A LINEAR ALGEBRA APPROACH TO SYSTEMS OF POLYNOMIAL EQUATIONS WITH APPLICATION TO DIGITAL COMMUNICATIONS

Jérôme Lebrun and Pierre Comon

Laboratoire I3S - CNRS/UNSA, Sophia-Antipolis, France
Email: {lebrun,comon}@i3s.unice.fr

ABSTRACT

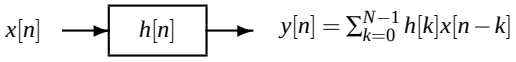
We introduce in this paper a new algebraic approach to some problems arising in signal processing and communications that can be described as or reduced to systems of multivariate quadratic polynomial equations. Based on methods from computational algebraic geometry, the approach achieves a full description 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 trace-matrix representation of the problem using normal forms. The solutions of the problem are then easily obtained from this representation by solving a single univariate polynomial equation. This approach is quite general and can be applied to a wide variety of problems: SISO channel identification of PSK modulations but also filter design and possibly MIMO blind source separation by deflation.

1. INTRODUCTION

Recently, major advances have been achieved in the field of computational algebraic geometry, which lead to new efficient ways to deal with one of the central application of computer algebra: solving systems of multivariate polynomial equations [2, 8, 15, 16, 20]. By using the new algorithms introduced, many practical problems can now be solved in a way that is very competitive with numerical methods as recently illustrated in the special issue on computer algebra and signal processing of the Journal of Symbolic Computation (Vol.37(2), Feb. 2004). In this issue [12], we detail the use of symbolic methods in order to solve some advanced design problems arising in signal processing, more precisely the construction of wavelet filters for which the usual spectral factorization approach (used for example to construct the well-known Daubechies filters) is not applicable. For these problems, we show how the design equations can be written as multivariate polynomial systems of equations and accordingly how Gröbner algorithms [2] offer an effective way to obtain solutions of practical interest in many of these cases. These examples of multiwavelet bases and wavelet frames could not have obtained without the use of tools from algebraic geometry and tend to prove that although their high computational and memory costs, Gröbner bases are indeed effective tools for the theoretical study and practical design of filter banks. In another direction, we have also investigated [9, 11] resultants methods [20] for some problems in digital communications similar to the one exposed in this paper.

However, among these most promising approaches to solve systems of polynomial equations, i.e. Gröbner bases, homotopic continuation, or resultants show some limitations [9, 12] (typ. very high computational cost in time and memory, difficulties to deal with parametric equations, limitations to 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 new ad-hoc approach derived from the works in [9, 22, 19]. In our approach, most of the expensive computation is done *offline* through the pre-computation of a parametric normal form of the system. The solutions of the system are then easily obtained through the computation of a Rational Univariate Representation (RUR). As a consequence, the on-line computational cost lies in isolating the roots of an univariate polynomial of degree the number of solutions (with multiplicities) of the system.

In this paper, we will deal with one important issue in digital communications (*e.g.* cellular): to mitigate the effects of the propagation channel. This is the role of the equalizer. Reliable equalizers have been developed, but usually need prior knowledge of the channel [17, ch.10]. A good estimation of the channel (also referred to as channel identification) is thus necessary and quite critical. We will consider here 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 $h[n]$. We assume furthermore that $h[n]$ has finite impulse response (FIR).



Most identification algorithms rely on the knowledge of the output $y[n]$ of the channel for a given input $x[n]$ [10, 13]. 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 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 the stealth interception of digital communications with no or encrypted pilot sequences.

Blind identification or equalization is not a new subject, for it has been addressed as early as in 1980 [7] [3]. 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 [4] [1] [5] [6] [24], or (ii) block calculations (i.e. removal of time recursions) [23] [25].

Our present contribution concerns block blind identification algorithms when diversity cannot be exploited. With this respect, our approach is similar to [23], where inputs are assumed to belong to the unit circle, and to [25, 18] 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, $\pi/4$-DQPSK, 8-PSK or $3\pi/8$-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 of the output $y[n]$. Now, making use of methods coming from computational algebraic geometry, we get an efficient and exhaustive estimate of $h[0],\ldots,h[N-1]$ from the sole observations $\{y[n]\}$.

2. POLYNOMIAL SETTINGS

For PSK-type modulations, the symbols are roots of unity [21]. By using this property and introducing *non-circular* statistics on $y[n]$, we get the following polynomial equations in $h[n]$.

BPSK, QPSK, 8-PSK and 2^M-PSK: For BPSK, $x[n]$ is iid discrete-uniform $\{-1,1\}$. We get then for $p=0,\ldots,N-1$,

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

For QPSK, $x[n]$ is iid discrete-uniform $\{1,j,-1,-j\}$, which gives $\mathrm{E}(y[n]y[n-p_1]y[n-p_2]y[n-p_3]) = \sum_{m=\max(p_1,p_2,p_3)}^{N-1} h[m]h[m-p_1]h[m-p_2]h[m-p_3]$. This case is easily reduced to the BPSK case by taking $p_1=0, p_3=p_2$ and $g[n] := h^2[n]$. Alike, the 8-PSK and in general all 2^M-PSK modulations can be reduced to the BPSK equations (1).

MSK, $\frac{\pi}{4}$-DQPSK, $\frac{3\pi}{8}$-D8PSK and D2^M-PSK: For MSK, we have $x[n] = j^n b[n]x[0]$ with $b[n]$ BPSK [11]. So, for $p=0,\ldots,N-1$,

$$\gamma_p := \mathrm{E}(y[n]y[n-p]|x[0]) = \sum_{m=p}^{N-1} (-1)^{n-m} h[m]h[m-p]. \tag{2}$$

As above, the $\frac{\pi}{4}$-DQPSK, $\frac{3\pi}{8}$-D8PSK and D2^M-PSK cases can be reduced to the MSK equations (2).

E.g. for $\frac{3\pi}{8}$-D8PSK and $N=3$, we get the following system of polynomial equations, where $\gamma_0,\gamma_1,\gamma_2$ are parameters:

$$\begin{cases} \gamma_0 - h[0]^8 + h[1]^8 - h[2]^8 = 0 \\ \gamma_1 - h[0]^4 h[1]^4 + h[1]^4 h[2]^4 = 0 \\ \gamma_2 - h[0]^4 h[2]^4 = 0. \end{cases} \tag{3}$$

Now, from Bézout's theorem [2], this system has either infinitely many solutions, either exactly 512 (with multiplicities), or no solution.

To illustrate our algorithm, we will focus on this example. This approach is easily generalized [11] to $N=2,\ldots,9$ and the two afore-mentioned families of modulations (BPSK, QPSK, 8-PSK and MSK, $\frac{\pi}{4}$-DQPSK, $\frac{3\pi}{8}$-D8PSK).

3. ALGEBRAIC GEOMETRY

By the following generic change of variables, $g[0] = h[0]^4 := x_1, g[1] = h[1]^4 := x_1 + x_2, g[2] = h[2]^4 := x_1 + x_2 + x_3$, system (3) can be rewritten as

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

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

$$\begin{cases} x_1^2 = \gamma_2 - x_1x_2 - x_1x_3 \\ x_2^2 = -\gamma_1 - x_1x_2 - x_1x_3 - x_2x_3 \\ x_3^2 = \gamma_0 - \gamma_2 + x_1x_2 - x_1x_3 - 2x_2x_3. \end{cases} \tag{4}$$

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

$$\mathscr{B} := \{1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}. \tag{5}$$

Using again Bézout's theorem, it is easily seen that $\mathscr{B}$ is indeed a linear base of the d-dimensional quotient algebra $\mathscr{A} := \mathbb{C}[x_1,\ldots,x_N]/I$ where $I = \langle P\rangle$ denotes the ideal generated by (P).

By working in this setting, solving system (P) is just a problem of linear algebra. More details on the use of linear algebra in algebraic geometry can be obtained from [15] or [20]. Intuitively, starting from a list (P) of polynomials such that the generated ideal $I = \langle P\rangle$ is zero-dimensional (finite number of solutions), the quotient space $\mathscr{A} := \mathbb{C}[x_1,\ldots,x_N]/I$ inherits a structure of finite-dimensional algebra. Constructing the multiplication table $[\omega_k\omega_l]_{k,l}$ of $\mathscr{A}$ gives then a full description of the linear algebraic framework associated to system (P). The central problem is then to choose a convenient linear basis $\mathscr{B} := \{\omega_1,\ldots,\omega_d\}$ called the *monomial basis* of $\mathscr{A}$ and get the associated normal form $\overline{p} = \mathrm{NF}(p,I) \in \mathscr{A}$ for $p \in \mathbb{C}[x_1,\ldots,x_N]$ (intuitively the "residue" modulo I of p in $\mathscr{A}$). A usual way to get a convenient monomial basis and its associated normal form is through the computation of a reduced Gröbner basis and the so-called monomials under the staircase [8, 19]. This is however not very efficient from a computational point of view in general and even more in our framework of PSK-type modulations, since the monomial basis given by (5) is in our case always a bonafide linear basis of $\mathscr{A}$. Also, any element $\overline{p} \in \mathscr{A}$ can be expressed as a vector $[p]$ in $\mathscr{B}$ as $\overline{p} = \sum_{k=1}^{d} [p]_k \omega_k$. In our example, using (4) we get

$$[x_1^2] = [\gamma_2 \quad 0 \quad 0 \quad 0 \quad -1 \quad -1 \quad 0 \quad 0]^\top.$$

A complete description of the normal form is easily obtained by multiplying and solving system (4) by the monomials in $\mathscr{B}$. We introduce the linear operator $\mathbf{M}_u$ on $\mathscr{A}$,

$$\begin{aligned} \mathbf{M}_u : \mathscr{A} &\to \mathscr{A} \\ \overline{p} &\mapsto \mathbf{M}_u\overline{p} := \overline{up}. \end{aligned}$$

and associate it with its $\mathbb{C}^{d\times d}$ matrix representation in the monomial basis of $\mathscr{A}$. This matrix is computed by expressing $u\omega_k$ in the monomial basis $\mathscr{B}$ which gives the k^{th} column of $\mathbf{M}_u$. For $[u] \in \mathscr{A}$, we thus get the multiplication matrix $\mathbf{M}_u[v] := [uv]$ on $\mathbb{C}^d$. E.g. for $u = x_1$, since

$$x_1\mathscr{B} = \{x_1, x_1^2, x_1x_2, x_1x_3, x_1^2x_2, x_1^2x_3, x_1x_2x_3, x_1^2x_2x_3\},$$

we get from (4) and the computation of the normal form,

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

and in the same way $\mathbf{M}_{x_2},\ldots,\mathbf{M}_{x_N}$.

The computation of $\mathbf{M}_u$ gives some important information on the set of solutions of the system, $\mathscr{Z}_{\mathbb{C}}(I) := \{\alpha \in \mathbb{C}^n \,|\, \forall p \in P, p(\alpha) = 0\}$ and the system in general. Denoting by $\mu(\alpha)$ the multiplicity of a solution α of (P), we get by Stickelberger theorem [14, 20] that $\mathbf{M}_u$ has eigenvalues $u(\alpha)$ with multiplicity $\sum_{\beta\in\mathscr{Z}(I), u(\beta)=u(\alpha)} \mu(\beta)$. As a consequence, we have the following properties

$$\begin{aligned} \det(\mathbf{M}_u) &= \prod_{\alpha\in\mathscr{Z}_{\mathbb{C}}(I)} u(\alpha)^{\mu(\alpha)} \\ \mathrm{trace}(\mathbf{M}_u) &= \sum_{\alpha\in\mathscr{Z}_{\mathbb{C}}(I)} \mu(\alpha)u(\alpha) \\ \chi_u(t) := \det(t\mathbf{I} - \mathbf{M}_u) &= \prod_{\alpha\in\mathscr{Z}_{\mathbb{C}}(I)} (t-u(\alpha))^{\mu(\alpha)}. \end{aligned}$$

Now, factorizing $\chi_u(t)$, the characteristic polynomial of $\mathbf{M}_u$, would then give $u(\alpha)$ for any solution α of the system. We would then easily get the solutions of the system by taking $u = x_1,\ldots,x_N$ and obtaining so the coordinates of α.

Unfortunately, computing directly the characteristic polynomial (incl. the determinant) of a matrix like $\mathbf{M}_u$ and factorizing it is very time and memory consuming (and in fact usually intractable).

We detail here an alternative method originally due to Kronecker. This is based on the computation of traces of matrices and takes advantage of the special structure of the matrices $\mathbf{M}_u$. Writing $\chi_u(t) = \sum_{k=0}^{d} b_k t^{d-k}$ and let $\chi_u'(t)$ be its derivative, then

$$\frac{\chi_u'(t)}{\chi_u(t)} = \sum_{\alpha \in \mathscr{Z}_{\mathbb{C}}(I)} \frac{\mu(\alpha)}{t-u(\alpha)} = \sum_{\alpha \in \mathscr{Z}_{\mathbb{C}}(I)} \frac{1}{t} \frac{\mu(\alpha)}{1-\frac{u(\alpha)}{t}}$$
$$= \sum_{\alpha \in \mathscr{Z}_{\mathbb{C}}(I)} \sum_{k \geq 0} \frac{1}{t} \mu(\alpha) u^k(\alpha) t^{-k} = \sum_{k \geq 0} \mathrm{trace}(\mathbf{M}_{u^k}) t^{-(k+1)}.$$

So, we have $\chi_u'(t) = \chi_u(t) \sum_{k \geq 0} \mathrm{trace}(\mathbf{M}_{u^k}) t^{-(k+1)}$, and since $\chi_u'(t) = \sum_{k=0}^{d-1} (d-k) b_k t^{d-1-k}$, this yields, using the definition of $\chi_u(t)$,

$$(d-k) b_k = \sum_{l=0}^{k} \mathrm{trace}(\mathbf{M}_{u^l}) b_{k-l}. \tag{6}$$

This gives a triangular system of linear equations involving the scalars: $\mathrm{trace}(\mathbf{M}_{u^k})$ for $k = 0, \ldots, d$. From (6), we easily compute b_k for $k = 0, \ldots, d$ and so $\chi_u(t)$.

Introducing the minimal polynomial $\tilde{\chi}_u(t)$,

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

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

$$\begin{array}{rcl} g_u : \mathscr{A} & \to & \mathbb{C}[x_1, \ldots, x_N] \\ \overline{v} & \mapsto & g_u(v,t) := \sum_{\alpha \in \mathscr{Z}_{\mathbb{C}}(I)} \mu(\alpha) v(\alpha) \frac{\tilde{\chi}_u(t)}{t-u(\alpha)}. \end{array}$$

This can be rewritten as

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

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

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

Hence, the central result of the rational univariate representation,

$$\frac{g_u(v, u(\alpha))}{g_u(1, u(\alpha))} = v(\alpha), \tag{7}$$

since for $v = x_1, \ldots, x_N$, we obtain

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

Hence, the following theorem giving a one-to-one mapping of the solutions of the multivariate system (P) onto the roots of the univariate polynomial $\chi_u(t)$,

Theorem. *If α is a solution of the system, then $u(\alpha)$ is a root of $\chi_u(t)$ with the same multiplicity and conversely, if ζ is a root of $\chi_u(t)$, then $\left[\frac{g_u(x_1,\zeta)}{g_u(1,\zeta)}, \frac{g_u(x_2,\zeta)}{g_u(1,\zeta)}, \ldots, \frac{g_u(x_N,\zeta)}{g_u(1,\zeta)} \right]$ 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 have

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

Writing $\tilde{\chi}_u(t) = \sum_{k=0}^{r} a_k t^{r-k}$ 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

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

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

$$\mathrm{Tr}(f) := [\mathrm{trace}(\mathbf{M}_{f\omega_1}), \quad \ldots, \quad \mathrm{trace}(\mathbf{M}_{f\omega_d})].$$

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

As a result, all the scalars $\mathrm{trace}(\mathbf{M}_{u^k v})$, for $k = 0, \ldots, r$ and $v = 1, x_1, \ldots, x_N$ are easily derived from the trace matrix $\mathrm{Tr}\mathbf{M}$ defined by $[\mathrm{Tr}\mathbf{M}]_{k,l} := \mathrm{trace}(\mathbf{M}_{\omega_k \omega_l})$, i.e.

$$\mathrm{Tr}\mathbf{M} := \begin{bmatrix} \mathrm{trace}(\mathbf{M}_{\omega_1\omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_1\omega_d}) \\ \vdots & & \vdots \\ \mathrm{trace}(\mathbf{M}_{\omega_d\omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_d\omega_d}) \end{bmatrix}.$$

Furthermore since $\mathrm{rank}(\mathrm{Tr}\mathbf{M}) = \#\mathscr{Z}_{\mathbb{C}}(I) = r$, we also have an easy way of testing whether a polynomial u is separating and thus of validating the solutions obtained: in such a case, $\deg(\tilde{\chi}_u)$ should be equal to r. Moreover, the set of linear polynomials $\mathscr{S}(I) := \{x_1 + kx_2 + \ldots + k^{N-1}x_N \,|\, 0 \leq k \leq (N-1)\binom{r}{2}\}$ contains at least one separating polynomial. Another way of getting with probability 1 a separating polynomial is to take at random $u = U_1 x_1 + \ldots + U_N x_n$ where $U_1, \ldots, U_N$ are iid continuous uniform $[0,1]$.

4. LINEAR ALGEBRA IN THE QUOTIENT

In this approach, most of the computational cost lies in getting the parametric trace matrix $\mathrm{Tr}\mathbf{M}(\gamma_0, \gamma_1, \gamma_2)$ of the system. This expensive symbolic computation is however done once for all, i.e. for any value of the parameters $\gamma_0, \gamma_1, \gamma_2$ and also for any type of modulation afore-mentioned. This gives us a sparse parametric matrix (given in Figure 1 for the case $N = 3$ and $3\pi/8$-D8PSK) that we can now evaluate on the considered block of signal by plugging in the set of parameters obtained from the non-circular statistics on $y[n]$. E.g. for system (P) with $\gamma_0 = 3, \gamma_1 = 0$ and $\gamma_2 = 1$, we get

$$\mathrm{Tr}\mathbf{M}(3,0,1) = \begin{bmatrix} 8 & 0 & 0 & 0 & -10 & 8 & -4 & 0 \\ 0 & 10 & -10 & 8 & 0 & 0 & 0 & -6 \\ 0 & -10 & 6 & 8 & 0 & 0 & 0 & -2 \\ 0 & 8 & -4 & 6 & 0 & 0 & 0 & 4 \\ -10 & 0 & 0 & 0 & 14 & -6 & -2 & 0 \\ 8 & 0 & 0 & 0 & -6 & 4 & 4 & 0 \\ -4 & 0 & 0 & 0 & -2 & 4 & -12 & 0 \\ 0 & -6 & -2 & 4 & 0 & 0 & 0 & -10 \end{bmatrix}.$$

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

$$\begin{aligned} \chi_u(t) &= t^8 - 45t^6 + 544t^4 - 6165t^2 + 4225 \\ \text{and} \quad g_u(1,t) &= 90t^6 - 2176t^4 + 36990t^2 - 33800, \\ g_u(x_1,t) &= 22t^7 - 776t^5 + 8450t^3 - 20800t, \\ g_u(x_2,t) &= -14t^7 + 600t^5 - 11890t^3 + 23400t, \\ g_u(x_3,t) &= 24t^7 - 650t^5 + 13080t^3 - 14950t. \end{aligned}$$

Now, the roots of $\chi_u(t)$ are usually easily isolated from the trace matrix [14]. But in this special case, we can even compute an exact factorization,

$$\chi_u(t) = (t - \tfrac{5}{2} - \tfrac{3}{2}\sqrt{5})(t - \tfrac{5}{2} + \tfrac{3}{2}\sqrt{5})(t + \tfrac{5}{2} - \tfrac{3}{2}\sqrt{5})(t + \tfrac{5}{2} + \tfrac{3}{2}\sqrt{5})(t-3-2j)(t-3+2j)(t+3-2j)(t+3+2j),$$

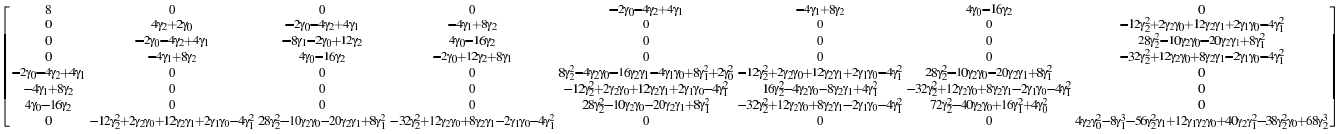


Figure 1: Parametric trace matrix for N=3.

and so the following eight solutions for $[h[0]^4, h[1]^4, h[2]^4]$

$$\{[-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{5}, 0, \tfrac{1}{2}+\tfrac{1}{2}\sqrt{5}], [-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}, 0, \tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}],$$
$$[\tfrac{1}{2}+\tfrac{1}{2}\sqrt{5}, 0, -\tfrac{1}{2}+\tfrac{1}{2}\sqrt{5}], [\tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}, 0, -\tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}],$$
$$[-1,-j,-1], [-1,j,-1], [1,-j,1], [1,j,1]\}.$$

By solving now for $[h[0], h[1], h[2]]$, we thus get 512 possible solutions for system (3).

This second (on-line) stage of the algorithm does not require any symbolic computation. The RUR of the system is easily computed from the evaluated trace matrix using Matlab or Scilab. The best solution is then selected from the set of possible solutions by introducing for example the circular statistics of $y[n]$, as in [9],

$$c_p := \mathrm{E}(y[n]y^*[n-p]) = \sum_{m=p}^{N-1} h[m]h^*[m-p]. \qquad (8)$$

or alternatively, another method making use of higher-order statistics to parse directly through the solutions $[h[0]^4, h[1]^4, h[2]^4]$ in order to reduce the size of the set of valid solutions.

5. CONCLUSION

We introduced 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 and depends only on the modulation type and the channel length but not on the channel itself. The solutions of the problem are then easily obtained from this representation by solving a single univariate polynomial equation. Also, this approach is general enough to be applied to many other problems that can be written in the form of systems of polynomial equations of the form (1) or (2).

REFERENCES

[1] K. Abed-Meraim et al. On subspace methods for blind identification of SIMO FIR systems. *IEEE Trans. Sig. Proc.*, 45(1):42–55, January 1997. Special issue on communications.

[2] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185 of *GTM*. Springer-Verlag, 1998.

[3] D. Donoho. On minimum entropy deconvolution. In *Applied time-series analysis II*, pages 565–609. Academic Press, 1981.

[4] D. Gesbert and P. Duhamel. Unbiased blind adaptive channel identification and equalization. *IEEE Trans. on Sig. Proc.*, 48(1):148–158, January 2000.

[5] D. Gesbert, P. Duhamel, and S. Mayrargue. On-line blind multichannel equalization based on mutually referenced filters. *IEEE Trans. Sig. Proc.*, 45(9):2307–2317, September 1997.

[6] G. B. Giannakis and S. D. Halford. Blind fractionally spaced equalization of noisy FIR channels: Direct and adaptive solutions. *IEEE Trans. Sig. Proc.*, 45(9):2277–2292, September 1997.

[7] D. Godard. Self recovering equalization and carrier tracking in two dimensional data communication systems. *IEEE Trans. Com.*, 28(11):1867–1875, November 1980.

[8] L. Gonzalez-Vega, F. Rouillier, and M.-F. Roy. *Some Tapas of Computer Algebra*, chapter Symbolic recipes for polynomial system solving. Springer-Verlag, 1999.

[9] O. Grellier, P. Comon, B. Mourrain, and P. Trebuchet. Analytical blind channel identification. *IEEE Trans. Signal Proc.*, 50(9), September 2002.

[10] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

[11] J. Lebrun and P. Comon. Blind identification of communication channels - Symbolic solution algorithms. Technical Report I3S/RR-2002-52-FR, Laboratoire I3S, CNRS/UNSA, 2002.

[12] J. Lebrun and I. Selesnick. Gröbner bases and wavelet design. *J. Symb. Comp., Special issue on Computer Algebra and Signal Processing*, 35(2):227–259, Feb. 2004.

[13] L. Ljung and T. Soderstrom. *Theory and Practice of Recursive Identification*. MIT Press, Cambridge, 1983.

[14] B. Mourrain. Computing isolated polynomial roots by matrix methods. *J. of Symb. Comp., Special Issue on Symbolic-Numeric Algebra for Polynomials*, 26(6):715–738, Dec. 1998.

[15] B. Mourrain. An introduction to linear algebra methods for solving polynomial equations. In E.A. Lipitakis, editor, *Proc. HERCMA'9*, pages 179–200, 1999.

[16] G. Pistone, E. Riccomagno, and H. P. Wynn. *Algebraic Statistics: Computational Commutative Algebra in Statistics*. Chapman & Hall, CRC Press, 2000.

[17] J. G. Proakis. *Digital Communications*. McGraw-Hill, 1995. 3rd edition.

[18] L. Rota and P. Comon. Blind equalizers based on polynomial criteria. In *ICASSP'04*, Montreal, May 17–21 2004.

[19] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *J. App. Alg. Eng., Comm. and Comp.*, 9:433–461, 1999.

[20] B. Sturmfels. *Solving Systems of Polynomial Equations*. Number 97 in CBMS series. AMS, 2002.

[21] G. L. Stüber. *Principles of Mobile Communications*. Kluwer, 1996.

[22] P. Trebuchet. *Vers une résolution stable et rapide des équations algèbriques*. PhD thesis, INRIA - Sophia-Antipolis, 2002.

[23] A. J. van der Veen and A. Paulraj. An analytical constant modulus algorithm. *IEEE Trans. Sig. Proc.*, 44(5):1136–1155, May 1996.

[24] G. Xu, H. Liu, L. Tong, and T. Kailath. A least-squares approach to blind channel identification. *IEEE Trans. Sig. Proc.*, 43(12):813–817, Dec. 1995.

[25] D. Yellin and B. Porat. Blind identification of FIR systems excited by discrete-alphabet inputs. *IEEE Trans. Sig. Proc.*, 41(3):1331–1339, 1993.