In *Proc. IEEE ISSPA*, Paris, France, July 1-4, 2003

AN ALGEBRAIC APPROACH TO BLIND IDENTIFICATION OF COMMUNICATION CHANNELS

Jérôme Lebrun and Pierre Comon

Projet Astre, I3S - CNRS/UNSA,
2000 route des Lucioles, BP.121,
F-06903 Sophia-Antipolis, France.
Email: {lebrun,comon}@i3s.unice.fr

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.

Keywords— 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 usually need prior knowledge of the channel [16, ch.10]. A good estimation of the channel (also referred to as channel identification) is thus necessary and quite critical.

In this paper, we consider 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).

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

Most identification algorithms rely on the knowledge of the output $y[n]$ of the channel for a given input $x[n]$ [18] [12] [9]. 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.

Blind identification or equalization is not a new subject, for it has been addressed as early as in 1980 [6] [2]. 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 [3] [1] [4] [5] [22], or (ii) block calculations (i.e. removal of time recursions) [21] [23].

Our contribution here lies in the field of block blind identification algorithms when diversity cannot be exploited. With this respect, our approach is similar to [21], where inputs are assumed to belong to the unit circle, and to [23] 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 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 EQUATIONS

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 $h[n]$.

BPSK, QPSK, 8-PSK: For BPSK, $x[n]$ is iid discrete-uni-

form $\{-1, 1\}$. We get for $p = 0, \ldots, N-1$,

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

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

$$\mathrm{E}(y[n]y[n-p_1]y[n-p_2]y[n-p_3]) = \sum_{m=\max(p_1,p_2,p_3)}^{N-1} h[m]h[m-p_1]h[m-p_2]h[m-p_3]. \quad (2)$$

This case 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^M-PSK modulations can be reduced to the BPSK case.

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

$$\gamma_p := \mathrm{E}(y[n]y[n-p]|x[0]) = \sum_{m=p}^{N-1} (-1)^{n-m} h[m]h[m-p]. \quad (3)$$

As above, 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.

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

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 [10]) for $N = 2, \ldots, 7$ 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

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 [7, 14, 15, 19]. 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 however some limitations [8, 11] (typ. high computational cost, non-parametric equations or only rational parameters) that hinder 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 [8], [20] and [17] in which most of the expensive computation is done offline through the pre-computation of a parametric normal form [20] 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 (4) can be rewritten as system (P),

$$(P) \begin{cases} \gamma_0 - x_1^2 - 2x_1x_3 - 2x_2x_3 - x_3^2, \\ \gamma_1 - x_1x_2 - x_2^2 - x_1x_3 - x_2x_3, \\ \gamma_2 - x_1^2 - x_1x_2 - x_1x_3. \end{cases} \quad (5)$$

We check that the monomials x_1^2, x_2^2 et x_3^2 can now be expressed in the monomial basis $\mathcal{B} = \{\omega_1, \ldots, \omega_d\}$ given by

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

It is then easily seen that $\mathcal{B}$ is indeed a linear base of the d-dimensional quotient algebra $\mathcal{A} := \mathbb{Q}[x_1, \ldots, x_N]/\langle P\rangle$ where $\langle P\rangle$ denotes the ideal generated by (P). By working in this setting, solving system (P) can now be seen as a problem of linear algebra. Namely, by introducing for any polynomial $[u] \in \mathcal{A}$, the multiplication operator $\mathbf{M}_u[v] := [uv]$ on $\mathcal{A}$ and expressing it in its matrix form in $\mathcal{A}$, we get by Stickelberger's theorem [13] that

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

where $\mathcal{Z}_{\mathbb{C}}(\langle P\rangle)$ denotes the set of complex solutions of system (P). Consequently for a well-chosen u (i.e. u separating the solutions of (P)), we get a one-to-one mapping of the solutions of the system of multivariate polynomial equations (P) onto the roots of the univariate polynomial $\chi_u(t)$. Furthermore, by introducing the following family of polynomials,

$$g_u(v,t) := \sum_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(\langle P\rangle)} \mu(\boldsymbol{\alpha}) v(\boldsymbol{\alpha}) \prod_{\boldsymbol{\beta} \in \mathcal{Z}_{\mathbb{C}}(\langle P\rangle) \setminus \{\boldsymbol{\alpha}\}} (t - u(\boldsymbol{\beta})),$$

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

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

From this, we derive the central result of rational univariate representation

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

Hence, for $v = x_1, \ldots, x_N$, we get an easy way to express the coordinates of the solutions of (P) from the roots of $\chi_u(t)$,

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

Theorem. *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 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, we still have to detail a practical way to compute $\chi_u(t)$ and $g_u(v, t)$. First, it is easily seen [17, 7, 10] that we can compute $\chi_u(t)$ from the scalars $\mathrm{trace}(\mathbf{M}_{u^k})$ for $k = 0, \ldots, d$ through the formula

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

Considering the minimal polynomial associated with $\chi_u(t)$,

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

we get in a similar way $g(v, t)$ by

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

Consequently, the $g_u(v, t)$ are easily computed from $\tilde{\chi}_u(t)$ and $\mathrm{trace}(\mathbf{M}_{u^k v})$, for $k = 0, \ldots, r$. Now, there is also an easy way to compute these traces since $\mathrm{trace}(\mathbf{M}_{fg}) = \mathrm{Tr}(f)[g]$ where

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

Also, since $\mathrm{Tr}(u^{k+1}) = \mathrm{Tr}(u^k)\mathbf{M}_u$, we get by induction $\mathrm{trace}(\mathbf{M}_{u^{k+1}}) = \mathrm{Tr}(u^k)[u]$ and $\mathrm{trace}(\mathbf{M}_{u^k v}) = \mathrm{Tr}(u^k)[v]$. So all the computations rely on the *trace matrix* defined by

$$[\mathrm{Tr}\mathbf{M}]_{i,j} := \mathrm{trace}(\mathbf{M}_{\omega_i \omega_j}) \tag{6}$$

Furthermore, $\mathrm{rank}(\mathrm{Tr}\mathbf{M}) = \#\mathcal{Z}_{\mathbb{C}}(I) = \deg(\tilde{\chi}_u) =: r$ iff u is separating. This gives an easy way to test if a polynomial is separating given that the set of polynomials $\mathcal{S}(I) := \{x_1 + kx_2 + \ldots + k^{N-1}x_N \,|\, 0 \leq k \leq (N-1)\binom{r}{2}\}$ contains at least one separating polynomial.

4. LINEAR ALGEBRA IN THE QUOTIENT

In this approach, most of the computational cost of a RUR $\{\chi_u(t), g_u(1, t), g_u(x_1, t), \ldots, g_u(x_N, t)\}$ thus lies in getting the parametric trace matrix of the system:

$$\mathrm{Tr}\mathbf{M}(\gamma_0, \gamma_1, \gamma_2) := \begin{bmatrix} \mathrm{trace}(\mathbf{M}_{\omega_1\omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_1\omega_d}) \\ \vdots & & \vdots \\ \mathrm{trace}(\mathbf{M}_{\omega_d\omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_d\omega_d}) \end{bmatrix}$$

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

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

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

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

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

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

By solving now for $[h[0], h[1], h[2]]$, we thus get the 64 possible solutions for system (4).

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 [8] (or alternatively higher-order statistics),

$$c_p := \mathrm{E}(y[n]y^*[n-p]) = \sum_{m=p}^{N-1} h[m]h^*[m-p]. \tag{7}$$

5. CONCLUSION

Inspired by the works in [8], [20] and [17], 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 (1) or (3).

6. 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. DONOHO. On minimum entropy deconvolution. In *Applied time-series analysis II*, pages 565–609. Academic Press, 1981.

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

[4] 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.

[5] 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.

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

[7] L. GONZALEZ-VEGA, F. ROUILLIER, and M.-F. ROY. *Some Tapas of Computer Algebra*, chapter Symbolic recipes for polynomial system solving. Springer-Verlag, 1999.

[8] O. GRELLIER, P. COMON, B. MOURRAIN, and P. TREBUCHET. Analytical blind channel identification. *IEEE Trans. Signal Proc.*, 50(9), September 2002.

[9] T. KAILATH. *Linear Systems*. Prentice-Hall, 1980.

[10] J. LEBRUN and P. COMON. Blind identification of communication channels - Symbolic solution algorithms. 2003. In preparation.

[11] J. LEBRUN and I. SELESNICK. Gröbner bases and wavelet design. *J. Symb. Comp.*, 35, 2003. To appear.

[12] L. LJUNG and T. SODERSTROM. *Theory and Practice of Recursive Identification*. MIT Press, Cambridge, 1983.

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

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

[15] G. PISTONE, E. RICCOMAGNO, and H. WYNN. *Algebraic Statistics: Computational Commutative Algebra in Statistics*. CRC Press, 2000.

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

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

[18] T. SODERSTROM and P. STOICA. *System Identification*. Prentice-Hall, 1989.

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

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

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

[22] 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.

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