NOVEL FULL-RATE NONCOHERENT ALAMOUTI ENCODING THAT ALLOWS POLYNOMIAL-COMPLEXITY OPTIMAL DECODING

Panos P. Markopoulos

Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
E-mail: pmarkopo@buffalo.edu

George N. Karystinos

Department of Electronic and Computer Engineering
Technical University of Crete
Chania, 73100, Greece
E-mail: karystinos@telecom.tuc.gr

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. The latter property is exploited to develop a polynomial-complexity maximum-likelihood noncoherent sequence decoder whose order is solely determined by the number of receive antennas. We show that the proposed scheme is superior to contemporary alternatives in terms of encoding rate, decoding complexity, and performance.

1. 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, 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]-[8]. If sequence detection is performed through exhaustive search among all possible data sequences, then exponential computational complexity is required. Moreover, 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 [9]. Interestingly, by means of differential space-time modulation (DSTM), this ambiguity problem can be easily resolved (see [10] and [11], based on the DSTM initially introduced in [12], [13]). However, all these schemes appear to be inefficient in terms of both transmission rate and computational complexity at the detector. In [14], ML noncoherent detection of full-rate QPSK OSTBC encoded data was proposed, which, however, utilizes a Viterbi decoder with prohibitive computational cost.

In this work, we propose for the first time a full-rate differential M-ary phase-shift keying (M-PSK) Alamouti scheme that also allows ML noncoherent sequence detection in polynomial time and does not suffer from code-induced ambiguity under Rayleigh fading. We tailor to our detection problem the algorithm in [15] and obtain a polynomial-time solution. We note that the polynomial complexity order is solely determined by the number of antennas used at the receiver. This is in sharp contrast to sphere-decoding approaches for ML blind detection [6], [7] that have exponential complexity.

This research has been co-financed by the European Union (European Social Fund ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) Research Funding Program THALES: Investing in knowledge society through the European Social Fund.

2. SYSTEM MODEL AND PROBLEM STATEMENT

We consider transmission of Alamouti matrices built upon M-PSK symbols. Each transmitted matrix $\mathbf{C}(\mathbf{a})$ corresponds to a 2×1 symbol vector $\mathbf{a} = \begin{bmatrix} a_1 & a_2 \end{bmatrix}^T \in \mathcal{A}_M^2$, where $\mathcal{A}_M \triangleq \{e^{j2\pi m/M} \mid m = 0, 1, \ldots, M-1\}$ and $M \in \{2^k \mid k = 1, 2, \ldots\}$, and is given by

$$\mathbf{C}(\mathbf{a}) = \begin{bmatrix} a_1 & a_2 \\ -a_2^* & a_1^* \end{bmatrix}. \quad (1)$$

Notice that Alamouti matrices are scaled unitary: $\mathbf{C}^H(\mathbf{a})\mathbf{C}(\mathbf{a}) = \mathbf{C}(\mathbf{a})\mathbf{C}^H(\mathbf{a}) = 2\mathbf{I}_2$. The communicated M-PSK sequence $\mathbf{s}$ 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 assume that the receiver is employed with D antennas and the channel remains stable during the interval of P successive Alamouti transmissions. The downconverted and pulse-matched equivalent ith received block of size $D \times 2$ is

$$\mathbf{Y}^{(i)} = \mathbf{H}\mathbf{C}(\mathbf{s}^{(i)}) + \mathbf{V}^{(i)} \quad (2)$$

where $\mathbf{H} \in \mathbb{C}^{D \times 2}$ represents the channel matrix between the 2 transmit and D 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. $\mathbf{V}^{(i)} \in \mathbb{C}^{D \times 2}$ denotes zero-mean additive spatially and temporally white circular complex Gaussian noise matrix with covariance $\sigma_v^2 \mathbf{I}_D$. The channel and noise matrices $\mathbf{H}$ and $\mathbf{V}^{(i)}$, respectively, are independent of each other.

In this work, we consider the channel matrix $\mathbf{H}$ to be unavailable to the receiver. Hence, 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 $D \times 2P$ observation matrix

$$\mathbf{Y} \triangleq \begin{bmatrix} \mathbf{Y}^{(0)} & \ldots & \mathbf{Y}^{(P-1)} \end{bmatrix} = \mathbf{H}\mathbf{G}(\mathbf{s}) + \mathbf{V} \quad (3)$$

where $\mathbf{V} \triangleq \left[\begin{array}{ccc} \mathbf{V}^{(0)} & \dots & \mathbf{V}^{(P-1)} \end{array} \right]$ and $\mathbf{G}(\mathbf{s})$ is the concatenated matrix of the transmitted Alamouti matrices

$$\mathbf{G}(\mathbf{s}) \triangleq \left[\begin{array}{ccc} \mathbf{C}(\mathbf{s}^{(0)}) & \dots & \mathbf{C}(\mathbf{s}^{(P-1)}) \end{array} \right] \in \mathbb{C}^{2\times 2P} \quad (4)$$

that satisfies the orthogonality property $\mathbf{G}(\mathbf{s})\mathbf{G}^H(\mathbf{s}) = 2P\mathbf{I}_2$. The ML detector makes the decision

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}_M{}^{2P}} f(\mathbf{Y}|\mathbf{s}) = \arg\max_{\mathbf{s}\in\mathcal{A}_M{}^{2P}} f(\mathbf{y}|\mathbf{s}) \quad (5)$$

where $\mathbf{y} \triangleq \text{vec}(\mathbf{Y}) \in \mathbb{C}^{2DP}$ and $f(\cdot|\cdot)$ represents the pertinent matrix/vector probability density function of the channel output conditioned on a symbol sequence. After algebraic computations and using $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$ [16], the optimization problem in (5) is rewritten as

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}_M{}^{2P}} \frac{1}{\pi^{2DP}|\mathbf{C}_y(\mathbf{s})|} \exp\{-\mathbf{y}^H\mathbf{C}_y^{-1}(\mathbf{s})\mathbf{y}\}. \quad (6)$$

where $\mathbf{C}_y(\mathbf{s}) = \sigma_h^2 \left(\mathbf{G}^T(\mathbf{s}) \otimes \mathbf{I}_D\right)\left(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_D\right) + \sigma_v^2\mathbf{I}_{2DP}$. Next, using Sylvester's determinant theorem and Sherman-Morrison-Woodbury formula [17], we rewrite the maximization problem in (6) as

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}_M{}^{2P}} \|\left(\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_D\right)\mathbf{y}\|^2. \quad (7)$$

A natural approach to (7) would be an exhaustive search among all M^{2P} symbol sequences $\mathbf{s} \in \mathcal{A}_M{}^{2P}$. However, such a receiver has two major drawbacks. First, it is impractical even for moderate values of P, since its complexity grows exponentially with P and, second, 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 $\hat{\mathbf{s}}_1 \in \mathcal{A}_M{}^{2P}$ to be a solution to the maximization problem in (7) and $\mathbf{C}(\hat{\mathbf{s}}_1^{(0)}), \mathbf{C}(\hat{\mathbf{s}}_1^{(1)}), \dots, \mathbf{C}(\hat{\mathbf{s}}_1^{(P-1)})$ to be the corresponding optimal Alamouti matrix sequence. Due to characteristic rotatability of Alamouti matrices [9], [18], there always exists at least one 2×2 unitary rotation matrix $\mathbf{\Theta} \neq \mathbf{I}_2$, so that $\mathbf{\Theta}\mathbf{C}(\hat{\mathbf{s}}_1^{(0)})$, $\mathbf{\Theta}\mathbf{C}(\hat{\mathbf{s}}_1^{(1)}), \dots, \mathbf{\Theta}\mathbf{C}(\hat{\mathbf{s}}_1^{(P-1)})$ is a valid Alamouti code sequence too, corresponding, however, to a different M-PSK symbol sequence, say $\hat{\mathbf{s}}_2$. Evidently, for all $k \in \{1, 2, \dots, P-1\}$,

$$\mathbf{C}^H(\hat{\mathbf{s}}_1^{(k-1)})\mathbf{C}(\hat{\mathbf{s}}_1^{(k)}) = \mathbf{C}^H(\hat{\mathbf{s}}_2^{(k-1)})\mathbf{C}(\hat{\mathbf{s}}_2^{(k)}), \quad (8)$$

which, by (4), yields $\mathbf{G}^H(\hat{\mathbf{s}}_1)\mathbf{G}(\hat{\mathbf{s}}_1) = \mathbf{G}^H(\hat{\mathbf{s}}_2)\mathbf{G}(\hat{\mathbf{s}}_2)$ and

$$\|(\mathbf{G}^*(\hat{\mathbf{s}}_1) \otimes \mathbf{I}_D)\mathbf{y}\| = \|(\mathbf{G}^*(\hat{\mathbf{s}}_2) \otimes \mathbf{I}_D)\mathbf{y}\|. \quad (9)$$

In fact, (8) is a sufficient and, with probability 1 (w.p.1), necessary[1] condition for $\hat{\mathbf{s}}_2$ to solve (7) as well. Certainly, phase ambiguity can be resolved by differential modulation at the transmitter according to [13] which, however, reduces the encoding rate and imposes constraints on the validity of the sequences that are considered in the optimization problem in (7). In Section III, we develop a novel differential modulation scheme for the resolution of this ambiguity that *(i)* attains full rate for any constellation order and *(ii)* guarantees that the encoded matrix maintains the characteristics of the initial codebook so that all possible sequences of Alamouti matrices become valid. Then, based 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 (7) with $\mathcal{O}\left((MP)^{4D}\right)$ calculations.

[1] It can be shown that $\text{P}\{\|(\mathbf{G}^*(\hat{\mathbf{s}}_1) \otimes \mathbf{I}_D)\mathbf{y}\| = \|(\mathbf{G}^*(\hat{\mathbf{s}}_2) \otimes \mathbf{I}_D)\mathbf{y}\| \,|\, \mathbf{G}^H(\hat{\mathbf{s}}_1)\mathbf{G}(\hat{\mathbf{s}}_1) \neq \mathbf{G}^H(\hat{\mathbf{s}}_2)\mathbf{G}(\hat{\mathbf{s}}_2)\} = 0$.

3. FULL-RATE DIFFERENTIAL ALAMOUTI ENCODING AND UNIQUE SEQUENCE DECODING

3.1. A Systematic Classification of Alamouti Matrices

We commence our developments by presenting and analyzing a particular systematic partitioning of the set of all Alamouti matrices (defined upon an M-PSK constellation)

$$\mathcal{C} \triangleq \{\mathbf{C}(\mathbf{a}) : \mathbf{a} \in \mathcal{A}_M^2\}. \quad (10)$$

Thereafter, we exploit these properties to design a full-rate differential Alamouti encoding scheme.

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

$$\mathbf{R}_{m,\gamma} \triangleq \begin{bmatrix} \mu^m & \gamma\mu^m \\ -\gamma\mu^{-m} & \mu^{-m} \end{bmatrix}, \quad (11)$$

$m = 0, 1, \dots, M-1$, $\gamma = \pm 1$, where $\mu \triangleq e^{j2\pi/M}$. By construction, for any $m = 0, 1, \dots, M-1$ and $\gamma = \pm 1$, $\mathbf{R}_{m,\gamma}$ is a complex rotation matrix; that is, $\mathbf{R}_{m,\gamma}$ is scaled unitary and $\det(\mathbf{R}_{m,\gamma}) = 1$. Accordingly, we define the *primary* rotation set

$$\mathcal{R} \triangleq \bigcup_{m=0}^{M-1} \{\mathbf{R}_{m,1}, \mathbf{R}_{m,-1}\} \quad (12)$$

that consists of all rotation matrices constructed by (11). The following lemma comprises the basic properties of the primary rotation set. Its proof is omitted due to lack of space.

Lemma 1 *The primary rotation set consists of $2M$ distinct complex rotation matrices and is closed under negation and conjugation; that is, for any $m \in \{0, 1, \dots, M-1\}$ and $\gamma \in \{-1, 1\}$, $-\mathbf{R}_{m,\gamma}$, $\mathbf{R}^*_{m,\gamma} \in \mathcal{R}$. Moreover, $\mathcal{R}^H\mathcal{R} = \mathbf{B}\mathcal{R}$, where $\mathbf{B} \triangleq \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$.* □

Next, we proceed with the classification synthesis by defining the $\frac{M}{2}$ *secondary* rotation matrices

$$\mathbf{T}_m \triangleq \frac{1}{2} \begin{bmatrix} 1+\mu^{-m} & \mu^m - 1 \\ 1-\mu^{-m} & \mu^m + 1 \end{bmatrix}, \quad (13)$$

$m = 0, 1, \dots, \frac{M}{2}-1$, and the accordingly formed *secondary* rotation set

$$\mathcal{T} \triangleq \{\mathbf{T}_0, \mathbf{T}_1, \dots, \mathbf{T}_{\frac{M}{2}-1}\}. \quad (14)$$

For any $m, l \in \{0, 1, \dots, \frac{M}{2}-1\}$, $\mathbf{T}_m$ is a complex rotation matrix, while $\mathbf{T}_m \neq \mathbf{T}_l$ if $m \neq l$. Hence, the cardinality of the secondary rotation set equals $\frac{M}{2}$. By combining the primary and secondary rotation sets, we define the $\frac{M}{2}$ code sets

$$\mathcal{C}_m \triangleq \mathcal{R}\mathbf{T}_m, \quad (15)$$

$m = 0, 1, \dots, \frac{M}{2} - 1$. In the sequel, Lemmas 2 and 3 describe the code sets defined in (15) and pave the way for Theorem 1 which concludes our systematic partitioning of $\mathcal{C}$. The proofs of Lemmas 2 and 3 are omitted due to lack of space.

Lemma 2 *For any $m \in \{0, 1, \dots, \frac{M}{2} - 1\}$, code set $\mathcal{C}_m$ consists of $2M$ distinct M-PSK Alamouti matrices.* □

Lemma 3 *Code sets $\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{\frac{M}{2}-1}$ are disjoint; that is, $\mathcal{C}_m \cap \mathcal{C}_l = \emptyset$ if $m \neq l$.* □

In view of the code set definition and Lemmas 2 and 3, the following theorem holds true.

Theorem 1 *$\mathcal{C}$ can be perfectly partitioned into the $\frac{M}{2}$ disjoint code sets defined in* (15). □

As a follow-up to Theorem 1, we note that

$$\mathcal{C} = \{\mathcal{R}\mathbf{T}_0, \mathcal{R}\mathbf{T}_1, \dots, \mathcal{R}\mathbf{T}_{\frac{M}{2}-1}\} = \mathcal{R}\mathcal{T}. \tag{16}$$

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

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 ($\mathbf{A}^H\mathbf{A} = \mathbf{A}\mathbf{A}^H = 2\mathbf{I}$, for all $\mathbf{A} \in \mathcal{C}$), the M^2 valid transition matrices for a specific Alamouti matrix $\mathbf{A} \in \mathcal{C}$ form set $\frac{1}{2}\mathbf{A}^H\mathcal{C}$. At this point, we define the mth *set-transition* set $\mathcal{F}_m$ as the set of all valid transition matrices for all Alamouti matrices in the mth code set $\mathcal{C}_m$, $m = 0, 1, \dots, \frac{M}{2} - 1$; that is,

$$\mathcal{F}_m \triangleq \bigcup_{\mathbf{A}\in\mathcal{C}_m} \frac{1}{2}\mathbf{A}^H\mathcal{C}, \tag{17}$$

$m = 0, 1, \dots, \frac{M}{2} - 1$. Following Lemma 1, the definition of the code sets in (15), and Theorem 1, we can re-express the mth set-transition set as $\mathcal{F}_m = \frac{1}{2}\mathcal{C}_m^H\mathcal{C} = \frac{1}{2}\mathbf{T}_m^H\mathcal{R}^H\mathcal{R}\mathcal{T} = \frac{1}{2}\mathbf{T}_m^H\mathbf{B}\mathcal{R}\mathcal{T}$, $m = 0, 1, \dots, \frac{M}{2} - 1$. We observe that, since both $\mathbf{B}$ and $\mathbf{T}_m$ are unitary matrices, $|\mathcal{C}| = |\mathcal{R}\mathcal{T}| = |\mathcal{F}_m| = M^2$, for any $m = 0, 1, \dots, \frac{M}{2} - 1$, where $|\mathcal{S}|$ denotes the cardinality of set $\mathcal{S}$. This conclusion, along with the union definition of $\mathcal{F}_m$ in (17), verifies the following lemma.

Lemma 4 *For any $m \in \{0, 1, \dots, \frac{M}{2} - 1\}$, the elements of $\mathcal{F}_m$ are valid transition matrices for all Alamouti matrices in $\mathcal{C}_m$; that is, $\mathcal{C}_m\mathcal{F}_m = \mathcal{C}$, $m = 0, 1, \dots, \frac{M}{2} - 1$.* □

Subsequently, we aim at exploring the correlations among the set-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,

$$\mathcal{F} \triangleq \bigcup_{\mathbf{A}\in\mathcal{C}} \frac{1}{2}\mathbf{A}^H\mathcal{C}. \tag{18}$$

In view of (16), the compound transition set can be re-expressed as $\mathcal{F} = \frac{1}{2}\mathcal{C}^H\mathcal{C} = \mathcal{T}^H\mathcal{R}^H\mathcal{R}\mathcal{T} = \mathcal{T}^H\mathbf{B}\mathcal{R}\mathcal{T}$. Thus, $|\mathcal{F}| \leq |\mathcal{T}||\mathcal{R}\mathcal{T}| = M^3/2$ and, in the nontrivial case $M > 2$, there certainly exist more than one transition matrices in $\mathcal{F}$ that appear in more than one set-transition sets[2]; in other words, the set-transition sets are overlapping. In fact, a rigorous study on their intersections results in the following lemma, the proof of which is omitted due to lack of space.

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

Next, we introduce the *global* transition set

$$\mathcal{G} \triangleq \bigcup_{l=0}^{M-1} \left\{ \begin{bmatrix} \mu^l & 0 \\ 0 & \mu^{-l} \end{bmatrix}, \begin{bmatrix} 0 & \mu^l \\ -\mu^{-l} & 0 \end{bmatrix} \right\}. \tag{19}$$

Evidently, the cardinality of $\mathcal{G}$ is $2M$ and $\mathcal{C}\mathcal{G} = \mathcal{C}$, since, for all $\mathbf{A} \in \mathcal{C}$ and $\mathbf{G} \in \mathcal{G}$, $\mathbf{AG} \in \mathcal{C}$. Hence, for all $l \in \{0, 1, \dots, \frac{M}{2} - 1\}$, $\mathcal{F}_l \cap \mathcal{G} = \mathcal{G}$ and for all $k \in \{0, 1, \dots, \frac{M}{2} - 1\} \setminus l$, $\mathcal{G} \subseteq \mathcal{F}_k \cap \mathcal{F}_l$. 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 set-transition sets, while each of the transition matrices in $\mathcal{F} \backslash \mathcal{G}$ may belong to one and only set-transition set.* □

An alternative way Theorem 2 can be interpreted is $\mathcal{F}_l \cap \mathcal{F}_k = \mathcal{G}$, for all $l \in \{0, 1, \dots, \frac{M}{2} - 1\}$ and $k \in \{0, 1, \dots, \frac{M}{2} - 1\} \setminus l$.

3.2. 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

$$\mathbf{C}(\mathbf{s}^{(k)}) = \mathbf{C}(\mathbf{s}^{(k-1)})\mathbf{D}_k, \tag{20}$$

$k = 1, 2, \dots, P - 1$, 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 encoder's 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 that is 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 [13], 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 entire respective set-transition set of cardinality M^2; that is, if $\mathbf{C}(\mathbf{s}^{(k-1)}) \in \mathcal{C}_l$, for some $l \in \{0, 1, \dots, \frac{M}{2} - 1\}$, 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 $\mathcal{C}$.

[2] For $M = 2$, $\mathcal{F} = \mathcal{F}_0 = \frac{1}{2}\mathbf{B}\mathcal{R}$ and $|\mathcal{F}| = |\mathcal{R}| = 2M = M^3/2$.

Input:
$\mathcal{D}$: The set of all bit sequences of length $2\log_2 M$.
$\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_{\frac{M}{2}-1}$: The $\frac{M}{2}$ set-transition sets.
$\mathcal{G}$: The set of global transition matrices.
Initialization:
$\mathcal{D}_G, \mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_{\frac{M}{2}-1} = \emptyset$.
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 $\mathcal{D}_G = \mathcal{D}_G \cup \{b\}$.
Set $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_{\frac{M}{2}-1} = \mathcal{D}_G$.
Step 2:
For $l = 0, 1, \ldots, \frac{M}{2} - 1$
  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 $\mathcal{D}_l = \mathcal{D}_l \cup \{b\}$.
Output:
An instance of the full-rate codebook.

Fig. 1: The algorithm for the construction of a full-rate codebook.

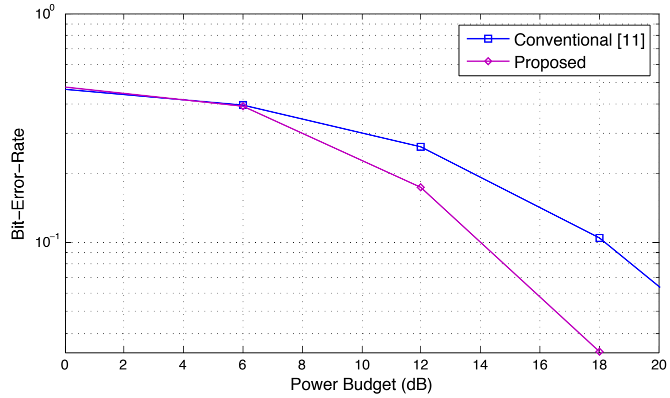

Fig. 2: BER versus overall power budget for the communication of 36 bits ($M = 4$, $D = 1$, $\sigma_h^2 = 1$, and $\sigma_v^2 = 1$).

3.3. 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 (7). Then, it builds the respective Alamouti sequence $\mathbf{C}(\hat{\mathbf{s}}^{(0)}), \mathbf{C}(\hat{\mathbf{s}}^{(1)}), \ldots, \mathbf{C}(\hat{\mathbf{s}}^{(P-1)})$ and, in accordance with the differential encoding procedure, computes the kth information-bearing transition code by

$$\hat{\mathbf{D}}_k = \frac{1}{2}\mathbf{C}^H(\hat{\mathbf{s}}^{(k-1)})\mathbf{C}(\hat{\mathbf{s}}^{(k)}), \tag{21}$$

$k = 1, 2, \ldots, P-1$. In view of (8), all equivalently optimal, in terms of (7), 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. 1.

This codebook design guarantees that, in every set-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 set-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 $2\log_2 M$. That is, maximal differential rate equal to $R = \frac{2\log_2 M}{2} = \log_2 M$ bits per transmit antenna is attained. This is in sharp contrast to conventional differential Alamouti encoding scheme [13] that utilizes solely global transition codes and achieves differential rate equal to $\log_2 \sqrt{2M}$ bits per transmit antenna.

4. ML SEQUENCE DETECTION WITH POLYNOMIAL COMPLEXITY

In this section, we prove that the complexity of the ML sequence detector in (7) 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 (4), can take the form

$$\mathbf{G}(\mathbf{s}) = \begin{bmatrix} \mathbf{s} & \left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^T\right) \mathbf{s}^* \end{bmatrix}^T. \tag{22}$$

Then, using $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$ [16] and (22), we rewrite the maximization argument in (7) as

$$\| (\mathbf{G}^*(\mathbf{s}) \otimes \mathbf{I}_D)\, \mathbf{y} \|^2 = \|\mathbf{\Gamma}^H \mathbf{s}\|^2$$

where $\mathbf{\Gamma} \triangleq \begin{bmatrix} \mathbf{Y}^T & \left(\mathbf{I}_P \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) \mathbf{Y}^H \end{bmatrix} \in \mathbb{C}^{2P \times 2D}$.
Finally, the ML sequence detector in (7) becomes

$$\hat{\mathbf{s}} = \underset{\mathbf{s} \in {\mathcal{A}_M}^{2P}}{\arg\max}\; \mathbf{s}^H \mathbf{\Gamma}\mathbf{\Gamma}^H \mathbf{s}. \tag{23}$$

For $P \geq D$, rank $(\mathbf{\Gamma}) \leq 2D$ and the the rank of the quadratic form in the maximization argument of (23) is not a function of the problem size. In the light of this analysis, we tailor to (23) the algorithm presented in [15] for the problem of rank-deficient quadratic form maximization over M-phase alphabet and establish that the initial ML sequence detection problem of (7) is, in fact, solvable in polynomial time $\mathcal{O}((MP)^{4D})$. The order of the polynomial is solely dictated by the number of antennas at the receiver.

5. SIMULATION STUDIES

Subsequently, we carry out a simulation study on the bit-error rate (BER) performance of the proposed differential modulation scheme. We consider the signal model described in Section II, for $M = 4$, $D = 1$, $\sigma_h^2 = 1$, 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. 2, we plot the BER attained by the proposed scheme over 1 000 independent simulation runs, as a function of the overall power budget. For reference purposes, we include the respective plot for the conventional rate-deficient differential modulation scheme (see [13], Ex. 3). Clearly, for intermediate and high power budget, the proposed differential scheme outperforms significantly its conventional counterpart, due to its rate efficiency. As per-bit power budget decreases, although the rate-driven BER advantage of the proposed scheme diminishes, its bandwidth efficiency merits are maintained.

6. 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] 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.

[5] 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.

[6] Q. Li and C. N. Georghiades, "Sphere decoding of orthogonal space-time block codes for incoherent channels," in *Proc. IEEE Intern. Symp. Intelligent Control*, Limassol, Cyprus, June 2005, pp. 702-706.

[7] T. Cui and C. Tellambura, "Efficient blind decoding of orthogonal space-time block codes over time-selective fading channels," in *Proc. IEEE WCNC 2006 - Wireless Commun. Networking Conf.*, Las Vegas, NV, Apr. 2006, pp. 1644-1649.

[8] 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.

[9] 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.

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

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

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

[13] B. L. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2567-2578, Nov. 2000.

[14] X. Shao and J. Yuan, "A new differential space-time block coding scheme," *IEEE Commun. Letters*, vol. 7, pp. 437-439, Sept. 2003.

[15] 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, pp. 3856-3859.

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

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

[18] 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.

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