In *Proc. GRETSI*, Paris, France, Sept. 8-11, 2003

Une approche algébrique de l'identification aveugle de canaux de communications

Jérôme LEBRUN et Pierre COMON
{lebrun,comon}@i3s.unice.fr
http://www.i3s.unice.fr/∼{lebrun,comon}

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

Résumé – Dans cet article est présentée une nouvelle approche au problème de l'identification aveugle de canaux SISO de communications pour les modulations de type PSK. L'intérêt majeur de cette approche issue de la géométrie algébrique réside dans l'obtention rapide d'une description exhaustive de l'espace des solutions permettant ainsi d'éviter les problèmes de minima locaux liés aux algorithmes adaptatifs. De plus, l'algorithme proposé requiert un faible coût de calcul *on-line* puisque, fondamentalement, il se réduit à l'isolation des racines d'un polynôme univarié; le pré-calcul symbolique d'une représentation paramétrique plus efficace du système étant réalisé *off-line* une fois pour toutes.

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.

Introduction

Un des problèmes essentiels en communications numériques, en particulier cellulaires, est la minimisation de l'influence du canal de communication. Un moyen usuel [19, ch.10] de résoudre ce problème consiste, dans un premier temps à estimer le canal, et ensuite à l'égaliser à l'aide d'un égalisateur (typiquement à boucle fermée afin de garantir la stabilité). Cette approche repose ainsi fortement sur la qualité de l'estimation, appelée aussi identification, du canal de communication.

Dans ce papier, nous nous restreignons au cas d'un canal de communication scalaire (SISO), linéaire et invariant dans le temps. Il peut alors être décrit comme le filtrage convolutif du signal émis $x[n]$ par un filtre $h[n]$ que nous supposons, de plus, à réponse impulsionnelle finie. Schématiquement, le modèle de canal envisagé est ainsi donné par :

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

La plupart des algorithmes d'identification repose sur la connaissance du signal reçu $y[n]$ pour un signal émis $x[n]$ donné [7, 12, 22] (utilisation de séquences pilotes comme dans le standard GSM ou d'un canal parallèle comme pour l'UMTS). Nous nous intéressons ici au problème plus général de l'identification aveugle où seul le signal reçu est connu. Actuellement, la plupart des algorithmes d'identification aveugle reposent sur une approche adaptative avec les limitations bien connues liées à la présence de minima locaux et à la lenteur de convergence. Diverses améliorations de ces algorithmes sont cependant possibles soit en utilisant les diversités spatiale, temporelle ou de bande-passante [26, 1, 4], soit par une approche par blocs mettant à profit les propriétés du signal $x[n]$ [27, 25], comme par exemple en communications numériques, où le signal émis $x[n]$ suit en général une loi de modulation connue (BPSK, MSK, QPSK, $\frac{\pi}{4}$-DQPSK, 8-PSK ou $\frac{3\pi}{8}$-D8PSK, et les diverses QAM pour les plus courantes). L'utilisation de cette information va ainsi nous permettre de reformuler le problème dans un cadre de géométrie algébrique et d'estimer efficacement et de façon exhaustive $h[0], \ldots, h[N-1]$ à partir des seules observations $\{y[n]\}$.

Formulation polynomiale du problème

En effet, pour les modulations de type PSK, les symboles sont des racines de l'unité. L'utilisation de statistiques *non-circulaires* sur le signal reçu $y[n]$ permet d'écrire le problème sous forme d'un système d'équations polynômiales en $h[n]$.

BPSK, QPSK, 8-PSK

Dans le cas BPSK, $x[n]$ est iid uniformément distribué sur $\{-1, 1\}$. On obtient alors pour $p = 0, \ldots, N-1$,

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

Pour le cas QPSK, $x[n]$ est iid uniformément distribué sur $\{1, j, -1, -j\}$ où $j^2 = -1$, ce qui donne

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

Ce cas se ramène au cas BPSK en prenant $p_1 = 0, p_3 = p_2$ et en posant $g[n] := h^2[n]$. De la même façon, les modulations 8-PSK et en général de type 2^M-PSK se réduisent au cas BPSK.

MSK, $\frac{\pi}{4}$-DQPSK, $\frac{3\pi}{8}$-D8PSK

Dans le cas MSK [8], on a $x[n] = j^n b[n] x[0]$, avec $b[n]$ BPSK et donc pour $p = 0, \ldots, N-1$,

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

De même que précédemment, les modulations $\frac{\pi}{4}$-DQPSK et $\frac{3\pi}{8}$-D8PSK se ramènent aisément au cas MSK.

Ainsi, pour une modulation MSK avec $N = 3$, on obtient le système d'équations polynômiales paramétriques en $\gamma_0, \gamma_1, \gamma_2$ suivant :

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

D'après le théorème de Bézout [23], ce système a soit une infinité de solutions, soit au plus huit solutions (en comptant les multiplicités).

Il nous reste maintenant à décrire une méthode efficace et robuste de résolution pour ce type de système d'équations polynômiales. A titre d'illustration, nous allons détailler dans le reste de l'article l'approche proposée pour le système (3). Cette approche se généralise (et a été implémentée avec succès) pour $N = 2, \ldots, 7$ dans le cadre des deux familles de modulations décrites ci-dessus (BPSK, QPSK, 8-PSK et MSK, $\frac{\pi}{4}$-DQPSK, $\frac{3\pi}{8}$-D8PSK).

Représentation rationnelle univariée

Récemment, diverses méthodes issues de la géométrie algébrique ont été appliquées avec succès à la résolution effective de systèmes d'équations polynômiales liés à des problèmes de traitement du signal [17, 3, 10, 9, 11, 13]. Ces approches algébriques présentent l'avantage d'une description exhaustive de l'espace des solutions et évite ainsi tout problème de minima locaux. De plus, depuis peu, diverses méthodes issues de la géométrie algébrique ont rendu possible et très compétitive la résolution effective de systèmes d'équations polynomiales [5, 2, 15, 18, 23]. Les approches les plus populaires que sont le calcul par bases de Gröbner, les méthodes de continuation homotopique et la résolution par résultants, présentent cependant dans leur implémentation classique, diverses limitations au niveau du coût de calcul et de la gestion de paramètres non rationnels dans les équations [6, 9]. Cela les rend relativement inadaptées à des cadres tels que ceux du traitement du signal ou des communications numériques où l'on ne dispose a priori que d'une faible puissance de calcul (typiquement le DSP d'un téléphone portable) avec de fortes contraintes temporelles (environnement évoluant rapidement, tel qu'un canal de communications mobiles). En témoigne le fait que, jusqu'à présent, l'utilisation de méthodes algébriques en traitement du signal a été essentiellement cantonnée à des problèmes de design de filtres, pour la plupart liés à la construction d'ondelettes [17, 3, 10, 9, 11, 13] ; les contraintes calculatoires et temporelles dans ces problèmes étant minimes. Également, dans la majorité des problèmes de traitement du signal et de communications numériques, les données sont essentiellement bruitées puisque obtenues par estimation statistique de moments. L'application directe de méthodes formelles pour la résolution des systèmes polynomiaux peut alors se révéler délicate (en particulier, la réduction à zéro dans le calcul de bases de Gröbner). De nouvelles approches [24, 6] permettant de mieux prendre en compte les aspects numériques dans les calculs algébriques, sont en train d'apparaître. C'est ainsi que nous avons été amenés à développer une nouvelle méthode adhoc [8] où l'on effectue un pré-calcul très coûteux, mais réalisé *off-line*, d'une forme normale paramétrique associée au système [24]. Le but de cette première étape est la réécriture de notre problème sous une forme paramétrique économique (stockage minimal), aisément exploitable (les solutions sont aisément obtenues) et robuste (une faible perturbation ne modifie pas trop les solutions). Dans une seconde étape, les solutions du système s'obtiennent alors aisément *on-line* après évaluation des paramètres ; ici, à partir d'une représentation univariée rationnelle (RUR) [5] du système (3), on a l'ensemble des solutions par un simple calcul des racines d'un polynôme univarié.

En effet, par le changement générique de variables $h[0] := x_1, h[1] := x_1 + x_2, h[2] := x_1 + x_2 + x_3$, on peut réécrire le système (3) sous une nouvelle forme :

$$(P) \begin{cases} \gamma_0 - x_1^2 - 2x_1x_3 - 2x_2x_3 - x_3^2, \\ \gamma_1 - x_1x_2 - x_2^2 - x_1x_3 - x_2x_3, \\ \gamma_2 - x_1^2 - x_1x_2 - x_1x_3. \end{cases} \tag{4}$$

Les monômes x_1^2, x_2^2 et x_3^2 peuvent désormais être décomposés dans la base monomiale $\mathcal{B} = \{\omega_1, \ldots, \omega_d\}$ donnée par

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

On montre aisément que $\mathcal{B}$ est une base linéaire de l'algèbre quotient (de dimension d) $\mathcal{A} := \mathbb{Q}[x_1, \ldots, x_N]/\langle P\rangle$ où $\langle P\rangle$ est l'idéal engendré par le système (P). Ré-écrites dans cette base, les équations du système (P) nous donnent une *forme normale* [24, 8] de $\mathbb{Q}[x_1, \ldots, x_N]$ dans l'algèbre quotient $\mathcal{A}$ qui à tout polynôme u associe le vecteur $[u] \in \mathbb{C}^d$ de décomposition dans la base $\mathcal{B}$ de la classe de u dans l'algèbre quotient $\mathcal{A}$. On est ainsi dans un cadre où la résolution du système (P) se réduit en fait à un problème d'algèbre linéaire. En effet, en introduisant pour tout polynôme u, l'opérateur de multiplication $\mathbf{M}_u[v] := [uv]$ sur $\mathcal{A}$ représenté par sa matrice $\mathbf{M}_u$ dans la base $\mathcal{B}$ (la k-ième colonne de cette matrice est obtenue en exprimant $[u\omega_k]$ dans la base monomiale $\mathcal{B}$), le théorème de Stickelberger nous donne alors [14, 23]

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

où $\mathcal{Z}_{\mathbb{C}}(\langle P\rangle)$ est l'ensemble des solutions complexes $\boldsymbol{\alpha}$ du système (P) et $\mu(\boldsymbol{\alpha})$ leurs multiplicités respectives. C'est à dire que pour un u bien choisi, i.e. un polynôme séparant les solutions, on a ainsi construit une bijection des solutions du système de polynômes multivariés (P) sur les racines du polynôme univarié $\chi_u(t)$. En introduisant désormais les polynômes

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

pour $\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)$ et $t = u(\boldsymbol{\alpha})$, on obtient

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

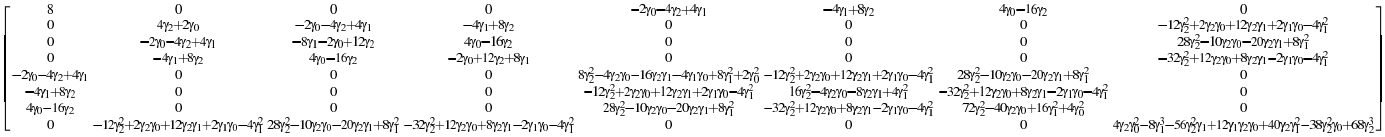

FIG. 1 – Matrice de trace paramétrique $\mathrm{TR}\mathbf{M}$ pour le cas MSK avec $N = 3$.

et le résultat central d'une représentation univariée rationnelle

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

En prenant successivement $v = x_1, \ldots, x_N$, on a donc un moyen rapide d'exprimer les coordonnés des solutions de (P) en fonction des racines de $\chi_u(t)$ puisque

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

D'où le théorème suivant :

Théorème. *Si $\boldsymbol{\alpha}$ est une solution du système (P), alors $u(\boldsymbol{\alpha})$ est une racine du polynôme univarié $\chi_u(t)$ avec la même multiplicité et réciproquement, si ζ est une racine de $\chi_u(t)$, alors*

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

est une solution du système (P) de même multiplicité.

Il nous reste enfin à montrer que l'on peut calculer facilement $\chi_u(t)$ et $g_u(v, t)$. Introduisons $\chi_u(t) = \sum_{k=0}^{d} b_k t^{d-k}$ ($b_0 = 1$) et $\chi'_u(t)$ sa dérivée, on a alors

$$\frac{\chi'_u(t)}{\chi_u(t)} = \sum_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} \frac{\mu(\boldsymbol{\alpha})}{t - u(\boldsymbol{\alpha})} = \sum_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} \frac{1}{t} \frac{\mu(\boldsymbol{\alpha})}{1 - \frac{u(\boldsymbol{\alpha})}{t}}$$

$$= \sum_{\boldsymbol{\alpha} \in \mathcal{Z}_{\mathbb{C}}(I)} \sum_{k \geq 0} \frac{1}{t} \mu(\boldsymbol{\alpha}) u^k(\boldsymbol{\alpha}) t^{-k} = \sum_{k \geq 0} \mathrm{trace}(\mathbf{M}_{u^k}) t^{-(k+1)}.$$

Ainsi, $\chi'_u(t) = \chi_u(t) \sum_{k \geq 0} \mathrm{trace}(\mathbf{M}_{u^k}) t^{-(k+1)}$, et comme $\chi'_u(t) = \sum_{k=0}^{d-1} (d-k) b_k t^{d-1-k}$, on obtient donc pour $k = 0, \ldots, d$,

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

Ce système triangulaire d'équations linéaires permet de calculer aisément $\chi_u(t)$ à partir des valeurs $\mathrm{trace}(\mathbf{M}_{u^k})$ pour $k = 0, \ldots, d$ [20, 5, 8]. En introduisant maintenant le polynôme minimal de $\mathbf{M}_u$,

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

et sa représentation de Hörner $H_k(\tilde{\chi}_u)(t) = \sum_{l=0}^{k} a_l t^{k-l}$ où $\tilde{\chi}_u(v, t) = \sum_{k=0}^{r} a_k t^{r-k}$, on obtient de la même façon

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

Les polynômes $g_u(v, t)$ se déduisent donc aisément de $\tilde{\chi}_u(t)$ et des valeurs $\mathrm{trace}(\mathbf{M}_{u^k v})$ pour $k = 0, \ldots, r$. Enfin, ces traces de matrices de multiplication sont facilement obtenues en remarquant que $\mathrm{trace}(\mathbf{M}_{fg}) = \mathrm{TR}(f)[g]$ où

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

Et comme $\mathrm{TR}(u^{k+1}) = \mathrm{TR}(u^k)\mathbf{M}_u$, on obtient les récurrences $\mathrm{trace}(\mathbf{M}_{u^{k+1}}) = \mathrm{TR}(u^k)[u]$ et $\mathrm{trace}(\mathbf{M}_{u^k v}) = \mathrm{TR}(u^k)[v]$. Ainsi, tous les calculs reposent sur l'obtention de la *matrice de trace* $\mathrm{TR}\mathbf{M}$ définie par :

$$[\mathrm{TR}\mathbf{M}]_{k,l} := \mathrm{trace}(\mathbf{M}_{\omega_k \omega_l}) \tag{5}$$

Enfin, comme $\deg(\tilde{\chi}_u) = \mathrm{rank}(\mathrm{TR}\mathbf{M}) = \#\mathcal{Z}_{\mathbb{C}}(I) =: r$ si et seulement si u est séparant et puisque l'ensemble

$$\{x_1 + k x_2 + \ldots + k^{N-1} x_N \,|\, 0 \leq k \leq (N-1)\binom{r}{2}\}$$

contient au moins un polynôme séparant [20, 5], on a également un moyen rapide de trouver un u séparant et par-là même occasion de valider l'ensemble des solutions trouvées.

Algèbre linéaire dans l'algèbre quotient

Dans cette approche, l'essentiel du coût de calcul d'une RUR $\{\chi_u(t), g_u(1, t), g_u(x_1, t), \ldots, g_u(x_N, t)\}$ du système (P) réside donc dans le pré-calcul de la matrice de trace paramétrique :

$$\mathrm{TR}\mathbf{M}(\gamma_0, \gamma_1, \gamma_2) := \begin{bmatrix} \mathrm{trace}(\mathbf{M}_{\omega_1 \omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_1 \omega_d}) \\ \vdots & & \vdots \\ \mathrm{trace}(\mathbf{M}_{\omega_d \omega_1}) & \ldots & \mathrm{trace}(\mathbf{M}_{\omega_d \omega_d}) \end{bmatrix}. \tag{6}$$

Ce pré-calcul est réalisé une fois pour toutes, i.e. $\forall(\gamma_0, \gamma_1, \gamma_2)$, de façon symbolique (dans notre cas grace au logiciel MuPAD [16]). Une RUR du système est alors aisément obtenue en évaluant la matrice de trace, donnée en Fig. 1, pour le jeu de paramètres estimés par les statistiques non-circulaires. Par exemple, pour le système (P) avec $\gamma_0 = 3, \gamma_1 = 0$ et $\gamma_2 = 1$, on obtient

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

On vérifie alors que le polynôme $u := x_1 + 2x_2 + 4x_3$ est séparant, ce qui nous donne la RUR suivante pour (P) :

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

On a ainsi huit solutions pour le système (3) en $[h[0], h[1], h[2]]$:

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

Cette seconde étape de l'algorithme est réalisée sous Scilab [21] et ne nécessite pas de calcul symbolique. La sélection finale de la meilleure solution peut finalement se faire en calculant les statistiques circulaires [6] sur $y[n]$

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

ou en utilisant des statistiques d'ordre supérieur [8].

Conclusion

Dans la continuation de travaux précédents [6], un nouvel algorithme de résolution basé sur le calcul de matrices de multiplications dans l'algèbre quotient et d'une représentation univariée rationnelle des solutions a ainsi été développé. L'intérêt majeur de cette méthode réside dans l'obtention rapide d'une description exhaustive de l'espace des solutions. L'algorithme proposé requiert en effet un faible coût de calcul *on-line* puisque essentiellement, il se réduit à l'isolation des racines d'un polynôme univarié de degré le nombre de solutions du système (le pré-calcul symbolique de la matrice de trace étant réalisé *off-line* une fois pour toute) ainsi qu'un faible coût de stockage puisque la matrice de trace paramétrique $\mathrm{Tr}\mathbf{M}$ s'avère être creuse. Cette approche a été appliquée avec succès à l'identification aveugle SISO dans le cadre des modulations de type BPSK et MSK (et leurs généralisations). On voit de plus aisément que cette méthode se généralise à tout problème décrit par un système d'équations du type (1) ou (2). De nombreuses autres applications en communications numériques sont ainsi envisageables.

Références

[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] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure & Appl. Algebra*, 139 :61–88, 1999. `https://calfor.lip6.fr/`

[3] J.-C. Faugère, F. Moreau de Saint-Martin, and F. Rouillier. Design of regular nonseparable bidimensional wavelets using Gröbner basis techniques. *IEEE Trans. Signal Proc.*, 46(4) :845–857, 1998.

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

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

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

[8] J. Lebrun and P. Comon. Blind identification of communication channels - Symbolic solution algorithms. 2003. In preparation.

[9] J. Lebrun and I. Selesnick. Gröbner bases and wavelet design. *J. Symb. Comp.*, 35, 2003. To appear.

[10] J. Lebrun and M. Vetterli. High order balanced multiwavelets : Theory, factorization and design. *IEEE Trans. Signal Proc.*, 49(9) :1918–1930, September 2001.

[11] J. Litlle. Solving the Selesnick-Burrus filter design equations using computational algebra and algebraic geometry. preprint, 2002.

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

[13] S. Mallat. Foveal approximations for singularities. *App. & Comp. Harm. Analysis*, 2001. submitted.

[14] 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.

[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] MuPAD. `http://www.mupad.com/`, Universität Paderborn, 2003.

[17] H. Park, T. Kalker, and M. Vetterli. Groebner bases and multidimensional fir multirate systems. *J. Multidimensional Sys. Signal*, 8 :11–30, 1996.

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

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

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

[21] Scilab. `http://www.scilab.org/`, INRIA, 2003.

[22] T. Soderstrom and P. Stoica. *System Identification*. Prentice-Hall, 1989.

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

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

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

[26] 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.

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