Space-Time Signaling based on Kerdock and Delsarte-Goethals Codes

A R. Calderbank  
Program in Applied and  
Computational Mathematics,  
Princeton University,  
Princeton, New Jersey, USA.  
Email: calderbank@math.princeton.edu

S N. Diggavi  
School of Computer and  
Communication Sciences  
Swiss Federal Institute of Technology (EPFL)  
EPFL-ISC-LICOS, Lausanne,  
Switzerland, CH 1015.  
Email: suhas.diggavi@epfl.ch

N. Al-Dhahir  
Department of Electrical Engineering  
University of Texas,  
Dallas, Texas, USA.  
Email: aldhahir@utdallas.edu

Abstract—This paper designs space-time codes for standard  
PSK and QAM signal constellations that have flexible rate,  
diversity and require no constellation expansion. Central to  
this construction are binary partitions of the PSK and QAM  
constellations that appear in codes designed for the Gaussian  
channel. The space-time codes presented here are designed by  
separately specifying the different levels of the binary partition  
in the space-time array. The individual levels are addressed by  
either the binary symmetric matrices associated with codewords  
in a Kerdock code or other families of binary matrices. Binary  
properties of these sets are sufficient to verify the diversity  
property of the codewords in the complex domain. Larger  
sets of binary symmetric matrices (such as the set used in  
Delsarte-Goethals codes) are used to trade diversity protection  
for increased rate.

I. INTRODUCTION

The information theoretic analysis by [7], [14] shows that  
multiple antennas at the transmitter and receiver enable very  
high data rate wireless communication. Space-time codes  
introduced in [13], improve the reliability of communication  
over fading channels by correlation of signals across the dif-  
ferent transmit antennas. A characterization of design criteria  
for such codes was given in [13], [8]. The technical focus of  
this paper is the design of space-time block codes.

Over the past few years there has been a significant research  
focus on design of space-time codes for a variety of scenar-  
ios. These include developments in space-time code design  
for inter-symbol interference fading channels [16] and non-  
These developments are complementary to the topic of this  
paper, where the focus is on the flat–fading channel with  
coherent reception. It has been observed in [13], [17] that there  
exists a fundamental trade-off between information rate and  
reliability (error probability annotated by diversity order). The  
recent developments in space-time codes focus on providing  
flexible rate and diversity order which are optimal with respect  
to the fundamental trade-off [3], [18].

In [4], [5] we introduced a different point of view where  
we asked whether we could construct a code with high rate  
which has a high diversity code embedded within it. In [4],  
[5] we formulated this question in the context of unequal  
error protection in the diversity domain. Furthermore in [4],  
[5] we gave some code constructions as well as bounds  
available by embedded diversity codes. In this paper we give  
further constructions of codes that have a diversity embedding  
property. The main theme of this paper is the use of constructs  
from binary coding theory to achieve design objectives in the  
complex domain. This is also the approach taken in [9], where  
codes with maximal diversity were constructed only for BPSK  
and QPSK constellations. Also, [18] used such properties to  
construct BPSK and QPSK codes that achieve a flexible rate  
and diversity, i.e., particular points in the rate-diversity trade-  
of region. Our work here differs from [18] in that we ask for  
the diversity embedding property of the space-time code as  
defined in [4], [5]. We make two main contributions in this  
paper. First is the method of designing space-time codes with  
design objectives in \( \mathbb{C} \), by using properties of binary codes  
over \( \mathbb{F}_2 \). This connection may have uses beyond the particular  
application proposed in this paper. The second contribution  
is the design of particular space-time codes based on these  
binary constructs, with a embedded diversity characteristics.  
Moreover, these codes are constructed for general QAM and  
PSK constellations, and are not specific to BPSK/QPSK signal  
sets.

The paper is organized as follows. In Section II we review  
the transmission model and code design criteria. Section III  
describes the algebraic framework for constructing binary  
partitions of standard PSK and QAM constellations. In Section  
IV, we propose the space-time code design based on separately  
specifying the different levels of the binary partition in the  
space-time array. Section V connects the binary matrices used  
to specify the different levels of the space-time array with  
codewords in the Kerdock and Delsarte-Goethals codes. We  
conclude the paper in Section VI with a brief discussion.

II. DATA MODEL

Our focus in this paper is on the quasi-static flat–fading  
channel where we transmit information coded over \( M_t \) trans-  
mit antennas and employ \( M_r \) antennas at the receiver. We  
assume that the transmitter has no channel state information,  
whereas the receiver is able to perfectly track the channel
Let $\mathbf{Y} = [\mathbf{y}(0), \ldots, \mathbf{y}(T-1)] \in \mathbb{C}^{M_r \times T}$ be the received sequence, $\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$ is the quasi-static channel fading matrix, $\mathbf{X} = [\mathbf{x}(0), \ldots, \mathbf{x}(T-1)] \in \mathbb{C}^{M_t \times T}$ is the space-time coded transmission sequence with transmit power constraint $P$, and $\mathbf{Z} = [\mathbf{z}(0), \ldots, \mathbf{z}(T-1)] \in \mathbb{C}^{M_r \times T}$ is assumed to be additive white Gaussian noise with variance $\sigma^2$.

The coding scheme is limited to one quasi-static transmission block. Similar arguments can be made if we are allowed to code across only a finite number of quasi-static transmission blocks [13]. This allows us to view the channel in (1) as a non-ergodic channel since the performance is determined by single randomly chosen channel fading matrix $\mathbf{H}$.

A coding scheme which has an average probability $P_c(\text{SNR})$ as a function of SNR that behaves as

$$
\lim_{\text{SNR} \to \infty} \frac{\log(P_c(\text{SNR}))}{\log(\text{SNR})} = -d
$$

is said to have a diversity order of $d$ [13], [17]. In words, a scheme with diversity order $d$ has an error probability at high SNR behaving as $P_c(\text{SNR}) \approx \text{SNR}^{-d}$.

The codebook structure proposed in [4], [5] takes several information streams and outputs the transmitted sequence $\{\mathbf{x}(k)\}$. The objective in [4], [5] is to ensure that each information stream gets the desired rate and diversity levels. To recall the terminology used in [4], [5], let us consider two message sets $\mathcal{A}$, $\mathcal{B}$ with rates $R(\mathcal{A})$ and $R(\mathcal{B})$ respectively. The decoder jointly decodes the two message sets and let $P_c(\mathcal{A})$ and $P_c(\mathcal{B})$ denote the average error probabilities. In [4], [5] we designed codes such that a certain tuple $(R_a, R_{db}, R_{sb}, D_a)$ of rates and diversities are achievable, where $R_a = R(\mathcal{A}) = \frac{\log(|\mathcal{A}|)}{SNR}$, $R_b = R(\mathcal{B}) = \frac{\log(|\mathcal{B}|)}{SNR}$, and analogous to (2),

$$
D_a = \lim_{\text{SNR} \to \infty} \frac{\log(P_c(\mathcal{A}))}{\log(\text{SNR})}, \quad D_b = \lim_{\text{SNR} \to \infty} \frac{\log(P_c(\mathcal{B}))}{\log(\text{SNR})}
$$

### A. Code Design Criteria

For codes designed for a finite (and fixed) rate, one can bound the error probability by using pairwise error probability (PEP) between two candidate codewords. This leads to the rank criterion for determining the diversity order of a space-time code [13], [8]. Consider a codeword sequence $\mathbf{X} = [\mathbf{x}^T(0), \ldots, \mathbf{x}^T(T-1)]$ as defined in (1), where $\mathbf{x}(k) = [x_1(k), \ldots, x_M(k)]^T$. The PEP between two codewords $\mathbf{x}$ and $\mathbf{e}$ can be determined by the codeword difference matrix $\mathbf{B}(\mathbf{x}, \mathbf{e})$ [13], [8], where

$$
\mathbf{B}(\mathbf{x}, \mathbf{e}) = 
\begin{pmatrix}
(x_1(0) - e_1(0)) & \cdots & (x_1(T-1) - e_1(T-1)) \\
\vdots & \ddots & \vdots \\
(x_M(0) - e_M(0)) & \cdots & (x_M(T-1) - e_M(T-1))
\end{pmatrix}
$$

For fixed rate codebook $\mathcal{C}$, it can be shown that the diversity order is given by [13]

$$
d = M_r \min_{\mathbf{x} \in \mathcal{C}} \text{rank}(\mathbf{B}(\mathbf{x}, \mathbf{e})).
$$

For diversity embedded codes, the design criterion for fixed rate codes is given by [4], [5],

$$
\min_{\mathbf{a}_1, \mathbf{a}_2 \in \mathcal{A}} \min_{\mathbf{b}_1, \mathbf{b}_2 \in \mathcal{B}} \text{rank}(\mathbf{B}(\mathbf{x}_{\mathbf{a}_1}, \mathbf{b}_1, \mathbf{x}_{\mathbf{a}_2}, \mathbf{b}_2)) \geq D_a / M_r
$$

$$
\min_{\mathbf{b}_1, \mathbf{b}_2 \in \mathcal{B}} \min_{\mathbf{a}_1, \mathbf{a}_2 \in \mathcal{A}} \text{rank}(\mathbf{B}(\mathbf{x}_{\mathbf{a}_1}, \mathbf{b}_1, \mathbf{x}_{\mathbf{a}_2}, \mathbf{b}_2)) \geq D_b / M_r.
$$

The error probability is determined by both the coding gain and the diversity order. Hence, the code design criterion prescribed in [13], [4], [5] is to design the codebook $\mathcal{C}$ so that the minimal rank of the codeword difference matrix corresponds to the required diversity order and the minimal determinant gives the corresponding coding gain. In this paper the focus is on the diversity order only, though we believe that the constructions also have good coding gains.

### III. Set Partitioning of QAM and QPSK Constellations

Let $\Gamma_1, \ldots, \Gamma_L$ be a $L$-level partition where $\Gamma_i$ is a refinement of partition $\Gamma_{i-1}$. We view this as a rooted tree, where the root is the entire signal constellation and the vertices at level $i$ are the subsets that constitute the partition $\Gamma_i$. In this paper we consider only binary partitions, and therefore subsets of partition $\Gamma_i$ can be labelled by binary strings $a_1, \ldots, a_i$, which specify the path from the root to the specified vertex.

Signal points in QAM constellations are drawn from some realization of the integer lattice $\mathbb{Z}^2$. We focus on the particular realization shown in Figure 1, where the integer lattice has been scaled by $\left[ \begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right]$ to give the lattice $D_2 = \{(a, b) | a, b \in \mathbb{Z}, a + b \equiv 0 \pmod{2} \}$, and then translated by $(1,0)$. The constellation is formed by taking all the points from $\Lambda$ that fall within a bounding region $\mathcal{R}$. The size of the constellation is proportional to the area of the bounding region, and in Figure 1, the bounding region encloses 16 points.

Binary partitions of QAM constellations are typically based on the following chain of lattices

$$
D_2 \supseteq 2\mathbb{Z}^2 \supseteq 2D_2 \supseteq 4\mathbb{Z}^2 \supseteq \ldots \supseteq 2^i\mathbb{Z}^2 \supseteq 2^{i+1}\mathbb{Z}^2 \supseteq \ldots
$$

In Figure 1, the subsets at level 1 are, to within translation, cosets of $2\mathbb{Z}^2$ in $D_2$ and the subsets at level 2 are cosets of $2D_2$. In general the subsets at level $2i$ are pairs of cosets of $2^{i}D_2$ where the union is a coset of $2^{i+1}\mathbb{Z}^2$, and the subsets at level $2i + 1$ are pairs of cosets of $2^{i+1}\mathbb{Z}^2$ where the union is a coset of $2^{i+2}D_2$. Note that implicit in Figure 1 is a binary partition of QPSK, where the points $1, -1, i, -i$ are labelled 00, 01, 11, 10 respectively. The binary partitions of PSK constellations can also be done in a similar manner.

#### A. Algebraic properties of binary partitions

In this section we focus on the algebraic properties of binary partitions of PSK constellations. Binary partitions of PSK constellations are based on a chain of subfields of the complex numbers $\mathbb{C}$. Let $\mathbb{Q}(\xi_2)$ be the field obtained by adjoining $\xi_2$ to the rationals $\mathbb{Q}$. The field $\mathbb{Q}(\xi_2)$ is a degree $2^{2-1}$ extension of $\mathbb{Q}$. Every
rational number is a quotient $a/b$, where $a, b \in \mathbb{Z}$, and every complex number in $\mathbb{Q}(i)$ is a quotient $a/b$, where $a, b$ are Gaussian integers. In general every complex number in $\mathbb{Q}(\zeta_{2^L})$ is a quotient $a/b$, where $a, b$ are integer linear combinations of $1, \zeta_{2^L}, \ldots, \zeta_{2^L}^{-1}$ and $b \neq 0$. For more details about cyclotomic fields see [15]. Note that $\zeta_{2^L}^{-1} = -1$, so that $\zeta_{2^L}^j = -\zeta_{2^L}^{-j}$, for $j = 0, 1, \ldots, 2^L - 1$.

We have a chain of fields $Q = \mathbb{Q}(\zeta_2) \subset \mathbb{Q}(\zeta_4) \subset \mathbb{Q}(\zeta_8) \ldots \subset \mathbb{Q}(\zeta_{2^L})$. Now let $Z[\zeta_{2^L}]$ be the ring obtained by adjoining $\zeta_{2^L}$ to the integers $Z$, i.e., the set of all integer linear combinations of $1, \zeta_{2^L}, \ldots, \zeta_{2^L}^{-1}$. If $a \in Z[\zeta_{2^L}]$, then the ideal $I(a)$ generated by $a$ is defined as [19],

$$I(a) = \{ b \in Z[\zeta_{2^L}] : b = ra, r \in Z[\zeta_{2^L}] \} \quad (6)$$

The quotient of $Z[\zeta_{2^L}]$ with respect to $I(a)$ (denoted as $Z[\zeta_{2^L}]/I(a)$) is in general a ring [19]. In particular, we are interested in the ideal generated by $(1 - \zeta_{2^L})^2$, and we can show that, $Z[\zeta_{2^L}]/I((1 - \zeta_{2^L})^2)$ has four congruence classes $\{0, 1, \zeta_{2^L}, 1 - \zeta_{2^L} \}$. This property is central to the proof of the diversity order achieved by the constructions given in the paper.

IV. SPACE-TIME CODES DERIVED FROM KERDOCK AND DELSARTE-GOETHALS CODES

A. Construction from Kerdock sets

A Kerdock set of order $m$ is a set of $2^m$ binary symmetric matrices with the property that the difference of any two of these matrices is non-singular. Kerdock sets are derived from Kerdock codes, and this correspondence is described briefly in Section V. Kerdock sets exist for all odd $m$, and there are examples where the set is closed under binary addition.

**Example:** For $m = 3$, the matrices

$$\begin{align*}
R_{000} &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & R_{001} &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & R_{010} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \\
R_{011} &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & R_{100} &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & R_{101} &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\
R_{110} &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & R_{111} &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.
\end{align*}$$

form a Kerdock set that is closed under binary addition, i.e., $P_a \otimes P_b = P_{a \oplus b}$. The mapping $a \rightarrow P_a$ encodes $3$ input bits as a matrix from the Kerdock set.

We now describe the space-time codes based on Kerdock sets that are matched to the binary partitions of QAM and PSK constellations presented in Section III. Encoding is by a selection of a sequence of matrices $K_1, \ldots, K_L$ from the Kerdock set. The matrix $K_j$ specifies the space-time array at level $j$. For example, in QAM constellations, setting $(K_1)_{ij} = 0$ means that the $i$th signal point $S_{ij}$ is in $2Z^2 + (1, 0)$, and setting $(K_1)_{ij} = 1$ means that $S_{ij}$ is in $2Z^2 + (1, 1) + (1, 0)$. The matrix $K_2$ refines this description and specifies the space-time array at level 2, and in general the matrix $K_j$ specifies the space-time array at level $j$. Encoding of PSK constellations is similar and we omit the details.

**Example:** For $m = 3$, and for QPSK (2-level binary partitioning of QAM constellations), a space-time codeword is a $3 \times 3$ array specified by 6 input bits. For example,

$$\begin{pmatrix} 010, 110 \end{pmatrix} \rightarrow \begin{pmatrix} P_{010}, P_{110} \end{pmatrix} \rightarrow \begin{pmatrix} -i & 1 & -1 \\ 1 & -1 & i \\ -1 & i & i \end{pmatrix}$$

Here encoding is non-linear, but there is no constellation expansion. Linear encoding is possible with modest constellation expansion by selecting a basis of $m$ matrices $B_k, k = 1, \ldots, m$, from the Kerdock set (here we assume closure under binary addition). Linear encoding would then allow us to decode using a sphere decoder [2]. Now, input bits $a_{jk}, j = 1, \ldots, L; k = 1, \ldots, m$ determine the signals $s_k, k = 1, \ldots, m$ by following the path $a_{1k}, a_{2k}, \ldots, a_{Lk}$ from the root to the corresponding vertex. The space-time codeword is given by

$$X = \sum_{k=1}^m s_k B_k. \quad (7)$$

**Example:** For $m = 3$, and for QPSK, inputs $010, 110$ determine signals $s_1 = -1, s_2 = i$ and $s_3 = 1$. We choose $B_1 = P_{010}, B_2 = P_{110},$ and $B_3 = P_{100}$ to minimize constellation expansion, and then

$$\begin{pmatrix} 010, 110 \end{pmatrix} \rightarrow \begin{pmatrix} 1 + i & -1 & 1 \\ -1 & 1 & i \\ 1 & i & -1 + i \end{pmatrix}. \quad (8)$$

The size of the constellation required at 2 of the 9 positions in the space-time array is effectively doubled, but now the sphere decoder can be used for efficient decoding [2].

B. Nested families of codes

A Delsarte-Goethals set of matrices is a nested family of $m \times m$ binary symmetric matrices,

$$DG(m + 1, (m + 1)/2) \subset DG(m + 1, (m - 1)/2) \subset \ldots \subset DG(m + 1, (m + 1)/2 - r) \subset \ldots$$

where the first member of this set $DG(m + 1, (m + 1)/2)$ is a Kerdock set. The set $DG(m + 1, (m + 1)/2 - r)$ contains $2^{m(r+1)}$ matrices and the rank of the differences of any two matrices in $DG(m + 1, (m + 1)/2 - r)$ is at least $m - 2r$. Fig. 1. A binary partition of a QAM constellation
Delsarte-Goethals sets are derived from Delsarte-Goethals codes, and this correspondence is described briefly in Section V. These sets exist for all odd \(m\), and there are examples where each family in the set is closed under binary addition.

It is possible to construct larger sets of matrices by dropping the condition that the matrices be symmetric. Consider the finite field \(\mathbb{F}_2\) of size \(2^m\), and let \(\phi: z \rightarrow z^2\) be the Frobenius map. Given field elements \(\alpha_i \in \mathbb{F}_{2^m}\), the map

\[
p(\alpha) = \alpha_0 + \alpha_1 \phi + \ldots + \alpha_r \phi^r
\]

is a linear transformation. Since \(\mathbb{F}_{2^m}\) is an \(m\)-dimensional vector space over the binary field \(\mathbb{F}_2\), we can represent \(p(\alpha)\) as a \(m \times m\) binary matrix. This defines a set \(P_{m,r}\) of \(2^{m(r+1)}\) binary matrices that is closed under binary addition. Note that

\[
P_{m,0} \subset P_{m,1} \subset P_{m,2} \ldots
\]

If \(\alpha \neq 0\), then the rank of \(p(\alpha)\) is at least \(m - r\) since the equation

\[\alpha_0 + \alpha_1 z + \ldots + \alpha_r z^r = 0\]

has at most \(2^r\) zeros. Hence the rank of the difference of any two matrices in \(P_{m,}\) is at least \(m - r\). Lu and Kumar in [18] use the set \(P_{m,r}\) to construct single layer space-time codes which achieve particular (optimal) points on the rate-diversity trade-off curve.

We are now ready to generalize the construction given in section IV-A to codes with nested diversities. The basic idea is that we choose sets \(K_1, \ldots, K_L\) from which the sequence of binary matrices which encode the constellations are chosen. In section IV-A, the choice was that \(K_i = \mathcal{K}, \forall i\), where \(\mathcal{K}\) was the Kerdock set. For diversity embedded codes, we choose the sets \(K_1, \ldots, K_L\), such that \(K_i = P_{m, r_i}\), i.e., the different families in the set has rank at least \(m - r_i\). Now the encoding is by selecting a sequence of matrices \(K_1, \ldots, K_L\), \(K_i \in K_i\), such that \(r_1, \ldots, r_L\).

In Section IV-B we will show that this construction achieves the rate tuple \((\ell_1 + 1, m - r_1), \ldots, (\ell_r + 1, m - r_L)\), with the overall equivalent single layer code achieving rate-diversity point \((\ell_1 + 1, m - r_L)\). We can have the desired number of layers by choosing several identical diversity/rate layers. For example, the maximal diversity construction in Section IV-A has one layer with rate 1 and maximal diversity \(m\). If we choose \(K_i = P_{m, r}\), \(\forall i\), then we achieve a rate \(r + 1\), with diversity order \(m - r\). However, the construction allows us to achieve diversity embedding with unequal diversity orders for different information streams as done in [4], [5].

\subsection*{C. Diversity order of constructions}

In order to construct diversity embedded space-time codes (such as those introduced in [4], [5]) we need different information streams to achieve different diversity levels. We accomplish this in the current setting by using matrices from different families to specify different levels in the space-time array.

One possible application of codes based on nested families of sets is balancing of the diversity gain and coding gain within a particular space-time code. The key observation here is that intra-subset distances increases with depth in the partition chain, so that less diversity may be required to achieve a given error rate at lower levels in the binary partition. A second potential application is to enable incremental redundancy based on the level of diversity protection. A potential value of the extra symmetry in the Delsarte-Goethals codes is to incorporate error detection in decoding.

We now verify that these codes achieve the desired diversity embedding. For PSK constellations, consider space-time codewords \(X, X'\) determined by sequences of \(L\) binary matrices \(\{B_j\}, \{B'_j\}\) and specified by \(L\) inputs \(\{a_j\}, \{a'_j\}\). We assume that the rank of \(B_j - B'_j\) over the binary field \(\mathbb{F}_2\) is at least \(d_j\), and that \(d_1 \geq d_2 \geq \ldots d_L\). If \(a_1 \neq a'_1\), then

\[
(X - X') = (1 - \xi L)(B_1 - B'_1) \mod (1 - \xi L)^2,
\]

where the notation means that we have taken the element-wise “remainder” of \((X - X')\) over the ideal generated by \((1 - \xi L)^2\). This results in a matrix which contains the elements \(\{0,1, \xi L, 1 - \xi L\}\). Now, we can show that since the elements of \(X, X'\) are in \(\{1, \xi L, \ldots, \xi L^{L-1}\}\), the result of taking the element-wise “remainder” can only result in matrix entries from the set \(\{0,1, \xi L\}\). This implies that we can take out the common factor \((1 - \xi L)\) and therefore obtain the result in equation (12). Since \(B_1 - B'_1\) has a rank of \(d_1\) over \(\mathbb{F}_2\), this implies that it has \(d_1\) rows that are linearly independent over \(\mathbb{F}_2\). Let \(f_1, \ldots, f_{d_1}\) be the \(d_1\) linearly independent rows of \(B_1 - B'_1\), and let \(c_1, \ldots, c_{d_1}\) be the corresponding rows of \((X - X')\). Therefore, just as in (12) we get,

\[
c_i = (1 - \xi L)f_i \mod (1 - \xi L)^2, \quad i = 1, \ldots, d_1,
\]

where the notation is interpreted in the same manner as (12). If the vectors \(\{c_i\}\) are linearly dependent over \(\mathbb{F}\), there exists a set of scalars \(\{\lambda_i\}\) in \(\mathbb{Z}[\xi L]\), not all divisible by \((1 - \xi L)^2\) such that \(\sum \lambda_i c_i = 0\). Reducing this equation modulo \((1 - \xi L)^2\), we obtain \(\sum \lambda_i c_i = 0\), where the elements \(\{\lambda_i\}\) are scalars in the set \(\{0,1, \xi L, 1 - \xi L\}\), and the elements of \(c_i\) are in \(\{0,1 - \xi L\}\) as given in the argument after (12). Now, absorbing \((1 - \xi L)\) into \(\lambda_i\) and since this absorption is done modulo \((1 - \xi L)^2\), we obtain the relationship \(\sum \lambda_i f_i = 0\), where now the elements \(\{\lambda_i\}\) and \(\{c_i\}\) are binary. Due to the relationship in (13) we see that \(\tilde{c}_i = f_i\) and hence we find that there exists a set \(\{\lambda_i\}\) in \(\mathbb{F}_2\) such that \(\sum \lambda_i f_i = 0\), which is clearly impossible. Hence the rank of \(X - X'\) over \(\mathbb{F}\) is at least \(d_1\).

Now, we can show that in general, if \(j\) is the first index for which \(a_j \neq a'_j\), then

\[
(X - X') = (1 - \xi L)^{j-1}(B_1 - B'_1) \mod (1 - \xi L)^j,
\]

where the interpretation of this statement is similar to the one given below (12). Given that we have chosen the nested family of binary sets such that \((B_j - B'_j)\) has a rank of at least \(d_j\) over \(\mathbb{F}_2\), the previous argument shows that the rank of \((X - X')\) is at least \(d_j\) over \(\mathbb{F}\). Therefore, we get the desired diversity embedding property.
The analysis for QAM constellations is similar (reduction modulo $(1+i)^2$ plays the role of reduction modulo $(1-\zeta_2)^2$) in the above analysis and we omit the details due to space constraints.

V. KERDOCK AND DELSARTE-GOETHALS CODES

Calderbank et al [1] connect Kerdock sets of order $m$ to classical Kerdock codes of length $2^{m+1}$ defined over the binary field, and to linear Kerdock codes of length $2^m$ defined over $\mathbb{Z}_4$, the ring of integers modulo 4. The classical binary Kerdock code is the union of $2^m$ cosets of the first Reed-Muller code $RM(1,m+1)$, and there is an additive correspondence between cosets and quadratic forms, each of which determines a $(m+1) \times (m+1)$ skew-symmetric binary matrix.

The rank of the skew-symmetric matrix is a function of the weight distribution of the associated coset (see [12]). The $2^m$ skew-symmetric matrices associated with the Kerdock code have the property that the difference of any two matrices is non-singular.

Hammons et al [10], showed that the classical binary Kerdock code is the image of a $\mathbb{Z}_4$-linear Kerdock code under the Gray map, which is an isometry from $(\mathbb{Z}_4^N, \text{Lee distance})$ to $(\mathbb{Z}_2^{2N}, \text{Hamming distance})$. The $\mathbb{Z}_4$-linear Kerdock code is the union of $2^m$ cosets of the inverse image of $RM(1,m+1)$. Calderbank et al [1] showed that there is an additive correspondence between these cosets and $\mathbb{Z}_4$-linear quadratic forms, each of which determines an $m \times m$ symmetric binary matrix. The correspondence between binary symmetric matrices $P$ and binary skew-symmetric matrices $M$ is given by,

$$M = \begin{pmatrix} P & d_P^T \\ d_P & 0 \end{pmatrix}$$

where the row vector $d_P$ is the main diagonal of $P$. This correspondence is rank preserving in the sense that if $M$ has rank $m+1-2i$, then $P$ has rank $m+1-2i$ or $m-2i$. In particular, the $2^m$ symmetric matrices associated with the $\mathbb{Z}_4$-linear Kerdock code have the property that the difference of any two matrices is non-singular, as needed in Section IV-C.

For odd $m$, let $\delta = (m+1)/2 - r$. Hammons et al [10] showed that the Delsarte-Goethals codes $DG(m+1, \delta)$, can be realized as binary codes of length $2^{m+1}$ or as $\mathbb{Z}_4$-linear codes of length $2^m$. The codes are nested, all contain the Kerdock code $(DG(m+1, (m+1)/2))$, and $DG(m+1, \delta)$ determines $2^{(r+1)m}$ binary symmetric $m \times m$ matrices as above, with the property that the rank of the difference of any two matrices is at least $m+1-2r$, as needed in the construction of diversity embedded codes.

VI. DISCUSSION

In this paper we explored the design of space-time codes which are constructed from nested families of binary codes. We have developed a framework for space-time code design, where constructs from binary coding theory are employed to achieve design objectives in the complex domain. This framework enables design of space-time codes with standard QAM and PSK constellations that have flexible diversity and require no constellation expansion. This new framework allowed us to construct space-time codes with embedded diversity. We can also use these codes to trade-off diversity with coding gain. We believe that the connection between these binary codes and space-time codes is both of theoretical and practical interest.

ACKNOWLEDGMENT

The authors would like to thank F. Voloch and P V. Kumar for bringing [18] to their attention.

REFERENCES