

Signal Space Diversity Techniques with Fast Decoding Based on MDS Codes

Yue Shang, *Member, IEEE*, Dong Wang, *Member, IEEE*, and Xiang-Gen Xia, *Fellow, IEEE*

Abstract—In wireless communication systems, signal space diversity techniques are usually adopted to combat channel fading by exploiting time diversity, frequency diversity, spatial diversity or a combination of them. Most existing schemes to achieve signal space diversity are based on linear constellation spreading. In this paper, we propose a novel nonlinear signal space diversity technique based on maximum distance separable (MDS) codes. The new technique provides a design flexibility for almost any number of diversity channels and desired diversity orders. We also propose a simple and suboptimal diversity channel selection (DCS) decoding for our new scheme. DCS decoding can greatly reduce the decoding complexity at a cost of marginal performance loss relative to the optimal detection while keeping the diversity order. Simulation results show that with the same throughput but a lower decoding and implementation complexity, our scheme can have superior performance than the optimal linear spreading schemes over either independent fading or additive white Gaussian noise (AWGN) channels.

Index Terms—Coding gain, diversity order, Euclidean distance, frequency diversity, signal space diversity, Latin square, MDS codes, modulation diversity, OFDM, product distance, spatial diversity, time diversity.

I. INTRODUCTION

IN wireless communication systems, signal space diversity or modulation diversity [1]-[3] is usually adopted to counteract channel fading. For signal space diversity, a fixed number of information bits are mapped to a multidimensional signal constellation, i.e., a vector of symbols, at transmitter side and consequently, multiple copies of each bit are sent over multiple diversity channels to achieve diversity gains as well as coding gains. This technique can be utilized to exploit, for instance, time diversity in a fast fading channel, frequency diversity in an orthogonal frequency-division multiplexing (OFDM) system [4]-[7] operating over a multipath channel, or spatial diversity via a diagonal space-time block code (STBC) [8]-[15] in a multi-input multi-output (MIMO) channel. The diversity order and coding gain are the minimum Hamming distance and the minimum product distance between any two coordinate vectors of constellation points, respectively.

Most existing methods to achieve signal space diversity are based on linear constellation spreading or rotation, see [1]-

[16], for example. To be specific, the information bits are first sequentially mapped to multiple symbols in a regular constellation which are subsequently rotated/multiplied by a square spreading matrix. The resulting rotated symbols are transmitted over multiple diversity channels. Other than the linear spreading technique, a nonlinear design from exhaustive search called multi-QAM modulation was proposed in [17] to achieve full diversity, where the information bits are directly modulated over a multidimensional QAM constellation. For almost all the known schemes, the diversity gain is achieved at the price of an exponentially increased maximum-likelihood (ML) decoding complexity. Although some simplified detection methods such as zero-forcing (ZF) or minimum mean square error (MMSE) equalizer are feasible, they will suffer a significant diversity loss [7].

In this paper, we propose a novel *nonlinear* signal space diversity technique based on maximum distance separable (MDS) codes. It is known that a code is called MDS if it achieves the Singleton bound [18] and hence maximizes the minimum distance among codeword pairs. The idea underlying the new design is totally different from the linear constellation rotation method, providing the design flexibility for almost any number of diversity channels and desired diversity orders as well as possessing a simple and suboptimal *diversity channel selection (DCS)* decoding that we propose later. Specifically, unlike the traditional linear spreading designs that are over the complex field, our proposed method is over the binary field, characterized by a MDS code and the constellation labelling. Our design is flexible in the sense that it can achieve any diversity order between one (no diversity) and the number of diversity channels (full diversity). Note that a higher diversity order usually requires a larger constellation, and our scheme always has all the modulated/rotated symbols on a smallest possible regular constellation so that the average transmit powers for all the diversity channels keep the same. With such flexibility, it is possible to design a partial diversity scheme with a reasonably small constellation in order to ease the practical implementation. At the receiver side, the DCS decoding can greatly reduce the decoding complexity at a cost of marginal performance loss relative to the optimal ML detection while keeping the diversity order. Besides presenting the systematic design idea above, we also provide some design examples for three and four diversity channels. Simulation results show that with the same throughput but a lower decoding and implementation complexity, our scheme, thanks to their nonlinear feature, can have superior performance than the optimal linear constellation spreading schemes over either independent fading or additive white Gaussian noise (AWGN) channels.

The rest of this paper is organized as follows. In Section

Paper approved by E. Ayanoglu, the Editor for Communication Theory and Coding Applications of the IEEE Communications Society. Manuscript received September 18, 2009; revised January 16, 2010.

Y. Shang is with the Signal Processing and Communications Group, MathWorks, Natick, MA 01760 USA (e-mail: yue.shang@mathworks.com).

D. Wang is with Philips Research North America, Briarcliff Manor, NY 10510 USA (e-mail: dong.wang@philips.com).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu).

X.-G. Xia's work was supported in part by the World Class University (WCU) Program 2008-000-20014-0, National Research Foundation, Korea, and the Air Force Office of Scientific Research (AFOSR) under Grant No. FA9550-08-1-0219.

Digital Object Identifier 10.1109/TCOMM.2010.09.090569

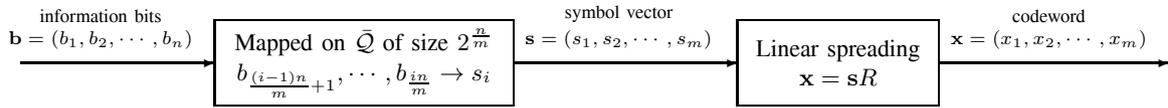


Fig. 1. Encoding of a linear spreading/rotation scheme.

II, we briefly review signal space diversity notation and the existing linear spreading schemes. In Section III, the general construction for our novel MDS code based technique and the associated suboptimal DCS decoding are proposed. In Section IV, we in particular investigate our design for 3 and 4 diversity channels to achieve diversity order of 2 and 3, respectively, in order to illustrate the advantages of our nonlinear construction method. We call the designs as triple-channel joint modulation (TCJM) and quaternary-channel joint modulation (QCJM), respectively. Simulation results are provided in Section V to show the superior performance of TCJM and QCJM over some optimal linear constellation rotation schemes. Finally, in Section VI, we conclude this paper.

II. PROBLEM FORMULATION AND LINEAR SPREADING SCHEMES

It is assumed that there are m independent diversity channels that totally carry n bits per channel use. So, the code \mathcal{X} under consideration for the signal space diversity specifies a one-to-one correspondence (mapping) between the n -length bit sequence $\mathbf{b} = (b_1, b_2, \dots, b_n)$ and the m -length codeword $\mathbf{x} = (x_1, x_2, \dots, x_m)$, i.e.,

$$\mathcal{X} = \{\mathbf{x} | \mathbf{x} = f(\mathbf{b}), \mathbf{b} \in \{0, 1\}^n\} \quad (1)$$

that contains 2^n codewords, where $f(\cdot)$ is a one-to-one mapping. In general, the component x_i of \mathbf{x} belongs to a regular constellation or its rotation and is transmitted over the i th diversity channel, $1 \leq i \leq m$. To achieve a diversity order of d , $1 \leq d \leq m$, any two distinct codewords of \mathcal{X} must have at least d symbols in difference, i.e., $d = \min_{\mathbf{x}_1 \neq \mathbf{x}_2 \in \mathcal{X}} w(\mathbf{x}_1 - \mathbf{x}_2)$, where $w(\cdot)$ denotes the Hamming weight of a vector.

Let us briefly review how a usual linear constellation spreading scheme works to achieve a nontrivial diversity order. In general, m divides n for such schemes. Given a regular constellation \bar{Q} of size $2^{\frac{n}{m}}$, the bit sequence \mathbf{b} is mapped to a symbol vector $\mathbf{s} = (s_1, s_2, \dots, s_m)$, where $s_i \in \bar{Q}$ is from the $\frac{n}{m}$ bits $b_{\frac{(i-1)n}{m}+1}, b_{\frac{(i-1)n}{m}+2}, \dots, b_{i\frac{n}{m}}$ in accordance with the labelling of \bar{Q} , $1 \leq i \leq m$. After that, the codeword $\mathbf{x} \in \mathcal{X}$ corresponding to \mathbf{b} is obtained from \mathbf{s} and a preassigned $m \times m$ constant spreading/rotation matrix R by

$$\mathbf{x} = \mathbf{s}R. \quad (2)$$

In Fig. 1, the linear spreading encoding described above is illustrated by a flow chart.

Two earlier spreading matrices are Hadamard and Fourier matrices [4] that, however, usually cannot achieve any diversity gain except for some special cases, while being able to be implemented by fast Hadamard transform (FHT) and fast Fourier transform (FFT), respectively. To improve them so that

full diversity is exploited, the rotated Hadamard and Fourier spreadings were proposed in, for example, [5], [6]. In [16], the diversity distribution for a Hadamard-like random spreading matrix is derived analytically. Vandermonde matrices, as spreading matrices, were also studied and the optimization designs were found when the number of diversity channels is a power of 2 [28]. In [9]-[15], spreading matrices were designed by lattice-based algebraic methods and the optimal matrix

$$R_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{j\frac{\pi}{6}} \\ 1 & e^{j\frac{5\pi}{6}} \end{pmatrix} \quad (3)$$

for 2 diversity channels was found in [14].

A unitary R in (2) is highly preferred to guarantee the same average transmit power for all the diversity channels and some efforts have been made to optimize such R for different m and various \bar{Q} in, for instance, [3], [7], [8]. In particular, when $m = 2$, the optimal unitary spreading matrix for BPSK modulations has been found in [8]. For $m > 2$, a usual method is to decompose a unitary matrix into the product of a series of (complex) Givens rotations and then make exhaustive computer search over discrete rotation angle values in order to either maximize coding gains [3], [8] or minimize the asymptotic union bound for the symbol error rate (SER) [7]. However, the complexity for such an overall search is prohibitively high and there are no optimal spreading matrices claimed in the literature yet. A fact for all the unitary linear rotation schemes is that they have exactly the same performance as the plain nonrotated scheme over an AWGN channel.

For linear constellation spreading schemes, an ML receiver is often necessary to exploit the designed nontrivial diversity order. Other simplified decoders exist, but often sacrifice the diversity order to reduce the complexity [7]. Also, the \mathbf{x} in (2) usually has its components (the rotated symbols) on an irregular large constellation on the complex plane, which is undesirable from an implementation point of view.

III. MDS CODES BASED SIGNAL SPACE DIVERSITY TECHNIQUE

For our signal space diversity scheme, all the symbols in the codeword \mathbf{x} in (1) are from a given q point constellation \bar{Q} with unit average energy, where q is a power of 2. So, we also call our scheme as *joint modulation* that modulates n information bits to m symbols on a fixed constellation. If we view the q points of \bar{Q} as the elements of a q -ary field, it is not difficult to see that the \mathcal{X} in (1) with diversity order d is equivalent to a q -ary $(m, 2^n, d)$ code. In practice, we always want q as small as possible for fixed m, n and d in order to optimize performance and ease the algorithm implementation. According to the Singleton bound [18], we have

$$2^n \leq q^{m-d+1} \Rightarrow q \geq 2^{\lceil \frac{n}{m-d+1} \rceil}, \quad (4)$$

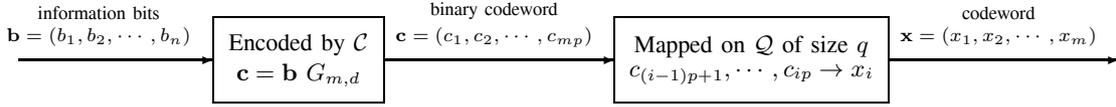


Fig. 2. Encoding of MDS code \mathcal{X} with diversity order (minimum Hamming distance) d .

where $\lceil \cdot \rceil$ denotes the ceiling function. When $m-d+1$ divides n , \mathcal{Q} has size $q = 2^{\frac{n}{m-d+1}}$ and the bound in (4) is achieved. At this time, \mathcal{X} is an MDS code of length m . If $(m-d+1) \nmid n$, on the other hand, q is set to $2^{\lceil \frac{n}{m-d+1} \rceil}$ and it suffices for us to construct a q -ary (m, q^{m-d+1}, d) MDS code from which 2^n codewords are picked to consist \mathcal{X} . Therefore, without loss of generality, we assume $(m-d+1)|n$ in the subsequent discussions unless otherwise specified and define

$$p \triangleq \frac{n}{m-d+1}. \quad (5)$$

So, $q = 2^p$, i.e., every p bits are mapped to a constellation point of \mathcal{Q} . Note that in general, p cannot be very large, no larger than 8 for example, for a real system. In what follows, we neglect the trivial case of $d = 1$.

We would like to mention that designing a q -ary (m, q^{m-d+1}, d) MDS code is equivalent to constructing a set of $d-1$ mutually orthogonal $(m-d+1)$ -dimensional Latin hypercubes of order q . Different Latin hypercube constructions as well as the mapping from the q -ary field to the constellation \mathcal{Q} usually result in different designs and performance. How to optimize the Latin hypercube based designs over a q -ary field could be difficult. Instead, our systematic method is over the binary field to design the generator matrix of a binary linear code, as explained in this and subsequent sections.

A. General Construction

There exist many classical constructions for MDS codes in, for example, [18], [29], [30] and some of them such as BCH codes are well known. Our construction for the q -ary $(m, 2^n, d)$ MDS code to be described below is based on a binary linear code as well as the labelling of \mathcal{Q} , and different from most existing ones. Specifically, given any labelling of \mathcal{Q} that determines the one-to-one mapping between its q symbols or, equivalently, the elements of the q -ary field and p bits, the MDS code \mathcal{X} is constructed as follows. First, we design a $[mp, n, \bar{d}]$ binary linear code \mathcal{C} whose standard form generator matrix is

$$G_{m,d} = (I_n | A), \quad (6)$$

where \bar{d} is the minimum Hamming distance of \mathcal{C} but unnecessary to specify, I_n is the identity matrix of dimension n and A is a $n \times p(d-1)$ binary matrix. We express the A in (6) as the following partitioned form

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,d-1} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,d-1} \\ \cdots & \cdots & \vdots & \cdots \\ A_{m-d+1,1} & A_{m-d+1,2} & \cdots & A_{m-d+1,d-1} \end{pmatrix} \quad (7)$$

with $A_{i,j}$ being a $p \times p$ submatrix of A , $1 \leq i \leq m-d+1$, $1 \leq j \leq d-1$. To encode a n -length bit sequence \mathbf{b} to a m -length

codeword \mathbf{x} of \mathcal{X} in (1), we begin with encoding \mathbf{b} to a mp -length codeword $\mathbf{c} = (c_1, c_2, \dots, c_{mp}) = \mathbf{b} G_{m,d}$ of \mathcal{C} . Then, the p bits $c_{(i-1)p+1}, c_{(i-1)p+2}, \dots, c_{ip}$ of \mathbf{c} is mapped to the i th symbol x_i of \mathbf{x} in accordance with the labelling of \mathcal{Q} , $1 \leq i \leq m$. The above encoding procedure from \mathbf{b} to \mathbf{x} is illustrated in Fig. 2 by a flow chart. Note that the resulting code \mathcal{X} is generally nonlinear on the q -ary field, which makes our method distinct from most existing designs for MDS codes.

Comparing Fig. 1 and Fig. 2, we can see that the encoding methods for our scheme and the linear spreading scheme are fairly different. For the conventional spreading technique, information redundancy is added into \mathbf{x} at the second step by spreading each symbol s_i over multiple diversity channels via a matrix multiplication. For our scheme, on the other hand, information is initially protected at the bit level by a binary linear code. Both the methods cannot guarantee the optimality of the resulting code \mathcal{X} (the overall optimality of the mapping f in (1)), but are feasible from the design and implementation aspects. An effort to directly find the optimal mapping f has been made in [17] by an exhaustive search.

Following the above encoding procedure, we can obtain a q -ary $(m, 2^n)$ code \mathcal{X} that is fully determined by the matrix $G_{m,d}$ in (6) and the labelling of \mathcal{Q} . In more details, x_i is decided by the $((i-1)p+1)$ th to (ip) th columns of $G_{m,d}$ as well as \mathcal{Q} , $1 \leq i \leq m$. However, the resulting code may not have the minimum Hamming distance or diversity order d ; that is, it may not be an MDS code. Remind that the maximum possible diversity order for \mathcal{X} is d due to the Singleton bound in (4). In the following theorem, a sufficient and necessary condition for \mathcal{X} to achieve this diversity order bound is provided.

Theorem 1: The \mathcal{X} constructed above is a q -ary $(m, 2^n, d)$ MDS code if and only if the square matrix

$$\begin{pmatrix} A_{i_1, j_1} & A_{i_1, j_2} & \cdots & A_{i_1, j_k} \\ A_{i_2, j_1} & A_{i_2, j_2} & \cdots & A_{i_2, j_k} \\ \cdots & \cdots & \vdots & \cdots \\ A_{i_k, j_1} & A_{i_k, j_2} & \cdots & A_{i_k, j_k} \end{pmatrix} \quad (8)$$

is of full rank for any $1 \leq k \leq \min\{m-d+1, d-1\}$, $1 \leq i_1 < i_2 < \dots < i_k \leq m-d+1$ and $1 \leq j_1 < j_2 < \dots < j_k \leq d-1$, where $A_{i,j}$ is defined in (7).

The proof of Theorem 1 is in Appendix A. What this theorem claimed is that for \mathcal{X} to be an MDS code, all the square matrices that are consisted of the partitions $A_{i,j}$ of A have to be full-rank. The requirement reduces to the full rankness of $A_{i,j}$ when $d = 2$ or $d = m$. Note that full-rank binary matrix set has been also used to construct space-time codes with some optimal properties [19]-[21].

Remark 1: A matrix A meeting the condition in Theorem 1 may not exist for certain m, n and d . For instance, if $m = 7$, $n = 10$ and $d = 3$, we have $p = 2$ from (5) and A is of

size 10×4 that is specified by 10 many 2×2 submatrices $A_{i,j}$, $1 \leq i \leq 5$, $1 \leq j \leq 2$, as in (7). Assume the condition in Theorem 1 is satisfied by A , then all its 10 rows must be different and have at least one 1 among their first two and also last two bits. This is because $A_{i,j}$ as well as matrix

$$\begin{pmatrix} A_{i_1,1} & A_{i_1,2} \\ A_{i_2,1} & A_{i_2,2} \end{pmatrix}, 1 \leq i_1 < i_2 \leq 5,$$

must be full-rank. However, it can be easily calculated that there are totally 9 such binary vectors of length 4 and hence a contradiction results. In general, one can easily show that a necessary condition for the existence of a matrix A meeting the requirement in Theorem 1 is that both $(q-1)^{d-1} \geq n$ and $(q-1)^{m-d+1} \geq p(d-1)$ (when $d \neq m$) hold.

Usually, the construction of a matrix A in (6) with Theorem 1 satisfied is not trivial except for $d = 2$ or $d = m$. On the other hand, even if such an A is found, the resulting MDS code \mathcal{X} does not always lead to good performance. Over independent fading diversity channels, the performance of \mathcal{X} is dominated by its codeword pairs with Hamming distance d [5], [8]. The minimum product distance or coding gain of \mathcal{X} is the metric

$$\zeta_{\mathcal{X}} = \min_{w(\Delta \mathbf{x})=d} \prod_{\substack{\Delta x_i \neq 0 \\ 1 \leq i \leq m}} |\Delta x_i|, \quad (9)$$

defined over these pairs, where $\Delta \mathbf{x} = (\Delta x_1, \Delta x_2, \dots, \Delta x_m)$ denotes the difference of two codewords.

As a result, except for finding a matrix A guided by Theorem 1 that is irrespective of \mathcal{Q} , we want to jointly optimize the design of A as well as the labelling of \mathcal{Q} to make $\zeta_{\mathcal{X}}$ as large as possible. Our method to do this will be clear until the next section where we study two design examples. Intuitively, we always expect a matrix A such that the code \mathcal{X} has a small number of codeword pairs with the minimum Hamming distance d . However, as the following corollary claims, this number is actually not affected by the choice of A . The proof of Corollary 1 is in Appendix B.

Corollary 1: For the constructed $(m, 2^n, d)$ MDS code \mathcal{X} , the number of its codeword pairs with the minimum Hamming distance d is independent of the choice of the matrix A in (7).

In summary, for given information bit number n and diversity channel number m , our signal space diversity scheme utilizes the *minimum* constellation size $q = 2^{\lceil \frac{n}{m-d+1} \rceil}$ to achieve a desired diversity order d . The larger the d , the larger the q and hence the higher the implementation complexity. So, in practice, how large the d needs to be depends on not only the performance requirement but also the complexity and resolution the system can tolerate. The ML detection complexity for our construction is $\mathcal{O}(2^n)$, the same as a linear spreading scheme. In Section III-B, we propose a suboptimal DCS decoding method that, while keeping the diversity order, can greatly reduce the decoding complexity at a cost of marginal performance loss. This is another important advantage of our scheme over the traditional schemes.

B. Suboptimal Diversity Channel Selection (DCS) Decoding

The m symbols in each codeword \mathbf{x} are transmitted over m independent diversity channels and the receive signal-to-noise ratio (SNR) for each channel depends on its realization. For

DCS decoding, the receiver first selects the best r channels $1 \leq l_1 < l_2 < \dots < l_r \leq m$ among all the m channels in terms of their receive SNR, $1 \leq r \leq m - d + 1$. The symbols $x_{l_1}, x_{l_2}, \dots, x_{l_r}$ conveyed on the r selected channels are decoded to $\hat{x}_{l_1}, \hat{x}_{l_2}, \dots, \hat{x}_{l_r} \in \mathcal{Q}$ by hard decision in accordance with \mathcal{Q} . After that, the detection of \mathbf{x} is made by a minimum Euclidean distance search among all the codewords of \mathcal{X} that are specified by the r decoded components, i.e., over the set

$$\mathcal{X}_{\mathcal{D}}^r = \{\mathbf{x} = (x_1, x_2, \dots, x_m) \in \mathcal{X} | x_{l_t} = \hat{x}_{l_t}, 1 \leq t \leq r\}. \quad (10)$$

Lemma 1: For any given r symbols $s_1, s_2, \dots, s_r \in \mathcal{Q}$, $1 \leq r \leq m - d + 1$, and $1 \leq l_1 < l_2 < \dots < l_r \leq m$, we have

$$|\{\mathbf{x} = (x_1, x_2, \dots, x_m) \in \mathcal{X} | x_{l_t} = s_t, 1 \leq t \leq r\}| = q^{m-d-r+1} \quad (11)$$

if \mathcal{X} satisfies the criterion in Theorem 1.

The proof of Lemma 1 is not hard by following the similar arguments as in the proofs of Theorem 1 and Corollary 1 and hence omitted. According to (11), the proposed DCS decoding has a complexity of

$$\mathcal{O}(rq + q^{m-d-r+1}), \quad (12)$$

which exponentially decreases as r increases from 0 to $m - d + 1$. At the extreme case of $r = 0$, i.e., no diversity channel is first picked for hard decision, the suboptimal decoding is equivalent to the optimal ML one. When $r = m - d + 1$, on the other hand, the search process after hard decision disappears as a codeword can already be uniquely determined from the $m - d + 1$ decoded symbols. This is easily understood because any two codewords have at most $m - d$ same symbols for a code \mathcal{X} with diversity order d . Note that from (12), the complexities for $r = m - d + 1$ and $r = m - d$ are the same for a given constellation.

The idea underlying our suboptimal DCS decoding is to shrink the candidate codeword set by first decoding a part of the most trustable symbols. The reliability of such a strategy may suffer from the case that there are more than $m - r$ diversity channels in deep fade. So, performance degrades as r increases and hence decoding complexity decreases. Fortunately, when r is small, the performance loss is only marginal relative to the ML decoding. In fact, we have observed that the DCS detection performance with $r = 1$ converges to ML decoding performance as SNR increases (Section V). Furthermore, whatever r is, the proposed decoding scheme does not sacrifice the diversity gain.

Theorem 2: With the suboptimal DCS decoding at the receiver, the constructed $(m, 2^n, d)$ MDS code \mathcal{X} still has the diversity order d .

Proof: The proof is not difficult and we only provide an intuitive explanation here. The DCS decoding consists of two phases: (I) hard decision from the r best (most reliable) diversity channels; (II) joint detection over the $q^{m-d-r+1}$ codewords of $\mathcal{X}_{\mathcal{D}}^r$ in (10). One can easily show that the detection performance for Phase I possesses a diversity order $m - r + 1$ by applying certain results of order statistics [22]. Furthermore, since $\mathcal{X}_{\mathcal{D}}^r$ still keeps a minimum Hamming distance d , the decoding of Phase II has a diversity order d .

The performance of DCS detection is dominated by the worse one of the two phases and therefore achieves a diversity order of $\min\{m - r + 1, d\} = d$ as $1 \leq r \leq m - d + 1$. ■

The result of Theorem 2 is not surprising by recognizing the similarity of DCS detection and antenna selection techniques for MIMO systems [22]-[26]. The above theories and speculation about DCS decoding performance will be verified by simulations in Section V.

IV. TRIPLE-CHANNEL AND QUATERNARY-CHANNEL JOINT MODULATIONS

In this section, we study two design examples for $m = 3$ and $m = 4$ diversity channels to further illustrate our construction and its advantages over the other existing techniques. We restrict to $n = 12$ for $m = 3$ and $n = 8$ for $m = 4$, i.e., each diversity channel carries 4 and 2 information bits in average per channel use, respectively. For both the cases, the required diversity order is $d = m - 1$. We call the two schemes as triple-channel joint modulation (TCJM) and quaternary-channel joint modulation (QCJM), denoted by \mathcal{M}_3 and \mathcal{M}_4 , respectively.

A. Triple-Channel Joint Modulation (TCJM)

According to (5), the constellation \mathcal{Q} has size $q = 2^6 = 64$ for $m = 3$, $n = 12$ and $d = 2$. Below we restrict \mathcal{Q} to be a QAM constellation but the method also applies to any other constellations such as PAM and PSK, etc. What we need to do now is to design a 64-ary $(3, 2^{12}, 2)$ MDS code \mathcal{M}_3 by the method introduced in Section III. We would like to mention that such a construction is equivalent to picking up a 64×64 Latin square over the 64-ary field [30], but we would not discuss many details about Latin squares. For \mathcal{M}_3 , the binary generator matrix in (6) is a 12×18 matrix

$$G_{3,2} = \left(I_{12} \mid A \right) = \left(\begin{array}{cc|cc} I_6 & 0 & A_{1,1} & \\ 0 & I_6 & A_{2,1} & \end{array} \right), \quad (13)$$

where 0 denotes an all-zero matrix of suitable dimension. From Theorem 1, the 6×6 matrices $A_{1,1}$ and $A_{1,2}$ in (13) must be full-rank to guarantee a diversity order of 2 for \mathcal{M}_3 .

The simplest way to design $A_{1,1}$ and $A_{2,1}$ is to set both of them to be an identity matrix, i.e.,

$$A_{1,1} = A_{2,1} = I_6, \quad (14)$$

and we use \mathcal{M}_3^α denote the resulting TCJM scheme. In this case, however, we have the minimum product distance (coding gain) $\zeta_{\mathcal{M}_3^\alpha} = (d_{\min}^{64})^2$ for \mathcal{M}_3^α regardless of the labelling of \mathcal{Q} , where d_{\min}^q denotes the minimum symbol distance of a q -QAM constellation with unit average energy. This result is definitely undesirable as $(d_{\min}^{64})^2$ is the minimum possible product distance for \mathcal{M}_3 only if it has diversity order 2. In fact, if we arbitrarily label \mathcal{Q} and pick a matrix A such that the condition in Theorem 1 is satisfied, the resulting \mathcal{M}_3 generally has the worst coding gain. To maximize $\zeta_{\mathcal{M}_3}$, we require a joint optimization for the A in (13) as well as the 64-QAM constellation labelling. Nevertheless, the complexity for such a problem is prohibitively high and we have to resort to other suboptimal solutions. Our method is to design A to make $\zeta_{\mathcal{M}_3}$ as large as possible under the restriction that the labelling of \mathcal{Q} is the usual *Gray mapping (labelling)*. A Gray mapping example for 64-QAM constellation is given in Fig. 3. In the

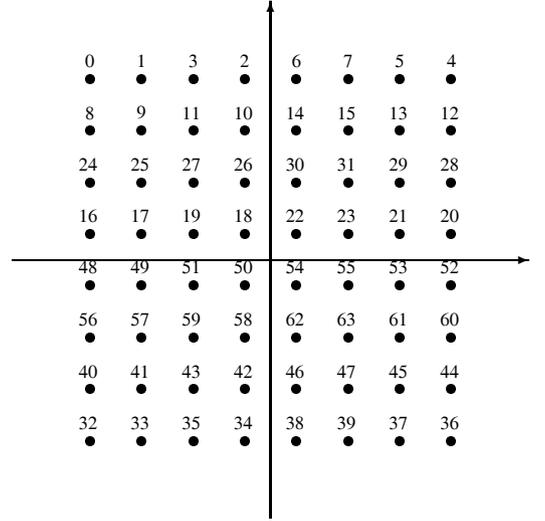


Fig. 3. 64-QAM constellation with Gray mapping, where the numbers are decimal representation (0 to 63) of 6 bits.

following theorem, we provide a sufficient condition such that $\zeta_{\mathcal{M}_3}$ is twice larger than the worst case of $(d_{\min}^{64})^2$.

Theorem 3: With a Gray labelled 64-QAM \mathcal{Q} and full-rank $A_{i,1}$, $i = 1, 2$, in (13), we have $\zeta_{\mathcal{M}_3} \geq 2(d_{\min}^{64})^2$ if the matrix $A = (A_{1,1}^T, A_{2,1}^T)^T$ in (13) satisfies the following three conditions:

- Each row of A has Hamming weight no less than 3;
- Any three rows of A are linearly independent;
- The summation of any two rows of $A_{i,1}$ has Hamming weight no less than 2, $i = 1, 2$,

where and thereafter $(\cdot)^T$ denotes the transpose of a matrix or vector.

The proof of Theorem 3 is in Appendix C, where we use the following basic facts about Gray mapping. Given a Gray labelled 2^p -QAM (q -QAM) constellation \mathcal{Q} , let $\mathbf{z}_i \in \{0, 1\}^p$ and y_i be the corresponding symbol of \mathbf{z}_i in \mathcal{Q} , $i = 1, 2$. Define $\Delta \mathbf{z} = \mathbf{z}_1 - \mathbf{z}_2$ and $\Delta y = y_1 - y_2$. Then,

$$w(\Delta \mathbf{z}) = 1 \Rightarrow |\Delta y| \geq d_{\min}^q, \quad (15a)$$

$$w(\Delta \mathbf{z}) = 2 \Rightarrow |\Delta y| \geq \sqrt{2}d_{\min}^q, \quad (15b)$$

$$w(\Delta \mathbf{z}) > 2 \Rightarrow |\Delta y| \geq \sqrt{5}d_{\min}^q. \quad (15c)$$

The advantage of Theorem 3 is to make the design of A independent of \mathcal{Q} only if the latter uses Gray mapping. It is not clear whether or not $\zeta_{\mathcal{M}_3}$ is upper bounded by $2(d_{\min}^{64})^2$, but to achieve a larger minimum product distance by the design of A seems difficult. For instance, by following the idea of Theorem 3 and utilizing the relationship between Hamming distances and symbol distances in (15), we can give the following sufficient conditions such that $\zeta_{\mathcal{M}_3} \geq \sqrt{5}(d_{\min}^{64})^2$ with a Gray labelled \mathcal{Q} :

- For the full-rank matrix $A_{i,1}$ in (13), $i = 1, 2$, any nonzero linear combination of its two rows has Hamming weight no less than 3;
- Any four rows of the matrix A in (13) are linearly independent.

However, there does not exist a 6×6 binary matrix $A_{i,1}$ such that (a) holds, as shown in Appendix D. So, the above

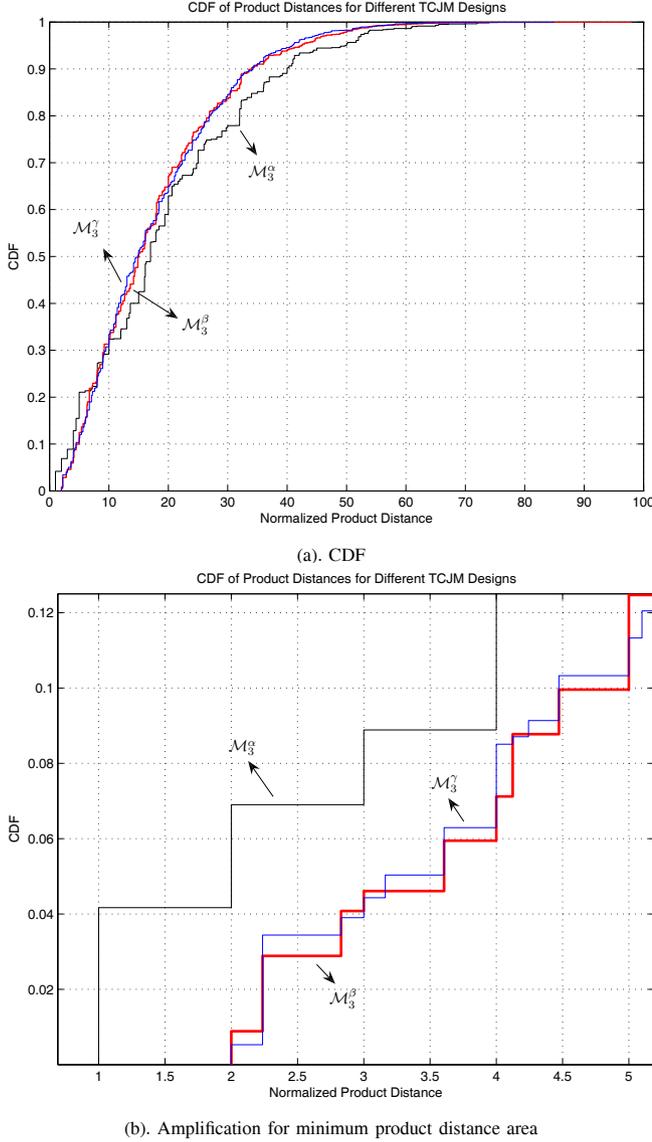


Fig. 4. Product distance CDF of \mathcal{M}_3^α , \mathcal{M}_3^β and \mathcal{M}_3^γ , where only the codeword pairs with Hamming distance 2 are taken into account and the product distances are normalized by $(d_{\min}^{64})^2$.

sufficient conditions for $\zeta_{\mathcal{M}_3} \geq \sqrt{5} (d_{\min}^{64})^2$ can never be met. In fact, to further improve $\zeta_{\mathcal{M}_3}$, we have to study the specific form of $\Delta \mathbf{z}$ as well as its relationship with $|\Delta y|$, rather than the simple inequalities in (15) that only depend on Hamming weight of $\Delta \mathbf{z}$. But in this case, designing the A in (13) will be dependent on \mathcal{Q} and become quite complicated. We conjecture that $2 (d_{\min}^{64})^2$ is already the maximum achievable $\zeta_{\mathcal{M}_3}$ by the construction method described above.

A pair of $A_{1,1}$ and $A_{2,1}$ satisfying the conditions in Theorem 3 is provided below:

$$A_{1,1} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad (16a)$$

$$A_{2,1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \quad (16b)$$

In (16), the i th column of $A_{1,1}$ is the same as the $(7-i)$ th column of $A_{2,1}$, $i = 1, 2, \dots, 6$. That is, $A_{2,1}$ is the reversed $A_{1,1}$. We denote the resulting TCJM scheme by \mathcal{M}_3^β that has coding gain $\zeta_{\mathcal{M}_3^\beta} = 2 (d_{\min}^{64})^2$. Note that the conditions of Theorem 3 are sufficient but not necessary. To see this, we give the following pair of matrices that, while violating the Theorem 3's requirements, also make $\zeta_{\mathcal{M}_3} = 2 (d_{\min}^{64})^2$ with the Gray labelled \mathcal{Q} in Fig. 3:

$$A_{1,1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad (17a)$$

$$A_{2,1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \quad (17b)$$

where $A_{2,1}$ is again the reversed $A_{1,1}$. The TCJM design by the matrix A in (17) and the 64-QAM constellation in Fig. 3 is denoted by \mathcal{M}_3^γ , where the construction of A has taken into consideration the specific Gray mapping format of the constellation. To illustrate the advantage of \mathcal{M}_3^β and \mathcal{M}_3^γ over the trivial \mathcal{M}_3^α brought by the deliberate design of the matrix A in (13), the cumulative distribution functions (CDF) of their product distances are plotted in Fig. 4, where figure (b) is the amplified figure (a) for the lower part of the CDF curves. The benefits from our designs for A can be clearly observed there.

We have studied the construction of \mathcal{M}_3 in terms of its coding gain $\zeta_{\mathcal{M}_3}$ over independent fading channels. Sometimes, the performance of \mathcal{M}_3 under AWGN channels is also of interest. For example, the diversity channels may be highly correlated since they are in the same coherent bandwidth (frequency diversity) or coherent time (time diversity). At this time, the performance metric for \mathcal{M}_3 changes to the minimum Euclidean distance

$$\xi_{\mathcal{M}_3} = \min_{\Delta \mathbf{x} \neq 0} |\Delta \mathbf{x}|. \quad (18)$$

With a trivial design for the A in (13), $A_{1,1} = A_{2,1} = I_6$ in (14) for example, we have $\xi_{\mathcal{M}_3^\alpha} = \sqrt{2} d_{\min}^{64}$ that is the worst case for $\xi_{\mathcal{M}_3}$ only if \mathcal{M}_3 is an MDS code. The following theorem reveals that a TCJM scheme designed by following Theorem 3 also achieves a large $\xi_{\mathcal{M}_3}$.

Theorem 4: With a Gray labelled 64-QAM \mathcal{Q} and full-rank $A_{i,1}$, $i = 1, 2$, in (13), we have $\xi_{\mathcal{M}_3} \geq 2d_{\min}^{64}$ if $A = (A_{1,1}^T, A_{2,1}^T)^T$ satisfies the three conditions in Theorem 3.

The proof of Theorem 4 is similar to that of Theorem 3 and hence omitted. We know from Theorem 4 that the $\xi_{\mathcal{M}_3^\beta} \geq$

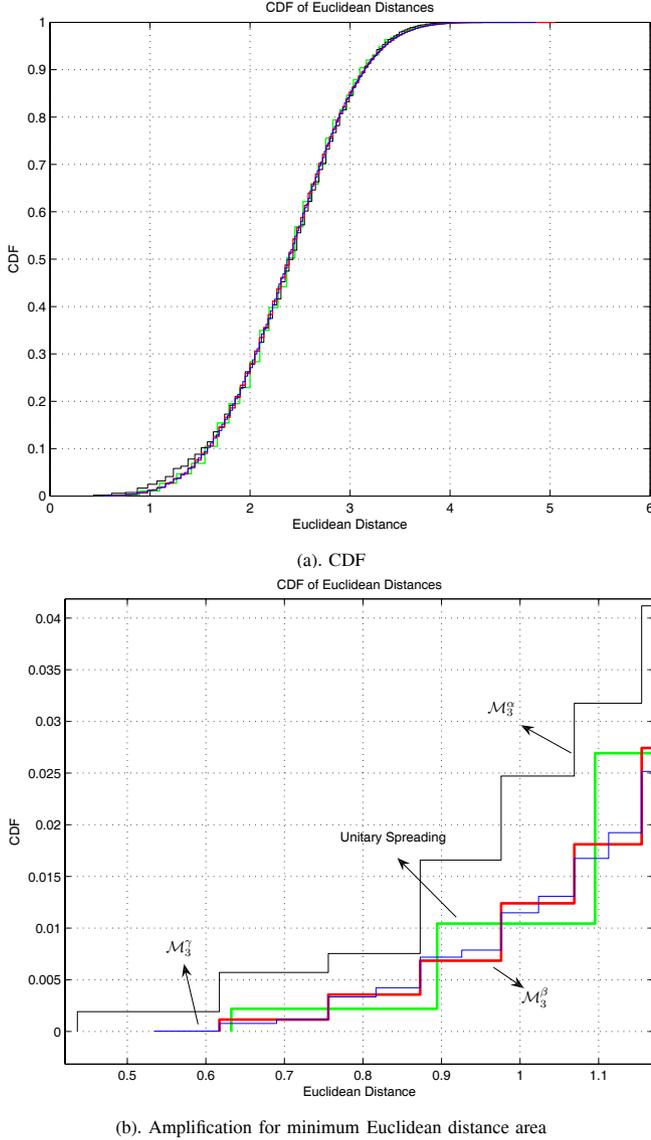


Fig. 5. Euclidean distance CDF for \mathcal{M}_3^α , \mathcal{M}_3^β , \mathcal{M}_3^γ and unitary linear constellation spreading (unspread) schemes.

$2d_{\min}^{64}$. In fact, it can be easily checked that $\xi_{\mathcal{M}_3^\beta} = 2d_{\min}^{64}$. For another matrix pair in (17), we have $\xi_{\mathcal{M}_3^\gamma} = \sqrt{3}d_{\min}^{64}$.

We would also like to compare our TCJM scheme with the conventional linear constellation rotation technique in terms of the minimum Euclidean distance. To have the same throughput as \mathcal{M}_3 , the constellation $\bar{\mathcal{Q}}$ in Fig. 1 for the spreading scheme has size $2^{\frac{n}{m}} = 16$. Let $\bar{\mathcal{Q}}$ be a 16-QAM constellation. Then, no matter what the matrix R in (2) is, the spreading scheme has its minimum Euclidean distance no larger than $d_{\min}^{16} = \sqrt{\frac{21}{5}}d_{\min}^{64}$ and the maximum value d_{\min}^{16} is achieved when R is a unitary matrix. In other words, there is no gain for spreading over AWGN channels. While our constructed TCJM can have $\xi_{\mathcal{M}_3} = 2d_{\min}^{64}$ that is still a little smaller than d_{\min}^{16} , we can design A such that \mathcal{M}_3 has a better Euclidean distance distribution than any unitary linear spreading scheme or, equivalently, the plain unspread scheme corresponding to an identity matrix R in (2). This advantage owes to the nonlinearity of our technique. To illustrate it, in Fig. 5, we plot the CDF of Euclidean distances for \mathcal{M}_3^α , \mathcal{M}_3^β and \mathcal{M}_3^γ . Also

plotted there is the CDF of Euclidean distances for a unitary rotation scheme. One can see from the amplified picture in Fig. 5(b) that our \mathcal{M}_3^β and \mathcal{M}_3^γ have fewer codeword pairs than the linear spreading scheme in the small Euclidean distance range. The superior performance of \mathcal{M}_3^β and \mathcal{M}_3^γ over AWGN channels will be shown in Section V.

To decode \mathcal{M}_3 , the ML detection has a complexity of $\mathcal{O}(2^{12})$. If the suboptimal DCS decoding is adopted at the receiver for fading diversity channels, the complexities for picking up one or two channels for hard decision (corresponding to $r = 1$ and $r = 2$ in (12)) are both $\mathcal{O}(2^7)$, a huge 2^5 times reduction relative to the ML decoding. Albeit the same complexity, selecting only the best channel to make hard decision can offer a much better performance than the other case of selecting two, as shown soon in Section V.

B. Quaternary-Channel Joint Modulation (QCJM)

For $m = 4$ diversity channels that carry $n = 8$ bits per channel use to achieve a diversity order $d = 3$, we require a 16-QAM constellation \mathcal{Q} from (4). So, the QCJM scheme is equivalent to designing a 16-ary $(4, 2^8, 3)$ MDS code \mathcal{M}_4 , or, the design of a pair of 16×16 mutually orthogonal Latin squares (MOLS) on the 16-ary field [30]. According to Theorem 1, it suffices to construct a 8×16 binary generator matrix

$$G_{4,3} = (I_8 | A) = \begin{pmatrix} I_4 & 0 & A_{1,1} & A_{1,2} \\ 0 & I_4 & A_{2,1} & A_{2,2} \end{pmatrix}, \quad (19)$$

where the 4×4 matrix $A_{i,j}$, $1 \leq i, j \leq 2$, and the 8×8 matrix A must be full-rank.

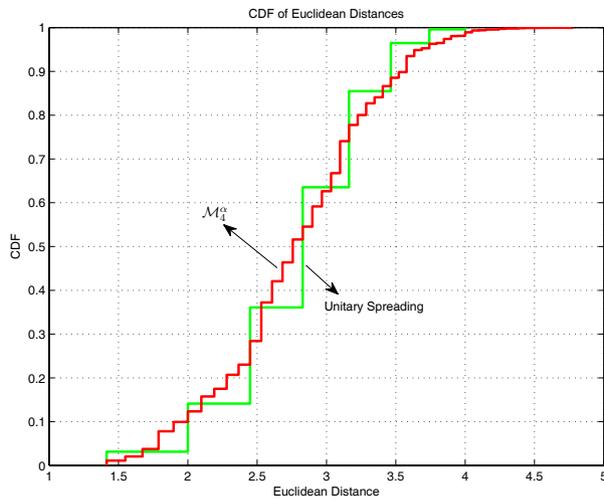
As for TCJM, \mathcal{Q} is Gray labelled for our construction of QCJM. The worst coding gain and minimum Euclidean distance for \mathcal{M}_4 are $\zeta_{\mathcal{M}_4} = (d_{\min}^{16})^3$ and $\xi_{\mathcal{M}_4} = \sqrt{3}d_{\min}^{16}$, respectively, and it is usually the case for an arbitrarily picked A in (19). Like Theorem 3 and Theorem 4, improvements of $\zeta_{\mathcal{M}_4}$ and $\xi_{\mathcal{M}_4}$ are feasible by deliberately designing the matrix A in (19).

Theorem 5: With a Gray labelled 16-QAM constellation \mathcal{Q} as well as full-rank $A_{i,j}$, $1 \leq i, j \leq 2$, and A in (19), we have $\zeta_{\mathcal{M}_4} \geq 2(d_{\min}^{16})^3$ and $\xi_{\mathcal{M}_4} \geq \sqrt{5}d_{\min}^{16}$ if A satisfies the following three conditions:

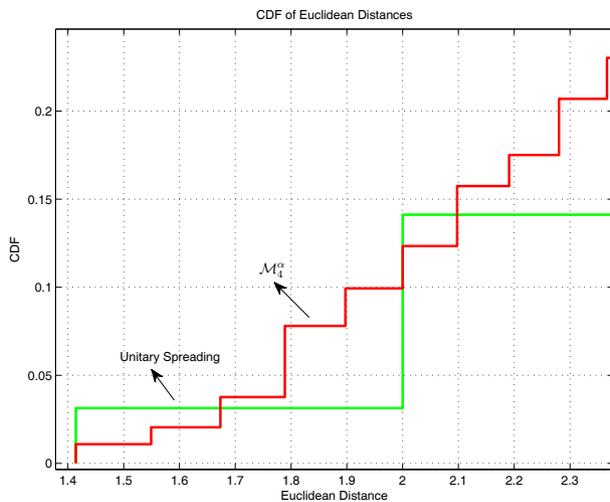
- (a). Each row of A has Hamming weight no less than 4;
- (b). The summation of any two rows of A has Hamming weight no less than 3;
- (c). The summation of any three rows of A has Hamming weight no less than 2.

Theorem 5 can be shown by following the similar arguments as in the proof of Theorem 3. The conditions in Theorem 5 as well as the Gray labelling feature of \mathcal{Q} provide us a guideline to design \mathcal{M}_4 by separating the construction of binary linear code from the specific labelling of \mathcal{Q} . While it is not clear whether or not $2(d_{\min}^{16})^3$ and $\sqrt{5}d_{\min}^{16}$ are already the upper bounds for $\zeta_{\mathcal{M}_4}$ and $\xi_{\mathcal{M}_4}$, respectively, but to further improve them is difficult. A construction for the 8×8 matrix A satisfying the requirements of Theorem 5 is given below:

$$A_{1,1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, A_{1,2} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad (20a)$$



(a). CDF



(b). Amplification for minimum Euclidean distance area

Fig. 6. Euclidean distance CDF for \mathcal{M}_4^α and unitary linear constellation spreading (unspread) schemes.

$$A_{2,1} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, A_{2,2} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \quad (20b)$$

Note that in (20), $A_{i,2}$ is obtained from $A_{i,1}$ by row permutation, $i = 1, 2$, and $A_{2,1}$ is the reversed $A_{1,2}$. We denote the resulting QCJM scheme from the matrix A in (20) by \mathcal{M}_4^α . It can be checked that $\zeta_{\mathcal{M}_4^\alpha} = 2(d_{\min}^{16})^3$ and $\xi_{\mathcal{M}_4^\alpha} = \sqrt{5}d_{\min}^{16}$.

To have the same throughput as QCJM, a linear spreading scheme needs a 4-QAM (QPSK) constellation \mathcal{Q} since each diversity channel conveys $\frac{n}{m} = 2$ information bits per channel use. So, the best minimum Euclidean distance for it is $d_{\min}^4 = \sqrt{5}d_{\min}^{16}$. Therefore, our designed \mathcal{M}_4^α does not sacrifice minimum Euclidean distance and in fact has a much better Euclidean distance distribution than any unitary rotation scheme as observed in Fig. 6, which leads to a significant performance gain as shown in the next section.

For ML detection, QCJM requires a complexity of $\mathcal{O}(2^8)$. With the suboptimal DCS decoding, on the other hand, the complexity is reduced to $\mathcal{O}(2^5)$ for both $r = 1$ and $r =$

TABLE I
DECODING COMPLEXITY PER FRAME FOR TCJM, QCJM AND TWO LINEAR SPREADING SCHEMES.

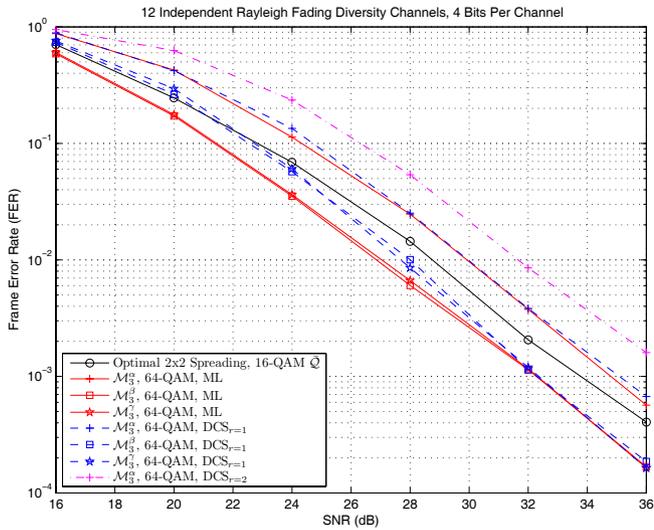
Scheme	ML	DCS _{r=1}	DCS _{r=2}
TCJM: $\mathcal{M}_3^\alpha, \mathcal{M}_3^\beta, \mathcal{M}_3^\gamma$	$\mathcal{O}(2^{14})$	$\mathcal{O}(2^9)$	$\mathcal{O}(2^9)$
2×2 Optimal Spreading	$\mathcal{O}(3 \cdot 2^9)$	/	/
QCJM: \mathcal{M}_4^α	$\mathcal{O}(3 \cdot 2^8)$	$\mathcal{O}(3 \cdot 2^5)$	$\mathcal{O}(3 \cdot 2^5)$
3×3 Vandermonde Spreading	$\mathcal{O}(2^8)$	/	/

2 in (12). Certainly, the $r = 1$ case, i.e., only the diversity channel with the least fading is selected for hard decision, is highly preferred due to its marginal performance loss and convergence to ML detection performance in the high SNR range.

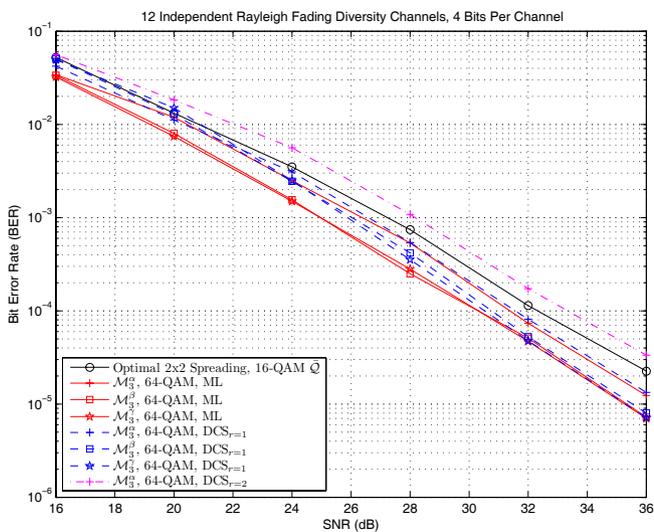
V. NUMERICAL AND SIMULATION RESULTS

In this section, we provide the simulation results for TCJM and QCJM in comparison with some known linear spreading schemes over either independent Rayleigh fading or AWGN channels. For Rayleigh fading channels, the linear rotation scheme always has a full diversity order that is the same as the diversity order of TCJM or QCJM in contrast. To have a fair comparison, we consider a frame transmission with each frame consisting of 12 fading/AWGN channels. This is because 12 is the least common multiple of 2, 3, 4 that represent the diversity order and diversity channel numbers of TCJM and QCJM. The frame error rate (FER) and bit error rate (BER) are measured for each scheme. All the schemes (TCJM, QCJM, linear spreading) use Gray labelled QAM constellation \mathcal{Q} or $\bar{\mathcal{Q}}$ and in particular, TCJM uses the 64-QAM constellation in Fig. 3.

In Fig. 7, we provide the performance of $\mathcal{M}_3^\alpha, \mathcal{M}_3^\beta$ and \mathcal{M}_3^γ for various decoding algorithms. Also plotted there is a linear spreading scheme from the matrix in (3) that has been claimed to be the optimal rotation to achieve a full diversity order 2. The linear rotation method uses a 16-QAM constellation to have the same throughput as TCJM. The decoding complexities per frame for the schemes are summarized in Table I, where we can see that a significant complexity reduction has been achieved by the DCS decoding. Fortunately, this overhead reduction at the receiver is not traded by a huge performance degrade. One can observe from Fig. 7 that the performance of TCJM with DCS_{r=1} decoding (only one diversity channel is picked for hard decision) actually converges and eventually coincides with the ML detection performance as SNR increases. For \mathcal{M}_3^β and \mathcal{M}_3^γ , the performance coincidence occurs when FER equals 10^{-3} or BER equals $5 \cdot 10^{-5}$. For \mathcal{M}_3^α , there is even no obvious gap between the two detection methods in the SNR range of interest. In contrast, DCS_{r=2} decoding suffers from an evident performance loss but can still keep the diversity gain as claimed by Theorem 2. To avoid making the figure too complicated, we do not provide the DCS_{r=2} detection performance for \mathcal{M}_3^β and \mathcal{M}_3^γ because they are not attractive relative to DCS_{r=1} detection. Notice that \mathcal{M}_3^β and \mathcal{M}_3^γ have very close performance for each decoding algorithm, which complies with our observation in Fig. 4. Compared with the optimal spreading scheme, our $\mathcal{M}_3^\alpha, \mathcal{M}_3^\beta$ and \mathcal{M}_3^γ can all outperform it for a maximum of about 2dB gain (at BER



(a)

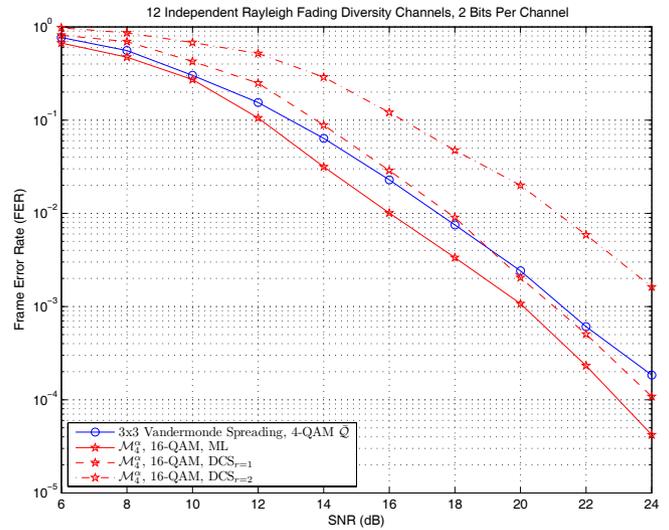


(b)

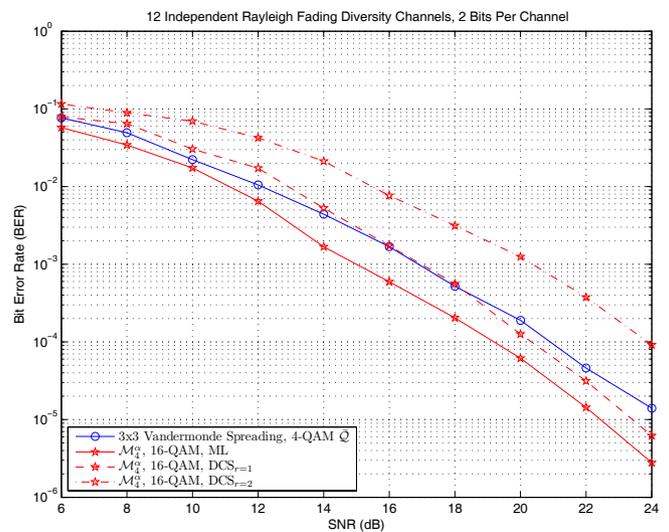
Fig. 7. Comparison of \mathcal{M}_3^α , \mathcal{M}_3^β , \mathcal{M}_3^γ and the optimal linear spreading scheme with the rotation matrix in (3) over 12 independent Rayleigh fading channels: (a) FER performance; (b) BER performance.

equal to $5 \cdot 10^{-5}$, for example) in terms of BER, even with the $\text{DCS}_{r=1}$ detection and hence $\frac{1}{3}$ decoding complexity. If the FER is concerned, \mathcal{M}_3^β and \mathcal{M}_3^γ with $\text{DCS}_{r=1}$ detection also enjoy a superior performance over the linear spreading scheme.

Similarly, in Fig. 8, we compare \mathcal{M}_4^α with a linear spreading scheme from the 3×3 Vandermonde rotation matrix [28, Section 4.4.2]. The Vandermonde spreading scheme uses a QPSK constellation for the same throughput as \mathcal{M}_4^α . The decoding complexities per frame for the two schemes are also referred in Table I. One can see from Fig. 8 that the ML and $\text{DCS}_{r=1}$ decodings for \mathcal{M}_4^α have about 1dB gap in the presented SNR range, and both of them achieve a larger coding gain than the spreading method. To be specific, the performance of \mathcal{M}_4^α with ML detection is consistently superior to the Vandermonde spreading. On the other hand, the \mathcal{M}_4^α with $\text{DCS}_{r=1}$ detection can outperform the spreading scheme with only $\frac{3}{8}$ complexity when SNR is reasonably high, i.e., there is a joint between their performance curves. We



(a)



(b)

Fig. 8. Comparison of \mathcal{M}_4^α and the Vandermonde linear spreading scheme over 12 independent Rayleigh fading channels: (a) FER performance; (b) BER performance.

anticipate that the $\text{DCS}_{r=1}$ detection performance eventually converges to the ML detection performance as SNR further increases. Finally, note that the 3×3 Vandermonde matrix is not unitary and therefore the diversity channels have unequal average powers for the linear spreading method. This is an undesired feature from an implementation point of view.

We also present the performance comparison for \mathcal{M}_3^α , \mathcal{M}_3^β , \mathcal{M}_3^γ and the plain unspread (unitary spreading) scheme on 16-QAM constellation over AWGN channels in Fig. 9. We have mentioned that there is no gain for spreading over AWGN channels and the plain modulation corresponding to an identity rotation matrix in (2) is already the best linear scheme. It can be seen in Fig. 9 that \mathcal{M}_3^β and \mathcal{M}_3^γ slightly outperform the traditional modulation, while \mathcal{M}_3^α has a much worse performance. This observation is consistent with Fig. 5, where although \mathcal{M}_3^α has a smaller minimum Euclidean distance than \mathcal{M}_3^β and the unitary spreading, the probability corresponding to this minimum distance is very small. Similarly, the performance comparison of \mathcal{M}_4^α with the plain modulation on

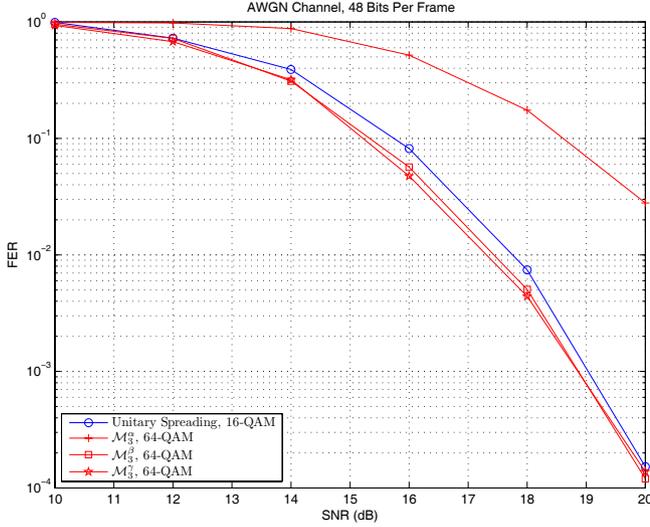


Fig. 9. Comparison of the FER performance for M_3^α , M_3^β , M_3^γ and the unitary linear spreading (unspread) scheme over AWGN channels.

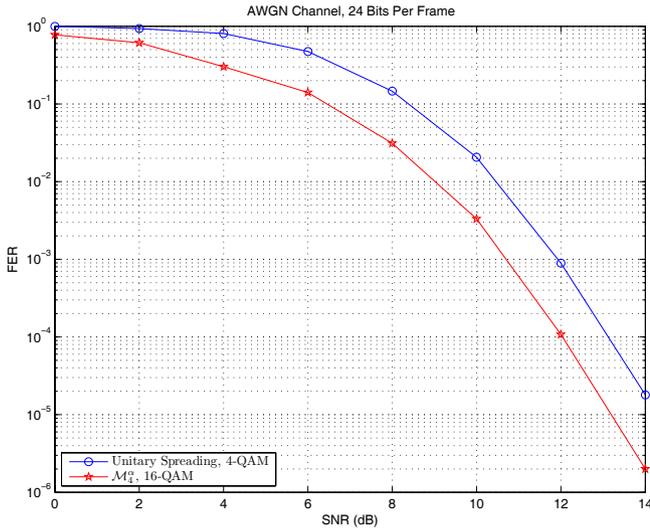


Fig. 10. Comparison of the FER performance for M_4^α and the unitary linear spreading (unspread) scheme over AWGN channels.

QPSK constellation over AWGN channels is provided in Fig. 10. Evidently, M_4^α has a significant gain (more than 1dB) than the latter.

The comparison in Fig. 7 - Fig. 10 has justified the flexibility of our MDS code based signal diversity techniques in various communication scenarios where the receiver has the option to choose different decoding algorithms depending on the channel feature and allowed computational overhead. But no channel information is required at the transmitter side for, for instance, adaptive modulation schemes.

VI. CONCLUSION

In this paper, we proposed a novel signal space diversity technique based on MDS codes and an associated suboptimal DCS decoding algorithm. The DCS decoding can significantly reduce the complexity relative to the optimal ML detection with only a marginal performance loss while keeping the diversity order. By providing two design examples called TCJM and

QCJM, we illustrated how to optimize the performance of our technique from a binary linear code construction as well as the constellation labelling. Simulation results showed that TCJM and QCJM can outperform some optimal linear spreading schemes over either Rayleigh fading or AWGN channels, even when they have a much lower decoding complexity endowed by DCS detection than the latter.

APPENDIX

A. Proof of Theorem 1

Proof: Consider two n -length information bit sequences $\mathbf{b}_i = (b_1^i, b_2^i, \dots, b_n^i)$, $i = 1, 2$. Correspondingly, we have $\mathbf{c}_i = (c_1^i, c_2^i, \dots, c_{mp}^i) = \mathbf{b}_i \cdot G_{m,d}$ and $\mathbf{x}_i = (x_1^i, x_2^i, \dots, x_m^i)$, $i = 1, 2$. Note that for a given constellation labelling, \mathbf{b}_i and $\mathbf{b}_i \cdot A$ decide the first $m-d+1$ and last $d-1$ symbols of \mathbf{x}_i , respectively. Let $\Delta \mathbf{b} = \mathbf{b}_1 - \mathbf{b}_2$, $\Delta \mathbf{c} = \mathbf{c}_1 - \mathbf{c}_2 = \Delta \mathbf{b} \cdot G_{m,d}$ and $\Delta \mathbf{x} = \mathbf{x}_1 - \mathbf{x}_2 = (\Delta x_1, \Delta x_2, \dots, \Delta x_m)$.

Let us first consider the sufficiency. Assume there are exactly k nonzero elements in $(\Delta x_1, \Delta x_2, \dots, \Delta x_{m-d+1})$, $1 \leq k \leq \min\{m-d+1, d-1\}$. From the condition, there are at most $k-1$ zeros in $(\Delta x_{m-d+2}, \Delta x_{m-d+3}, \dots, \Delta x_m)$ since, otherwise, we are able to find a $kp \times kp$ submatrix of A with the form in (8) that is singular. Therefore, $w(\Delta \mathbf{x}) \geq k + (d-1) - (k-1) = d$ and the code \mathcal{X} achieves a diversity order of at least d . To show that the diversity order is exactly d , it suffices to consider the case of $k=1$ by utilizing the condition.

To prove the necessity, assume there exist $1 \leq k_0 \leq \min\{m-d+1, d-1\}$, $1 \leq i_1^0 < i_2^0 < \dots < i_{k_0}^0 \leq m-d+1$ and $1 \leq j_1^0 < j_2^0 < \dots < j_{k_0}^0 \leq d-1$ such that matrix

$$\tilde{A} = \begin{pmatrix} A_{i_1^0, j_1^0} & A_{i_1^0, j_2^0} & \dots & A_{i_1^0, j_{k_0}^0} \\ A_{i_2^0, j_1^0} & A_{i_2^0, j_2^0} & \dots & A_{i_2^0, j_{k_0}^0} \\ \dots & \dots & \ddots & \dots \\ A_{i_{k_0}^0, j_1^0} & A_{i_{k_0}^0, j_2^0} & \dots & A_{i_{k_0}^0, j_{k_0}^0} \end{pmatrix}$$

is singular. Then, we can find a binary vector $\tilde{\mathbf{b}} = (\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_{k_0 p})$ of length $k_0 p$ such that $\tilde{\mathbf{b}} \cdot \tilde{A} = 0$. Define the bit sequence \mathbf{b}_1 by $b_{(i_t^0 - 1)p + u}^1 = \tilde{b}_{(t-1)p + u}$, $1 \leq t \leq k_0, 1 \leq u \leq p$, and 0 for all the other components. Let $\mathbf{b}_2 = 0$. Then, there are exactly k_0 nonzero elements in $(\Delta x_1, \Delta x_2, \dots, \Delta x_{m-d+1})$ and $\Delta x_{m-d+1+j_t^0} = 0$ for $1 \leq t \leq k_0$, which implies $w(\Delta \mathbf{x}) \leq k_0 + (d-1) - k_0 = d-1$. This contradicts with the condition that \mathcal{X} has a diversity order d . ■

B. Proof of Corollary 1

Proof: Using the symbols and notations defined in the first paragraph of Appendix A, we focus on the codeword difference $\Delta \mathbf{x}$ with $w(\Delta \mathbf{x}) = d$. If the d nonzero components of $\Delta \mathbf{x}$ are all in $(\Delta x_1, \Delta x_2, \dots, \Delta x_{m-d+1})$ ($m-d+1 \geq d$), this case is irrespective of the matrix A in (7) and we hence neglect it.

Assume there are exactly k and $d-k$ nonzero components in $(\Delta x_1, \Delta x_2, \dots, \Delta x_{m-d+1})$ and $(\Delta x_{m-d+2}, \Delta x_{m-d+3}, \dots, \Delta x_m)$, respectively, $1 \leq k \leq \min\{m-d+1, d-1\}$. Let these nonzero components

be $\Delta x_{i_1}, \Delta x_{i_2}, \dots, \Delta x_{i_k}$ and $\Delta x_{m-d+1+j_1}, \Delta x_{m-d+1+j_2}, \dots, \Delta x_{m-d+1+j_{d-k}}, 1 \leq i_1 < i_2 < \dots < i_k \leq m-d+1, 1 \leq j_1 < j_2 < \dots < j_{d-k} \leq d-1$. The number of $\Delta \mathbf{b}$ such that $\Delta x_{i_t}, 1 \leq t \leq k$, and $\Delta x_{m-d+1+j_s}, 1 \leq s \leq d-k$, are nonzero is the size of the set

$$\mathcal{U} = \left\{ (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k) \mid \sum_{t=1}^k \mathbf{v}_t A_{i_t, j_s} \neq 0 \right. \\ \left. \text{for } 1 \leq \forall s \leq d-k, 0 \neq \mathbf{v}_t \in \{0, 1\}^p, 1 \leq t \leq k \right\}.$$

We know from $w(\Delta \mathbf{x}) = d$ that $\sum_{t=1}^k \mathbf{v}_t A_{i_t, j_1} \neq 0$ ($\Delta x_{m-d+1+j_1} \neq 0$) implies $\sum_{t=1}^k \mathbf{v}_t A_{i_t, j_s} \neq 0$ ($\Delta x_{m-d+1+j_s} \neq 0$) for $2 \leq s \leq d-k$. So, \mathcal{U} can be equivalently reduced to

$$\mathcal{U} = \left\{ (\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k) \mid \sum_{t=1}^k \mathbf{v}_t A_{i_t, j_1} \neq 0, \right. \\ \left. 0 \neq \mathbf{v}_t \in \{0, 1\}^p, 1 \leq t \leq k \right\}.$$

It is easy to see that $|\mathcal{U}|$ is independent of $A_{i_1, j_1}, A_{i_2, j_1}, \dots, A_{i_k, j_1}$ if they are full-rank. Hence, we have completed the proof. ■

C. Proof of Theorem 3

Proof: We continue to use the symbols and notations defined in the first paragraph of Appendix A with $m = 3, n = 12, d = 2$ and $p = 6$. Furthermore, let $\Delta \mathbf{b}_i = (b_{p(i-1)+1}^1 - b_{p(i-1)+1}^2, b_{p(i-1)+2}^1 - b_{p(i-1)+2}^2, \dots, b_{pi}^1 - b_{pi}^2), i = 1, 2$, and hence $\Delta \mathbf{b} = (\Delta \mathbf{b}_1, \Delta \mathbf{b}_2)$. Consider the following five cases for $i = 1$ or 2 that cover all the possibilities:

- If $w(\Delta \mathbf{b}_i) > 2, |\Delta x_i| \geq \sqrt{5}d_{\min}^{64}$ from (15);
- If $w(\Delta \mathbf{b}_i) = 1$ and $w(\Delta \mathbf{b}_{3-i}) = 0, |\Delta x_3| \geq \sqrt{5}d_{\min}^{64}$ from condition (a) and (15);
- If $w(\Delta \mathbf{b}_i) = 2$ and $w(\Delta \mathbf{b}_{3-i}) = 0, |\Delta x_i|, |\Delta x_3| \geq \sqrt{2}d_{\min}^{64}$ from condition (c) and (15);
- If $w(\Delta \mathbf{b}_i) = 1$ or 2 and $w(\Delta \mathbf{b}_{3-i}) = 1, \Delta x_1, \Delta x_2, \Delta x_3 \neq 0$ from condition (b);
- If $w(\Delta \mathbf{b}_1) = w(\Delta \mathbf{b}_2) = 2, |\Delta x_1|, |\Delta x_2| \geq \sqrt{2}d_{\min}^{64}$ from (15).

From the above discussion, if $w(\Delta \mathbf{x}) = 2$, the absolute values of its two nonzero components have product no less than $2(d_{\min}^{64})^2$. Hence, we have completed the proof. ■

D. On the nonexistence of a binary 6×6 full-rank matrix such that any nonzero linear combination of its two rows has Hamming weight no less than 3

Proof: Let us first consider how many rows of weight 3 we can have at most in a 6×6 full-rank matrix M . Assume that there are h such rows forming a $h \times 6$ submatrix H of M . In H , we cannot find 3 entry 1 on its any column because otherwise, two of the three rows with entry 1 on that column will add to a vector with weight less than 3. Therefore, any column of H has weight no larger than 2 and furthermore, any two columns with weight 2 must be different. So, we have $h \leq 4$ from $\binom{h}{2} \leq 6$. If $h = 4$, however, all the 4 rows

of H will add to 0, which contracts with the full rankness of M . So, we can have at most 3 rows of weight 3 in M . Following the above analysis for weight 3 case, we can show that there are at most 2 rows of weight 4 in M . Finally, it is easy to know M has at most one row of weight 5 or 6.

As a result, we have the only choice that M is composed of 3 rows of weight 3, two rows of weight 4 and 1 row of weight 5. Without loss of generality, M must have the following form

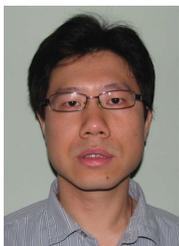
$$\begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (21)$$

so that the summation of each of the first 5 rows with the last row has weight larger than 2. But the form in (21) contradicts with our previous conclusion that any column of H has weight less than 3. Hence, we have completed the proof. ■

REFERENCES

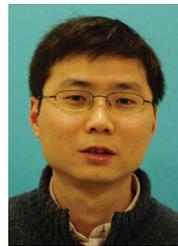
- [1] K. Boule and J.-C. Belfiore, "Modulation schemes designed for the Rayleigh fading channel," in *Proc. Conf. Inform. Sci. Syst. (CISS'92)*, Princeton, NJ, USA, Mar. 1992.
- [2] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 938-952, May 1997.
- [3] J. Boutros and E. Viterbo, "Signal space diversity: a power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1453-1467, July 1998.
- [4] S. Kaiser, "OFDM code-division multiplexing in fading channels," *IEEE Trans. Commun.*, vol. 50, no. 8, pp. 1266-1273, Aug. 2002.
- [5] A. Bury, J. Egle, and J. Lindner, "Diversity comparison of spreading transforms for multicarrier spread spectrum transformation," *IEEE Trans. Commun.*, vol. 51, no. 5, pp. 774-781, May 2003.
- [6] D. Goeckel and G. Ananthaswamy, "On the design of multidimensional signal sets for OFDM systems," *IEEE Trans. Commun.*, vol. 50, no. 3, pp. 442-452, Mar. 2002.
- [7] M. L. McCloud, "Analysis and design of short block OFDM spreading matrices for use on multipath fading channels," *IEEE Trans. Commun.*, vol. 53, no. 4, pp. 656-665, Apr. 2005.
- [8] V. M. Dasilva and E. S. Sousa, "Fading-resistant modulation using several transmitter antennas," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1236-1244, Oct. 1997.
- [9] H. El Gamal and A. R. Hammons Jr., "A new approach to layered space-time code and signal processing," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2321-2334, Sep. 2001.
- [10] M. O. Damen, K. A. Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628-636, Mar. 2002.
- [11] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753-760, Mar. 2002.
- [12] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebra," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.
- [13] G. Wang, H. Liao, H. Wang, and X.-G. Xia, "Systematic and optimal cyclotomic lattices and diagonal space-time block code designs," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3348-3360, Dec. 2004.
- [14] H. Wang and X.-G. Xia, "Optimal normalized diversity product of 2×2 lattice-based diagonal space-time codes from QAM signal constellations," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1814-1818, Apr. 2008.
- [15] H. Liao, H. Wang, and X.-G. Xia, "Some designs and normalized diversity product upper bounds for lattice-based diagonal and full-rate space-time block codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 569-583, Feb. 2009.
- [16] C. Lamy and J. Boutros, "On random rotations diversity and minimum MSE decoding of lattices," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1584-1589, July 2000.
- [17] A. Seyedi, "Multi-QAM modulation: a low-complexity full-rate diversity scheme," in *Proc. Int. Conf. Commun. (ICC'06)*, Istanbul, Turkey, June 2006, pp. 1470-1475.

- [18] R. Singleton, "Maximum distance Q -nary codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 116-118, Apr. 1964.
- [19] A. R. Hammons and H. El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 524-542, Mar. 2000.
- [20] H.-F. Lu and P. V. Kumar, "Rate-diversity trade-off of space-time codes with fixed alphabet and optimal constructions for PSK modulation," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2747-2751, Oct. 2003.
- [21] H.-F. Lu and P. V. Kumar, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1709-1730, May 2005.
- [22] X. N. Zeng and A. Ghayeb, "Performance bounds for space-time block codes with receive antenna selection," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2130-2137, Sep. 2004.
- [23] R. W. Heath Jr. and A. Paulraj, "Antenna selection for spatial multiplexing systems based on minimum error rate," in *Proc. IEEE Intern. Conf. Commun. (ICC'01)*, Helsinki, Finland, June 2001, pp. 2276-2280.
- [24] D. Gore and A. Paulraj, "MIMO antenna subset selection with space-time coding," *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2580-2588, Oct. 2002.
- [25] A. Gorokhov, D. Gore, and A. Paulraj, "Performance bounds for antenna selection in MIMO systems," in *Proc. IEEE Intern. Conf. Commun. (ICC'03)*, Anchorage, AK, USA, May 2003, pp. 3021-3025.
- [26] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microw. Mag.*, vol. 5, no. 1, pp. 46-56, Mar. 2004.
- [27] E. Soedarmadji, "Latin hypercubes and MDS codes," *Discrete Math.*, vol. 306, no. 12, pp. 1232-1239, June 2006.
- [28] C.-C. Kuo, S.-H. Tsai, L. Tadjpour, and Y.-H. Chang, *Precoding Techniques for Digital Communication Systems*. New York: Springer, 2008.
- [29] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*. North Holland, 1983.
- [30] R. Hill, *A First Course in Coding Theory*. Clarendon Press, 1986.
- [31] S. Roman, *Coding and Information Theory*. New York: Springer-Verlag, 1992.



Yue Shang received the B.S. degree in mathematics and the M.S. degree in probability and statistics from Nankai University, Tianjin, China, in 2001 and 2004, respectively, and the Ph.D. degree in electrical engineering from University of Delaware, Newark, DE, in 2008. He was an intern at Philips Research North America, Briarcliff Manor, NY, from August 2007 to January 2008, and at MathWorks, Natick, MA, from May 2008 to November 2008. Since January 2009, he has been with MathWorks as a senior signal processing and communications engineer. His

research interests are in information theory, signal processing and wireless communications. He has 15 journal and conference papers published and three U.S. patents granted. He is a recipient of the University Graduate Fellowship and the University Dissertation Fellowship from University of Delaware for 2006-2007 and 2007-2008 academic years, respectively. He received the Signal Processing & Communications Graduate Faculty Award from University of Delaware in 2007.



Dong Wang received the B.S. and M.S. degrees from Zhejiang University, Hangzhou, China, in 1996 and 1999, respectively, and the Ph.D. degree from University of Delaware, Newark, DE, in 2005, all in electrical engineering. From Apr. 1999 to Sep. 2000, he was employed as a senior system engineer at Shanghai No.2 R&D institute, ZTE corporation. From Oct. 2000 to June 2002, he was with Philips Research East Asia, Shanghai, China, as a research scientist. From May 2005 to Dec. 2005, he worked at Mitsubishi Electrical Research Labs, Cambridge MA. Since 2006, he has been with Philips Research North America, Briarcliff Manor, NY, as a senior member research staff. His research interests are in the general areas of signal processing and wireless communications. He has authored or coauthored over 20 journal and referred conference papers and has some 28 US/European patents granted or pending. He received the Competitive Fellowship Award, in 2004, and the Signal Processing & Communication Faculty Award, in 2005, both from University of Delaware.



Xiang-Gen Xia (M'97, S'00, F'09) received his B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, and his M.S. degree in mathematics from Nankai University, Tianjin, China, and his Ph.D. degree in Electrical Engineering from the University of Southern California, Los Angeles, in 1983, 1986, and 1992, respectively. He was a Senior/Research Staff Member at Hughes Research Laboratories, Malibu, California, during 1995-1996. In September 1996, he joined the Department of Electrical and Computer Engineering, University of

Delaware, Newark, Delaware, where he is the Charles Black Evans Professor. He was a Visiting Professor at the Chinese University of Hong Kong during 2002-2003, where he is an Adjunct Professor. Before 1995, he held visiting positions in a few institutions. His current research interests include space-time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. Dr. Xia has over 200 refereed journal articles published and accepted, and seven U.S. patents awarded and is the author of the book *Modulated Coding for Intersymbol Interference Channels* (New York, Marcel Dekker, 2000).

Dr. Xia received the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Program Award in 1997, the Office of Naval Research (ONR) Young Investigator Award in 1998, and the Outstanding Overseas Young Investigator Award from the National Nature Science Foundation of China in 2001. He also received the Outstanding Junior Faculty Award of the Engineering School of the University of Delaware in 2001. He is currently an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, *Signal Processing (EURASIP)*, and the *Journal of Communications and Networks (JCN)*. He was a guest editor of *Space-Time Coding and Its Applications in the EURASIP Journal of Applied Signal Processing* in 2002. He served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING during 1996 to 2003, the IEEE TRANSACTIONS ON MOBILE COMPUTING during 2001 to 2004, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY during 2005 to 2008, the IEEE SIGNAL PROCESSING LETTERS during 2003 to 2007, and the *EURASIP Journal of Applied Signal Processing* during 2001 to 2004. Dr. Xia served as a Member of the Signal Processing for Communications Committee from 2000 to 2005 and a Member of the Sensor Array and Multichannel (SAM) Technical Committee from 2004 to 2009 in the IEEE Signal Processing Society. He serves as IEEE Sensors Council Representative of IEEE Signal Processing Society (from 2002) and served as the Representative of IEEE Signal Processing Society to the Steering Committee for IEEE TRANSACTIONS ON MOBILE COMPUTING during 2005 to 2006. Dr. Xia is Technical Program Chair of the Signal Processing Symp., Globecom 2007 in Washington D.C. and the General Co-Chair of ICASSP 2005 in Philadelphia.