

LABORATOIRE



INFORMATIQUE, SIGNAUX ET SYSTÈMES  
DE SOPHIA ANTIPOLIS  
UMR 6070

# BLIND IDENTIFICATION OF COMMUNICATION CHANNELS SYMBOLIC SOLUTION ALGORITHMS

*J. Lebrun, P. Comon*

*Projet ASTRE*

Rapport de recherche  
I3S/RR-2002-52-FR

Octobre 2002

---

RÉSUMÉ :

MOTS CLÉS :

---

ABSTRACT:

In this paper, a new algorithm for the blind identification of SISO communication channels is introduced. Based on methods from computational algebraic geometry, the approach achieves a full description of the solution space and thus avoids the local minima issue of adaptive algorithms. Furthermore, unlike most symbolic methods, the computational cost is kept low by a split of the problem into two stages. First, a symbolic pre-computation is done offline, once for all, to get a more convenient parametric representation of the problem. The solutions of the problem are then easily obtained from this representation by solving a single univariate polynomial equation.

KEY WORDS :

blind channel identification, high-order statistics, non-circularity, phase shift keying, algebraic geometry, rational univariate representation

# Blind Identification of Communication Channels Symbolic Solution Algorithms

J. Lebrun and P. Comon

*Lab. I3S, CNRS/UNSA,  
2000 route des Lucioles, BP.121,  
F-06903 Sophia-Antipolis, France.*

---

## Abstract

In this paper, a new algorithm for the blind identification of SISO communication channels is introduced. Based on methods from computational algebraic geometry, the approach achieves a full description of the solution space and thus avoids the local minima issue of adaptive algorithms. Furthermore, unlike most symbolic methods, the computational cost is kept low by a split of the problem into two stages. First, a symbolic pre-computation is done offline, once for all, to get a more convenient parametric representation of the problem. The solutions of the problem are then easily obtained from this representation by solving a single univariate polynomial equation.

*Key words:* blind channel identification, high-order statistics, non-circularity, phase shift keying, algebraic geometry, rational univariate representation.

---

## 1 Introduction

One important issue in digital communications (*e.g.* cellular) is to mitigate the effects of the propagation channel. This is the role of the equalizer. Reliable equalizers have been developed, but need prior knowledge of the channel [1, ch.10]. In a first stage, a good estimation of the channel (also referred to as channel identification) is thus necessary and quite critical.

Consider a complex-valued discrete-time signal  $x[n]$ . This sequence is unknown and is modeled as a stochastic process, having known statistical properties, and carries the message transmitted through the channel. In this paper, we consider

---

*Email address:* {lebrun,comon}@i3s.unice.fr (J. Lebrun and P. Comon).

the case of a linear and time-invariant (LTI) scalar (SISO) communication channel. Such a channel can be described as the convolutive filtering of the input signal  $x[n]$  by a filter with complex taps  $h[n]$ . We assume provisionally that  $h[n]$  is causal with finite impulse response (FIR) and thus represented by

$$x[n] \longrightarrow \boxed{h[n]} \longrightarrow y[n] = \sum_{k=0}^{N-1} h[k]x[n-k] \quad (1)$$

Most identification algorithms rely on the knowledge of the output  $y[n]$  of the channel for a given input  $x[n]$  [2–4]. So-called pilot sequences are usually transmitted, either in the middle of each data block as in GSM, or as background signal, in a parallel channel as in UMTS.

On the contrary, our concern here is *blind* channel identification, that is, identification without the knowledge of input symbols,  $x[n]$ . Advantages of such approaches include in particular the possibility to reduce or remove the pilot sequence, which permits an increase in the throughput but also applications such as the interception of communications.

Blind identification or equalization is not a new subject, for it has been addressed as early as in 1980 [5,6]. However, most of the algorithms are *adaptive*, that is, recursive in time, and converge quite slowly (sometimes even to local minima). Improvements made since early algorithms include (i) the use of the diversity induced by space, time, or excess bandwidth, to modify the model into a Single Input Multiple Output problem [7–11], or (ii) block calculations (i.e. removal of time recursions) [12,13].

Our contribution lies in the field of block blind identification algorithms when diversity cannot be exploited. With this respect, our approach is similar to [12], where inputs are assumed to belong to the unit circle, and to [13] where they are assumed to belong to a finite alphabet. The underlying idea makes sense in digital communications for the emitted signal  $x[n]$  normally comes from a modulation scheme (typ. BPSK, MSK, QPSK,  $\frac{\pi}{4}$ -DQPSK, 8-PSK or  $\frac{3\pi}{8}$ -D8PSK, or one type of QAM). Our algorithm is based on this discrete character via polynomial relations linking the channel taps with high order statistics on the output  $y[n]$ . Now, making use of methods coming from computational algebraic geometry, we get an efficient and exhaustive estimate of  $h[0], \dots, h[N-1]$  from the sole observations  $\{y[n]\}$ .

## 2 Definitions and basic properties

In this section, we introduce the discrete-time stochastic processes that are exciting the input of the system. These processes are widely used in digital

communications [14,15,1]. For instance, the Minimum Shift Keying (MSK) modulation is a good approximation of that employed in the GSM standard, the  $\pi/4$ -Phase shifted Differential Quadrature Phase Shift Keying ( $\pi/4$ -DQPSK) modulation is used in the American standard IS54, whereas the Quadrature Phase Shift Keying (QPSK) modulation is used in IS95 as well as UMTS third generation standards.

**Definition 2.1** *An independently and identically distributed (iid) stochastic process is referred to as Binary Phase Shift Keying (BPSK) if it takes its values in the set  $\{1, -1\}$  with equal probabilities, as QPSK if it takes its values in the set  $\{1, i, -1, -i\}$  with equal probabilities and in general as  $2^K$ -PSK if it takes its values in the set  $\{\exp(ik\frac{2\pi}{K}) \mid k = 0, \dots, M - 1\}$  with equal probabilities.*

MSK processes are defined by the recursion

$$x[n + 1] = ix[n]b[n], \quad (2)$$

where  $b[n]$  is BPSK. The original value  $x[0]$  remains unspecified, but is of unit modulus. Then it can be noticed that  $x[n] = i^n x[0] B[n]$  where  $B[n] := \prod_{k=1}^n b[k]$ . For our purpose, it is equivalent to use the less well known simpler definition given by the Proposition below.

**Proposition 2.2 (MSK definition)** *An iid stochastic process is referred to as MSK if it is modeled by  $x[n] = i^n b[n]x[0]$ , where  $b[n]$  is BPSK.*

Note that if  $x[0] = 1$ , then  $x[n]$  takes its values in  $\{1, i, -1, -i\}$ . When used with a particular transmit filter, the MSK modulation enjoys other properties [14,15], which have justified its name. But it can also be seen alternatively as a  $\pi/2$ -phase shifted Differential BPSK.

The  $\pi/4$ -DQPSK modulation is defined by  $x[n + 1] = w_8 x[n] q[n]$ , where  $w_8 := \exp(i\pi/4)$  and  $q[n]$  is QPSK. For similar reasons as above, one may assume the simpler equivalent definition:

**Proposition 2.3 ( $\pi/4$ -DQPSK definition)** *An iid stochastic process is referred to as  $\pi/4$ -DQPSK if it can be modeled as  $w[n] = w_8^n q[n]w[0]$ , where  $q[n]$  is QPSK.*

Remark that  $w[n]$  takes 8 equidistant values on the unit circle.

**Proof.** These two alternative definitions given by Propositions 2.2 and 2.3 are a direct consequence of the following surprising property. Let  $q_1$  and  $q_2$  be two independent random variables equally distributed on  $K$ -th roots of unity with  $K > 1$ , then the product  $q_1 q_2$  is statistically independent of  $q_1$ . ■

These discrete processes enjoy some deterministic and statistical properties that will be used in the remainder.

**Corollary 2.4 (Deterministic properties)** *If  $b[n]$ ,  $q[n]$ ,  $x[n]$ ,  $w[n]$  denote BPSK, QPSK, MSK, and  $\frac{\pi}{4}$ -DQPSK processes, respectively, then they satisfy  $b^2[n] = 1$ ,  $q^4[n] = 1$ ,  $x^2[n] = (-1)^n x^2[0]$ ,  $w^4[n] = (-1)^n w^4[0]$ , for any time index  $n$ .*

The four processes defined above are zero-mean, and their autocorrelation is null everywhere except at the origin, *e.g.*

$$c_x[k] := \mathbb{E}(x[n]x^*[n-k]) = \delta[k] \quad (3)$$

where (\*) denotes complex conjugation, and  $\delta[n] := 0, \forall n \neq 0$ , and  $\delta[0] := 1$ . However, for complex processes, there is another autocorrelation of interest, namely

$$\gamma_x[k, n] := \mathbb{E}(x[n]x[n-k]|x[0]) \quad (4)$$

This correlation is sometimes referred to as *non circular*, as opposed to  $c[k]$  referred to as *circular*. It turns out that two of the processes considered are not stationary, as revealed by the non circular statistics below.

**Corollary 2.5 (Cyclo-stationarity)** *MSK processes have a periodic non circular autocorrelation of period 2,*

$$\gamma_x[k, n] = (-1)^n x^2[0]\delta[k] \quad (5)$$

whereas  $\frac{\pi}{4}$ -DQPSK exhibit the same cyclo-stationarity at order 4

$$\mathbb{E}(w^2[n]w^2[n-k]|w[0]) = (-1)^n w^2[0]\delta[k]$$

Beside these relations, all the other second-order moments are stationary, and can be summarized by

**Corollary 2.6** *Denote  $b[n]$ ,  $q[n]$  and  $w[n]$  BPSK, QPSK, and  $\frac{\pi}{4}$ -DQPSK processes, respectively. Then  $\forall n$*

$$\gamma_b[k] := \mathbb{E}(b[n]b[n-k]) = \delta[k] \quad (6)$$

$$\gamma_q[k] := \mathbb{E}(q[n]q[n-k]) = 0 \quad (7)$$

$$\gamma_w[k, n] := \mathbb{E}(w[n]w[n-k]|w[0]) = 0 \quad (8)$$

### 3 Polynomial systems

The goal of this section is to build the equations that will allow to compute the channel coefficients  $h[k]$  from the statistics of the observation,  $y[n]$ .

First, for all inputs under consideration, one can deduce from (3) and (1) that

$$c_y[k] := \mathbb{E}(y[n]y^*[n-k]) = \sum_{l=k}^{N-1} h[l]h^*[l-k] \quad (9)$$

Additional equations are necessary in order to uniquely determine the set  $\{h[0], h[1], \dots, h[N-1]\}$ . From (5) and (1), we obtain the relations for MSK inputs

$$\gamma_y[k, n] := \mathbb{E}(y[n]y[n-k] | x[0]) = \sum_{l=k}^{N-1} (-1)^{n-l} h[l]h[l-k] \quad (10)$$

This system contains  $N$  equations in  $N$  complex unknowns, and has generically by Bezout's theorem  $2^N$  solutions. System (9) can be used to select the best one.

Next, (7) and (1) yield, for QPSK inputs

$$\gamma_y(p) := \mathbb{E}(y[n]y[n-p]) = 0 \quad (11)$$

and (8) and (1) yield eventually for  $\frac{\pi}{4}$ -DQPSK inputs

$$\gamma_y(p; n) := \mathbb{E}(y[n]y[n-p]|w[0]) = 0 \quad (12)$$

For PSK modulations, the symbols are of roots of unity. By using this property and introducing *non-circular* statistics on  $y[n]$ , we get the following polynomial equations in  $h[n]$ . More precisely,

**BPSK, QPSK, 8-PSK:** For BPSK, i.e.  $x[n]$  iid discrete-uniform  $\{-1, 1\}$ , we get for  $p = 0, \dots, N-1$ ,

$$\gamma_p := \mathbb{E}(y[n]y[n-p]) = \sum_{m=p}^{N-1} h[m]h[m-p]. \quad (13)$$

For QPSK,  $x[n]$  is iid discrete-uniform  $\{1, j, -1, -j\}$ , which gives

$$\begin{aligned} \mathbb{E}(y[n]y[n-p_1]y[n-p_2]y[n-p_3]) = \\ \sum_{m=\max(p_1, p_2, p_3)}^{N-1} h[m]h[m-p_1]h[m-p_2]h[m-p_3]. \end{aligned} \quad (14)$$

Now, these equations can easily be reduced to the BPSK case by taking  $p_1 = 0, p_3 = p_2$  and  $g[n] := h^2[n]$ . In a similar manner, the 8-PSK and in general all  $2^K$ -PSK modulations can be reduced to the BPSK case.

**MSK,  $\frac{\pi}{4}$ -DQPSK,  $\frac{3\pi}{8}$ -D8PSK:** For MSK, we have  $x[n] = i^n b[n]x[0]$  with  $b[n]$  BPSK. So, for  $p = 0, \dots, N - 1$ ,

$$\gamma_p := E(y[n]y[n-p]|x[0]) = \sum_{m=p}^{N-1} (-1)^{n-m} h[m]h[m-p]. \quad (15)$$

As above, for  $\frac{\pi}{4}$ -DQPSK, we get

$$E(y[n]y[n-p_1]y[n-p_2]y[n-p_3]) = \sum_{m=\max(p_1, p_2, p_3)}^{N-1} (-1)^{n-m} h[m]h[m-p_1]h[m-p_2]h[m-p_3]. \quad (16)$$

Consequently, the  $\frac{\pi}{4}$ -DQPSK and  $\frac{3\pi}{8}$ -D8PSK cases can be reduced to the MSK case.

E.g. for  $\frac{\pi}{4}$ -DQPSK and  $N = 3$ , we get the following system of polynomial equations, where  $\gamma_0, \gamma_1, \gamma_2$  are parameters.

$$\begin{cases} \gamma_0 - h[0]^4 + h[1]^4 - h[2]^4 = 0 \\ \gamma_1 - h[0]^2 h[1]^2 + h[1]^2 h[2]^2 = 0 \\ \gamma_2 - h[0]^2 h[2]^2 = 0. \end{cases} \quad (17)$$

From Bézout's theorem, this system has either infinitely many solutions, either exactly 64 (with multiplicities), or no solution.

To illustrate our algorithm, we will focus on this example. Our approach is easily generalized (and has been implemented [16]) for  $N = 2, \dots, 9$  and the two afore-mentioned families of modulations (BPSK, QPSK, 8-PSK and MSK,  $\frac{\pi}{4}$ -DQPSK,  $\frac{3\pi}{8}$ -D8PSK).

## 4 Algebraic geometry

Recently, major advances have been achieved in the field of computational algebraic geometry that lead to new efficient ways to deal with one of the central application of computer algebra: solving systems of multivariate polynomial equations [17–20]. By using the new algorithms introduced, practical problems can now be solved in a way that is very competitive with numerical methods. However, among the most promising approaches to solve systems of

polynomial equations, Gröbner bases, homotopic continuation, or resultants show some limitations [21,22] (typ. high computational cost, non-parametric equations or only rational parameters). This hinders seriously their interest in a framework with only limited computational power (typ. the DSP of a mobile phone) and stringent time-constraints (fast evolution of the communication channel). We introduce here an ad-hoc approach inspired by [21], [23] and [24] in which most of the expensive computation is done offline through the pre-computation of a parametric normal form [23] of the system. The solutions of the system are then easily obtained through the computation of a rational univariate representation (RUR). Most of the on-line computational cost lies then in isolating the roots of an univariate polynomial of degree the number of solutions (with multiplicities) of the system.

Namely, by the following generic change of variables,  $g[0] = h[0]^2 := x_1$ ,  $g[1] = h[1]^2 := x_1 + x_2$ ,  $g[2] = h[2]^2 := x_1 + x_2 + x_3$ , system (17) can be rewritten as system:

$$(P) \begin{cases} \gamma_0 - x_1^2 - 2x_1x_3 - 2x_2x_3 - x_3^2, \\ \gamma_1 + x_1x_2 + x_2^2 + x_1x_3 + x_2x_3, \\ \gamma_2 - x_1^2 - x_1x_2 - x_1x_3. \end{cases} \quad (18)$$

Now by solving in  $x_1^2, x_2^2, x_3^2$ , we get:

$$\begin{cases} x_1^2 = \gamma_2 - x_1x_2 - x_1x_3 \\ x_2^2 = -\gamma_1 - x_1x_2 - x_1x_3 - x_2x_3 \\ x_3^2 = \gamma_0 - \gamma_2 + x_1x_2 - x_1x_3 - 2x_2x_3. \end{cases} \quad (19)$$

Hence, the monomials  $x_1^2, x_2^2, x_3^2$  can be expressed in the monomial basis  $\mathcal{B} = \{\omega_1, \dots, \omega_d\}$  given by

$$\mathcal{B} = \{1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}.$$

Using, Bézout's theorem, it is easily seen that  $\mathcal{B}$  is indeed a linear base of the  $d$ -dimensional quotient algebra  $\mathcal{A} := \mathbb{Q}[x_1, \dots, x_N]/\langle P \rangle$  where  $\langle P \rangle$  denotes the ideal generated by  $(P)$ . By working in this setting, solving system  $(P)$  is now be seen as a problem of linear algebra.

More generally, we will now details how the linear algebra approach to solve these equations works. For more details, the reader can read the surveys on the subject in [18] or [20]. Starting from a list  $P$  of polynomials such that the generated ideal  $I = \langle P \rangle$  is zero-dimensional, it is easily seen that the quotient space  $\mathcal{A} := \mathbb{Q}[x_1, \dots, x_N]/I$  inherits a structure of finite-dimensional algebra. Now, we need to choose a linear basis  $\mathcal{B} := \{\omega_1, \dots, \omega_d\}$  called the *monomial basis* of  $\mathcal{A}$  and its associated normal form  $\bar{p} = \text{NF}(p, I)$  with  $p \in \mathbb{Q}[x_1, \dots, x_N]$ . Finally, by constructing the multiplication table  $[\omega_k \omega_l]_{k,l}$  of  $\mathcal{A}$ , we get a full description of the linear algebraic framework in which we will deal with the

polynomials. Also, any element  $\bar{p} \in \mathcal{A}$  can be expressed as a vector  $[p]$  since  $\bar{p} = \sum_{k=1}^d [p]_k \omega_k$ . For example,

$$[x_1^2] = \begin{bmatrix} \gamma_2 & 0 & 0 & 0 & -1 & -1 & 0 & 0 \end{bmatrix}^\top.$$

Now, for any polynomial  $u$ , we introduce the linear operator  $\mathbf{M}_u$  on  $\mathcal{A}$ ,

$$\begin{aligned} \mathbf{M}_u : \mathcal{A} &\rightarrow \mathcal{A} \\ \bar{f} &\mapsto \mathbf{M}_u \bar{f} := \overline{uf}. \end{aligned} \tag{20}$$

We will also identify  $\mathbf{M}_u$  with its  $\mathbb{C}^{d \times d}$  matrix representation in the monomial basis of  $\mathcal{A}$ . This matrix is easily computed by expressing  $\bar{u}\omega_k$  in the monomial basis, this gives the  $k^{\text{th}}$  column of  $\mathbf{M}_u$ . Now, for  $[u] \in \mathcal{A}$ , we get the multiplication operator  $\mathbf{M}_u[v] := [uv]$  on  $\mathbb{R}^d$ . For example, for  $u = x_1$ , since

$$x_1 \mathcal{B} = \{x_1, x_1^2, x_1 x_2, x_1 x_3, x_1^2 x_2, x_1^2 x_3, x_1 x_2 x_3, x_1^2 x_2 x_3\},$$

we get

$$\mathbf{M}_{x_1} = \begin{bmatrix} 0 & \gamma_2 & 0 & 0 & 0 & 0 & 0 & \gamma_2 \gamma_1 \\ 1 & 0 & 0 & 0 & \gamma_2 - \gamma_0 & -\gamma_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\gamma_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \gamma_2 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & -\gamma_1 + \gamma_2 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & \gamma_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \gamma_2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{21}$$

We will denote by  $\mu(\boldsymbol{\alpha})$  the multiplicity of a solution  $\boldsymbol{\alpha}$ . In this alternative approach to Gröbner bases developed by [24,17], one constructs a list  $\{\chi_u(t), g_u(1, t), g_u(x_1, t), \dots, g_u(x_N, t)\}$  of polynomials of  $\mathbb{Q}[x_1, \dots, x_N]$  such that: if  $\boldsymbol{\alpha}$  is a solution of the system, then  $u(\boldsymbol{\alpha})$  is a root of  $\chi_u(t)$  with the same multiplicity and conversely, if  $\zeta$  is a root of  $\chi_u(t)$ , then

$$\left[ \frac{g_u(x_1, \zeta)}{g_u(1, \zeta)}, \frac{g_u(x_2, \zeta)}{g_u(1, \zeta)}, \dots, \frac{g_u(x_N, \zeta)}{g_u(1, \zeta)} \right] \tag{22}$$

is a solution of the system with the same multiplicity. Hence,  $\mathcal{Z}_{\mathbb{C}}(I)$  is fully characterized.

From the computation of  $\mathbf{M}_u$ , we derive some important information on  $\mathcal{Z}_{\mathbb{C}}(I)$  and the system in general. Namely, by the Stickelberger theorem [24], we get that  $\mathbf{M}_u$  has eigenvalues  $u(\boldsymbol{\alpha})$  with multiplicity  $\sum_{\boldsymbol{\beta} \in \mathcal{Z}(I), u(\boldsymbol{\beta})=u(\boldsymbol{\alpha})} \mu(\boldsymbol{\beta})$ , where  $\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)$ . This gives that

- $\det(\mathbf{M}_u) = \prod_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} u(\boldsymbol{\alpha})^{\mu(\boldsymbol{\alpha})}$ .
- $\text{trace}(\mathbf{M}_u) = \sum_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} \mu(\boldsymbol{\alpha}) u(\boldsymbol{\alpha})$ .
- $\chi_u(t) := \det(t\mathbf{I} - \mathbf{M}_u) = \prod_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} (t - u(\boldsymbol{\alpha}))^{\mu(\boldsymbol{\alpha})}$ .

$\chi_u(t)$  is the characteristic polynomial of  $\mathbf{M}_u$ . Computing directly the characteristic polynomial (incl. the determinant) of a matrix like  $\mathbf{M}_u$  can be very time and memory consuming. We detail here an alternative method originally due to Kronecker based on traces of matrices and taking advantage of the special structure of the matrices  $\mathbf{M}_u$ . Let  $\chi_u(t) = \sum_{k=0}^d b_k t^{d-k}$  and  $\chi'_u(t)$  be its derivative, then

$$\begin{aligned} \frac{\chi'_u(t)}{\chi_u(t)} &= \sum_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} \frac{\mu(\alpha)}{t - u(\alpha)} = \sum_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} \frac{1}{t} \frac{\mu(\alpha)}{1 - \frac{u(\alpha)}{t}} \\ &= \sum_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} \sum_{k \geq 0} \frac{1}{t} \mu(\alpha) u^k(\alpha) t^{-k} = \sum_{k \geq 0} \text{trace}(\mathbf{M}_{u^k}) t^{-(k+1)}. \end{aligned} \quad (23)$$

So, we have

$$\chi'_u(t) = \chi_u(t) \sum_{k \geq 0} \text{trace}(\mathbf{M}_{u^k}) t^{-(k+1)},$$

and also

$$\chi'_u(t) = \sum_{k=0}^{d-1} (d-k) b_k t^{d-1-k},$$

we then get

$$(d-k) b_k = \sum_{l=0}^k \text{trace}(\mathbf{M}_{u^l}) b_{k-l}.$$

Thus, we can compute  $\chi_u(t)$  from the scalars:  $\text{trace}(\mathbf{M}_{u^k})$  for  $k = 0, \dots, d$ . We also introduce the square-free part of  $\chi_u(t)$ :

$$\tilde{\chi}_u(t) := \prod_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} (t - u(\alpha)) = \frac{\chi_u(t)}{\text{gcd}(\chi_u(t), \chi'_u(t))}. \quad (24)$$

Now, assume  $u$  is separating  $\mathcal{Z}_{\mathbb{C}}(P)$ , i.e. on  $\mathcal{Z}_{\mathbb{C}}(I)$ ,  $\alpha \neq \beta \Rightarrow u(\alpha) \neq u(\beta)$  (that implies that  $\mathbf{M}_u$  has eigenvalues  $u(\alpha)$  with multiplicity exactly  $\mu(\alpha)$ ), we finally introduce

$$\begin{aligned} g_u : \mathcal{A} &\rightarrow \mathbb{Q}[x_1, \dots, x_N] \\ \bar{v} &\mapsto g_u(v, t) := \sum_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} \mu(\alpha) v(\alpha) \frac{\tilde{\chi}_u(t)}{t - u(\alpha)}. \end{aligned} \quad (25)$$

This can be rewritten as

$$g_u(v, t) = \sum_{\alpha \in \mathcal{Z}_{\mathbb{C}}(I)} \mu(\alpha) v(\alpha) \prod_{\beta \in \mathcal{Z}_{\mathbb{C}}(I) \setminus \{\alpha\}} (t - u(\beta)). \quad (26)$$

Taking  $\alpha \in \mathcal{Z}_{\mathbb{C}}(I)$  and  $t = u(\alpha)$ , we get

$$g_u(v, u(\alpha)) = \mu(\alpha) v(\alpha) \prod_{\beta \in \mathcal{Z}_{\mathbb{C}}(I) \setminus \{\alpha\}} (u(\alpha) - u(\beta)). \quad (27)$$

We then get the central result of the rational univariate representation,

$$\frac{g_u(v, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))} = v(\boldsymbol{\alpha}). \quad (28)$$

Thus, for  $v = x_1, \dots, x_N$ , we have

$$\boldsymbol{\alpha} = \left[ \frac{g_u(x_1, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))}, \frac{g_u(x_2, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))}, \dots, \frac{g_u(x_N, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))} \right]. \quad (29)$$

**Theorem 4.1** *If  $\boldsymbol{\alpha}$  is a solution of the system, then  $u(\boldsymbol{\alpha})$  is a root of  $\chi_u(t)$  with the same multiplicity and conversely, if  $\zeta$  is a root of  $\chi_u(t)$ , then*

$$\left[ \frac{g_u(x_1, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))}, \frac{g_u(x_2, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))}, \dots, \frac{g_u(x_N, u(\boldsymbol{\alpha}))}{g_u(1, u(\boldsymbol{\alpha}))} \right]$$

*is a solution of the system with the same multiplicity.*

Now, all we have to detail is a practical way to compute  $g_u(v, t)$ . In a similar way to what is done to compute  $\chi_u(t)$ , we get

$$\frac{g_u(v, t)}{\tilde{\chi}_u(t)} = \sum_{k \geq 0} \text{trace}(\mathbf{M}_{u^k v}) t^{-(k+1)}. \quad (30)$$

Writing  $\tilde{\chi}_u(v, t) = \sum_{k=0}^r a_k t^{r-k}$  and let  $H_k(\tilde{\chi}_u)(t) = \sum_{l=0}^k a_l t^{k-l}$  be its Hörner sequence of polynomials, we then get

$$g_u(v, t) = \sum_{k=0}^{r-1} \text{trace}(\mathbf{M}_{u^k v}) H_{r-1-k}(\tilde{\chi}_u)(t). \quad (31)$$

So, the  $g_u(v, t)$  are easily computed from  $\tilde{\chi}_u(t)$  and the  $\text{trace}(\mathbf{M}_{u^k v})$ , for  $k = 0, \dots, r$ . There is furthermore an easy way to compute these traces by noticing that  $\text{trace}(\mathbf{M}_{fg}) = \text{Tr}(f)[g]$  where

$$\text{Tr}(f) := \left[ \text{trace}(\mathbf{M}_{f\omega_1}), \dots, \text{trace}(\mathbf{M}_{f\omega_d}) \right]. \quad (32)$$

Now, since  $\text{Tr}(u^{k+1}) = \text{Tr}(u^k)\mathbf{M}_u$ , we get by induction on  $k$  that  $\text{trace}(\mathbf{M}_{u^{k+1}}) = \text{Tr}(u^k)[u]$  and  $\text{trace}(\mathbf{M}_{u^k v}) = \text{Tr}(u^k)[v]$ .

To really complete the algorithm, we introduce the matrix defined by  $[\text{TrM}]_{i,j} := \text{trace}(\mathbf{M}_{\omega_i \omega_j})$ , i.e.

$$\text{TrM} := \begin{bmatrix} \text{trace}(\mathbf{M}_{\omega_1 \omega_1}) & \dots & \text{trace}(\mathbf{M}_{\omega_1 \omega_d}) \\ \vdots & & \vdots \\ \text{trace}(\mathbf{M}_{\omega_d \omega_1}) & \dots & \text{trace}(\mathbf{M}_{\omega_d \omega_d}) \end{bmatrix}. \quad (33)$$

We easily prove that  $r := \#\mathcal{Z}_{\mathbb{C}}(I) = \text{rank}(\text{TrM})$ . This gives us an easy way of testing whether a polynomial  $u$  is separating: in such a case,  $\deg(\tilde{\chi}_u)$  should be equal to  $r$ . Furthermore, we have that the set of polynomials  $\mathcal{S}(I) := \{x_1 + kx_2 + \dots + k^{N-1}x_N \mid 0 \leq k \leq (N-1)\binom{r}{2}\}$  contains at least one separating polynomial.

## 5 Linear algebra in the quotient

In this approach, most of the computational cost of a RUR thus lies in getting the parametric trace matrix of the system:

$$\text{TrM}(\gamma_0, \gamma_1, \gamma_2) := \begin{bmatrix} \text{trace}(\mathbf{M}_{\omega_1 \omega_1}) & \dots & \text{trace}(\mathbf{M}_{\omega_1 \omega_d}) \\ \vdots & & \vdots \\ \text{trace}(\mathbf{M}_{\omega_d \omega_1}) & \dots & \text{trace}(\mathbf{M}_{\omega_d \omega_d}) \end{bmatrix}$$

This expensive symbolic computation is however done once for all,  $\forall(\gamma_0, \gamma_1, \gamma_2)$  (here offline using Maple) and also for any type of modulation afore-mentioned. This gives us a parametric matrix

$$\begin{bmatrix} 8 & 0 & 0 & 0 & 0 & -2\gamma_0 - 4\gamma_1 + 4\gamma_2 & -4\gamma_1 + 8\gamma_2 & 4\gamma_1 - 16\gamma_2 & 0 \\ 0 & 4\gamma_1 + 2\gamma_0 & -2\gamma_0 - 4\gamma_1 + 4\gamma_2 & -4\gamma_1 + 8\gamma_2 & 0 & 0 & 0 & 0 & -12\gamma_1^2 + 2\gamma_0\gamma_1 + 12\gamma_2\gamma_1 + 2\gamma_0\gamma_2 - 4\gamma_1^2 \\ 0 & -2\gamma_0 - 4\gamma_1 + 4\gamma_2 & -8\gamma_1 - 2\gamma_0 + 12\gamma_2 & 4\gamma_1 - 16\gamma_2 & 0 & 0 & 0 & 0 & 28\gamma_1^2 - 10\gamma_0\gamma_1 - 2\gamma_0\gamma_2 + 8\gamma_1^2 \\ 0 & -4\gamma_1 + 8\gamma_2 & 4\gamma_1 - 16\gamma_2 & -2\gamma_0 + 12\gamma_2 + 8\gamma_1 & 0 & 0 & 0 & 0 & -32\gamma_1^2 + 12\gamma_0\gamma_1 + 8\gamma_2\gamma_1 - 2\gamma_0\gamma_2 - 4\gamma_1^2 \\ -2\gamma_0 - 4\gamma_1 + 4\gamma_2 & 0 & 0 & 0 & 8\gamma_1^2 - 4\gamma_0\gamma_1 - 16\gamma_2\gamma_1 - 4\gamma_1\gamma_2 + 8\gamma_1^2 + 2\gamma_0^2 & -12\gamma_1^2 + 2\gamma_0\gamma_1 + 12\gamma_2\gamma_1 + 2\gamma_0\gamma_2 - 4\gamma_1^2 & 28\gamma_1^2 - 10\gamma_0\gamma_1 - 2\gamma_0\gamma_2 + 8\gamma_1^2 & 0 & 0 \\ -4\gamma_1 + 8\gamma_2 & 0 & 0 & 0 & -12\gamma_1^2 + 2\gamma_0\gamma_1 + 12\gamma_2\gamma_1 - 2\gamma_0\gamma_2 - 4\gamma_1^2 & 16\gamma_1^2 - 4\gamma_0\gamma_1 - 8\gamma_2\gamma_1 + 4\gamma_1^2 & -32\gamma_1^2 + 12\gamma_0\gamma_1 + 8\gamma_2\gamma_1 - 2\gamma_0\gamma_2 - 4\gamma_1^2 & 0 & 0 \\ 4\gamma_1 - 16\gamma_2 & 0 & 0 & 0 & 28\gamma_1^2 - 10\gamma_0\gamma_1 - 2\gamma_0\gamma_2 + 8\gamma_1^2 & -12\gamma_1^2 + 2\gamma_0\gamma_1 + 12\gamma_2\gamma_1 + 2\gamma_0\gamma_2 - 4\gamma_1^2 & 28\gamma_1^2 - 10\gamma_0\gamma_1 - 2\gamma_0\gamma_2 + 8\gamma_1^2 & 0 & 0 \\ 0 & -12\gamma_1^2 + 2\gamma_0\gamma_1 + 12\gamma_2\gamma_1 + 2\gamma_0\gamma_2 - 4\gamma_1^2 & 28\gamma_1^2 - 10\gamma_0\gamma_1 - 2\gamma_0\gamma_2 + 8\gamma_1^2 & -32\gamma_1^2 + 12\gamma_0\gamma_1 + 8\gamma_2\gamma_1 - 2\gamma_0\gamma_2 - 4\gamma_1^2 & 0 & 0 & 0 & 4\gamma_0\gamma_1 - 8\gamma_1^2 - 56\gamma_1\gamma_2 + 12\gamma_0\gamma_2 + 40\gamma_1\gamma_2 - 38\gamma_2^2\gamma_0 + 68\gamma_2^2\gamma_1 \end{bmatrix}$$

that we can now evaluate on the set of parameters obtained from the non-circular statistics of  $y[n]$ . E.g. for system  $(P)$  with  $\gamma_0 = 3$ ,  $\gamma_1 = 0$  and  $\gamma_2 = 1$ , we get

$$\text{TrM}(3, 0, 1) = \begin{bmatrix} 8 & 0 & 0 & 0 & -10 & 8 & -4 & 0 \\ 0 & 10 & -10 & 8 & 0 & 0 & 0 & -6 \\ 0 & -10 & 6 & 8 & 0 & 0 & 0 & -2 \\ 0 & 8 & -4 & 6 & 0 & 0 & 0 & 4 \\ -10 & 0 & 0 & 0 & 14 & -6 & -2 & 0 \\ 8 & 0 & 0 & 0 & -6 & 4 & 4 & 0 \\ -4 & 0 & 0 & 0 & -2 & 4 & -12 & 0 \\ 0 & -6 & -2 & 4 & 0 & 0 & 0 & -10 \end{bmatrix}$$

From this matrix, we get that  $u := x_1 + 2x_2 + 4x_3$  is separating, and thus the following RUR for  $(P)$ :

$$\begin{aligned} \chi_u(t) &= (t - \frac{5}{2} - \frac{3}{2}\sqrt{5})(t - \frac{5}{2} + \frac{3}{2}\sqrt{5})(t + \frac{5}{2} - \frac{3}{2}\sqrt{5}) \\ &\quad (t + \frac{5}{2} + \frac{3}{2}\sqrt{5})(t - 3 - 2j)(t - 3 + 2j) \\ &\quad (t + 3 - 2j)(t + 3 + 2j) \end{aligned}$$

$$\begin{aligned} \text{and } g_u(1, t) &= 90t^6 - 2176t^4 + 36990t^2 - 33800, \\ g_u(x_1, t) &= 22t^7 - 776t^5 + 8450t^3 - 20800t, \\ g_u(x_2, t) &= -14t^7 + 600t^5 - 11890t^3 + 23400t, \\ g_u(x_3, t) &= 24t^7 - 650t^5 + 13080t^3 - 14950t. \end{aligned}$$

Hence, the following eight solutions for  $[h[0]^2, h[1]^2, h[2]^2]$

$$\begin{aligned} & \{[-\frac{1}{2} + \frac{1}{2}\sqrt{5}, 0, \frac{1}{2} + \frac{1}{2}\sqrt{5}], [-\frac{1}{2} - \frac{1}{2}\sqrt{5}, 0, \frac{1}{2} - \frac{1}{2}\sqrt{5}], \\ & [\frac{1}{2} + \frac{1}{2}\sqrt{5}, 0, -\frac{1}{2} + \frac{1}{2}\sqrt{5}], [\frac{1}{2} - \frac{1}{2}\sqrt{5}, 0, -\frac{1}{2} - \frac{1}{2}\sqrt{5}], \\ & [-1, -j, -1], [-1, j, -1], [1, -j, 1], [1, j, 1]\}. \end{aligned}$$

By solving now for  $[h[0], h[1], h[2]]$ , we thus get the 64 possible solutions for system (17).

This second (on-line) stage of the algorithm does not require any symbolic computation. The RUR of the system is easily derived from the evaluated matrix using Matlab or Scilab. The best solution is then selected from the possible solutions by introducing circular statistics of  $y[n]$  as in [21] (or alternatively higher-order statistics),

$$c_p := \text{E}(y[n]y^*[n-p]) = \sum_{m=p}^{N-1} h[m]h^*[m-p]. \quad (34)$$

## 6 Conclusion

Inspired by the works in [21], [23] and [24], we introduce here a new approach to the problem of blind channel identification for PSK-like modulations. With this approach, we are able to get an exhaustive description of the solution space. Furthermore, the algorithm proposed shows a rather small on-line computational cost since the expensive symbolic computation of the parametric trace-matrix is obtained offline once for all. The solutions of the problem are then easily obtained from this representation by solving a single univariate polynomial equation. Also, this approach should also generalize easily to many problems that can be written in the form of systems of polynomial equations of the form (13) or (15).

## References

- [1] J. G. Proakis, Digital Communications, McGraw-Hill, 1995, 3rd edition.
- [2] T. Soderstrom, P. Stoica, System Identification, Prentice-Hall, 1989.
- [3] L. Ljung, T. Soderstrom, Theory and Practice of Recursive Identification, MIT Press, Cambridge, 1983.
- [4] T. Kailath, Linear Systems, Prentice-Hall, 1980.

- [5] D. Godard, Self recovering equalization and carrier tracking in two dimensional data communication systems, *IEEE Trans. Com.* 28 (11) (1980) 1867–1875.
- [6] D. Donoho, On minimum entropy deconvolution, in: *Applied time-series analysis II*, Academic Press, 1981, pp. 565–609.
- [7] D. Gesbert, P. Duhamel, Unbiased blind adaptive channel identification and equalization, *IEEE Trans. on Sig. Proc.* 48 (1) (2000) 148–158.
- [8] K. Abed-Meraim, et al., On subspace methods for blind identification of SIMO FIR systems, *IEEE Trans. Sig. Proc.* 45 (1) (1997) 42–55, special issue on communications.
- [9] D. Gesbert, P. Duhamel, S. Mayrargue, On-line blind multichannel equalization based on mutually referenced filters, *IEEE Trans. Sig. Proc.* 45 (9) (1997) 2307–2317.
- [10] G. B. Giannakis, S. D. Halford, Blind fractionally spaced equalization of noisy FIR channels: Direct and adaptive solutions, *IEEE Trans. Sig. Proc.* 45 (9) (1997) 2277–2292.
- [11] G. Xu, H. Liu, L. Tong, T. Kailath, A least-squares approach to blind channel identification, *IEEE Trans. Sig. Proc.* 43 (12) (1995) 813–817.
- [12] A. J. van der Veen, A. Paulraj, An analytical constant modulus algorithm, *IEEE Trans. Sig. Proc.* 44 (5) (1996) 1136–1155.
- [13] D. Yellin, B. Porat, Blind identification of FIR systems excited by discrete-alphabet inputs, *IEEE Trans. Sig. Proc.* 41 (3) (1993) 1331–1339.
- [14] S. Benedetto, E. Biglieri, V. Castellani, *Digital Transmission Theory*, Prentice-Hall, 1987.
- [15] G. L. Stüber, *Principles of Mobile Communications*, Kluwer, 1996.
- [16] J. Lebrun, P. Comon, Blind identification of communication channels - Symbolic solution algorithms In preparation.
- [17] L. Gonzalez-Vega, F. Rouillier, M.-F. Roy, *Some Tapas of Computer Algebra*, Springer-Verlag, 1999, Ch. Symbolic recipes for polynomial system solving.
- [18] B. Mourrain, An introduction to linear algebra methods for solving polynomial equations, in: E. Lipitakis (Ed.), *Proc. HERCMA'9, 1999*, pp. 179–200.
- [19] G. Pistone, E. Riccomagno, H. P. Wynn, *Algebraic Statistics: Computational Commutative Algebra in Statistics*, Chapman & Hall, CRC Press, 2000.
- [20] B. Sturmfels, *Solving Systems of Polynomial Equations*, no. 97 in CBMS series, AMS, 2002.
- [21] O. Grellier, P. Comon, B. Mourrain, P. Trebuchet, Analytical blind channel identification, *IEEE Trans. Signal Proc.* 50 (9).
- [22] J. Lebrun, I. Selesnick, Gröbner bases and wavelet design, *J. Symb. Comp.* 35, to appear.

- [23] P. Trebuchet, Vers une résolution stable et rapide des équations algébriques, Ph.D. thesis, INRIA - Sophia-Antipolis (2002).
- [24] F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, *J. App. Alg. Eng., Comm. and Comp.* 9 (1999) 433–461.