remains the same.

2.4. Solution of the polynomial system

Consider a system $\mathcal{P}$ of L polynomial equations of degree d in L unknowns:

$$f_\ell(\boldsymbol{\xi}) = 0,\ \boldsymbol{\xi} \stackrel{\text{def}}{=} (h_1, h_2, \dots h_L),\ 1 \le \ell \le L. \tag{5}$$

Denote by $\mathcal{R} = \mathbb{C}[\boldsymbol{\xi}]$ the ring of polynomials in the variables $h_1, \dots, h_L$ with coefficients in $\mathbb{C}$ and by $\mathcal{I}$ the ideal generated by polynomials $\{f_1, \dots, f_L\}$. Bézout's theorem [8][p. 227] states that either the set of solutions is infinite, or its cardinality is at most d^L.

A classical way to compute these solutions is to reduce the problem to an eigenvector computation. More precisely, consider the quotient ring $\mathcal{A}$ of the ring of polynomials $\mathcal{R}$ by the ideal $\mathcal{I}$: $\mathcal{A} = \mathcal{R}/\mathcal{I}$. If the number of solutions of (5) is finite, then $\mathcal{A}$ is also a finite vector space. Let $\mathcal{M}_a$ be the operator of multiplication by a fixed element $a \in \mathcal{A}$.

$$\begin{aligned}\mathcal{M}_a : \mathcal{A} &\to \mathcal{A} \\ q &\mapsto q\,a\end{aligned} \tag{6}$$

and denote M_a the matrix of $\mathcal{M}_a$ in a fixed basis (m_i) of $\mathcal{A}$. The transposed matrix M_a^{t} represents the transposed map from the dual $\widehat{\mathcal{A}}$ to itself. Recall that $\widehat{\mathcal{A}}$ is the set of linear forms from $\mathcal{A}$ to $\mathbb{C}$. Our approach is based on the following property [12] [1] [14]:

Lemma 1 *The linear forms $\mathbf{1}_\zeta : p \mapsto p(\zeta)$, where ζ is any solution of $\mathcal{P}$, are eigenvectors of all matrices $(M_a^{\mathrm{t}})_{a\in\mathcal{A}}$. The corresponding eigenvalues are $a(\zeta)$.*

As an application, if one chooses $a(\boldsymbol{\xi}) = h_1$, then the eigenvalues of M_a will yield the d^L solutions $h_1 = \lambda_m$, $1 \le m \le d^L$. This procedure could be repeated for every component h_ℓ (see lemma 2 in appendix).

But it turns out that there is a better way to address the problem via eigenvectors of M_a^{t}. Indeed, the eigenvectors of the transposed operators yield directly the roots of $\mathcal{P}$, for they represent (up to a scalar) the evaluation at theses roots. Take for instance $\{1, h_1, h_2, \dots, h_1h_2, \dots\}$ as a basis of $\mathcal{A}$. Then the entries of the eigenvectors will be $\{1, \xi_{o1}, \xi_{o2}, \dots, \xi_{o1}\xi_{o2}, \dots\}$, where ξ_o is a root of (5).

The crucial point is thus to compute one of these matrices of multiplication M_a.

One can use for instance Gröbner basis techniques [5], in order to get a basis of $\mathcal{A}$ and the matrices of multiplication through normal form computations. This method has to be performed in exact arithmetic, which often means computations with big numbers. Gröbner bases can also be used to eliminate $L-1$ variables and reduce the computation of roots to those of a univariate polynomials (of degree at most d^L). But both of these methods are expensive and not adapted to input polynomials f_i with approximate coefficients.

We retained here another approach, which is somewhat more stable. It is a modification of the old method by Macaulay [10], utilized for the construction of resultants; it can be viewed as an extension of Sylvester's theorem to polynomials in several variables. Macaulay matrices represent mappings of the form

$$\begin{aligned}\mathcal{S}:\ V_0 \times \cdots \times V_L &\to V \\ (q_0, \dots, q_L) &\mapsto \sum_{i=0}^{L} q_i f_i\end{aligned}$$

where $f_0 \in R$ is fixed, *e.g.* $f_0 = a$ as in the above sections, and $V_0, \ldots, V_L$ are finite vector subspaces of R. Let $d_i = \deg(f_i)$, and $\nu = \sum_{i=0}^{L} d_i - L + 1$. Then first define V as the set of monomials of degree smaller than or equal to ν. Next define $h_n^{d_n} V_n$ as the subset of V of polynomials which are divisible by $h_n^{d_n}$, $h_{n-1}^{d_{n-1}} V_{n-1}$ the subset of polynomials of $V - h_n^{d_n} V_n$ which are divisible by $h_{n-1}^{d_{n-1}}$, and so forth for $V_{n-2}, \ldots V_0$. In this construction, V_0 is eventually generated by the $\prod d_i$ monomials of the form $h_1^{a_1} \cdots h_n^{a_n}$ with $0 \leq a_i \leq d_i - 1$.

For instance, in the case of two univariate polynomials f_0 and f_1, V_0 would be generated by $1, h, \ldots, h^{d_1 - 1}$, V_1 by $1, h, \ldots, h^{d_0-1}$, and S would be the well-known Sylvester matrix.

In the generic case of this construction [10] [12], a basis of V_0 is also a basis of $\mathcal{A}$. In our problem, the matrix of $\mathcal{S}$ can be divided into 4 blocks

$$S = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

in such a way that D is invertible, possibly after a change of coordinates. Now it is desired to find the coordinates of $\mathcal{M}_{f_o}(V_0)$ in the basis of V_0.

Since V_0 is a basis of $\mathcal{A}$, the matrix of multiplication by f_0 in this basis is obtained by reducing the multiples $m\, f_0$, $m \in V_0$, modulo the polynomials $f_1, \ldots, f_n$. In order to do this in terms of matrix operations, one looks for linear combinations of the columns of the second block, $[B^{\mathrm{t}}\ D^{\mathrm{t}}]^{\mathrm{t}}$, that would produce a zero block in the place of C if added to the first block $[A^{\mathrm{t}}\ C^{\mathrm{t}}]^{\mathrm{t}}$. This can be done explicitly, by right-multiplication of the matrix S by the matrix

$$\begin{pmatrix} \mathbf{I} & 0 \\ -D^{-1}C & \mathbf{I} \end{pmatrix},$$

which yields the formula $M_{f_0} = A - B\, D^{-1}\, C$.

Taking into account the geometry of the monomials involved in this computation, we can replace the inversion of the big square matrix D, of size $\binom{L\,d+1}{L} - d^L$, by $L\, d - L$ inversions of smaller systems of size $s_1, \ldots, s_{L\,(d-1)}$ such that $s_1 + \cdots + s_{L\,(d-1)} = L\, d^{L-1}$. This new algorithm is illustrated in the next section and yields the multiplication map, in $\mathcal{A}$, by any fixed element f_0, and thus provides us with the roots of the system $\mathcal{P}$ given in (5).

2.5. SISO algorithm with 3 taps

In this section, it is assumed that $L = 3, d = 2$, and the system $\mathcal{P}$ to be solved is the one given by (4). According to the previous section, the standard Macaulay construction procedure would lead to the solution of a linear system of size $\binom{6+1}{3} - 2^3 = 27$, whereas our procedure needs the solution of $6 - 3 = 3$ smaller linear systems. In fact, their respective sizes are $s_1 = 3$, $s_2 = 3$, and $s_3 = 6$, and we can check out that $s_1 + s_2 + s_3 = 3\, 2^2 = 12$.

Given N samples $y(n), 1 \leq n \leq N$, the algorithm proceeds in six steps.

1. **Computation of system $\mathcal{P}$.** The left-hand side of (4) is replaced by the following unbiased estimates, $0 \leq \ell \leq L - 1$:

$$d(\ell) = \frac{1}{N} \sum_{n=1}^{N} (-1)^n y(n) y(n - \ell).$$

2. **Change of variables.** Variables $\mathbf{z} = T\mathbf{h}$ are utilized instead of $\mathbf{h}$, in order to avoid singularity of the systems to solve. Matrix T is chosen to be (but many others could have been assumed):

$$T = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix}$$

3. **Expression of every monomial in the basis.** The canonical basis is formed of the 8 entries of $\mathbf{b} = (1, z_1, z_2, z_3, z_1 z_2, z_1 z_3, z_2 z_3, z_1 z_2 z_3)^{\mathrm{t}}$. System (4) can then be rewritten as

$$A_1\, \mathbf{z}[2] = B_1\, \mathbf{b} \qquad (7)$$

where

$$\mathbf{z}[2] = \begin{bmatrix} z_1^2 \\ z_2^2 \\ z_3^2 \end{bmatrix}, \quad A_1 = \begin{pmatrix} 3 & 2 & 0 \\ 2 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix},$$

$$B_1 = \begin{pmatrix} d_1 & 0 & 0 & 0 & -4 & 2 & 2 & 0 \\ d_2 & 0 & 0 & 0 & -2 & -1 & -2 & 0 \\ d_3 & 0 & 0 & 0 & 2 & -2 & -1 & 0 \end{pmatrix}.$$

Thus the monomials z_ℓ^2 can be expressed in the basis $\mathbf{b}$ by solving the 3×3 linear system (7) by $\mathbf{z}[2] = C_1 \mathbf{b}$, denoting $C_1 = A_1^{-1} B_1$. Similarly, one can express the 6 third degree monomials $z_1^2 z_2, z_1^2 z_3, z_2^2 z_1, z_2^2 z_3, z_3^2 z_1, z_3^2 z_2$ in the basis $\mathbf{b}$ by solving another 6×6 linear system:

$$A_2\, \mathbf{z}[3] = B_2\, \mathbf{b} \;\Rightarrow\; \mathbf{z}[3] = C_2\, \mathbf{b} \qquad (8)$$

Finally, the 3 fourth degree monomials $z_1^2 z_2 z_3, z_1 z_2^2 z_3, z_1 z_2 z_3^2$ are expressed in the basis by solving a 3×3 linear system.

$$A_3\, \mathbf{z}[4] = B_3\, \mathbf{b} \;\Rightarrow\; \mathbf{z}[4] = C_3\, \mathbf{b} \qquad (9)$$

4. **Construction of M_a^{t}.** The multiplication by $a(z_1, z_2, z_3) = z_1$ can be represented in the same

basis by the following matrix:

$$M_a = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & & C1(1,:) & & & \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ & & & & C2(1,:) & & & \\ & & & & C2(2,:) & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & & & & C3(1,:) & & & \end{pmatrix}$$

where $C_i(j,:)$ the jth row of C_i. To obtain this, it suffices to compute the image of vector $\mathbf{b}$, and to use the previous relations.

5. **Computation of eigenvectors.** The 8 eigenvectors $\mathbf{u}_m$ of M_a^{t} are computed; their multiplicative factor are chosen so that their first entry equals 1. Then the entries $2, 3, 4$ of each of these vectors provide us with a possible solution for $\mathbf{z} = (z_1, z_2, z_3)$. The corresponding filters are obtained by transforming back $\mathbf{h} = T^{-1}\mathbf{z}$.

6. **Choice of the best solution.** In order to select the proper filter, one computes the circular moments $\mathrm{E}\{y(n)y(n-\ell)^*\}$, and select the filter that best matches them.

3. COMPUTER RESULTS

Once the channel impulse response $\mathbf{h}$ has been identified by a filter $\hat{\mathbf{h}}$, it is wished to compare the performances obtained. One could choose a Relative Mean Square Error between (RMSE) $\mathbf{h}$ and $\hat{\mathbf{h}}$. The inconvenience is that a large error does not necessarily yield a large bit error. So this RMSE would not be very meaningful. Because the goal is to transmit a sequence of bits, the most natural criterion is the Bit Error Rate (BER) itself. But this performance measure requires that an informed equalizer be applied to the observation sequence $y(n)$. Two equalizers are available, namely the Zero-Forcing $\mathbf{g}_{ZF}$, and the Wiener $\mathbf{g}_{MSE}$ equalizers. In absence of constraint on the finiteness of the impulse response, they are given by:

$$g_{ZF}(z) = h(z)^{-1}, \quad g_{MSE}(z) = c_x(z)\, h(z)^{\dagger}\, c_y(z)^{-1}$$

If both channel and equalizer are FIR of length L and L', respectively, then the tap vector $\mathbf{g}$ can be obtained from the L' by $L+L'-1$ Töplitz matrix H built on $\mathbf{h}$ as: $\mathbf{g}^{\mathrm{t}} = \mathbf{e}^{\mathrm{t}}\, C_x\, H^{\dagger}\, C_y^{-1}$, where $\mathbf{e}$ denotes the $L+L'-1$ dimensional vector, whose entries are all null but the first one, set to 1, $C_x = \mathrm{E}\{\mathbf{x}(n; L+L'-1)\mathbf{x}(n; L+L'-1)^{\dagger}\}$, and $C_y = \mathrm{E}\{\mathbf{y}(n; L')\mathbf{y}(n; L')^{\dagger}\}$. It is assumed that $c_x = 1$.

In a first experiment, we take a minimum phase MA2 channel with zeros $0.5+0.6$i and $0.4-0.5$i. One reports in figure 1 the BERs obtained with the AR ZF equalizer (the inverse) and the MA MSE equalizer of length 15. In each case, true and identified channels are compared. 400 trials have been run with 500 samples each.

In the second experiment, we have assumed a channel with zeros $1.2 + 0.8$i and $0.4 - 0.5$i, which does not admit a stable inverse. The BERs reported in figure 2 correspond to a AR ZF and ARMA MSE equalizers.

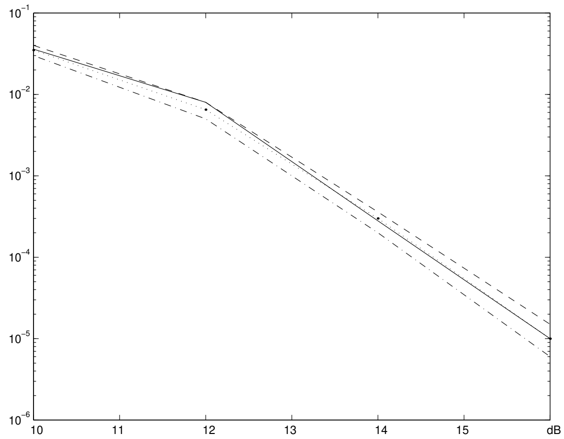

Figure 1: Bit Error rates of the linear equalizer output obtained when the channel admits a stable inverse; solid: True ZF, dashed: Estimated ZF, dashdotted: True MSE, dotted: Estimated MSE.

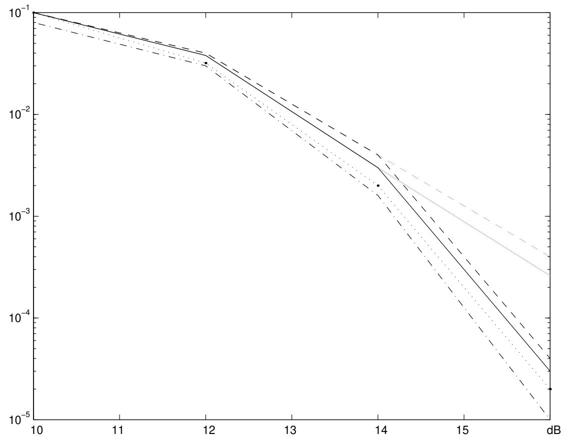

Figure 2: Bit Error rates of the DFE equalizer output when the channel does not admit a stable inverse; solid: True ZF, dashed: Estimated ZF, dashdotted: True MSE, dotted: Estimated MSE.

4. CONCLUDING REMARKS

The blind identification scheme proposed in this paper is dedicated to MSK or BPSK inputs. But the same principle applies to other modulations such as QPSK, to the price of an increase in the polynomial degrees, and thus in complexity. Computer simulations have been limited to the SISO MSK case but could be carried out in the MIMO case as well.

A related problem that needs to be addressed is the one of semi-blind identification. In the present framework, it means that additional linear equations should be taken into account, so that the system to solve becomes overdetermined.

5. REFERENCES

[1] W. AUZINGER, H. J. STETTER, "An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations", in *Proc. Intern. Conf. on Numerical Math.* 1988, vol. 86 of *Int. Series of Numerical Math*, pp. 11–30, Birkhäuser Verlag.

[2] S. BENEDETTO, E. BIGLIERI, V. CASTELLANI, *Digital Transmission Theory*, Prentice-Hall, 1987.

[3] D. BOSS, K. D. KAMMEYER, "Blind identication of mixed-phase FIR systems with application to mobile communication channels", in *ICASSP*, Munich, Apr. 1997, pp. 3589–3592.

[4] P. COMON, O. GRELLIER, "Closed-form blind and semi-blind equalizers", in *ICASSP*, Phoenix, March 15-19 1999, submitted.

[5] D. COX, J. LITTLE, D. O'SHEA, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics. Springer, 1992.

[6] E. DeCARVALHO, D. T. M. SLOCK, "Cramer-Rao bounds for semi-blind, blind and training sequence based channel estimation", in *Proc. SPAWC 97 Conf.*, Paris, France, Apr. 1997, pp. 129–132.

[7] O. GRELLIER, P. COMON, "Blind separation and equalization of a channel with MSK inputs", in *SPIE Conference*, San Diego, July 19-24 1998.

[8] J. HARRIS, *Algebraic Geometry, a first course*, vol. 133 of *Graduate Texts in Math.*, Springer, 1992.

[9] P. A. LAURENT, "Exact and approximate construction of digital phase modulations by superposition of amplitude modulated pulses", *IEEE Trans. Com.*, vol. 34, pp. 150–160, Feb. 1986.

[10] F. S. MACAULAY, "Some formulae in elimination", *Proc. London Math. Soc.*, vol. 1, no. 33, pp. 3–27, 1902.

[11] E. MOULINES, P. DUHAMEL, et al., "Subspace methods for the blind identification of multichannel FIR filters", *IEEE Trans. Sig. Proc.*, vol. 43, no. 2, pp. 516–525, Feb. 1995.

[12] B. MOURRAIN, "Computing isolated polynomial roots by matrix methods", *J. Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, Dec. 1998.

[13] B. MOURRAIN, V. Y. PAN, "Multivariate polynomials, duality and structured matrices", Rapport de Recherche 3513, INRIA, 1998.

[14] H. J. STETTER, "Eigenproblems are at the Heart of Polynomial System Solving", *SIGSAM Bulletin*, vol. 30, no. 4, pp. 22–25, 1996.

[15] A. SWAMI, G. GIANNAKIS, S. SHAMSUNDER, "Multichannel ARMA processes", *IEEE Trans. Sig. Proc.*, vol. 42, no. 4, pp. 898–913, Apr. 1994.

[16] L. TONG, "Identification of multichannel MA parameters using higher-order statistics", *Signal Processing, Elsevier*, vol. 53, no. 2, pp. 195–209, Sept. 1996, special issue on High-Order Statistics.

[17] L. TONG, G. XU, T. KAILATH, "Blind identification and equalization based on second-order statistics: a time domain approach", *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 340–349, Mar. 1994.

6. APPENDIX

Definitions. For any ideal $\mathcal{I} \subset \mathcal{R}$, the quotient algebra $\mathcal{R}/\mathcal{I}$ is the set of classes of polynomials $p \in \mathcal{R}$, modulo the ideal $\mathcal{I}$: $p \equiv q$ iff $p - q \in \mathcal{I}$. The quotient algebra is denoted by $\mathcal{A}$.

The dual space of $\mathcal{R}$ is the set of linear forms from $\mathcal{R}$ to the field $\mathbb{C}$. It is denoted by $\widehat{\mathcal{R}}$. The special linear form which evaluates a polynomial p at a point ζ is denoted by $\mathbf{1}_\zeta$: $\mathbf{1}_\zeta(p) = p(\zeta)$. The dual space $\widehat{\mathcal{A}}$ of $\mathcal{A}$ is the subset of $\widehat{\mathcal{R}}$ of linear forms which vanish on the ideal $\mathcal{I}$. We easily check that the evaluation $\mathbf{1}_\zeta$ is in $\widehat{\mathcal{A}}$ iff ζ is a root of all the polynomials in $\mathcal{I}$.

Given an element $a \in \mathcal{A}$, we define the operator of multiplication by a as the map (6). The transpose operator from $\widehat{\mathcal{A}}$ to $\widehat{\mathcal{A}}$ is by definition the map $\mathcal{M}_a^t$ such that $\langle q, M_a^{\mathfrak{t}}\Lambda\rangle = \langle M_a q, \Lambda\rangle = \langle aq, \Lambda\rangle$, $\forall\Lambda \in \widehat{\mathcal{A}}$, $\forall q \in \mathcal{R}$ so that we have $\mathcal{M}_a^{\mathfrak{t}}(\Lambda)(q) = \Lambda(q\,a)$.

Lemma 2 *Let a be a fixed given polynomial of $\mathcal{R}$. Then the eigenvalues in $\mathcal{A}$ of the operator $\mathcal{M}_a$ are the roots of system $\mathcal{P}$.*

Proof of lemma 2. Assume that for some $q \neq 0$, $\mathcal{M}_a \cdot q = \lambda q$ in $\mathcal{A}$. Then $(a - \lambda)q = 0$ in $\mathcal{A}$ means $(a-\lambda)q = \sum_{i=1}^{L} f_i\, q_i$ in R. But $q \neq 0$ also in R, thus $\exists\boldsymbol{\xi}_o$ such that $f_i(\boldsymbol{\xi}_o) = 0$ and $q(\boldsymbol{\xi}_o) \neq 0$. Thus $(a-\lambda)\,q$ cancels for some $\boldsymbol{\xi}_o$ satisfying $\mathcal{P}$ such that $q(\boldsymbol{\xi}_o) \neq 0$, which yields $a(\boldsymbol{\xi}_o) = \lambda$. □

If one chooses $a = h_1$, then the eigenvalues of M_a will yield the d^L solutions $h_1 = \lambda_m$, $1 \leq m \leq d^L$. In practice, the linear operator M_a can be defined by its matrix in a canonical basis (see section 2.5). This procedure could be repeated for every component h_ℓ. By using lemma 1, every eigenvector provides us with all the unknowns related to each solution. This makes the task easier compared to lemma 2.

Proof of lemma 1. Apply the definition of $M_a^{\mathfrak{t}}$ to the linear forms $\mathbf{1}_{\boldsymbol{\xi}_o}$ Then $\forall q$, $M_a^{\mathfrak{t}}(\mathbf{1}_{\boldsymbol{\xi}_o})(q) = \mathbf{1}_{\boldsymbol{\xi}_o}(a\,q) = a(\boldsymbol{\xi}_o)\,\mathbf{1}_{\boldsymbol{\xi}_o}(q)$ In other words, $M_a^{\mathfrak{t}}(\mathbf{1}_{\boldsymbol{\xi}_o}) = a(\boldsymbol{\xi}_o)\,\mathbf{1}_{\boldsymbol{\xi}_o}$. This shows that the forms $\mathbf{1}_{\boldsymbol{\xi}_o}$ are eigenvectors of $M_a^{\mathfrak{t}}$ associated with eigenvalues $a(\boldsymbol{\xi}_o)$. □

The converse, unused in this paper, is proved in [12].