ELSEVIER

Systems & Control Letters 47 (2002) 279–286

SYSTEMS & CONTROL LETTERS

www.elsevier.com/locate/sysconle

Finite alphabet source recovery in polynomial systems☆

Jonathan H. Manton*

ARC Special Research Centre for Ultra-Broadband Information Networks, Department of Electrical and Electronic Engineering, The University of Melbourne, Melbourne, Victoria 3010, Australia

Received 6 November 2001; received in revised form 8 April 2002; accepted 8 May 2002

Abstract

Consider a parameterised system whose output vector is a polynomial function of the elements of both the source vector and the parameter vector. Assume there are only a finite number of possible source vectors. Source recovery endeavours to determine the source vector given only the output vector and, in particular, without knowledge of the parameter vector. This paper, after proving both the decidability and implementability of source recovery, focuses on the task of deriving necessary and sufficient conditions for source recovery to be feasible. Although it is difficult to derive a condition which is readily verifiable for most systems, this paper derives a relatively simple condition for source recovery to be feasible in bilinear and other affine-in-parameter systems. An application of this result to wireless communications is given; it is proved that guard intervals in transmission systems enable the receiver to recover the source symbols using only a single received block and without knowledge of the channel parameters.

Keywords: System identification; Polynomial equations; Decidability; Invertibility

1. Introduction

Any discrete time deterministic system observed over a finite period of time can be described by $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$, where the vectors $\boldsymbol{s}$, $\boldsymbol{y}$ and $\boldsymbol{h}$ are the collated input, collated output and initial state, respectively. The finite alphabet source recovery problem is to determine $\boldsymbol{s}$ given both $\boldsymbol{y}$ and the knowledge that $\boldsymbol{s}$ belongs to a finite set Ω of possible input vectors; the set Ω naturally arises when the input $\boldsymbol{s}$ is a digital signal and its elements are restricted to the values -1 or 1, for instance. The source recovery problem is related to, but distinct from, the observability problem of determining $\boldsymbol{h}$ given $\boldsymbol{y}$. Under the restriction that F is a polynomial map over the field of complex numbers, this paper proves that the feasibility of source recovery is both a decidable question and an implementable task. That is to say, a computer (specifically, a Turing machine) can determine in a finite number of steps whether or not source recovery is feasible, and moreover, if source recovery is feasible, a computer can recover $\boldsymbol{s}$ given $\boldsymbol{y}$. This paper also derives necessary and sufficient conditions for source recovery to be feasible and applies this theory to a practical problem in wireless communications. This is now elaborated on.

In wireless communications, the received signal is the convolution of the transmitted signal with the impulse response of the wireless channel (modelled as

☆ This work was performed in part while the author was visiting ENST/TSI in Paris, France.

* Tel.: +61383446791; fax: +61383446678.
E-mail address: jon@ee.mu.oz.au (J.H. Manton).

0167-6911/02/$ - see front matter
PII: S0167-6911(02)00180-9

a linear FIR channel) [13]. By sampling the received signal, the system can be modelled by $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$, where $\boldsymbol{s}$ represents one or more blocks of transmitted data, $\boldsymbol{h}$ is the impulse response of the channel, $\boldsymbol{y}$ is the received vector and F is the bilinear map convolving $\boldsymbol{s}$ with $\boldsymbol{h}$. Because $\boldsymbol{s}$ is a digital signal (or codeword), the set of all possible transmitted signals Ω is a finite set. Recovering $\boldsymbol{s}$ from $\boldsymbol{y}$ is often done indirectly by first determining $\boldsymbol{h}$ from $\boldsymbol{y}$, a process known as blind identification [7], and then deconvolving $\boldsymbol{y}$ with $\boldsymbol{h}$ to obtain $\boldsymbol{s}$. Blind identification usually relies on statistical properties of $\boldsymbol{s}$ and thus requires a relatively large amount of output data for accurate identification. Exploiting finite alphabet properties rather than statistical properties has been investigated [16] as a way of reducing the required amount of output data. Conditions for source recovery to be feasible in uncoded wireless communications are given in [4]. Here, uncoded means Ω contains all N^p sequences of p symbols coming from an alphabet of size N.

The necessary and sufficient conditions derived here for source recovery to be feasible in a general polynomial system F simplify considerably when F is a bilinear map. These simplified conditions complement those in [4] and are valid for both coded and uncoded communications (that is, for arbitrary Ω). Furthermore, it is proved the receiver can recover the source symbols given only a single received block if guard intervals (sequences of zeros clearing the memory of the channel) are inserted between blocks. This is an interesting result because, without guard intervals present, certain non-persistently exciting input sequences exist for which source recovery is not feasible [4].

Caveats: Only complex-valued polynomial maps are considered because the approach taken here relies on the base field being algebraically closed. In general, the symbolic methods alluded to for deciding and implementing source recovery are too computationally intensive to be practical. The effect of noise (trying to recover $\boldsymbol{s}$ from $\boldsymbol{y} + \boldsymbol{n}$ where $\boldsymbol{n}$ represents an additive disturbance) is not considered.

Notation and conventions: The usual topology is used throughout. Closure and set complement of X are denoted by $\bar{X}$ and X^{c}, respectively. A superscript T denotes vector transpose. Standard results in algebraic geometry are taken from [2,5,6,1].

2. Decidability and implementability of source recovery

Let $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ be a polynomial map and $\Omega \subset \mathbb{C}^p$ a finite set of candidate source vectors. The source recovery problem is to determine the source vector $\boldsymbol{s}$ from the output vector $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$ given that $\boldsymbol{s}$ is an element of Ω but with essentially no knowledge of the parameter vector $\boldsymbol{h} \in \mathbb{C}^m$. Specifically, it is required to find a function $r : \mathbb{C}^n \to \mathbb{C}^p$ satisfying

$$r(F(\boldsymbol{s}, \boldsymbol{h})) = \boldsymbol{s} \tag{1}$$

for all $\boldsymbol{s} \in \Omega$ and, ideally, for all $\boldsymbol{h} \in \mathbb{C}^m$. Unfortunately, Example 1 shows this property is too stringent to be of interest.

Example 1. Let $F(s, h) = (h, sh)$. Clearly, s can be determined from y unless $h = 0$.

It is therefore appropriate to require (1) to hold for almost all $\boldsymbol{h}$ rather than for all $\boldsymbol{h}$.

Definition 2 (Source recovery). Let $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ be a polynomial map and $\Omega \subset \mathbb{C}^p$ a finite set of candidate source vectors. Source recovery is feasible if there exists a function $r : \mathbb{C}^n \to \mathbb{C}^p$ and an open dense set $\mathscr{H} \subset \mathbb{C}^m$ such that (1) holds for all $\boldsymbol{s} \in \Omega$ and $\boldsymbol{h} \in \mathscr{H}$.

The openness condition on $\mathscr{H}$ is desirable for otherwise choosing $\mathscr{H}$ to be the set of complex numbers with rational real part makes $s \in \Omega = \{1, \pi\}$ recoverable from $y = F(s, h) = sh$.

Source recovery is equivalent to the following injectivity property of F. The trivial proof is omitted.

Lemma 3. *Source recovery is feasible if and only if there exists an open dense set $\mathscr{H}$ such that, for all $\boldsymbol{h}_1, \boldsymbol{h}_2 \in \mathscr{H}$ and $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega, F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ implies $\boldsymbol{s}_1 = \boldsymbol{s}_2$.*

Sets defined by the vanishing of a finite number of polynomials are called varieties [2]. (An alternative convention is to call such sets algebraic sets, with the term variety reserved for what will be called here an irreducible variety.) Whereas open dense sets cannot be manipulated by computers, varieties can. The following is therefore a key technical result; its proof follows shortly.

Theorem 4. *Source recovery is feasible if and only if there exists a proper subvariety V of $\mathbb{C}^m$ such that, for all $\boldsymbol{h}_1, \boldsymbol{h}_2 \in \mathbb{C}^m - V$ and $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, $F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ implies $\boldsymbol{s}_1 = \boldsymbol{s}_2$.*

A variety V satisfying the conditions in Theorem 4 is called a blacklist because, as Example 5 illustrates, a source recovery algorithm might have to assume the parameter $\boldsymbol{h}$ does not belong to V. This is often a reasonable assumption because V, being a proper subvariety, is a nowhere dense set [2]. When this is not a reasonable assumption, the stricter definition of source recovery introduced in Section 3 should be used instead.

Example 5. Let $F(s,h) = sh$, $\Omega = \{0,1\}$ and $V = \{0\}$. Source recovery is feasible. However, because $F(1,0) = F(0,1) = 0$, the only way to decide whether $s = 0$ or $s = 1$ given $F(s,h) = 0$ is to exclude the possibility that $h \in V$. A side effect is that incorrect decisions are possible if $h \in V$.

The main results of this section are now stated.

Theorem 6 (Decidable). *There exists an algorithm, implementable on a computer and terminating in finite time, taking as input a polynomial map $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ and a finite set $\Omega \subset \mathbb{C}^p$, and outputting "feasible" or "not feasible" depending on whether or not source recovery is feasible according to Definition 2.*

Theorem 7 (Implementable). *If source recovery is feasible then there exists a source recovery algorithm implementing the source recovery function r in Definition 2. This algorithm is implementable on a computer and terminates in finite time.*

The proofs of the above theorems depend on being able to construct a blacklist V. Algorithm 8 is proposed for generating V; that it generates a valid blacklist is not obvious and is proved later. First some definitions. For any pair of distinct elements $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, define the sets

$$W = \{(\boldsymbol{h}_1, \boldsymbol{h}_2) \in \mathbb{C}^m \times \mathbb{C}^m : F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)\}, \tag{2}$$

$$W_1 = \{\boldsymbol{h}_1 \in \mathbb{C}^m : \exists \boldsymbol{h}_2 \in \mathbb{C}^m,\ F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)\}, \tag{3}$$

$$W_2 = \{\boldsymbol{h}_2 \in \mathbb{C}^m : \exists \boldsymbol{h}_1 \in \mathbb{C}^m,\ F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)\}. \tag{4}$$

The sets W_1 and W_2 are constructible sets [2,6] because they are projections of the variety W. Therefore, their closures are varieties and have well-defined dimensions [2]. (Recall the usual topology and not the Zariski topology is used throughout. However, the closure in the usual topology and the Zariski closure of a constructible set are equal.) Define

$$V_{\boldsymbol{s}_1,\boldsymbol{s}_2} = \begin{cases} \bar{W}_1 & \text{if } \dim \bar{W}_1 \leqslant \dim \bar{W}_2, \\ \bar{W}_2 & \text{otherwise,} \end{cases} \tag{5}$$

where V is subscripted to indicate the dependence on $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$.

Algorithm 8 (Blacklist). *Assume Ω consists of N elements, $\Omega = \{\boldsymbol{s}_1, \ldots, \boldsymbol{s}_N\}$. For any pair $\boldsymbol{s}_i, \boldsymbol{s}_j$, construct the variety $V_{\boldsymbol{s}_i,\boldsymbol{s}_j}$ as in (5). Form the blacklist V as the union*

$$V = \bigcup_{1 \leqslant i < j \leqslant N} V_{\boldsymbol{s}_i,\boldsymbol{s}_j}. \tag{6}$$

Since a finite union of varieties is a variety, V in (6) is a variety. Moreover, V can be constructed on a computer because symbolic techniques exist for manipulating varieties [1–3].

The following lemma implies V is a valid blacklist provided it is a proper subvariety. The proof below of Theorem 4 will show V is a proper subvariety if and only if source recovery is feasible.

Lemma 9. *Define V as in (6). Then, for all $\boldsymbol{h}_1, \boldsymbol{h}_2 \in \mathbb{C}^m - V$ and $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, $F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ implies $\boldsymbol{s}_1 = \boldsymbol{s}_2$.*

Proof. Let $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ be distinct and define W, W_1, W_2 as in (2)–(4). If $F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ then $(\boldsymbol{h}_1, \boldsymbol{h}_2) \in W$, hence $\boldsymbol{h}_1 \in W_1$ and $\boldsymbol{h}_2 \in W_2$. In particular, it follows from (5) and (6) that either $\boldsymbol{h}_1 \in V$ or $\boldsymbol{h}_2 \in V$, proving the lemma. □

Proof of Theorem 4. One direction is clear; if V is a proper subvariety then $\mathscr{H} = \mathbb{C}^m - V$ is an open dense set and source recovery is feasible by Lemma 3. To prove the other direction, it is shown that if

source recovery is feasible then V in (6) is a proper subvariety. Theorem 4 then follows from Lemma 9.

Assume V is not a proper subvariety. Then $V = \mathbb{C}^m$ and hence there must exist a pair of distinct points $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ such that, in (3) and (4), $\bar{W}_1 = \bar{W}_2 = \mathbb{C}^m$. Define $g_1(\boldsymbol{h}_1) = F(\boldsymbol{s}_1, \boldsymbol{h}_1)$ and $g_2(\boldsymbol{h}_2) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ so that $(\boldsymbol{h}_1, \boldsymbol{h}_2) \in W$ if and only if $g_1(\boldsymbol{h}_1) = g_2(\boldsymbol{h}_2)$; see (2). Assume to the contrary that source recovery is feasible and let $\mathscr{H}$ satisfy the conditions in Lemma 3. By definition of $\mathscr{H}$, for any $\boldsymbol{h}_1 \in W_1$, either $\boldsymbol{h}_1$ is excluded from $\mathscr{H}$ or all the pre-images $g_2^{-1}(g_1(\boldsymbol{h}_1))$ are excluded from $\mathscr{H}$. Equivalently, if $Z = g_2^{-1}(g_1(\mathscr{H}))$ then $Z \subset \mathscr{H}^c$ must hold. It will be shown that Z contains a non-empty open set, contradicting the denseness of $\mathscr{H}$.

Let $U_1, U_2 \subset \mathbb{C}^n$ be the images of g_1, g_2 respectively. Since g_1, g_2 are polynomial maps, $\bar{U}_1, \bar{U}_2$ are irreducible varieties [2,6]. It is first shown that $\bar{U}_1 = \bar{U}_2$. Assume to the contrary that $\bar{U}_1 \cap \bar{U}_2 \subsetneq \bar{U}_1$. Then, because $\bar{U}_1 \cap \bar{U}_2$ is a proper subvariety of the irreducible variety $\bar{U}_1$, there exists a non-empty set $Y \subset U_1 \cap U_2^c$ open in $\bar{U}_1$. For any $\boldsymbol{h}_1 \in g_1^{-1}(Y)$, $g_1(\boldsymbol{h}_1) = g_2(\boldsymbol{h}_2)$ has no solution. In particular, $g_1^{-1}(Y)$ is a non-empty open set contained in W_1^c, contradicting $\bar{W}_1 = \mathbb{C}^m$. This proves $\bar{U}_1 \cap \bar{U}_2 = \bar{U}_1$ and, by symmetry, $\bar{U}_1 = \bar{U}_2$ too. Since $\mathscr{H}$ is non-empty and open, the Open Mapping Theorem [14] ensures there exists a non-empty set $Y \subset g_1(\mathscr{H})$ open in $\bar{U}_1$. Then Y is open in $\bar{U}_2$ and hence $g_2^{-1}(Y)$ is a non-empty open set contained in Z, the desired contradiction. □

Proof of Theorem 6. The proof of Theorem 4 shows source recovery is feasible if and only if V in (6) satisfies $V \neq \mathbb{C}^m$. It has already been mentioned that V can be constructed on a computer using symbolic techniques. The theorem follows. □

Proof of Theorem 7. Given a polynomial map $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ and a set $\Omega \subset \mathbb{C}^p$, let V be variety (6); it can be constructed on a computer. It has already been shown in the proof of Theorem 4 that V is a proper subvariety if source recovery is feasible. It therefore suffices to derive an algorithm mapping $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$ to $\boldsymbol{s}$ for any $\boldsymbol{s} \in \Omega$ and $h \in \mathbb{C}^m - V$. The following algorithm does just this. Given the output vector $\boldsymbol{y} \in \mathbb{C}^n$, symbolic techniques exist [1–3] for constructing the set $S = \{\boldsymbol{s} \in \Omega : \exists \boldsymbol{h} \in \mathbb{C}^m - V, F(\boldsymbol{s}, \boldsymbol{h}) = \boldsymbol{y}\}$. If $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$ for some $\boldsymbol{s} \in \Omega$ and $\boldsymbol{h} \in \mathbb{C}^m - V$ then, by Lemma 9, the set S contains a single element; source recovery is accomplished by outputting this element. □

3. Strict source recovery

The definition of source recovery in Definition 2 was shown in Example 5 to have two potential disadvantages; source recovery may require knowledge of the blacklist, and furthermore, incorrect decisions are possible. This section states a stricter definition of source recovery simultaneously removing the need for a blacklist and the potential for incorrect decisions.

In Lemma 3, assume $\boldsymbol{s}_1$ and $\boldsymbol{h}_1$ represent the true source and channel vectors while $\boldsymbol{s}_2$ and $\boldsymbol{h}_2$ represent any combination resulting in the same output. Restricting $\boldsymbol{h}_2$ to lie in $\mathscr{H}$ is the reason a source recovery algorithm may require knowledge of the blacklist. This motivates the following definition.

Definition 10 (Strict source recovery). Let $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ be a polynomial map and $\Omega \subset \mathbb{C}^p$ a finite set of candidate source vectors. Strict source recovery is feasible if there exists an open dense set $\mathscr{H} \subset \mathbb{C}^m$ such that for all $\boldsymbol{h}_1 \in \mathscr{H}$, $\boldsymbol{h}_2 \in \mathbb{C}^m$ and $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, $F(\boldsymbol{s}_1, \boldsymbol{h}_1) = F(\boldsymbol{s}_2, \boldsymbol{h}_2)$ implies $\boldsymbol{s}_1 = \boldsymbol{s}_2$.

Definition 10 is indeed stricter than Definition 2; source recovery but not strict source recovery is feasible in Example 5. Moreover, Definition 10 is not vacuous because strict source recovery is feasible in Example 1.

Theorem 11 proves results analogous to Theorems 4, 6 and 7 but for strict source recovery. Theorem 12 proves incorrect decisions are avoidable under Definition 10.

Theorem 11. *For a given F and Ω as in Definition* 10, *construct the variety $V \subset \mathbb{C}^m$ as in* (6) *of Algorithm* 8 *but with $V_{\boldsymbol{s}_1,\boldsymbol{s}_2} = \bar{W}_1 \cup \bar{W}_2$ replacing* (5). *Strict source recovery is feasible if and only if $V \neq \mathbb{C}^m$. Moreover, if strict source recovery is feasible then $\mathscr{H} = \mathbb{C}^m - V$ satisfies the conditions in Definition* 10. *Strict source recovery is both decidable and implementable.*

Proof. Define $\mathscr{H} = \mathbb{C}^m - V$. If $V \neq \mathbb{C}^m$ then V is a proper subvariety of $\mathbb{C}^m$ and hence $\mathscr{H}$ is open and dense. Moreover, if $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ and $\boldsymbol{h}_1, \boldsymbol{h}_2 \in \mathbb{C}^m$ are such

that $F(\boldsymbol{s}_1,\boldsymbol{h}_1)=F(\boldsymbol{s}_2,\boldsymbol{h}_2)$ but $\boldsymbol{s}_1\neq\boldsymbol{s}_2$ then, from the definition of V, it can be deduced that $\boldsymbol{h}_1\in V$ and hence $\boldsymbol{h}_1\notin\mathscr{H}$. This proves $V\neq\mathbb{C}^m$ implies strict source recovery is feasible. Assume now that $V=\mathbb{C}^m$. Then there exists a distinct pair $\boldsymbol{s}_1,\boldsymbol{s}_2\in\Omega$ such that $V_{\boldsymbol{s}_1,\boldsymbol{s}_2}=\bar{W}_1\cup\bar{W}_2=\mathbb{C}^m$, and hence either $\bar{W}_1=\mathbb{C}^m$ or $\bar{W}_2=\mathbb{C}^m$. By interchanging $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ if necessary, assume $\bar{W}_1=\mathbb{C}^m$. By definition of W_1, if strict source recovery is feasible then $\mathscr{H}$ in Definition 10 must satisfy $\mathscr{H}\subset W_1^c$. Because $\mathscr{H}$ is non-empty and open and W_1 is dense, this is not possible, proving $V=\mathbb{C}^m$ implies strict source recovery is not feasible. That strict source recovery is decidable and implementable follows analogously to the proofs of Theorems 6 and 7. (Replace S in the proof of Theorem 7 by $S=\{\boldsymbol{s}\in\Omega\colon\exists\boldsymbol{h}\in\mathbb{C}^m,\ F(\boldsymbol{s},\boldsymbol{h})=\boldsymbol{y}\}$.) □

Theorem 12. *If source recovery is feasible but strict source recovery is not, there exists an $\boldsymbol{s}\in\Omega$ and $h\notin\mathscr{H}$ such that an incorrect decision is made; see Definition 2 and Example 5 for notation. Conversely, if strict source recovery is feasible then incorrect decisions*[1] *are avoidable.*

Proof. Assume source recovery is feasible and let $\mathscr{H}$ be a set satisfying the conditions in Lemma 3. Because source recovery but not strict source recovery is feasible, there exist distinct $\boldsymbol{s}_1,\boldsymbol{s}_2\in\Omega$ such that $\bar{W}_1=\mathbb{C}^m$ but $\bar{W}_2\neq\mathbb{C}^m$ in (3) and (4); see the proofs of Theorems 4 and 11. For any point $(\boldsymbol{h}_1,\boldsymbol{h}_2)\in W$, either $\boldsymbol{h}_1$ or $\boldsymbol{h}_2$ must be excluded from $\mathscr{H}$ because $F(\boldsymbol{s}_1,\boldsymbol{h}_1)=F(\boldsymbol{s}_2,\boldsymbol{h}_2)$. Since W_1 is dense and $\mathscr{H}$ is open and dense, there must exist a point $(\boldsymbol{h}_1,\boldsymbol{h}_2)\in W$ such that $\boldsymbol{h}_2$ is excluded from $\mathscr{H}$ but $\boldsymbol{h}_1$ is not. Since $\boldsymbol{h}_1\in\mathscr{H}$, r in (1) must satisfy $r(F(\boldsymbol{s}_1,\boldsymbol{h}_1))=\boldsymbol{s}_1$. However, this means $r(F(\boldsymbol{s}_2,\boldsymbol{h}_2))=\boldsymbol{s}_1$ because $F(\boldsymbol{s}_1,\boldsymbol{h}_1)=F(\boldsymbol{s}_2,\boldsymbol{h}_2)$ by construction. That is, an incorrect decision is made.

Assume strict source recovery is feasible. Referring to the proof of Theorem 11, given $\boldsymbol{y}$, source recovery can be performed by forming the set $S=\{\boldsymbol{s}\in\Omega\colon\exists\boldsymbol{h}\in\mathbb{C}^m,\ F(\boldsymbol{s},\boldsymbol{h})=\boldsymbol{y}\}$ and outputting the element of S if S contains a single element and outputting "unrecoverable" otherwise. Because S always contains the true source vector (that is, if $\boldsymbol{y}=F(\boldsymbol{s},\boldsymbol{h})$ then $\boldsymbol{s}\in S$), an incorrect decision is never made. □

Remark 13. Identifiability results in the literature usually take the following form. First, a set of channel assumptions is imposed on the channel; this is equivalent to requiring $\boldsymbol{h}$ lies in the set $\mathscr{H}$ in Definition 2. Then the equation $F(\boldsymbol{s},\boldsymbol{h})=F(\tilde{\boldsymbol{s}},\tilde{\boldsymbol{h}})$ is studied for multiple solutions indicating identification is not possible. Here, some studies assume $\tilde{\boldsymbol{h}}$ also satisfies the channel assumptions whereas other studies do not. The former corresponds to Definition 2 (see also Lemma 3) while the latter corresponds to Definition 10.

4. An equivalent condition for feasibility of source recovery

Sections 2 and 3 showed that feasibility of source recovery can always be proved or disproved using symbolic techniques. Sometimes it is desirable to prove source recovery is feasible without using symbolic techniques. To facilitate this, a condition more convenient than in Definition 2 for source recovery to be feasible is derived below.

Referring to Lemma 3, it might be hoped that, for fixed $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$, if there exists a point $\boldsymbol{h}_1$ such that $F(\boldsymbol{s}_1,\boldsymbol{h}_1)=F(\boldsymbol{s}_2,\boldsymbol{h}_2)$ has no solution in $\boldsymbol{h}_2$ then a continuity argument implies $F(\boldsymbol{s}_1,\boldsymbol{h}_1)=F(\boldsymbol{s}_2,\boldsymbol{h}_2)$ has no solution for almost all $\boldsymbol{h}_1$. Example 14 shows this is not so due to possible solutions at infinity.

Example 14. Let $F(s,(h_1,h_2))=(sh_1h_2-h_1,h_2)$ and $\Omega=\{0,1\}$. Define $g_1(h_1,h_2)=F(0,(h_1,h_2))=(-h_1,h_2)$ and $g_2(h_1,h_2)=F(1,(h_1,h_2))=(h_1h_2-h_1,h_2)$. Consider the choice $h_1=5$ and $h_2=1$. Then $g_1(h_1,h_2)=(-5,1)$ and, in particular, $g_2(h_1',h_2')=(-5,1)$ appears to have no solution. However, there is a solution of $g_2(h_1',h_2')=(-5,1)$ hiding at infinity; the divergent sequence $\{(-5k,1+1/k)\}_{k=0}^{\infty}$ is such that $g_2(-5k,1+1/k)=(-5,1+1/k)$ converges to $(-5,1)$. In particular, this means that for most (h_1,h_2), $g_1(h_1,h_2)=g_2(h_1',h_2')$ has a solution, contrary to what might have been thought had the solution at infinity not been detected.

Proving no solution at infinity exists is tantamount to verifying the condition in the following theorem.

[1] Making an incorrect decision refers to recovering $\boldsymbol{s}$ incorrectly, as in Example 5, and is distinct from not being able to recover $\boldsymbol{s}$ if $\boldsymbol{h}\notin\mathscr{H}$, as in Example 1.

Theorem 15. *Source recovery is feasible if and only if, for any pair of distinct points* $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$,

$\exists$ *non-empty open* $X_1, X_2 \subset \mathbb{C}^m$ *with one dense*,

$$\forall \boldsymbol{h}_1 \in X_1,\ \forall \boldsymbol{h}_2 \in X_2, \quad F(\boldsymbol{s}_1, \boldsymbol{h}_1) \neq F(\boldsymbol{s}_2, \boldsymbol{h}_2). \tag{7}$$

Strict source recovery is feasible if and only if, for any pair of distinct points $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$,

$\exists$ *non-empty open* $X \subset \mathbb{C}^m$, $\forall \boldsymbol{h}_1 \in X$, $\forall \boldsymbol{h}_2 \in \mathbb{C}^m$,

$$F(\boldsymbol{s}_1, \boldsymbol{h}_1) \neq F(\boldsymbol{s}_2, \boldsymbol{h}_2). \tag{8}$$

Note that the sets X_1, X_2 *and* X *can depend on* $\boldsymbol{s}_1$ *and* $\boldsymbol{s}_2$.

Proof. Assume source recovery is feasible and let $\mathscr{H}$ be any set satisfying the conditions in Lemma 3. Then (7) holds with the choice $X_1 = X_2 = \mathscr{H}$. Similarly, if $\mathscr{H}$ satisfies the conditions in Definition 10 then (8) holds with the choice $X = \mathscr{H}$. Conversely, if source recovery is not feasible then the proof of Theorem 4 shows there exist distinct $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ such that the closures of the images of g_1 and g_2 are identical, and moreover, if X_1, X_2 are non-empty open sets then both $g_2^{-1}(g_1(X_1))$ and $g_1^{-1}(g_2(X_2))$ contain non-empty open sets. Since (7) implies both $g_2^{-1}(g_1(X_1)) \subset X_2^c$ and $g_1^{-1}(g_2(X_2)) \subset X_1^c$, neither X_1 nor X_2 can be dense, proving (7) cannot hold. If strict source recovery is not feasible then the proof of Theorem 11 shows there exist distinct $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ such that $\bar{W}_1 = \mathbb{C}^m$ in (3). In particular, no open set $X \subset W_1^c$ exists, hence (8) cannot hold.

Remark 16. Polynomial systems F with the property that $\{(\boldsymbol{s}', \boldsymbol{h}')\colon F(\boldsymbol{s}', \boldsymbol{h}') = F(\boldsymbol{s}, \boldsymbol{h})\}$ contains only a finite number of elements for almost all $(\boldsymbol{s}, \boldsymbol{h})$ are called weakly identifiable in [11]. This property is readily established by checking the Jacobian matrix of F has full column rank [10,11]. A straightforward argument shows that for almost any Ω, source recovery is feasible.[2] However, for a specific Ω, using (7) to prove source recovery appears unavoidable. Indeed, it is required to study the behaviour of F in a neighbourhood of a point rather than at a single point to ensure solutions at infinity and other non-generic behaviour are detected.

[2] Provided $\boldsymbol{s}$ is a generic point [11], if $\boldsymbol{s} \in \Omega$ then there are at most a finite number of points $\boldsymbol{s}'$ which must be excluded from Ω as a consequence. As almost all points are generic points, it follows that almost any Ω will satisfy this condition.

5. Source recovery in affine-in-parameter systems

The map $F(\boldsymbol{s}, \boldsymbol{h})$ is bilinear if it is linear in $\boldsymbol{s}$ with $\boldsymbol{h}$ held fixed and linear in $\boldsymbol{h}$ with $\boldsymbol{s}$ held fixed. The conditions for source recovery in Theorem 15 simplify greatly if F is bilinear. This generalises to the wider class of systems now defined.

Definition 17 (Affine in parameters). The polynomial map $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ is affine in its parameter vector $\boldsymbol{h} \in \mathbb{C}^m$ for all source vectors $\boldsymbol{s} \in \Omega \subset \mathbb{C}^p$ if it satisfies

$$\forall \boldsymbol{s} \in \Omega,\ \forall \boldsymbol{h}_1, \boldsymbol{h}_2 \in \mathbb{C}^m,\ \forall \lambda \in \mathbb{C},$$

$$F(\boldsymbol{s}, \lambda \boldsymbol{h}_1 + (1-\lambda)\boldsymbol{h}_2) = \lambda F(\boldsymbol{s}, \boldsymbol{h}_1) + (1-\lambda) F(\boldsymbol{s}, \boldsymbol{h}_2). \tag{9}$$

Theorem 18. *Let* $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ *be a polynomial map satisfying* (9) *for some finite set of candidate source vectors* $\Omega \subset \mathbb{C}^p$. *Source recovery is feasible if and only if, for any pair of distinct points* $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, *there exists an* $\boldsymbol{h} \in \mathbb{C}^m$ (*possibly depending on* $\boldsymbol{s}_1$ *and* $\boldsymbol{s}_2$) *such that either* $F(\boldsymbol{s}_1, \boldsymbol{h}) = F(\boldsymbol{s}_2, \boldsymbol{h}')$ *or* $F(\boldsymbol{s}_2, \boldsymbol{h}) = F(\boldsymbol{s}_1, \boldsymbol{h}')$ *or both has no solution in* $\boldsymbol{h}' \in \mathbb{C}^m$. *Strict source recovery is feasible if and only if, for any pair of distinct points* $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, *there exists an* $\boldsymbol{h} \in \mathbb{C}^m$ (*possibly depending on* $\boldsymbol{s}_1$ *and* $\boldsymbol{s}_2$) *such that* $F(\boldsymbol{s}_1, \boldsymbol{h}) = F(\boldsymbol{s}_2, \boldsymbol{h}')$ *has no solution in* $\boldsymbol{h}' \in \mathbb{C}^m$.

Proof. One direction follows immediately from Theorem 15. To prove the other direction, for fixed $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$, define $g_1(\boldsymbol{h}) = F(\boldsymbol{s}_1, \boldsymbol{h})$ and $g_2(\boldsymbol{h}) = F(\boldsymbol{s}_2, \boldsymbol{h})$. Assume there exists an $\boldsymbol{h}$ such that $g_1(\boldsymbol{h}) = g_2(\boldsymbol{h}')$ has no solution. Since $g_2(\mathbb{C}^m)$ is an affine space, it is closed. Therefore, there exists a neighbourhood X_1 of $\boldsymbol{h}$ such that $g_1(X_1)$ and $g_2(\mathbb{C}^m)$ are disjoint sets. In particular, such an X_1 satisfies (7) with $X_2 = \mathbb{C}^m$ and satisfies (8) with $X = X_1$, proving feasibility of source recovery. □

Remark 19. There is still a distinction between source recovery and strict source recovery in a system affine in its parameters. A system F can be con-

structed such that, in the proof of Theorem 18, $g_1(\mathbb{C}^m)$ is strictly contained in $g_2(\mathbb{C}^m)$. Source recovery but not strict source recovery would be possible.

Remark 20. The key ingredient in the proof of Theorem 18 is that, for any $\boldsymbol{s} \in \Omega$, the set $F(\boldsymbol{s}, \mathbb{C}^m)$ is known to be closed. This prevents the situation in Example 14 from arising. It also suggests that source recovery in complex projective space is more easily studied because the image of a homogeneous polynomial is always closed [2].

6. An application to wireless communications

For practical reasons, it is not uncommon for a wireless communications system to break the sequence of source symbols to be transmitted into blocks of fixed length and transmit a single block at a time, with guard intervals inserted between blocks [12,15]. This section proves the novel result that the presence of guard intervals allows the source symbols to be recovered given only a single received block.

For consistency with the digital communications literature [13], the system model is first described in matrix form. Later, a connection with systems theory is made. For a given channel vector $\boldsymbol{h} = [h_0, \ldots, h_{m-1}]^{\mathrm{T}} \in \mathbb{C}^m$, define the matrix $H \in \mathbb{C}^{n \times p}$ to be the lower triangular Toeplitz matrix having $[h_0, \ldots, h_{m-1}, 0, \ldots, 0]^{\mathrm{T}}$ as its first column; see Example 21. Define $F : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ as $F(\boldsymbol{s}, \boldsymbol{h}) = H\boldsymbol{s}$ where $\boldsymbol{s} \in \mathbb{C}^p$ and $n = p + m - 1$; the output block $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$ is the result of passing the source block $\boldsymbol{s}$, whose elements are the source symbols to be transmitted, through a convolutive channel with finite impulse response $\{h_0, \ldots, h_{m-1}\}$ modelling the wireless link. The structure of H accounts for the transmitted symbols being prefixed and suffixed by $m - 1$ consecutive zeros known as a guard interval [8,9]. The finite set $\Omega \subset \mathbb{C}^p$ is defined to be the set of all blocks of source symbols the digital communications system can transmit.

Example 21. An unrealistically small but otherwise representative example is the following. Let p=3, m= 2 and hence $n = p + m - 1 = 4$. Element-wise, $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h}) = H\boldsymbol{s}$ is given by $y_1 = h_0 s_1$, $y_2 = h_0 s_2 + h_1 s_1$, $y_3 = h_0 s_3 + h_1 s_2$ and $y_4 = h_1 s_3$; by convention, elements of $\boldsymbol{h}$ are indexed from zero. If Quadrature Amplitude Modulation is used then each element of $\boldsymbol{s}$ lies in the set $\{e^{j\pi/4}, e^{j3\pi/4}, e^{j5\pi/4}, e^{j7\pi/4}\}$. Thus, Ω is the set of all $4^p = 64$ permutations. (If channel coding is used then Ω is chosen instead to be the set of all possible codewords.)

An alternative interpretation is obtained by taking the z-transform of $\boldsymbol{y} = F(\boldsymbol{s}, \boldsymbol{h})$. Specifically, if $y(z) = \sum_{k=1}^{n} y_k z^{k-1}$ and similarly for $h(z)$ and $s(z)$, then $y(z) = h(z)s(z)$. In other words, the effect of the guard intervals is to make the communication system mimic an input/output system on a *per-block basis*.

Remark 22. Since $F(\lambda \boldsymbol{s}, \lambda^{-1} h) = F(\boldsymbol{s}, \boldsymbol{h})$ for any non-zero $\lambda \in \mathbb{C}$, a necessary condition for source recovery is that $\boldsymbol{s} \in \Omega$ implies $\lambda \boldsymbol{s} \notin \Omega$ for any $\lambda \neq 0, 1$.

Theorem 23. *Define $F(\boldsymbol{s}, \boldsymbol{h}) = H\boldsymbol{s}$ as above and let $\Omega \subset \mathbb{C}^p$ be any finite set satisfying the scale condition in Remark* 22. *Source recovery is feasible. Moreover, if $[0, \ldots, 0]^{\mathrm{T}} \notin \Omega$ then strict source recovery is feasible.*

Proof. Since F is bilinear, it suffices to verify the conditions in Theorem 18. Let $\boldsymbol{s}_1, \boldsymbol{s}_2 \in \Omega$ be distinct points and assume $[0, \ldots, 0]^{\mathrm{T}} \notin \Omega$, so that $\boldsymbol{s}_1(z) \not\equiv 0$ and $\boldsymbol{s}_2(z) \not\equiv 0$. As previously explained, the equation $F(\boldsymbol{s}_1, \boldsymbol{h}) = F(\boldsymbol{s}_2, \boldsymbol{h}')$ can be written as $s_1(z)h(z) = s_2(z)h'(z)$ where $h(z)$ and $h'(z)$ have degree at most $m - 1$. Choose $h(z)$ to be a polynomial of degree $m - 1$ coprime to $s_2(z)$; such a choice always exists. It is shown $s_1(z)h(z) = s_2(z)h'(z)$ has no solution in $h'(z)$. Indeed, if it did, $h(z)$ must divide $h'(z)$, but since the degree of $h'(z)$ is at most $m - 1$, this implies $h'(z) = \lambda h(z)$ for some non-zero $\lambda \in \mathbb{C}$ and thus $s_1(t) = \lambda s_2(t)$, contradicting the scale condition on Ω. Hence, strict source recovery is feasible by Theorem 18. An analogous argument proves source recovery is feasible even if $[0, \ldots, 0]^{\mathrm{T}} \in \Omega$. □

Remark 24. In communication systems, the set Ω may not satisfy the scale condition in Remark 22. In such cases, a straightforward extension of Theorem 23 shows the source vector $\boldsymbol{s}$ can be always recovered up to an unknown scaling factor. This is often sufficient in practice; either differential coding or a pilot symbol can be used to overcome scale ambiguity [13].

7. Conclusion

This paper considered the problem of recovering the source vector from the output vector of a parameterised polynomial system without knowledge of the parameter vector but with knowledge that the source vector belongs to a finite set of candidates. The problem was studied from several aspects ranging from theoretical considerations, namely the decidability and implementability of the problem, to more applied considerations, such as how to prove source recovery is feasible in any particular system. A specific example to an important problem in wireless communications was given; it was proved that source recovery is always possible in digital communication systems using guard intervals.

Acknowledgements

The author thanks Professors Iven Mareels and Walter Neumann for discussions inspiring this paper. The author also thanks Professor Uwe Helmke for critical comments on an earlier draft.

References

[1] T. Becker, V. Weispfenning, Grobner Bases: A Computational Approach to Commutative Algebra, Springer, Berlin, 1993.

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

[3] G.-M. Greuel, G. Pfister, H. Schönemann, Singular version 1.2 User Manual, Reports On Computer Algebra, 21, Centre for Computer Algebra, University of Kaiserslautern, June 1998. http://www.mathematik.uni-kl.de/~zca/Singular

[4] F. Gustafsson, B. Wahlberg, Blind equalization by direct examination of the input sequences, IEEE Trans. Comm. 43 (7) (1995) 2213–2222.

[5] J. Harris, Algebraic Geometry: A First Course, Springer, Berlin, 1992.

[6] R. Hartshorne, Algebraic Geometry, Springer, Berlin, 1977.

[7] S. Haykin (Ed.), Blind Deconvolution, Prentice-Hall, Englewood Cliffs, NJ, 1994.

[8] J.H. Manton, Dissecting OFDM: the independent roles of the cyclic prefix and the IDFT operation, IEEE Comm. Lett. 5 (12) (2001) 474–476.

[9] J.H. Manton, An OFDM interpretation of zero padded block transmissions, Systems Control Lett., to appear.

[10] J.H. Manton, J.R.J. Groves, Y. Hua, On properties of the solutions of systems of polynomial equations, in: The Third Asian Control Conference, Shanghai, China, July 2000.

[11] J.H. Manton, W.D. Neumann, P.T. Norbury, On the algebraic identifiability of finite impulse response channels driven by linearly precoded signals, Systems Control Lett. 2001, submitted for publication.

[12] A. Peled, A. Ruiz, Frequency domain data transmission using reduced computational complexity algorithms, in: Proceedings of the International Conference on Acoustics, Speech and Signal Processing, 1980, pp. 964–967.

[13] J.G. Proakis, Digital Communications, 3rd Edition, McGraw-Hill, New York, 1995.

[14] W. Rudin, Real and Complex Analysis, McGraw-Hill, New York, 1987.

[15] A. Ruiz, J.M. Cioffi, S. Kasturia, Discrete multiple tone modulation with coset coding for the spectrally shaped channel, IEEE Trans. Comm. 40 (1992) 1012–1019.

[16] A. van der Veen, S. Talwar, A. Paulraj, A subspace approach to blind space-time signal processing for wireless communication systems, IEEE Trans. Signal Process. 45 (1) (1997) 173–190.