Unitary Space-Time Pulse Position Modulation for Differential Unipolar MIMO IR-UWB Communications

Chadi Abou-Rjeily, *Senior Member IEEE*

***Abstract*—In this paper, we present a general technique for constructing minimal-delay unitary differential Space-Time (ST) block codes for Pulse Position Modulation (PPM) with an arbitrary number of transmit antennas and signal set cardinality. A typical application corresponds to Multiple Input Multiple Output (MIMO) Impulse-Radio Ultra-Wideband (IR-UWB) systems where neither the transmitter nor the receiver knows the channel. The proposed scheme is a pulse-based solution where the information is encoded differentially through the relative shifts of the pulses in one block with respect to the pulse positions in the previous block where each block extends over P symbol durations with P standing for the number of transmit antennas. This technique of time-domain encoding avoids all types of amplitude constellation expansions and achieves a full transmit diversity order while maintaining a single unipolar pulse transmission per symbol in a way that is completely equivalent to single-antenna PPM communications. We also propose a simplified decoder that can be associated with the proposed ST code and we perform a detailed complexity analysis that allows to quantify the reduction in the number of operations offered by this simplified decoding strategy. Finally, the results are validated numerically and through a semi-analytical evaluation of the conditional symbol error rate.**

***Index Terms*—Ultra-Wideband, UWB, differential, space-time, MIMO, performance analysis, simplified decoding, decoder complexity, Pulse Position Modulation, PPM.**

I. Introduction

Differential modulation constitutes an attractive and well-explored method of communications in the scenario where the channel is not known to the transmitter and the receiver. This communication technique gained central importance and promptly found application in the context of Impulse-Radio (IR) Ultra-Wideband (UWB) systems. In IR-UWB communications, the energy of the ultra-short sub-nanosecond transmitted pulses is spread over a very large number of multi-path components. Consequently, collecting a sufficient amount of signal energy at the output of this highly frequency selective channel requires combining a large number of multi-path components. If this task is to be carried out in a coherent manner, a large number of channel parameters needs to be estimated which might induce a prohibitive implementation complexity. A popular alternative was based on solutions that do not require any kind of channel estimation. These include transmitted-reference solutions [1]–[3], noncoherent solutions based on energy detection [4]–[7] as well as differential solutions where the modulation and demodulation techniques are similar to those used in Differential Binary Phase Shift Keying (DBPSK) [8]–[11]. In this context, it is worth noting that [1]–[11] targeted single-antenna systems.

On the other hand, a popular way for Multiple Input Multiple Output (MIMO) narrowband communications when the channel is not known corresponds to unitary differential Space-Time (ST) coding which can be perceived as an extension of DPSK to the multi-antenna scenario. This constitutes a well established research field that attracted a huge amount of attention [12]–[20]. The numerous proposed codes include Cayley unitary ST codes [14], codes based on cyclic division algebras [15], codes constructed on the Grassmannian manifold [16], codes optimized for given numbers of transmit antennas and rates [17]–[19] and non-orthogonal codes with non-unitary constellations [20] along with many other differential ST coding techniques.

Despite the rich literature on differential single-antenna modulation in the IR-UWB context, on one hand, and on differential ST coding in the narrowband context, on the other hand, a limited number of contributions targeted the problem of differential ST coding for IR-UWB [21]–[23]. IR-UWB possesses a number of particularities that render the direct application of the existing narrowband unitary differential ST codes not possible and make the extension of these ST techniques not straightforward. In what follows, we will elaborate further on the distinctiveness of IR-UWB vis-à-vis the differential ST code construction. (i): IR-UWB is a carrier-less transmission technology where all information on the phase is not retained since UWB signals occupy several GHz of bandwidth. In this context, almost all narrowband differential ST codes are complex-valued and hence based on phase rotations making them not suitable for real-valued carrier-less UWB transmissions. In this context, differential ST codes for IR-UWB must satisfy the key constraint of being totally-real. (ii): IR-UWB differs from narrowband communications in the type of modulation that is used. In particular, given the fine temporal resolution of UWB systems, these systems are often associated with Pulse Position Modulation (PPM) whereas this modulation is never used for narrowband communications. In this context, the QAM or PSK differential ST codes in [12]–[20] can not be applied with PPM. (iii): In IR-UWB it is hard to control the amplitude of the very low duty-cycle pulses. In this context, polarity inversions and amplitude constellation expansions, even though real-valued and hence feasible, are not preferable for maintaining simple and cost-effective UWB

The author is with the Department of Electrical and Computer Engineering of the Lebanese American University (LAU), Byblos, Lebanon. (e-mail: chadi.abourjeily@lau.edu.lb).

transmitters that transmit unipolar pulses.

Based on the above constraints and preferences under which IR-UWB systems operate, we can highlight the advantages and disadvantages of the existing differential ST codes. All complex-valued codes (that are QAM or PSK codes in the narrowband context) such as [12]–[20] can not be applied with IR-UWB. Regarding the remaining minority of real-valued differential ST codes, such as the codes based on the orthogonal design [24], these codes can be applied with IR-UWB and can be easily extended to PPM; however, they suffer from the limitation of not being shape-preserving with PPM. For example, [24] was extended to 2×2 IR-UWB systems with binary PAM in [21] and to 2×2 IR-UWB systems with PPM in [22]; however, these extensions suffer from undesirable constellation expansions. In particular, [21], [22] require transmitting four amplitude levels; namely, the initial reference amplitude (the same as the one transmitted by single-antenna systems), twice this amplitude and the opposites of these two amplitudes. In this context, the extension of UWB transmitters from the single-antenna case to the multi-antenna case induces an increased complexity to invert and control the amplitudes of the sub-nanosecond pulses. Beside this limitation of losing the advantage of simple and low-cost unipolar PPM transmissions, the second main limitation resides in the fact that such differential ST codes can not be applied with any number of transmit antennas. Finally, solutions like [23] take advantage from the pulse repetitions in Time-Hopping (TH) UWB systems to render the data streams transmitted from the different antennas orthogonal and, hence, can not be applied in the absence of pulse repetitions rendering them unsuitable for high data rate applications. Moreover, [23] is not shape-preserving with PPM since it entails polarity inversions.

In this paper, we propose a unitary differential ST code for IR-UWB communications with PPM. The proposed construction responds to a large number of construction constraints. (i): The proposed solution is a minimal-delay solution that extends over P symbol durations where P stands for the number of transmit antennas. (ii): The proposed code can be applied with an arbitrary number of transmit antennas; a feature that is shared with a limited number of the existing ST constructions since the majority of the existing solutions are often specific to a ceratin number of transmit antennas. (iii): The proposed ST code can be applied with M-ary PPM constellations for any value of M. (iv): The proposed code is fully diverse in the sense that the difference between any two non-identical transmitted matrices has a full rank of P. (v): The proposed code is totally real. (vi): The proposed code is shape-preserving with PPM where, in a way that is completely equivalent to single-antenna communications, each antenna transmits only one unipolar pulse in one of the M PPM positions rendering the proposed solution appealing to low-cost IR-UWB systems. While respecting all of the above construction constraints, the proposed code suffers from a single disadvantage that resides in a reduced data-rate where this code transmits at the rate of $\frac{1}{P}\log_2(MP)$ bits per channel use (pcu) resulting in a normalized rate of $\frac{\log_2(MP)}{P\log_2(M)} \leq 1$ with respect to single-antenna systems deploying M-PPM. However, this rate of $\frac{1}{P}\log_2(MP)$ can largely exceed the rate of 1 bit pcu that is achieved by all existing single-antenna differential IR-UWB solutions based on DBPSK [8]–[11].

Other contributions of the paper are as follows. First, we perform a semi-analytical performance analysis where we derive closed-form expressions for the conditional symbol error rates that can be achieved by the proposed scheme. We also propose a simplified suboptimal, yet diversity-preserving, decoder that can be associated with the proposed ST code. We evaluate the number of multiplications and additions required by each of the optimal and suboptimal decoders and prove that the complexity of the former scales as M^2 while the complexity of the latter increases linearly with M.

Of direct relevance to this work is the noncoherent ST code proposed in [25]. While both codes are fully-diverse, shape-preserving with PPM, of minimal-delay and can be applied with any number of transmit antennas without the knowledge of the channel, they differ by the following. (i): The code in [25] is based on energy detection where the energy collected in the different PPM slots of the symbols within each block are used for detection while the scheme proposed in this paper encodes the information differentially among two consecutive blocks. Based on the considered system model, the complexities of both schemes are comparable. (ii): While the proposed code can be applied with M-PPM for all values of M, the code in [25] can be applied only for $M > P+1$. (iii): The codes also differ by their rates that are equal to $\frac{1}{P}\log_2(MP)$ and $\frac{1}{P}\log_2\binom{M-1}{P}$ bits pcu for the proposed code and [25], respectively. Comparing these rates shows that it is more advantageous to apply the differential (resp. noncoherent) ST code for small (resp. large) values of M. For example, it is better to apply the proposed differential ST code for $M \leq 6$, $M \leq 7$, $M \leq 7$, $M \leq 8$ and $M \leq 9$ with 2, 3, 4, 5 and 6 transmit antennas, respectively.

The rest of this paper is organized as follows. The system model is described in section II. The encoder structure and the main properties of the code are highlighted in section III. The performance analysis is provided in section IV. In section V, we propose the simplified decoding strategy and we perform a detailed complexity analysis. Simulation results over the realistic UWB channel model [26] are provided in section VI while section VII concludes the paper. In what follows, boldface letters indicate vectors (lower case) or matrices (upper case).

II. System Model

The encoding/decoding schemes that we consider in this work can be applied with M-ary PPM constellations where the information symbols are represented by the M-dimensional vectors carved from the following signal set:

$$\mathcal{C}_{\text{PPM}} = \{\mathbf{e}_m \ ; \ m = 1, \ldots, M\} \tag{1}$$

where $\mathbf{e}_m$ stands for the m-th column of the $M \times M$ identity matrix $\mathbf{I}_M$.

Consider a MIMO IR-UWB system where the transmitter is equipped with P antennas and the receiver is equipped with Q

antennas. The channel is used in blocks of P symbol durations each where the transmitted information is represented by the sequence of matrices $\{\mathbf{S}^{(t)}\}$ where $t = 0, 1, \ldots$ represents the block channel use. For M-dimensional constellations, $\mathbf{S}^{(t)}$ is a $PM \times P$ matrix that can be written under the form $\mathbf{S}^{(\mathbf{t})} = [\mathbf{s}_{i,j}^{(t)}]_{i,j=1,\ldots,P}$ where $\mathbf{s}_{i,j}^{(t)}$ is an M-dimensional vector corresponding to the M-ary PPM symbol transmitted by the j-th transmit antenna during the i-th symbol duration of the t-th block.

The receiver is a Rake-based solution where the signal received in each PPM slot at a given antenna is correlated with L shifted versions of the UWB pulse shape in order to achieve a sufficient level of multi-path diversity. Denoting the pulse width by T_w, this corresponds to collecting the signal energy over an integration time of LT_w. Evidently, as L increases, an increased amount of energy corresponding to a larger number of multipath components is collected at the expense of an increased complexity[1]. This Rake-based solution is not associated with any channel estimation procedure used for estimating the amplitudes of the multi-path components as in the cases of Maximum Ratio Combining (MRC) and Equal Gain Combining (EGC), for example. In this context, the proposed solution is classified as a non-coherent solution that can be implemented without any knowledge of the Channel State Information (CSI). As will be explained later in more details, the signals received in the t-th ST block are compared with the signals received in the $(t-1)$-th ST block for the sake of extracting the differentially-encoded t-th information symbol. The decision variables are then used to construct the $PM \times QL$ decision matrix $\mathbf{Y}^{(t)}$ whose $((p-1)M+m, (q-1)L+l)$-th element corresponds to the output of the l-th correlator placed after the q-th receive antenna during the m-th PPM slot of the p-th symbol duration (of the t-th block) for $l = 1, \ldots, L$, $q = 1, \ldots, Q$, $m = 1, \ldots, M$ and $p = 1, \ldots, P$. If the channel is assumed to be constant over two consecutive blocks, the baseband inputs and outputs of the channel are related to each other by:

$$\mathbf{Y}_{PM\times QL}^{(t)} = \mathbf{S}_{PM\times P}^{(t)} \mathbf{H}_{P\times QL} + \mathbf{N}_{PM\times QL}^{(t)} \tag{2}$$

where the subscripts indicate the dimensions of the corresponding matrices. $\mathbf{N}^{(t)}$ stands for the noise matrix whose components are independent and normally distributed with zero mean and variance $\frac{N_0}{2}$. In (2), $\mathbf{H}$ is the $P \times QL$ channel matrix whose $(p, (q-1)L+l)$-th element is equal to (for $p = 1, \ldots, P$, $q = 1, \ldots, Q$ and $l = 1, \ldots, L$):

$$H_{p,(q-1)L+l} = \int_0^{T_w} r_{p,q}(\tau) w(\tau - (l-1)T_w) \mathrm{d}\tau \tag{3}$$

where $w(\tau)$ corresponds to the transmitted UWB pulse shape having a duration of T_w (τ is the time variable) while $r_{p,q}(\tau)$ stands for the convolution between $w(\tau)$ and the impulse response of the UWB channel between the p-th transmit antenna and the q-th receive antenna. Note that correlating the received signal with shifted replicas of the transmitted waveform at multiple of T_w corresponds to a suboptimal Partial-Rake receiver [27]. This uncomplicated receiver that has a finite time resolution suffers from intra-pulse interference resulting from the multi-path components arriving within the pulse duration. Despite this limitation, Partial-Rakes are characterized by a remarked simplicity where there is no need to estimate the time-of-arrival of the various multi-path components. This renders this type of receivers perfectly adapted to our differential solution that needs to be implemented without requiring any kind of information about the underlying channel. The proposed differential scheme can be applied in the scenario where the channel matrix $\mathbf{H}$ is unknown to both the transmitter and the receiver. It is also worth noting that (2) holds in the case where the received PPM constellation maintains its orthogonality after multi-path propagation; in other words, when the PPM delay is larger than the channel delay spread.

[1]This occurs below a certain threshold value of L above which the performance is no longer enhanced by increasing L since the amount of noise collected will exceed the harvested signal energy [1]–[4].

III. Differential PPM Space-Time Codes

A. General Structure of the Proposed Unitary Code

We use differential unitary ST modulation where the ST matrix transmitted in block t is related to the space-time matrix transmitted in block $t-1$ by the following differential encoding rule:

$$\mathbf{S}^{(t)} = \mathbf{C}_{z_t} \mathbf{S}^{(t-1)} \quad ; \quad t = 1, 2, \ldots \tag{4}$$

where z_t is the data to be transmitted and which assumes values in the set $\{0, \ldots, PM-1\}$. In (4), $\mathbf{C}_{z_t}$ is a $PM \times PM$ matrix and the set $\mathcal{C}$ that comprises all possible values of $\mathbf{C}$ constitutes the constellation to be designed. The reference matrix is assumed to take the following value: $\mathbf{S}^{(0)} = \mathbf{I}_P \otimes \mathbf{e}_1$ where $\otimes$ stands for the Kronecker product.

In this work, we propose the following differential unitary space-time construction:

$$\mathcal{C} = \{\mathbf{C}_i = \mathbf{A}^i \mid i = 0, \ldots, PM-1\} \tag{5}$$

where $\mathbf{A}$ is the $PM \times PM$ matrix whose elements can be equal to either zero or one:

$$\mathbf{A} = \begin{bmatrix} \mathbf{0}_{M\times M} & \cdots & \mathbf{0}_{M\times M} & \mathbf{\Omega} \\ \mathbf{I}_M & \cdots & \mathbf{0}_{M\times M} & \mathbf{0}_{M\times M} \\ \vdots & \ddots & \vdots & \vdots \\ \mathbf{0}_{M\times M} & \cdots & \mathbf{I}_M & \mathbf{0}_{M\times M} \end{bmatrix} \tag{6}$$

where $\mathbf{0}_{m\times n}$ stands for the $m \times n$ all-zero matrix and $\mathbf{\Omega}$ is the $M \times M$ permutation matrix given by:

$$\mathbf{\Omega} = \begin{bmatrix} \mathbf{0}_{\mathbf{1}\times(\mathbf{M-1})} & 1 \\ \mathbf{I}_{\mathbf{M-1}} & \mathbf{0}_{(\mathbf{M-1})\times\mathbf{1}} \end{bmatrix} \tag{7}$$

Evidently, from (5) and (6), $\mathbf{C}_i^T = \mathbf{A}^{-i}$ and the matrices in $\mathcal{C}$ are unitary: $\mathbf{C}_i\mathbf{C}_i^T = \mathbf{C}_i^T\mathbf{C}_i = \mathbf{A}^i\mathbf{A}^{-i} = \mathbf{A}^{-i}\mathbf{A}^i = \mathbf{I}_{PM}$.

B. Shape-Preserving Property of the Code

One of the major desirable properties of the proposed scheme resides in the fact that it is a shape-preserving code that does not result in any constellation expansion of the original PPM signal set. In other words, as in single-antenna PPM systems, each transmit antenna transmits exactly one unipolar UWB pulse in one of the M available PPM slots.

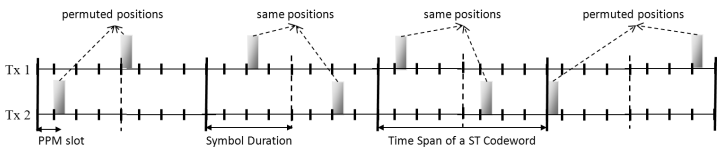

Fig. 1. The transmission scheme with two transmit antennas and 4-PPM. The information symbols are $\{1, 3, 6, 5\}$.

For example, for $P = 2$ and $M = 4$, for the transmission of the information symbols $\{1, 3, 6, 5\}$, the following sequence of matrices is transmitted: $\mathbf{S}^{(1)} = \begin{bmatrix} \mathbf{0}_{M\times 1} & \mathbf{\Omega}\mathbf{e}_1 \\ \mathbf{e}_1 & \mathbf{0}_{M\times 1} \end{bmatrix}$, $\mathbf{S}^{(2)} = \begin{bmatrix} \mathbf{\Omega}^2\mathbf{e}_1 & \mathbf{0}_{M\times 1} \\ \mathbf{0}_{M\times 1} & \mathbf{\Omega}^2\mathbf{e}_1 \end{bmatrix}$, $\mathbf{S}^{(3)} = \begin{bmatrix} \mathbf{\Omega}^5\mathbf{e}_1 & \mathbf{0}_{M\times 1} \\ \mathbf{0}_{M\times 1} & \mathbf{\Omega}^5\mathbf{e}_1 \end{bmatrix}$ and $\mathbf{S}^{(4)} = \begin{bmatrix} \mathbf{0}_{M\times 1} & \mathbf{\Omega}^8\mathbf{e}_1 \\ \mathbf{\Omega}^7\mathbf{e}_1 & \mathbf{0}_{M\times 1} \end{bmatrix}$. This is better illustrated in Fig. 1 that shows the pulses transmitted by the different antennas in the different PPM slots. Following from $\mathbf{\Omega}\mathbf{e}_1 = \mathbf{e}_2$, $\mathbf{\Omega}^2\mathbf{e}_1 = \mathbf{e}_3$, $\mathbf{\Omega}^5\mathbf{e}_1 = \mathbf{e}_2$, $\mathbf{\Omega}^7\mathbf{e}_1 = \mathbf{e}_4$ and $\mathbf{\Omega}^8\mathbf{e}_1 = \mathbf{e}_1$, and in general $\mathbf{\Omega}^m\mathbf{e}$ being a permutation of order m of $\mathbf{e}$ that belongs to the set $\mathcal{C}_{\text{PPM}}$ in (1) whenever $\mathbf{e} \in \mathcal{C}_{\text{PPM}}$, then only PPM symbols are transmitted by the different antennas resulting in no constellation expansion.

The above observation can be extended to all values of P and M. First, from (6), we observe that $\mathbf{A}^{PM} = \mathbf{I}_{PM}$ and, consequently, for any integer $i \in \mathbb{Z}$, $\mathbf{A}^i = \mathbf{A}^{i'}$ where $i' = (i \mod PM) \in \{0, \ldots, PM-1\}$ and hence $\mathbf{A}^i = \mathbf{A}^{i'} = \mathbf{C}_{i'}$ which is a codeword of $\mathcal{C}$ for any integer value of i. Hence, any integer power of the matrix $\mathbf{A}$ is a codeword.

We also define the function $f(.)$ that will be used extensively in the upcoming sections as follows:

$$f(i) = (k, m) \mid i' = (i \mod PM) = mP + k \quad ; \quad m \in \{0, \ldots, M-1\}\ ,\ k \in \{0, \ldots, P-1\} \tag{8}$$

In other words, this function associates with any integer i the integers m and k such that the codeword $\mathbf{A}^i$ can be indexed as $\mathbf{C}_{mP+k}$ where $k = (i' \mod P)$ and $m = \frac{i'-k}{P}$.

From (4), $\mathbf{S}^{(t)}$ can be written as: $\mathbf{S}^{(t)} = \left[\prod_{t'=1}^{t} \mathbf{C}_{z_{t'}}\right] \mathbf{S}^{(0)}$ which from (5) can be written as: $\mathbf{S}^{(t)} = \mathbf{A}^i\mathbf{S}^{(0)}$ where $i = \sum_{t'=1}^{t} z_{t'}$. This expression can be written as: $\mathbf{S}^{(t)} = \mathbf{C}_{mP+k}\mathbf{S}^{(0)}$ where $(k, m) = f(i)$ from (8). A careful inspection of equations (5)-(7) shows that the transmission of $\mathbf{C}_{mP+k}\mathbf{S}^{(0)}$ corresponds to (i): transmitting the PPM symbol $\mathbf{\Omega}^m\mathbf{e}_1$ by antenna p during the symbol duration $p + k$ for $p = 1, \ldots, P-k$ and (ii): transmitting the PPM symbol $\mathbf{\Omega}^{m+1}\mathbf{e}_1$ by antenna p during the symbol duration $p-(P-k)$ for $p = P-(k-1), \ldots, P$. In other words, only PPM symbols are transmitted by the different antennas and the proposed code is shape-preserving with PPM.

C. Rate of the Code

From (5), the total number of codewords in the codebook $\mathcal{C}$ is equal to PM. Since each block extends over P symbol durations, then the transmission rate is:

$$R = \frac{1}{P}\log_2(PM) \quad \text{(bits per channel use)} \tag{9}$$

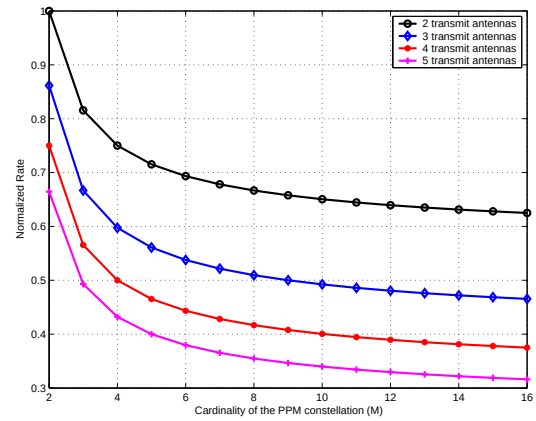

Fig. 2. The normalized rate of the proposed code.

Since a single-antenna system deploying M-PPM transmits at the rate of $\log_2(M)$ bits pcu, then the proposed scheme incurs a data-rate reduction by a factor of $\frac{\log_2(PM)}{P\log_2(M)} \leq 1$. This normalized rate (with respect to single-antenna systems) is plotted in Fig. 2 as a function of M for different values of P. This figure shows that the normalized rate is a decreasing function of both M and P and hence the smallest data-rate reductions are obtained for small values of P and M where, for example, no data-rate reduction is observed for two transmit antennas with binary PPM.

It is worth noting that the data-rate reduction follows mainly from the shape-preserving constraint where all forms of polarity inversion, amplitude scaling and symbol combining are not allowed. As a simple example, the codes based on the orthogonal design [24] involve a polarity inversion. While this polarity inversion is shape-preserving with PAM, QAM and PSK constellations that are deployed in the narrow-band context, this operation results in a constellation expansion when associated with unipolar PPM systems. It is worth noting that rate-1 PPM shape-preserving codes were proposed in [28] (for given numbers of transmit antennas and signal set cardinalities); however, these coherent codes do not lend themselves to differential detection in the absence of channel state information. In fact, these codes are not unitary while limiting the construction to the set of unitary matrices constitutes the main challenge in the differential ST code design. As a conclusion, PPM shape-preserving differential ST codes were never proposed before and our work constitutes the first step in this direction.

D. Diversity Order

Consider the two transmitted matrices $\mathbf{S}^{(t)} = \mathbf{C}_i\mathbf{S}^{(0)}$ and $\mathbf{S}'^{(t)} = \mathbf{C}_j\mathbf{S}^{(0)}$ that are associated with two distinct codewords $\mathbf{C}_i$ and $\mathbf{C}_j$ for $j \neq i$. The proposed scheme is fully diverse if the following relation is satisfied [29]:

$$\text{rank}\left(\mathbf{S}^{(t)} - \mathbf{S}'^{(t)}\right) = \text{rank}\left[\left(\mathbf{C}_i - \mathbf{C}_j\right)\mathbf{S}^{(0)}\right] = P \quad \forall\ i \neq j \in \{0, \ldots, PM-1\} \tag{10}$$

From (5), $\left(\mathbf{C}_i - \mathbf{C}_j\right)\mathbf{S}^{(0)} = \left(\mathbf{A}^i - \mathbf{A}^j\right)\mathbf{S}^{(0)} = \mathbf{A}^j\left(\mathbf{A}^{i-j} - \mathbf{I}_{PM}\right)\mathbf{S}^{(0)}$ which has the same rank as the matrix

$\left(\mathbf{A}^{i-j}-\mathbf{I}_{PM}\right)\mathbf{S}^{(0)}$ since the matrix $\mathbf{A}^j$ is invertible following from the fact that the proposed code is unitary. On the other hand, we have proven in subsection III-B that any integer power of $\mathbf{A}$ belongs to the set $\mathcal{C}$ and, consequently, (10) can be written as:

$$\text{rank}\left[\mathbf{D}_i\right]=\text{rank}\left[\left(\mathbf{A}^i-\mathbf{I}_{PM}\right)\mathbf{S}^{(0)}\right]=P\ \forall\ i\in\{1,\ldots,PM-1\} \tag{11}$$

Proposition 1: Equation (11) is satisfied for all values of P and M and, consequently, the proposed code is fully diverse with any M-ary PPM constellation for any number of transmit antennas.

Proof: In order to offer more insights on the properties of the code, we first consider the special case of $P=2$. The general proof that holds for any value of P is provided in Appendix A.

The structure of the codeword depends on the values of k and m where $(k,m)=f(i)$ from (8). For $P=2$, $k\in\{0,1\}$. For $k=0$, the M corresponding codewords take the following form:

$$\mathbf{A}^i=\begin{bmatrix}\mathbf{\Omega}^m & \mathbf{0}_{M\times M}\\ \mathbf{0}_{M\times M} & \mathbf{\Omega}^m\end{bmatrix}\quad;\quad m=0,\ldots,M-1 \tag{12}$$

while for $k=1$, the M corresponding codewords take the following form:

$$\mathbf{A}^i=\begin{bmatrix}\mathbf{0}_{M\times M} & \mathbf{\Omega}^{m+1}\\ \mathbf{\Omega}^m & \mathbf{0}_{M\times M}\end{bmatrix}\quad;\quad m=0,\ldots,M-1 \tag{13}$$

From (11) and (12), for $k=0$, $\mathbf{D}_i=\begin{bmatrix}\mathbf{\Omega}^m\mathbf{e}_1-\mathbf{e}_1 & \mathbf{0}_{M\times 1}\\ \mathbf{0}_{M\times 1} & \mathbf{\Omega}^m\mathbf{e}_1-\mathbf{e}_1\end{bmatrix}$ where the condition $i\neq 0$ in (11) implies that $(k,m)\neq(0,0)$ and hence, for $k=0$, $m\in\{1,\ldots,M-1\}$. In this case, $\mathbf{\Omega}^m\mathbf{e}_1=\mathbf{e}_{m+1}$ can not be equal to $\mathbf{e}_1$ for $m\neq 0$. The matrix $\mathbf{D}_i$ is rank deficient if there exist two nonzero scalars c_1 and c_2 such that $c_1\mathbf{d}_{i,1}+c_2\mathbf{d}_{i,2}=\mathbf{0}_{2M\times 1}$ where $\mathbf{d}_{i,j}$ stands for the j-th column of $\mathbf{D}_i$. This implies that $c_1(\mathbf{e}_{m+1}-\mathbf{e}_1)=\mathbf{0}_{M\times 1}$ and $c_2(\mathbf{e}_{m+1}-\mathbf{e}_1)=\mathbf{0}_{M\times 1}$ resulting in $c_1=c_2=0$ since $\mathbf{e}_{m+1}-\mathbf{e}_1\neq\mathbf{0}_{M\times 1}$ (the first component of this vector is equal to -1, the $(m+1)$-th component is equal to $+1$ while the remaining components are zero). As a conclusion, the matrix $\mathbf{D}_i$ has a full rank of $P=2$ for $f(i)=(0,m)$ with $m\neq 0$.

From (11) and (13), for $k=1$, $\mathbf{D}_i=\begin{bmatrix}-\mathbf{e}_1 & \mathbf{\Omega}^{m+1}\mathbf{e}_1\\ \mathbf{\Omega}^m\mathbf{e}_1 & -\mathbf{e}_1\end{bmatrix}$ where in this case m can be equal to zero. The relation $c_1\mathbf{d}_{i,1}+c_2\mathbf{d}_{i,2}=\mathbf{0}_{2M\times 1}$ implies that $-c_1\mathbf{e}_1+c_2\mathbf{\Omega}^{m+1}\mathbf{e}_1=\mathbf{0}_{M\times 1}$ and $c_1\mathbf{\Omega}^m\mathbf{e}_1-c_2\mathbf{e}_1=\mathbf{0}_{M\times 1}$. Evidently, if $c_1=0$ then $c_2\mathbf{e}_1=\mathbf{0}_{M\times 1}$ implying that $c_2=0$ and if $c_2=0$ then $c_1\mathbf{e}_1=\mathbf{0}_{M\times 1}$ implying that $c_1=0$. Hence, we need only to consider the case $c_1\neq 0$ and $c_2\neq 0$. In this case, the first equation implies that $\mathbf{e}_1=\frac{c_2}{c_1}\mathbf{\Omega}^{m+1}e_1$ while the second equation results in $\mathbf{\Omega}^m e_1=\frac{c_2}{c_1}\mathbf{e}_1$ where combining these equations results in $\mathbf{e}_1=\left(\frac{c_2}{c_1}\right)^2\mathbf{\Omega}^1 e_1=\left(\frac{c_2}{c_1}\right)^2 e_2$ which is impossible since $\mathbf{e}_1$ can not be proportional to $\mathbf{e}_2$. As a conclusion, the relation $c_1\mathbf{d}_{i,1}+c_2\mathbf{d}_{i,2}=\mathbf{0}_{2M\times 1}$ holds only for $c_1=c_2=0$. As a conclusion, the matrix $\mathbf{D}_i$ has a full rank of $P=2$ for $f(i)=(1,m)$.

From the cases $k=0$ and $k=1$ we conclude that (11) holds for $(k,m)\neq(0,0)$ (i.e. $i\neq 0$) and the proposed scheme is fully diverse with two transmit antennas. For $P>2$, the proof is more involved and is provided in Appendix A.

IV. Performance Analysis

In this section, we derive expressions for the conditional pairwise error probability (PEP) of the proposed code.

For the differential schemes, the matrix transmitted in block $t-1$ serves as a reference for the detection of the matrix transmitted in block t and thus the maximum-likelihood (ML) decoder is given by [30]:

$$\hat{z}_t=\arg\min_{i=0,\ldots,PM-1}\left\|\mathbf{Y}^{(t)}-\mathbf{C}_i\mathbf{Y}^{(t-1)}\right\|^2 \tag{14}$$

where the expression of the decision matrix is provided in (2).

For the sake of the performance analysis, (2) can be written in a more convenient form as:

$$\mathbf{y}^{(t)}=\left(\mathbf{I}_{QL}\otimes\mathbf{S}^{(t)}\right)\mathbf{h}+\mathbf{n}^{(t)} \tag{15}$$

where $\mathbf{y}^{(t)}$ and $\mathbf{n}^{(t)}$ are $PMQL$-dimensional vectors obtained from stacking the columns of $\mathbf{Y}^{(t)}$ and $\mathbf{N}^{(t)}$, respectively, vertically one after the other. Vector $\mathbf{h}$ is the PQL-dimensional vector constructed from the channel matrix $\mathbf{H}$ in the same way.

Based on this new notation, (14) can be rewritten as:

$$\hat{z}_t=\arg\min_{i=0,\ldots,PM-1}\left\|\mathbf{y}^{(t)}-\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i\right)\mathbf{y}^{(t-1)}\right\|^2 \tag{16}$$

The Frobenius norm can be expanded as follows:

$$[\mathbf{y}^{(t)}]^T\mathbf{y}^{(t)}+[\mathbf{y}^{(t-1)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i^T\right)\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i\right)\mathbf{y}^{(t-1)} - 2[\mathbf{y}^{(t)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i\right)\mathbf{y}^{(t-1)} \tag{17}$$

where the first term does not depend on the index i of the codeword. Moreover, the second term can be written as $[\mathbf{y}^{(t-1)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i^T\mathbf{C}_i\right)\mathbf{y}^{(t-1)}=[\mathbf{y}^{(t-1)}]^T\mathbf{y}^{(t-1)}$ since the codewords $\mathbf{C}_i$ are unitary and, thus, this term does not depend on i as well. Consequently, (16) can be expressed as:

$$\hat{z}_t=\arg\max_{i=0,\ldots,PM-1}\left[[\mathbf{y}^{(t)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i\right)\mathbf{y}^{(t-1)}\right] \tag{18}$$

From (18), the conditional PEP of differentially encoding the symbol $z_t=i$ and deciding in favor of the symbol $\hat{z}_t=j$ is given by:

$$P(\mathbf{C}_i\rightarrow\mathbf{C}_j)= \Pr\left([\mathbf{y}^{(t)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_j\right)\mathbf{y}^{(t-1)}\geq[\mathbf{y}^{(t)}]^T\left(\mathbf{I}_{QL}\otimes\mathbf{C}_i\right)\mathbf{y}^{(t-1)}\right) \tag{19}$$

which from (4) and (15) can be written as:

$$P(\mathbf{C}_i\rightarrow\mathbf{C}_j)=\Pr\left(\left[\mathbf{h}^T\left(\mathbf{I}_{QL}\otimes[\mathbf{S}^{(t-1)}]^T\mathbf{C}_i^T\right)+[\mathbf{n}^{(t)}]^T\right]\left(\mathbf{I}_{QL}\otimes(\mathbf{C}_j-\mathbf{C}_i)\right)\left[\left(\mathbf{I}_{QL}\otimes\mathbf{S}^{(t-1)}\right)\mathbf{h}+\mathbf{n}^{(t-1)}\right]\geq 0\right) \tag{20}$$

As will be proven later, and in a way analogous to the diversity order analysis in subsection III-D, the expression of the conditional PEP $P(\mathbf{C}_i\rightarrow\mathbf{C}_j)$ can be completely determined

from the values of k and m such that $(k,m)=f(j-i)$ where the function $f(.)$ is defined in (8). In other words, different values of i and j yielding the same values of k and m will have the same conditional PEP and, hence, it is better to index this PEP by k and m rather than i and j. Based on this observation, (20) can be written under the following form:

$$P(\mathbf{C}_i \to \mathbf{C}_j) \triangleq P_{k,m} \triangleq \Pr\left(\eta_{k,m}^{(ss)} + \eta_{k,m}^{(sn)} + \eta_{k,m}^{(nn)} \geq 0\right) \tag{21}$$

where $\eta_{k,m}^{(ss)}$, $\eta_{k,m}^{(sn)}$ and $\eta_{k,m}^{(nn)}$ stand for the signal-cross-signal, signal-cross-noise and noise-cross-noise terms, respectively.

Based on (21), the conditional PEP given by $P_{e|\mathbf{H}} = \frac{1}{PM}\sum_{i=0}^{PM-1}\sum_{\substack{j=0\\ j\neq i}}^{PM-1} P(\mathbf{C}_i \to \mathbf{C}_j)$ can be evaluated from the following expression:

$$P_{e|\mathbf{H}} = \sum_{k=0}^{P-1}\sum_{\substack{m=0\\ (k,m)\neq(0,0)}}^{M-1} P_{k,m} \tag{22}$$

From (20) and (21):

$$\eta_{k,m}^{(ss)} = \mathbf{h}^T\left[\mathbf{I}_{QL}\otimes\left([\mathbf{S}^{(t-1)}]^T\mathbf{C}_i^T(\mathbf{C}_j-\mathbf{C}_i)\mathbf{S}^{(t-1)}\right)\right]\mathbf{h} \tag{23}$$

The recursive application of (4) shows that $\mathbf{S}^{(t-1)}$ can be written as $\mathbf{S}^{(t-1)} = \mathbf{A}^x\mathbf{S}^{(0)}$ where $x=\sum_{t'=1}^{t-1} z_{t'}$. Replacing $\mathbf{S}^{(t-1)} = \mathbf{A}^x\mathbf{S}^{(0)}$, $[\mathbf{S}^{(t-1)}]^T = [\mathbf{S}^{(0)}]^T\mathbf{A}^{-x}$, $\mathbf{C}_i = \mathbf{A}^i$, $\mathbf{C}_j = \mathbf{A}^j$ and $\mathbf{C}_i^T = \mathbf{A}^{-i}$ in (23) results in:

$$\eta_{k,m}^{(ss)} = \mathbf{h}^T\left[\mathbf{I}_{QL}\otimes\left([\mathbf{S}^0]^T(\mathbf{A}^{j-i}-\mathbf{I}_{PM})\mathbf{S}^{(0)}\right)\right]\mathbf{h} \tag{24}$$

$$= \sum_{l=1}^{QL}\mathbf{h}_l^T\left([\mathbf{S}^0]^T(\mathbf{A}^{j-i}-\mathbf{I}_{PM})\mathbf{S}^{(0)}\right)\mathbf{h}_l \tag{25}$$

where $\mathbf{h} = [\mathbf{h}_1^T\cdots\mathbf{h}_{QL}^T]^T$ (or $\mathbf{h}_l$ is the l-th column of the matrix $\mathbf{H}$ in (2)).

Following from the independence between the noise terms in blocks t and $t-1$, then from (20) and (21), $\eta_{k,m}^{(sn)}$ can be expressed as the sum of two independent terms as follows:

$$\eta_{k,m}^{(sn)} = \sum_{l=1}^{QL}[\mathbf{n}_l^{(t)}]^T(\mathbf{C}_j-\mathbf{C}_i)\mathbf{S}^{(t-1)}\mathbf{h}_l + \sum_{l=1}^{QL}\mathbf{h}_l^T[\mathbf{S}^{(t-1)}]^T\mathbf{C}_i^T(\mathbf{C}_j-\mathbf{C}_i)\mathbf{n}_l^{(t-1)} \tag{26}$$

where $\mathbf{n}^{(t')} = [[\mathbf{n}_1^{(t')}]^T\cdots[\mathbf{n}_{QL}^{(t')}]^T]^T$ for $t'=t-1,t$ (or $\mathbf{n}_l^{(t')}$ is the l-th column of the matrix $\mathbf{N}^{(t')}$ in (2)). It is then straightforward to prove that $\eta_{k,m}^{(sn)}$ is a zero-mean Gaussian random variable whose variance takes the following expression:

$$\text{var}(\eta_{k,m}^{(sn)}) = N_0\sum_{l=1}^{QL}\mathbf{h}_l^T\left([\mathbf{S}^0]^T(2I_{PM}-\mathbf{A}^{j-i}-\mathbf{A}^{i-j})\mathbf{S}^{(0)}\right)\mathbf{h}_l \tag{27}$$

Finally, from (20) and (21):

$$\eta_{k,m}^{(nn)} = \sum_{l=1}^{QL}[\mathbf{n}_l^{(t)}]^T\left(\mathbf{A}^j-\mathbf{A}^i\right)\mathbf{n}_l^{(t-1)} \tag{28}$$

which is a zero-mean random variable with variance:

$$\text{var}(\eta_{k,m}^{(nn)}) = 2MPQL\left(\frac{N_0}{2}\right)^2 \tag{29}$$

where, evidently, this variance does not depend on k and m.

In appendix B, we prove that (25) and (27) can be written as:

$$\eta_{k,m}^{(ss)} = -\nu_{k,m} \quad ; \quad \text{var}(\eta_{k,m}^{(sn)}) = 2N_0\nu_{k,m} \tag{30}$$

where:

$$\nu_{k,m} = \mathbf{h}^T\mathbf{h} - \begin{cases} R(k), & k\neq 0, m=0;\\ R(P-k), & k\neq 0, m=M-1;\\ 0, & \text{otherwise.}\end{cases} \tag{31}$$

where $R(k)=\sum_{l=1}^{QL}R_l(k)$ where $R_l(k)$ is equal to the sum of the elements on the k-th upper diagonal of the $P\times P$ matrix $\mathbf{h}_l\mathbf{h}_l^T$.

Replacing $\eta_{k,m}^{(ss)}$ by its value from (30), equation (21) can be written as:

$$P_{k,m} = \Pr\left(\eta_{k,m}^{(sn)} + \eta_{k,m}^{(nn)} \geq \nu_{k,m}\right) \tag{32}$$

Adopting the assumption that the noise-cross-noise term can be approximated by a Gaussian distribution especially for large values of the product $MPQL$ (by central-limit theorem arguments) [1], [2], [8], then the term $\eta_{k,m}^{(sn)} + \eta_{k,m}^{(nn)}$ can be modeled as a Gaussian random variable whose variance is $\text{var}(\eta_{k,m}^{(sn)}) + \text{var}(\eta_{k,m}^{(nn)}) = 2N_0\nu_{k,m} + 2MPQL\left(\frac{N_0}{2}\right)^2$ where (29) and (30) were invoked. Consequently, (32) can be written as:

$$P_{k,m} = Q\left(\frac{\nu_{k,m}}{\sqrt{2N_0\nu_{k,m} + 2MPQL\left(\frac{N_0}{2}\right)^2}}\right) \tag{33}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty}\exp\left(-\frac{t^2}{2}\right)\mathrm{d}t$ is the Q-function.

Consequently, from (22) and (31):

$$P_{e|\mathbf{H}} = \sum_{(k,m)\in\mathcal{S}} P_{k,m} + \sum_{k=1}^{P-1}P_{k,0} + \sum_{k=1}^{P-1}P_{k,M-1} \tag{34}$$

where $\mathcal{S} = \{(k,m) \mid k=0, m=1\cdots M-1\ ,\ k\neq 0, m=1\cdots M-2\}$ that comprises $[M-1+(P-1)(M-2)] = PM-2P+1$ elements. The third summation in (34) can be written in an alternative way as $\sum_{k=1}^{P-1}P_{P-k,M-1}$. Observing that $\nu_{P-k,M-1}=\nu_{k,0}$ for $k\neq 0$ from (31), then the second and third summations in (34) are equal. Finally, from (31) and (33), equation (34) can be written as:

$$P_{e|\mathbf{H}} = [PM-2P+1]\,Q\left(\frac{\mathbf{h}^T\mathbf{h}}{\sqrt{2N_0\mathbf{h}^T\mathbf{h} + 2MPQL\left(\frac{N_0}{2}\right)^2}}\right) + 2\sum_{k=1}^{P-1}Q\left(\frac{\mathbf{h}^T\mathbf{h}-R(k)}{\sqrt{2N_0[\mathbf{h}^T\mathbf{h}-R(k)] + 2MPQL\left(\frac{N_0}{2}\right)^2}}\right) \tag{35}$$

From Appendix B, $R(k)$ can be written as $R(k) = \sum_{l=1}^{QL}\sum_{p=1}^{P-k}h_{l,p}h_{l,p+k}$ where $h_{l,p}$ is the p-th component of $\mathbf{h}_l$ (which is also equal to the channel coefficient defined in (3)).

Given that the channel coefficients can be positive or negative with the same probability, then the cross-correlation terms $\{R(k)\}_{k\neq 0}$ (where each $R(k)$ corresponds to the summation of $(P-k)QL$ terms with random polarities) assume values that are very small compared to $R(0)=\mathbf{h}^T\mathbf{h}=\sum_{l=1}^{QL}\sum_{p=1}^{P}h_{l,p}^2$ (that corresponds to the summation of PQL positive terms). This observation is especially true for large values of the product PQL.

From (35) we can deduce the conditional PEP of a SIMO system deploying the differential modulation scheme $\mathbf{S}^{(t)}=\mathbf{\Omega}^{z_t}\mathbf{S}^{(t-1)}$ (where $\mathbf{S}^{(t)}$ stands for the PPM symbol transmitted in the t-th symbol duration) as follows:

$$P_{e|\mathbf{H}}^{(\text{SIMO})}=(M-1)Q\left(\frac{\mathbf{h}^T\mathbf{h}}{\sqrt{2N_0\mathbf{h}^T\mathbf{h}+2MQL\left(\frac{N_0}{2}\right)^2}}\right) \quad (36)$$

where in this case $\mathbf{h}^T\mathbf{h}=\sum_{l=1}^{QL}h_{l,1}^2$.

Finally, in the absence of exact expressions of the joint probability density function of $\mathbf{H}$, (35) and (36) will be integrated numerically to yield the results in section VI.

V. Simplified Decoding

In this section, we propose a simplified decoder that can be associated with the proposed differential scheme. In order to highlight the advantage of this decoder, we compare the number of operations (multiplications and additions) required by the ML decoder and the simplified decoder.

A. Complexity of the ML Decoder

The ML decision rule is based on (18) that can be written as:

$$\hat{z}_t=\arg\max_{i=0,\ldots,PM-1}\left[\sum_{l=1}^{QL}[\mathbf{y}_l^{(t)}]^T\mathbf{C}_i\mathbf{y}_l^{(t-1)}\right] \quad (37)$$

where the $PMQL$-dimensional decision vectors $\mathbf{y}^{(t')}$ in (18) are written as $\mathbf{y}^{(t')}=[[\mathbf{y}_1^{(t')}]^T\cdots[\mathbf{y}_{QL}^{(t')}]^T]^T$ for $t'=t-1,t$. In this case, $\mathbf{y}_l^{(t-1)}$ and $\mathbf{y}_l^{(t)}$ are PM-dimensional vectors for $l=1,\ldots,QL$.

Note that the components of the codewords $\mathbf{C}_i$'s are equal to 0 or 1. Moreover, every row of $\mathbf{C}_i$ contains exactly $PM-1$ zero components and one nonzero component that is equal to 1. Consequently, the vector $\mathbf{C}_i\mathbf{y}_l^{(t-1)}$ corresponds to a simple rearrangement of the elements of $\mathbf{y}_l^{(t-1)}$ and, hence, this vector can be evaluated without performing any multiplication operations.

In a more concise manner:

$$\mathbf{C}_i\mathbf{y}_l^{(t-1)}=\Big[[\mathbf{\Omega}^{m+1}\mathbf{y}_{l,\sigma^k(1)}^{(t-1)}]^T,\cdots,[\mathbf{\Omega}^{m+1}\mathbf{y}_{l,\sigma^k(k)}^{(t-1)}]^T,$$
$$[\mathbf{\Omega}^{m}\mathbf{y}_{l,\sigma^k(k+1)}^{(t-1)}]^T,\cdots,[\mathbf{\Omega}^{m}\mathbf{y}_{l,\sigma^k(P)}^{(t-1)}]^T\Big]^T \quad (38)$$

where the multiplication by the matrix $\mathbf{\Omega}^m$ corresponds to a permutation of order m. In (38), $(k,m)=f(i)$ from (8), $\mathbf{y}_l^{(t-1)}=[[\mathbf{y}_{l,1}^{(t-1)}]^T\cdots[\mathbf{y}_{l,P}^{(t-1)}]^T]^T$ and $\sigma^k(.)$ defines a permutation of order k among the elements of $\{1,\ldots,P\}$:

$$\sigma^k(p)=[(p-k-1)\mod P]+1\ ;\ p=1,\ldots,P \quad (39)$$

In other words, multiplying $\mathbf{y}_l^{(t-1)}$ by $\mathbf{C}_i$ corresponds to performing a double permutation. The first permutation is among the P vectors $\{\mathbf{y}_{l,p}^{(t-1)}\}_{p=1}^{P}$ while the second permutation is among the M components of each of these vectors.

Based on the above observation, the evaluation of $[\mathbf{y}_l^{(t)}]^T\mathbf{C}_i\mathbf{y}_l^{(t-1)}$ necessitates PM multiplications and $PM-1$ additions for one particular value of (i,l). Therefore, the implementation of (37) requires $PM\times QL\times PM=QL(PM)^2$ multiplications for the detection of one information symbol. Assuming that finding the maximum among n elements necessitates n additions, then the total number of additions is $PM\times(QL-1)\times(PM-1)+PM=(QL-1)(PM)^2-PM(QL-2)$.

Note that the number of multiplications varies as the square of the ST constellation size PM and, hence, the complexity of the ML decoder might be prohibitive for large values of the number of transmit antennas and/or cardinality of the PPM signal set thus justifying the interest in a simplified decoder.

B. A Simplified Decoding Procedure

The simplified decoder profits from the structure of the proposed code and, following from the equivalence between the codeword index i and the integers $(k,m)=f(i)$, solves for the integers $\hat{k}$ and $\hat{m}$ such that:

$$(\hat{k},\hat{m})=\arg\max_{\substack{k=0,\ldots,P-1\\ m=0,\ldots,M-1}}\left[\sum_{l=1}^{QL}\left[\sum_{p=1}^{k}[\mathbf{y}_{l,p}^{(t)}]^T\mathbf{\Omega}^{m+1}\mathbf{y}_{l,\sigma^k(p)}^{(t-1)}\right.\right.$$
$$\left.\left.+\sum_{p=k+1}^{P}[\mathbf{y}_{l,p}^{(t)}]^T\mathbf{\Omega}^{m}\mathbf{y}_{l,\sigma^k(p)}^{(t-1)}\right]\right] \quad (40)$$

where this equation follows from replacing (38) in (37) and where the decoder decides in favor of $\hat{z}_t=\hat{m}P+\hat{k}$.

In what follows, $t'\in\{t-1,t\}$. Consider the M-dimensional vector $\mathbf{y}_{l,p}^{(t')}$ that, for a certain value of l, comprises the decision variables collected in the M PPM positions of the p-th symbol duration of the t'-th block. Only one component of $\mathbf{y}_{l,p}^{(t')}$ comprises a signal part while the remaining $M-1$ components comprise only noise following from the structure of the proposed code where exactly one transmit antenna is pulsed within each symbol duration. Based on this fact, we define the position $\tilde{m}_p^{(t')}$ as the PPM position in which the maximum amount of energy is collected:

$$\tilde{m}_p^{(t')}=\arg\max\sum_{l=1}^{QL}[\mathbf{y}_{l,p}^{(t')}\circ\mathbf{y}_{l,p}^{(t')}] \quad (41)$$

where $\circ$ stands for the element-wise Hadamard product and the function $\arg\max(\mathbf{v})$ returns the position of the maximum component of the vector $\mathbf{v}$.

Based on (41), we define the alternative decision vector $\tilde{\mathbf{y}}_{l,p}^{(t')}$ as:

$$\tilde{\mathbf{y}}_{l,p}^{(t')}=y_{l,p,\tilde{m}_p^{(t')}}^{(t')}\mathbf{e}_{\tilde{m}_p^{(t')}}\triangleq x_{l,p}^{(t')}\mathbf{e}_{\tilde{m}_p^{(t')}} \quad (42)$$

where $y_{l,p,m}^{(t')}$ is the m-th component of $\mathbf{y}_{l,p}^{(t')}$. Note that $\tilde{\mathbf{y}}_{l,p}^{(t')}$ is equivalent to $\mathbf{y}_{l,p}^{(t')}$ where all components corresponding to the

PPM slots containing only noise, based on the decision made in (41), are set to zero. In this context:

$$\tilde{y}^{(t')}_{l,p,\tilde{m}^{(t')}_p} = y^{(t')}_{l,p,\tilde{m}^{(t')}_p} = x^{(t')}_{l,p} \tag{43}$$

Replacing the vectors $\{\mathbf{y}^{(t')}_{l,p}\}$ by the vectors $\{\tilde{\mathbf{y}}^{(t')}_{l,p}\}$ in (40) results in:

$$(\hat{k},\hat{m}) = \arg \max_{\substack{k=0,\ldots,P-1\\ m=0,\ldots,M-1}} \left[\sum_{l=1}^{QL}\left[\sum_{p=1}^{k}[\tilde{\mathbf{y}}^{(t)}_{l,p}]^T \mathbf{\Omega}^{m+1}\tilde{\mathbf{y}}^{(t-1)}_{l,\sigma^k(p)} + \sum_{p=k+1}^{P}[\tilde{\mathbf{y}}^{(t)}_{l,p}]^T \mathbf{\Omega}^{m}\tilde{\mathbf{y}}^{(t-1)}_{l,\sigma^k(p)}\right]\right] \tag{44}$$

which can be written under the following form:

$$(\hat{k},\hat{m}) = \arg \max_{\substack{k=0,\ldots,P-1\\ m=0,\ldots,M-1}} \left[\sum_{p=1}^{k}\left[\sum_{l=1}^{QL}\sum_{m'=1}^{M}[\tilde{y}^{(t)}_{l,p,m'}\tilde{y}^{(t-1)}_{l,\sigma^k(p),\tau^{m+1}(m')}\right] + \sum_{p=k+1}^{P}\left[\sum_{l=1}^{QL}\sum_{m'=1}^{M}[\tilde{y}^{(t)}_{l,p,m'}\tilde{y}^{(t-1)}_{l,\sigma^k(p),\tau^{m}(m')}\right]\right] \tag{45}$$

where the function $\tau^m(.)$ defines a permutation of order m among the elements of $\{1,\ldots,M\}$:

$$\tau^m(m') = [(m'-m-1) \mod M]+1 \;\; ; \;\; m'=1,\ldots,M \tag{46}$$

The simplified decoder is based on the assumption that the PPM slots that comprise UWB pulses are actually the slots that will result in the maximum amount of collected energy based on (41). Under this assumption, the zero components of the vectors $\tilde{\mathbf{y}}^{(t)}_{l,p}$ and $\mathbf{\Omega}^{m+1}\tilde{\mathbf{y}}^{(t-1)}_{l,\sigma^k(p)}$ (resp. $\mathbf{\Omega}^{m}\tilde{\mathbf{y}}^{(t-1)}_{l,\sigma^k(p)}$) will coincide for $p=1,\ldots,k$ (resp. $p=k+1,\ldots,P$). Consequently, the maximization in (45) will become independent of m and will simplify to the following expression:

$$\hat{k} = \arg \max_{k=0,\ldots,P-1} \left[\sum_{p=1}^{k}\sum_{l=1}^{QL}\tilde{y}^{(t)}_{l,p,\tilde{m}^{(t)}_p}\tilde{y}^{(t-1)}_{l,\sigma^k(p),\tilde{m}^{(t-1)}_{\sigma^k(p)}} + \sum_{p=k+1}^{P}\sum_{l=1}^{QL}\tilde{y}^{(t)}_{l,p,\tilde{m}^{(t)}_p}\tilde{y}^{(t-1)}_{l,\sigma^k(p),\tilde{m}^{(t-1)}_{\sigma^k(p)}}\right] \tag{47}$$

which can be written in a simpler way as:

$$\hat{k} = \arg \max_{k=0,\ldots,P-1} \left[\sum_{p=1}^{P} D_{p,k}\right] \tag{48}$$

where:

$$D_{p,k} \triangleq \sum_{l=1}^{QL} x^{(t)}_{l,p}x^{(t-1)}_{l,\sigma^k(p)} \tag{49}$$

where (43) was invoked.

The transition from (45) to (47) will hold if the following P equations are satisfied:

$$\begin{cases} \tilde{m}^{(t)}_p = \tau^{m+1}(\tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p}) & p=1,\ldots,\hat{k};\\ \tilde{m}^{(t)}_p = \tau^{m}(\tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p}) & p=\hat{k}+1,\ldots,P. \end{cases} \tag{50}$$

Solving (50) for m implies that this integer must satisfy the following P equations simultaneously:

$$\begin{cases} m = \tilde{m}^{(t)}_p - \tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p} - 1 \mod M & p=1,\ldots,\hat{k};\\ m = \tilde{m}^{(t)}_p - \tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p} \mod M & p=\hat{k}+1,\ldots,P. \end{cases} \tag{51}$$

Evidently, discrepancies might arise between the above equations that do not yield the same solution following from the fact that the adopted assumption does not necessarily hold and hence the positions of the transmitted pulses are not inevitably as predicted by (41). Our approach for solving (51) resides in weighing the corresponding equations by the decision metrics $D_{p,k}$'s; a task that can be realized if the reconstructed value $\hat{m}$ is selected to satisfy the following equation:

$$\hat{m} = \arg\max \left[\sum_{p=1}^{\hat{k}} D_{p,\hat{k}}\mathbf{e}_{(\tilde{m}^{(t)}_p - \tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p} - 1 \mod M+1)} + \sum_{p=\hat{k}+1}^{P} D_{p,\hat{k}}\mathbf{e}_{(\tilde{m}^{(t)}_p - \tilde{m}^{(t-1)}_{\sigma^{\hat{k}}p} \mod M+1)}\right] - 1 \tag{52}$$

To summarize, the simplified decoder solves for $(\hat{k},\hat{m})$ in the following steps:

- *Step 1:* Find the values of $\tilde{m}^{(t')}_p$ in (41) for $t'=t-1,t$ and $p=1,\ldots,P$.
- *Step 2:* Evaluate the values of the P^2 metrics $D_{p,k}$ in (49) for $p=1,\ldots,P$ and $k=0,\ldots,P-1$.
- *Step 3:* Find $\hat{k}$ according to (48).
- *Step 4:* Using the values of $\tilde{m}^{(t-1)}_p$, $\tilde{m}^{(t)}_p$ and $D_{p,k}$ found in step-1 and step-2, find $\hat{m}$ according to (52).

C. Complexity of the Simplified Decoder

We quantify the complexity of the proposed decoder by evaluating the number of operations required in each of the above four steps.

Step 1: From (41), evaluating a single value of $\tilde{m}^{(t')}_p$ requires raising QL vectors to the power two, adding these vectors and finding the maximum value of the resultant M-dimensional vector. Consequently, this step requires QLM multiplications and $(QL-1)M+M=QLM$ additions where, as in subsection V-A, it is assumed that finding the maximum among M components necessitates M additions. Consequently, for evaluating $\tilde{m}^{(t')}_1,\ldots,\tilde{m}^{(t')}_P$, $QLMP$ multiplications and $QLMP$ additions are required. Note that $\tilde{m}^{(t')}_p$ enters in the decision process of the two consecutive information symbols $z_{t'}$ and $z_{t'+1}$ and hence the above number of operations needs to be considered only once (and not two times for $t'=t-1$ and $t'=t$). In a more concise manner, for communicating N_s information symbols, N_s+1 blocks are needed (taking into consideration the reference block), and hence the total number of multiplications (or additions) needed is $(N_s+1)QLPM$ implying that the number of multiplications (or additions) for decoding one symbol is $\frac{N_s+1}{N_s}QLPM$ which tends to $QLPM$ for large values of N_s. As a conclusion,

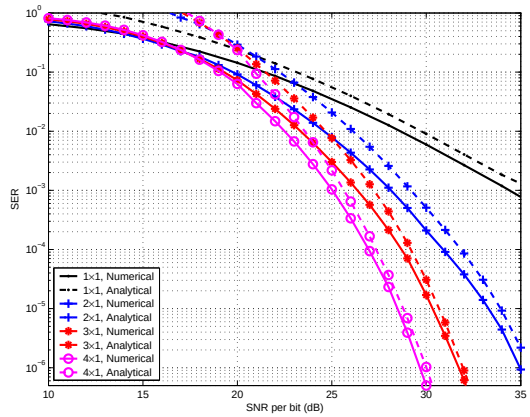

Fig. 3. Performance with 8-PPM and $L = 4$.

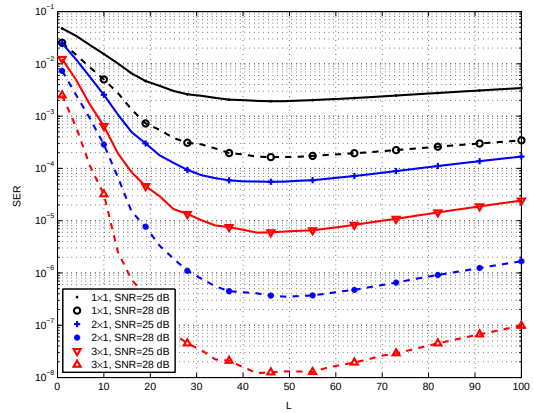

Fig. 4. Performance as a function of L with 2-PPM.

step-1 is realized through $QLPM$ multiplications and $QLPM$ additions.

Step 2: From (43), the variable $x_{l,p}^{(t')}$ is nothing but a component of the decision vector $\mathbf{y}_{l,p}^{(t')}$ and hence can be acquired without requiring any additions or multiplications. Consequently, calculating the P^2 decision variables $D_{p,k}$ in (49) requires P^2QL multiplications and $P^2(QL-1)$ additions.

Step 3: From (48), evaluating $\sum_{p=1}^{P} D_{p,k}$ for a single value of k in $\{0,\ldots,P-1\}$ requires $P-1$ additions. Consequently, finding the value of $\hat{k}$ requires $P(P-1)+P=P^2$ additions without requiring any multiplications.

Step 4: The multiplication of the metrics $D_{p,\hat{k}}$'s by the columns of the identity matrix in (52) does not require any number of multiplications. Regarding the number of additions in (52). (i): The evaluation of the subscripts of the vectors $\mathbf{e}$ requires $3\hat{k}+2(P-\hat{k})=2P+\hat{k}$ which is at most equal to $3P-1$ when $\hat{k}$ takes its maximum possible value of $P-1$. Here it is assumed that the $\mod$ operator does not require any number of additions since it can be evaluated using a look-up table. (ii): The evaluation of the summation of P multiples of columns of the identity matrix requires at most $P-1$ additions when all the nonzero components of these vectors coincide. (iii): The $\max$ operator requires M additions. (iv): The substraction of 1 at the end requires one addition. As a conclusion, the number of additions in this step is at most $(3P-1)+(P-1)+M+1=4P+M-1$.

As a conclusion, the implementation of the simplified decoder requires $QLP(M+P)$ multiplications and $QLP(M+P)+4P+M-1$ additions for the detection of one information symbol. Therefore, the number of multiplications is divided by a factor of $\frac{QL(PM)^2}{QLP(M+P)}=\frac{PM^2}{M+P}$ compared to the ML decoder. For example, for binary PPM with two transmit antennas, the simplified decoder requires two times less multiplications compared to the ML decoder.

VI. Numerical Results

In this section, we present some numerical results that show the variations of the symbol error rate (SER) as a function of the signal-to-noise ratio (SNR) per information bit. The SNR per information bit is defined as $\frac{1}{RN_0}$ where the average energy of the M-PPM constellations was normalized to unity and where R is given in (9) for the proposed code and $R=\log_2(M)$ for single-antenna systems. The UWB channels between the different transmit and receive antennas are generated independently according to the IEEE 802.15.3a NLOS channel model recommendation CM2 [26]. A Gaussian pulse with a duration of $T_w=0.5$ ns is used and the modulation delay is set to $\delta=100$ ns in order to eliminate the interference between the different PPM slots.

Fig. 3 shows the performance with 8-PPM and $L=4$ (which corresponds to an integration time of 2 ns) where the ML decoder is applied. We compare the numerical results with the analytical results derived in section IV. Results show the high performance levels and the enhanced diversity orders achieved by the proposed scheme. For example, performance gains in the order of 9 dB with respect to single-antenna systems can be observed with four transmit antennas at a SER of 10^{-3}. Results in Fig. 3 also show that the numerical and analytical results are close to each other. Moreover, the corresponding curves are parallel to each for large values of the SNR and, hence, the derived closed-form expressions of the conditional PEP can be used to predict the achievable diversity orders. It is worth noting that the difference between the numerical and analytical curves results from two reasons. The first reason resides in the fact that in section IV we derived the pairwise error probability and hence the derived expressions constitute upper-bounds that originate from the union bound. The second reason follows from the Gaussian approximation of the noise-cross-noise term.

Fig. 4 shows the impact of the number of combined multi-path components (through the parameter L) on the performance of single-antenna and MIMO UWB systems. In this figure, the SER is plotted as a function of L in the case of 2-PPM with one receive antenna. This figure highlights the usefulness of spatial diversity even in UWB systems that profit from rich multi-path diversity. This follows mainly from the high correlation between the different multi-path components of the same channel [26]. At a given SNR, increasing the value of L does not always enhance the performance where the results accentuate on the existence of an optimal value of L beyond which the performance degrades when L increases. This follows from the fact that more noise is integrated in the

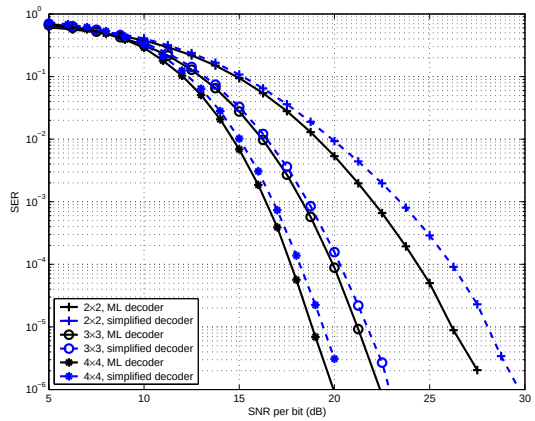

Fig. 5. Performance of the simplified decoder with 2-PPM and $L = 5$.

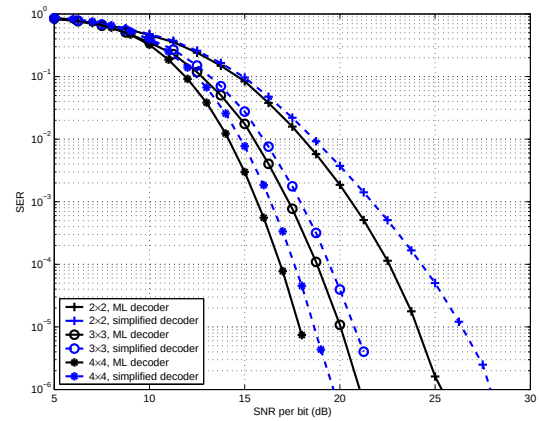

Fig. 6. Performance of the simplified decoder with 8-PPM and $L = 5$.

receiver when L increases while the multi-path components at the tail of the channel impulse response assume small values. In this context, increasing the number of antennas always enhances the performance. For example, at a SNR of 25 dB, the best performance that can be achieved by single-antenna systems is 2×10^{-3} (for $L = 45$). Any value of L no matter how large it is can not decrease this SER value. However, systems with two and three transmit antennas can achieve comparable performance levels with only $L = 10$ and $L = 6$, respectively. In the same way, at a SNR of 28 dB, the optimal SER value decreases from 1.6×10^{-4} with single-antenna systems to 3.5×10^{-7} and 1.2×10^{-8} with 2×1 and 3×1 systems, respectively.

In Fig. 5 we compare the ML decoder and the simplified decoder with 2-PPM, $L = 5$ and $P \times P$ systems for $P = 2, 3, 4$. The numbers of multiplications required by the ML decoder for the detection of one symbol are 160, 540 and 1280 while the simplified decoder requires 80, 225 and 480 multiplications for $P = 2$, 3 and 4, respectively. In other words, the numbers of multiplications are reduced by factors of 2, 2.4 and 2.66, respectively, implying significant savings in the computationally-involved multiplication operations. In the same way, the numbers of additions are reduced from 112, 426 and 1072 to 89, 238 and 497 for $P = 2$, 3 and 4, respectively. The obtained results highlight the interest of the simplified decoder where the performance levels achieved by this decoder are very close to those achieved by the optimal ML decoder especially for large values of P. In this context, the performance degradations induced by the suboptimal detection are in the order of 1.8 dB, 0.4 dB and 0.5 dB at a SER of 10^{-4} for $P = 2$, 3 and 4, respectively. Moreover, the results show that the simplified decoder possesses the desirable property of being a diversity-preserving decoder where the error curves corresponding to the ML and simplified detection are practically parallel for large values of the SNR. In this context, associating the proposed code with the simplified decoder does not induce any losses in terms of the achievable diversity order.

In Fig. 6 we compare the ML decoder and the simplified decoder with 8-PPM, $L = 5$ and $P \times P$ systems for $P = 2, 3, 4$. The findings are similar to those in Fig. 5 where the simplified decoder is found to be diversity-preserving and incurs limited performance losses especially with large number of antennas. Note that in this case where M takes a large value, the simplified decoder reduces the number of multiplications by factors of 12.8, 17.45 and 21.33 as well as the number of additions by factors of 10.12, 15 and 19.2 for $P = 2$, 3 and 4, respectively.

In Fig. 7 we compare different ST codes with $P = 2$, $M = 4$ and $L = 6$ (or equivalently an integration time of 3 ns). The codes that we compare are as follows. (i): The proposed differential ST code that transmits at the rate of $\frac{1}{P}\log_2(MP) = 1.5$ bits pcu. (ii): The noncoherent code in [25] that in this case transmits at the rate of $\frac{1}{P}\log_2\binom{M-1}{P} = 0.7925$ bits pcu. (iii): The coherent PPM code in [28] that transmits at the full rate of $\log_2(M) = 2$ bits pcu. (iv): The repetition code where the differentially-encoded PPM symbols are transmitted separately by the two transmit antennas in two consecutive symbol durations. This code transmits at the rate of $\frac{1}{P}\log_2(M) = 1$ bit pcu. (v): The differential code in [22] that corresponds to a PPM extension of the code in [24] where the rate is $\log_2(M) = 2$ bits pcu. Note that all of the above codes are shape-preserving with PPM except for the last one. Results show that all considered codes achieve the same diversity order where all the SER curves are practically parallel to each other for large values of the SNR. Evidently, the best performance is achieved by the coherent code where full channel state information is available at the receiver. Results also show the superiority of the proposed differential code with respect to the noncoherent and repetition codes since, in this case, the differential code is transmitting at a higher rate (while all three codes respect equally the remaining design constraints). Compared to [22], results show a 1.2 dB performance loss at high SNR. This loss is not surprising since the proposed code respects the additional constraint of being shape-preserving unlike [22]. In fact, while the proposed code transmits pulses that have the same amplitude, four amplitude levels are transmitted by [22]. In other words, the performance loss follows from the additional shape-preserving design constraint that is imposed on the proposed code. It is worth noting that, unlike [22], the proposed code can be applied with any number of transmit antennas. As a conclusion, the shape-

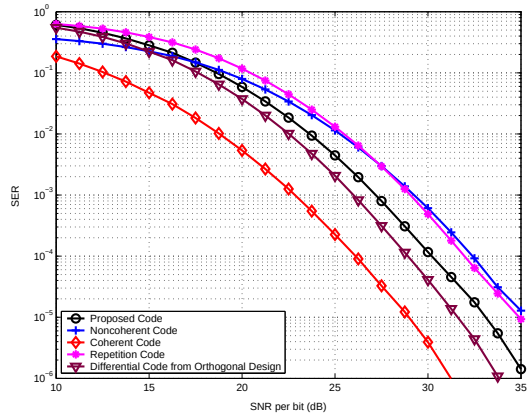

Fig. 7. Comparison between different ST codes with 4-PPM for $P = 2$ and $L = 6$.

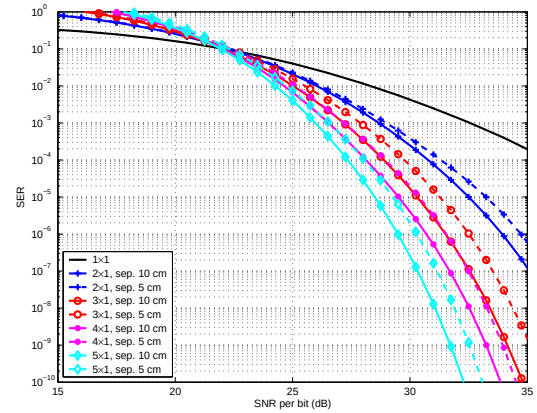

Fig. 8. Performance of 2-PPM over the Kunisch-Pamp profile-2 model [31].

preserving property constitutes a restricting constraint that has a critical impact on the achievable performance levels.

While all of the previous simulations were performed assuming that the MIMO channels are independent, Fig. 8 shows the performance over the space-variant UWB channel model proposed in [31]. Simulations are performed over profile 2 that corresponds to an office NLOS scenario for antenna array separations of 5 cm and 10 cm. The analytical curves are plotted for 2-PPM with $L = 10$. Results show the high performance levels over this realistic MIMO model that takes spatial correlation into consideration. Despite the fact that the different channels are correlated, increasing the number of antennas always enhances the performance especially for large values of the SNR. It can also be observed that the different array separations achieve the same diversity order where the corresponding SER curves are practically parallel to each other for large values of the SNR. In this context, the smaller separation results in a slightly worse performance in the order of 0.75 dB at a SER of 10^{-6}. Finally, it is worth noting that while the channel correlation has a direct impact on the achievable performance gains with respect to single-antenna systems, it does not influence the ST code design, conditional SER performance and decoder structure presented in sections III, IV and V, respectively.

VII. Conclusion

We considered the problem of differential space-time coding for IR-UWB communications and we proposed the first-known family of unitary codes that is shape-preserving with PPM. The proposed construction responds to the practical need of realizing MIMO IR-UWB communications in an easy manner that avoids any channel estimation procedure. The novel idea of joint symbol and position permutations of one encoded block with respect to the previous block replaced the conventional techniques based on amplitude-scaling and phase-rotation thus allowing to maintain unipolar transmissions. The proposed solution is appealing since it renders the extension of the single-antenna systems to the MIMO scenario simple and cost-effective without imposing any additional constraints on the RF circuitry to control the phase or the amplitude of the very low duty cycle sub-nanosecond pulses. The above advantages came at the expense of a reduced data rate; however, this data rate reduction is small for small values of the signal set cardinality rendering the proposed differential solution superior to the noncoherent space-time solutions under this operating scenario. We hope that this first construction will inspire future constructions and will motivate more research in the direction of achieving higher rates with unipolar PPM systems. An adapted suboptimal decoding strategy was also proposed which further contributes to the implementation simplicity of the proposed MIMO IR-UWB system.

Appendix A

We start our proof with the following preliminary.

Preliminary 1: The following relation holds:

$$-c\mathbf{e}_1+c'\mathbf{\Omega}^n\mathbf{e}_1 = \mathbf{0}_{M\times 1} \Rightarrow \begin{cases} c' = c, & n = 0 \mod M; \\ c' = c = 0, & n \neq 0 \mod M. \end{cases} \quad (53)$$

Proof: For $n = (0 \mod M)$, $\mathbf{\Omega}^n = \mathbf{I}_M$ and the relation in (53) reduces to $(-c + c')\mathbf{e}_1 = \mathbf{0}_{M\times 1}$ implying that $c' = c$. For $n \neq (0 \mod M)$, $\mathbf{\Omega}^n \neq \mathbf{I}_M$ and $\mathbf{\Omega}^n\mathbf{e}_1$ is equal to a certain element $\mathbf{e}_{n'}$ in $\mathcal{C}_{\text{PPM}}$ that is different from $\mathbf{e}_1$ (in particular $n' = (n \mod M) + 1$). In this case, the relation in (53) can be written as $c\mathbf{e}_1 = c'\mathbf{e}_{n'}$ implying that $c' = c = 0$ since $\mathbf{e}_1$ can not be proportional to $\mathbf{e}_{n'}$ for $n' \neq 1$. ■

The linear dependence between the columns of $\mathbf{D}_i$ in (11) implies the existence of the scalars $c_1, \ldots, c_P$ such that $\sum_{p=1}^{P} c_p\mathbf{d}_{i,p} = \mathbf{0}_{PM\times 1}$ where $\mathbf{d}_{i,p}$ is the p-th column of $\mathbf{D}_i$. We will next prove that this relation holds only in the case of $c_1 = \cdots = c_P = 0$ implying that $\mathbf{D}_i$ has a full rank of P for $i \neq 0$. As in subsection III-D, the structure of $\mathbf{D}_i$ depends on the values of k and m where $(k, m) = f(i)$ from (8). It is worth noting that k takes values in $\{0, \ldots, P-1\}$ while the values of m are limited to the set $\{0, \ldots, M-1\}$.

Viewing the $PM \times P$ matrix $\mathbf{D}_i$ as a $P \times P$ block matrix composed of blocks of dimensions $M \times 1$, the following can be observed regarding the structure of $\mathbf{D}_i$. (i): The blocks on the main diagonal are equal to $-\mathbf{e}_1$. (ii): The blocks on the k-th lower diagonal are equal to $\mathbf{\Omega}^m\mathbf{e}_1$. (iii): The blocks on the $(P-k)$-th upper diagonal are equal to $\mathbf{\Omega}^{m+1}\mathbf{e}_1$. (iv): The remaining blocks are equal to $\mathbf{0}_{M\times 1}$. Note that for $k = 0$ the

above structure corresponds to a block diagonal matrix whose diagonal blocks are equal to $\mathbf{\Omega}^m\mathbf{e}_1 - \mathbf{e}_1$ where in this case $m \neq 0$ so that $i = mP + k \neq 0$.

Based on the above, the relation $\sum_{p=1}^{P} c_p \mathbf{d}_{i,p} = \mathbf{0}_{PM\times 1}$ can be written as the following set of P equations:

$$-c_i\mathbf{e}_1 + c_{\sigma^k(i)}\mathbf{\Omega}^{m+1}\mathbf{e}_1 = \mathbf{0}_{M\times 1} \;\; ; \;\; i = 1,\ldots,k \tag{54}$$

$$-c_i\mathbf{e}_1 + c_{\sigma^k(i)}\mathbf{\Omega}^{m}\mathbf{e}_1 = \mathbf{0}_{M\times 1} \;\; ; \;\; i = k+1,\ldots,P \tag{55}$$

where the first (resp. second) set of k (resp. $P-k$) equations describes the linear dependence between the diagonal blocks and the upper (resp. lower) blocks. In (54)-(55), the function $\sigma^k(.)$ defines a permutation of order k among the elements of $\{1,\ldots,P\}$:

$$\sigma^k(i) = [(i-k-1) \mod P] + 1 \;\; ; \;\; i = 1,\ldots,P \tag{56}$$

We first consider the simplest case of $k = 0$. In this case, (54)-(55) can be written as:

$$-c_i\mathbf{e}_1 + c_i\mathbf{\Omega}^{m}\mathbf{e}_1 = \mathbf{0}_{M\times 1} \;\; ; \;\; i = 1,\ldots,P \tag{57}$$

Since $m \neq 0$ for $k = 0$, then applying preliminary 1 with $n = m \neq 0 \mod M$ (in this case $m \in \{1,\ldots,M-1\}$), (57) implies that $c_i = 0$ for $i = 1,\ldots,P$ completing the proof for this special case.

In what follows, we take $k \neq 0$ where the following cases arise.

Case 1: $m \neq 0$ and $m \neq M-1$; in other words $m \in \{1,\ldots,M-2\}$. In this case, $m+1 \neq 0 \mod M$, then applying preliminary 1 with $n = m+1$, (54) implies that $c_i = 0$ for $i = 1,\ldots,k$. In the same way, since $m \neq 0 \mod M$, then applying preliminary 1 with $n = m$, (55) implies that $c_i = 0$ for $i = k+1,\ldots,P$. Therefore, $c_i = 0$ for $i = 1,\ldots,P$ completing the proof for this case.

For the remaining cases, (54)-(55) will be written in a more convenient form as follows:

$$-c_i\mathbf{e}_1 + c_{\sigma^k(i)}\mathbf{\Omega}^{m+1}\mathbf{e}_1 = \mathbf{0}_{M\times 1} \;\; ; \;\; i = 1,\ldots,k \tag{58}$$

$$-c_{\sigma^{-k}(i)}\mathbf{e}_1 + c_i\mathbf{\Omega}^{m}\mathbf{e}_1 = \mathbf{0}_{M\times 1} \;\; ; \;\; i = 1,\ldots,P-k \tag{59}$$

where $\sigma^{-k}(.)$ can be obtained from (56) by replacing k with $-k$.

Case 2: $m = 0$. In this case, applying preliminary 1 with $n = m+1 = 1 \neq 0 \mod M$, (58) results in the following k equalities:

$$c_i = 0 \;\; ; \;\; i = 1,\ldots,k \tag{60}$$

as well as the equalities $c_{\sigma^k(i)} = 0$ for $i = 1,\ldots,k$ that can be written in a more convenient way as $c_{i+(P-k)} = 0$ since $\sigma^k(i) = i+(P-k)$ for $i \in \{1,\ldots,k\}$. Finally, these equalities can be written as:

$$c_i = 0 \;\; ; \;\; i = (P-k)+1,\ldots,P \tag{61}$$

Moreover, applying preliminary 1 with $n = m = 0 \mod M$, (59) results in $c_i = c_{\sigma^{-k}(i)}$ for $i = 1,\ldots,P-k$ that can be written in a more convenient way as $c_i = c_{i+k}$ since $\sigma^{-k}(i) = i+k$ for $i \in \{1,\ldots,P-k\}$. Finally, these equalities can be written as:

$$c_i = c_{i-k} \;\; ; \;\; i = k+1,\ldots,P \tag{62}$$

We will next prove that (60)-(62) imply that $c_i = 0$ for all values of i. The proof calls for distinguishing the two cases $k > P-k$ and $k \leq P-k$.

Case 2.1: $k > P-k$. In this case, $k \geq (P-k)+1$ and (60) and (61) will imply that $c_i = 0$ for all values of i in $\{1,\ldots,P\}$.

Case 2.2: $k \leq P-k$. In this case, replacing $c_1 = \cdots = c_k = 0$ from (60) in (62) results in $c_{k+1} = \cdots = c_{2k} = 0$. Replacing these k zero values in (62) a second time results in $c_{2k+1} = \cdots = c_{3k} = 0$. As a conclusion, applying the relation in (62) recursively over blocks of k values of c_i's keeping in mind that the values in the previous block are zero results in $c_1 = \cdots = c_P = 0$.

Case 3: $m = M-1$. In this case, applying preliminary 1 with $n = m = M-1 \neq 0 \mod M$, (59) results in the following $P-k$ equalities:

$$c_i = 0 \;\; ; \;\; i = 1,\ldots,P-k \tag{63}$$

as well as the equalities $c_{\sigma^{-k}(i)} = 0$ for $i = 1,\ldots,P-k$ that can be written in a more convenient way as $c_{i+k} = 0$ since $\sigma^{-k}(i) = i+k$ for $i \in \{1,\ldots,P-k\}$. Finally, these equalities can be written as:

$$c_i = 0 \;\; ; \;\; i = k+1,\ldots,P \tag{64}$$

Moreover, applying preliminary 1 with $n = m+1 = M = 0 \mod M$, (58) results in $c_i = c_{\sigma^k(i)}$ for $i = 1,\ldots,k$ that can be written in a more convenient way as $c_i = c_{i+(P-k)}$ since $\sigma^k(i) = i+(P-k)$ for $i \in \{1,\ldots,k\}$. Finally, these equalities can be written as:

$$c_i = c_{i-(P-k)} \;\; ; \;\; i = (P-k)+1,\ldots,P \tag{65}$$

For $m = M-1$, we consider the two cases $k < P-k$ and $k \geq P-k$.

Case 3.1: $k < P-k$. Since in this case $P-k \geq k+1$, (63) and (64) will imply that $c_i = 0$ for $i = 1,\ldots,P$.

Case 3.2: $k \geq P-k$. In this case, replacing $c_1 = \cdots = c_{P-k} = 0$ from (63) in (65) results in $c_{(P-k)+1} = \cdots = c_{2(P-k)} = 0$. As a conclusion, applying the relation in (65) recursively over blocks of $P-k$ values of c_i's keeping in mind that the values in the previous block are zero results in $c_1 = \cdots = c_P = 0$.

It is worth noting the analogy between cases 2.1 and 3.1 ($(m = 0, k > P-k)$ and $(m = M-1, k < P-k)$) on one hand and cases 2.2 and 3.2 $(m = 0, k \leq P-k)$ and $(m = M-1, k \geq P-k)$) on the other hand.

As a conclusion, all the above cases show that the matrix $\mathbf{D}_i$ has a full rank of P for $i \neq 0$ completing the proof.

Appendix B

From (25), define the $P \times P$ matrix $\mathbf{E}_{k,m}$ as $\mathbf{E}_{k,m} = [\mathbf{S}^0]^T(\mathbf{A}^{j-i} - \mathbf{I}_{PM})\mathbf{S}^{(0)}$ where $(k,m) = f(j-i)$ from (8). Similarly, from (27), define the $P \times P$ matrix $\mathbf{F}_{k,m}$ as $\mathbf{F}_{k,m} = [\mathbf{S}^0]^T(2I_{PM} - \mathbf{A}^{j-i} - \mathbf{A}^{i-j})\mathbf{S}^{(0)}$. Consequently, (25)

and (27) can be written as:

$$\eta_{k,m}^{(ss)} = \sum_{l=1}^{QL} \mathbf{h}_l^T \mathbf{E}_{k,m} \mathbf{h}_l \tag{66}$$

$$\text{var}(\eta_{k,m}^{(sn)}) = N_0 \sum_{l=1}^{QL} \mathbf{h}_l^T \mathbf{F}_{k,m} \mathbf{h}_l \tag{67}$$

We first consider the simple case of $k = 0$ where in this case $m \neq 0$ since $j \neq i$ and hence $(k, m) \neq (0, 0)$. In this case, $\mathbf{E}_{k,m}$ is a diagonal matrix whose diagonal elements are equal to $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 - \mathbf{e}_1^T \mathbf{e}_1 = -1$ since $m \neq 0$ resulting in $\mathbf{E}_{k,m} = -\mathbf{I}_P$ and $\eta_{k,m}^{(ss)} = -\sum_{l=1}^{QL} \mathbf{h}_l^T \mathbf{h}_l = -\mathbf{h}^T \mathbf{h}$ from (66). In the same way, $\mathbf{F}_{k,m}$ is a diagonal matrix whose diagonal elements are equal to $2\mathbf{e}_1^T \mathbf{e}_1 - \mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 - \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1 = 2$ since $m \neq 0$ which implies that $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1 = 0$. Consequently, $\mathbf{F}_{k,m} = 2\mathbf{I}_P$ and $\text{var}(\eta_{k,m}^{(sn)}) = 2N_0 \mathbf{h}^T \mathbf{h}$ from (67). As a conclusion, (30)-(31) are satisfied for $k = 0$.

In what follows, we consider the case $k \neq 0$. In this case, $\mathbf{A}^{j-i}$ is a block matrix where the blocks on the k-th lower diagonal are equal to $\mathbf{\Omega}^m$, the blocks on the $(P-k)$-th upper diagonal are equal to $\mathbf{\Omega}^{m+1}$ while the remaining blocks are zero. Consequently, the nonzero elements of $\mathbf{E}_{k,m}$ are the diagonal elements that are equal to -1, the elements of the k-th lower diagonal that are equal to $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1$ and the elements of the $(P-k)$-th upper diagonal that are equal to $\mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1$. Similarly, the nonzero elements of $\mathbf{F}_{k,m}$ are (i): the diagonal elements that are equal to 2, (ii): the elements of the k-th lower diagonal that are equal to $-\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1$, (iii): the elements of the k-th upper diagonal that are equal to $-\mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1$, (iv): the elements of the $(P-k)$-th upper diagonal that are equal to $-\mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1$ and (v): the elements of the $(P-k)$-th lower diagonal that are equal to $-\mathbf{e}_1^T \mathbf{\Omega}^{-m-1} \mathbf{e}_1$. In the case where $k = P - k$, the elements of the k-th lower diagonal are $-\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 - \mathbf{e}_1^T \mathbf{\Omega}^{-m-1} \mathbf{e}_1$ while the elements of the k-th upper diagonal are $-\mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1 - \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1$. For $k \neq 0$, we need to distinguish between the following three cases.

Case 1: $m \neq 0$ and $m \neq M - 1$. In this case, $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m-1} \mathbf{e}_1 = 0$ since $\mathbf{\Omega}^m$ and $\mathbf{\Omega}^{m+1}$ are different from the identity matrix $\mathbf{I}_M$. Consequently, $\mathbf{E}_{k,m} = -\mathbf{I}_P$ and $\mathbf{F}_{k,m} = 2\mathbf{I}_P$ and (66)-(67) take the same values as in the case $k = 0$ completing the proof of (30)-(31) in this case.

Case 2: $m = 0$. In this case, $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1 = 1$ while $\mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m-1} \mathbf{e}_1 = 0$. Consequently, $\mathbf{E}_{k,m} = -\mathbf{I}_P + \mathbf{L}_k$ and $\mathbf{F}_{k,m} = 2\mathbf{I}_P - \mathbf{L}_k - \mathbf{U}_k$ where $\mathbf{L}_k$ (resp. $\mathbf{U}_k$) stands for the matrix whose elements are all zero except for the elements on the k-th lower (resp. upper) diagonal. Therefore, (66) simplifies to $\eta_{k,m}^{(ss)} = -\mathbf{h}^T \mathbf{h} + \sum_{l=1}^{QL} \mathbf{h}_l^T \mathbf{L}_k \mathbf{h}_l = -\mathbf{h}^T \mathbf{h} + \sum_{l=1}^{QL} \sum_{p=1}^{P-k} h_{l,p} h_{l,p+k}$ where $h_{l,p}$ stands for the p-th element of $\mathbf{h}_l$. Defining $R_l(k) \triangleq \sum_{p=1}^{P-k} h_{l,p} h_{l,p+k}$, then this term corresponds to the sum of the elements on the k-th upper (or lower) diagonal of the symmetrical matrix $\mathbf{h}_l \mathbf{h}_l^T$. Consequently, $\eta_{k,m}^{(ss)} = -\mathbf{h}^T \mathbf{h} + R(k)$ where $R(k) \triangleq \sum_{l=1}^{QL} R_l(k)$. Similarly, (67) simplifies to $\text{var}(\eta_{k,m}^{(sn)}) = N_0(2\mathbf{h}^T \mathbf{h} - R(k) - R(k)) = 2N_0(\mathbf{h}^T \mathbf{h} - R(k))$ completing the proof of (30)-(31).

Case 3: $m = M - 1$. In this case, $\mathbf{e}_1^T \mathbf{\Omega}^{m+1} \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m-1} \mathbf{e}_1 = 1$ while $\mathbf{e}_1^T \mathbf{\Omega}^m \mathbf{e}_1 = \mathbf{e}_1^T \mathbf{\Omega}^{-m} \mathbf{e}_1 = 0$. Consequently, $\mathbf{E}_{k,m} = -\mathbf{I}_P + \mathbf{L}_{P-k}$ and $\mathbf{F}_{k,m} = 2\mathbf{I}_P - \mathbf{L}_{P-k} - \mathbf{U}_{P-k}$. Therefore, in a way similar to case 2, $\eta_{k,m}^{(ss)} = -\mathbf{h}^T \mathbf{h} + R(P-k)$ and $\text{var}(\eta_{k,m}^{(sn)}) = 2N_0(\mathbf{h}^T \mathbf{h} - R(P-k))$ completing the proof of (30)-(31).

References

[1] J. Choi and W. Stark, "Performance of ultra-wideband communications with suboptimal receivers in multipath channels," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 9, pp. 1754–1766, December 2002.

[2] T. Quek and M. Win, "Analysis of UWB transmitted-reference communication systems in dense multipath channels," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 9, pp. 1863 – 1874, September 2005.

[3] Y. Chao and R. Scholtz, "Ultra-wideband transmitted reference systems," *IEEE Trans. Veh. Technol.*, vol. 54, pp. 1556 – 1569, September 2005.

[4] M. Sahin, I. Guvenc, and H. Arslan, "Optimization of energy detector receivers for UWB systems," in *Proceedings IEEE Vehicular Technology Conference*, vol. 2, 2005, pp. 1386 – 1390.

[5] C. Carbonelli and U. Mengali, "M-PPM noncoherent receivers for UWB applications," *IEEE Trans. Wireless Commun.*, vol. 5, no. 8, pp. 2285–2294, August 2006.

[6] A. A. D'Amico, U. Mengali, and E. A. de Reyna, "Energy-detection UWB receivers with multiple energy measurements," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2652–2659, July 2007.

[7] F. Wang, Z. Tian, and B. M. Sadler, "Weighted energy-detection for noncoherent ultra-wideband receiver design," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 710–720, February 2011.

[8] Y. Chao and R. Scholtz, "Optimal and suboptimal receivers for ultra-wideband transmitted reference systems," in *Proceedings IEEE Globecom*, vol. 6, December 2003, pp. 759–763.

[9] G. Durisi and S. Benedetto, "Performance of coherent and non-coherent receivers for UWB communications," in *Proceedings IEEE International Conference on Communications*, vol. 6, June 2004, pp. 3429–3433.

[10] K. Witrisal, G. Leus, M. Pausini, and C. Krall, "Equivalent system model and equalization of differential impulse radio UWB systems," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 9, pp. 1851–1862, September 2005.

[11] Q. Zhou and X. Ma, "Receiver designs for differential UWB systems with multiple access interference," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 126–134, January 2014.

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

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

[14] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1485–1503, June 2002.

[15] F. Oggier, "Cyclic algebras for noncoherent differential space-time coding," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3053–3065, September 2007.

[16] I. Kammoun and J.-C. Belfiore, "A new family of Grassmann space-time codes for non-coherent MIMO systems," *IEEE Commun. Lett.*, vol. 7, pp. 528–530, November 2003.

[17] X. Liang and X. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: parametric codes, optimal designs, and bounds," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2291 – 2322, August 2002.

[18] D. Smith and L. Hanlen, "New group product differential unitary space-time codes with simplified design and detection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4825 – 4830, December 2008.

[19] M. Hajiaghayi and C. Tellambura, "Unitary signal constellations for differential space-time modulation," *IEEE Commun. Lett.*, vol. 11, no. 1, pp. 25 – 27, January 2007.

[20] M. Bhatnagar, A. Hjorungnes, and L. Song, "Differential coding for non-orthogonal space-time block codes with non-unitary constellations over arbitrarily correlated Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3985 – 3995, August 2009.

[21] Q. Zhang and C. Ng, "Differential space-time coded impulse radio systems using MIMO autocorrelation receivers in UWB channel," in *Proceedings IEEE Conference on UWB*, September 2006, pp. 441 – 446.

[22] C. Abou-Rjeily, N. Daniele, and J.-C. Belfiore, “Differential space-time ultra-wideband communications,” in *Proceedings IEEE Int. Conf. on Ultra-Wideband*, September 2005, pp. 248–253.

[23] L. Yang and G. B. Giannakis, “Analog space-time coding for multi-antenna ultra-wideband transmissions,” *IEEE Trans. Commun.*, vol. 52, pp. 507–517, March 2004.

[24] V. Tarokh and H. Jafarkhani, “A differential detection scheme for transmit diversity,” *IEEE J. Sel. Areas Commun.*, vol. 18, no. 7, pp. 1169–1174, July 2000.

[25] C. Abou-Rjeily, “Permutation-based noncoherent space-time codes with analog energy detection for IR-UWB communications with PPM,” *IEEE Trans. Wireless Commun.*, submitted for publication.

[26] J. Foerster, “Channel modeling sub-committee Report Final,” Technical report IEEE 802.15-02/490, IEEE 802.15.3a WPANs, 2002.

[27] D. Cassioli, M. Z. Win, F.Vatalaro, and A. F. Molisch, “Performance of low-complexity rake reception in a realistic UWB channel,” in *Proceedings IEEE Int. Conf. on Commun.*, May 2002, pp. 763–767.

[28] C. Abou-Rjeily and W. Fawaz, “Space-time codes for MIMO ultra-wideband communications and MIMO free-space optical communications with PPM,” *IEEE J. Sel. Areas Commun.*, vol. 26, no. 6, pp. 938–947, August 2008.

[29] V. Tarokh, N. Seshadri, and A. Calderbank, “Space-time codes for high data rate wireless communication : Performance criterion and code construction,” *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, March 1998.

[30] F. Oggier and B. Hassibi, “Algebraic Cayley differential space-time codes,” *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1911–1919, May 2007.

[31] J. Kunisch and J. Pamp, “An ultra-wideband space-variant multipath indoor radio channel model,” in *Proceedings IEEE Conf. on UWB Systems and Technologies*, November 2003, pp. 290 – 294.