Inversion of polynomial systems and separation of nonlinear mixtures of finite-alphabet sources

Marc Castella

Inversion of polynomial systems and separation of nonlinear mixtures of finite-alphabet sources

Marc Castella
IT/TELECOM SudParis/Département CITI/UMR-CNRS 5157
9 rue Charles Fourier, 91011 Evry Cedex - France
e-mail: marc.castella@it-sudparis.eu
Tel: +33 1 60 76 41 71 Fax: +33 1 60 76 44 33

***Abstract*— In this contribution, Multi-Input Multi-Output (MIMO) mixing systems are considered, which are instantaneous and nonlinear but polynomial. We first address the problem of invertibility, searching the inverse in the class of polynomial systems. It is shown that Groebner bases techniques offer an attractive solution for testing the existence of an exact inverse and computing it.**

By noticing that any nonlinear mapping can be interpolated by a polynomial on a finite set, we tackle the general nonlinear case. Relying on a finite alphabet assumption of the input source signals, theoretical results on polynomials allow us to represent nonlinear systems as linear combinations of a finite set of monomials. We then generalize the first results to give a condition for the existence of an exact nonlinear inverse. The proposed method allows to compute this inverse in polynomial form.

In the light of the previous results, we go further to the blind source separation problem. It is shown that for sources in a finite alphabet, the nonlinear problem is tightly connected with both problems of underdetermination and of dependent sources. We concentrate on the case of two binary sources, for which an easy solution can be found. By simulation, this solution is compared to techniques borrowed from classification methods.

***Index Terms*— nonlinear systems, polynomials, Groebner bases, blind source separation, finite alphabet**

I. Introduction

For the last decades, deconvolution and signal restoration issues have been active research fields. In a multidimensional context for instance, the problem of source separation has received considerable attention [9], [11], [33], [30], [7]. It consists in the restoration of several original signals from the observation of several mixtures of them. Depending on context, different approaches may be considered: if a strong information on the mixing system is available, then non-blind separation methods can be developped based on this information. On the contrary, blind methods do not assume any a priori knowledge of the mixing system but they generally rely on the strong assumption of statistical independence of the source signals: this is the case in "Independent Component Analysis" (ICA) which is now a well recognized concept which corresponds to blind separation of an instantaneous linear mixture. Recently, other models have been considered, such as convolutive [12], [42], [39] or nonlinear ones [45], [31], [24].

In this paper, the case of a nonlinear mixture is tackled. More precisely, the aim is to answer the following two questions: (i) Does an inverse exist for a given nonlinear mixture? (ii) If yes, propose a method for blind recovery of the nonlinearly mixed sources. Both questions are obviously challenging and are tackled in a restricted context that allows to give an answer: polynomial nonlinearities are assumed to answer (i) and a finite-alphabet assumption is added to deal with (ii).

In the linear context, perfect invertibility conditions of Multi-Input/Multi-Output (MIMO) linear time invariant systems are well-known and they reduce to left-invertibility of matrices. The elements of the mixing and separating matrix are either scalars in the instantaneous case, or polynomials in the case of MIMO finite impulse response (FIR) filters. Polynomials in the matrices may have several variables in the case where multi-dimensional (e.g. images) and multi-channel signals are considered (see e.g. [43], [49]). On the other hand, we are not aware of any such general result in the nonlinear case, although previous results include [3], which presents an invertibility criterion but no method for computing the inverse and [10] for a particular class of nonlinear systems. The general class of nonlinear systems is often too wide to enable us to deal with the associated problem and we should preferably try to restrict to a smaller class of systems. Obtaining perfect invertibility conditions on a class of nonlinear mixtures will help considering such models in a blind context [29], [20]. This motivates our interest for polynomial systems, which to a certain extent can be considered as one of the simplest form of nonlinearity. In the first part of this paper we show that methods exist which allow to compute a polynomial inverse (if it exists) of a polynomial MIMO mixing system. We illustrate their validity and effectiveness through examples.

The blind source separation problem serves as an example of the utility of the previous considerations. This issue still faces unanswered questions, in particular in the nonlinear case, although this case has already been addressed [45], [2]. Generally, specific structures have been assumed on the nonlinear mixture: indeed, a general nonlinear mixture of independent sources cannot be identified without additionnal constraint on the mixture. For example, a conformal mapping is assumed in [31]. First published in [35], more general results concerning identifiability of a large class of nonlinearities satisfying an addition theorem have been pointed out recently in [21], [34]. Other structures have been introduced; the post-nonlinear one is probably one of the most popular [45], [32],

[36], [22], [5], [4], [6]. On the other hand, the case of sources in a discrete or finite alphabet has been considered for long [37], [47], [23], [25] and the strength of the discrete sources assumption has been recognized. It indeed allows to relax some usual assumptions, such as the statistical independence of the sources [38], or to deal with underdetermined mixtures —that is mixtures with more sources than sensors— [40], [13], [17], [19]. However the nonlinear source separation problem seems still open for discrete sources, although a geometrical approach may appear as well suited [1]. In this paper, we show how results from commutative algebra give more insight in the case of nonlinear mixtures. We then propose a solution to blind separation in the simple case of binary sources.

The new and original points in the paper are the following:

- We use tools borrowed from commutative algebra. These powerful tools seem still ignored in the signal processing community although they have been successfully applied in many contexts (e.g. statistics [44], channel identification [25]). We translate and apply the corresponding results in a MIMO source separation context.
- We propose an equivalent linear model for any nonlinear MIMO mixture of finite-alphabet sources.
- We apply the previous methods to the case of blind separation of binary sources: in our particular case, a separation is surprisingly obtained although the sources of the equivalent linear model are not independent.

Section II describes the issue which is addressed in the paper. Necessary mathematical tools and definitions are introduced in Section III. Section IV explains how to compute a polynomial inverse. If it does not exist, an alternative solution is shortly discussed. Section V is concerned with the case of finite alphabet sources. It is shown how an equivalent linear model can be used by introducing virtual sources. The invertibility issue is also addressed. Section VI is concerned with the nonlinear blind source separation problem of two binary sources. It is shown that in specific situations, ICA techniques can be successful although the virtual sources introduced by the equivalent linear model are dependent. Finally, Section VII concludes the paper. All examples which have been computed can be reproduced using Appendix III.

Throughout the paper, $\mathbb{K}$ denotes a field (the complex numbers $\mathbb{C}$ or the real numbers $\mathbb{R}$ or possibly any subfield of $\mathbb{C}$). $\mathbb{K}[\mathbf{s}]$ is the set of polynomials with coefficients in $\mathbb{K}$ and variables $\mathbf{s} = (s_1, \ldots, s_N)$. $\mathrm{E}\{.\}$ is the mathematical expectation of any random variable and $\mathrm{Cum}\{.\}$ stands for the cumulant of a set of random variables.

II. Problem statement

A. Source separation

We consider a set of Q sensors acquiring Q observation signals which compose the vector valued signal $(\mathbf{x}(n))_{n\in\mathbb{Z}} = ((x_1(n))_{n\in\mathbb{Z}}, \ldots, (x_Q(n))_{n\in\mathbb{Z}})^{\mathrm{T}}$. In a source separation context, one assumes that these observations come from another set of signals, called the sources and denoted by the vector $(\mathbf{s}(n))_{n\in\mathbb{Z}} \triangleq ((s_1(n))_{n\in\mathbb{Z}}, \ldots, (s_N(n))_{n\in\mathbb{Z}})^{\mathrm{T}}$. Both the observations and the sources may be real or complex-valued signals. We assume a deterministic relation between the sources and the observations. More precisely, the paper focuses on instantaneous nonlinear transforms of the sources. Dropping the time index n, we thus write $\mathbf{x} = \mathbf{f}(\mathbf{s})$ where $\mathbf{f}$ is a nonlinear function, $\mathbf{f} : \mathbb{K}^N \to \mathbb{K}^Q$. Componentwise, the corresponding mixing equations read:

$$\left\{ \begin{array}{ccc} x_1 & = & f_1(s_1, \ldots, s_N) \\ \vdots & & \vdots \\ x_Q & = & f_Q(s_1, \ldots, s_N) \end{array} \right. \quad (1)$$

where $f_1, \ldots, f_Q$ constitute the components of $\mathbf{f}$.

The source separation problem consists in recovering the sources $s_1, \ldots, s_N$ from the observations $x_1, \ldots, x_Q$. This is equivalent to finding the inverse MIMO system $\mathbf{g} : \mathbb{K}^Q \to \mathbb{K}^N$. In other words, we look for the components $g_i : \mathbb{K}^Q \to \mathbb{K}$ of $\mathbf{g} = \mathbf{f}^{-1}$ such that for all i:

$$s_i = g_i(x_1, \ldots, x_Q). \quad (2)$$

The first contribution of this paper addresses the problem of computing an inverse for a known and given mixing system such as (1).

In the case where no information is available on the mixing system (1), the separation problem is referred to as the *blind* source separation problem. This issue, which consists in estimating the sources from the observations only, is addressed in the case of binary sources.

B. Nonlinear functions and polynomials

This paper focuses on the particular case where the functions $f_i, i \in \{1, \ldots, Q\}$ in (1) are polynomials, that is for all i, $f_i \in \mathbb{K}[\mathbf{s}]$. This restriction is partly justified by the difficulty to tackle the nonlinear case because of its generality. In addition, polynomials constitute an important class of nonlinear models which may represent acceptable approximations of certain nonlinearities. Finally, an important reason to deal with this model is the following one.

Consider the case where the multidimensional source vector belongs to a finite set: $\mathbf{s} \in \mathcal{A} = \{\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n_a)}\}$. Although seemingly restrictive, this situation is highly interesting since it occurs in digital communications, where the emitted source sequences belong to a finite alphabet depending on the modulation used.

An important observation is that *if $\mathbf{s} \in \mathcal{A}$ and $\mathcal{A}$ is finite, all instantaneous mixtures of the sources can be expressed as polynomial mixtures*. This follows immediately from the fact that any function on a finite set can be interpolated by a polynomial in a way similar to Lagrange polynomial interpolation [16]. It follows that polynomial mixtures constitute the general model of nonlinear mixtures in the case of sources belonging to a finite alphabet. On the other hand, one should notice that the well-known post-nonlinear model is not easier to deal with in the case of finite alphabet sources [36]: generically, a scalar variable which is a linear combination of discrete sources has a number of distinct values equal to the number of possible states of the source vector. Each of these distinct values can be freely mapped to any value: hence one can see that in the generic case, and for finite alphabet sources, any nonlinear mapping can be represented by a post-nonlinear mapping, which makes both problems equivalent.

III. Mathematical preliminaries

A. Definitions

Assuming that the model (1) is polynomial, and in order be able to resort to algebraic techniques, we will restrict the separator to the class of polynomial functions in $x_1, \ldots, x_Q$, that is: $\forall i, g_i \in \mathbb{K}[\mathbf{x}]$. Then, algebra and Groebner basis techniques are powerful methods for the study of multivariate polynomials. They have been applied only recently in signal processing [41], [49], [46]. It is out of the scope of this paper to explain the associated notions (see [15] for a detailed introduction to the subject) but we recall some basic definitions required here for comprehension. We will introduce the definitions in $\mathbb{K}[\mathbf{s}]$. In the following, boldface letters denote N-tuples and for any $\boldsymbol{\alpha} \in \mathbb{N}^N$ we write: $\mathbf{s}^{\boldsymbol{\alpha}} \triangleq s_1^{\alpha_1} \ldots s_N^{\alpha_N}$.

Definition 1: Let $h_1, \ldots, h_p \in \mathbb{K}[\mathbf{s}]$ be polynomials. The ideal generated by these polynomials in $\mathbb{K}[\mathbf{s}]$ is the subset of $\mathbb{K}[\mathbf{s}]$ which consists of all linear combinations $a_1 h_1 + \ldots + a_p h_p$ where $a_1, \ldots, a_p$ are polynomials in $\mathbb{K}[\mathbf{s}]$. It is denoted by $\langle h_1, \ldots, h_p \rangle$.

Definition 2: A monomial ordering $\prec$ on $\mathbb{K}[\mathbf{s}]$ is a total ordering relation on the set of monomials such that:

- if $\mathbf{s}^{\boldsymbol{\alpha}} \prec \mathbf{s}^{\boldsymbol{\beta}}$ then $\mathbf{s}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \prec \mathbf{s}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$
- $\prec$ is a well-ordering, that is, every nonempty collection of different monomials has a smallest element under $\prec$.

A simple example of monomial ordering is the lexicographic order, where by definition $\mathbf{s}^{\boldsymbol{\alpha}} \prec \mathbf{s}^{\boldsymbol{\beta}}$ if and only if in the vector difference $\boldsymbol{\beta} - \boldsymbol{\alpha}$, the left-most nonzero entry is positive. Here is a set of monomials illustrating this order in $\mathbb{K}[s_1, s_2]$:

$$1 \prec s_2 \prec s_2^2 \prec \ldots \prec s_1 \prec s_1 s_2 \prec s_1 s_2^2 \prec \ldots \prec s_1^2 \prec s_1^2 s_2 \prec \ldots$$

Given a monomial ordering, for a polynomial which reads $h = \sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$, its leading term is defined by $\mathrm{LT}(h) = c_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ where $c_{\boldsymbol{\alpha}}$ is referred to as the leading coefficient and $\mathbf{x}^{\boldsymbol{\alpha}}$, called the leading monomial, is the largest monomial appearing in h in the ordering $\prec$. Then, we can also define a division algorithm, which generalizes the division algorithm in the case of one variable:

Theorem 1 (division algorithm): Let $(h_1, \ldots, h_p)$ be an ordered p-tuple of polynomials. Every polynomial h can be written as:

$$h = a_1 h_1 + \ldots + a_p h_p + r \tag{3}$$

where a_i, h_i are polynomials and r is a linear combination with coefficients in $\mathbb{K}$ of monomials, none of which is divisible by any leading term of $h_1, \ldots, h_p$. (possibly, $r = 0$).

If we consider the ideal $\mathbf{I} = \langle h_1, \ldots, h_p \rangle$, the division algorithm provides a way to write any polynomial as the sum $h = h_{\mathbf{I}} + r$ where $h_{\mathbf{I}}$ lies in $\mathbf{I}$ and no term of r is divisible by any of the leading terms of $h_1, \ldots, h_p$. Unfortunately, the remainder r in this decomposition is not unique in general. A remarkable exception is when the set of generators satisfy the following definition.

Definition 3: The set $\{h_1, \ldots, h_p\}$ is a *Groebner basis* of the ideal $\mathbf{I} = \langle h_1, \ldots, h_p \rangle$ if and only if the remainder r in (3) is uniquely determined for all $h \in \mathbb{K}[\mathbf{s}]$.

Importantly, there exist an algorithm, initially developped by Buchberger for converting a given generating set to a Groebner basis [8]. For a given ideal $\mathbf{I}$, there may exist several Groebner bases, which justifies that the notion of *reduced* Groebner basis is introduced.

Definition 4: A *reduced Groebner basis* for a polynomial ideal $\mathbf{I}$ is a Groebner basis G for $\mathbf{I}$ such that for all h in G:

- the leading coefficient of h is 1.
- no monomial of h lies in the ideal $\langle \mathrm{LT}(G - \{h\}) \rangle$ generated by the leading terms of the set $G - \{h\}$.

For a given monomial ordering, any ideal different from $\{0\}$ has a unique reduced Groebner basis.

B. Example

We illustrate the previous definitions: consider $h_1 = s_1 s_2 - s_1 + 1$, $h_2 = s_2^2 - 1$ and $h = s_1 s_2 - s_1 + s_2 + 2$ in $\mathbb{K}[s_1, s_2]$ with lexicographic order. We define the ideal $\mathbf{I} = \langle h_1, h_2 \rangle$. A possible remainder after division of h by (h_1, h_2) is $s_2 + 1$ since indeed $h = 1.h_1 + 0.h_2 + (s_2 + 1)$ and neither s_2 nor 1 can be divided by $\mathrm{LT}(h_1)$ or $\mathrm{LT}(h_2)$.

However, non uniqueness of the remainder can be observed writing $h = (s_2 + 2).h_1 - s_1.h_2$. This is no surprise because the set $\{h_1, h_2\}$ is not a Groebner basis for $\mathbf{I}$, which is related to the fact that $s_2 + 1 = (s_2 + 1).h_1 - s_1.h_2$ is a polynomial with leading term lower than the leading terms of h_1 and h_2 (note indeed that a cancelling of the leading terms occured). Going further, one can write $-2s_1 + 1 = h_1 - s_1.(s_2 + 1) = (-s_1 s_2 - s_1 + 1).h_1 + s_1^2.h_2$. Hence $-2s_1 + 1$ and $s_2 + 1$ belong to $\mathbf{I}$ and one can prove $\{-2s_1 + 1, s_2 + 1\}$ is a Groebner basis of $\mathbf{I}$. So is any set of polynomials in $\mathbf{I}$ set containing these two polynomials. The reduced Groebner basis of $\mathbf{I}$ is the set $\{s_1 - 1/2, s_2 + 1\}$.

IV. Invertibility

Based on the previous notions, we show that existing results can be used to find a polynomial inverse to a given polynomial MIMO system. Another question of great importance would be to find a generic condition or a minimum number of equations to ensure invertibility or separability as defined in Section IV-B. This question will not be treated here and still remains open. Finally, the reader should notice that the results presented in this section require the exact knowledge or a prior identification of the mixing system.

A. Perfect invertibility

The problem of finding a polynomial g_i such that (2) is satisfied is a particular case of the subalgebra or subring membership problem [15], [26]: to see this, we shall now put our problem differently and precise some notations.

In the present context of non blind inversion, the polynomials $f_i \in \mathbb{K}[\mathbf{s}], i \in \{1, \ldots, Q\}$ are given, and the inversion condition (2) should be written correctly

$$s_i = g_i(f_1(\mathbf{s}), \ldots, f_Q(\mathbf{s})). \tag{4}$$

For ease of notation, we will no longer write explicitly the dependence of $f_1, \ldots, f_Q$ in $\mathbf{s}$. Restricting ourself to polynomial inverses, $g_i(f_1, \ldots, f_Q)$ is a polynomial expression in

$f_1, \ldots, f_Q$ with coefficients in $\mathbb{K}$. Let $\mathbb{K}[\mathbf{f}]$ be the subset of $\mathbb{K}[\mathbf{s}]$ consisting of all such expressions. Introduce the variables $x_1, \ldots, x_Q$ (of course, they will represent the observations) and consider the set $\mathbb{K}[\mathbf{x}]$ of polynomials in these variables. Any element of $\mathbb{K}[\mathbf{f}]$ can be obtained by sustituting $f_1, \ldots, f_Q$ for $x_1, \ldots, x_Q$ in a polynomial of $\mathbb{K}[\mathbf{x}]$. Then, the initial problem amounts to saying whether $s_i \in \mathbb{K}[\mathbf{f}]$ or equivalently whether a polynomial $g_i \in \mathbb{K}[\mathbf{x}]$ exists or not such that (4) is satisfied. The answer is provided by the following theorem [15, p.334] which requires to work in the set $\mathbb{K}[\mathbf{s}, \mathbf{x}]$ of polynomials in the variables $s_1, \ldots, s_N, x_1, \ldots, x_Q$:

Theorem 2: Fix a monomial ordering in $\mathbb{K}[\mathbf{s}, \mathbf{x}]$ where any monomial involving one of $s_1, \ldots, s_N$ is greater than all monomials in $\mathbb{K}[\mathbf{x}]$. Let G be a Groebner basis of the ideal $\langle f_1 - x_1, \ldots, f_Q - x_Q \rangle \subset \mathbb{K}[\mathbf{x}, \mathbf{s}]$. Given $h \in \mathbb{K}[\mathbf{s}]$, let g be the remainder of h on division by G. Then:

1) $h \in \mathbb{K}[\mathbf{f}]$ if and only if $g \in \mathbb{K}[\mathbf{x}]$.
2) if $h \in \mathbb{K}[\mathbf{f}]$, then $h = g(f_1, \ldots, f_Q)$ is an expression of h as a polynomial in $f_1, \ldots, f_Q$.

Monomial orderings satisfying the condition in the above theorem are called elimination orderings for $s_1, \ldots, s_N$. One should note that this condition is satisfied by the lexicographic order in $\mathbb{K}[\mathbf{s}, \mathbf{x}]$ but other monomial orderings also satisfy this condition [15]. The invertibility result will not depend on the chosen ordering, but different inverses may be found. The method for perfect inversion with a polynomial separator then follows from the above proposition which can be applied successively to the polynomials $s_1, \ldots, s_N$ in $\mathbb{K}[\mathbf{s}]$. It reads:

1) Choose in $\mathbb{K}[\mathbf{s}, \mathbf{x}]$ an elimination ordering for $s_1, \ldots, s_N$ and define $\mathbf{I} = \langle f_1 - x_1, \ldots, f_Q - x_Q \rangle$.
2) Compute a Groebner basis G of $\mathbf{I}$.
3) For $i = 1 \ldots N$, compute the division of s_i by G. If the remainder g_i of the division is in $\mathbb{K}[\mathbf{x}]$, we have $s_i = g_i(f_1, \ldots, f_Q)$ (that is, g_i satisfies (2)), otherwise, s_i cannot be recovered exactly by a polynomial in $f_1, \ldots, f_Q$.

1) Example: Throughout the paper, we will consider the example provided by the following equations:

$$\begin{cases} x_1 = f_1(s_1, s_2) = 3s_1^2 + 2s_1s_2 + 4s_2^2 + 7s_1 + 4s_2 \\ x_2 = f_2(s_1, s_2) = -3s_1^2 + 5s_1s_2 + 2s_1 + s_2 \\ x_3 = f_3(s_1, s_2) = -3s_1 + 6s_2 \\ x_4 = f_4(s_1, s_2) = 6s_1^2 - s_1s_2 + 4s_2^2 + 3s_1 - 9s_2 \end{cases} \quad (5)$$

Groebner basis computation and polynomial division are implemented in many computer algebra systems. Using the lexicographic order in $\mathbb{K}[s_1, s_2, x_1, x_2, x_3, x_4]$, the following inverse of (5) has been computed (see Appendix III):

$$\begin{cases} s_1 = \frac{17}{144}x_1 - \frac{1}{12}x_2 - \frac{1}{432}x_3^2 - \frac{91}{432}x_3 - \frac{7}{72}x_4 \\ s_2 = \frac{17}{288}x_1 - \frac{1}{24}x_2 - \frac{1}{864}x_3^2 + \frac{53}{864}x_3 - \frac{7}{144}x_4 \end{cases}$$

Remark 1: The method which has been described of course also applies when the polynomials $f_1, \ldots, f_Q$ each have total degree one. In this case, the mixture is actually a linear instantaneous one and consists in a simple matrix product. The above computation is then similar to a Gaussian elimination procedure [15, p.91].

B. Separability

The previous section gives a condition to be able to recover exactly one source with a polynomial expression of the observations. If not possible, it may sometimes be enough to recover a function (here, a polynomial function) of each source instead of recovering the source itself (e.g. in blind separation). A simple example of this particular case is given by the mixing system $x_1 = s_1^2 + s_2^2, x_2 = s_1^2 - s_2^2$ where one can easily recover s_1^2 and s_2^2 and may not be interested in s_1 and s_2. It would hence be interesting to be able to describe $\mathbb{K}[\mathbf{f}]$ which is the set of polynomials in $s_1, \ldots, s_N$ which can be obtained as polynomial expressions in the observations $x_1, \ldots, x_Q$. One would in this case be more particularly interested in knowing something about $\mathbb{K}[s_i] \cap \mathbb{K}[\mathbf{f}]$ which are the polynomials in s_i only which can be computed using the observations only. Unfortunately, $\mathbb{K}[\mathbf{f}]$ does not have the structure of an ideal in $\mathbb{K}[\mathbf{s}]$ and hence cannot be described by a set of generators. In the case where the system is not invertible by the previous method, we hence propose the following solution to this difficulty:

1) For $i \in \{1, \ldots, N\}$, test for algebraic dependence between $f_1, \ldots, f_Q$ and s_i, that is test whether there exist a polynomial δ such that $\delta(s_i, f_1, \ldots, f_Q) = 0$. This problem admits an algebraic solution [26, p.84].
2) For $i \in \{1, \ldots, N\}$, if $f_1, \ldots, f_Q$ and s_i are algebraically dependent, then try to determine whether simple polynomials in the variable s_i only belong to $\mathbb{K}[\mathbf{f}]$.

The above procedure should be interesting mainly to discard situations where no solution should be expected from polynomial methods, that is situations where there exists no algebraic dependence between the polynomials $f_1, \ldots, f_Q$ and s_i. In addition, even if these polynomials are algebraically dependent, one has no information whether there exist or not polynomials in $\mathbb{K}[s_i] \cap \mathbb{K}[\mathbf{f}]$. Finally, the minimum degree of the polynomials in $\mathbb{K}[s_i] \cap \mathbb{K}[\mathbf{f}]$, if any, is not known. For large values of this degree and for computational load reasons, one may not be able to get an answer to the second step of the procedure.

1) Example: We consider the system in Equation (5) where only x_1, x_2 and x_3 are observed. (That is, the mixing system has 2 sources, 3 sensors and the last equation in (5) is ignored). In this case, one can check with the previous method that the system is no longer invertible. However, one can also check that there exist algebraic relations between the polynomials f_1, f_2, f_3 in Equation (5) and s_i for $i = 1, 2$. Going further, one can compute (see Appendix III):

$$\begin{cases} s_1^2 + b_1 s_1 = (2b_1 - \frac{15}{7})s_2 + \frac{5}{28}x_1 - \frac{3}{14}x_2 - \frac{5}{252}x_3^2 \\ \qquad\qquad + (-\frac{b_1}{3} + \frac{23}{84})x_3 \\ s_2^2 + b_2 s_2 = (b_2 - \frac{7}{4})s_2 + \frac{1}{16}x_1 + \frac{1}{8}x_2 + \frac{1}{48}x_3^2 + \frac{11}{48}x_3 \end{cases}$$

Choosing $b_1 = 15/14$ (resp. $b_2 = 7/4$), one thus obtains the separation of the sources, that is a polynomial in s_1 (resp. s_2) only, which is expressed depending on x_1, x_2 and x_3 only.

V. Finite-alphabet sources

Section IV-A describes a method for computing a perfect inverse of a polynomial MIMO mixture. If the latter does not

exist, Section IV-B shows how, giving up the exact restitution of the sources, one can possibly separate them only. Even this is however not always possible and consequently, il should be interesting to use general nonlinearities. According to Section II-B, the general case of nonlinear functions can be treated with polynomials if the sources belong to a finite alphabet: this point is detailed in the present section. We first study the vector space of nonlinear mixtures on a finite set to derive an equivalent linear model. Then, we generalize the previous results on invertibility.

A. Nonlinear mixtures of finite-alphabet sources

1) Vector space of polynomial functions on a zero-dimensional variety: We assume now that the sources belong to a finite alphabet. Hence the multidimensional source vector belongs to a finite set $\mathbf{s} \in \mathcal{A} = \{\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(n_a)}\}$ where n_a is the number of elements in $\mathcal{A}$. For all i, let $(a_1^{(i)}, \ldots, a_N^{(i)})$ be the coordinates of $\mathbf{a}^{(i)}$ and let us introduce the ideals in $\mathbb{K}[\mathbf{s}]$:

$$\forall i \in \{1, \ldots, n_a\} \qquad \mathbf{I}_{\{\mathbf{a}^{(i)}\}} \triangleq \langle s_1 - a_1^{(i)}, \ldots, s_N - a_N^{(i)} \rangle \tag{6}$$

$$\mathbf{I}_{\mathcal{A}} \triangleq \bigcap_{i=1}^{n_a} \mathbf{I}_{\{\mathbf{a}^{(i)}\}} \tag{7}$$

It is a well-known fact that the set of all polynomials vanishing on any given subset of $\mathbb{K}^N$ is an ideal. Actually, one can see that $\mathbf{I}_{\{\mathbf{a}^{(i)}\}}$ is the ideal of polynomials vanishing at point $\mathbf{a}^{(i)}$ and that the intersection ideal $\mathbf{I}_{\mathcal{A}}$ is also the ideal of all polynomials vanishing on $\mathcal{A}$. Going further, two polynomials f and $\tilde{f}$ define the same function on $\mathcal{A}$ if and only if $f - \tilde{f} \in \mathbf{I}_{\mathcal{A}}$. In this situation, it is common to identify all polynomials $\tilde{f}$ such that $f - \tilde{f} \in \mathbf{I}_{\mathcal{A}}$ and consider only one representative f of this set (see [15] for details): by definition, the set of all representatives corresponds to the quotient space $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$. Nonlinear functions of the discrete sources in $\mathcal{A}$ are thus in one-to-one correspondence with the elements of $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$. In addition, we have the following property, which is the key to find an equivalent linear model to a nonlinear mixture.

Property 1: Let $\langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}}) \rangle$ be the ideal generated by all leading terms in $\mathbf{I}_{\mathcal{A}}$ and let $\mathrm{M}(\mathbf{I}_{\mathcal{A}}) \triangleq \{\mathbf{s}^{\boldsymbol{\alpha}}, \mathbf{s}^{\boldsymbol{\alpha}} \notin \langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}}) \rangle\}$. The quotient space $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$ is a finite dimensional vector space of dimension n_a which is isomorphic to: $S \triangleq \mathrm{span}(\mathrm{M}(\mathbf{I}_{\mathcal{A}}))$. Each element of $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$ has a unique representative as a $\mathbb{K}$-linear combination of monomials in $\mathrm{M}(\mathbf{I}_{\mathcal{A}})$.

Proof: Based on the specificity of $\mathbf{I}_{\mathcal{A}}$, this property is classically known when $\mathbb{K} = \mathbb{C}$ [16, p.43]. The proof in [16] can be adapted when $\mathbb{K} \subsetneq \mathbb{C}$: $\mathbf{I}_{\mathcal{A}}$ indeed consists of all polynomials vanishing on $\mathcal{A}$ and $\mathcal{A}$ itself is the variety defined such that any polynomials in $\mathbf{I}_{\mathcal{A}}$ vanishes on $\mathcal{A}$. ■

Importantly, a fundamental property of a Groebner basis $G = \{h_1, \ldots, h_p\}$ of $\mathbf{I}_{\mathcal{A}}$ is that[1] $\langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}}) \rangle = \langle \mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_p) \rangle$. Hence the set $\mathrm{M}(\mathbf{I}_{\mathcal{A}})$ can be deduced from the computation of a Groebner basis of $\mathbf{I}_{\mathcal{A}}$: $\mathrm{M}(\mathbf{I}_{\mathcal{A}})$ consists indeed of all monomials which cannot be divided by any of $\mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_p)$. According to Property 1, this gives a basis of $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$ and thus also a finite basis composed of monomials for the vector space of nonlinear functions on $\mathcal{A}$. This is the basic idea which allows us in the next section to transform a nonlinear mixture into a linear model. Before that, we explain how a Groebner basis for $\mathbf{I}_{\mathcal{A}}$ can be easily obtained in the particular case where $\mathcal{A}$ is a cartesian product. This case is important, since $\mathcal{A}$ necessarily has this form for statistically independent sources, which will be considered later.

Property 2: Assume $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_N$ where for $i = 1, \ldots, N$, $\mathcal{A}_i \triangleq \{\tilde{a}_i^{(1)}, \ldots, \tilde{a}_i^{(l_i)}\}$ is the set of all possible values of the i-th component. Let:

$$\forall i \in \{1, \ldots, N\}, \qquad q_i(s_i) \triangleq \prod_{k=1}^{l_i} (s_i - \tilde{a}_i^{(k)})$$

Then, $\mathbf{I}_{\mathcal{A}} = \langle q_1, \ldots, q_N \rangle$ and $\{q_1, \ldots, q_N\}$ is the reduced Groebner basis of $\mathbf{I}_{\mathcal{A}}$ for any monomial ordering $\prec$.

Proof: This property can be found in [44]. We prove it in Appendix I for completeness. ■

2) From a polynomial mixture to a linear equivalent model: As explained in Section II-B, any nonlinear mixture of finite alphabet sources reduces to a polynomial mixture and a consequence of Property 1 is that we know explicitly the finite dimensional vector space of nonlinear transforms. We can then introduce new variables and define the column vector $\tilde{\mathbf{s}}$ which contains the monomials in $\mathrm{M}(\mathbf{I}_{\mathcal{A}})$. Using Property 1, we obtain that there exists a matrix $\tilde{\mathbf{A}}$ such that:

$$\forall \mathbf{s} \in \mathcal{A} \qquad \mathbf{x} = \mathbf{f}(\mathbf{s}) = \tilde{\mathbf{A}}\tilde{\mathbf{s}} \tag{8}$$

In so doing, we have transformed any nonlinear instantaneous mixture into a linear mixture of the extended source vector $\tilde{\mathbf{s}}$. The number of entries in $\tilde{\mathbf{s}}$ is n_a: it is precisely the dimension of the vector space $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$ representing all nonlinear functions from $\mathcal{A}$ to $\mathbb{K}$ and this corresponds to the number of points in $\mathcal{A}$ as one intuitively expects. The minimum number of monomials required to represent all nonlinear mappings from $\mathcal{A}$ to $\mathbb{K}$ are hence listed in $\mathrm{M}(\mathbf{I}_{\mathcal{A}})$ (or in $\tilde{\mathbf{s}}$). Finally, note that except in specific cases, $\tilde{\mathbf{s}}$ includes the monomials $s_1, \ldots, s_N$, which is the reason why $\tilde{\mathbf{s}}$ appears as a vector containing "virtual" sources in addition to the true ones.

Let us see some consequences in the context of blind source separation: one may wish to reduce nonlinear blind separation of discrete sources to a problem of blind separation of an instantaneous linear mixture. However, this differs from the well-known case of blind separation of independent sources (a.k.a. independent component analysis or ICA), because of two major difficulties which appear:

- contrary to an ICA context, the sources are no longer mutually independent, but are linked by algebraic equations. Indeed, the virtual sources $\tilde{\mathbf{s}}$ are monomials depending on $s_1, \ldots, s_N$.
- the model will in most situations become largely underdetermined since very often, the number of sensors is limited, which generally implies $N < n_a$.

It follows that nonlinear mixtures, dependent sources and underdetermination are related challenging issues in blind separation of finite-alphabet sources.

[1] This property is often considered as the definition of a Groebner basis.

3) Example: case of binary sources: We illustrate the previous discussion in the case of N binary sources. Using Property 2, one immediately obtains that $\langle s_1^2-1,\dots,s_N^2-1\rangle$ is a Groebner basis for $\mathbf{I}_{\mathcal{A}}$ when $\mathcal{A}=\{-1;+1\}^N$. It follows that $\langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}})\rangle = \langle s_1^2,\dots,s_N^2\rangle$ and the monomials not in $\langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}})\rangle$ are $\mathrm{M}(\mathbf{I}_{\mathcal{A}}) = \{s_1^{\alpha_1}\dots s_N^{\alpha_N}; \forall i, 0\le\alpha_i\le 1\}$: if indeed a monomial contains $s_i^{\alpha_i}$ in factor with $\alpha_i\ge 2$, then s_i^2 divides the monomial, which proves that it belongs to $\langle \mathrm{LT}(\mathbf{I}_{\mathcal{A}})\rangle$. According to Property 1, we deduce that there is an isomorphism between the following spaces:

$$\mathbb{C}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}} \cong \mathrm{span}(s_1^{\alpha_1}\dots s_N^{\alpha_N}; \forall i, 0\le\alpha_i\le 1)$$

and consequently, any polynomial (or nonlinear) function of the sources can be written as a $\mathbb{C}$-linear combination of the above monomials. The original nonlinear model hence transforms into the model given by Equation (8) where $n_a = 2^N$ and $\tilde{\mathbf{s}}$ contains all monomials $s_1^{\alpha_1}\dots s_N^{\alpha_N}; \forall i, 0\le\alpha_i\le 1$ (this includes in $\tilde{\mathbf{s}}$ a constant term 1 and the monomials $s_1,\dots,s_N$). Actually, in the case of binary sources, this result can be seen more pragmatically by the fact that $\forall i, s_i^2 = 1$ and hence any monomial can be obviously simplified and reduces to one among the given ones.

In particular, for two binary sources, any scalar observation of a polynomial (and also nonlinear) mixture of the sources can be written as:

$$x = as_1s_2 + bs_1 + cs_2 + d, \tag{9}$$

where a, b, c and d are scalar constants.

4) Example: case of PAM4 sources: In the case of N PAM4 telecommunication sources, which are sources which take four different possible values, we have that the polynomials q_i defined in Property 2 have degree four. Using Property 2, it follows that the set of monomials to be considered in $\tilde{\mathbf{s}}$ is given by $\mathrm{M}(\mathbf{I}_{\mathcal{A}}) = \{s_1^{\alpha_1}\dots s_N^{\alpha_N}; \forall i, 0\le\alpha_i\le 3\}$.

B. Computing an inverse on a zero-dimensional variety

Section IV-A describes a method for computing a perfect inverse of a polynomial MIMO mixture with no restriction on the sources. If we assume that the sources are in a finite alphabet, it is sufficient that the polynomials $g_i, i\in\{1,\dots,N\}$ of the inverse system satisfy:

$$\forall \mathbf{s}\in\mathcal{A} \qquad s_i = g_i(f_1(\mathbf{s}),\dots,f_Q(\mathbf{s})) \tag{10}$$

and they need not verify the above equation for all $\mathbf{s}$ in $\mathbb{K}^N$. In other terms, the inverse g_i should be such that $s_i - g_i(f_1,\dots,f_Q)$ vanishes identically on $\mathcal{A}$, that is:

$$s_i - g_i(f_1,\dots,f_Q)\in\mathbf{I}_{\mathcal{A}}.$$

We can prove a generalization of Theorem 2 that is conceptually equivalent to considering the quotient space $\mathbb{K}[\mathbf{s}]/\mathbf{I}_{\mathcal{A}}$. We need the following definition:

Definition 5: The sum of two ideals $\mathbf{I}=\langle h_1,\dots,h_p\rangle$ and $\mathbf{J}=\langle h_{p+1},\dots,h_n\rangle$ is the ideal $\mathbf{I}+\mathbf{J} \triangleq \{u+v; u\in\mathbf{I}, v\in\mathbf{J}\}$. It is generated by the union of generating sets of $\mathbf{I}$ and $\mathbf{J}$, that is: $\mathbf{I}+\mathbf{J} = \langle h_1,\dots,h_p,h_{p+1},\dots,h_n\rangle$.

The following proposition then holds:

Proposition 1: Fix a monomial ordering in $\mathbb{K}[\mathbf{s},\mathbf{x}]$ where any monomial involving one of $s_1,\dots,s_N$ is greater than all monomials in $\mathbb{K}[\mathbf{x}]$. Let G be a Groebner basis of the ideal $\mathbf{I}_{\mathcal{A}} + \langle f_1-x_1,\dots,f_Q-x_Q\rangle \subset \mathbb{K}[\mathbf{x},\mathbf{s}]$. Given $h\in\mathbb{K}[\mathbf{s}]$, let g be the remainder of h on division by G. Then:

1) $g\in\mathbb{K}[\mathbf{x}]$ if and only if there exists $r\in\mathbf{I}_{\mathcal{A}}$ such that $h-r\in\mathbb{K}[\mathbf{f}]$.
2) if the above condition holds, then $g(f_1,\dots,f_Q)$ is an expression such that $h-g(f_1,\dots,f_Q)\in\mathbf{I}_{\mathcal{A}}$.

Proof: The proof is an adaptation of the proof of Theorem 2: it is sketched in Appendix II. ■

Similarly to Section IV-A, the method for computing an inverse follows from the above proposition.

1) Choose in $\mathbb{K}[\mathbf{s},\mathbf{x}]$ an elimination ordering for $s_1,\dots,s_N$ and find for $\mathbf{I}_{\mathcal{A}}$ a generating set $\langle q_1,\dots,q_P\rangle$ (e.g. use Property 2 if possible or use (7) otherwise). Define $\mathbf{I} = \langle f_1-x_1,\dots,f_Q-x_Q,q_1,\dots,q_P\rangle$.
2) Compute a Groebner basis G of $\mathbf{I}$.
3) For $i=1\dots N$, compute the division of s_i by G. If the remainder g_i of the division is in $\mathbb{K}[\mathbf{x}]$, we have $s_i = g(f_1,\dots,f_Q)$ for all $\mathbf{s}$ in $\mathcal{A}$, otherwise, s_i cannot be recovered exactly by a polynomial in $f_1,\dots,f_Q$.

Let us stress that a nonlinear inverse exists if and only if a polynomial inverse exists since polynomial transforms cover the general case of nonlinear transforms for finite alphabet sources. In the case of finite alphabet sources, Proposition 1 thus provides an answer for the general question of the existence of a nonlinear inverse.

1) Example: Assume that for all i the sources s_i belong to $\{\pm\frac{1}{2};\pm\frac{3}{2}\}$. This is typically the case of PAM4 telecommunication sources. Defining x_1, x_2 and x_3 as in (5), the following equalities hold for all (s_1,s_2) in $\{\pm\frac{1}{2};\pm\frac{3}{2}\}^2$ (see Appendix III):

$$\begin{cases} s_1 = -\frac{32864}{52732215}x_2x_3^5 + \frac{17600}{10546443}x_2x_3^4 + \frac{153488}{3515481}x_2x_3^3 \\ \quad - \frac{132800}{1171827}x_2x_3^2 - \frac{900538}{1953045}x_2x_3 + \frac{44740}{43401}x_2 \\ \quad - \frac{417616}{807277479435}x_3^9 + \frac{16}{1055264679}x_3^8 + \frac{2223128}{29899165905}x_3^7 \\ \quad + \frac{127768}{1423769805}x_3^6 - \frac{121412}{31639329}x_3^5 - \frac{177568}{31639329}x_3^4 \\ \quad + \frac{10508731}{130279590}x_3^3 + \frac{474367}{27342630}x_3^2 - \frac{2547283}{5911920}x_3 + \frac{5715}{13616} \\ s_2 = -\frac{16432}{52732215}x_2x_3^5 + \frac{8800}{10546443}x_2x_3^4 + \frac{76744}{3515481}x_2x_3^3 \\ \quad - \frac{66400}{1171827}x_2x_3^2 - \frac{450269}{1953045}x_2x_3 + \frac{22370}{43401}x_2 \\ \quad - \frac{208808}{807277479435}x_3^9 + \frac{8}{1055264679}x_3^8 + \frac{1111564}{29899165905}x_3^7 \\ \quad + \frac{63884}{1423769805}x_3^6 - \frac{60706}{31639329}x_3^5 - \frac{88784}{31639329}x_3^4 \\ \quad + \frac{10508731}{260559180}x_3^3 + \frac{474367}{54685260}x_3^2 - \frac{576643}{11823840}x_3 + \frac{5715}{27232} \end{cases}$$

This illustrates that with PAM4 sources, the mixture (5) can be exactly inverted using x_1, x_2 and x_3 only. Actually, using this method, it appears that for the considered discrete sources, no more than two of the observations (in the above example, x_2 and x_3) in Equation (5) are required for exact inversion.

VI. Blind separation of two binary sources

We now consider the particular case of two binary sources (that is $\forall i\in\{1,2\}, s_i\in\{-1;+1\}$) and show how the above results allow to solve the nonlinear blind separation of two such sources. The case of binary sources has already been

considered from different point of views (see among others [40], [17], [19]) and it has long been noticed that discrete sources can be blindly separated even in an underdetermined scenario. The approach described here concerns specifically the nonlinear case but it is complementary to existing ones in the underdetermined case.

A. MIMO blind separation of a nonlinear mixture of two binary sources

1) Model and assumptions: So far, only non-blind inversion of a known mixing system has been considered and thus, contrary to the context of ICA, no statistical assumption has been made, such as mutual independence of the sources. We introduce it now and show that it allows one to separate blindly nonlinear mixtures of two sources. More precisely, we will consider two sources which are referred to as Binary Phase Shift Keying (BPSK) in a digital communication context, that is we assume:

A1. s_1, s_2 are binary ($\forall i, s_i \in \{-1; +1\}$), centered and mutually independent.

According to Section V-A.2 and the example in Equation (9) of Section V-A.3, any nonlinear mixture of the above two BPSK sources can be written as a linear combination of the monomials $1, s_1, s_2, s_1 s_2$. For a mixture on the Q sensors of $\mathbf{x}$, this can be written:

$$\mathbf{x} = \mathbf{A} \begin{pmatrix} s_1 \\ s_2 \\ s_1 s_2 \end{pmatrix} + \mathbf{B} \tag{11}$$

where $\mathbf{A}$ is a $Q \times 3$ matrix and where the $Q \times 1$ column vector $\mathbf{B}$ corresponds to the contribution of the constant monomial 1: this is actually equivalent to writing Eq. (8) where the constant monomial 1 is treated separately and not included in $\tilde{\mathbf{s}}$. Noting now that $\mathrm{E}\{s_1\} = \mathrm{E}\{s_2\} = \mathrm{E}\{s_1 s_2\} = 0$, one can introduce the centered observations

$$\mathbf{x}_{\mathrm{c}} \triangleq \mathbf{x} - \mathbf{B} = \mathbf{x} - \mathrm{E}\{\mathbf{x}\} \tag{12}$$

and the above model simplifies to:

$$\mathbf{x}_{\mathrm{c}} = \mathbf{A} \begin{pmatrix} s_1 \\ s_2 \\ s_1 s_2 \end{pmatrix} \tag{13}$$

In addition, we have the following key property:

Lemma 1: The sources s_1, s_2 and $s_3 = s_1 s_2$ where s_1, s_2 satisfy A1 are mutually dependent. Nevertheless they are centered, uncorrelated, pairwise independent and their fourth-order cross-cumulants vanish, that is:

$$\mathrm{Cum}\{s_i, s_j\} = 0 \text{ except if } i = j, \tag{14}$$

$$\mathrm{Cum}\{s_i, s_j, s_k, s_l\} = 0 \text{ except if } i = j = k = l. \tag{15}$$

Proof: The lemma can be checked easily after expressing the cumulants as functions of the moments and using assumption A1. (14) and (15) then follow, whereas $\mathrm{Cum}\{s_1, s_2, s_3\} = 1 \neq 0$ shows that the sources are mutually dependent. Finally, one easily proves pairwise independence by writing all pairwise probability density functions. ■

Many source separation methods have been developped relying on properties in Equations (14) and (15) only. Among these, we find the algorithms in [11] (referred to as CoM2) or in [9] (referred to as JADE). It follows that these classical ICA algorithms allow to separate the three sources s_1, s_2 and $s_3 = s_1 s_2$ where s_1, s_2 satisfy A1. Consequently, the same algorithms will succeed in separating a nonlinear mixture of two binary sources on three or more sensors ($Q \geq 3$). We sum up and stress this fact in the following proposition:

Proposition 2: Any ICA method which relies only on second and fourth order cumulants, will successfully separate instantaneous and linear mixtures of the sources s_1, s_2, s_3, where s_1, s_2 are given by A1 and $s_3 = s_1 s_2$. The same ICA method, when applied on a nonlinear mixture of the two sources s_1, s_2 on three or more sensors, will lead to the recovery of s_1, s_2, s_3 up to permutation and scaling ambiguity (the scaling ambiguity reduces to a sign ambiguity since the sources are binary).

2) Simulations: For illustration purpose, we considered the following nonlinear mixing system:

$$\begin{cases} x_1 = \cos(s_1 - s_2 + 2) \\ x_2 = \cos(s_1) + 1.32 s_2 + 0.56 s_1 s_2 + \log(1 + 0.215 s_1 s_2) \\ x_3 = \exp(s_1 + s_2) \end{cases} \tag{16}$$

We have simulated realizations of two BPSK sources and we have mixed them according to (16). The data have been centered and the algorithm in [11] has been applied to these centered observations $\mathbf{x}_{\mathrm{c}}$ as defined in (12). The sources s_1, s_2 as well as the fictive source $s_3 = s_1 s_2$ have been successfully separated. Typical results are given in Figure 1 in the noiseless case and in Figure 2 with 20dB additive noise on the sensors. Figure 3 represents the average value of the mean square error (MSE) on the three sources $s_1, s_2, s_3 = s_1 s_2$ for different number of samples and for different values of SNR. The results have been obtained by averaging on 1000 Monte-Carlo runs. They clearly confirm the ability of classical algorithms to separate a nonlinear mixture of two BPSK sources on three or more sensors.

B. Blind separation of a nonlinear mixture of two binary sources on one sensor

It is well known that in the case of discrete sources, underdetermined mixtures can be sucessfully separated [13], [40], [19]. The similarity between the underdetermined case and the nonlinear case invites us to see the possibilities to separate binary sources mixed nonlinearly on one sensor only.

1) Noiseless case: We first consider the ideal case when no noise is present.

a) Separation method: According to the example in Section V-A.3, the general form of a nonlinear mixture of two binary sources is given by (9). Using the method in Section V-B (and working with four parameters a, b, c and d), we easily

obtain that for all $(s_1, s_2) \in \{-1, +1\}^2$ (see Appendix III):

$$s_1 = \frac{1}{2(a^2-b^2)(b^2-c^2)}\Big[bx^3 + (-ac-3bd)x^2 + (-a^2b+2acd-3b^3-bc^2+3bd^2)x + (a^3c+a^2bd-5ab^2c+ac^3-acd^2+3b^3d+bc^2d-bd^3)\Big] \quad (17)$$

This equation shows that s_1 can be recovered when $(a^2 - b^2)(b^2 - c^2) \neq 0$ (which amounts to say that $a^2 \neq b^2$ and $b^2 \neq c^2$). s_2 has a similar expression where b and c should only be exchanged. It follows that the nonlinear mixture of two binary sources given by (9) can be inverted under the condition: $a^2 \neq b^2, a^2 \neq c^2$ and $b^2 \neq c^2$. This condition holds generically for mixtures which have coefficients drawn from a continuous joint probability density function. Relying on previous equation, it is immediate to recover the sources after identification of a, b, c and d. This is easy as soon as one has noticed that x actually takes only 4 distinct values, say ξ_1, ξ_2, ξ_3 and ξ_4. Then, we obtain:

- $d = (\xi_1 + \xi_2 + \xi_3 + \xi_4)/4$
- $|a|, |b|, |c|$ are given by the values of $|\xi_i + \xi_j - 2d|/2$, where $i \neq j, 1 \leq i, j \leq 4$.
- Observing x only, some inherent indeterminacies necessarily remain. First, the permutation ambiguity between s_1, s_2 and the fictive source $s_3 = s_1 s_2$ cannot be removed: since the three sources play an identical role, this yields a permutation ambiguity on a, b and c. In addition, there will remain a sign ambiguity on two of the sources, but not on the third one because of the relation $s_3 = s_1 s_2$. It implies that a mixture equivalent to (9) can be obtained by choosing arbitrarily the sign of two of the coefficients, for instance a and b. The sign of the third coefficient c can then be uniquely determined by estimating the sign of $\mathrm{E}\{x^3\} = 6abc$.

Remark 2: It is interesting to make a connection between Section V-A and the above result which actually constitutes a particular case. Indeed, the condition that $a^2 \neq b^2$, $a^2 \neq c^2$ and $b^2 \neq c^2$ ensures that x takes four distinct values, which each correspond to one value of (s_1, s_2). Consequently, it should be no surprise that the mixture can be inverted in this case.

Now, we can caracterize all nonlinear transforms from the finite set $\{\xi_1, \xi_2, \xi_3, \xi_4\}$ of values of x to $\mathbb{C}$: they indeed constitute a vector space of dimension 4 and they can be expressed as linear combinations of the monomials $1, x, x^2, x^3$. This easy result is a particular case, the generalization of which is given by Property 2 (and Property 1). The original sources s_1 and s_2 are indeed recovered depending on these monomials only in Equation (17).

b) Simulations: We illustrate the previous paragraph with the mixture:

$$x = \log\left(1 + \frac{1}{(0.2 + s_1 + 0.3s_2)^2}\right) \quad (18)$$

One can then easily identify that this nonlinear equation is equivalent to (9) with : $a \approx 0.3608$, $b \approx 0.2600$, $c \approx 0.1427$ and $d \approx 0.8459$. Simulations show that in noise-free conditions, almost perfect separation can be obtained blindly with the method in paragraph VI-B.1.a: this is illustrated by Figure 4. The only difficulty in this noiseless case consists in estimating the sign of $\mathrm{E}\{x^3\}$ in the case where it is close to zero. Since this situation may occur depending on the particular mixing system, some mixtures are more difficult to separate using this method. The case of noisy observations is treated in the next section.

2) Noisy case: The above method is not applicable when there is additive noise on the sensor: different methods which can cope with this situation are now presented and discussed. More precisely, we assume that we observe $\tilde{x} = x + \varepsilon$ where ε is a Gaussian centered random variable with variance σ^2 and x is the noiseless nonlinear mixture of the sources s_1, s_2 (that is, x is given by (18) in the case of previous example or by (9) in the general case). The noise term ε is assumed independent of the sources s_1, s_2.

a) Separation methods: Following the ideas of exact inversion in the noiseless case, a solution one may think of consists in blindly identifying the coefficients of the mixing system (9) and then computing the exact inverse to recover the sources. From the discussion in Section VI-B.1.a, the problem amounts to estimating the values $\xi_1, \ldots, \xi_4$ from the noisy observations. Fortunately, as noticed in [18], $\tilde{x}$ follows a law given by a mixture of Gaussians whose centers are given by $\xi_1, \ldots, \xi_4$. In this situation, there exist well-known techniques to estimate $\xi_1, \ldots, \xi_4$ from the data: the Expectation-Maximization (EM) algorithm seems appropriate for this purpose, although other methods exist (see [28]).

As a byproduct of the EM algorithm [48], it is well known that we easily obtain the maximum a posteriori (MAP) estimates of the values of $x \in \{\xi_1, \ldots, \xi_4\}$. Hence, we are able to classify the samples of $\tilde{x}$ according to the noiseless value of $x \in \{\xi_1, \ldots, \xi_4\}$. Then, from the value of $x \in \{\xi_1, \ldots, \xi_4\}$, it is possible to trace back the value of the source vector (s_1, s_2) up to a sign and permutation ambiguity. We hence considered this separation method for comparison purposes.

Finally, another method for separating the sources from a unique observation sensor consists in introducing additional virtual measurements as proposed in [13], [14] for the case of underdetermined mixtures. With the model (9), one can define the column vector $\mathbf{x} = (x, x^2, x^3)^{\mathrm{T}}$. Then, the linear model (11) (or equivalently (13) with centered observations) holds with the matrix $\mathbf{A}$ given by Equation (19). It is then possible to simply apply an ICA algorithm such as CoM2 [11] or JADE [9]: this allows to separate the sources s_1, s_2 and $s_3 = s_1 s_2$.

b) Simulations: We implemented the EM algorithm in the simplified case where the variance of the noise is known. In practice, the variance should be estimated. However this simplified case gives an indication of the performance which can be expected from this method, which is given here only for comparison purpose. The initial value of the EM algorithm has been initialized as the result of a K-means step. Then, the three methods described above for recovering the sources have been considered and compared:

1) EM + inversion: the sources have been recovered using the exact inverse expression of the estimated system. A

$$\mathbf{A} = \begin{pmatrix} a & b & c \\ 2(ad+bc) & 2(ac+bd) & 2(ab+cd) \\ a^3+3ab^2+3ac^2+3ad^2+6bcd & 3a^2b+6acd+b^3+3bc^2+3bd^2 & 3a^2c+6abd+3b^2c+c^3+3cd^2 \end{pmatrix} \quad (19)$$

hard decision (sign function) has then been applied on the estimated sources to eliminate residual noise.

2) EM + MAP: we considered the result of the MAP classification and mapped it to the corresponding sources.
3) virtual meas. + ICA: the signals x^2 and x^3 have been computed and considered as additional observations before performing ICA (in our simulations, we used the JADE algorithm [9]). A hard decision (sign function) has then been applied on the estimated sources to eliminate residual noise.
   Note that when the variance σ^2 of the noise ε is known, this information can be used to obtain an unbiased estimate of the covariance of the vector of virtual measurements, leading probably to an improved performance of the method.

Figure 5 and Table I shortly illustrate the validity of the third separation method (virtual meas. + ICA) in the case when the mixture is given by (18). Figure 5 shows the MSE obtained on the reconstructed sources (before elimination of residual noise with a hard decision) and Table I gives the Bit Error Rate (BER) (after applying a sign function). All values have been obtained by averaging on 1000 Monte-Carlo runs. One can notice that in low noise conditions, the nonlinear mixture is perfectly inverted.

Tables II and III compare the three separation methods described above. One can see in Table II that resorting to MAP estimation gives better results than using the exact inversion formula: this is no surprise since the exact inverse is only valid in the noiseless case. However, the method considering virtual measurements outperforms the classification by MAP: this is actually due to the difficulty of initializing the EM algorithm which may get trapped in a local maximum [17]. If a good initialization point was given to the EM algorithm, the EM + MAP separation method would outperform all the other ones. Note also that these results are not specific to the mixture (18). According to the simulations in Table II, they remain when the mixture is given by (9) with randomly generated parameters a, b, c, d. Finally, another advantage of the proposed method of virtual measurements is illustrated in Table III where one can see that the execution time is constant. Again, this advantage is due to the difficulty of initializing the EM algorithm: if badly initialized, it may converge slowly or even require a new initialization step.

It follows from these observations that the proposed method is complementary to the (EM + MAP) classification and one can hence think about combining both in order to improve the quality of the result: one apparently attrative solution consists in using the result given by (virtual meas. + ICA) as an initialization point to the (EM + MAP) method. This has been tried and results are given on the line indicated by ICA + EM + MAP in Table II.

VII. Conclusion

In this paper, we have illustrated that algebraic methods constitute powerful methods to deal with the particular class of polynomial MIMO systems. They offer an attractive answer to the problem of their inversion. Many interesting signals, such as telecommunication ones, admit a finite number of values: in this case, the former tools show that there is more flexibility concerning inversion. In addition, we have shown that there exist a linear model which is equivalent to the original nonlinear one. In a blind context, this equivalent linear model suffers from the problem of underdetermination and of dependency between virtual sources. Finally, we have applied our result to the problem of blind separation of two binary sources mixed nonlinearly: based on the specificity of these sources, and although the virtual sources of the equivalent model are not independent, classical ICA algorithms succeed to separate the virtual sources.

Appendix I
Proof of Property 2

Proof: For any ideal $\mathbf{I}$ and for the polynomial with distinct roots $q_1(s_1) = \prod_{k=1}^{l_1} \left(s_1 - \tilde{a}_1^{(k)}\right)$, we have [16, p.45] (see Definition 5 for the sum of two ideals):

$$\mathbf{I} + \langle q_1 \rangle = \bigcap_{k_1=1}^{l_1} \left(\mathbf{I} + \langle s_1 - \tilde{a}_1^{(k_1)} \rangle\right)$$

It follows that we can write:

$$\begin{aligned} \langle q_1, \ldots, q_N \rangle &= \langle q_2, \ldots, q_N \rangle + \langle q_1 \rangle \\ &= \bigcap_{k_1} \left(\langle q_2, \ldots, q_N \rangle + \langle s_1 - \tilde{a}_1^{(k_1)} \rangle \right) \end{aligned}$$

and decomposing similarly $\langle q_2, \ldots, q_N \rangle + \langle s_1 - \tilde{a}_1^{(k_1)} \rangle$:

$$\langle q_1, \ldots, q_N \rangle = \bigcap_{k_1 k_2} \left(\langle q_3, \ldots, q_N \rangle + \langle s_1 - \tilde{a}_1^{(k_1)}, s_2 - \tilde{a}_2^{(k_2)} \rangle \right)$$

Il we repeat further this operation, we finally obtain:

$$\langle q_1, \ldots, q_N \rangle = \bigcap_{k_1 \ldots k_N} \langle s_1 - \tilde{a}_1^{(k_1)}, \ldots, s_N - \tilde{a}_N^{(k_N)} \rangle = \mathbf{I}_{\mathcal{A}}$$

Finally, to prove that $\{q_1, \ldots, q_N\}$ is a Groebner basis, observe that the q_i are univariate polynomials. Their terms are hence ordered independently of the ordering $\prec$ on $\mathbb{K}[\mathbf{s}]$ and their leading terms are $s_1^{l_1}, \ldots, s_N^{l_N}$ respectively. One can then check that these polynomials satisfy the criterion on the S-polynomials [15, p.82] for $\{q_1, \ldots, q_N\}$ to be a Groebner basis. Finally, one can verify that $\{q_1, \ldots, q_N\}$ is indeed a reduced Groebner basis. ■

APPENDIX II
PROOF OF PROPOSITION 1

Proof: The proof is very similar to the proof of Theorem 2 in [15, p.334].

Choose $q_1, \ldots, q_P$ in $\mathbb{K}[\mathbf{s}]$ such that $\mathbf{I}_{\mathcal{A}} = \langle q_1, \ldots, q_P \rangle$ and let $\mathbf{I} = \mathbf{I}_{\mathcal{A}} + \langle f_1 - x_1, \ldots, f_Q - x_Q \rangle = \langle q_1, \ldots, q_P, f_1 - x_1, \ldots, f_Q - x_Q \rangle$. If g is the remainder of h on division by the Groebner basis G of $\mathbf{I}$, we can write:

$$h = B_1(\mathbf{s}, \mathbf{x})(f_1 - x_1) + \cdots + B_Q(\mathbf{s}, \mathbf{x})(f_Q - x_Q) + C_1(\mathbf{s}, \mathbf{x})q_1 + \cdots + C_P(\mathbf{s}, \mathbf{x})q_P + g$$

where $B_1, \ldots, B_Q, C_1, \ldots, C_P$ are in $\mathbb{K}[\mathbf{s}, \mathbf{x}]$. If $g \in \mathbb{K}[\mathbf{x}]$, substituting f_i for x_i in the above expression, we obtain:

$$h = C_1(\mathbf{s}, \mathbf{f})q_1 + \ldots C_P(\mathbf{s}, \mathbf{f})q_P + g(f_1, \ldots, f_Q)$$

and thus with $r = C_1(\mathbf{s}, \mathbf{f})q_1 + \ldots C_P(\mathbf{s}, \mathbf{f})q_P \in \mathbf{I}_{\mathcal{A}}$, we have $h - r = g(f_1, \ldots, f_Q) \in \mathbb{K}[\mathbf{f}]$

Conversely, assume there is $r \in \mathbf{I}_{\mathcal{A}}$ such that $h - r \in \mathbb{K}[\mathbf{f}]$. Then we can write $h - r = \tilde{g}(f_1, \ldots, f_Q)$ for a polynomial $\tilde{g}$ in $\mathbb{K}[\mathbf{x}]$. Similarly to [15, p.315, Eq. (4)], we can write:

$$\tilde{g}(f_1, \ldots, f_Q) = \tilde{g}(x_1, \ldots, x_Q) + E_1(f_1 - x_1) + \cdots + E_Q(f_Q - x_Q)$$

where $E_1, \ldots, E_Q$ are in $\mathbb{K}[\mathbf{s}, \mathbf{x}]$. Then:

$$h = \tilde{g}(x_1, \ldots, x_Q) + E_1(f_1 - x_1) + \cdots + E_Q(f_Q - x_Q) + r$$

Now let $G' = G \cap \mathbb{K}[\mathbf{x}]$ and $\tilde{\tilde{g}}$ be the remainder of the division of $\tilde{g}$ by G'. We have then: $h = h_{\mathbf{I}} + \tilde{\tilde{g}} + r$, where $h_{\mathbf{I}} \in \mathbf{I}$.

Relying on the elimination property of the ordering, we can use the same arguments as in [15, p.335] to prove that $\tilde{\tilde{g}}$ is the remainder of division of h by G. Hence we have $\tilde{\tilde{g}} = g$, which proves that $g \in \mathbb{K}[\mathbf{x}]$.

The second part of the proposition follows from the above arguments. ■

APPENDIX III
IMPLEMENTATION OF THE PROVIDED EXAMPLES

In this appendix, we show how the results in the paper are obtained using a computer algebra system. We used SINGULAR [27] which is a software freely available on the web.

A. Example from Section IV-A

The ring should first be defined, and then the polynomials corresponding to Equation (5):

```
ring r=0,(s1,s2,x1,x2,x3,x4),lp;
poly f1= 3*s1^2+2*s1*s2+4*s2^2+7*s1+4*s2;
poly f2=-3*s1^2+5*s1*s2+2*s1+s2;
poly f3=-3*s1+6*s2;
poly f4=6*s1^2-s1*s2+4*s2^2+3*s1-9*s2;
```

The following lines define the ideal $\mathbf{I}$, compute its Groebner basis (denoted `G1`) and perform the division of s_1, s_2 by `G1`:

```
ideal I1=f1-x1,f2-x2,f3-x3,f4-x4;
ideal G1=groebner(I1);
reduce(s1,G1); reduce(s2,G1);
```

B. Example from Section IV-B

The following lines show that s_1, s_2 cannot be recovered from x_1, x_2, x_3 only:

```
ideal I2=f1-x1,f2-x2,f3-x3;
ideal G2=groebner(I2);
reduce(s1,G2); reduce(s2,G2);
```

We then test the algebraic dependence between f_1, f_2, f_3 :

```
LIB "algebra.lib";
algDependent(ideal(f1,f2,f3))[1];
```

The example in Section IV-B is then obtained by computing in the ring denoted `r2`:

```
ring r2=(0,b1,b2),(s1,s2,x1,x2,x3,x4),lp;
ideal G2=imap(r,G2);
reduce((s1^2+b1*s1),G2);
reduce((s2^2+b2*s2),G2);
```

C. Example from Section V-B

The only difference in the case of finite alphabet sources is that we should enter and define the ring $\mathbf{I}_{\mathcal{A}}$ (The first line switches back to the working ring denoted `r` since we defined `r2` above).

```
setring r;
ideal Ia=
    (s1-1/2)*(s1-3/2)*(s1+1/2)*(s1+3/2),
    (s2-1/2)*(s2-3/2)*(s2+1/2)*(s2+3/2);
ideal I3=f1-x1,f2-x2,f3-x3,Ia;
ideal G3=groebner(I3);
reduce(s1,G3); reduce(s2,G3);
```

D. Example how to derive Equation (17)

```
ring r3=(0,a,b,c,d),(s1,s2,x),lp;
ideal I4=a*s1*s2+b*s1+c*s2+d-x,s1^2-1,
    s2^2-1;
ideal G4=groebner(I4);
reduce(s1,G4); reduce(s2,G4);
```

REFERENCES

[1] S. Achard and C. Jutten. Identifiability of post-nonlinear mixtures. *IEEE Signal Processing Letters*, 12(5):423–426, May 2005.

[2] H. Arfa, S. E. Asmi, and S. Belghith. A nonlinear channel equalization using an algebraic approach and the affine projection algorithm. In *European Signal Processing Conference (EUSIPCO)*, Florence, Italy, September 2006.

[3] S. E. Asmi and M. Mboup. On the equalizability of nonlinear/time-varying multi-user channels. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, volume 4, pages 2133–2136, May 2001.

[4] M. Babaie-Zadeh. *On blind source separation in convolutive and nonlinear mixtures*. PhD thesis, INP of Grenoble, France, 2002.

[5] M. Babaie-Zadeh and C. Jutten. A general approach for mutual information minimization and its application to blind source separation. *Signal Processing*, 85(5):975–995, May 2005.

[6] M. Babaie-Zadeh, C. Jutten, and K. Nayebi. Blind separating convolutive post non-linear mixtures. In *Proc. of ICA'01*, pages 138–143, San Diego, December 2001.

[7] A. J. Bell and T. J. Sejnowski. An information-maximisation approach to blind separation and blind deconvolution. *Neural computation*, 7(6):1129–1159, November 1995.

[8] B. Buchberger. Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3-4):475–511, March-April 2006.

[9] J.-F. Cardoso and A. Souloumiac. Blind beamforming for non gaussian signals. In *IEEE- Proceedings-F*, volume 140, pages 362–370, 1993.

[10] A. Carini, V. Mathew, and G. Sicuranza. Equalization of recursive polynomial systems. *IEEE Signal Processing Letters*, 6(12):312–314, December 1999.

[11] P. Comon. Independent component analysis, a new concept. *Signal Processing*, 36(3):287–314, April 1994.

[12] P. Comon. Contrasts for multichannel blind deconvolution. *IEEE Signal Processing Letters*, 3(7):209–211, July 1996.

[13] P. Comon. Blind identification and source separation in 2×3 under-determined mixtures. *IEEE Trans. Signal Processing*, 52(1):11–22, January 2004.

[14] P. Comon and O. Grellier. Non-linear inversion of underdetermined mixtures. In *Proc. of ICA'99*, pages 461–465, Aussois, France, January 1999.

[15] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2nd edition, 1996.

[16] D. A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, second edition, 1998.

[17] K. I. Diamantaras. A clustering approach for the blind separation of multiple finite alphabet sequences from a single linear mixture. *Signal Processing*, 86(4):877–891, April 2006.

[18] K. I. Diamantaras and E. Chassioti. Blind separation of n binary sources from one observation: a deterministic approach. In *Proc. of ICA'00*, Helsinki, Finland, June 2000.

[19] K. I. Diamantaras and T. Papadimitriou. Blind deconvolution of multi-input single-output systems with binary sources. *IEEE Trans. Signal Processing*, 54(10):3720–3731, October 2006.

[20] L. T. Duarte and C. Jutten. Blind source separation of a class of nonlinear mixtures. In *Proc. of ICA'07, LNCS 4666*, pages 41–48, 2007.

[21] J. Eriksson and V. Koivunen. Blind identifiability of class of nonlinear instantaneous ICA models. In *European Signal Processing Conference (EUSIPCO)*, volume 2, pages 7–10, Toulouse, France, September 2002.

[22] J. Eriksson and V. Koivunen. Blind separation of a class of nonlinear ICA models. In *IEEE International Symposium on Circuits and Systems ISCAS 2005*, volume 6, pages 5890–5893, May 2005.

[23] F. Gamboa and E. Gassiat. Source separation when the input sources are discrete or have constant modulus. *IEEE Trans. Signal Processing*, 45(12):3062–3072, December 1997.

[24] P. Gao, L. Khor, W. L. Woo, and S. Dlay. Blind source separation of nonlinearly constrained mixed sources using polynomial series reversion. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Toulouse, France, 2006.

[25] O. Grellier, P. Comon, B. Mourrain, and P. Trébuchet. Analytical blind channel identification. *IEEE Trans. Signal Processing*, 50(9):2196–2207, September 2002.

[26] G.-M. Greuel and G. Pfister. *A Singular Introduction to Commutative Algebra*. Springer-Verlag, 2002.

[27] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0.2. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2006. `http://www.singular.uni-kl.de`.

[28] S. Haykin. *Neural Networks: a comprehensive foundation*. Prentice Hall, second edition, 1999.

[29] S. Hosseini and Y. Deville. Blind separation of linear-quadratic mixtures of real sources using a recurrent structure. In J. Mira and J. R. A. eds, editors, *Proc. of IWANN 2003*, volume 2, pages 241–248, Mao, Menorca, Spain, June 2003. (Springer).

[30] A. Hyvärinen and E. Oja. Independent component analysis: Algorithms and applications. *Neural Networks*, 13(4-5):411–430, 2000.

[31] A. Hyvärinen and P. Pajunen. Nonlinear independent component analysis: Existence and uniqueness results. *Neural Networks*, 12(3):429–439, April 1999.

[32] C. Jutten, M. Babaie-Zadeh, and S. Hosseini. Three easy ways for separating nonlinear mixtures? *Signal Processing*, 84(2):217–229, February 2004.

[33] C. Jutten and J. Herault. Blind separation of sources, part i: An adaptative algorithm based on neuromimetic architecture. *Signal Processing*, 24(1):1–10, 1991.

[34] C. Jutten and J. Karhunen. Advances in blind source separation (BSS) and independent component analysis (ICA) for nonlinear mixtures. *Int. J. Neural Systems*, 14(5):267–292, 2004.

[35] A. M. Kagan, Y. V. Linnik, and C. R. Rao. *Characterization Problems in Mathematical Statistics*. John Wiley & Sons, 1973.

[36] B. Lachover and A. Yeredor. Separation of polynomial post non-linear mixtures of discrete sources. In *Proc. of the 2005 IEEE Workshop on Statistical Signal Processing (SSP2005)*, Bordeaux, France, July 2005.

[37] T.-H. Li. Blind identification and deconvolution of linear systems driven by binary random sequences. *IEEE Trans. on Information Theory*, 38(1):26–38, January 1992.

[38] T.-H. Li. Finite-alphabet information and multivariate blind deconvolution and identification of linear systems. *IEEE Trans. on Information Theory*, 49(1):330–337, January 2003.

[39] E. Moreau and J.-C. Pesquet. Generalized contrasts for multichanel blind deconvolution of linear systems. *IEEE Signal Processing Letters*, 4(6):182–183, June 1997.

[40] P. Pajunen. Blind separation of binary sources with less sensors than sources. In *Proc. of the 1997 Int. Conf. on Neural Networks (ICNN-97*.

[41] H. Park, T. Kalker, and M. Vetterli. Gröbner bases and multidimensional FIR multirate systems. *Multidimensional Systems and Signal Processing*, 8:11–30, 1997.

[42] J.-C. Pesquet, B. Chen, and A. P. Petropulu. Frequency-domain contrast functions for separation or convolutive mixtures. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, volume 5, pages 2765–2768, Salt Lake City, USA, May 2001.

[43] R. Rajagopal and L. C. Potter. Multivariate MIMO FIR inverses. *IEEE Trans. on Image Processing*, 12(4):458–465, April 2003.

[44] L. Robbiano. Gröbner Bases and Statistic. In B.Buchberger and F.Winkler, editors, *Gröbner Bases and Applications (Proc. of the Conf. 33 Years of Gröbner Bases)*, volume 251 of *London Mathematical Society Lecture Notes Series*, pages 179–204. Cambridge University Press, 1998.

[45] A. Taleb and C. Jutten. Sources separation in post-nonlinear mixtures. *IEEE Trans. Signal Processing*, 49(10):2807–2820, October 1999.

[46] P. Vandewalle, L. Sbaiz, and M. Vetterli. Signal reconstruction from multiple unregistered set of samples using groebner bases. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, volume 3, pages 604–607, Toulouse, France, May 2006.

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

[48] J. Zhang, J. W. Modestino, and D. A. Langan. Maximum-likelihood parameter estimation for unsupervised stochastic model-based image segmentation. *IEEE Trans. on Image Processing*, 3(4):404–420, July 1994.

[49] J. Zhou and M. N. Do. Multidimensional multichannel FIR deconvolution using Gröbner bases. *IEEE Trans. on Image Processing*, 15(10):2998–3007, October 2006.

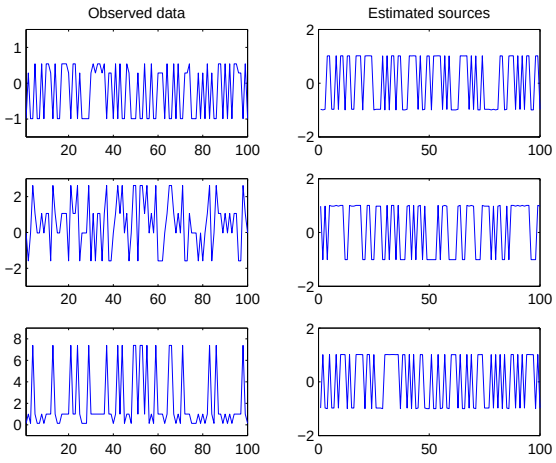

Fig. 1. Typical results for the inversion of the nonlinear system given by (16) (no additive noise).

mixing sytem	separation method	SNR in dB 10	20	30	40	50
Eq.(16)	EM + inversion	3.51e-1	1.18e-1	1.20e-1	1.40e-1	1.15e-1
	EM + MAP	2.20e-1	6.93e-2	9.24e-2	1.22e-1	8.59e-2
	virtual meas. + ICA	1.63e-1	1.83e-2	1.88e-4	0	0
	ICA + EM + MAP	2.08e-1	1.10e-2	0	0	0
random	EM + inversion	2.75e-1	1.83e-1	1.31e-1	8.10e-2	3.48e-2
	EM + MAP	1.76e-1	1.28e-1	1.10e-1	7.15e-2	2.94e-2
	virtual meas. + ICA	1.68e-1	5.98e-2	1.99e-2	7.56e-3	2.91e-3

TABLE II

AVERAGE BER FOR DIFFERENT SEPARATION METHODS (5000 SAMPLES, 1000 MONTE-CARLO REALIZATIONS).

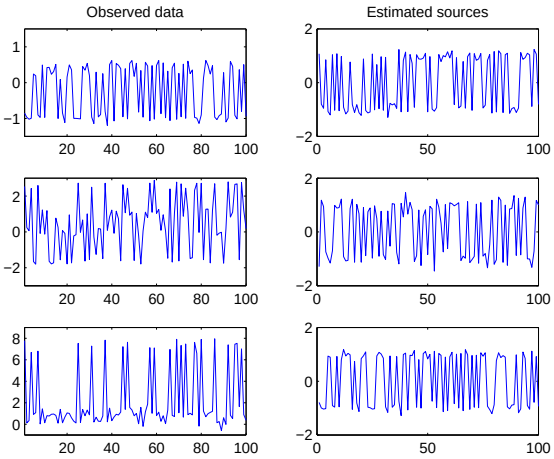

Fig. 2. Typical results for the inversion of the nonlinear system given by (16) (20dB noise).

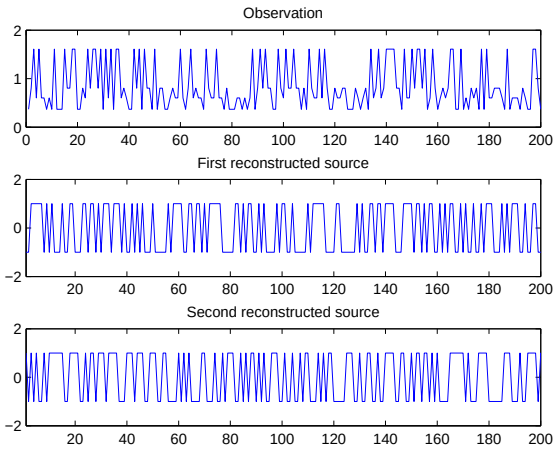

Fig. 4. Nonlinear mixture of two BPSK sources on one sensor: typical separation result in the noiseless case.

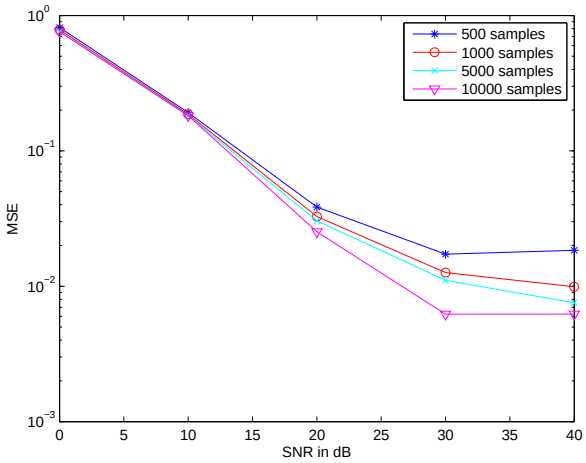

Fig. 3. Average MSE on the reconstruction of the sources versus SNR for different number of samples for the mixing system given by (16).

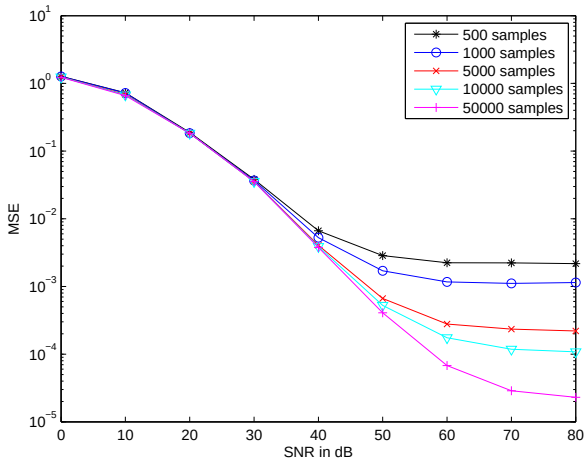

Fig. 5. Nonlinear mixture of two BPSK sources on one sensor: average MSE versus SNR in dB (mixture given by Eq. (18)).

Samples \ SNR (dB)	0	10	20	30	40
500	0.3297	0.1873	0.0203	0.0002	0
5000	0.3267	0.1614	0.0184	0.0002	0
50000	0.3130	0.1490	0.0182	0.0002	0

TABLE I

NONLINEAR MIXTURE OF TWO BPSK SOURCES ON ONE SENSOR: AVERAGE BER VERSUS SNR IN dB (MIXTURE GIVEN BY EQ. (18)).

separation method	SNR in dB				
	10	20	30	40	50
EM + MAP	3.53e-1	1.96e-1	1.45e-1	1.24e-1	1.21e-1
virtual meas. + ICA	1.33e-1	1.33e-1	1.34e-1	1.33e-1	1.34e-1

TABLE III

AVERAGE EXECUTION TIME FOR THE (EM + MAP) ALGORITHM AND THE ICA ALGORITHMS ON VIRTUAL MEASUREMENTS (5000 SAMPLES, 1000 MONTE-CARLO REALIZATIONS, RANDOMLY DRIVEN MIXING SYSTEM).

Marc Castella was born in 1976 in Courbevoie, France. In 2000, he received the "Agrégation" degree in the field of applied physics and in 2001 he received the M.Sc. degree in electrical engineering, from both the "École Normale Supérieure de Cachan" and the "Université Paris-Sud, Orsay" (France). He obtained his Ph.D. degree from "Université de Marne-la-Vallée" (France) in 2004. Since then, he has been "Maître de Conférence" in Evry (France) at "TELECOM & Management SudParis" (formerly "Institut National des Télécommunications (INT)"). He is also a member of the UMR-CNRS 5157 research team SAMOVAR. His research activities have focused on the problem blind source separation in general.