Blind ML Detection of Orthogonal Space-Time Block Codes: Identifiability and Code Construction

Wing-Kin Ma*

Final Version

October 2006

To appear in *IEEE Trans. Signal Processing*

Abstract

The blind maximum-likelihood (ML) detection of a general space-time block code (STBC) is considered a challenging implementation problem. Recent work has revealed that for the orthogonal STBCs (OSTBCs), their special code structures can be exploited to formulate highly effective blind ML-based algorithms. Attracted by this realization merit, this paper investigates the blind ML identifiability of OSTBCs, with an emphasis on the binary PSK (BPSK) and quaternary PSK (QPSK) constellations. We find a class of OSTBCs, called the non-rotatable OSTBCs, that can be uniquely identified up to a sign (UIUTS) almost surely under a few mild assumptions. For example, for an independently distributed Rayleigh channel with any number of receiver antennas, a non-rotatable OSTBC can be UIUTS with probability 1. While this identifiability looks appealing already, we further examine a subclass of non-rotatable OSTBCs, called the non-intersecting subspace (NIS) OSTBCs. We prove that NIS-OSTBCs are UIUTS for any nonzero channel. However, NIS-OSTBCs are not available in the existing literature. To fill this gap, we devise a code construction procedure that can convert any (BPSK or QPSK) OSTBC to an NIS-OSTBC.

Index terms— space-time block code, maximum likelihood detection, decoding, blind and semiblind detection, blind identifiability, performance analysis

SP-EDICS: SPC-c Blind/semiblind estimation and equalization, SPC-f Space-time coding, design, and analysis, MSP-d MIMO space-time coding and decoding algorithms

*Wing-Kin Ma is the corresponding author. Address: Institute of Communications Engineering, National Tsing Hua University, 101 Sec. 2 Kuang Fu Road, Hsinchu, Taiwan 30013. E-mail: wkma@ieee.org, Tel.: +886 3 571 5131 ext. 34143, Fax: +886 3 575 1787

Preliminary version of this paper appeared as a conference paper in ICASSP 2004. This paper also serves as a correct version of that conference paper, in which there are errata. This work was supported in part by the National Science Council, R.O.C., under grant NSC 95-2221-E-007-004.

I. Introduction

In multiple-input-multiple-output (MIMO) systems, blind detection [1], [2] or noncoherent detection [3]–[5] is an attractive approach when channel state information (CSI) is not available at the receiver. In a number of cases, we can safely assume CSI being known at the receiver[1]. That is because CSI can be estimated reliably by transmitting pilot signals, which has little loss in the data rate if there is an abundant power resource at the transmitter (e.g., the downlink channel) and/or if channel fading is slow. However, for channels having smaller coherence time, accurate pilot-assisted CSI acquisition requires more frequent pilot retransmission. Consequently, the power and bandwidth overheads for the pilots would no longer be negligible. In those cases, an alternative worth considering is the blind or noncoherent detection methods, which either estimate CSI from received data or bypass CSI in detection.

A popular noncoherent MIMO scheme is differential unitary space-time modulation [6]–[9], which requires the channel to be static over two space-time code blocks only. The differential scheme, however, incurs an approximately 3dB performance penalty compared to its coherent counterpart. On the other hand, in the signal processing context there has been much interest in developing blind detection methods for space-time block codes [1], [2], [10]–[17]. In this direction we consider 'quasi-static' channel fading, where the channel is assumed to be static over multiple space-time code blocks but where pilot-assisted CSI acquisition is still inefficient. Blind detection methods may achieve near coherent detection performance, particularly when there is a sufficiently large data length (or number of blocks in which quasi-static fading remains valid).

In this paper the emphasis is placed on the blind maximum-likelihood (ML) detection of orthogonal space-time block codes (OSTBCs) [18]–[25]. In the coherent space-time coding scenario, OSTBCs have been well known for their maximal spatial diversity and low ML receiver complexity. Recent research has revealed that OSTBCs are attractive in the noncoherent scenario, as well. Essentially, given a generic MIMO or space-time block coding (STBC) scheme, implementing the blind ML receiver is a highly nonlinear optimization problem. As a problem common to general multimodal nonlinear optimization, it is hard to guarantee, in every problem instance, that an optimal or near-optimal blind ML solution be obtained. The OSTBC scheme is an exception where one can utilize the special code structures to design

[1]In the signal processing context, 'blind detection' is used to to describe detection without CSI. In the information theory context, 'noncoherent detection' is frequently employed. The developments in the two contexts are, in many ways, different. Very roughly speaking, in signal processing the focus is often on the blind receiver realization aspects, while in information theory the subjects of interest are the noncoherent channel capacity and code designs.

more effective blind ML algorithms, either optimally or suboptimally. In [2] (also the textbook [26]), Stoica *et. al* proposed a cyclic minimization method for blind ML OSTBC detection. This cyclic ML receiver exploits the low coherent receiver complexity, and is simple to implement compared to the same method applied to some other MIMO/STBC schemes; e.g., spatial multiplexing [10]. As an additional merit, cyclic ML can be generalized to handle unknown Gaussian noise covariance [13]. However, cyclic ML requires initialization of either the channel estimate or the symbol decisions. By simulation experience, the cyclic ML performance can be unsatisfactory given a mediocre initialization. In [2], a blind closed-form method jointly estimating the channel and symbols was proposed to initialize cyclic ML. That blind closed-form method is also based on the special characteristics of OSTBCs. Interestingly, the closed-form method is functionally equivalent to the blind subspace OSTBC channel estimator in [16]; see the discussion in [14, pp. 741, Footnote 2]. (We should point out though that the work in [16] is original from a blind subspace viewpoint.) Empirical studies showed that the closed-form and cyclic ML methods exhibit near coherent ML performance for large data length, say for 50 space-time code blocks or more [2], [16]. To yield near optimal performance with smaller data length, it has been suggested [2], [13] that a semiblind cyclic ML receiver be used, in which a few pilot STBCs are required.

A more recent endeavor [14] reveals that even in the regime of small to moderate data length, blind ML OSTBC detection can be implemented in an exactly optimal or near-optimal fashion. By focusing on binary PSK (BPSK) or quaternary PSK (QPSK) constellations, it is shown that the blind ML problem can be simplified to a Boolean quadratic program (BQP). The reformulation is done by exploiting the orthogonal and linear dispersion characteristics of OSTBCs. The BQP is still a computationally hard optimization problem, and [14] illustrates how the blind ML BQP can be handled effectively by using either the optimal sphere decoding algorithms [27], [28] or the quasi-optimal semidefinite relaxation (SDR) algorithm [29]. The performance and complexity comparisons of the two methods are described in details in [29]. Sphere decoding and SDR are computationally more expensive than the closed-form and cyclic ML receivers mentioned above: For example, the complexity of SDR is approximately cubic in the data length, while the complexity of the closed-form method is only linear in the data length. However, simulation results [14] have indicated that sphere decoding and SDR ML implementations provide considerably better bit error performance than the closed-form and cyclic ML methods, especially in the regime of small to moderate data length (say, 10 to 20 space-time code blocks).

This paper is a sequel of [14]. We turn our attention from blind receiver realization to the blind ML OSTBC identifiability, with an emphasis on the BPSK and QPSK constellations. Our analysis shows that OSTBCs can provide very favorable identifiability conditions, though not all OSTBCs have such

benefits. First, we identify a class of codes called the *rotatable* OSTBCs. Rotatable OSTBCs can never be uniquely identified up to a sign (UIUTS). An example of rotatable OSTBCs is the famous Alamouti code [30], which, in some earlier studies [1], [16], [31], has been found to suffer from some code ambiguity effects. Second, the class of *non-rotatable* OSTBCs is considered. We show that for a broad class of Gaussian channel fading, non-rotatable OSTBCs can be UIUITS with probability 1. For example, for an independent and identically distributed (i.i.d.) Rayleigh channel, a non-rotatable OSTBC can be UIUTS with probability 1 even when the number of receiver antennas is one. These identifiability benefits are under a mild assumption on data, which usually holds for large data length. We show that there exists a subclass of non-rotatable OSTBCs, called the *strictly non-rotatable* OSTBCs, that achieves the probability 1 identifiability condition without requiring the data assumption. Finally, we examine a further subclass of strictly non-rotatable codes, called the *non-intersecting subspace* (NIS) OSTBCs. From a blind identifiability standpoint NIS-OSTBCs are 'perfect' in that they are UIUTS for any nonzero channel. However, we also prove that NIS-OSTBCs may incur reduction in data rate. To our best knowledge, none of the OSTBCs given in the existing literature [18]–[25] is NIS. To fill this gap we devise a code construction procedure that can convert any (BPSK or QPSK) OSTBC to an NIS-OSTBC. From our NIS-OSTBC idea, we further propose a modified OSTBC scheme that also enjoys 'perfect' identifiability and can have a smaller rate loss than the direct application of NIS-OSTBCs.

TABLE I

SUMMARY OF BLIND ML OSTBC IDENTIFIABILITY.

Code class	Identifiability	Characteristics	Details
rotatable	Not uniquely identifiable up to a sign (UIUTS)		Section III-A
non-rotatable	UIUTS with prob. 1 for many Gaussian fading channels, under a mild assumption on data		Sections III-B to III-C
strictly non-rotatable	UIUTS with prob. 1 for many Gaussian fading channels	$M_t < T$; subclass of non-rotatable codes	Sections III-B to III-C
non-intersecting subspace (NIS)	UIUTS for any nonzero channel	$2M_t \leq T$; subclass of strictly non-rotatable codes; full rate may not be possible	Section IV

In Table I we summarize the blind ML identifiability of the various classes of OSTBCs; their details are presented in Sections III and IV. The organization of this paper is as follows. Background review for blind ML OSTBC detection is given in Section II. Section III studies the rotatable, non-rotatable, and strictly non-rotatable OSTBCs. Their characteristics and identifiability are also examined in that section. In Section IV we present the NIS-OSTBCs, their properties, and how to construct them.

II. BACKGROUND

We review some key concepts essential to the ensuing development. The first subsection considers OSTBCs and their structures. The second subsection describes blind ML OSTBC detection. The respective blind identifiability problem statement is discussed in the third subsection. In that subsection we also provide an OSTBC identifiability condition obtained easily from some existing results.

A. Orthogonal Space-Time Block Codes

In orthogonal space-time block coding, the transmitted code matrix can generally be formulated as

$$\mathbf{C}(\mathbf{s}) = \sum_{k=1}^{K} s_k \mathbf{X}_k \in \mathbb{C}^{M_t \times T}, \tag{1}$$

where

M_t	number of transmitter antennas;
T	time length of the code;
$\mathbf{X}_k \in \mathbb{C}^{M_t \times T}$	basis matrices of the code;
$\mathbf{s} \in \mathbb{R}^K$	vector containing K *real* information symbols;
s_k	kth element of $\mathbf{s}$.

Eq. (1) represents not only OSTBCs with real symbol constellations, but also those with complex symbol constellations. In the latter case, an OSTBC can be expressed as [19]

$$\mathbf{C}(\mathbf{s}) = \sum_{k=1}^{K/2} s_k \mathbf{A}_k + j s_{k+K/2} \mathbf{B}_k \tag{2}$$

for some real-valued basis matrices $\mathbf{A}_k, \mathbf{B}_k \in \mathbb{R}^{M_t \times T}$, where $j = \sqrt{-1}$. In Equation (2), $s_k + j s_{k+K/2}$ forms a complex symbol for $k = 1, \ldots, K/2$ and the number of complex symbols per block is $K/2$. By letting $\{\mathbf{X}_1, \ldots, \mathbf{X}_K\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_{K/2}, j\mathbf{B}_1, \ldots, j\mathbf{B}_{K/2}\}$, the complex code in (2) can be reformulated as (1). In this paper we assume BPSK and QPSK constellations, in which case we have $\mathbf{s} \in \{\pm 1\}^K$. The basis matrices are specially designed to satisfy [18], [19], [21]

$$\mathbf{X}_k \mathbf{X}_\ell^H = \begin{cases} \mathbf{I}, & k = \ell \\ -\mathbf{X}_\ell \mathbf{X}_k^H, & k \neq \ell \end{cases} \tag{3}$$

such that every codeword is row orthogonal; i.e.,

$$\mathbf{C}(\mathbf{s})\mathbf{C}^H(\mathbf{s}) = \|\mathbf{s}\|_2^2 \mathbf{I} = K\mathbf{I} \tag{4}$$

for any $\mathbf{s} \in \{\pm 1\}^K$. Here $\|.\|_2$ denotes the 2-norm.

In the coherent detection scenario, the code properties in (1), (3), and (4) result in the well-known advantages of simple ML detection structures and the maximum spatial diversity [18], [19]. Orthogonal space-time block coding also provides benefits in the noncoherent scenario, as we will review next.

Remark 1. In principle, any matrix function satisfying (1) and (3) is said to be an OSTBC. OSTBCs are usually obtained by applying the theory of *generalized orthogonal designs* (GODs) [18]–[25], in which there are additional restrictions on the code structures. In real GODs, the entries of $\mathbf{C}(\mathbf{s})$ are constrained to be drawn from $\{0, \pm s_1, \ldots, \pm s_K\}$. Hence, the basis matrices must satisfy the integer structure $\mathbf{X}_k \in \{0, \pm 1\}^{M_t \times T}$ for all k. As for complex GODs, let

$$u_k = s_k + j s_{k+K/2} \tag{5}$$

for notational convenience. The entries of $\mathbf{C}(\mathbf{s})$ in this case are drawn from $\{0, \pm u_1, \pm u_1^*, \ldots, \pm u_{K/2}, \pm u_{K/2}^*\}$, thereby $\mathbf{X}_k \in \{0, \pm 1\}^{M_t \times T}$ for $k = 1, \ldots, K/2$, and $\mathbf{X}_k \in \{0, \pm j\}^{M_t \times T}$ for $k = K/2 + 1, \ldots, K$. For example, the complex Alamouti code

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} u_1 & -u_2^* \\ u_2 & u_1^* \end{bmatrix} \tag{6}$$

is a GOD. The analysis in this paper is established from (1) and (3), and GODs will not be assumed unless specified. Hence our analysis is applicable to all OSTBCs, including non-GOD codes (e.g., the 'sporadic' codes [18]).

B. Blind ML Detection

We consider a standard scenario [13] where a sequence of OSTBCs is transmitted over a frequency-flat, quasi-static channel. The received signal model is given by

$$\mathbf{Y}_p = \mathbf{H}\mathbf{C}(\mathbf{s}_p) + \mathbf{V}_p, \qquad p = 1, \ldots, P, \tag{7}$$

where

$\mathbf{Y} \in \mathbb{C}^{M_r \times T}$	received code matrix at pth code block;
$\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$	MIMO channel matrix;
M_r	number of receiver antennas;
P	frame length or number of code blocks in which the channel remains static;
$\mathbf{s}_p \in \{\pm 1\}^K$	block of information bits transmitted at the pth code block;
$\mathbf{V}_p \in \mathbb{C}^{M_r \times T}$	additive white Gaussian noise (AWGN) matrix.

Let

$$\mathbf{S} = [\ \mathbf{s}_1, \ldots, \mathbf{s}_P\ ] \in \{\pm 1\}^{K \times P}. \tag{8}$$

In the blind or noncoherent scenario, a usual assumption is that $\mathbf{H}$ is a deterministic unknown. The respective blind ML detector is shown to be [10], [13]

$$\{\hat{\mathbf{H}}, \hat{\mathbf{S}}\} = \arg \min_{\substack{\tilde{\mathbf{H}} \in \mathbb{C}^{M_r \times M_t}, \\ \tilde{\mathbf{S}} \in \{\pm 1\}^{K \times P}}} \sum_{p=1}^{P} \|\mathbf{Y}_p - \tilde{\mathbf{H}}\mathbf{C}(\tilde{\mathbf{s}}_p)\|_F^2 \tag{9}$$

where the unknown $\mathbf{H}$ and $\mathbf{S}$ are estimated jointly. Here $\|.\|_F$ stands for the Frobenius norm. If $\mathbf{C}(.)$ is a generic linear STBC function, then solving (9) is challenging due to the biconvexity of the objective function and the ± 1 constraints on $\mathbf{S}$. When $\mathbf{C}(.)$ is an OSTBC, one can however exploit the linear dispersion and orthogonal structures to simplify the process of solving Problem (9), either optimally or suboptimally. As discussed in the introduction, the presently available algorithms for handling (9) include the closed-form method [2], [16] (also [14]), the cyclic ML method [2], [13], SDR and sphere decoding [14]. Some performance and complexity comparisons of the various algorithms have been presented in the prequel of this work [14].

C. Blind Identifiability Problem Statement

The implementation simplicity of blind ML OSTBC detection motivates us to investigate the blind identifiability aspects. For ease of exposition of the identifiability problem, suppose that the true channel $\mathbf{H}$ and data matrix $\mathbf{S}$ is a solution of the blind ML problem in (9). This solution is unique only when we cannot find another solution, denoted by $\{\tilde{\mathbf{H}}, \tilde{\mathbf{S}}\}$, such that the following channel-code ambiguity equations are satisfied

$$\mathbf{H}\mathbf{C}(\mathbf{s}_p) = \tilde{\mathbf{H}}\mathbf{C}(\tilde{\mathbf{s}}_p), \qquad p = 1, \ldots, P. \tag{10}$$

An obvious situation leading to (10) is when $\{\tilde{\mathbf{H}}, \tilde{\mathbf{S}}\} = \{-\mathbf{H}, -\mathbf{S}\}$. In practice this sign ambiguity problem can be easily resolved by a number of ways; e.g., using channel coding [10], or setting one element of $\mathbf{S}$ to be a pilot. Throughout this paper we are interested in examining other possible ambiguities, and in finding OSTBCs that can avoid those situations.

Before proceeding to present our main results in the ensuing sections, we describe a blind OSTBC identifiability condition obtained by applying a result due to Talwar *et al.* [10]. The result was developed for proving sufficient blind identifiability conditions of the spatial multiplexing scheme, and its essence is summarized as a lemma stated as follows:

Lemma 1 (Talwar-Viberg-Paulraj) *Let* $\mathbf{F} \in \mathbb{R}^{M\times K}$ *and* $\mathbf{S} = [\ \mathbf{s}_1, \ldots, \mathbf{s}_P\ ] \in \{\pm 1\}^{K\times P}$. *Suppose that* $\mathbf{F}$ *has full column rank, and that the columns of* $\mathbf{S}$ *contain at least* 2^{K-1} *distinct bit vectors*[2]. *The equations*

$$\mathbf{F}\mathbf{s}_p = \tilde{\mathbf{F}}\tilde{\mathbf{s}}_p, \qquad p = 1, \ldots, P \tag{11}$$

are satisfied for some $\{\tilde{\mathbf{F}}, \tilde{\mathbf{S}}\} \in \mathbb{C}^{M\times K} \times \{\pm 1\}^{K\times P}$ *only when*

$$\mathbf{\Pi}\mathbf{D}\mathbf{S} = \tilde{\mathbf{S}}, \qquad \mathbf{F}\mathbf{D}\mathbf{\Pi}^T = \tilde{\mathbf{F}}, \tag{12}$$

where $\mathbf{\Pi} \in \{0, 1\}^{K\times K}$ *is a permutation matrix and* $\mathbf{D} \in \mathbb{R}^{K\times K}$ *is diagonal with* $\mathrm{diag}(\mathbf{D}) \in \{\pm 1\}^K$.

Now, suppose that the channel-code ambiguity equations in (10) are satisfied. By applying a standard vectorization property [32], Eq. (10) can be reexpressed as

$$(\mathbf{I}_T \otimes \mathbf{H})\boldsymbol{\mathcal{X}}\mathbf{s}_p = (\mathbf{I}_T \otimes \tilde{\mathbf{H}})\boldsymbol{\mathcal{X}}\tilde{\mathbf{s}}_p, \qquad p = 1, \ldots, P, \tag{13}$$

where $\mathbf{I}_n$ is the $n \times n$ identity matrix, $\otimes$ is the Kronecker product,

$$\boldsymbol{\mathcal{X}} = [\ \mathrm{vec}(\mathbf{X}_1), \ldots, \mathrm{vec}(\mathbf{X}_K)\ ] \in \mathbb{C}^{M_t T\times K}, \tag{14}$$

and $\mathrm{vec}(.)$ is the vectorization. Let us define an operator, denoted by overline, so that $\overline{\mathbf{A}} = [\ \mathrm{Re}\{\mathbf{A}\}^T\ \mathrm{Im}\{\mathbf{A}\}^T\ ]^T$. Eq. (13) can be rewritten as

$$\mathbf{F}\mathbf{s}_p = \tilde{\mathbf{F}}\tilde{\mathbf{s}}_p, \qquad p = 1, \ldots, P, \tag{15}$$

where $\mathbf{F} = \overline{(\mathbf{I}_T \otimes \mathbf{H})\boldsymbol{\mathcal{X}}} \in \mathbb{R}^{2M_r T\times K}$ and $\tilde{\mathbf{F}} = \overline{(\mathbf{I}_T \otimes \tilde{\mathbf{H}})\boldsymbol{\mathcal{X}}} \in \mathbb{R}^{2M_r T\times K}$. It can be shown that $\mathbf{F}$ is of full column rank for every nonzero $\mathbf{H}$; see for example [16]. Applying Lemma 1 to (15), we obtain the following identifiability condition:

Lemma 2 *Suppose that the columns of* $\mathbf{S}$ *contain at least* 2^{K-1} *distinct bit vectors. Given every nonzero* $\mathbf{H} \in \mathbb{C}^{M_r\times M_t}$ *and an arbitrary OSTBC* $\mathbf{C}(.)$, *the equations*

$$\mathbf{H}\mathbf{C}(\mathbf{s}_p) = \tilde{\mathbf{H}}\tilde{\mathbf{C}}(\tilde{s}_p), \qquad p = 1, \ldots, P \tag{16}$$

are satisfied for some $\{\tilde{\mathbf{H}}, \tilde{\mathbf{S}}\} \in \mathbb{C}^{M_r\times M_t} \times \{\pm 1\}^{K\times P}$ *only when*

$$\mathbf{\Pi}\mathbf{D}\mathbf{S} = \tilde{\mathbf{S}}, \tag{17}$$

where $\mathbf{\Pi} \in \{0, 1\}^{K\times K}$ *is a permutation matrix and* $\mathbf{D} \in \mathbb{R}^{K\times K}$ *is diagonal with* $\mathrm{diag}(\mathbf{D}) \in \{\pm 1\}^K$.

[2]Here, two vectors $\mathbf{a}$ and $\mathbf{b}$ are said to be distinct if $\mathbf{a} \neq \pm\mathbf{b}$. A vector $\mathbf{a}$ is said to be a bit vector of dimension n if $\mathbf{a} \in \{\pm 1\}^n$.

Lemma 2 shows that OSTBCs are uniquely identifiable up to permutations and sign changes in the rows of $\mathbf{S}$, under a mild assumption on $\mathbf{S}$. In the next sections we will illustrate a number of even more interesting results, in which we find OSTBCs that can be uniquely identifiable up to a sign only.

III. Non-Rotatability and Blind Identifiability

This section shows that there is a class of OSTBCs, called rotatable OTSBCs, that fails to provide unique blind identification up to a sign. This problem motivates us to consider non-rotatable OSTBCs and their characteristics. In particular, it is proven that non-rotatable OSTBCs can achieve unique identification up to a sign, with probability 1. In the first subsection, we describe rotatable OSTBCs . Then, non-rotatable OSTBCs and their identifiability conditions are studied in the second and third subsections, respectively.

A. The Code Rotation Problem

The following is the definition of rotatable OSTBCs:

Definition 1 *An OSTBC $\mathbf{C}(.)$ is said to be rotatable if there exists a matrix $\mathbf{Q} \in \mathbb{C}^{M_t \times M_t}$ such that for any $\mathbf{s} \in \{\pm 1\}^K$,*

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\tilde{\mathbf{s}}) \tag{18}$$

for some $\tilde{\mathbf{s}} \in \{\pm 1\}^K$, $\tilde{\mathbf{s}} \neq \pm \mathbf{s}$. Otherwise, $\mathbf{C}(.)$ is said to be non-rotatable. Such a $\mathbf{Q}$, if exists, is called a code rotation matrix.

A code rotation matrix is unitary: if (18) is true then

$$\mathbf{Q}\mathbf{Q}^H = \frac{1}{K}\mathbf{Q}\mathbf{C}(\mathbf{s})\mathbf{C}(\mathbf{s})^H\mathbf{Q}^H \tag{19}$$

$$= \frac{1}{K}\mathbf{C}(\tilde{\mathbf{s}})\mathbf{C}(\tilde{\mathbf{s}})^H = \mathbf{I}, \tag{20}$$

where we have used the row orthogonality $\mathbf{C}(\mathbf{s})\mathbf{C}(\mathbf{s})^H = \|\mathbf{s}\|_2^2\mathbf{I}$ in the above equations. Moreover, if $\mathbf{Q}$ is a code rotation matrix then $-\mathbf{Q}$ is also a code rotation matrix. The problem with rotatable OSTBCs is that for each code rotation matrix $\mathbf{Q}$, the channel-code ambiguity equations

$$\mathbf{H}\mathbf{C}(\mathbf{s}_p) = \mathbf{H}\mathbf{Q}^H\mathbf{Q}\mathbf{C}(\mathbf{s}_p) = (\mathbf{H}\mathbf{Q}^H)\mathbf{C}(\tilde{\mathbf{s}}_p) \tag{21}$$

are satisfied for some $\tilde{\mathbf{s}}_p \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}_p\}$, $p = 1, \ldots, P$. Thus, rotatable codes always result in ambiguity. Indeed, the well-known Alamouti code is rotatable as illustrated in the following example:

Example 1 Consider the real-valued Alamouti code [18] where $M_t = T = K = 2$:

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{bmatrix}. \tag{22}$$

Its basis matrices are given by

$$\mathbf{X}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{X}_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{23}$$

Let $\mathbf{Q} = \mathbf{X}_2$. Since $\mathbf{Q}\mathbf{X}_1 = \mathbf{X}_2$ and $\mathbf{Q}\mathbf{X}_2 = -\mathbf{X}_1$, we have

$$\mathbf{Q}\mathbf{C}([\ s_1\ s_2\ ]^T) = \mathbf{C}([\ -s_2\ s_1\ ]^T) \tag{24}$$

Hence, this code is rotatable. Similarly, it can be verified that the complex-valued Alamouti code

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} u_1 & -u_2^* \\ u_2 & u_1^* \end{bmatrix} \tag{25}$$

where $u_1 = s_1 + js_3$ and $u_2 = s_2 + js_4$, is rotatable. □

The following theorem shows a sufficient and necessary condition of rotatable OSTBCs.

Theorem 1 *The following statements are equivalent:*

i) $\mathbf{C}(.)$ *is a rotatable OSTBC.*

ii) *There exist* $\mathbf{Q} \in \mathbb{C}^{M_t \times M_t}$ *satisfying*

$$\mathbf{Q}\mathbf{X}_k = d_k \mathbf{X}_{i_k}, \qquad k = 1, \ldots, K, \tag{26}$$

where $d_k \in \{\pm 1\}$*, and* $i_k \in \{1, \ldots, K\}$ *is an index with* $i_k \neq k$ *and* $i_k \neq i_\ell$ *for* $k \neq \ell$*.*

iii) *There exist* $\mathbf{Q} \in \mathbb{C}^{M_t \times M_t}$ *satisfying*

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\mathbf{\Pi}\mathbf{D}\mathbf{s}), \tag{27}$$

where $\mathbf{\Pi} \in \{0,1\}^{K \times K}$ *is a permutation matrix with* $\mathrm{diag}(\mathbf{\Pi}) = \mathbf{0}$*, and* $\mathbf{D}$ *is diagonal with* $\mathrm{diag}(\mathbf{D}) \in \{\pm 1\}^K$.

It is straightforward that Statements ii) and iii) are equivalent, and that if Statement ii) or iii) is true then Statement i) is true. But it is not as obvious that Statement i) implies Statements ii) and iii). The proof of this part is given in Appendix A. Theorem 1 indicates that a rotatable OSTBC always exhibits permutation ambiguities.

Let us consider some implication of Theorem 1. The equivalent rotatable code condition in (26) implies $\mathbf{Q} = d_k \mathbf{X}_{i_k} \mathbf{X}_k^H$ for all $k = 1, \ldots, K$ (due to $\mathbf{X}_k \mathbf{X}_k^H = \mathbf{I}$). Hence, we have the following necessary code rotation condition:

Corollary 1 *A code rotation matrix* $\mathbf{Q}$*, if exists, must be one of the following candidates*

$$\left\{ \pm \mathbf{X}_2 \mathbf{X}_1^H, \pm \mathbf{X}_3 \mathbf{X}_1^H, \ldots, \pm \mathbf{X}_K \mathbf{X}_1^H \right\}. \tag{28}$$

Corollary 1 is useful in facilitating the numerical inspection of code rotatability: We only need to check the $K - 1$ possibilities of $\mathbf{Q}$ in (28) instead of the considerably larger possibilities in (18).

The following example illustrates two non-rotatable OSTBCs:

Example 2 Consider the following complex maximal-rate code with $M_t = 3$, $T = 4$, and $K/2 = 3$ [19]:

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} u_1 & -u_2^* & -u_3^* & 0 \\ u_2 & u_1^* & 0 & -u_3^* \\ u_3 & 0 & u_1^* & u_2^* \end{bmatrix} \tag{29}$$

where $u_k = s_k + j s_{k+K/2}$. Its basis matrices are

$$\mathbf{X}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \mathbf{X}_2 = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{30}$$

$$\mathbf{X}_3 = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \mathbf{X}_4 = \begin{bmatrix} j & 0 & 0 & 0 \\ 0 & -j & 0 & 0 \\ 0 & 0 & -j & 0 \end{bmatrix}, \tag{31}$$

$$\mathbf{X}_5 = \begin{bmatrix} 0 & j & 0 & 0 \\ j & 0 & 0 & 0 \\ 0 & 0 & 0 & -j \end{bmatrix}, \mathbf{X}_6 = \begin{bmatrix} 0 & 0 & j & 0 \\ 0 & 0 & 0 & j \\ j & 0 & 0 & 0 \end{bmatrix} \tag{32}$$

If $\mathbf{C}(.)$ is rotatable, then from (26) the condition

$$\mathbf{Q}\mathbf{X}_1 = \mathbf{X}_i \tag{33}$$

must be satisfied for some $\mathbf{Q}$ and $i \neq 1$. By observing the basis matrices, we see that there does not exist $\mathbf{Q}$ satisfying (33) for all $i \neq 4$: The 4th column of $\mathbf{X}_1$ is all zero, while the 4th column of $\mathbf{X}_i$ for $i \neq 4$ is not. It is impossible find a $\mathbf{Q}$ such that the 4th column of $\mathbf{Q}\mathbf{X}_1$ is a nonzero vector. Now the

problem remained is the case of $i = 4$. Eq. (33) is satisfied for $i = 4$, but by inspection we found that the resultant $\mathbf{Q} = \mathbf{X}_4\mathbf{X}_1^H$ does not satisfy (26) for all k. We conclude that the code in (29) is non-rotatable.

In a similar way, we found that the following 3×4 real full-rate OSTBC [18]

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} s_1 & -s_2 & -s_3 & -s_4 \\ s_2 & s_1 & s_4 & -s_3 \\ s_3 & -s_4 & s_1 & s_2 \end{bmatrix} \tag{34}$$

is non-rotatable. □

Remark 2. It is commonly thought that for an STBC with complex constellations, blind detection is always subject to a phase rotation in the detected symbols. Example 2 shows an interesting example where the complex code in (29) is subject only to a sign change (assuming the QPSK constellation). This is attributed to the salient characteristic that the entries of the code matrix contain the complex symbols and their conjugates, thereby giving the code some form of immunity to phase rotations.

B. Non-Rotatable and Strictly Non-Rotatable Codes

While the development above shows that rotatable OSTBCs are always susceptible to code ambiguities, an interesting question is whether the ambiguities can be avoided by using non-rotatable OSTBCs. We notice from Definition 1 that for a non-rotatable code, there does not exist a unitary $\mathbf{Q}$ such that

$$\mathbf{Q}\mathbf{C}(\mathbf{s}') = \mathbf{C}(\mathbf{s}''), \qquad \mathbf{s}'' \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}'\} \tag{35}$$

can be satisfied for *every* $\mathbf{s}' \in \{\pm 1\}^K$. The non-rotatable code definition, however, does not rule out the possibility that (35) can be satisfied for *some* $\mathbf{s}' \in \{\pm 1\}^K$. Suppose that $\mathbf{C}(.)$ is non-rotatable but satisfies (35) for two particular distinct bit vectors $\mathbf{s}', \mathbf{s}''$. Then, one can verify that the equations

$$\mathbf{Q}\mathbf{C}(\mathbf{s}_p) = \mathbf{C}(\tilde{\mathbf{s}}_p), \quad \tilde{\mathbf{s}}_p \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}_p\} \tag{36}$$

for $p = 1, \ldots, P$ may not be satisfied for every $\mathbf{S} \in \{\pm 1\}^{K \times P}$, but is satisfied when $\mathbf{S} = \pm[\ \mathbf{s}', \mathbf{s}', \ldots, \mathbf{s}'\ ]$ or when $\mathbf{S} = \pm[\ \mathbf{s}'', \mathbf{s}'', \ldots, \mathbf{s}''\ ]$. Nevertheless, one would argue intuitively that when P increases, such a situation is unlikely to happen. This is in fact true, and to illustrate this we consider the following assumption:

A1) The columns of $\mathbf{S} \in \{\pm 1\}^{K \times P}$ contains at least 2^{K-1} distinct bit vectors.[3]

To satisfy $\mathbf{A1})$ it is necessary that $P \geq 2^{K-1}$. For sufficiently large P there is a high probability that $\mathbf{A1})$ holds [10], given the standard assumption that each element of $\mathbf{S} \in \{\pm 1\}^{K \times P}$ is i.i.d. and uniform distributed. The following property shows that if $\mathbf{A1})$ is true then code rotation ambiguity is impossible:

Property 1 *If* $\mathbf{C}(.)$ *is non-rotatable and* **A1)** *is satisfied, then there does not exist a* $\mathbf{Q}$ *such that*

$$\mathbf{Q}\mathbf{C}(\mathbf{s}_p) = \mathbf{C}(\tilde{\mathbf{s}}_p), \quad \tilde{\mathbf{s}}_p \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}_p\} \tag{37}$$

for all $p = 1, \ldots, P$.

Proof: Suppose that (37) is satisfied for all $p = 1, \ldots, P$, and without loss of generality assume that $\mathbf{S}$ contains exactly 2^{K-1} distinct bit vectors. Then we have $\{\pm \mathbf{s}_1, \ldots, \pm \mathbf{s}_P\} = \{\pm 1\}^K$, and subsequently

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\tilde{\mathbf{s}}), \quad \tilde{\mathbf{s}} \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}\} \tag{38}$$

can be satisfied for every $\mathbf{s} \in \{\pm 1\}^K$. By Definition 1 such an OSTBC is rotatable. ■

A simulation example verifying Property 1 is as follows.

Example 3 We simulated a noise free situation

$$\mathbf{Y}_p = \mathbf{H}\mathbf{C}(\mathbf{s}_p), \qquad p = 1, \ldots, P$$

where $\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$ is zero-mean i.i.d. circular Gaussian distributed, and $\mathbf{S} \in \{\pm 1\}^{K \times P}$ is i.i.d. and uniform distributed. The code function used is (29), which has been shown to be non-rotatable. The number of receiver antennas is $M_r = 1$. We applied a blind SDR-ML detector [14] to obtain an ML decision $\hat{\mathbf{S}}$ from the observation $\{\mathbf{Y}_p\}_{p=1}^P$. From Property 1, we expect that the error probability $\Pr[\, \hat{\mathbf{S}} \neq \pm \mathbf{S} \,]$ should decrease with P particularly for $P \gg 2^{K-1}$. Fig. 1 plots the error probability versus P. The results in the figure confirm our expectation. It is also interesting to see that the error probability in Fig. 1 approaches zero for $P > 3$, which is far less than $2^{K-1} = 32$. This implies that $\mathbf{A1})$ is a conservative sufficient condition for avoiding code rotation ambiguities.

This simulation example also reveals that for an i.i.d. Gaussian channel, non-rotatable OSTBCs with large P can achieve unique identifiability with a probability that is almost 1. This aspect is further analyzed in the next subsection. □

[3]As an aside, $\mathbf{A1})$ usually serves as one of the sufficient blind identifiability conditions for some MIMO/STBC schemes such as spatial multiplexing [10] and Khatri-Rao space-time coding [11].

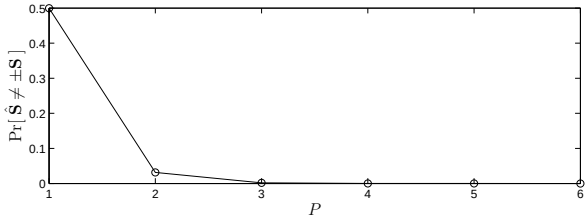


Fig. 1. Error probability in the absence of noise. $M_r = 1$; number of simulation trials= $100,000$.

On the other hand, there exists a subclass of non-rotatable OSTBCs that exhibits better immunity to the code rotation ambiguities. Its definition is as follows:

Definition 2 *An OSTBC* $\mathbf{C}(.)$ *is said to be strictly non-rotatable if there does not exist a matrix* $\mathbf{Q} \in \mathbb{C}^{M_t \times M_t}$ *such that*

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\tilde{\mathbf{s}}) \tag{39}$$

for any $\mathbf{s}, \tilde{\mathbf{s}} \in \{\pm 1\}^K$, $\tilde{\mathbf{s}} \neq \pm\mathbf{s}$.

It is clear from the definition that a strictly non-rotatable OSTBC does not suffer from the rotation ambiguity problem in (36), even for $P = 1$. Let $\mathcal{R}(\mathbf{A})$ denote the range space of $\mathbf{A}$. The following code property is a direct consequence of matrix analysis results [33]:

Property 2 *An OSTBC* $\mathbf{C}(.)$ *is strictly non-rotatable if and only if*

$$\mathcal{R}(\mathbf{C}^T(\mathbf{s})) \neq \mathcal{R}(\mathbf{C}^T(\tilde{\mathbf{s}})) \tag{40}$$

for any $\mathbf{s}, \tilde{\mathbf{s}} \in \{\pm 1\}^K$, $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$.

From Property 2 we infer that

Property 3 *All strictly non-rotatable OSTBCs have* $M_t < T$.

Strictly non-rotatable codes exist, at least for the real case:

Theorem 2 *If* M_t *is odd and* $\mathbf{C}(.)$ *is real valued, then* $\mathbf{C}(.)$ *is strictly non-rotatable.*

The proof of the above theorem is shown in Appendix B. Table II shows the rotatability of various real-valued OSTBCs. The results were obtained by numerical inspection. To check non-rotatability, the fast numerical inspection idea in Corollary 1 was used. As for checking strict non-rotatability, an

exhaustive inspection procedure following Definition 2 was used. Table II illustrates that real-valued OSTBCs are indeed strictly non-rotatable for odd M_t. In Table III we show the rotatability of various complex-valued OSTBCs. As a minor remark, the strict non-rotatability of the complex OSTBC with $(T, M_t, K/2) = (15, 5, 10)$ is marked 'not known' in Table III, because the number of possibilities involved (i.e., $(2^{K-1})^2 = 4^{19}$ combinations) is computationally too ovewhelming. It is interesting to see that in contrast to the real case, a complex-valued OSTBC with odd M_t is not necessarily strictly non-rotatable.

TABLE II

ROTATABILITY OF VARIOUS REAL-VALUED OSTBCS. MOST CODES CAN BE FOUND IN [18].

(T, M_t, K) real OSTBC	non-rotatable?	strictly non-rotatable?
$(2, 2, 2)$	no	no
$(4, 3, 4)$	yes	yes
$(4, 4, 4)$	no	no
$(8, 5, 8)$	yes	yes
$(8, 6, 8)$	yes	no
$(8, 7, 8)$	yes	yes
$(8, 8, 8)$	yes	no

TABLE III

ROTATABILITY OF VARIOUS COMPLEX-VALUED OSTBCS.

$(T, M_t, K/2)$ complex OSTBC	origin, & remarks	non-rotatable?	strictly non-rotatable?
$(2, 2, 2)$	Alamouti	no	no
$(4, 3, 3)$	[20, Eq. (3.1)]; GOD	yes	no
$(4, 4, 3)$	[20, Eq. (3.1)]; GOD	yes	no
$(4, 4, 3)$	[18, Eq. (40)]; sporadic	yes	no
$(15, 5, 10)$	[21, Eq. (100)]; GOD	yes	not known
$(8, 5, 4)$	[22, Eq. (8)]; GOD	yes	yes
$(8, 6, 4)$	[22, Eq. (8)]; GOD	yes	yes
$(8, 7, 4)$	[22, Eq. (8)]; GOD	yes	no
$(8, 8, 4)$	[22, Eq. (8)]; GOD	yes	no

Remark 3. Tables II and III show that many existing OSTBCs are rotatable, particularly when M_t is even. This leads to a natural question of how to obtain a non-rotatable or strictly non-rotatable OSTBC, fixing an M_t. This aspect will be further addressed in Section IV.

C. Identifiability Conditions

Using non-rotatable or strictly non-rotatable OSTBCs is a necessary condition for unique identifiability up to a sign, as shown in the last subsections. Now, an interesting question is what are the sufficient

identifiability conditions for these two code classes. Consider a standard MIMO assumption given as follows:

A2) The channel matrix $\mathbf{H}$ is complex circular Gaussian distributed, possibly with nonzero mean and with correlated entries.

Note that $\mathbf{A2})$ encompasses the popular i.i.d. Rayleigh channel model (or, equivalently, the i.i.d. zero-mean Gaussian channel model). Let $\mathbf{h}_i$ denotes the ith row of $\mathbf{H}$; i.e.,

$$\mathbf{H}^T = [\ \mathbf{h}_1, \ldots, \mathbf{h}_{M_r}\ ]. \tag{41}$$

A blind identifiability condition is as follows:

Theorem 3 *Suppose that* $\mathbf{C}(.)$ *is non-rotatable. Under* **A2)**, $\mathbf{S}$ *is uniquely identifiable up to a sign (UIUTS) with probability* 1 *if*

1) *one of the covariance matrices* $\mathrm{cov}(\mathbf{h}_1), \ldots, \mathrm{cov}(\mathbf{h}_{M_r})$ *is positive definite, and*
2) $\mathbf{A1})$ *holds.*

In addition, the same condition holds without requiring **A1)** *if the code is strictly non-rotatable.*

The proof of this theorem is given in Appendix C. A direct consequence of Theorem 3 is as follows:

Corollary 2 *For i.i.d. Rayleigh channels, non-rotatable OSTBCs are UIUTS with probability* 1 *if* **A1)** *holds. The same condition holds without requiring* **A1)** *if the code is strictly non-rotatable.*

Theorem 3 gives the important implication that for many random Gaussian channel fading models, it is almost impossible for strictly non-rotatable OSTBCs to encounter ambiguity given every $P \geq 1$ and $\mathbf{S} \in \{\pm 1\}^{K \times P}$. As for non-rotatable OSTBCs, the same identifiability condition usually holds for a sufficiently large data length P, where there is a high chance that **A1)** holds (c.f., the discussion after **A1)**). We should also point out that Theorem 3 places no restriction on the number of receiver antennas M_r. Hence, the probability 1 blind identifiability result holds even in multiple-input-single-output (MISO) systems. In fact, the simulation in Example 3 serves as a testimony to this attractive identifiability result.

As a side product of proving Theorem 3, we found in Appendix C that

Lemma 3 *For any full column rank* $\mathbf{H}$*, non-rotatable OSTBCs are always UIUTS if* **A1)** *holds. The same condition holds without requiring* **A1)** *if the code is strictly non-rotatable.*

Lemma 3 is not as profound as Theorem 3, but it is interesting because not all MIMO/STBC scheme can be UIUTS given a full column rank channel; e.g., spatial multiplexing [10]. (It should be noted, though, that spatial multiplexing can be uniquely identifiable up to a permutation.)

IV. Non-Intersecting Subspaces, Perfect Identifiability, and Code Construction

This section considers construction of OSTBCs with good blind identifiability. This development is motivated by the fact that many existing OSTBCs are rotatable, as noticed in the previous section. We examine a subclass of strictly non-rotatable OSTBCs, viz. the non-intersecting subspace (NIS). This class of OSTBCs exhibits 'perfect' blind identifiability, in the sense that the codes are uniquely identifiable up to a sign for *every* nonzero channel and data matrix. The disadvantage of NIS-OSTBCs, though, is data rate reduction (under some standard assumption). All these aspects are described in the first subsection. In the second subsection, we propose a simple code construction procedure that can convert the existing OSTBCs to NIS-OSTBCs. In the third subsection, we describe a simple way of reducing the rate loss problem in NIS-OSTBC.

A. Non-Intersecting Subspace OSTBCs

The class of NIS-OSTBCs is defined as follows:

Definition 3 *An OSTBC is said to be a non-intersecting subspace (NIS) OSTBC if*

$$\mathcal{R}(\mathbf{C}^T(\mathbf{s})) \cap \mathcal{R}(\mathbf{C}^T(\tilde{\mathbf{s}})) = \{\mathbf{0}\} \tag{42}$$

for every $\mathbf{s}, \tilde{\mathbf{s}} \in \{\pm 1\}^K$, $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$.

The NIS concepts were introduced in the noncoherent space-time coding literature [34] for achieving the maximum *noncoherent spatial diversity* [3], [5] in an i.i.d. Rayleigh channel. However, up to this point there is no study regarding the existence and construction of NIS-OSTBCs. An NIS-OSTBC is strictly non-rotatable [compare (42) and Property 2], but the vice versa is not true. Moreover, NIS-OSTBCs have an additional constraint on the code length:

Property 4 *All NIS-OSTBCs have* $2M_t \leq T$.

Property 4 can be proven using standard matrix results [33], [35]. In contrast, strictly non-rotatable codes require $M_t < T$ only (Property 3). We found that many existing OSTBCs do not satisfy Property 4, let alone being NIS.

The following theorem shows that NIS-OSTBCs are 'perfect' from a blind identifiability standpoint:

Theorem 4 *Given every nonzero channel channel* $\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$ *and data matrix* $\mathbf{S} \in \{\pm 1\}^{K \times P}$, $\mathbf{S}$ *is UIUTS if and only if* $\mathbf{C}(.)$ *is an NIS-OSTBC.*

Proof: One can easily show that to be UIUTS for any $\mathbf{S} \in \{\pm 1\}^{K \times P}$ and nonzero $\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$, it is sufficient and necessary that the following statement holds: For every pair of distinct bit vectors $\mathbf{s}, \tilde{\mathbf{s}}$, the condition

$$\mathbf{h}^T \mathbf{C}(\mathbf{s}) = \tilde{\mathbf{h}}^T \mathbf{C}(\tilde{\mathbf{s}}) \tag{43}$$

cannot be satisfied by any $\mathbf{h}$, $\tilde{\mathbf{h}} \in \mathbb{C}^{M_t} \setminus \{\mathbf{0}\}$. By noting that

$$\begin{aligned} &\mathcal{R}(\mathbf{C}^T(\mathbf{s})) \cap \mathcal{R}(\mathbf{C}^T(\tilde{\mathbf{s}})) \\ &\quad = \left\{ \mathbf{y} \;\middle|\; \mathbf{y} = \mathbf{C}^T(\mathbf{s})\mathbf{h} = \mathbf{C}^T(\tilde{\mathbf{s}})\tilde{\mathbf{h}}, \quad \mathbf{h}, \tilde{\mathbf{h}} \in \mathbb{C}^{M_t} \right\} \end{aligned} \tag{44}$$

and by comparing (44) and (43), we have the conclusion that the condition in (43) is equivalent to have $\mathcal{R}(\mathbf{C}^T(\mathbf{s})) \cap \mathcal{R}(\mathbf{C}^T(\tilde{\mathbf{s}})) = \{\mathbf{0}\}$ for any $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$. ■

There is a price for employing the NIS-OSTBCs, however.

Lemma 4 *Suppose that* $\mathbf{C}(.)$ *is based on real or complex GODs (see Remark 1, Section II-A for the descriptions regarding GODs). If* $\mathbf{C}(.)$ *is also an NIS-OSTBC, then it does not achieve the full rate; i.e.,* $K < T$ *for real GODs and* $K/2 < T$ *for complex GODs.*

The proof of Lemma 4 is given in Appendix D. Lemma 4 has more impacts on the real case, because full-rate real GODs exist for any M_t while full-rate complex GODs exist only for $M_t = 2$ [18], [21].

B. A Simple NIS Code Construction

We use the hints provided by Property 4 and Lemma 4 to come up with the following OSTBC construction:

Construction I:

Given an OSTBC function $\mathbf{C}_o(\mathbf{s}) = \sum_{k=1}^{K} s_k \mathbf{X}_k \in \mathbb{C}^{M_t \times T}$, where K is even.

Step 1. Set $\mathbf{C}_1(\mathbf{s}) = \sum_{k=1}^{K-1} s_k \mathbf{X}_k$.

Step 2. Output $\mathbf{C}_{new}(\mathbf{s}) = [\ \mathbf{C}_1(\boldsymbol{\mu})\ \ \mathbf{C}_o(\boldsymbol{\nu})\ ] \in \mathbb{C}^{M_t \times 2T}$ as the new OSTBC, where $\boldsymbol{\mu} = [\ s_1, \ldots, s_{K-1}\ ]^T$ and $\boldsymbol{\nu} = [\ s_K, \ldots, s_{2K-1}\ ]^T$.

Note that that most OSTBCs have a even K. In the above construction we concatenate two OSTBCs, thereby forming a longer code that satisfies Property 4. Moreover, we drop 1 bit so as not to enable full rate; cf., Lemma4. Surprisingly, by doing so it is sufficient to obtain an NIS-OSTBC:

Theorem 5 *Given any OSTBC function* $\mathbf{C}_o : \mathbb{R}^K \to \mathbb{C}^{M_t \times T}$ *where* K *is even, the code generated by Construction I is an NIS-OSTBC.*

The proof of this theorem is described in Appendix E. It is interesting to look at some examples of NIS-OSTBCs from Construction I. For $M_t = 2$, we convert the real-valued Alamouti code to the following NIS-OSTBC

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} s_1 & 0 & s_2 & -s_3 \\ 0 & s_1 & s_3 & s_2 \end{bmatrix}. \tag{45}$$

For the complex counterpart, let us define

$$u_{k,\ell} = s_k + j s_\ell \tag{46}$$

for notational simplicity. The following NIS-OSTBC is established from the complex Alamouti code:

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} u_{1,3} & -s_2 & u_{4,6} & -u_{5,7}^* \\ s_2 & u_{1,3}^* & u_{5,7} & u_{4,6}^* \end{bmatrix}. \tag{47}$$

It is interesting to note that the new OSTBC contains both BPSK and QPSK symbols, because Construction I drops the imaginary part of one complex symbol. For $M_t = 3$, we obtain the following real NIS-OSTBC from (34)

$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} s_1 & -s_2 & -s_3 & 0 & s_4 & -s_5 & -s_6 & -s_7 \\ s_2 & s_1 & 0 & -s_3 & s_5 & s_4 & s_7 & -s_6 \\ s_3 & 0 & s_1 & s_2 & s_6 & -s_7 & s_4 & s_5 \end{bmatrix}. \tag{48}$$

Similarly, from (29) we construct a complex 3×8 NIS-OSTBC

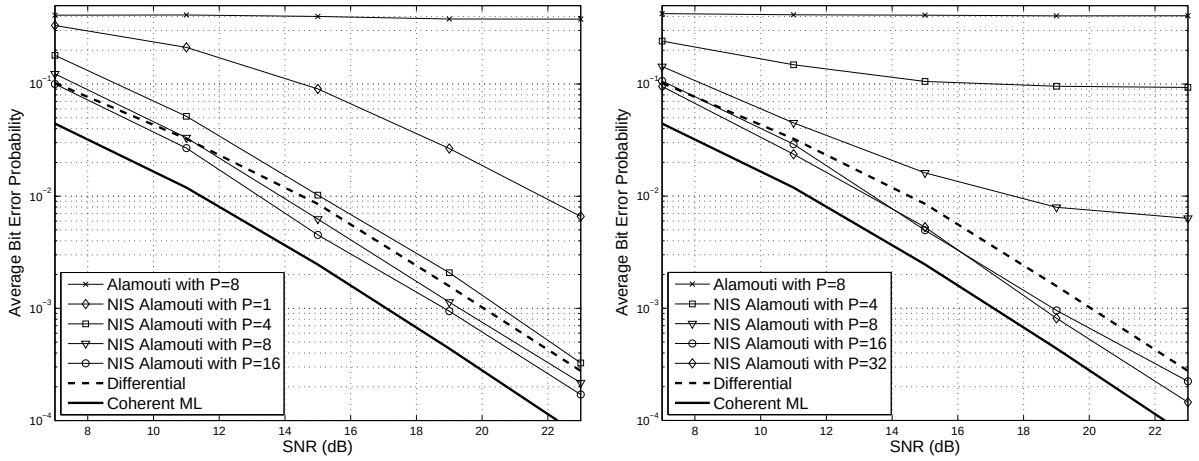
$$\mathbf{C}(\mathbf{s}) = \begin{bmatrix} u_{1,4} & -u_{2,5}^* & -s_3 & 0 & u_{6,9} & -u_{7,10}^* & -u_{8,11}^* & 0 \\ u_{2,5} & u_{1,4}^* & 0 & -s_3 & u_{7,10} & u_{6,9}^* & 0 & -u_{8,11}^* \\ s_3 & 0 & u_{1,4}^* & u_{2,5}^* & u_{8,11} & 0 & u_{6,9}^* & u_{7,10}^* \end{bmatrix}. \tag{49}$$

A simulation example verifying the theoretical results is as follows.

Example 4 We consider the QPSK Alamouti code, and its NIS counterpart in (47). In the simulation the number of receiver antennas is $M_r = 1$, and the channel is i.i.d. zero-mean Gaussian distributed. The sign ambiguity effect is eliminated by assuming that one of the bit symbols is known at the receiver.

Fig. 2(a) shows the bit error performance of the original Alamouti code and the NIS Alamouti code when the blind SDR-ML receiver [14] is used. As a reference we also plotted the performance of the corresponding coherent and differential [8], [9] Alamouti schemes. In the figure, we see that the original Alamouti code fails to provide consistent performance with respect to the SNRs. This is because the Alamouti code is rotatable. In contrast, the performance of the NIS Alamouti code is promising: First, we observe that for all the values of P tested, the bit error probability asymptotically decays at the same rate as that of the coherent ML. This gives an implication that the NIS code achieves the full noncoherent spatial diversity, from a viewpoint of noncoherent space-time code performance analysis [5]. Second, the bit error rate improves as P increases. For $P = 16$, the NIS Alamouti code attains a performance that is 1dB better (in terms of the SNR) than the differential Alamouti scheme.

SDR-ML is only one of the effective alternatives to blind detection. In Fig. 2(b), the performance of another blind receiver, namely the cyclic ML in [2], is illustrated. One can observe that the cyclic ML receiver also provides excellent performance for sufficiently large P.



(a) SDR-ML (b) Cyclic ML

Fig. 2. Bit error rate of the NIS Alamouti code, with the blind receiver being (a) the SDR-ML method; and (b) the cyclic ML.

Let us use this example to discuss the rate and power issues of NIS-OSTBCs. In the original QPSK Alamouti code, the average bit rate is $K/T = 4/2 = 2$ bits per channel use. For the NIS counterpart, it is $K/T = 7/4 = 1.75$ bits per channel use. Moreover, the average code power, given by $\mathrm{E}\{\|\mathbf{C}(\mathbf{s})\|_F^2\}/T = M_t K/T$, is $2M_t$ for the original Alamouti code and $1.75M_t$ for the NIS Alamouti code. [We should recall that our formulation has the bit energy being constant for a fixed M_t, but not the average code

power; c.f., Eqs. (1) and (4).] If the simulation is repeated by comparing the two codes with the same average code power, the NIS Alamouti code will yield an extra SNR gain by about 0.5dB. □

C. A Modified OSTBC Scheme

The NIS-OSTBCs generated by Construction I have a data rate of $(2K-1)/(2T)$ bits per channel use (bpcu). This rate is relatively lower than that of their original counterpart; that is, K/T bpcu. To reduce the rate loss, we propose the following modified transmission scheme:

Modified OSTBC Transmission Scheme

Given an OSTBC $\mathbf{C}_o(\mathbf{s}) = \sum_{k=1}^{K} s_k \mathbf{X}_k \in \mathbb{C}^{M_t \times T}$ where K is even, and a frame length $P \geq 2$.

Step 1. Set $\mathbf{C}_1(\mathbf{s}) = \sum_{k=1}^{K-1} s_k \mathbf{X}_k$.

Step 2. For $p = 1$, transmit $\mathbf{C}_1(\mathbf{s}_1)$ where $\mathbf{s}_1 \in \{\pm 1\}^{K-1}$.

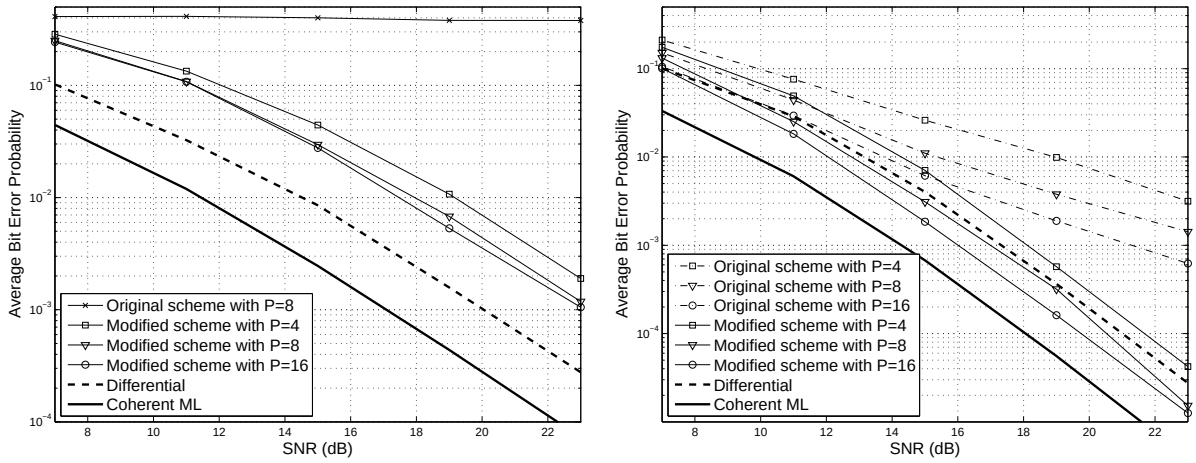
Step 3. For $p = 2, \ldots, P$, transmit $\mathbf{C}_o(\mathbf{s}_p)$ where $\mathbf{s}_p \in \{\pm 1\}^{K}$.

The difference between the original and modified transmission schemes lies in the first transmitted code block only, where the modified scheme transmits a 1-bit-reduced OSTBC $\mathbf{C}_1(.)$ in place of $\mathbf{C}_o(.)$ in the original case. Since the first two code blocks $\mathbf{C}_1(\mathbf{s}_1)$ and $\mathbf{C}_o(\mathbf{s}_2)$ can be seen as one NIS-OSTBC, perfect identification of $\mathbf{H}$ (up to a sign) is guaranteed and it follows that the rest of the code blocks $\mathbf{C}_o(\mathbf{s}_3), \ldots, \mathbf{C}_o(\mathbf{s}_P)$ are also perfectly identifiable. Alternatively, the code frame $[\mathbf{C}_1(\mathbf{s}_1), \mathbf{C}_o(\mathbf{s}_2), \ldots, \mathbf{C}_o(\mathbf{s}_P)]$ can regarded as a supercode that has the NIS property inherited from $[\mathbf{C}_1(\mathbf{s}_1), \mathbf{C}_o(\mathbf{s}_2)]$. The rate of the modified scheme is $(2KP-1)/(2TP)$ bpcu. Hence, for large P, the rate of the modified scheme approaches that of the original.

The performance of the modified OSTBC scheme is illustrated by simulations as follows:

Example 5 This example compares the performance of the original and modified OSTBC transmission schemes. The simulation settings here are identical to that in Example 4, and the SDR-ML detector was employed. Fig. 3(a) plots the performance in the QPSK Alamouti case. We see that the modified scheme has its bit error probability being consistent and decaying at the same rate as that of the coherent ML (thereby having the full noncoherent spatial diversity). However, increasing P is not very helpful in improving the performance, unlike the promising NIS-Alamouti code in Example 4. In fact, the modified scheme fails to provide performance better than the differential Alamouti scheme.

In Fig. 3(b) we consider the BPSK OSTBC 3×4 code [in (34)]. This code is strictly non-rotatable, meaning that it is already UIUTS with probability 1. From a blind identifiability standpoint it seems to be sufficient to use the original scheme, but we were still curious about the performance difference of the



(a) QPSK Alamouti (b) BPSK 3×4 OSTBC

Fig. 3. Bit error rate of the the original and modified OSTBC schemes. The SDR-ML detector was used.

original and modified schemes. Remarkably, we see from the figure that the modified scheme in this case can achieve near coherent ML performance, unlike the previous Alamouti case. In the original scheme, the bit error probability decays at a rate lower than that of the coherent ML. The modified scheme does not have this problem, and its performance improves quite well with respect to P. It also yields better performance than the differential scheme for $P \geq 8$, by about 1.5dB when $P = 16$.

This example demonstrates an interesting issue: Achieving perfect blind identifiability is desirable, but it does not always lead to excellent, near coherent ML performance. How to design OSTBCs for achieving good noncoherent error performance appears to be an interesting future direction, but is beyond reach of this paper. □

V. Conclusion and Discussion

In this paper, the blind ML identifiability of OSTBCs with BPSK or QPSK constellations has been studied. Our analysis leads to the conclusion that orthogonal space-time block coding provides very appealing blind identifiability, in the sense that there exist OSTBCs that can be uniquely identified up to a sign (UIUTS) almost surely for many Gaussian fading channels, or UIUTS deterministically for all nonzero channels. These characteristics imply that even in harsh channel environments such as rank deficient channel matrix and one receiver antenna, blind orthogonal space-time block coding can still operate properly. We have not only identified blindly-identifiable OSTBCs from the existing OSTBCs, a procedure has also been proposed to construct OSTBCs with excellent blind identifiability.

This paper considers the case of BPSK and QPSK constellations only. Extensions to higher-order PSK and QAM constellations would be a future direction worth studying. In addition, it would be interesting to investigate how the present results are related to the identifiability of non-standard OSTBC transmission schemes in [16] and [36], [37], where unequal symbol powers and unequal symbol constellations are respectively used to fix the non-identifiability issue in rotatable OSTBCs.

APPENDIX

A. Proof of Theorem 1

The nontrivial part of Theorem 1 lies in showing that if $\mathbf{C}(.)$ is rotatable, then Statement iii) of Theorem 1 holds. Suppose that $\mathbf{S} = [\ \mathbf{s}_1, \ldots, \mathbf{s}_P\ ] \in \{\pm 1\}^{K \times P}$ is a matrix where its columns contain all combinations of vectors in $\{\pm 1\}^K$. For a rotatable $\mathbf{C}(.)$ with a (unitary) code rotation matrix $\mathbf{Q}$, the following condition holds according to the definition:

$$\mathbf{Q}\mathbf{C}(\mathbf{s}_p) = \mathbf{C}(\tilde{\mathbf{s}}_p), \quad p = 1, \ldots, P \tag{50}$$

for some $\tilde{\mathbf{s}}_p \in \{\pm 1\}^K \setminus \{\pm \mathbf{s}_p\}$, $p = 1, \ldots, P$; or equivalently

$$\mathbf{C}(\mathbf{s}_p) = \mathbf{Q}^H \mathbf{C}(\tilde{\mathbf{s}}_p), \quad p = 1, \ldots, P. \tag{51}$$

From the above equation, it is straightforward to verify that $\mathbf{Q} \neq \pm \mathbf{I}$. By using derivations similar to Eqs. (13)-(15), Eq. (51) can be reexpressed as

$$\overline{\boldsymbol{\mathcal{X}}}\mathbf{s}_p = \overline{(\mathbf{I}_T \otimes \mathbf{Q}^H)\boldsymbol{\mathcal{X}}}\tilde{\mathbf{s}}_p, \quad p = 1, \ldots, P. \tag{52}$$

where the overline means that $\overline{\mathbf{A}} = [\ \mathrm{Re}\{\mathbf{A}\}^T\ \mathrm{Im}\{\mathbf{A}\}^T\ ]^T$, and that $\boldsymbol{\mathcal{X}} = [\ \mathrm{vec}(\mathbf{X}_1), \ldots, \mathrm{vec}(\mathbf{X}_K)\ ]$. By applying the property $\overline{\mathbf{B}}^T\overline{\mathbf{A}} = \mathrm{Re}\{\mathbf{B}^H\mathbf{A}\}$ (which is easy to verify) and by using (3), we have that

$$\overline{\boldsymbol{\mathcal{X}}}^T\overline{\boldsymbol{\mathcal{X}}} = M_t\mathbf{I}. \tag{53}$$

Premultiplying (52) by $\overline{\boldsymbol{\mathcal{X}}}^T$, we obtain

$$\mathbf{s}_p = \boldsymbol{\Gamma}\tilde{\mathbf{s}}_p, \quad p = 1, \ldots, P, \tag{54}$$

where $\boldsymbol{\Gamma} = \frac{1}{M_t}\overline{\boldsymbol{\mathcal{X}}}^T\overline{(\mathbf{I}_T \otimes \mathbf{Q}^H)\boldsymbol{\mathcal{X}}}$. Since we have assumed that the columns of $\mathbf{S}$ contain all combinations of vectors in $\{\pm 1\}^K$, there exist 2^{K-1} distinct bit vectors in the columns of $\mathbf{S}$. By applying Lemma 1 to (54), we obtain $\boldsymbol{\Gamma} = \mathbf{D}\boldsymbol{\Pi}^T$ and $\tilde{\mathbf{s}}_p = \boldsymbol{\Pi}\mathbf{D}\mathbf{s}_p$, where $\boldsymbol{\Pi} \in \{0,1\}^{K \times K}$ is a permutation matrix, and $\mathbf{D} \in \mathbb{R}^{K \times K}$ is diagonal with $\mathrm{diag}(\mathbf{D}) \in \{\pm 1\}^K$. Substituting this result into (50), we conclude that

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\boldsymbol{\Pi}\mathbf{D}\mathbf{s}) \tag{55}$$

for $\mathbf{s} \in \{\pm 1\}^K$. It can be proven that (55) holds for $\mathbf{s} \in \mathbb{R}^K$ as well, by using the linearity of $\mathbf{C}(.)$. The matrix $\mathbf{\Pi}$ must have zero main diagonals. To see this, suppose that the (k,k)th element of $\mathbf{\Pi}$ equals 1. By letting $\mathbf{e}_k$ be a vector whose kth element is 1 and whose remaining elements are 0, we have that

$$\mathbf{Q}\mathbf{X}_k = \mathbf{Q}\mathbf{C}(\mathbf{e}_k) = \mathbf{C}(\mathbf{\Pi}\mathbf{D}\mathbf{e}_k) = d_k\mathbf{X}_k, \tag{56}$$

where $d_k \in \{\pm 1\}$ is the kth diagonal of $\mathbf{D}$. Since $\mathbf{X}_k\mathbf{X}_k^H = \mathbf{I}$, Eq. (56) is a contradiction to $\mathbf{Q} \neq \pm\mathbf{I}$.

B. Proof of Theorem 2

The proof is by contradiction. A real OSTBC $\mathbf{C}(\mathbf{s}) = \sum_{k=1}^K s_k\mathbf{X}_k$ has its basis matrices $\mathbf{X}_k$ being all real. Suppose that M_t is odd, and that $\mathbf{C}(.)$ is not strictly non-rotatable such that

$$\mathbf{Q}\mathbf{C}(\mathbf{s}) = \mathbf{C}(\tilde{\mathbf{s}}) \tag{57}$$

is satisfied for some $\mathbf{Q} \in \mathbb{R}^{M_t \times M_t}$, $\mathbf{s}, \tilde{\mathbf{s}} \in \{\pm 1\}^K$, $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$. The row orthogonality of $\mathbf{C}(.)$ [Eq. (4)] implies that $\mathbf{Q}$ must be unitary. Post-multiplying (57) by $\mathbf{C}^T(\mathbf{s})/K$, we get

$$\mathbf{Q} = \tfrac{1}{K}\mathbf{C}(\tilde{\mathbf{s}})\mathbf{C}^T(\mathbf{s}). \tag{58}$$

From the OSTBC properties in (1) and (3), Eq. (58) can be decomposed to

$$\mathbf{Q} = \alpha\mathbf{I} + \mathbf{B}, \tag{59}$$

where

$$\alpha = \frac{1}{K}\sum_{k=1}^K s_k\tilde{s}_k, \quad \mathbf{B} = \frac{1}{K}\sum_{k=1}^K \sum_{\ell=1,\ell\neq k}^K s_k\tilde{s}_\ell\mathbf{X}_k\mathbf{X}_\ell^T. \tag{60}$$

Since $\mathbf{X}_k\mathbf{X}_\ell^T$ is skew symmetric for $k \neq \ell$ [cf., Eq. (3)], $\mathbf{B}$ is also skew symmetric.

Let $\lambda_1(\mathbf{A}), \ldots, \lambda_n(\mathbf{A})$ denote the eigenvalues of $\mathbf{A} \in \mathbb{C}^{n\times n}$. Since $\mathbf{Q}$ is unitary, it must be true that $|\lambda_i(\mathbf{Q})| = 1$ for all $i = 1, \ldots, M_t$. From (59), we have $\lambda_i(\mathbf{Q}) = \alpha + \lambda_i(\mathbf{B})$ for $i = 1, \ldots, M_t$. Using the fact that a (real) symmetric matrix with odd dimension must be singular [38], we know that at least one of the $\lambda_1(\mathbf{B}), \ldots, \lambda_{M_t}(\mathbf{B})$ equals zero. Consequently, we have that $\lambda_i(\mathbf{Q}) = \alpha$ for some i. But, from (60) it is easy to check that $|\alpha| < 1$ for any $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$, a contradiction to $|\lambda_i(\mathbf{Q})| = 1$ for all i.

C. Proof of Theorem 3

Let $\sigma_{\max}(\mathbf{A})$ and $\sigma_{\min}(\mathbf{A})$ define the maximum and minimum singular values of $\mathbf{A}$, respectively. We will require the following lemma:

Lemma 5 *Let* $\mathbf{E}, \mathbf{F} \in \mathbb{C}^{M\times T}$*, and suppose that* $\mathbf{E}\mathbf{E}^H = \mathbf{F}\mathbf{F}^H = \mathbf{I}$*. Then,*

$$\sigma_{\max}(\mathbf{E}\mathbf{F}^H) \leq 1. \tag{61}$$

Moreover, the condition

$$\sigma_{\min}(\mathbf{E}\mathbf{F}^H) < 1 \tag{62}$$

holds if $\mathcal{R}(\mathbf{E}^T) \neq \mathcal{R}(\mathbf{F}^T)$.

Proof of Lemma 5: Eq. (61) is straightforward since $\sigma_{\max}(\mathbf{E}\mathbf{F}^H) = \|\mathbf{E}\mathbf{F}^H\|_2 \leq \|\mathbf{E}\|_2\|\mathbf{F}\|_2 = 1$, where $\|.\|_2$ denotes the matrix 2-norm. To prove (62), we use the results in distance between subspaces [35]. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be subspaces with equal dimension. The distance between $\mathcal{S}_1$ and $\mathcal{S}_2$ are defined by $\mathrm{dist}(\mathcal{S}_1, \mathcal{S}_2) = \|\mathbf{P}_1 - \mathbf{P}_2\|_2$, where $\mathbf{P}_1$ and $\mathbf{P}_2$ denotes respectively the orthogonal projectors of $\mathcal{S}_1$ and $\mathcal{S}_2$. The distance $\mathrm{dist}(\mathcal{S}_1, \mathcal{S}_2)$ equals zero only when $\mathcal{S}_1 = \mathcal{S}_2$. Now, it can be shown that [35, p. 76–77]

$$\mathrm{dist}^2(\mathcal{R}(\mathbf{E}^T), \mathcal{R}(\mathbf{F}^T)) = 1 - \sigma^2_{\min}(\mathbf{E}^*\mathbf{F}^T) = 1 - \sigma^2_{\min}(\mathbf{E}\mathbf{F}^H). \tag{63}$$

Hence, we have $\sigma^2_{\min}(\mathbf{E}\mathbf{F}^H) < 1$ whenever $\mathcal{R}(\mathbf{E}^T) \neq \mathcal{R}(\mathbf{F}^T)$. ■

To prove Theorem 3, suppose that

$$\mathbf{H}\mathbf{C}(\mathbf{s}_p) = \tilde{\mathbf{H}}\mathbf{C}(\tilde{\mathbf{s}}_p), \qquad p = 1, \ldots, P, \tag{64}$$

for some $\{\tilde{\mathbf{H}}, \tilde{\mathbf{S}}\} \neq \pm\{\mathbf{H}, \mathbf{S}\}$. Let

$$\mathbf{E} = \tfrac{1}{\sqrt{KP}}[\ \mathbf{C}(\mathbf{s}_1), \ldots, \mathbf{C}(\mathbf{s}_P)\ ], \tag{65}$$

$$\mathbf{F} = \tfrac{1}{\sqrt{KP}}[\ \mathbf{C}(\tilde{\mathbf{s}}_1), \ldots, \mathbf{C}(\tilde{\mathbf{s}}_P)\ ] \tag{66}$$

so that (64) can be reexpressed as

$$\mathbf{H}\mathbf{E} = \tilde{\mathbf{H}}\mathbf{F}. \tag{67}$$

The matrices $\mathbf{E}$ and $\mathbf{F}$ satisfy $\mathbf{E}\mathbf{E}^H = \mathbf{F}\mathbf{F}^H = \mathbf{I}$. When $\mathbf{C}(.)$ is strictly non-rotatable, from Property 2 we obtain $\mathcal{R}(\mathbf{E}^T) \neq \mathcal{R}(\mathbf{F}^T)$. When $\mathbf{C}(.)$ is non-rotatable and **A1)** holds, from Property 1 we know that there does not exist a $\mathbf{Q}$ such that $\mathbf{Q}\mathbf{E} = \mathbf{F}$, thereby $\mathcal{R}(\mathbf{E}^T) \neq \mathcal{R}(\mathbf{F}^T)$. Eq. (67) can be rewritten as

$$\mathbf{H}\mathbf{E}\mathbf{F}^H = \tilde{\mathbf{H}}. \tag{68}$$

By taking the Frobenius norm on the two sides of (67) and (68), we obtain $\|\mathbf{H}\|_F = \|\tilde{\mathbf{H}}\|_F$ and $\|\mathbf{H}\mathbf{E}\mathbf{F}^H\|_F = \|\tilde{\mathbf{H}}\|_F$, respectively. It follows that

$$\|\mathbf{H}\|_F^2 = \|\mathbf{H}\mathbf{E}\mathbf{F}^H\|_F^2. \tag{69}$$

Using Lemma 5, an expression for the singular value decomposition of $\mathbf{EF}^H$ is obtained:

$$\mathbf{EF}^H = [\ \mathbf{U}_1\ \mathbf{U}_2\ ] \begin{bmatrix} \mathbf{I}_r & \\ & \mathbf{\Sigma}_2 \end{bmatrix} \begin{bmatrix} \mathbf{V}_1^H \\ \mathbf{V}_2^H \end{bmatrix}, \tag{70}$$

where $r < M_t$ is the number of unit singular values of $\mathbf{EF}^H$, $\mathbf{\Sigma}_2$ is diagonal containing the singular values that are less than 1, $\mathbf{U}_1$ and $\mathbf{V}_1$ are respectively the left and right singular matrices associated with the unit singular values, and $\mathbf{U}_2$ and $\mathbf{V}_2$ are respectively the left and right singular matrices associated with the less-than-1 singular values. Substituting (70) to the right hand side of (69) yields

$$\|\mathbf{HEF}^H\|_F^2 = \|\mathbf{HU}_1\|_F^2 + \|\mathbf{HU}_2\mathbf{\Sigma}_2\|_F^2. \tag{71}$$

On the other hand, using the unitarity of $[\ \mathbf{U}_1\ \mathbf{U}_2\ ]$, the left hand side of (69) can be decomposed to

$$\|\mathbf{H}\|_F^2 = \|\mathbf{HU}_1\|_F^2 + \|\mathbf{HU}_2\|_F^2. \tag{72}$$

It follows that

$$\|\mathbf{HU}_2\|_F^2 = \|\mathbf{HU}_2\mathbf{\Sigma}_2\|_F^2, \tag{73}$$

which can be shown to be equivalent to

$$\mathrm{tr}\{\mathbf{HU}_2(\mathbf{I} - \mathbf{\Sigma}_2^2)\mathbf{U}_2^H\mathbf{H}^H\} = 0. \tag{74}$$

Since $\mathbf{I} - \mathbf{\Sigma}_2^2 \succ \mathbf{0}$ (where $\mathbf{A} \succ \mathbf{0}$ means that $\mathbf{A}$ is positive definite), to satisfy (74) it is sufficient and necessary to have

$$\mathbf{HU}_2 = \mathbf{0}. \tag{75}$$

Let us consider the probability that (75) holds, which is equivalent to the probability that (64) holds. Let $\boldsymbol{\mu}_i$ and $\mathbf{R}_i$ denote the mean and covariance of $\mathbf{h}_i$, where $\mathbf{H}^T = [\ \mathbf{h}_1, \ldots, \mathbf{h}_{M_r}\ ]$. The probability of (75) is bounded by

$$\begin{aligned} \Pr[\mathbf{HU}_2 = \mathbf{0}] &= \Pr\left[\ \cap_{i=1}^{M_r} \{\mathbf{U}_2^T\mathbf{h}_i = \mathbf{0}\}\ \right] \\ &\leq \Pr[\mathbf{U}_2^T\mathbf{h}_i = \mathbf{0}], \end{aligned} \tag{76}$$

for any $i = 1, \ldots, M_r$. Under **A2)**, each random vector $\mathbf{U}_2^T\mathbf{h}_i$ follows a circular complex Gaussian distribution with mean $\mathbf{U}_2^T\boldsymbol{\mu}_i$ and covariance $\mathbf{U}_2^T\mathbf{R}_i\mathbf{U}_2^*$. If $\mathbf{R}_i \succ \mathbf{0}$ for some i, then it can be shown that $\Pr[\mathbf{U}_2^T\mathbf{h}_i = \mathbf{0}]$ is of measure zero for those i. Subsequently, from (76) we have $\Pr[\mathbf{HU}_2 = \mathbf{0}] = 0$.

As a side product, we note that (75) can never be satisfied if $\mathbf{H}$ is of full column rank. This observation leads to Lemma 3.

D. Proof of Lemma 4

Lemma 4 is shown by constructing a situation such that

$$\mathbf{C}^T(\mathbf{s})\mathbf{h} = \mathbf{C}^T(\tilde{\mathbf{s}})\tilde{\mathbf{h}} \tag{77}$$

for some distinct pair of bit vectors $(\mathbf{s}, \tilde{\mathbf{s}})$ and for some $\mathbf{h}, \tilde{\mathbf{h}} \in \mathbb{C}^{M_t} \backslash \{\mathbf{0}\}$, thereby obtaining the conclusion $\mathcal{R}(\mathbf{C}^T(\mathbf{s})) \cap \mathcal{R}(\mathbf{C}^T(\tilde{\mathbf{s}})) \neq \{\mathbf{0}\}$.

Assume that $\mathbf{C}(.)$ is a full-rate real GOD. In this case the code matrix can be expressed as

$$\mathbf{C}^T(\mathbf{s}) = [\ \mathbf{E}_1\mathbf{s}, \ldots, \mathbf{E}_{M_t}\mathbf{s}\ ], \tag{78}$$

where $\mathbf{E}_i \in \mathbb{R}^{T\times T}$ are code constituent matrices that satisfy the following structures [21]: i) $\mathbf{E}_i^T\mathbf{E}_i = \mathbf{E}_i\mathbf{E}_i^T = \mathbf{I}$; ii) $\mathbf{E}_i^T\mathbf{E}_k = -\mathbf{E}_k^T\mathbf{E}_i$ for $i \neq k$; and iii) each $\mathbf{E}_i$ is a ± 1 permutation matrix in the form of

$$\mathbf{E}_i = \mathbf{\Pi}_i\mathbf{D}_i \tag{79}$$

where $\mathbf{\Pi}_i \in \{0,1\}^{T\times T}$ is a permutation matrix and $\mathbf{D}_i \in \mathbb{R}^{T\times T}$ is diagonal with $\mathrm{diag}(\mathbf{D}_i) \in \{\pm 1\}^T$. Now, fixing $\mathbf{s} \in \{\pm 1\}^K$, choose

$$\tilde{\mathbf{s}} = \mathbf{E}_2^T\mathbf{E}_1\mathbf{s}. \tag{80}$$

It is easy to show that $\mathbf{E}_2^T\mathbf{E}_1$ is also a ± 1 permutation matrix. Hence, we have $\tilde{\mathbf{s}} \in \{\pm 1\}^T$. Moreover, it must be true that $\tilde{\mathbf{s}} \neq \pm\mathbf{s}$ given any $\mathbf{s} \in \{\pm 1\}^T$. The reason is as follows: If $\tilde{\mathbf{s}} = \pm\mathbf{s}$, then $\mathbf{E}_2^T\mathbf{E}_1$ must have one eigenvalue equal to ± 1. But $\mathbf{E}_2^T\mathbf{E}_1$ is a skew-symmetric matrix, the eigenvalues of which are either pure imaginary or zero [33]. With the above settings, one can show that

$$\mathbf{C}^T(\mathbf{s})\mathbf{e}_1 = \mathbf{C}^T(\tilde{\mathbf{s}})\mathbf{e}_2. \tag{81}$$

For the case of full-rate complex GODs where $K = 2T$, let $\mathbf{s}_R = [\ s_1, \ldots, s_T\ ]^T$ and $\mathbf{s}_I = [\ s_{T+1}, \ldots, s_{2T}\ ]^T$. The code matrix can be expressed as [19]

$$\mathbf{C}^T(\mathbf{s}) = [\ \mathbf{E}_1\mathbf{s}_R + j\mathbf{F}_1\mathbf{s}_I, \ldots, \mathbf{E}_{M_t}\mathbf{s}_R + j\mathbf{F}_{M_t}\mathbf{s}_I\ ] \tag{82}$$

where $\mathbf{E}_i \in \mathbb{R}^{T\times T}$ and $\mathbf{F}_i \in \mathbb{R}^{T\times T}$. The structures of $\mathbf{E}_i$ are identical to those in real GODs, while $\mathbf{F}_i$ follow the same structures; namely that $\mathbf{F}_i\mathbf{F}_i^T = \mathbf{I}$, $\mathbf{F}_i^T\mathbf{F}_k = -\mathbf{F}_k^T\mathbf{F}_i$ for $i \neq k$, and each $\mathbf{F}_i$ is a ± 1 permutation matrix. The rest of the proof are then almost the same as in the real case, and are omitted for brevity.

E. Proof of Theorem 5

This theorem is proven by contradiction. Suppose that $\mathbf{C}_{new}(.)$ is not an NIS-OSTBC such that for some distinct pair of bit vectors $(\mathbf{s}, \tilde{\mathbf{s}})$, there exist $\mathbf{h}, \tilde{\mathbf{h}} \in \mathbb{C}^{M_t} \setminus \{\mathbf{0}\}$ such that

$$\mathbf{h}^T \mathbf{C}_{new}(\mathbf{s}) = \tilde{\mathbf{h}}^T \mathbf{C}_{new}(\tilde{\mathbf{s}}). \tag{83}$$

From Construction I, Eq. (83) can be decomposed to two sets of equations

$$\mathbf{h}^T \mathbf{C}_1(\boldsymbol{\mu}) = \tilde{\mathbf{h}}^T \mathbf{C}_1(\tilde{\boldsymbol{\mu}}), \tag{84}$$

$$\mathbf{h}^T \mathbf{C}_o(\boldsymbol{\nu}) = \tilde{\mathbf{h}}^T \mathbf{C}_o(\tilde{\boldsymbol{\nu}}), \tag{85}$$

where $\mathbf{s} = [\ \boldsymbol{\mu}^T\ \ \boldsymbol{\nu}^T\ ]^T$ and $\tilde{\mathbf{s}} = [\ \tilde{\boldsymbol{\mu}}^T\ \ \tilde{\boldsymbol{\nu}}^T\ ]^T$. Postmultiplying (84) and (85) by $\mathbf{C}_1(\boldsymbol{\mu})$ and $\mathbf{C}_o(\boldsymbol{\nu})$ respectively, we obtain

$$\mathbf{h}^T = \tilde{\mathbf{h}}^T \mathbf{Q}_1, \quad \mathbf{h}^T = \tilde{\mathbf{h}}^T \mathbf{Q}_2, \tag{86}$$

where

$$\mathbf{Q}_1 = \tfrac{1}{K-1} \mathbf{C}_1(\tilde{\boldsymbol{\mu}}) \mathbf{C}_1^H(\boldsymbol{\mu}), \quad \mathbf{Q}_2 = \tfrac{1}{K} \mathbf{C}_o(\tilde{\boldsymbol{\nu}}) \mathbf{C}_o^H(\boldsymbol{\nu}). \tag{87}$$

Eqs. (86) lead to

$$\tilde{\mathbf{h}}^T (\mathbf{Q}_1 - \mathbf{Q}_2) = \mathbf{0}, \tag{88}$$

implying that $\mathbf{Q}_1 - \mathbf{Q}_2$ is singular.

We now show that $\mathbf{Q}_1 - \mathbf{Q}_2$ cannot be singular. The matrices $\mathbf{Q}_1$ and $\mathbf{Q}_2$ can be expressed as

$$\mathbf{Q}_1 = \frac{\alpha_1}{K-1} \mathbf{I} + \mathbf{B}_1, \quad \mathbf{Q}_2 = \frac{\alpha_2}{K} \mathbf{I} + \mathbf{B}_2 \tag{89}$$

where

$$\alpha_1 = \sum_{k=1}^{K-1} \mu_k \tilde{\mu}_k \in \{\pm 1, \pm 3, \ldots, \pm (K-1)\}, \tag{90}$$

$$\alpha_2 = \sum_{k=1}^{K} \nu_k \tilde{\nu}_k \in \{0, \pm 2, \pm 4, \ldots, K\}, \tag{91}$$

and $\mathbf{B}_1 = \frac{1}{K-1} \sum_k \sum_{\ell \neq k} \tilde{\mu}_k \mu_\ell \mathbf{X}_k \mathbf{X}_\ell^H$ and $\mathbf{B}_2 = \frac{1}{K} \sum_k \sum_{\ell \neq k} \tilde{\nu}_k \nu_\ell \mathbf{X}_k \mathbf{X}_\ell^H$ are skew-Hermitian [cf., Eq. (3)]. Hence,

$$\mathbf{Q}_1 - \mathbf{Q}_2 = \gamma \mathbf{I} + (\mathbf{B}_1 - \mathbf{B}_2), \tag{92}$$

where

$$\gamma = \frac{\alpha_1}{K-1} - \frac{\alpha_2}{K}. \tag{93}$$

If $\mathbf{Q}_1 - \mathbf{Q}_2$ is singular, then at least one of its eigenvalues has to be 0. From (92), the eigenvalues of $\mathbf{Q}_1 - \mathbf{Q}_2$ are given by $\lambda_i(\mathbf{Q}_1 - \mathbf{Q}_2) = \gamma + \lambda_i(\mathbf{B}_1 - \mathbf{B}_2)$, $i = 1, \ldots, M_t$. Since $\mathbf{B}_1 - \mathbf{B}_2$ is skew-Hermitian, its eigenvalues $\lambda_i(\mathbf{B}_1 - \mathbf{B}_2)$ are either pure imaginary or zero [33]. Hence, to have a singular $\mathbf{Q}_1 - \mathbf{Q}_2$ it is necessary that $\gamma = 0$. Since K is even, it can be represented by $K = 2m$ for some integer m. Likewise, α_2 can be represented by $\alpha_2 = 2c$ where $c \in \{0, \pm 1, \ldots, \pm m\}$. The condition $\gamma = 0$ implies that

$$\alpha_1 = \frac{K-1}{K}\alpha_2 = \frac{(2m-1)c}{m} = 2c - \frac{c}{m}. \tag{94}$$

From (90) α_1 is an odd number, but Eq. (94) indicates that α_1 is not an integer unless $c = 0$ or $c = \pm m$. For $c = 0$ we have $\alpha_1 = 0$, a contradiction. For $c = \pm m$, we have $\alpha_1 = \pm(K-1)$ and $\alpha_2 = \pm K$. Such a condition can only be satisfied when $[\ \boldsymbol{\mu}^T\ \boldsymbol{\nu}^T\ ]^T = \pm[\ \tilde{\boldsymbol{\mu}}^T\ \tilde{\boldsymbol{\nu}}^T\ ]^T$, a contradiction to $\mathbf{s} \neq \pm\tilde{\mathbf{s}}$.

REFERENCES

[1] A. L. Swindlehurst and G. Leus, "Blind and semi-blind equalization for generalized space-time block codes," *IEEE Trans. Signal Processing*, vol. 50, no. 10, pp. 2589–2498, 2002.

[2] P. Stoica and G. Ganesan, "Space-time block codes: trained, blind, and semi-blind detection," *Digital Signal Processing*, vol. 13, pp. 93–105, 2003.

[3] B. Hochwald and T. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 543–564, 2000.

[4] L. Zheng and D. N. C. Tse, "Communications on the Grassman manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inform. Theory*, vol. 48, pp. 359–383, 2002.

[5] J.-C. Belfiore and A. M. Cipriano, "Space-time coding for noncoherent channels," in *Space-Time Wireless Systems: From Array Processing to MIMO Communications*, Chapter 10, 2005.

[6] B. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2567–2578, 2000.

[7] B. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2041–2052, 2000.

[8] G. Ganesan and P. Stoica, "Differential modulation using space-time block codes," *IEEE Signal Processing Lett.*, vol. 9, no. 2, pp. 57–60, 2002.

[9] X.-B. Liang and X.-G. Xia, "Fast differential unitary space-time demodulation via square orthogonal designs," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1331–1336, 2005.

[10] S. Talwar, M. Viberg, and A. Paulraj, "Blind separation of synchronous co-channel digital signals using an antenna array—part I: algorithms," *IEEE Trans. Signal Processing*, vol. 44, no. 5, pp. 1184–1197, 1996.

[11] N. D. Sidiropoulos and R. S. Budampati, "Khatri-Rao space-time codes," *IEEE Trans. Signal Processing*, vol. 50, no. 10, pp. 2396–2407, 2002.

[12] E. G. Larsson, P. Stoica, and J. Li, "On maximum-likelihood detection and decoding for space-time coding systems," *IEEE Trans. Signal Processing*, vol. 50, no. 4, pp. 937–944, 2002.

[13] ——, "Orthogonal space-time block codes: Maximum likelihood detection for unknown channels and unstructured interferences," *IEEE Trans. Signal Processing*, vol. 51, no. 2, pp. 362–372, 2003.

[14] W.-K. Ma, B.-N. Vo, T. N. Davidson, and P. C. Ching, "Blind ML detection of orthogonal space-time block codes: Efficient high-performance implementations," *IEEE Trans. Signal Process.*, pp. 738–751, Feb. 2006.

[15] Z. Ding and D. B. Ward, "Subspace approach to blind and semi-blind channel estimation for space-time block codes," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 357–362, 2005.

[16] S. Shahbazpanahi, A. Gershman, and J. Manton, "Closed-form blind MIMO channel estimation for orthogonal space-time block codes," *IEEE Trans. Signal Processing*, vol. 53, no. 12, pp. 4506–4517, Dec. 2005.

[17] F.-J. Chen, M.-W. Kwan, C.-W. Kok, and S. Kwong, "A class of space-time code for blind detection," *IEEE Intl. Symp. Circuits and Systems (ISCAS)*, May 2005.

[18] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1456–1467, 1999.

[19] G. Ganesan and P. Stoica, "Space-time block codes: a maximum SNR approach," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1650–1656, 2001.

[20] W. Su and X.-G. Xia, "On space-time codes from complex orthogonal designs," *Wireless Personal Commun.*, vol. 25, pp. 1–26, 2003.

[21] X.-B. Liang, "Orthogonal designs with maximal rates," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2468–2503, 2003.

[22] W. Su and X.-G. Xia, "Two generalized complex orthogonal space-time block codes of rates $7/11$ and $3/5$ for 5 and 6 transmit antennas," *IEEE Trans. Inform. Theory*, vol. 49, no. 1, pp. 313–316, 2003.

[23] W. Su, X.-G. Xia, and K. J. R. Liu, "A systematic design of high-rate complex orthogonal space-time block codes," *IEEE Commun. Lett.*, vol. 8, no. 6, pp. 380–382, 2004.

[24] K. Lu, S. Fu, and X.-G. Xia, "Closed-form designs of complex orthogonal space-time block codes for rates $(k+1)/(2k)$ for $2k-1$ and $2k$ transmit antennas," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4340–4347, 2005.

[25] H. Kan and H. Shen, "A counterexample of the open problem on the minimal delays of orthogonal designs with maximal rates," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 355–359, 2005.

[26] E. G. Larsson and P. Stoica, *Space-Time Coding for Wireless Communications*. Cambridge University Press, May 2003.

[27] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, pp. 463–471, 1985.

[28] M. O. Damen, H. E. Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2389–2402, 2003.

[29] W.-K. Ma, T. N. Davidson, K. M. Wong, Z.-Q. Luo, and P. C. Ching, "Quasi-maximum-likelihood multiuser detection using semi-definite relaxation with applications to synchronous CDMA," *IEEE Trans. Signal Processing*, vol. 50, no. 4, pp. 912–922, 2002.

[30] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, 1998.

[31] W.-K. Ma, P. C. Ching, T. N. Davidson, and X.-G. Xia, "Blind maximum-likelihood decoding for orthogonal space-time block codes: A semidefinite relaxation approach," *Proc. IEEE 2003 Global Commun. Conf.*, Dec. 2003.

[32] R. Horn and C. Johnson, *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, U.K., 1994.

[33] ——, *Matrix Analysis*. Cambridge University Press, Cambridge, U.K., 1990.

[34] F. E. Oggier, N. J. A. Sloane, S. N. Diggavi, and A. R. Calderbank, "Nonintersecting subspaces based on finite alphabets," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4320–4325, 2005.

[35] G. Golub and C. V. Loan, *Matrix Computations*, 3rd ed. The Johns Hopkins University Press, 1996.

[36] L. Zhou, J.-K. Zhang, and K. M. Wong, "Unique blind identification of Alamouti space-time coded channel via signal designs and transmission diversity," *Proc. 8th Int. Symp. Signal Processing and its Applications, Sydney, Australia*, Aug. 2005.

[37] ——, "A novel signaling scheme for blind unique identification of Alamouti space-time block coded channel," to appear in *IEEE Trans. Signal Process.*, 2006.

[38] P. Lancaster, *Theory of Matrices*. Academic Press, 1969.