BLIND IDENTIFIABILITY ANALYSIS IN A MIMO LTI SYSTEM WITH INPUTS FROM A FINITE-ALPHABET SET

Soonman Kwon [*], **D. R. Fuhrmann** [**],
Seog-Joo Kim [*], **Jongmoo Lee** [*]

[*] *Korea Electrotechnology Research Institute*
Changwon, Gyungnam, 641-120 Korea
{smkwon, sjkim, jmlee}@keri.re.kr
[**] *Department of Electrical Engineering,*
Washington University, St. Louis, MO 63130, U.S.A.
danf@ee.wustl.edu

Abstract: A blind separation problem in a multiple-input-multiple-output (MIMO) linear time-invariant (LTI) system with finite-alphabet inputs is considered. A discrete-time matrix equation model is used to describe the input-output relation of the system in order to make full use of the advantages of modern digital signal processing techniques. At first, ambiguity problem is investigated. Then, based on the results of the investigation, a new identifiability condition is proposed for the case of an alphabet set which is widely used in digital communication. The proposed condition is compared to an existing condition in terms of the probability of satisfying each condition for an arbitrary input matrix. A probability bound such that an arbitrary input matrix satisfies the identifiability condition is derived. Monte-Carlo simulation is performed to demonstrate the fact that the identifiability conditions found so far are still very loose.

Keywords: MIMO, Blind identification, Finite-alphabet, Ambiguity

1. INTRODUCTION

For an impulse response of a linear system, $a(t)$, with an input $s(t)$, the output $z(t)$ can be given by the convolution of the two functions,

$$z(t) = \int_{-\infty}^{\infty} a(\tau)s(t-\tau)\,d\tau + n(t) \qquad (1)$$

where $n(t)$ is a corrupted noise whose statistics may be known or previously measured.

A typical signal processing problem is to determine one of $s(t)$ and $a(t)$ from the measurement $z(t)$ when one of them is previously given or statistically known. If $s(t)$ is given or known statistically, it is called a *system identification* problem. On the other hand, if $a(t)$ is previously known or statistically given, the problem becomes an *equalization* problem.

Optimal solutions of the above two problems are relatively straightforward and well-known. However, in many important practical situations, it happens that only the measurements are available. In this case it is required to resolve $s(t)$ and $a(t)$ simultaneously from the measurement.

Blind estimation methods could be a good candidate to solve this problem. Blind methods exploit some side-information about the system or the inputs. The finite-alphabet (FA) property or cyclostationarity of the inputs may be some of the examples used as side-information.

The early approaches to blind estimation and identification methods were mainly done on the signal separation in wireless communication systems. The methods are usually based on the statistical description of the system inputs. While the techniques based on higher-order statistics were developed at the beginning of the research (Mendel, 1991; Tsatsanis and Giannakis, 1996), second-order statistics play an important role in the techniques developed later (Tong *et al.*, 1995). Subspace methods (Hua, 1996; Moulines *et al.*, 1995) based on second-order statistics method have been reported with promising results.

A more direct approach than the above methods is direct blind signal separation, proposed in several works (Swindlehurst and Yang, 1994; Talwar *et al.*, 1996; van der Veen *et al.*, 1997). These works focused on separating the signal directly without determining the system characteristics. Talwar *et al.* (1996) proposed some blind separation methods by exploiting the FA property of digital inputs. In the work, the identifiability issue was considered first and then two blind estimation algorithms were proposed. Although more practical case was studied by Veen *et al.* (1997), both methods still suffer from an ambiguity problem.

In this paper the ambiguity problem is further investigated first. Based on the results of the ambiguity analysis, a new identifiability condition, which is more useful in blind identification process, will be proposed and analyzed.

This paper is organized as follows. In Section 2, the problem is formulated. In the following Section 3, the ambiguity problem in the blind separation is explained. In Section 4, a new identifiability condition is proposed and then proved. A probabilistic analysis with a computer simulation are done in Section 5 to measure the validity of the identifiability condition. A brief conclusion follows at the end.

2. PROBLEM STATEMENT

2.1 Notation

The following notation will be used.

- Scalar sets are represented with special characters such as $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{C}$ etc.
- Vector and matrix sets are denoted with calligraphic letters, for examples, $\mathcal{B}$, $\mathcal{D}$, $\mathcal{H}$.
- Matrices are denoted with bold capital letters such as $\mathbf{A}$, $\mathbf{D}$, $\mathbf{T}$, and $\mathbf{S}$. Vectors are represented with bold lower-case letters like $\mathbf{a}$, $\mathbf{b}$.

2.2 Problem

Consider an input-output relation of a discrete-time MIMO LTI system which is given by

$$\mathbf{Z} = \mathbf{A}\mathbf{S} + \mathbf{W}, \tag{2}$$

where $\mathbf{Z}$, $\mathbf{A}$, $\mathbf{S}$, and $\mathbf{W}$ are measurement, system, input, and additive noise matrix, respectively.

A typical example of this model may be a wireless multiple access system where the information-bearing signal $\mathbf{S}$ is transmitted through the channel $\mathbf{A}$ to a base station. In some cases such as M-ary phase-shift-keying in digital communication systems, the elements of $\mathbf{S}$ usually come from a FA set.

Main subject in the blind estimation problem is to find an efficient way to separate $\mathbf{A}$ and $\mathbf{S}$ from their product $\mathbf{Z}$. In this paper, the problem of a blind separation of the matrices $\mathbf{A}$ and $\mathbf{S}$ from the measurement $\mathbf{Z}$ using the FA property of the $\mathbf{S}$ is considered. It is very difficult to consider the problem for a general case of the alphabet set. Therefore, the consideration is limited to the following case that is widely used in real communication systems nowadays.

Let the sets, $\mathbb{N} = \{+1, -1\}$ and $\mathbb{Q} = \{a + jb \mid a, b \in \mathbb{N}\}$, respectively, and denote the set of all $m \times n$ matrices with elements from a set $\mathbb{Z}$ as $\mathcal{M}_{m\times n}(\mathbb{Z})$. Then the system model under no-noise assumption of (2) may be rewritten as

$$\mathbf{Z} = \mathbf{A}\mathbf{S}, \tag{3}$$

with $\mathbf{Z} \in \mathcal{M}_{M\times N}(\mathbb{C})$, $\mathbf{A} \in \mathcal{M}_{M\times d}(\mathbb{C})$, and $\mathbf{S} \in \mathcal{M}_{d\times N}(\mathbb{Q})$. $\mathbb{C}$ denotes the set of complex numbers.

The blind signal separation in this model requires the factorization of the given measurement $\mathbf{Z}$ into $\mathbf{A}$ and $\mathbf{S}$. Basically, if there are no constraints on $\mathbf{A}$ and $\mathbf{S}$, there are infinitely many solutions for the pair of $\{\mathbf{A}, \mathbf{S}\}$. In our problem, $\mathbf{A}$ is arbitrary, but the possible values for the elements of $\mathbf{S}$ are limited. Also, the matrices $\mathbf{A}$ and $\mathbf{S}$ are assumed to be full rank.

3. AMBIGUITY

The model given in (3) can be further expanded mathematically as

$$\mathbf{Z} = \mathbf{A}\mathbf{S} = (\mathbf{A}\mathbf{T}^{-1})(\mathbf{T}\mathbf{S}) \triangleq \bar{\mathbf{A}}\bar{\mathbf{S}} \tag{4}$$

where $\mathbf{T}$ is any $d \times d$ full rank matrix and $\bar{\mathbf{S}} \in \mathcal{M}_{d\times N}(\mathbb{Q})$. The relation in (4) implies the existence of another solution pair which can be represented as $\bar{\mathbf{A}} \triangleq \mathbf{A}\mathbf{T}^{-1}$ and $\bar{\mathbf{S}} \triangleq \mathbf{T}\mathbf{S}$.

Denote a set as $\mathbb{N}_c \triangleq \{+1, -1, +j, -j\}$ to define a useful matrix set as follows.

Definition 1. A matrix set $\mathcal{D}_r(\mathbb{N}_c)$ is defined as the set of all possible $r \times r$ diagonal matrices with their elements from $\mathbb{N}_c$.

Then, it can be easily noted that $\mathbf{T}$ may be basically described as $\mathbf{T} = \mathbf{PD}$ where $\mathbf{P}$ is a permutation matrix and $\mathbf{D} \in \mathcal{D}_d(\mathbb{N}_c)$. This fact implies that, in the factorization process of $\mathbf{Z}$ into $(\mathbf{A}, \mathbf{S})$ in (3), ordering (by $\mathbf{P}$) and phase (by $\mathbf{D}$) ambiguities inherently follow. These kinds of ambiguities will be called *low-level ambiguity.* If there exist other $\mathbf{T}$'s than in the form of $\mathbf{PD}$ or $\mathbf{DP}$, it is said that there exists *high-level ambiguity* in the solution for $\mathbf{S}$.

Since $\mathbf{A}$ and $\bar{\mathbf{A}}$ are arbitrary and full rank, the relation in (4) can be considered as a problem given by

$$\mathbf{TS} = \bar{\mathbf{S}}, \tag{5}$$

where $\mathbf{T}$ is a $d \times d$ matrix, and $\mathbf{S}, \bar{\mathbf{S}} \in \mathcal{M}_{d\times N}(\mathbb{Q})$.

3.1 Low-level ambiguity

As pointed out in the previous discussion, there exist two different kinds of low-level ambiguity inherently in the solutions for $\mathbf{S}$ of (3) which are ordering and phase ambiguities. However, the low-level ambiguity may not be a serious problem in retrieving the original information as in the previous discussion in (Kwon and Fuhrmann, 1997).

3.2 High-level ambiguity

The fundamental theorem for systems of linear equations gives the following facts for the existence of the solutions for $\mathbf{T}$ of (5). Define two variables, r_1 and r_2, such that

$$r_1 \triangleq rank\ (\mathbf{S}) \ \text{ and } \ r_2 \triangleq rank\ ([\mathbf{S}^T\ \bar{\mathbf{S}}^T]). \tag{6}$$

Then, if $N \geq d$, which is the determined or overdetermined case,

- equation (5) has solutions iff $r_1 = r_2$.
- if $r_1 = r_2 = d$, there exists a unique solution which is given by $\mathbf{T} = \bar{\mathbf{S}}\mathbf{S}^T(\mathbf{S}\mathbf{S}^T)^{-1}$.
- if $r_1 = r_2 < d$, there are infinitely many solutions.

Note that if $N < d$ (which is underdetermined case) then there always exist solutions. Also if $r_1 \neq r_2$ with $N \geq d$, there are no solutions.

The system, $\mathbf{Z} = \mathbf{AS}$, is defined to be *identifiable* if there exists only low-level ambiguities among the possible solutions for $\mathbf{S}$. Based on this definition on identifiability, an identifiability condition for this system is considered in the following section.

4. A NEW IDENTIFIABILITY CONDITION

Talwar *et al.* showed a sufficient identifiability condition in (Talwar *et al.*, 1996) as written in the following Theorem 2.

Theorem 2. (Theorem 3.2 in (Talwar *et al.*, 1996)). Let $\mathbf{Z} = \mathbf{AS}$ where $\mathbf{A}_{M\times d}$ is an arbitrary full-rank matrix with $d \leq M$, and $\mathbf{S}_{d\times N}$ is a full-rank matrix with elements in the set $\{\pm1, \pm3, \cdots, \pm(L-1)\} \oplus \{\pm j, \pm j3, \cdots, \pm j(L-1)\}$. If the columns of $\mathbf{S}$ include all the $L^{2d}/2$ possible distinct (up to a sign) d-vectors with elements in $\{\pm1, \pm3, \cdots, \pm(L-1)\} \oplus \{\pm j, \pm j3, \cdots, \pm j(L-1)\}$, then $\mathbf{A}$ and $\mathbf{S}$ can be uniquely identified up to a matrix $\mathbf{T}$ with exactly one non-zero element, $\{+1, -1, +j, -j\}$, in each row and column.

The identifiability condition described in this theorem can not be easily satisfied for a randomly generated $\mathbf{S}$ with a reasonable size. Therefore, a new identifiability condition is investigated.

4.1 Definitions

Definition 3. An equivalent class of a d-vector $\mathbf{a}$ is denoted by $\mathcal{E}(\mathbf{a})$ and defined as

$$\mathcal{E}(\mathbf{a}) = \{+\mathbf{a},\ -\mathbf{a},\ +j\mathbf{a},\ -j\mathbf{a}\}. \tag{7}$$

Definition 4. (Element-wise (α, k)-rotation). *Element-wise (α, k)-rotation* is defined as a transformation on a vector such that k-th element of the vector is phase-shifted (or rotated on the complex plane) by α.

Denote this operation on a vector $\mathbf{x}$ as $\mathcal{T}(\mathbf{x}; \alpha, k)$. Also denote a vector $\tilde{\mathbf{a}}_k(\theta)$ as $\tilde{\mathbf{a}}_k(\theta) \triangleq \mathcal{T}(\mathbf{a}; \theta, k)$. Then if $\mathbf{a} \triangleq [a_1\ a_2\ \cdots\ a_k\ \cdots\ a_{d-1}\ a_d]^T$, $\tilde{\mathbf{a}}_k(\theta) = [a_1\ a_2\ \cdots\ a_k e^{j\theta}\ \cdots\ a_{d-1}\ a_d]^T$.

Definition 5. Define $\mathcal{C}(\mathbf{a}, \theta)$ as a set of some equivalent classes such that

$$\mathcal{C}(\mathbf{a}, \theta) \triangleq \{\mathcal{E}(\mathbf{a}), \mathcal{E}(\tilde{\mathbf{a}}_1(\theta)), \mathcal{E}(\tilde{\mathbf{a}}_2(\theta)),\ \cdots, \mathcal{E}(\tilde{\mathbf{a}}_d(\theta))\}. \tag{8}$$

Then an equivalent class $\mathcal{R}(\mathbf{a}, \theta)$ is defined as the set of all possible different $\mathbf{C}(\mathbf{a})$'s where $\mathbf{C}(\mathbf{a})$ is a vector set which consists of exactly one vector from each element of $\mathcal{C}(\mathbf{a}, \theta)$.

Note that each element of $\mathcal{C}(\mathbf{a}, \theta)$ is indeed an equivalent class. The cardinality of $\mathcal{R}(\mathbf{a}, \theta)$ is given by

$$|\mathcal{R}(\mathbf{a}, \theta)| = |\mathbb{Q}|^{d-1}, \tag{9}$$

which is the number of different $\mathbf{C}(\mathbf{a})$'s.

Definition 6. A vector set $\mathcal{O}(\mathbf{S})$ is defined as the set of all different column vectors of the matrix $\mathbf{S}$.

4.2 A new sufficient identifiability condition

For the case of the alphabet, $\mathbb{Q}_\phi \triangleq \{e^{j\phi}, e^{j(\phi+\frac{\pi}{2})}, e^{j(\phi+\pi)}, e^{j(\phi+\frac{3\pi}{2})}\}$, where ϕ is an arbitrary angle, the following theorem for the identifiability is proposed.

Theorem 7. (A new identifiability condition). For a linear system $\mathbf{Z} = \mathbf{AS}$, where $\mathbf{A} \in \mathcal{M}_{M\times d}(\mathbb{C})$ is full-rank and $\mathbf{S} \in \mathcal{M}_{d\times N}(\mathbb{Q}_\phi)$, if any element of either $\mathcal{R}(\mathbf{a}, \frac{\pi}{2})$ or $\mathcal{R}(\mathbf{a}, -\frac{\pi}{2})$ is a subset of $\mathcal{O}(\mathbf{S})$ for any $\mathbf{a} \in \mathcal{O}(\mathbf{S})$, then the system is identifiable.

Note that the smallest number of columns needed to fulfill the identifiability condition is $d+1$.

PROOF. In the relation (5) which is

$$\mathbf{TS} = \bar{\mathbf{S}} \tag{10}$$

where $\bar{\mathbf{S}}$ can be any element in $\mathcal{M}_{d\times N}(\mathbb{Q}_\phi)$, but not equal to $\mathbf{S}$, by rearranging the order of the columns of $\mathbf{S}$ and $\bar{\mathbf{S}}$ and then dividing them into two sub-matrices each, it can be derived that

$$\mathbf{T}[\mathbf{S}_{d+1} \;\; \mathbf{S}_{N-d-1}] = [\bar{\mathbf{S}}_{d+1} \;\; \bar{\mathbf{S}}_{N-d-1}] \tag{11}$$

where $\mathbf{S}_{d+1}$ is a sub-matrix composed by the necessary $d+1$ columns in $\mathbf{S}$ for the identifiability and $\mathbf{S}_{N-d-1}$ is the remainder. Consequently, $\bar{\mathbf{S}}_{d+1}$ and $\bar{\mathbf{S}}_{N-d-1}$ are the corresponding sub-matrices of $\bar{\mathbf{S}}$ to $\mathbf{S}_{d+1}$ and $\mathbf{S}_{N-d-1}$, respectively. Then, our proof will be enough to show that the solution of $\mathbf{T}$ for the first part of (11) given by

$$\mathbf{TS}_{d+1} = \bar{\mathbf{S}}_{d+1} \tag{12}$$

since at most the second part of (11) will further reduce the possible solution sets for $\mathbf{T}$. Here the equation is solved for $\mathbf{T}$ where the sets of $\mathbf{S}_{d+1}$ and $\bar{\mathbf{S}}_{d+1}$ are given. However, note that this is overdetermined system since there are $d+1$ equations for each set. Therefore, the existence of solutions will depend on the selection of $\mathbf{S}_{d+1}$ and $\bar{\mathbf{S}}_{d+1}$ pair, that is, the rank of $[\mathbf{S}_{d+1} \; \bar{\mathbf{S}}_{d+1}]$. Rewriting (12) as

$$\mathbf{S}_{d+1}^\dagger \mathbf{T}^\dagger = \bar{\mathbf{S}}_{d+1}^\dagger, \tag{13}$$

d sets of $d+1$ linear equations are given as

$$\mathbf{S}_{d+1}^\dagger \mathbf{t}_k^\dagger = \bar{\mathbf{s}}_{d+1,k}^\dagger, \quad k = 1, 2, \cdots, d, \tag{14}$$

where $\mathbf{t}_k$ and $\bar{\mathbf{s}}_{d+1,k}$ are k-th row vectors of $\mathbf{T}$ and $\bar{\mathbf{S}}_{d+1}$, respectively. Thus it can be rewritten as

$$\begin{bmatrix} e^{j\phi_1} & e^{j\phi_2} & \dots & e^{j\phi_d} \\ e^{j(\phi_1+\theta)} & e^{j\phi_2} & \dots & e^{j\phi_d} \\ \vdots & \vdots & \vdots & \vdots \\ e^{j\phi_1} & e^{j\phi_2} & \dots & e^{j(\phi_d+\theta)} \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_d \end{bmatrix} = \begin{bmatrix} e^{j\psi_1} \\ e^{j\psi_2} \\ \vdots \\ e^{j\psi_{d+1}} \end{bmatrix}, \tag{15}$$

where the first matrix is a general representation of $\mathbf{S}_{d+1}$ which satisfies the condition in our theorem if $\theta = \pm\frac{\pi}{2}$, $\mathbf{t}_k^\dagger = [t_1 \quad t_2 \quad \cdots \quad t_d]^T$, and $\bar{\mathbf{s}}_{d+1,k}^\dagger = [e^{j\psi_1} \quad e^{j\psi_2} \quad \cdots \quad e^{j\psi_{d+1}}]^T$.

Now consider the first and second equations in (15) only. Then the result becomes

$$(e^{j\phi_1} - e^{j(\phi_1+\theta)})t_1 = e^{j\phi_1} - e^{j\phi_1}. \tag{16}$$

Thus, a solution for t_1 is given by

$$t_1 = \frac{1}{\sqrt{2}} e^{-j(\phi_1 - \frac{\theta}{2})}(e^{j\psi_1} - e^{j\psi_2}). \tag{17}$$

Therefore, from all of the equation pairs which are related to each of the second row to the last row of $\mathbf{S}_{d+1}^\dagger$ with its first row, the solution for t_i is given by

$$t_i = \frac{1}{\sqrt{2}} e^{-j(\phi_i - \frac{\theta}{2})}(e^{j\psi_1} - e^{j\psi_{i+1}}), \quad i = 1, 2, \cdots, d. \tag{18}$$

Inserting this solution into the first equation in (15) gives a result given by

$$de^{j\psi_1} - \sqrt{2}e^{j(\psi_1 - \frac{\theta}{2})} = \sum_{i=2}^{d+1} e^{j\psi_i}. \tag{19}$$

Without loss of generality, $e^{j\psi_1}$ is assumed to be any one element of $\mathbb{Q}_\phi$, for example, say $e^{j\psi_1} = e^{j\phi}$. Then the problem can be solved graphically from Figure 1.

Using Figure 1, it is concluded that $d-1$ terms among $\{e^{j\psi_i}\}_{i=2}^{d+1}$ should be equal to $e^{j\psi_1}$ and the only remaining one term must be equal to $e^{j(\phi+\theta)}$ or $e^{j(\phi-\theta)}$ in (19).

This result implies that $d-1$ variables among $\{t_i\}_{i=1}^{d}$ in (18) become zeros and the only nonzero t_i will have a value given by

$$t_i = e^{j(\phi - \phi_i)}, \tag{20}$$

where $(\phi - \phi_i) \in \{0, \frac{\pi}{2}, -\frac{\pi}{2}, \pi\}$. Therefore, this nonzero t_i can only have a value from the set $\{1, -1, j, -j\}$.

Similar results come out for all k in (14).

Now the columns of $\mathbf{T}$ should be independent from each other to satisfy the fact that $\mathbf{S}_{d+1}$ and $\bar{\mathbf{S}}_{d+1}$ are full rank. Consequently, $\mathbf{T}$ should have exactly one non-zero element in each row and column to make itself full rank. Therefore our theorem shows a sufficient condition for the identifiability.

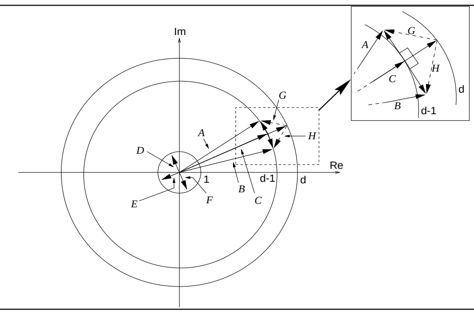

Fig. 1. Graphical representation of the relation (19) where $C = (d-1)e^{j\phi}$, $D = e^{j(\phi+\frac{\pi}{2})}$, $E = e^{j(\phi+\pi)}$, $F = e^{j(\phi+\frac{3\pi}{2})}$, $G = -\sqrt{2}e^{j(\phi-\frac{\pi}{4})}$, and $H = -\sqrt{2}e^{j(\phi+\frac{\pi}{4})}$.

Note that our theorem is invariant to any phase shift of the alphabet. Therefore, it can be applied to all types of FA sets if the elements of the alphabet are related to each other by $\pm\frac{n\pi}{2}$ phase shift with an integer n.

The problem is considered for the case where the columns of $\mathbf{S}$ are different to each other in only one element. Therefore, it is undoubted that there may be a lot more possible structure of $\mathbf{S}$ which satisfy the identifiability. Even though that part is remained for future work, it can be shown that the new identifiability condition can be easily achieved with high probability in a reasonable number of samples as shown in Section 5.

5. PROBABILISTIC CONSIDERATION

A bound of the probability that a randomly generated matrix satisfies the identifiability condition is derived. Then Monte-Carlo simulation is done to see if the bound is valid.

5.1 A bound

Consider a probabilistic bound for Theorem 2 first. Let L denote the alphabet size.

Lemma 8. Let $\mathcal{F}$ be the event that all the $\frac{L^{2d}}{2}$ distinct vectors are picked in N independent samples. Then, A probabilistic bound for $\mathcal{F}$ can be given as

$$P_r(\mathcal{F}) \geq 1 - \frac{L^{2d}}{2}\left(\frac{L^{2d}-2}{L^{2d}}\right)^N. \qquad (21)$$

PROOF. Omitted.

Figure 2 shows this bound when $d = 4$. It is noticed that a hugh number of samples are needed to fulfill the identifiability condition given in Theorem 2 with probability close to one.

Now consider a bound for the new condition.

Lemma 9. For the identifiability condition given in Theorem 7, a bound can be given by

$$P_r(\mathcal{A}) \geq 1 - \left[(d+1)(1-4^{1-d})^N\right]^{2\times 4^{d-1}} \qquad (22)$$

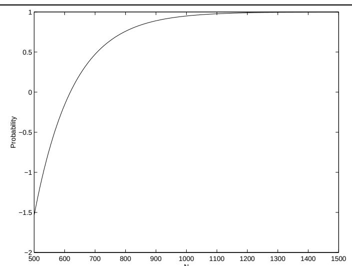

Fig. 2. The value of (21) when $d = 4$.

where $\mathcal{A}$ denotes the event such that a randomly generated $d \times N$ data matrix contains any combination of the possible vector sets which are sufficient to satisfy our identifiability condition.

PROOF. Let $\mathcal{A}|\mathbf{S}_i$ be the event that all the $d+1$ distinct vectors in a possible identifiability set $\mathbf{S}_i$ are included in N samples. As mentioned earlier, there are 4^{d-1} different vectors which are not connected to each other by the sign or real-imaginary ambiguity. From this set of different vectors, $2 \times 4^{d-1}$ different combinations of $d \times (d+1)$ matrices, which satisfy our identifiability condition, can be constructed. Therefore, i has the values from 1 to k where $k \triangleq 2 \times 4^{d-1}$.

Then, it is easily shown that

$$P_r(\mathcal{A}^c|\mathbf{S}_i) = P_r\left(\cup_{n=1}^{d+1}\mathcal{A}_n^c\right) \leq \sum_{n=1}^{d+1} P_r(\mathcal{A}_n^c|\mathbf{S}_i),$$

and

$$\sum_{n=1}^{d+1} P_r(\mathcal{A}_n^c|\mathbf{S}_i) = (d+1)\left(1-\frac{1}{4^{d-1}}\right)^N, \qquad (23)$$

for $i = 1, 2, \cdots, k$.

Note that

$$P_r(\mathcal{A}^c|\mathbf{S}_i) = P_r(\mathcal{A}^c|\mathbf{S}_j) \quad \text{for all } i, j \qquad (24)$$

and

$$P_r(\mathcal{A}^c|\mathbf{S}_i \cap \mathcal{A}^c|\mathbf{S}_j) \leq P_r(\mathcal{A}^c|\mathbf{S}_i)P_r(\mathcal{A}^c|\mathbf{S}_j) \quad (25)$$

with equality if and only if the events $\mathcal{A}^c|\mathbf{S}_i$ and $\mathcal{A}^c|\mathbf{S}_j$ are independent. However, the following lemma tells us that all of them are not independent in pairs.

Lemma 10. For any two d-vectors, $\mathbf{a}_1, \mathbf{a}_2 \in \mathcal{O}(\mathbf{S})$, which satisfy the condition, $\mathcal{E}(\mathbf{a}_1) \neq \mathcal{E}(\mathbf{a}_2)$, it is true that $|\mathcal{R}(\mathbf{a}_1, \theta) \cup \mathcal{R}(\mathbf{a}_2, \theta)| \leq 2$ if $d > 3$.

PROOF. Omitted.

Therefore,

$$P_r(\mathcal{A}^c|\mathbf{S}_1 \cap \mathcal{A}^c|\mathbf{S}_2 \cap \cdots \cap \mathcal{A}^c|\mathbf{S}_k) < \prod_{i=1}^{k} P_r(\mathcal{A}^c|\mathbf{S}_i),$$

and

$$\prod_{i=1}^{k} P_r(\mathcal{A}^c|\mathbf{S}_i) = \left[(d+1)\left(1-\frac{1}{4^{d-1}}\right)^N\right]^k \qquad (26)$$

where $k = 2 \times 4^{d-1}$.

Figure 3 shows the minimum numbers of samples with respect to d to satisfy the identifiability condition with approximately probability one. This numbers were calculated using the bounds in (21) and (22).

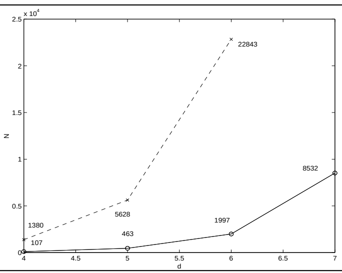

Fig. 3. The number of samples with probability greater than 0.9999: our case (solid line) and Talwar's case (dashed line).

5.2 Monte-Carlo Simulation

Figure 4 shows a result of Monte-Carlo simulation and the derived bound when $d = 4$. Under the uniform distribution assumption, 10000 samples are generated to calculate each point. It is seen that the bound is very loose.

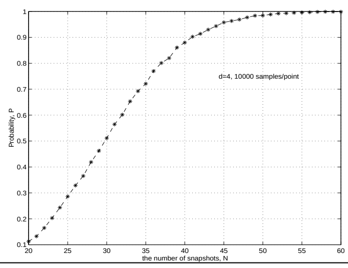

Fig. 4. Probability for a data matrix **S** to satisfy the identifiability condition.

It is noticed that the probability rapidly approaches to one within a reasonable number of samples so that the probability becomes greater than or equal to 0.9999 if the number of samples is greater than 66.

Also it should be pointed out that this probability is actually a lower bound. Therefore, it is expected that the identifiability is achieved in fewer samples than the numbers shown here.

6. CONCLUSION

In this paper, the identifiability problem in the blind separation of **A** and **S** for the MIMO LTI system equation, $\mathbf{X} = \mathbf{AS}$, was investigated. For a full rank arbitrary **A** with a finite alphabet for the elements of **S**, it was shown that there still exist multiple solutions for **S**.

A new sufficient condition for the identifiability was proposed. The new condition was compared to the previously proposed condition in view of the probability bound of satisfying the condition for **S**. A quantitative probabilistic consideration of satisfying this condition for a randomly generated **S** was given.

The probabilistic analysis revealed that the probability of satisfying the identifiability for a pair of randomly generated **A** and **S** rapidly approaches to one within a reasonable number of samples. In other words, it was verified that the identifiability in the blind signal separation of a system given by $\mathbf{Z} = \mathbf{AS}$ can be achieved within far fewer samples than it has been thought.

Monte-Carlo simulation showed the probabilistic aspect of satisfying identifiability for randomly generated signal matrices. From the numerical examples, it can be concluded that the two identifiability conditions discussed here are still very loose.

REFERENCES

Hua, Yingbo (1996). Fast Maximum Likelihood for Blind Identification of Multiple FIR Channels. *IEEE Transactions on Signal Processing* **44**(3), 661–672.

Kwon, S. and D. R. Fuhrmann (1997). Identifiability Problem in Blind Separation of Synchronous BPSK Signals in Digital Wireless Communication. In: *Proceedings of the 35th Annual Allerton Conference*. pp. 291–300.

Mendel, J. (1991). Tutorial on Higher-Order Statistics (Spectra) in Signal Processing and System Theory: Theoretical Results and Some Applications. In: *Proceedings of IEEE*. Vol. 79. pp. 278–305.

Moulines, Eric, Pierre Duhamel, Jean-Francois Cardoso and Sylvie Mayrargue (1995). Subspace Methods for the Blind Identification of Multichannel FIR Filters. *IEEE Transactions on Signal Processing* **43**(2), 516–525.

Swindlehurst, A. and J. Yang (1994). Using Least Squares to Improve Blind Signal Copy Performance. *IEEE Signal Processing Letters* **1**(5), 80–82.

Talwar, Shilpa, Mats Viberg and A. Paulraj (1996). Blind Separation of Synchronous Co-Channel Digital Signals Using an Antenna Array — Part I: Algorithms. *IEEE Transactions on Signal Processing* **44**(5), 1184–1197.

Tong, L., G. Xu, B. Hassibi and T. Kailath (1995). Blind Channel Identification based on Second-Order Statistics: A Frequency-Domain Approach. *IEEE Transactions on Information Theory* **41**(1), 329–333.

Tsatsanis, Michail K. and Georgios B. Giannakis (1996). Equalization of Rapidly Fading Channels: Self-Recovering Methods. *IEEE Transactions on Communications* **44**(5), 619–630.

van der Veen, Alle-Jan, Shilpa Talwar and Arogyaswami Paulraj (1997). A Subspace Approach to Blind Space-Time Signal Processing for Wireless Communication Systems. *IEEE Transactions on Signal Processing* **45**(1), 173–190.