Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Systems & Control Letters 48 (2003) 113–119

SYSTEMS & CONTROL LETTERS

www.elsevier.com/locate/sysconle

Totally blind channel identification by exploiting guard intervals[☆]

Jonathan H. Manton[a,*], Walter D. Neumann[b]

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

[b] Department of Mathematics, Barnard College, Columbia University, New York, NY 10027, USA

Received 28 November 2001; accepted 3 September 2002

Abstract

Blind identification techniques estimate the impulse response of a channel by exploiting known finite alphabet or statistical properties of the transmitted symbols. Alternatively, oversampling the output is known to introduce dependencies also exploitable for channel identification. This paper proves the feasibility of estimating the channel by relying instead on the short sequences of zeros, known as guard intervals or zero padding, introduced between transmitted blocks by a number of communication protocols. Since no property of the transmitted information symbols is assumed, the method is called totally blind channel identification. It is proved that totally blind channel identification requires only two received blocks to estimate the channel.

Keywords: Partially coupled polynomial equations; Invertibility of polynomial equations; Polynomial systems; Algebraic channel identification; Wireless communications; Communication systems

1. Introduction

Estimating the impulse response of the channel over which a communication system operates is complicated by the source symbols being a-priori unknown to the receiver. Blind channel identification techniques [1,3,4,6,7,17,21,24,25] have been applied extensively to this problem. Blind techniques must exploit a known property of the transmitted signal, such as a statistical or finite alphabet property or a bandwidth constraint if the technique requires the received signal to be over-sampled. This paper presents a different approach; it makes no assumptions on the source symbols themselves but rather relies on the communication system introducing a guard interval between each transmitted block. It is proved that the channel is identifiable (up to an inherent scaling factor) from just two received blocks. This complements the recent result that one block suffices if finite alphabet properties of the source symbols in addition to guard intervals are exploited [9].

The main result of this paper is captured in the following unrealistically small but otherwise representative example of a communication system using guard intervals.

[☆] This work was undertaken in part while the first author was visiting ENST/TSI in Paris, France.

[*] Corresponding author. Tel.: +61383446791; fax: +61383-446678.

E-mail address: jon@ee.mu.oz.au (J.H. Manton).

0167-6911/03/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0167-6911(02)00278-5

Example 1. Assume the source symbols $1,2,3,4$ are broken into two blocks and guard intervals inserted, forming the transmitted signal $0,1,2,0,3,4,0$. Let $\boldsymbol{h}=[h_0,h_1]^{\mathrm{T}}\in\mathbb{C}^2$ with $h_0=1$ and $h_1=-1$ denote the impulse response of the channel. The receiver sees the transmitted signal convolved with the channel impulse response, namely $1,1,-2,3,1,-4$. More generally, if s_1,s_2,s_3,s_4 denote the source symbols then the received symbols are $y_1=h_0s_1,\ y_2=h_0s_2+h_1s_1,\ y_3=h_1s_2,\ y_4=h_0s_3,\ y_5=h_0s_4+h_1s_3$ and $y_6=h_1s_4$. The proposed idea is to invert this set of polynomial equations, thus identifying the channel. If $y_1=y_2=1$ and $y_3=-2$ then the first three equations reduce to $2h_0^2+h_0h_1-h_1^2=0$. Assume $h_0\neq 0$ and set $\lambda=h_1/h_0$. The equation becomes $h_0^2(2+\lambda-\lambda^2)=0$ with solutions $\lambda=-1,2$. Note that $\lambda=-1$ is indeed the ratio h_1/h_0 of the impulse response used to generate the output $1,1,-2$. Repeating the process with the second block, namely $y_4=3,\ y_5=1$ and $y_6=-4$, yields the two solutions $\lambda=-1,\frac{4}{3}$. In particular, the only solution in common is $\lambda=-1$. The ratio h_1/h_0 of the channel impulse response has been recovered without knowledge of the source symbols.

Three observations are made. The channel is recoverable only up to a scaling factor because the equations in Example 1 are bilinear; if the source symbols are doubled and the impulse response halved, the output remains the same. A single received block does not provide enough information to identify the channel but it narrows the possibilities down to a finite number. Two blocks suffice to recover the channel. The main result of this paper is that these three observations generalise to arbitrarily sized communication systems and even remain true if additive noise is present.

Since the proposed identification technique relies on guard intervals, a brief discussion on guard intervals ensues. Guard intervals, also known as null guards or zero padding, are sequences of $L-1$ consecutive zeros inserted between blocks to prevent inter-block interference [2,16,19,26]. Here, L is an upper bound on the length of the channel over which the system operates and inter-block interference refers to the problem of the kth output block depending not only on the kth transmitted block but also on the $(k-1)$th transmitted block due to the memory of the channel. A sequence of $L-1$ zeros empties the memory of the channel and thus prevents inter-block interference. These guard intervals are often used in time division multiple access (TDMA) systems, such as the current GSM standard for mobile telephones. They can also be used in orthogonal frequency division multiplexing (OFDM) systems [18–20]. Although originally there to prevent inter-block interference, it is now known that guard intervals have additional advantages, such as always allowing the source symbols to be recovered if the channel is known (and non-zero) and ensuring that channel deconvolution is always a stable operation [8,12]; see also [11]. The present paper presents yet another advantage of guard intervals; they enable the receiver to identify the channel without any knowledge of the source symbols whatsoever. Note that the parameter L must be known a-priori to both the transmitter and the receiver.

The remainder of this paper is organised as follows. Section 2 defines two types of channel identifiability, one related to the noise free case and the other to when the received signal is corrupted by additive noise. It also states the result from [15] that not only are both definitions equivalent, but that channel identification is possible if and only if a related polynomial map is rationally invertible. Determining if a polynomial map is rationally invertible is difficult in general. However, Section 3 shows this task simplifies if a certain repeated structure is present. Section 4 then applies this result to prove that if guard intervals are inserted between transmitted blocks, the receiver can identify the channel using just two received blocks. Section 4 remarks that the main ideas in this paper extend to proving identifiability of a wider class of linearly and affinely precoded communication systems. Section 5 concludes the paper.

2. Problem statement and known results

In a communication system operating over a channel of length at most L and with guard intervals of length $L-1$ inserted between blocks, the kth block of p source symbols $\boldsymbol{s}_k\in\mathbb{C}^p$ is received as

$$\boldsymbol{y}_k=H\boldsymbol{s}_k,\qquad \boldsymbol{y}_k\in\mathbb{C}^{p+L-1},\tag{1}$$

where $H\in\mathbb{C}^{(p+L-1)\times p}$ is the lower triangular Toeplitz matrix having $[h_0,\ldots,h_{L-1},0,\ldots,0]^{\mathrm{T}}$, the impulse response of the channel padded with p zeros, as its first column. Since the impulse response $\boldsymbol{h}=[h_0,\ldots,h_{L-1}]^{\mathrm{T}}\in\mathbb{C}^L$ is unknown, it is appropriate to write (1) in the form of a polynomial equation, namely

$$\boldsymbol{y}_k = F(\boldsymbol{s}_k,\boldsymbol{h}), \quad F:\mathbb{C}^p\times\mathbb{C}^L\to\mathbb{C}^{p+L-1}. \tag{2}$$

From Example 1, which corresponds to the case $p=2$ and $L=2$, it is seen that (1) is nothing more than the convolution of the source symbols with the channel impulse response and where the guard intervals consisting of $L-1$ consecutive zeros on either side of $\boldsymbol{s}_k$ are accounted for in the definition of H.

The augmentation of K blocks is denoted

$$\boldsymbol{y}^{[K]} = F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h}),$$
$$F^{[K]}:\mathbb{C}^{pK}\times\mathbb{C}^L\to\mathbb{C}^{(p+L-1)K} \tag{3}$$

where $\boldsymbol{y}^{[K]}=[\boldsymbol{y}_1^{\mathrm{T}},\ldots,\boldsymbol{y}_K^{\mathrm{T}}]^{\mathrm{T}}$ and $\boldsymbol{s}^{[K]}=[\boldsymbol{s}_1^{\mathrm{T}},\ldots,\boldsymbol{s}_K^{\mathrm{T}}]^{\mathrm{T}}$.

For any non-zero $\lambda\in\mathbb{C}$, $F^{[K]}(\lambda\boldsymbol{s}^{[K]},\lambda^{-1}\boldsymbol{h}) = F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h})$. Thus, at best, the channel $\boldsymbol{h}$ is recoverable up to an unknown complex valued scaling factor. This motivates the following definition, some parts of which are justified below.

Definition 2 (Noise free identifiability). The system (2) is identifiable using K blocks if there exists a non-zero polynomial $g:\mathbb{C}^{pK}\times\mathbb{C}^L\to\mathbb{C}$ such that, for any $\boldsymbol{s}^{[K]}$ and $\boldsymbol{h}$ satisfying $g(\boldsymbol{s}^{[K]},\boldsymbol{h})\neq 0$,

$$\forall\tilde{\boldsymbol{s}}^{[K]}\in\mathbb{C}^{pK},\ \forall\tilde{\boldsymbol{h}}\in\mathbb{C}^L,$$
$$F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h}) = F^{[K]}(\tilde{\boldsymbol{s}}^{[K]},\tilde{\boldsymbol{h}}) \text{ implies } \exists\lambda\in\mathbb{C},\ \lambda\neq 0,$$
$$\tilde{\boldsymbol{s}}^{[K]}=\lambda\boldsymbol{s}^{[K]},\ \ \tilde{\boldsymbol{h}}=\lambda^{-1}\boldsymbol{h}. \tag{4}$$

A condition such as $g(\boldsymbol{s}^{[K]},\boldsymbol{h})\neq 0$ in Definition 2 is clearly necessary; if either $\boldsymbol{h}=0$ or $\boldsymbol{s}^{[K]}=0$ then $\boldsymbol{y}^{[K]}=0$ and the channel is unidentifiable. The specific condition $g(\boldsymbol{s}^{[K]},\boldsymbol{h})\neq 0$ is the natural one to use in Definition 2 because it is proved in [15] that there exists a non-zero polynomial g such that the number of non-equivalent elements in the set $\{(\tilde{\boldsymbol{s}}^{[K]},\tilde{\boldsymbol{h}}): F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h})=F^{[K]}(\tilde{\boldsymbol{s}}^{[K]},\tilde{\boldsymbol{h}})\}$, where the elements $(\boldsymbol{s}_1^{[K]},\boldsymbol{h}_1),(\boldsymbol{s}_2^{[K]},\boldsymbol{h}_2)$ are equivalent if there exists a non-zero λ such that $(\boldsymbol{s}_1^{[K]},\boldsymbol{h}_1)=(\lambda\boldsymbol{s}_2^{[K]},\lambda^{-1}\boldsymbol{h}_2)$, is the same for any $(\boldsymbol{s}^{[K]},\boldsymbol{h})$ satisfying $g(\boldsymbol{s}^{[K]},\boldsymbol{h})\neq 0$. Thus, Definition 2 states that the channel is identifiable if and only if this number is unity.

The condition (4) requires not only that the channel can be identified, but that the transmitted source symbols $\boldsymbol{s}^{[K]}$ can be determined too. In fact, this condition is equivalent to the weaker condition of only requiring channel identifiability because once the channel is known, the transmitted source symbols can almost always be determined, a consequence of H in (1) having full column rank for all $\boldsymbol{h}\neq 0$.

If additive noise $\boldsymbol{n}^{[K]}$ is present, (3) can be inverted in the least-squares sense by finding a pair $(\tilde{\boldsymbol{s}}^{[K]},\tilde{\boldsymbol{h}})$ which minimises the Euclidean norm

$$\|F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h})+\boldsymbol{n}^{[K]}-F^{[K]}(\tilde{\boldsymbol{s}}^{[K]},\tilde{\boldsymbol{h}})\|^2, \tag{5}$$

where $F^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h})+\boldsymbol{n}^{[K]}$ is the noise corrupted received signal. (An algorithm for doing so appears in [10].) The channel is said to be identifiable if the global minimum is unique up to scale for most noise realisations $\boldsymbol{n}^{[K]}$. Definition 3 formalises this.

Definition 3 (Identifiability in noise). Let $\boldsymbol{n}^{[K]}\in\mathbb{C}^{(p+L-1)K}$ be a random vector whose probability measure is absolutely continuous with respect to Lebesgue measure. For any triple $\boldsymbol{s}^{[K]},\boldsymbol{h},\boldsymbol{n}^{[K]}$, define $\Theta_{\boldsymbol{s}^{[K]},\boldsymbol{h},\boldsymbol{n}^{[K]}}$ to be the set of all global minima of (5). The system (2) corrupted by additive noise $\boldsymbol{n}^{[K]}$ is identifiable using K blocks if there exists a non-zero polynomial $g:\mathbb{C}^{pK}\times\mathbb{C}^L\to\mathbb{C}$ such that, for any $\boldsymbol{s}^{[K]}$ and $\boldsymbol{h}$ satisfying $g(\boldsymbol{s}^{[K]},\boldsymbol{h})\neq 0$,

$$(\boldsymbol{s}_1^{[K]},\boldsymbol{h}_1),(\boldsymbol{s}_2^{[K]},\boldsymbol{h}_2)\in\Theta_{\boldsymbol{s}^{[K]},\boldsymbol{h},\boldsymbol{n}^{[K]}} \text{ implies } \exists\lambda\in\mathbb{C},$$
$$\lambda\neq 0,\ \ \boldsymbol{s}_1^{[K]}=\lambda\boldsymbol{s}_2^{[K]},\ \ \boldsymbol{h}_1=\lambda^{-1}\boldsymbol{h}_2 \tag{6}$$

holds almost surely.

One of the main results in [15] states not only that Definitions 2 and 3 are equivalent, but that the channel is identifiable if and only if $F^{[K]}$ is invertible *with the prior knowledge that* $h_0=1$ *in* (1). (This is tantamount to assuming $h_0\neq 0$ in Example 1.) Theorem 4 makes this precise. It requires the function $G^{[K]}$ defined analogously to $F^{[K]}$ in (3) but with h_0 fixed to unity. Specifically,

$$G^{[K]}(\boldsymbol{s}^{[K]},\boldsymbol{h}) = F^{[K]}(\boldsymbol{s}^{[K]},[1\quad \boldsymbol{h}^{\mathrm{T}}]^{\mathrm{T}}),$$
$$G^{[K]}:\mathbb{C}^{pK}\times\mathbb{C}^{L-1}\to\mathbb{C}^{(p+L-1)K} \tag{7}$$

where the entry h_0 is omitted from $\boldsymbol{h}=[h_1,\ldots,h_{L-1}]^{\mathrm{T}}$.

Theorem 4. *The system* (2) *is identifiable using* K *blocks*, *either in the sense of Definition* 2 *or* 3, *if and only if the polynomial map* $G^{[K]}$, *defined in* (7), *is rationally invertible* (*see below*).

A polynomial map G is rationally invertible if there exists a rational map F such that the composition $F \circ G$ is the identity map whenever it is well-defined [5]. An equivalent definition is that the equation $G(\tilde{z}) = G(z)$ has just the one solution $\tilde{z} = z$ for almost all z; see Appendix A.

3. Partially coupled polynomial equations

Proving invertibility of a polynomial map is difficult in general [15,22,23]. This section derives a necessary and sufficient condition for an augmented map of the form found in Theorem 4 to be rationally invertible.

Throughout this section, $G : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ denotes a full rank polynomial map; see Appendix A for the meaning of full rank. As in Section 2, the notation $G^{[2]}$ denotes the augmented map $G^{[2]} : \mathbb{C}^{2p} \times \mathbb{C}^m \to \mathbb{C}^{2n}$ defined by $G^{[2]}((\boldsymbol{s}_1, \boldsymbol{s}_2), \boldsymbol{h}) = (G(\boldsymbol{s}_1, \boldsymbol{h}), G(\boldsymbol{s}_2, \boldsymbol{h}))$. Theorem 8, the main result of this section, shows that $G^{[2]}$ is rationally invertible unless G has a certain property that is relatively easy to detect in practice.

Definition 5 (Strongly unidentifiable). The parameter $\boldsymbol{h} \in \mathbb{C}^m$ is strongly unidentifiable with respect to G if

$$\exists \tilde{\boldsymbol{h}} \in \mathbb{C}^m,\ \exists \text{ open dense } X \subset \mathbb{C}^p,\ \forall \boldsymbol{s} \in X,\ \exists \tilde{\boldsymbol{s}} \in \mathbb{C}^p \\ \text{such that } G(\boldsymbol{s}, \boldsymbol{h}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}) \text{ and} \\ (\boldsymbol{s}, \boldsymbol{h}) \neq (\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}). \tag{8}$$

The motivation for Definition 5 is that if the pair $\boldsymbol{h}, \tilde{\boldsymbol{h}}$ satisfies (8) then for almost any $\boldsymbol{s}_1, \boldsymbol{s}_2$, the equation $G^{[2]}((\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2), \tilde{\boldsymbol{h}}) = G^{[2]}((\boldsymbol{s}_1, \boldsymbol{s}_2), \boldsymbol{h})$ has a solution $((\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2), \tilde{\boldsymbol{h}})$ distinct from $((\boldsymbol{s}_1, \boldsymbol{s}_2), \boldsymbol{h})$.

Lemma 6. *The parameter* $h \in \mathbb{C}^m$ *is strongly unidentifiable with respect to* G *if*

$$\exists \tilde{\boldsymbol{h}} \in \mathbb{C}^m,\ \exists \text{ open } B \subset \mathbb{C}^p,\ \forall \boldsymbol{s} \in B,\ \exists \tilde{\boldsymbol{s}} \in \mathbb{C}^p \\ \text{such that } G(\boldsymbol{s}, \boldsymbol{h}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}) \\ \text{and } (\boldsymbol{s}, \boldsymbol{h}) \neq (\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}). \tag{9}$$

Proof. Define the polynomial maps $G_1(\boldsymbol{s}) = G(\boldsymbol{s}, \boldsymbol{h})$ and $G_2(\tilde{\boldsymbol{s}}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$. If $\boldsymbol{h} = \tilde{\boldsymbol{h}}$ then $G_1 \equiv G_2$ and (9) combined with Part 1 of Theorem A.1 in Appendix A implies $G_1(\tilde{\boldsymbol{s}}) = G_1(\boldsymbol{s})$ generically has two or more solutions and thus (8) holds. If G_1 does not have full rank then Part 2 of Theorem A.1 implies G_1 generically has an infinite number of solutions and thus (8) holds with the choice $\tilde{\boldsymbol{h}} = \boldsymbol{h}$. Assume then that $\boldsymbol{h} \neq \tilde{\boldsymbol{h}}$ and G_1 has full rank. For $i = 1, 2$, define the image $V_i = G_i(\mathbb{C}^p)$ and note that its closure $\bar{V}_i$ is an irreducible variety and that $W_i = \overline{\bar{V}_i - V_i}$ is a variety nowhere dense in $\bar{V}_i$ [5]. Moreover, $\dim \bar{V}_1 = p$ because G_1 has full rank while $\dim \bar{V}_2 \leqslant p$ [5]. There are two cases, either $\bar{V}_1 \cap \bar{V}_2 = \bar{V}_1$ or $\bar{V}_1 \cap \bar{V}_2 \subsetneq \bar{V}_1$. Since $\bar{V}_1, \bar{V}_2$ are irreducible varieties satisfying $\dim \bar{V}_2 \leqslant \dim \bar{V}_1$, the first case implies $\bar{V}_1 = \bar{V}_2$ while the second case implies $\bar{V}_1 \cap \bar{V}_2$ is nowhere dense in $\bar{V}_1$, in turn implying $G_1^{-1}(\bar{V}_2)$ is nowhere dense in $\mathbb{C}^P$ and contradicting (9) because B is an open set contained in $G_1^{-1}(\bar{V}_2)$. Thus, $\bar{V}_1 = \bar{V}_2$, and in particular, W_2 is a nowhere dense variety in $\bar{V}_1$, implying $X = G_1^{-1}(W_2^{\mathrm{c}})$ is an open dense set satisfying (8), where c denotes set complement. □

Definition 7 (Dyslexic). The map $G : \mathbb{C}^p \times \mathbb{C}^m \to \mathbb{C}^n$ is dyslexic if

$$\exists \text{ open dense } Y \subset \mathbb{C}^m,\ \forall \boldsymbol{h} \in Y,\ (8) \text{ holds}. \tag{10}$$

Theorem 8. *Let* G *have full rank. The augmented map* $G^{[2]}$ *is rationally invertible if and only if* G *is not dyslexic.*

Proof. Since G has full rank by assumption, $G^{[2]}$ also has full rank. Define the set Z such that $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h}) \in Z$ if and only if $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h})$ is a generic point of $G^{[2]}$ and $(\boldsymbol{s}_1, \boldsymbol{h})$ and $(\boldsymbol{s}_2, \boldsymbol{h})$ are generic points of G; since generic points form an open dense set (see Theorem A.1 in Appendix A), it follows that Z itself is open and dense. To prove one direction, assume $G^{[2]}$ is rationally invertible yet G is dyslexic. Let $B_1, B_2 \subset \mathbb{C}^p$ and $B_3 \subset \mathbb{C}^m$ be open sets such that $B_1 \times B_2 \times B_3 \subset Z$. Define Y as in (10) and choose any point $\boldsymbol{h} \in Y \cap B_3$. Define $\tilde{\boldsymbol{h}}$ and X as in (8). Choose any two points $\boldsymbol{s}_1 \in B_1 \cap X$ and $\boldsymbol{s}_2 \in B_2 \cap X$. Then, from (8), there exist points $\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2$ such that $G^{[2]}(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h}) = G^{[2]}(\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}})$ and $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h}) \neq (\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}})$, contradicting the fact that since $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h})$ is a generic point of

$G^{[2]}$, $G^{[2]}(\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}}) = G^{[2]}(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h})$ should have only the one solution $(\tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}}) = (\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h})$.

To prove the other direction, assume $G^{[2]}$ is not rationally invertible. Define Y to be the projection of Z onto the $\boldsymbol{h}$-coordinate. Note that Y so defined is open and dense. It will be shown that this choice of Y satisfies (10). Pick any point $\boldsymbol{h} \in Y$ and choose $(\boldsymbol{s}_1, \boldsymbol{s}_2)$ such that $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h}) \in Z$. Part 3 of Theorem A.1 implies there exists a diffeomorphism $f: N \to \tilde{N}$, where $N, \tilde{N} \subset Z$ are disjoint open sets with $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h}) \in N$, such that $G^{[2]}(p) = G^{[2]}(f(p))$ for any $p \in N$. Define $(\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}}) = f(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{h})$. By swapping $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ if necessary, it can be assumed that $(\boldsymbol{s}_1, \boldsymbol{h}) \neq (\tilde{\boldsymbol{s}}_1, \tilde{\boldsymbol{h}})$. Since $G^{-1}(G(\boldsymbol{s}_2, \boldsymbol{h}))$ contains a finite number of elements, with $(\tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}})$ one of them, it can be assumed, by decreasing the sizes of N and $\tilde{N}$ if necessary, that $(\tilde{\boldsymbol{s}}_1', \tilde{\boldsymbol{s}}_2', \tilde{\boldsymbol{h}}') \in \tilde{N}$ with $G(\tilde{\boldsymbol{s}}_2', \tilde{\boldsymbol{h}}') = G(\boldsymbol{s}_2, \boldsymbol{h})$ implies $(\tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}}') = (\tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}})$. Let B be any open set satisfying $B \times \{\boldsymbol{s}_2\} \times \{\boldsymbol{h}\} \subset N$. For any $\boldsymbol{s} \in B$, define $(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{s}}_2', \tilde{\boldsymbol{h}}') = f(\boldsymbol{s}, \boldsymbol{s}_2, \boldsymbol{h})$. This implies $G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}') = G(\boldsymbol{s}, \boldsymbol{h})$ and $G(\tilde{\boldsymbol{s}}_2', \tilde{\boldsymbol{h}}') = G(\boldsymbol{s}_2, \boldsymbol{h})$. From above, the latter implies $(\tilde{\boldsymbol{s}}_2', \tilde{\boldsymbol{h}}') = (\tilde{\boldsymbol{s}}_2, \tilde{\boldsymbol{h}})$ Thus, $G(\boldsymbol{s}, \boldsymbol{h}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$. Moreover, by choosing B to be a sufficiently small neighbourhood of $\boldsymbol{s}_1$, it can be assumed that $(\boldsymbol{s}, \boldsymbol{h}) \neq (\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$. Hence, Lemma 6 implies (8) holds, as required. □

Corollary 9. *Provided G has full rank, the map $G^{[2]}$ is rationally invertible if and only if*

$$\begin{aligned} &\exists \text{ open } Y \subset \mathbb{C}^m,\ \forall \boldsymbol{h} \in Y,\ \forall \tilde{\boldsymbol{h}} \in \mathbb{C}^m, \\ &\quad \exists \text{ open } B \subset \mathbb{C}^p,\ \forall \boldsymbol{s} \in B,\ \forall \tilde{\boldsymbol{s}} \in \mathbb{C}^p, \\ &\quad G(\boldsymbol{s}, \boldsymbol{h}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}) \text{ implies } (\boldsymbol{s}, \boldsymbol{h}) = (\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}}). \end{aligned} \tag{11}$$

Proof. It is readily seen that if (11) holds then G is not dyslexic and vice versa. □

4. Totally blind channel identification

This section uses Theorem 4 and Corollary 9 to prove the system (2) is identifiable using just two blocks.

Lemma 10. *For any $p \geqslant 1$ and $L \geqslant 1$, let $H, \tilde{H} \in \mathbb{C}^{(p+L-1)\times p}$ be lower triangular Toeplitz matrices whose first column ends in $p-1$ zeros. The range space of H is contained in the range space of $\tilde{H}$ if and only if $H = \lambda \tilde{H}$ for some $\lambda \in \mathbb{C}$.*

Proof. A straightforward proof by induction is possible. Alternatively, a z-domain argument can be used, as in [9, Proof of Theorem 23]. □

Theorem 11. *For any $p \geqslant 1$ and $L \geqslant 2$, the system (2) is identifiable, according to both Definitions 2 and 3, using two blocks. Moreover, it is identifiable using just one block if and only if $p = 1$.*

Proof. Define G and $G^{[2]}$ as in (7) with $K = 1$ and 2, respectively. From Theorem 4, it suffices to prove G is not rationally invertible unless $p = 1$ whereas $G^{[2]}$ is always rationally invertible. If $p = 1$, direct expansion of $G(\boldsymbol{s}, \boldsymbol{h}) = G(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$ shows that G, and hence $G^{[2]}$ too, is rationally invertible. Henceforth, assume $p > 1$. That G has full rank but is not rationally invertible follows from the observation that the points $(\boldsymbol{s}, \boldsymbol{h})$ and $(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$, defined by $\boldsymbol{s} = [0, \ldots, 0, 1, 0, \ldots, 0, 1]^{\mathrm{T}}$, $\boldsymbol{h} = [0, \ldots, 0]^{\mathrm{T}}$, $\tilde{\boldsymbol{s}} = [0, \ldots, 0, 1, 0, \ldots, 0]^{\mathrm{T}}$ and $\tilde{\boldsymbol{h}} = [0, \ldots, 0, 1]^{\mathrm{T}}$ where the middle 1 in both $\boldsymbol{s}$ and $\tilde{\boldsymbol{s}}$ is in the $(p-L+1)$th position, satisfy the requirements in Theorem A.3 in Appendix A; note that the Jacobian matrix at $(\boldsymbol{s}, \boldsymbol{h})$ is upper triangular with ones along the diagonal while interchanging several rows of the Jacobian matrix at $(\tilde{\boldsymbol{s}}, \tilde{\boldsymbol{h}})$ makes it lower triangular with ones along the diagonal. Finally, to prove $G^{[2]}$ is rationally invertible, it is shown that (11) holds with the choice $Y = \mathbb{C}^{L-1}$. To this end, let $\boldsymbol{h}, \tilde{\boldsymbol{h}} \in \mathbb{C}^{L-1}$ be any pair of vectors and define the matrices H and $\tilde{H}$ such that $G(\boldsymbol{s}, \boldsymbol{h}) = H\boldsymbol{s}$ and similarly for $\tilde{H}$; see Section 2. Note that since $h_0 = 1$ in (7), H always has full rank, and moreover, $H = \lambda \tilde{H}$ for some $\lambda \in \mathbb{C}$ if and only if $H = \tilde{H}$. If $\boldsymbol{h} = \tilde{\boldsymbol{h}}$ then $H\boldsymbol{s} = H\tilde{\boldsymbol{s}}$ implies $\boldsymbol{s} = \tilde{\boldsymbol{s}}$ because H has full column rank and hence (11) is satisfied. If $\boldsymbol{h} \neq \tilde{\boldsymbol{h}}$ then Lemma 10 implies the range space of H is not contained in the range space of $\tilde{H}$. Thus, there exists an open set B such that $\boldsymbol{s} \in B$ implies $H\boldsymbol{s}$ is not in the range space of $\tilde{H}$, and in particular, that (11) holds with this choice of B, completing the proof. □

Remark 12. Corollary 9 facilitates identifiability proofs for more general linearly precoded communication systems studied in [15]. Indeed, if $G(\boldsymbol{s}, \boldsymbol{h}) = HP\boldsymbol{s}$ for some channel matrix H and precoder matrix P,

(11) is satisfied whenever there exists a channel matrix H such that HP has full column rank and the range space of HP is not contained in the range space of $\tilde{H}P$ for any other channel matrix $\tilde{H} \neq H$. As in Lemma 10, this is readily verified by showing there cannot exist a matrix S such that $HP = \tilde{H}PS$. Similarly, affine precoders [14] can also be studied using this framework.

5. Conclusion

Guard intervals are often inserted between transmitted blocks in a communication system to prevent inter-block interference. This paper proved that the repeated structure introduced by the guard intervals enables the receiver to identify the channel after receiving just two blocks by solving a system of polynomial equations. Moreover, it was remarked that the same method of proving identifiability extends to more general linearly and affinely precoded communication systems.

Acknowledgements

The first author would like to thank Prof. Philippe Loubaton for informative discussions on guard intervals in communication systems. The second author acknowledges support of the NSF.

Appendix A. Properties of polynomial equations

Standard properties of polynomial equations are summarised below. They are adapted from a similar summary in [15]. Despite the somewhat cumbersome statements of these results, Example A.2 below shows the essence of each result is readily understand.

Let $G:\mathbb{C}^m \to \mathbb{C}^n$ denote an arbitrary polynomial map. Its Jacobian matrix J has as its ijth element the derivative of the ith component of G with respect to its jth variable. Since the elements of J are polynomials, J has a well-defined rank as a matrix over the ring of polynomials. *The map G is said to have full rank if its Jacobian matrix J has full column rank.* To prove that G has full rank, it suffices to find a single point $z \in \mathbb{C}^m$ at which $J_z \in \mathbb{C}^{n\times m}$, the matrix obtained by evaluating the entries of J at the point z, has full column rank. (Note that J_z is simply the derivative of G at z.)

Theorem A.1. *Let $G:\mathbb{C}^m \to \mathbb{C}^n$ be a polynomial map. There exists a non-zero polynomial $g:\mathbb{C}^m \to \mathbb{C}$ and a unique number N with the following properties*: (1) *If $g(z) \neq 0$ then $G(\tilde{z}) = G(z)$ has precisely N solutions in $\tilde{z}$, and moreover, each of these solutions satisfies $g(\tilde{z}) \neq 0$.* (2) *The map G has full rank if and only if $N < \infty$.* (3) *If $2 \leqslant N < \infty$ and z_1 and z_2 are distinct points such that $G(z_1) = G(z_2)$* and *$g(z_1) \neq 0$ then there exists a diffeomorphism $f:N_1 \to N_2$ from an open neighbourhood $N_1 \subset \mathbb{C}^m$ of z_1 to an open neighbourhood $N_2 \subset \mathbb{C}^m$ of z_2 such that $z_2 = f(z_1)$ and $G(f(z)) = G(z)$ for any $z \in N_1$ both hold.* (*Clearly, N_1 and N_2 can be chosen to be disjoint sets and such that $g(z) \neq 0$ and $g(f(z)) \neq 0$ for any $z \in N_1$.*)

Referring to Theorem A.1, *the number N is called the generic number of solutions of G and a point z at which $g(z) \neq 0$ is called a generic point of G.* It is well-known [13] that *G is rationally invertible if and only if $N = 1$.*

Example A.2. Consider the map $G(z) = z^2$. Its 1 × 1 Jacobian matrix is $J = 2z$. It has full column rank since $2z$ is not the zero polynomial and hence G is said to have full rank. Moreover, observe that for almost all z (in particular, for $z \neq 0$), the matrix $J_z = 2z$ is non-zero and hence has full column rank. Part 1 of Theorem A.1 holds with the choice $g(z) = z$ and $N = 2$ because $\tilde{z}^2 = z^2$ has two solutions unless $z = 0$. The diffeomorphism $f(z) = -z$ satisfies part 2 of Theorem A.1 if N_1 is an open interval not containing the origin.

Although the map $G(x) = (x^2, x^3 - x)$ generically has one solution, $G(\tilde{x}) = G(x)$ has two solutions $\tilde{x} = -1, 1$ at the non-generic point $x = 1$. Theorem A.3 states this cannot happen if the number of equations equals the number of variables. (The Jacobian condition is necessary because a rationally invertible map may still have an infinite number of solutions at non-generic points.)

Theorem A.3. *Let $G:\mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If there exist distinct points $z, \tilde{z} \in \mathbb{C}^n$ such that*

$G(z) = G(\tilde{z})$ and both J_z and $J_{\tilde{z}}$ have full rank then G is not rationally invertible.

References

[1] K. Abed-Meraim, E. Moulines, P. Loubaton, Prediction error method for second-order blind identification, IEEE Trans. Signal Process. 45 (3) (1997) 694–705.

[2] S. Benedetto, E. Biglieri, V. Castellani, Digital Transmission Theory, Prentice-Hall, Englewood Cliffs, NJ, 1987.

[3] A. Benveniste, M. Goursat, G. Ruget, Robust identification of a non-minimum phase system: blind adjustment of a linear equalizer in data communication, IEEE Trans. Automatic Control 25 (3) (1980) 385–399.

[4] J.A. Cadzow, Blind deconvolution via cumulant extrema, IEEE Signal Process. Mag. 13 (3) (1996) 24–42.

[5] 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.

[6] C.R. Johnson, Admissibility in blind adaptive channel equalization, IEEE Control System Magazine (January 1991), 3–15.

[7] H. Liu, G. Xu, L. Tong, T. Kailath, Recent developments in blind channel equalization: from cyclostationarity to subspaces, Signal Process. 50 (1996) 83–99.

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

[9] J.H. Manton, Finite alphabet source recovery in polynomial systems, Systems Control Lett. (2002), accepted.

[10] J.H. Manton, An improved least squares blind channel identification algorithm for linearly and affinely precoded communication systems, IEEE Signal Process. Lett. 47 (5) (2002) 393–399.

[11] J.H. Manton, An OFDM interpretation of zero padded block transmissions, Systems Control Lett. (2002), accepted.

[12] J.H. Manton, On the importance of using a cyclic prefix or null guard in block transmissions over FIR channels, in: Information, Decision and Control, Adelaide, Australia, February 2002.

[13] 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.

[14] J.H. Manton, I.M.Y. Mareels, Y. Hua, Affine precoders for reliable communications, in: IEEE Conference on Acoustics, Speech and Signal Processing, Vol. V, Istanbul, Turkey, June 2000, pp. 2749–2752.

[15] 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., submitted.

[16] H. Meyr, M. Moeneclaey, S.A. Fechtel, Digital Communication Receivers: Synchronization, Channel Estimation, and Signal Processing, Wiley, Berlin, 1997.

[17] E. Moulines, P. Duhamel, J.-F. Cardoso, S. Mayrargue, Subspace methods for the blind identification of multichannel FIR filters, IEEE Trans. Signal Process. 43 (2) (1995) 516–525.

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

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

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

[21] O. Shalvi, E. Weinstein, New criteria for blind deconvolution of nonminimum phase systems (channels), IEEE Trans. Inform. Theory 36 (2) (1990) 312–321.

[22] E.D. Sontag, On the observability of polynomial systems, I: Finite-time problems, SIAM J. Control Optim. 17 (1) (1979) 139–151.

[23] E.D. Sontag, Y. Rouchaleau, On discrete-time polynomial systems, Nonlinear Analysis Theory Methods Appl. 1 (1976) 55–64.

[24] L. Tong, R.-W. Liu, V.C. Soon, Y.-F. Huang, Indeterminacy and identifiability of blind identification, IEEE Trans. Circuits Syst. 38 (5) (1991) 499–509.

[25] L. Tong, G. Xu, T. Kailath, Blind identification and equalization based on second-order statistics: a time domain approach, IEEE Trans. Inform. Theory 40 (2) (1994) 340–349.

[26] W.T. Webb, L. Hanzo, Modern Quadrature Amplitude Modulation: Principles and Applications for Fixed and Wireless Channels, IEEE Press, New York, 1994.