TECHNICAL UNIVERSITY OF CRETE
DEPARTMENT OF ELECTRONIC AND COMPUTER ENGINEERING

Full-rate Differential M-PSK Alamouti Modulation with Polynomial-complexity Maximum-likelihood Noncoherent Detection

by

Panagiotis P. Markopoulos

Submitted in partial fulfillment of the requirements for the

M.Sc. degree in Electronic and Computer Engineering.

Thesis Committee
Ass. Prof. George Karystinos (supervisor)
Prof. Athanasios Liavas
Ass. Prof. Aggelos Bletsas

Chania, August 2012

Abstract

We consider Alamouti encoding that draws symbols from M-ary phase-shift keying (M-PSK) and develop a new differential modulation scheme that attains full rate for any constellation order. In contrast to past work, the proposed scheme guarantees that the encoded matrix maintains the characteristics of the initial codebook and, at the same time, attains full rate so that all possible sequences of space-time matrices become valid. Surprisingly, although the validity of all sequences could be thought as a drawback with respect to noncoherent sequence decoding, in fact it turns out to be an advantage. Based on recent results in the context of reduced-rank quadratic-form maximization over an M-PSK alphabet, we exploit the full-rate property of the proposed scheme to develop a polynomial-complexity ML noncoherent sequence decoder whose order is solely determined by the number of receive antennas. Numerical studies show the superiority of the proposed scheme in comparison with contemporary alternatives in terms of both encoding rate and decoding complexity.

I. INTRODUCTION

Orthogonal space-time block codes (OSTBCs) [1], [2] achieve full antenna-diversity gain with linear-complexity single-symbol maximum-likelihood (ML) coherent detection; i.e., when channel state information (CSI) is available at the receiver [2], [3]. However, the very nature of wireless channels suggests rapidly varying channel conditions which render channel estimation rather inefficient. Even when the fading channel coefficients are not fast varying, channel estimation requires transmission of long pilot symbol sequences, especially for the cases where large antenna arrays are used [4], with the direct implication of reduced effective transmission rate.

Certainly, when OSTBCs are used and the receiver has no CSI, ML noncoherent sequence detection has to be performed on the entire coherence interval for optimal performance [3], [5]-[7]. However, if sequence detection is performed through exhaustive search among all possible data sequences, then exponential computational complexity is required. Moreover, according to [8], the use of rotatable OSTBCs, such as the Alamouti codes, gives rise to a phase ambiguity in the M-ary quadratic form or trace maximization problem to which most of the aforementioned detectors are induced. In other words, two or more different equiprobable symbol-streams are being detected at receiver, and no certain (unambiguous) decision is feasible. Interestingly, by means of differential space-time modulation (DSTM), this ambiguity problem can be easily resolved. Most DSTM schemes presented, e.g., in [9] and [10], are based on the DSTMs initially introduced in [11], [12]. However, all these schemes appear to be inefficient in terms of both transmission rate and computational complexity at the detector. In [13], a full-rate ML noncoherent QPSK OSTBC detection scheme has been proposed, which, however, utilizes a Viterbi decoder with prohibitive computational cost.

In this work, we consider the case of static Rayleigh channels, consisted of independent and identically distributed (i.i.d.) coefficients, and propose for the first time a full-rate differential M-ary phase-shift keying (M-PSK) Alamouti scheme, that allows ML noncoherent sequence detection in polynomial time and does not suffer from code-induced ambiguity. We note that the polynomial complexity order is solely determined by the number of antennas used at the receiver. We tailor to our detection problem the algorithm in [14] which treats the problem of rank-deficient quadratic form maximization over the M-phase alphabet and observe that the polynomial in time solution lies in the utilization of multiple auxiliary spherical variables. The optimal M-PSK sequence is proven to belong to a polynomial in size set of M-ary vectors that is built in polynomial time, altogether resulting in an efficient, reduced-complexity algorithm.

The rest of this work is organized as follows. In section II, we introduce the system model and formulate the sequence detection problem. Section III is devoted to the derivation of our novel full-rate differential Alamouti encoding scheme. Section IV develops the polynomial time ML sequence detector. Finally, Section V presents illustrative simulation studies, while a few concluding remarks are drawn in Section VI.

II. System Model and Problem Statement

We consider a MIMO system with 2 transmit and M_r receive antennas that employs transmission of Alamouti matrices built upon M-PSK symbols. Each transmitted matrix $\mathbf{C}(\mathbf{a})$ corresponds to a 2×1 symbol vector $\mathbf{a} = \left[\begin{array}{cc} a_1 & a_2 \end{array}\right]^T \in {\mathcal{A}_M}^2$, where $\mathcal{A}_M = \{e^{j2\pi m/M} \mid m = 0, 1, \ldots, M-1\}$ and $M \in \{2^k \mid k = 1, 2, \ldots\}$, and is given by

$$\mathbf{C}(\mathbf{a}) = \left[\begin{array}{cc} a_1 & a_2 \\ -a_2^* & a_1^* \end{array}\right]. \tag{1}$$

Notice that Alamouti matrices are scaled unitary, such that

$$\mathbf{C}^H(\mathbf{a})\mathbf{C}(\mathbf{a}) = \mathbf{C}(\mathbf{a})\mathbf{C}^H(\mathbf{a}) = 2\mathbf{I}_2, \tag{2}$$

where $(\cdot)^H$ is the conjugate-transpose operator. The communicated M-PSK sequence s of length, say, $2P$ is split into P 2×1 vectors $\mathbf{s}^{(0)}, \mathbf{s}^{(1)}, \ldots, \mathbf{s}^{(P-1)}$ which form the corresponding matrices $\mathbf{C}(\mathbf{s}^{(0)}), \mathbf{C}(\mathbf{s}^{(1)}), \ldots, \mathbf{C}(\mathbf{s}^{(P-1)})$ that are successively transmitted. We consider the channel to remain stable during the interval of P successive Alamouti transmissions. The downconverted and pulse-matched equivalent ith received block of size $M_r \times 2$ is

$$\mathbf{Y}^{(i)} = \mathbf{H}\mathbf{C}(\mathbf{s}^{(i)}) + \mathbf{V}^{(i)}, \tag{3}$$

where $\mathbf{H} \in \mathbb{C}^{M_r \times 2}$ represents the channel matrix between the 2 transmit and M_r receive antennas and consists of i.i.d. coefficients that are modeled as zero-mean circular complex Gaussian random variables with variance σ_h^2 and account for Rayleigh flat fading. $\mathbf{V}^{(i)} \in \mathbb{C}^{M_r \times 2}$ denotes zero-mean additive spatially and temporally white circular complex Gaussian noise matrix with covariance $\sigma_v^2 \mathbf{I}_{M_r}$. The channel and noise matrices $\mathbf{H}$ and $\mathbf{V}^{(i)}$, respectively, are independent of each other. If the receiver has knowledge of the channel matrix, then coherent maximum-likelihood (ML) detection simplifies to one-shot block decisions according to

$$\hat{\mathbf{s}}^{(i)} = \arg \min_{\mathbf{s}^{(i)} \in {\mathcal{A}_M}^2} \|\mathbf{Y}^{(i)} - \mathbf{H}\mathbf{C}(\mathbf{s}^{(i)})\|_F^2, \tag{4}$$

for $i = 0, 1, \ldots, P-1$. In this work, we consider the channel matrix $\mathbf{H}$ to be unavailable to the receiver. Hence, coherent detection in (4) cannot be utilized and the ML receiver takes the form of a sequence detector. We consider a sequence of P matrices consecutively transmitted by the source and collected by the receiver in the form of matrices $\mathbf{Y}^{(0)}, \mathbf{Y}^{(1)}, \ldots, \mathbf{Y}^{(P-1)}$ and form the $M_r \times 2P$ observation matrix

$$\mathbf{Y} \triangleq \begin{bmatrix} \mathbf{Y}^{(0)} & \ldots & \mathbf{Y}^{(P-1)} \end{bmatrix} = \mathbf{H}\mathbf{G}(\mathbf{s}) + \mathbf{V}, \tag{5}$$

where $\mathbf{V} \triangleq \begin{bmatrix} \mathbf{V}^{(0)} & \ldots & \mathbf{V}^{(P-1)} \end{bmatrix}$ and $\mathbf{G}(\mathbf{s})$ is the concatenated matrix of the transmitted Alamouti matrices

$$\mathbf{G}(\mathbf{s}) \triangleq \begin{bmatrix} \mathbf{C}(\mathbf{s}^{(0)}) & \ldots & \mathbf{C}(\mathbf{s}^{(P-1)}) \end{bmatrix} \in \mathbb{C}^{2 \times 2P} \tag{6}$$

that satisfies the orthogonality property

$$\mathbf{G}(\mathbf{s})\mathbf{G}^H(\mathbf{s}) = 2P\mathbf{I}_2. \tag{7}$$

The ML detector for the M-PSK data sequence $\mathbf{s}$ maximizes the conditional probability density function of $\mathbf{Y}$ given $\mathbf{s}$. Thus, the optimal decision is given by

$$\hat{\mathbf{s}} = \arg \max_{\mathbf{s} \in {\mathcal{A}_M}^{2P}} f(\mathbf{Y}|\mathbf{s}) = \arg \max_{\mathbf{s} \in {\mathcal{A}_M}^{2P}} f(\mathbf{y}|\mathbf{s}), \tag{8}$$

where $\mathbf{y} \triangleq \text{vec}(\mathbf{Y}) \in \mathbb{C}^{2M_rP}$ and $f(\cdot|\cdot)$ represents the pertinent matrix/vector probability density function of the channel output conditioned on a symbol sequence. According to [15],

$$\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B}). \tag{9}$$

Then, in view of (5) and (9), the received observation vector can be written as

$$\mathbf{y} = \text{vec}\left(\mathbf{HG}\left(\mathbf{s}\right) + \mathbf{V}\right) = \text{vec}\left(\mathbf{I}_{M_r}\mathbf{HG}\left(\mathbf{s}\right)\right) + \text{vec}\left(\mathbf{V}\right) = \left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\mathbf{h} + \mathbf{v}, \tag{10}$$

where $\mathbf{h} \triangleq \text{vec}(\mathbf{H}) \in \mathbb{C}^{2M_r}$, $\mathbf{v} \triangleq \text{vec}(\mathbf{V}) \in \mathbb{C}^{2M_rP}$, and operator $\otimes$ denotes the Kronecker tensor product [16]. Due to Rayleigh fading, the vectorized single-transmission channel matrix $\mathbf{h}$ is a zero-mean circular complex Gaussian vector of length $2M_r$ with covariance matrix $\mathbf{C}_h \triangleq E\{\mathbf{hh}^H\} = {\sigma_h}^2\mathbf{I}_{2M_r}$, with $E\{\cdot\}$ denoting the statistical expectation. Then, it can be proven that $\mathbf{y}$ given $\mathbf{s}$ is a complex Gaussian vector with mean $E\{\mathbf{y}|\mathbf{s}\} = E\{\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes I_{M_r}\right)\mathbf{h} + \mathbf{v}|\mathbf{s}\} = \left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)E\{\mathbf{h}\} + E\{\mathbf{v}\} = \mathbf{0}_{2M_rP}$ and covariance matrix

$$\mathbf{C}_y\left(\mathbf{s}\right) = E\{\left(\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\mathbf{h} + \mathbf{v}\right)\left(\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\mathbf{h} + \mathbf{v}\right)^H|\mathbf{s}\} \tag{11}$$

$$= \sigma_h^2\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\left(\mathbf{G}^*\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right) + \sigma_v^2\mathbf{I}_{2M_rP}. \tag{12}$$

Therefore, the optimization problem in (8) is rewritten as

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}_M{}^{2P}} \frac{1}{\pi^{2M_rP}|\mathbf{C}_y\left(\mathbf{s}\right)|}\exp\{-\mathbf{y}^H\mathbf{C}_y^{-1}\mathbf{y}\}. \tag{13}$$

Next, we use Sylvester's determinant theorem and Sherman-Morrison-Woodbury formula for the inverse of a rank-deficient update (also known as matrix inversion lemma) [16], to compute

$$|\mathbf{C}_y\left(\mathbf{s}\right)| = |\sigma_v^2\mathbf{I}_{2M_rP}||\mathbf{I}_{2M_r} + \frac{\sigma_h^2}{\sigma_v^2}\left(\mathbf{G}^*\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)| \tag{14}$$

$$= \sigma_v^{4M_rP}|\frac{2\sigma_h^2P+1}{\sigma_v^2}\mathbf{I}_{2M_r}| = \sigma_v^P\left(2\sigma_h^2P+1\right)^{2M_r} \tag{15}$$

and

$$\mathbf{C}_y^{-1}\left(\mathbf{s}\right) = \left(\sigma_h^2\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\left(\mathbf{G}^*\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right) + \sigma_v^2\mathbf{I}_{2M_rP}\right)^{-1} \tag{16}$$

$$= \frac{1}{\sigma_v^2}\mathbf{I}_{2M_rP} - \frac{\sigma_h^2}{\left(2\sigma_h^2P+1\right)\sigma_v^2}\left(\mathbf{G}^T\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right)\left(\mathbf{G}^*\left(\mathbf{s}\right) \otimes \mathbf{I}_{M_r}\right). \tag{17}$$

We observe that $|\mathbf{C}_y(\mathrm{s})|$ is independent of the transmitted sequence s and drop it from the maximization in (13). Substituting (17) in (13), we finally obtain

$$\hat{\mathrm{s}} = \arg \max_{\mathbf{s} \in \mathcal{A}_M{}^{2P}} \mathbf{y}^H (\mathbf{G}^T(\mathbf{s}) \otimes \mathbf{I}_{M_r})(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_{M_r})\mathbf{y}. \tag{18}$$

A natural approach to (18) would be an exhaustive search among all M^{2P} symbol sequences $\mathrm{s} \in \mathcal{A}_M{}^{2P}$. However, such a receiver has two major drawbacks. Firstly, it is impractical even for moderate values of P, since its complexity grows exponentially with P and, secondly, it suffers from inherent phase ambiguity, risen by the rotatability of Alamouti codes. To clarify the ambiguity concept, we provide the following analysis.

We consider $\hat{\mathrm{s}}_1 \in \mathcal{A}_M{}^{2P}$ to be a solution of the maximization problem in (18) and $\mathbf{C}(\hat{\mathrm{s}}_1^{(0)})$, $\mathbf{C}(\hat{\mathrm{s}}_1^{(1)}), \ldots, \mathbf{C}(\hat{\mathrm{s}}_1^{(P-1)})$ to be the corresponding optimal Alamouti matrix sequence. Due to characteristic rotatability of Alamouti matrices [8], [21], there always exists at least one 2×2 unitary rotation matrix $\mathbf{\Theta} \neq \mathbf{I}_2$, so that $\mathbf{\Theta C}(\hat{\mathrm{s}}_1^{(0)})$, $\mathbf{\Theta C}(\hat{\mathrm{s}}_1^{(1)}), \ldots, \mathbf{\Theta C}(\hat{\mathrm{s}}_1^{(P-1)})$ is a valid Alamouti code sequence too, corresponding to a different M-PSK symbol sequence, say $\hat{\mathrm{s}}_2$. Evidently, for all $k \in \{1, 2, \ldots, P-1\}$,

$$\mathbf{C}^H(\hat{\mathrm{s}}_1^{(k-1)})\mathbf{C}(\hat{\mathrm{s}}_1^{(k)}) = \mathbf{C}^H(\hat{\mathrm{s}}_2^{(k-1)})\mathbf{C}(\hat{\mathrm{s}}_2^{(k)}), \tag{19}$$

which, by (6), yields $\mathbf{G}^H(\hat{\mathrm{s}}_1)\mathbf{G}(\hat{\mathrm{s}}_1) = \mathbf{G}^H(\hat{\mathrm{s}}_2)\mathbf{G}(\hat{\mathrm{s}}_2)$ and

$$\|(\mathbf{G}^*(\hat{\mathrm{s}}_1) \otimes \mathbf{I}_{M_r})\mathbf{y}\| = \|(\mathbf{G}^*(\hat{\mathrm{s}}_2) \otimes \mathbf{I}_{M_r})\mathbf{y}\|. \tag{20}$$

Hence, (19) is a sufficient and, w.p.1[1], necessary condition for $\hat{\mathrm{s}}_2$ to solve (18) as well. Certainly, phase ambiguity can be resolved by differential modulation at the transmitter according to [12] which, however, reduces the encoding rate and imposes constraints on the validity of the sequences that are considered in the optimization problem in (18). In Section III, we develop a novel differential modulation scheme for the resolution of this ambiguity, that attains full rate for any constellation order, while guarantees that the encoded matrix maintains the characteristics of the initial codebook so that all possible sequences of Alamouti matrices become valid. Then, based

[1] We consider $\mathrm{P}\{\|(\mathbf{G}^*(\hat{\mathrm{s}}_1) \otimes \mathbf{I}_{M_r})\mathbf{y}\| = \|(\mathbf{G}^*(\hat{\mathrm{s}}_2) \otimes \mathbf{I}_{M_r})\mathbf{y}\| \mid \mathbf{G}^H(\hat{\mathrm{s}}_1)\mathbf{G}(\hat{\mathrm{s}}_1) \neq \mathbf{G}^H(\hat{\mathrm{s}}_2)\mathbf{G}(\hat{\mathrm{s}}_2)\} = 0$.

on recent results in the context of reduced-rank quadratic-form maximization over an M-PSK alphabet, in Section IV we exploit the full-rate property of the proposed scheme to develop a polynomial-complexity ML noncoherent sequence detector which performs the maximization in (18) with $\mathcal{O}\left((MP)^{4M_r}\right)$ calculations.

III. Full-rate Differential Alamouti Encoding and Unique Sequence Decoding

A. A Systematic Classification of Alamouti Matrices

We commence our developments by presenting a particular systematic partitioning of $\mathcal{C}$, the set of all Alamouti matrices defined upon an M-PSK constellation, and analyzing the advantageous properties it yields. Thereafter, we exploit these properties to design a full-rate differential Alamouti encoding scheme.

To begin with, we introduce the $2M$ *primary rotation matrices*

$$\mathbf{R}_{l,\gamma} \triangleq \frac{1}{2}\mathbf{B}\begin{bmatrix} \mu^l & \gamma\mu^l \\ -\gamma\mu^{-l} & \mu^{-l} \end{bmatrix}, \quad l = 0, 1, \ldots, M-1, \quad \gamma = \pm 1, \tag{21}$$

where $\mu \triangleq e^{j2\pi/M}$ and $\mathbf{B} \triangleq \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. By construction, for all $l \in \{0, 1, \ldots, M-1\}$ and $\gamma \in \{-1, 1\}$, $\mathbf{R}_{l,\gamma}$ is a complex rotation matrix; that is, $\mathbf{R}_{l,\gamma}$ is unitary and $\det(\mathbf{R}_{l,\gamma}) = 1$. Next, we define the *primary rotation set* $\mathcal{R}$, consisting of all rotation matrices constructed by (21)

$$\mathcal{R} \triangleq \bigcup_{l=0}^{M-1} \{\mathbf{R}_{l,1}, \mathbf{R}_{l,-1}\}. \tag{22}$$

The following Lemma 1 comprises the basic properties of the primary rotation set and its proof lies in the Appendix of this manuscript.

Lemma 1: The primary rotation set consists of $2M$ distinct complex rotation matrices and is closed under negation, conjugation, transposition, and multiplication; that is, for all $m, m' \in \{0, 1, \ldots, M-1\}$ and $\gamma, \gamma' \in \{-1, 1\}$, $-\mathbf{R}_{m,\gamma}$, $\mathbf{R}^*_{m,\gamma}$, $\mathbf{R}^T_{m,\gamma}$, and $\mathbf{R}_{m,\gamma}\mathbf{R}_{m',\gamma'}$ are members of $\mathcal{R}$. $\square$

Next, we proceed with the classification synthesis by presenting the $M/2$ *secondary rotation* *matrices*

$$\mathbf{T}_l \triangleq \frac{1}{2}\mathbf{B}\begin{bmatrix} 1 & \mu^l \\ -\mu^{-l} & 1 \end{bmatrix}, \quad l = 0, 1, \ldots, M/2-1, \tag{23}$$

and the accordingly formed *secondary rotation set*

$$\mathcal{T} \triangleq \{\mathbf{T}_0, \mathbf{T}_1, \ldots, \mathbf{T}_{M/2-1}\}. \tag{24}$$

For all $l \in \{0, 1, \ldots, M/2-1\}$, $\mathbf{T}_l$ is a complex rotation matrix, while $\mathbf{T}_k \neq \mathbf{T}_l$, for all $k \in \{0, 1, \ldots, M/2-1\} \setminus l$. Hence, the cardinality of the secondary rotation set equals $M/2$. By means of the primary and secondary rotation sets, we define the $M/2$ *code-groups*

$$\mathcal{C}_l \triangleq \mathbf{B}^T \mathcal{R} \mathbf{T}_l, \quad l = 0, 1, \ldots, M/2-1. \tag{25}$$

In the sequel, Lemma 2 and Lemma 3 describe the code-groups defined in (25) and pave the way for the following Theorem 1, which concludes our systematic partitioning of $\mathcal{C}$. The respective proofs of Lemma 2 and Lemma 3 are given in the Appendix.

Lemma 2: For all $l \in \{0, 1, \ldots, M/2-1\}$, code-group $\mathcal{C}_l$ consists of $2M$ distinct M-PSK Alamouti matrices. □

Lemma 3: Code-groups $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{M/2-1}$ are disjoint; that is, $\bigcap_{l=0}^{M/2-1} \mathcal{C}_l \equiv \emptyset$. □

In view of the code-group definition, Lemma 2, and Lemma 3, the following theorem holds.

Theorem 1: The set of all Alamouti matrices can be perfectly partitioned into the $M/2$ disjoint code-groups defined in (25); that is, $\mathcal{C} \equiv \{\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{M/2-1}\}$. □

As a follow-up to Theorem 1, we note the equivalence

$$\mathcal{C} \equiv \{\mathbf{B}^T \mathcal{R} \mathbf{T}_0, \mathbf{B}^T \mathcal{R} \mathbf{T}_1, \ldots, \mathbf{B}^T \mathcal{R} \mathbf{T}_{M/2-1}\} \equiv \mathbf{B}^T \mathcal{R} \mathcal{T}. \tag{26}$$

With the establishment of Theorem 1, the proclaimed systematic classification of the Alamouti matrices defined upon a certain M-PSK constellation is complete[2]. Next, we switch our attention from design to analysis.

[2]We notice that in the trivial case where $M = 2$ (BPSK), $\mathcal{C}$ is "partitioned" into a single code-group, $\mathcal{C} \equiv \mathcal{C}_0 \equiv \mathbf{B}^T \mathcal{R} \mathbf{T}_0 \equiv \mathbf{B}^T \mathcal{R}$.

For any M-PSK Alamouti matrix $\mathbf{A} \in \mathcal{C}$, we call $\mathbf{F} \in \mathbb{C}^{2\times 2}$ a valid *transition matrix* for $\mathbf{A}$, if and only if $\mathbf{AF} \in \mathcal{C}$. Since $\mathcal{C}$ consists of scaled unitary matrices (for all $\mathbf{A} \in \mathcal{C}$, $\mathbf{A}^H\mathbf{A} = \mathbf{A}\mathbf{A}^H = 2\mathbf{I}$), the M^2 valid transition matrices for a specific Alamouti matrix $\mathbf{A} \in \mathcal{C}$ form the set $\frac{1}{2}\mathbf{A}^H\mathcal{C}$. In this point, we denote by $\mathcal{F}_l$ the lth *group-transition set*, defined as the set of all valid transition matrices for all Alamouti matrices in the lth code-group $\mathcal{C}_l$, $l = 0, 1, \ldots, M/2-1$. Mathematically stated,

$$\mathcal{F}_l \triangleq \bigcup_{\mathbf{A}\in\mathcal{C}_l} \frac{1}{2}\mathbf{A}^H\mathcal{C}, \quad l = 0, 1, \ldots, M/2-1. \tag{27}$$

Following Lemma 1, the definition of the code-groups in (25), and Theorem 1, we can re-express the lth group-transition set as

$$\mathcal{F}_l \equiv \frac{1}{2}\mathcal{C}_l^H\mathcal{C} \equiv \frac{1}{2}\mathbf{T}_l^H\mathcal{R}^H\mathbf{B}\mathbf{B}^T\mathcal{R}\mathcal{T} \equiv \mathbf{T}_l^H\mathcal{R}\mathcal{T}, \quad l = 0, 1, \ldots, M/2-1. \tag{28}$$

We observe that, since both $\mathbf{B}$ and $\mathbf{T}_l$, $l = 0, 1, \ldots, M/2-1$, are unitary matrices, $|\mathcal{C}| = |\mathcal{R}\mathcal{T}| = |\mathcal{F}_l| = M^2$, for all $l \in \{0, 1, \ldots, M/2-1\}$, where $|\mathcal{S}|$ denotes the cardinality of set $\mathcal{S}$. This conclusion, along with the union definition of $\mathcal{F}_l$ in (27), verifies the following lemma[3].

Lemma 4: For all $l \in \{0, 1, \ldots, M/2-1\}$, the elements of $\mathcal{F}_l$ are valid transition matrices for all Alamouti matrices in $\mathcal{C}_l$; that is, $\mathcal{C}_l\mathcal{F}_l \equiv \mathcal{C}$, $l = 0, 1, \ldots, M/2-1$. $\square$

Subsequently, we aim at exploring the correlations among the group-transition sets. In this direction, we define the *compound transition set* as the set of the valid transition matrices for all Alamouti matrices in $\mathcal{C}$; that is,

$$\mathcal{F} \triangleq \bigcup_{\mathbf{A}\in\mathcal{C}} \frac{1}{2}\mathbf{A}^H\mathcal{C}. \tag{29}$$

In view of (26), the compound transition set can be re-expressed as

$$\mathcal{F} \equiv \frac{1}{2}\mathcal{C}^H\mathcal{C} \equiv \frac{1}{2}\mathcal{T}^H\mathcal{R}^H\mathbf{B}\mathbf{B}^T\mathcal{R}\mathcal{T} \equiv \mathcal{T}^H\mathcal{R}\mathcal{T}. \tag{30}$$

Thus, $|\mathcal{F}| \leq |\mathcal{T}||\mathcal{R}\mathcal{T}| = M^3/2$ and, in the non-trivial case where $M > 2$, there certainly exist more than one transition matrices in $\mathcal{F}$ that appear in more than one group-transition sets[4]; in other

[3]Alternatively, $\mathcal{C}_l\mathcal{F}_l \equiv \mathbf{B}^T\mathcal{R}\mathbf{T}_l\mathbf{T}_l^H\mathcal{R}\mathcal{T} \equiv \mathbf{B}^T\mathcal{R}\mathcal{T} \equiv \mathcal{C}$, $l = 0, 1, \ldots, M/2-1$.

[4]For $M = 2$, $\mathcal{F} \equiv \mathcal{F}_0 \equiv \mathcal{R}$ and $|\mathcal{F}| = |\mathcal{R}| = 2M = M^3/2$.

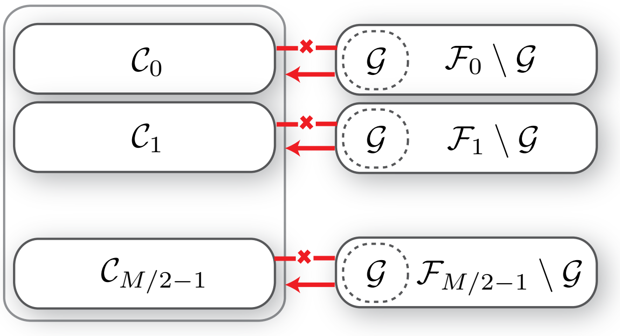

Fig. 1: Schematic representation of Lemma 4 and Theorem 2.

words, the group-transition sets are overlapping. In fact, a rigorous study on their intersections results in the following lemma, the proof of which can be found in the Appendix of this work.

Lemma 5: The intersection of any two group-transition sets consists of exactly $2M$ matrices; that is, $|\mathcal{F}_l \cap \mathcal{F}_k| = 2M$, for all $l \in \{0, 1, \ldots, M/2-1\}$ and $k \in \{0, 1, \ldots, M/2-1\} \setminus l$. □

Next, we introduce the *global transition set*

$$\mathcal{G} \triangleq \bigcup_{l=0}^{M-1} \left\{ \begin{bmatrix} \mu^l & 0 \\ 0 & \mu^{-l} \end{bmatrix}, \begin{bmatrix} 0 & \mu^l \\ -\mu^{-l} & 0 \end{bmatrix} \right\}. \tag{31}$$

Evidently, the cardinality of $\mathcal{G}$ is $2M$ and $\mathcal{C}\mathcal{G} \equiv \mathcal{C}$, since, for all $\mathbf{A} \in \mathcal{C}$ and $\mathbf{G} \in \mathcal{G}$, $\mathbf{AG} \in \mathcal{C}$. Hence, for all $l \in \{0, 1, \ldots, M/2-1\}$, $\mathcal{F}_l \cap \mathcal{G} \equiv \mathcal{G}$ and for all $k \in \{0, 1, \ldots, M/2-1\} \setminus l$, $\mathcal{G} \subseteq \mathcal{F}_l \cap \mathcal{F}_k$. This conclusion, along with Lemma 5, verifies the following theorem, which brings to an end our analysis on the properties of the presented classification of Alamouti matrices.

Theorem 2: $\mathcal{G}$ is a subset of all group-transition sets, while each of the transition matrices in $\mathcal{F} \setminus \mathcal{G}$ may belong to one and only group-transition set. □

An alternative way Theorem 2 can be interpreted is

$$\mathcal{F}_l \cap \mathcal{F}_k \equiv \mathcal{G}, \tag{32}$$

for all $l \in \{0, 1, \ldots, M/2-1\}$ and $k \in \{0, 1, \ldots, M/2-1\} \setminus l$. For clarity purposes, Fig. 1 depicts a schematic representation of Lemma 4 and Theorem 2.

B. Differential Alamouti Encoding

To initialize transmission, the transmitter sends an arbitrary Alamouti matrix $\mathbf{C}(\mathbf{s}^{(0)}) \in \mathcal{C}$, that conveys no information. Thereafter, the transmission procedure resumes as follows.

The kth Alamouti matrix transmitted is differentially defined as

$$\mathbf{C}(\mathbf{s}^{(k)}) = \mathbf{C}(\mathbf{s}^{(k-1)})\mathbf{D}_k, \quad k = 1, 2, \ldots, P-1, \tag{33}$$

where $\mathbf{D}_k$ is the kth, so called, transition code and conveys the information bits for the kth block transmission. Certainly, if one makes no use of the encoders knowledge on the previously transmitted code, the set of all candidate transition codes for the kth Alamouti transmission must be a subset of $\mathcal{G}$, so that $\mathbf{C}(\mathbf{s}^{(k)})$ is guaranteed to be a valid Alamouti matrix. Hence, the number of information bits that can be encoded is upper bounded by $\log_2 2M$, a bound met, if all matrices in $\mathcal{G}$ are available for the kth transition. Evidently, this memoryless method, considered to be the state-of-the-art differential Alamouti encoding scheme [12], imposes significant rate degradation by restricting the number of possible Alamouti matrices for the kth transmission to $2M$: given $\mathbf{C}(\mathbf{s}^{(k-1)})$, $\mathbf{C}(\mathbf{s}^{(k)})$ may only belong to the subset of $\mathcal{C}$ that is reachable by $\mathbf{C}(\mathbf{s}^{(k-1)})$ using solely global transition matrices.

In the proposed differential Alamouti encoding method, contrary to any other proposed scheme, the transmitter exploits its knowledge on the previously transmitted block in the transition code selection process to achieve differential encoding of $2\log_2 M$ bits per Alamouti transmission. Being aware of $\mathbf{C}(\mathbf{s}^{(k-1)})$ and, hence, the code-group it belongs, the encoder is able to choose $\mathbf{D}_k$ from the whole respective group-transition set of cardinality M^2; that is, if $\mathbf{C}(\mathbf{s}^{(k-1)}) \in \mathcal{C}_l$, for some $l \in \{0, 1, \ldots, M/2-1\}$, any matrix from $\mathcal{F}_l$ can be utilized for the kth transition, providing the essential guarantee that $\mathbf{C}(\mathbf{s}^{(k)})$ will belong in $\mathcal{C}$.

C. Unambiguous Decodability of the Sequence Detector

To initialize the decoding process, the receiver makes a decision $\hat{\mathbf{s}} \in {\mathcal{A}_M}^{2P}$ on the transmitted symbol sequence using the ML detector in (18). Then, it builds the respective Alamouti sequence

Input:
$\mathcal{D}$: The set of all bit sequences of length $2\log_2 M$.
$\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{M/2-1}$: The $M/2$ group-transition sets.
$\mathcal{G}$: The set of global transition matrices.
Initialization:
$\mathcal{D}_G, \mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_{M/2-1} \equiv \emptyset$.
Step 1:
For all $\mathbf{F} \in \mathcal{G}$
    Choose arbitrarily a bit sequence $b \in \mathcal{D} \setminus \mathcal{D}_G$ and assign it to $\mathbf{F}$.
    Update $\mathcal{D}_G \equiv \mathcal{D}_G \cup \{b\}$.
Set $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_{M/2-1} \equiv \mathcal{D}_G$.
Step 2:
For $l = 0, 1, \ldots, M/2 - 1$
    For all $\mathbf{F} \in \mathcal{F}_l \setminus \mathcal{G}$
        Choose arbitrarily a bit sequence $b \in \mathcal{D} \setminus \mathcal{D}_l$ and assign it to $\mathbf{F}$.
        Update $\mathcal{D}_l \equiv \mathcal{D}_l \cup \{b\}$.
Output:
An instance of the full-rate codebook.

Fig. 2: The algorithm for the construction of a full-rate codebook.

$\mathbf{C}(\hat{\mathbf{s}}^{(0)}), \mathbf{C}(\hat{\mathbf{s}}^{(1)}), \ldots, \mathbf{C}(\hat{\mathbf{s}}^{(P-1)})$ and, in accordance with the differential encoding procedure, computes the kth information-bearing transition code by

$$\hat{\mathbf{D}}_k = \frac{1}{2}\mathbf{C}^H(\hat{\mathbf{s}}^{(k-1)})\mathbf{C}(\hat{\mathbf{s}}^{(k)}), \tag{34}$$

for $k = 1, 2, \ldots, P-1$. In view of (19), all equivalently optimal, in terms of (18), symbol sequences will correspond w.p.1 to the same information-bearing transition code sequence $\hat{\mathbf{D}}_1, \hat{\mathbf{D}}_2, \ldots, \hat{\mathbf{D}}_{P-1}$. At this point, we exploit the properties of the introduced systematic classification of Alamouti matrices to deliver an algorithm for the construction of a differential encoding/decoding codebook that will allow for the unambiguous decoding of the detected Alamouti sequence. The codebook construction algorithm lies in Fig. 2.

This codebook design guarantees that, in every group-transition set, each of the M^2 bit sequences of length $2\log_2 M$ will be assigned to a distinct transition matrix. Moreover, each transition matrix in $\mathcal{F}$ will correspond to a unique bit sequence, regardless of the group-transition set(s) it appears in. Thus, the kth detected transition code $\hat{\mathbf{D}}_k$, $k = 1, 2, \ldots, P-1$, will be unambiguously decoded by being mapped to a distinct bit sequence of length $2\log_2 M$. Thus,

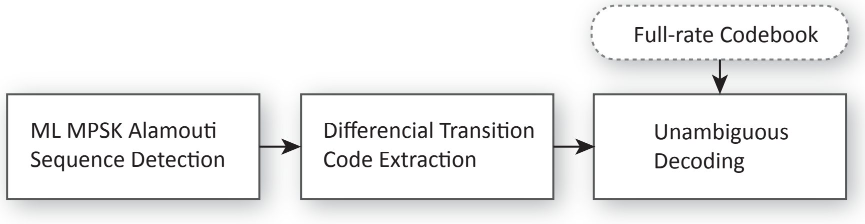

Fig. 3: Block diagram of the proposed full-rate receiver.

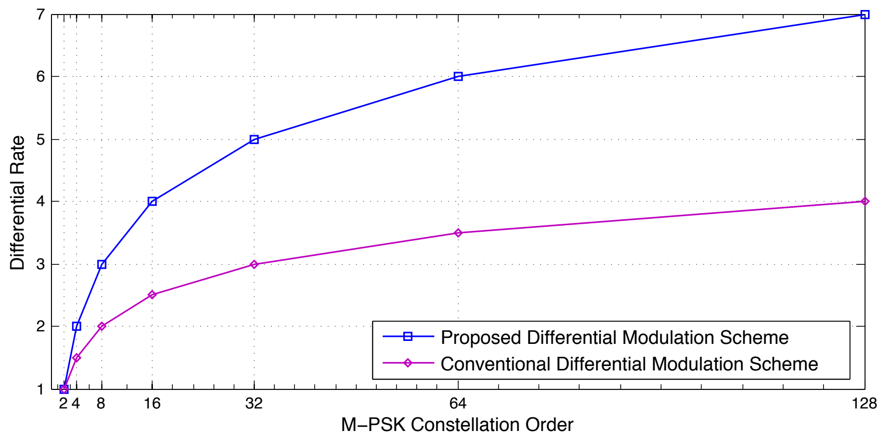

Fig. 4: Differential rate (in bits per transmit antenna) achieved by the proposed and the conventional ([12]) differential modulation schemes, versus the constellation order M.

according to [12], the differential rate attained equals

$$R = \frac{2\log_2 M}{2} = \log_2 M \text{ bits per transmit antenna.} \tag{35}$$

We recall that the differential rate achieved by means of the conventional differential Alamouti encoding scheme (utilizing solely global transition codes) equals $\log_2 \sqrt{2M}$ bits per transmit antenna [12]. In Fig. 3 we present the block diagram of the proposed receiver, while Fig. 4 holds a comparison between R and $\log_2 \sqrt{2M}$ for varying constellation order M.

IV. ML M-ary Sequence Detection with Polynomial Complexity

In this section, we prove that the complexity of the ML sequence detector in (18) can be polynomial in the sequence length P. Interestingly, the order of the polynomial complexity depends strictly on the number of antennas used at the receiver. We begin our developments by observing that the concatenated matrix of the transmitted Alamouti codes, introduced in (6), can take the form

$$\mathbf{G}(\mathbf{s}) = \begin{bmatrix} \mathbf{s}^T \\ \mathbf{s}^H \left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right) \end{bmatrix}. \tag{36}$$

Then, using (9) and (36), we rewrite vector $(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_{M_r})\,\mathbf{y}$ that appears in (18) as

$$(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_{M_r})\,\mathbf{y} = \mathrm{vec}\left(\mathbf{Y}\mathbf{G}^H(\mathbf{s})\,\mathbf{I}_2\right) = (\mathbf{I}_2 \otimes \mathbf{Y})\,\mathrm{vec}\left(\mathbf{G}^H(\mathbf{s})\right) = \begin{bmatrix} \mathbf{Y}\mathbf{s}^* \\ \mathbf{Y}\left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \mathbf{s} \end{bmatrix}. \tag{37}$$

Accordingly, the maximization argument in (18) can be rewritten as

$$\|(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_{M_r})\,\mathbf{y}\|^2 = \|\mathbf{Y}\mathbf{s}^*\|^2 + \|\mathbf{Y}\left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \mathbf{s}\|^2 \tag{38}$$

$$= \|\mathbf{Y}^*\mathbf{s}\|^2 + \|\mathbf{Y}\left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \mathbf{s}\|^2 \tag{39}$$

$$= \|\boldsymbol{\Gamma}^H\mathbf{s}\|^2, \tag{40}$$

where $\boldsymbol{\Gamma} \triangleq \begin{bmatrix} \mathbf{Y}^T & \left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right) \mathbf{Y}^H \end{bmatrix} \in \mathbb{C}^{2P \times 2M_r}$. Finally, the ML sequence detector in (18) becomes

$$\hat{\mathbf{s}} = \arg \max_{\mathbf{s} \in {\mathcal{A}_M}^{2P}} \mathbf{s}^H \boldsymbol{\Gamma}\boldsymbol{\Gamma}^H \mathbf{s}. \tag{41}$$

For $2P \geq M_r$, which is a rather legitimate assumption, $\mathrm{rank}(\boldsymbol{\Gamma}) = 2Mr$ and the the rank of the quadratic form in the maximization argument of (41) is not a function of the problem size. In the light of this analysis, we tailor to (41) the algorithm presented in [14] for the problem of rank-deficient quadratic form maximization over M-phase alphabet and establish that the initial ML sequence detection problem of (18) is, in fact, solvable in polynomial time $\mathcal{O}\left((MP)^{4M_r}\right)$. Interestingly, the order of the polynomial is solely dictated by the number of antennas at the receiver. In Fig. 5, we present the complexity order of the proposed sequence detector along with the complexity of the conventional (exhaustive) one versus the sequence length P, for $M = 4, 16$ and $M_r = 1$.

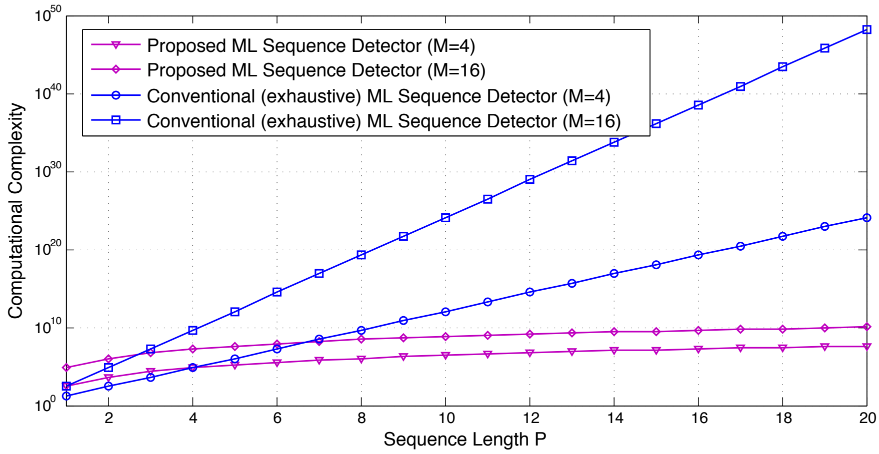

Fig. 5: Computational complexity of the proposed ML sequence detector and the conventional (exhaustive) sequence detector, versus the sequence length P, for $M = 4, 16$ and $M_r = 1$.

V. Simulation Studies

In this section, we carry out a simulation study on the bit-error rate (BER) performance of the proposed differential modulation scheme. Specifically, we consider the signal model described in Section II, for $M = 4$, $M_r = 1$, $\sigma_h^2 = 1$, and $\sigma_v^2 = 1$ and attempt the communication of 36 bits under fixed power budget uniformly distributed among the consecutive Alamouti transmissions. In Fig. 6, we plot the BER attained by the proposed scheme over 1 000 independent simulation runs, as a function the overall power budget. For reference purposes we include the respective plot for the conventional rate-deficient differential modulation scheme [12] and the theoretical lower bound, set by the coherent ML detector. As clearly documented, the proposed differential scheme outperforms the counterpart, due to its rate efficiency.

VI. Conclusions

In this work, we have considered M-PSK Alamouti transmissions and developed a novel differential modulation scheme that attains full rate for any constellation order. In contrast to past work, the proposed scheme guarantees that the encoded matrix maintains in the set of M-PSK Alamouti matrices while, at the same time, attains full rate so that all possible sequences of Alamouti transmissions become valid. Then, based on recent results in the context of reduced-

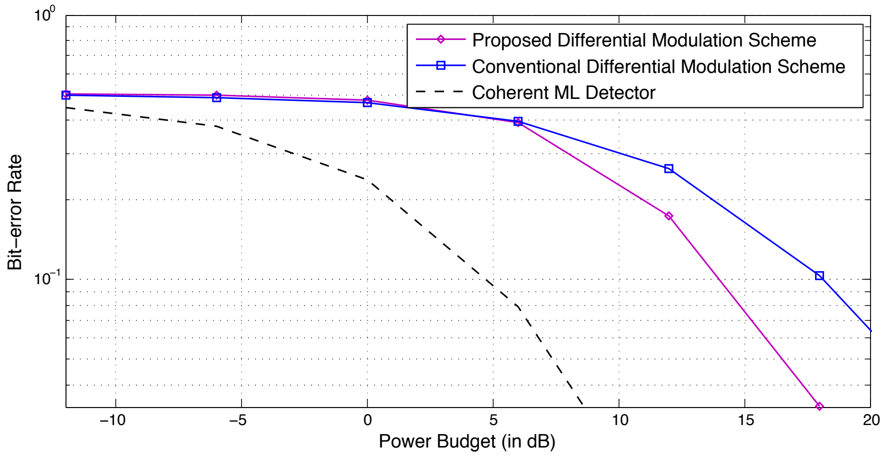

Fig. 6: BER versus overall power budget for the communication of 36 bits ($M = 4$, $M_r = 1$, $\sigma_h^2 = 1$, and $\sigma_v^2 = 1$).

rank quadratic-form maximization over an M-PSK alphabet, we exploit the full-rate property of the proposed scheme to develop a novel polynomial-complexity ML noncoherent sequence decoder.

APPENDIX

A. Proof of Lemma 1

Consider $m, m' \in \{0, 1, \ldots, M-1\}$ and $\gamma, \gamma' \in \{-1, 1\}$. In view of (21), and keeping in mind that $\mathbf{B}$ is a unitary matrix, $\mathbf{R}_{m,\gamma} = \mathbf{R}_{m',\gamma'}$, if and only if $(m, \gamma) = (m', \gamma')$. Thus, the cardinality of R is $2M$. Moreover, working on (21), we obtain $-\mathbf{R}_{m,\gamma} = \mathbf{R}_{(m-M/2) \bmod M,\gamma}$, $\mathbf{R}^*_{m,\gamma} = \mathbf{R}_{(-m) \bmod M,\gamma}$, $\mathbf{R}^T_{m,\gamma} = \gamma \mathbf{R}_{m,\gamma}$, and $\mathbf{R}_{m,\gamma}\mathbf{R}_{m',\gamma'} = \begin{cases} \gamma \mathbf{R}_{(m+\gamma m') \bmod M,1}, & \gamma = \gamma' \\ \mathbf{R}_{(m+\gamma m') \bmod M,-1}, & \gamma = -\gamma' \end{cases}$, where $(\cdot) \bmod (\cdot)$ denotes the remainder of the floored division, so that $\forall a, n \in \mathbb{Z}$, $a \bmod n = a - \lfloor \frac{a}{n} \rfloor n \in \{0, 1, \ldots, n-1\}$ [22]. Therefore, $\forall a \in \mathbb{Z}$, $a \bmod M \in \{0, 1, \ldots, M-1\}$ and $-\mathbf{R}_{m,\gamma}, \mathbf{R}^*_{m,\gamma}, \mathbf{R}^T_{m,\gamma}, \mathbf{R}_{m,\gamma}\mathbf{R}_{m',\gamma'} \in \mathcal{R}$, for all $m, m' \in \{0, 1, \ldots, M-1\}$ and $\gamma, \gamma' \in \{-1, 1\}$. ■

B. Proof of Lemma 2

Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be two elements of $\mathcal{C}_l$, for some $l \in \{0, 1, \ldots, M/2-1\}$. Then, by the definition of the code-groups in (25), there exist $m, m' \in \{0, 1, \ldots, M-1\}$ and $\gamma, \gamma' \in \{-1, 1\}$, such that $\mathbf{A}_1 = \mathbf{B}^T \mathbf{R}_{m,\gamma} \mathbf{T}_l$ and $\mathbf{A}_2 = \mathbf{B}^T \mathbf{R}_{m',\gamma'} \mathbf{T}_l$. For the first part of this lemma, we show that $\mathbf{A}_1$ is an element of $\mathcal{C}$, by expanding it as

$$\mathbf{A}_1 = \begin{cases} \begin{bmatrix} \mu^{m} & \mu^{(l+m) \bmod M} \\ -\mu^{-((l+m) \bmod M)} & \mu^{-m} \end{bmatrix}, & \gamma = 1 \\ \begin{bmatrix} \mu^{(m-l) \bmod M} & \mu^{(m+M/2) \bmod M} \\ -\mu^{-((m+M/2) \bmod M)} & \mu^{-((m-l) \bmod M)} \end{bmatrix}, & \gamma = -1 \end{cases}. \tag{42}$$

Concerning the second part of this lemma, since $\mathbf{B}$ and $\mathbf{T}_l$ are unitary matrices, $\mathbf{A}_1 = \mathbf{A}_2$, if and only if $\mathbf{R}_{m,\gamma} = \mathbf{R}_{m',\gamma'}$. However, by Lemma 1, the latter holds, if and only if $(m, \gamma) = (m', \gamma')$. Thus, $|\mathcal{C}_l| = 2M$, for all $l \in \{0, 1, \ldots, M/2-1\}$. ■

C. Proof of Lemma 3

We consider two Alamouti codes $\mathbf{A}_1 = \mathbf{B}^T \mathbf{R}_{m,\gamma} \mathbf{T}_l$ and $\mathbf{A}_2 = \mathbf{B}^T \mathbf{R}_{m',\gamma'} \mathbf{T}_{l'}$, for some $m, m' \in \{0, 1, \ldots, M-1\}$, $\gamma, \gamma' \in \{-1, 1\}$, and $l, l' \in \{0, 1, \ldots, M/2-1\}$. Subsequently, we follow the expansion of $\mathbf{A}_1$ and $\mathbf{A}_2$ as in (42) and prove that $\mathbf{A}_1 = \mathbf{A}_2$, if and only if $(m, \gamma, l) = (m', \gamma', l')$. For $\gamma = \gamma'$, it is evident that $\mathbf{A}_1 = \mathbf{A}_2$, if and only if $(m, l) = (m', l')$. On the other hand, for

$\gamma = -\gamma'$ (let $\gamma = 1$, w.l.o.g.), we distinguish the following complementary cases. *Case 1:* $M/2 \leq m' < M$. In this case, $(m'+M/2) \bmod M = m' - M/2$ and $(m'-l') \bmod M = m'-l'$. Thus, if $l+m < M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' - M/2$, while if $l+m \geq M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' + M/2$. Hence, in this case, $\mathbf{A}_1 \neq \mathbf{A}_2$. *Case 2:* $0 \leq m' < M/2$. In this case, $(m' + M/2) \bmod M = m' + M/2$. Next, we distinguish two sub-cases. In the first sub-case, $0 \leq m' - l' < M$ and $(m' - l') \bmod M = m' - l'$. Thus, if $l + m < M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' + M/2$, while if $l + m \geq M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' + 3M/2$. In the second sub-case, $m' - l' < 0$ and $(m' - l') \bmod M = m' - l' + M$. Thus, if $l + m < M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' - M/2$, while if $l + m \geq M$, $\mathbf{A}_1 = \mathbf{A}_2$, only if $l = l' + M/2$. Hence, in this case, $\mathbf{A}_1 \neq \mathbf{A}_2$ as well. Summarizing, $\mathbf{A}_1 = \mathbf{A}_2$, if and only if $(m, \gamma, l) = (m', \gamma', l')$, and, consequently, $\mathcal{C}_l \cap \mathcal{C}_{l'} \equiv \emptyset$, for every $l' \in \{0, 1, \ldots, M/2 - 1\} \setminus l$. ■

D. Proof of Lemma 5

For any $l \in \{0, 1, \ldots, M/2 - 1\}$ and $k \in \{0, 1, \ldots, M/2 - 1\} \setminus l$, the cardinality of $\mathcal{F}_l \cap \mathcal{F}_k$ equals the number of matrices in $\mathcal{F}_k$ that are valid transition matrices for every $\mathbf{A} \in \mathcal{C}_l$. In this proof, we fix arbitrary $j \in \{0, 1, \ldots, M-1\}$ and $\gamma \in \{-1, 1\}$ and demonstrate that there are exactly $2M$ elements of $\mathcal{F}_{l'}$ that are valid transition matrices for $\mathbf{A} = \mathbf{B}^T \mathbf{R}_{j,\gamma} \mathbf{T}_l$. To proceed, we expand $\mathbf{A}$ as

$$\mathbf{A} = \mathbf{B}^T \mathbf{R}_{j,\gamma} \mathbf{T}_l = \begin{cases} \begin{bmatrix} \mu^l & 0 \\ 0 & \mu^{-l} \end{bmatrix} \begin{bmatrix} 1 & \mu^j \\ -\mu^{-j} & 1 \end{bmatrix}, & \gamma = 1 \\ \begin{bmatrix} 0 & -\mu^l \\ \mu^{-l} & 0 \end{bmatrix} \begin{bmatrix} 1 & \mu^j \\ -\mu^{-j} & 1 \end{bmatrix}, & \gamma = -1 \end{cases}. \tag{43}$$

and re-express the kth group-transition set as

$$\mathcal{F}_k \equiv \mathbf{T}_k^H \mathcal{R} \mathcal{T} \equiv \frac{1}{2} \begin{bmatrix} 1 & -\mu^k \\ \mu^{-k} & 1 \end{bmatrix} \mathbf{B}^T \mathcal{R} \mathcal{T} \equiv \frac{1}{2} \begin{bmatrix} 1 & -\mu^k \\ \mu^{-k} & 1 \end{bmatrix} \mathcal{C}. \tag{44}$$

Next, we consider $\mathbf{F} = \frac{1}{2} \begin{bmatrix} 1 & -\mu^k \\ \mu^{-k} & 1 \end{bmatrix} \begin{bmatrix} \mu^m & \mu^n \\ -\mu^{-n} & \mu^{-m} \end{bmatrix}$ to be an arbitrarily chosen transition matrix in $\mathcal{F}_k$, for some $m, n \in \{0, 1, \ldots, M-1\}$. In the sequel, we show that there are exactly $2M$ values of (m, n), such that $\mathbf{AF}$ is an Alamouti code. Following (43) and (44), $\mathbf{AF} \in \mathcal{C}$, if and only if $\begin{bmatrix} 1 & \mu^j \\ -\mu^{-j} & 1 \end{bmatrix} \mathbf{F} \in \mathcal{C}$; that is, if and only if

$$\frac{1}{2}\begin{bmatrix} \mu^n + \mu^{j-k+n} + \mu^{k-m} + \mu^{j-m+M/2} & \mu^m + \mu^{j-k+m} + \mu^{k-n+M/2} + \mu^{j-n} \\ -\mu^{-m} - \mu^{-j+k-m} - \mu^{-k+n-M/2} - \mu^{-j+n} & \mu^{-n} + \mu^{-j+k-n} + \mu^{-k+m} + \mu^{-j+m-M/2} \end{bmatrix} \in \mathcal{C}. \tag{45}$$

By inspection, for (45) to hold, it must either $\mu^{m+n} = \mu^k$, or $\mu^{m+n} = \mu^{k+M/2}$. Evidently, for any fixed $k \in \{0, 1, \ldots, M/2-1\}$, there are exactly M distinct values of (m, n) that satisfy each one of these conditions. Hence, there are in total $2M$ distinct values of (m, n), so that $\mathbf{AF} \in \mathcal{C}$, and $|\mathcal{F}_l \cap \mathcal{F}_k| = 2M$, for all $l \in \{0, 1, \ldots, M/2-1\}$ and $k \in \{0, 1, \ldots, M/2-1\} \setminus l$. ■

REFERENCES

[1] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451-1458, Oct. 1998.

[2] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1456-1467, July 1999.

[3] E. G. Larsson, P. Stoica, and J. Li, "On maximum-likelihood detection and decoding for space-time coding systems," *IEEE Trans. Signal Process.*, vol. 50, pp. 937-944, Apr. 2002.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, pp. 744-765, Mar. 1998.

[5] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 45, pp. 139-157, Jan. 1999.

[6] B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1962-1973, Sept. 2000.

[7] E. G. Larsson, P. Stoica, and J. Li, "Orthogonal space-time block codes: Maximum likelihood detection for unknown channels and unstructured interferences," *IEEE Trans. Signal Process.*, vol. 51, pp. 362-372, Feb. 2003.

[8] T. Cui and C. Tellambura, "Efficient blind receiver design for orthogonal space-time block codes," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 1890-1899, May 2007.

[9] G. Ganesan and P. Stoica, "Differential modulation using space-time block codes," *IEEE Sig. Proc. Letters*, vol. 9, no. 2, Sept. 2002.

[10] E. G. Larsson and P. Stoica, "On maximum-likelihood detection and decoding for space-time coding systems," *IEEE Trans. Signal Process.,* vol. 50, no. 4, Apr. 2002.

[11] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 7, July 2000.

[12] B. L. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, Nov. 2000.

[13] X. Shao and J. Yuan, "A new differential space-time block coding scheme," *IEEE Commun. Letters*, vol. 7, no. 9, Sept. 2003.

[14] A. T. Kyrillidis and G. N. Karystinos, "Rank-deficient quadratic-form maximization over M-phase alphabet: Polynomial-complexity solvability and algorithmic developments," in *Proc. IEEE ICASSP 2011 - Intern. Conf. Acoust., Speech and Signal Proc.*, Prague, Czech Republic, May 2011.

[15] A. Graham, *Kronecker Products and Matrix Calculus with Applications*. Chichester, U.K.: Ellis Horwood, 1981.

[16] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*. Philadelphia, PA: SIAM, 2000.

[17] 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.*, vol. 54, pp. 738-751, Feb. 2006.

[18] D. S. Papailiopoulos and G. N. Karystinos, "Maximum-likelihood noncoherent OSTBC detection with polynomial complexity," *IEEE Trans. Wireless Commun.*, vol. 9, June 2010.

[19] W. Su, S. N. Batalama and D. A. Pados, "On orthogonal space-time block codes and transceiver signal linearization," *IEEE Commun. Letters*, vol. 10, Feb. 2006.

[20] E. G. Larsson and P. Stoica, *Space-time block coding for wireless communications*. Cambridge, U.K.: Cambridge University Press, 2003.

[21] W.-K. Ma, "Blind ML detection of orthogonal space-time block codes: Identifiability and code construction," *IEEE Trans. Signal Process.*, vol. 55, pp. 3312-3324, July 2007.

[22] D. E. Knuth, *The Art of Computer Programming*, vol. 1, *Fundamental Algorithms*. Reading, MA: Addison-Wesley, 1972.