

# Field Extension Code Based Dispersion Matrices for Coherently Detected Space-Time Shift Keying

Rakshith Rajashekar and K.V.S. Hari  
Department of Electrical Communication Engineering  
Indian Institute of Science, Bangalore 560012  
{ rakshithmr, hari }@ece.iisc.ernet.in

L. Hanzo  
School of ECS  
University of Southampton, UK  
lh@ecs.soton.ac.uk

**Abstract**—Motivated by the recent Coherent Space-Time Shift Keying (CSTSK) philosophy, we construct new dispersion matrices for rotationally invariant PSK signaling sets. Given a specific PSK signal constellation, the dispersion matrices of the existing CSTSK scheme were chosen by maximizing the mutual information over randomly generated sets of dispersion matrices. In this contribution we propose a general method for constructing a set of structured dispersion matrices for arbitrary PSK signaling sets using Field Extension (FE) codes and then study the attainable Symbol Error Rate (SER) performance of some example constructions. We demonstrate that the proposed dispersion scheme is capable of outperforming the existing dispersion arrangement at medium to high SNRs.

**Index Terms**—Field Extensions, Cyclotomic Fields, Space-Time Shift Keying, Coding gain, Diversity

## I. INTRODUCTION

Coherent Space-Time Shift Keying (CSTSK) is capable of striking a flexible tradeoff between the attainable diversity and multiplexing gain [1], [2]. This scheme was shown to exhibit a better performance than Spatial Modulation (SM) [3], [4] and Space Shift Keying (SSK) [5], since it is capable of achieving both transmit and receive diversity. Specifically, the CSTSK scheme activates one out of  $Q$   $M \times T$ -element Dispersion Matrices (DM), which is then multiplied by one of the legitimate symbols from an  $L$ -symbol constellation, where  $M$  is the number of transmit antennas and  $T$  is the number of time-slots. This scheme achieves a throughput of  $R = \frac{1}{T} \log_2(Q \cdot L)$  bits/channel use (bpcu). The DMs of this scheme [1], [2] were obtained by maximizing the Discrete-Input Continuous-Output Memoryless Channel (DCMC) capacity over a large set of randomly generated, unity-average-power, complex-valued random Gaussian matrices [1]. Since, the designs generated this way for maximizing the capacity are unable to guarantee achieving the maximum attainable coding gain, they do not necessarily minimize the BER [6].

In this contribution we design DMs that exhibit desirable properties, such as achieving a high coding gain, full diversity and low-complexity decodability. We will invoke Field Extension (FE) codes [7], [8] and demonstrate that FE codes defined over rotationally invariant constellations result in DMs exhibiting the above-mentioned benefits.

The financial support of the DST, India and of the EPSRC, UK under the auspices of the India-UK Advanced Technology Centre (IU-ATC) is gratefully acknowledged.

**Notations** : Boldface uppercase letters represent matrices and are indexed as  $\mathbf{X}_i$ . Furthermore,  $\text{tr}[\mathbf{X}]$  and  $\mathbf{X}^H$  denote the Trace and Hermitian of the matrix  $\mathbf{X}$ , respectively.  $\mathbf{I}_r$  denotes an  $r \times r$  identity matrix.  $\{p_1, p_2, p_3, \dots, p_k\}$  denotes the set of  $k$  prime numbers. Polynomials are represented as a function of  $x$ , for example  $p(x)$ . Calligraphic uppercase letters represent sets of matrices, for example  $\mathcal{E}$ .  $\mathcal{D} \subset \mathcal{E}$  implies that  $\mathcal{D}$  is a subset of  $\mathcal{E}$  and  $|\mathcal{D}|$  represents cardinality of  $\mathcal{D}$ . Blackboard-bold font letters like  $\mathbb{Q}$  represent fields. Upper case letters are used to represent sets, fields, and extended fields. The extended field  $F = \mathbb{Q}(S)$  represents the extension of field of rational numbers  $\mathbb{Q}$  over some set  $S$ .

## II. SYSTEM MODEL

We consider a MIMO system having  $M$  transmit as well as  $N$  receive antennas and a quasi-static, frequency-flat fading channel, yielding:

$$\mathbf{Y}_i = \sqrt{\frac{\rho}{M}} \mathbf{H}_i \mathbf{X}_i + \mathbf{N}_i, \quad (1)$$

where  $\mathbf{X}_i \in \mathbb{C}^{M \times T}$  is the transmitted Space-Time (ST) matrix,  $\mathbf{Y}_i \in \mathbb{C}^{N \times T}$  is the received ST matrix,  $\mathbf{H}_i \in \mathbb{C}^{N \times M}$  and  $\mathbf{N}_i \in \mathbb{C}^{N \times T}$  are the channel- and noise-matrices, respectively. The entries of the channel- and noise-matrices are from a circularly symmetric complex-valued Gaussian distribution i.e.,  $\mathcal{CN}(0,1)$  and  $\mathcal{CN}(0, N_0)$ , respectively, where  $N_0$  is the noise variance,  $\rho$  is the average Signal to Noise Ratio (SNR) at each receive antenna and  $i$  indicates the block index in all the matrices. Throughout this paper we assume  $M = T$ .

### A. CSTSK scheme

For the CSTSK scheme [1], we have

$$\mathbf{X}_i = s_{i,q} \mathbf{A}_{i,p}, \quad (2)$$

where  $s_{i,q} \in \mathbb{C}$  is a symbol from an  $L$ -symbol constellation, and  $\mathbf{A}_{i,p} \in \mathbb{C}^{M \times T}$  is a DM from  $\mathcal{D}$ , a set of DMs with  $|\mathcal{D}| = Q$ . All the DMs satisfy the unity average transmission power constraint, i.e.,

$$\text{tr}[\mathbf{A}_{i,p}^H \mathbf{A}_{i,p}] = T \text{ for } 1 \leq p \leq Q. \quad (3)$$

The notational representation of a typical CSTSK scheme used is formulated as 'CSTSK( $M, N, T, Q$ ),  $L$ -symbol con-

stellation' [1]. We assume perfect Channel State Information (CSI) and ML decoding at the receiver, yielding

$$(\hat{p}, \hat{q})_{ML} = \arg \min_{p,q} \|\mathbf{Y}_i - \sqrt{\frac{\rho}{M}} \mathbf{H}_i \mathbf{A}_{i,p} s_{i,q}\|_F^2, \quad (4)$$

where  $1 \leq p \leq Q$ ,  $1 \leq q \leq L$ .

As DMs  $\mathbf{A}_{i,p}$  in the existing scheme were chosen by maximizing the mutual information, we refer to this scheme here as the Capacity Optimized Dispersion Matrix (CO-DM) based scheme.

### III. PROPOSED FIELD EXTENSION CODE BASED DM SET CONSTRUCTION

#### A. Motivation

In the existing CSTSK scheme, DMs are chosen by maximizing the mutual information, which we see as a variant of Linear Dispersion Codes (LDC) with DMs optimized for mutual information [9]. It was shown in [8] that Field Extension codes perform better than LDCs with the aid of capacity-optimized DMs at high SNRs due to their better coding gain. This motivates us for using FE codes to derive DMs for CSTSK schemes. For the sake of completeness, a brief review of FE codes is provided at the end of the paper in the Appendix.

#### B. DM set for PSK constellation using Field Extension Codes

Considering the chain of field extensions given in eqn.(13) (in Appendix), we get Field Extension codes over  $F$  as

$$\mathcal{C} = \left\{ \sum_{i=0}^{n-1} f_i \mathbf{M}^i \mid f_i \in F, i = 0, 1, \dots, n-1 \right\}, \quad (5)$$

where  $\mathbf{M}$  is given in eq.(14). This can be written as

$$\mathcal{C} = \left\{ f_k \mathbf{M}^k + \sum_{i=0, i \neq k}^{n-1} f_i \mathbf{M}^i \mid f_i \in F, i = 0, 1, \dots, n-1 \right\} \quad (6)$$

for some  $k$  satisfying  $0 \leq k \leq n-1$ .

If we restrict  $F$  to be a set which is closed under multiplication and has an *identity element*, then we can write

$$\mathcal{C} = \left\{ f_k (\mathbf{M}^k + \sum_{i=0, i \neq k}^{n-1} f_i'' \mathbf{M}^i) \mid f_i'' \in F, i = 0, 1, \dots, n-1 \right\} \quad (7)$$

Note that any PSK signal set can be used as  $F$ , since it satisfies both the conditions mentioned above. Let

$$\mathcal{C}' = F \times \mathcal{E}, \quad (8)$$

where  $\times$  denotes the Cartesian product and

$$\mathcal{E} = \left\{ \mathbf{M}^k + \sum_{i=0, i \neq k}^{n-1} f_i'' \mathbf{M}^i \mid f_i'' \in F, i = 0, 1, \dots, n-1 \right\}, \quad (9)$$

while  $\zeta$  is a product-map over a set of ordered pairs,  $X = \{(x_1, x_2) \mid x_1 \in X_1, x_2 \in X_2\}$  where  $X_1$  and  $X_2$  are two arbitrary sets, given by  $\zeta : (x_1, x_2) \mapsto x_1 x_2$ . From eq.(7) and eq.(8) we can write  $\zeta : F \times \mathcal{E} \mapsto \mathcal{C}$ .

Any  $\mathcal{D} \subseteq \mathcal{E}$  may be used as a set of dispersion matrices in conjunction with  $S$  in the CSTSK scheme.  $\mathcal{D} \subset \mathcal{E}$  can be chosen to maximize the coding gain. When we have  $\mathcal{D} = \mathcal{E}$ , the CSTSK scheme will be using codes completely defined over  $\mathcal{C}$ . In this case the coding gain is given by  $G$ . Thus any  $\mathcal{D} \subseteq \mathcal{E}$  will guarantee a minimum coding gain of  $G$ . Furthermore, if  $F$  is a PSK signal set it enables sphere decodability [7]. We refer to this scheme as a Field Extension Code based Dispersion Matrix (FEC-DM) based arrangement in the rest of this paper.

#### C. Computational Complexity

It was shown that the SM/SSK [3], [5] and CSTSK [1] schemes required a relatively low complexity ML receiver compared to the Vertical Bell Laboratories Layered Space-Time (V-BLAST) scheme and LDCs, since CSTSK relies on an Inter-Channel Interference (ICI) free system model. Here, the computational complexity was quantified in terms of the number of real multiplications involved in ML detection. It may be readily shown that the complexity of the CSTSK scheme relying on the proposed FEC-DMs remains the same as that using conventional DMs. However, we show that a particular class of LDCs also lends itself to low-complexity ML detection [11].

An LDC is a set of matrices of the form given by

$$\mathcal{C} = \left\{ \sum_{i=0}^{n-1} f_i \mathbf{M}_i + f_i^* \mathbf{M}'_i \mid f_i \in F, i = 0, 1, \dots, n-1 \right\}, \quad (10)$$

where  $F$  is an arbitrary signal set, while  $\mathbf{M}_i$  and  $\mathbf{M}'_i$  are DMs. We consider a special class of LDCs in which the DMs  $\mathbf{M}'_i$  are zero matrices and  $F$  represents an arbitrary PSK signal set. An FE code defined over a PSK constellation and given by eqn.(5), is one such code. It may be inferred from eqns.(5)-(8) that any such code may be defined by the Cartesian product of a set of matrices  $\mathcal{E}$  and of the signal set  $F$ , which has an ICI-free system model [1]. We refer to this class of codes as Decomposable Dispersion Code (DDC). Since, schemes that offer an ICI-free system model also lend themselves to low-complexity ML detection, all DDCs rely on low-complexity ML detection such as the CSTSK scheme.

#### D. Example constructions

In this section we present some examples considering irreducible polynomials of the form  $x^n - \gamma$  conceived for QPSK constellation associated with  $M = N = T = 2$ .

*Example 1 :* When considering  $L = 4$ ,  $M = n = 2$  and  $b = 1$ ,  $x^2 - \omega_4$  becomes irreducible. Thus for  $F = S = \{1, -1, j, -j\}$ , from eqn.(9) we have

$$\mathcal{E} = \left\{ \begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix} \begin{bmatrix} j & j \\ 1 & j \end{bmatrix} \begin{bmatrix} -1 & j \\ 1 & -1 \end{bmatrix} \begin{bmatrix} -j & j \\ 1 & -j \end{bmatrix} \right\}.$$

We can choose  $\mathcal{D}$  to be any subset of  $\mathcal{E}$ . Given  $\mathcal{D} = \mathcal{E}$  we get four DMs. The coding gain of this scheme may be shown to be  $G = 1$ . To generate more than four DMs for QPSK we may use a higher-order constellation, say 8-PSK to get eight DMs and instead of taking a subset of  $\mathcal{E}$  as a set of DMs we consider QPSK signals as a subset of 8-PSK, which results in QPSK associated with eight DMs. The above four matrices are normalized to have a unity average energy and are then used in our investigations relying on the QPSK constellation.

*Example 2 :* In this design example we invoke the DMs obtained in *Example 1* for BPSK signaling. A straightforward approach is to view the BPSK signal set as a subset of the QPSK constellation, while retaining all four DMs given in  $\mathcal{E}$  of *Example 1* above. This will give a coding gain of  $G = 1$ . However, we can generate DMs that are capable of attaining a better coding gain for a BPSK signal set by optimizing the DMs for achieving the maximum attainable coding gain, which yields the following set of matrices

$$\left\{ \begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & j \\ 1 & -j \end{bmatrix} \begin{bmatrix} j & 1 \\ -j & j \end{bmatrix} \begin{bmatrix} -j & 1 \\ -j & -j \end{bmatrix} \right\}$$

resulting in  $G = 2$ , when used for the BPSK signaling set. In other words, four matrices from  $\mathcal{C}$  are chosen in conjunction with the BPSK constellation that gives the maximum attainable coding gain.

The following set of matrices is obtained in a similar way for the  $Q = 2$  case that gives a coding gain of  $G = 4$ :

$$\left\{ \begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ j & -1 \end{bmatrix} \right\}$$

#### IV. RESULTS AND DISCUSSIONS

In this section we compare the performance of the proposed FEC-DM scheme to that of the existing CO-DM scheme, while considering both BPSK and QPSK constellations. For both constellations,  $Q = 2$  and  $Q = 4$  dispersion matrices are considered and the Symbol Error Rate (SER) performance is evaluated. We also provide the coding gain comparison of the proposed FEC-DM scheme and of the CO-DM scheme considering both of the above-mentioned constellations. The coding gains of the various schemes that appear in this paper are computed using numerical simulations. Furthermore, while considering a SER of  $10^{-t}$ , we have used at least  $10 \times 10^t$  symbols in our simulations.

For the FEC-DM scheme, we employ the DMs given in *Example 1* in conjunction with the QPSK constellation and the CO-DMs given in *Example 2* for the BPSK constellation. For the CO-DM scheme we used the DMs optimized for QPSK in [1] in conjunction with both BPSK and QPSK constellations. These are given by

$$\mathbf{A}_1 = \begin{bmatrix} 0.0002 + j0.1810 & 0.8053 + j0.0538 \\ -1.0650 - j0.3093 & -0.2929 + j0.0047 \end{bmatrix}$$

$$\mathbf{A}_2 = \begin{bmatrix} -0.0945 + j0.9968 & -0.6147 + j0.0826 \\ 0.1045 - j0.1268 & -0.7007 - j0.3077 \end{bmatrix}$$

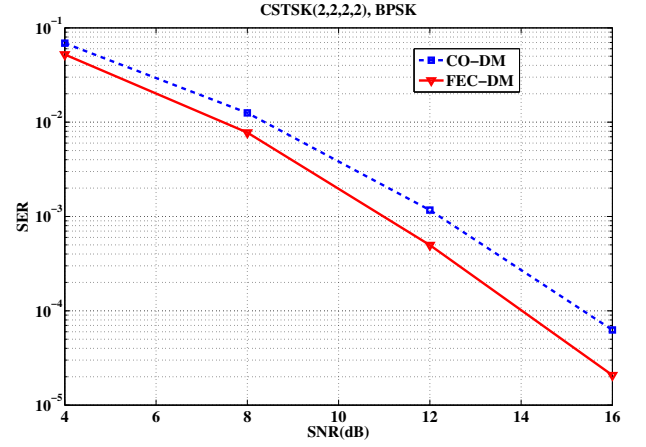


Fig. 1. SER performance curves of FEC-DM and CO-DM in CSTSK(2,2,2,2), BPSK ( $R = 1$ )

$$\mathbf{A}_3 = \begin{bmatrix} -0.8263 - j0.2239 & 0.2992 + j0.6753 \\ 0.0804 + j0.0062 & -0.8362 + j0.1261 \end{bmatrix}$$

$$\mathbf{A}_4 = \begin{bmatrix} -0.4286 - j0.1219 & -0.4714 - j0.2877 \\ -0.5521 - j0.5868 & -0.0195 + j0.9203 \end{bmatrix}.$$

For a Rayleigh fading channel, the upperbound of the average Pair wise symbol Error Probability (PEP) [10] is given by

$$\text{PEP} \leq \left( \frac{1}{\det(\mathbf{I}_M + \frac{\rho}{4} \Delta \Delta^H)} \right)^N, \quad (11)$$

where  $\rho$  is the SNR as defined earlier,  $\Delta = \mathbf{X} - \hat{\mathbf{X}}$  being the code word error matrix such that  $\mathbf{X}$  is the transmitted ST matrix and  $\hat{\mathbf{X}} \neq \mathbf{X}$  is the wrongly decoded ST matrix at the receiver. With  $\rho' = \rho/4$ , the term in the right hand side of eqn.(11) may be written as

$$\det(\mathbf{I}_M + \rho' \Delta \Delta^H) = 1 + \rho' \text{tr}(\Delta \Delta^H) + \dots$$

$$\dots + (\rho')^M \det(\Delta \Delta^H). \quad (12)$$

It may be inferred from eqn.(12) that the PEP is sensitive to the Euclidian distance between the transmitted ST matrices at low values of SNR and to the coding gain at high values of SNR. Thus a set of ST matrices with higher coding gain is expected to perform better than the lower ones at high SNRs.

##### A. Performance of BPSK modulation

When considering the family of CSTSK(2,2,2, $Q$ ) schemes and BPSK combined with  $Q = 2$  and  $Q = 4$ , the coding gains offered by the DMs of *Example 2* and those of the CO-DM scheme are tabulated as follows

Scheme	$Q = 2$	$Q = 4$
CO-DM [1]	1.3363	0.5521
FEC-DM	4	2

*Remark 1 :* It is clear from the table that the coding gain offered by the proposed FEC-DM scheme is higher than that offered by the existing CO-DM scheme. Hence, due to its

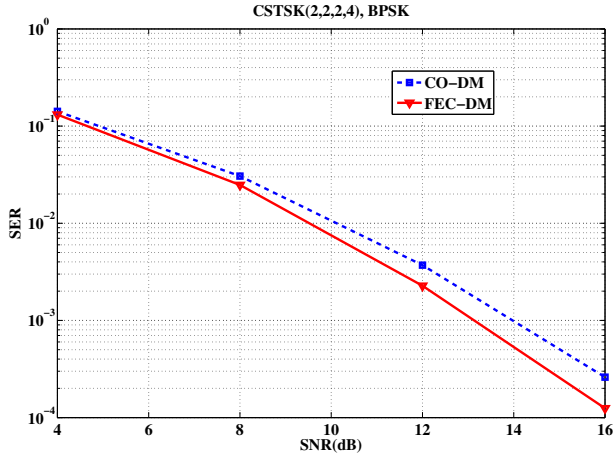


Fig. 2. SER performance curves of FEC-DM and CO-DM in CSTSK(2,2,2,4), BPSK ( $R = 1.5$ )

higher coding gain we can expect the proposed scheme to perform better than the CO-DM scheme at high SNRs.

Fig. 1 and Fig. 2 characterize the SER performance of both the proposed scheme and of the existing scheme in conjunction with BPSK for  $Q = 2$  and  $Q = 4$ , respectively. We observe that the proposed FEC-DM scheme outperforms the CO-DM scheme in both cases at all SNRs. Performance improvement at low SNRs is attributed to the suboptimality of QPSK-optimized DMs for BPSK constellation and that at high SNRs is due to higher coding gain. The SNR improvement of the FEC-DM scheme over the CO-DM scheme for  $Q = 2$  was about 1.5dB at a SER of  $10^{-4}$  and for  $Q = 4$  case it is about 1dB at the SER of  $10^{-3}$ .

#### B. Performance of QPSK modulation

The following table summarizes the coding gains offered by the proposed scheme using the DMs given in *Example 1* and those of the CO-DM scheme for CSTSK(2,2,2,2), 4-PSK ( $R = 1.5$ ) and CSTSK(2,2,2,4), 4-PSK ( $R = 2$ ).

Scheme	$Q = 2$	$Q = 4$
CO-DM [1]	0.4788	0.1882
FEC-DM	1	1

*Remark 2* : It is clear from the table that upon increasing  $Q$ , the coding gain of CO-DM is reduced, while that offered by the proposed scheme remains constant, as a benefit of its specific design. Thus, the proposed FEC-DM scheme is expected to outperform the CO-DM scheme at high rates or throughputs.

Fig. 3 and Fig. 4 characterize the SER performance of both the proposed as well as of the existing scheme in conjunction with the QPSK constellation for the  $Q = 2$  and  $Q = 4$  cases, respectively. In the  $Q = 2$  scenario the proposed FEC-DM scheme performs better than the existing CO-DM scheme for SNRs higher than about 17dB. In the  $Q = 4$  case the proposed scheme exhibits an SNR gain of about 1dB over the existing scheme. Thus, upon increasing the rate the relative

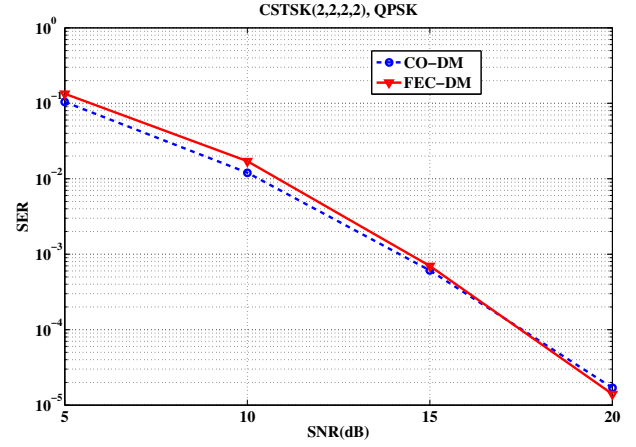


Fig. 3. SER performance curves of FEC-DM and CO-DM in CSTSK(2,2,2,2), QPSK ( $R = 1.5$ )

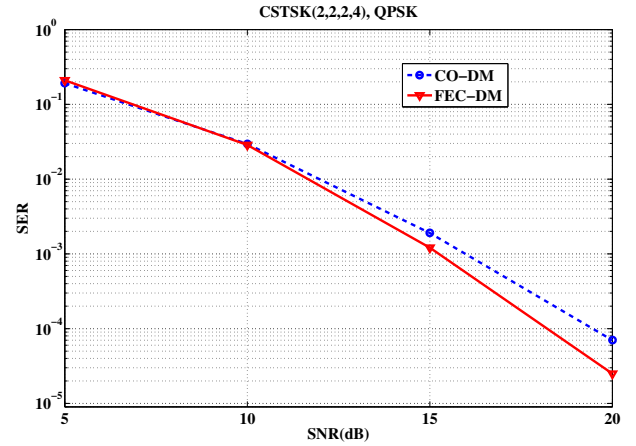


Fig. 4. SER performance curves of FEC-DM and CO-DM in CSTSK(2,2,2,4), QPSK ( $R = 2$ )

performance gain of the proposed scheme with respect to the CO-DM scheme becomes higher.

## V. CONCLUSIONS

Dispersion matrices have been proposed for the PSK signal set of CSTSK schemes by providing a systematic construction method using FE codes. The proposed FEC-DMs exhibited full diversity and a beneficial coding gain. It was shown using simulation results that the proposed scheme is capable of outperforming the existing CO-DM scheme with optimal DMs in the medium to high SNR region and the relative performance gain of the proposed scheme with respect to the existing CSTSK regime is expected to increase at high rates.

## VI. APPENDIX

### REVIEW OF FIELD EXTENSION CODES

For the sake of completeness, we briefly highlight code construction using Field Extensions with the aid of an example and then present their generalized form [7], [8].



The field of reals,  $\mathbb{R}$ , can be extended by appending an element which is not an element of  $\mathbb{R}$ , for example,  $\mathbb{C}$  is a degree-2 extension of  $\mathbb{R}$  with  $(1, j)$  as the basis. The element  $j \notin \mathbb{R}$  is a root of  $x^2 + 1 = 0$ , which is an irreducible polynomial over  $\mathbb{R}$ . Thus, the roots of any irreducible polynomial over the base field can be chosen as the set of basis elements of the extended field. Every element  $k \in \mathbb{C}$  is associated with a unique matrix in  $\mathbb{R}^{2 \times 2}$ , where the association is established by the map  $\lambda_k : u \mapsto ku$  for any  $u \in \mathbb{C}$ . Hence, with the aid of  $k = k_r + jk_i$ ,  $u = u_r + ju_i$ , we get  $ku = (k_ru_r - k_iu_i) + j(k_iu_r + k_ru_i)$ . In the basis form this is written as

$$\begin{bmatrix} k_ru_r - k_iu_i \\ k_iu_r + k_ru_i \end{bmatrix} = \underbrace{\begin{bmatrix} k_r & -k_i \\ k_i & k_r \end{bmatrix}}_{\text{unique matrix associated with } k} \begin{bmatrix} u_r \\ u_i \end{bmatrix}.$$

The unique matrix associated with  $k$  may be written as

$$\begin{bmatrix} k_r & -k_i \\ k_i & k_r \end{bmatrix} = k_r \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + k_i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

For a general polynomial,  $x^2 + a_0 = 0$ , the associated unique matrix of  $k$  is given by

$$\begin{bmatrix} k_r & -k_i \\ k_i & k_r \end{bmatrix} = k_r \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + k_i \begin{bmatrix} 0 & -a_0 \\ 1 & 0 \end{bmatrix}.$$

The generalization of this is as follows. Consider the following chain of field extensions,

$$\mathbb{Q} \subset \mathbb{Q}(S) = F \subset \mathbb{Q}(S, \alpha) = F(\alpha) = K, \quad (13)$$

where  $\mathbb{Q}$  is a field of rational numbers,  $S \subset \mathbb{C}$  represents the  $L$ -symbol constellation,  $F$  is the field generated by extending  $\mathbb{Q}$  over  $S$ , and  $K$  is the  $n$ th degree extension of  $F$  over  $\alpha$ , for some  $\alpha \in K$  that is algebraic over  $F$  i.e., for some irreducible monic polynomial  $p(x) \in F[x]$ ,  $p(\alpha) = 0$ . Let  $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ . Any  $k \in K$  may be written as  $\sum_{i=0}^{n-1} f_i\alpha^i$ , where the coefficients  $f_i$ 's are from  $F$ . Then the natural map  $P$  from  $K$  to  $\text{End}_F(K)$  is given by  $k \mapsto \lambda_k$ , where  $\lambda_k$  maps any  $v \in K$  to the element  $kv$  i.e.,  $P$  embeds  $K$  in  $M_n(F)$  [7]. Then the matrix corresponding to  $\lambda_\alpha$  is given by its companion matrix as

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}. \quad (14)$$

Matrices corresponding to higher powers of  $\alpha$  are simply obtained by raising  $\mathbf{M}$  to the corresponding powers. Thus we have

$$f_0\mathbf{I}_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \dots + f_{n-1}\mathbf{M}^{n-1} \quad (15)$$

corresponding to  $\sum_{i=0}^{n-1} f_i\alpha^i$ . This gives a set of matrices  $\mathcal{C}$  for all  $f_i$  in  $F$ , with  $|\mathcal{C}| = L^n$  for  $F = S$ . If  $K$  is a division algebra, then  $\mathcal{C}$  will be a matrix ring, and the difference of any two matrices in this set lies in the set and will be of full rank [8]. The coding gain of this code is [8]

$$G = \min_{\mathbf{c}, \mathbf{c}' \in \mathcal{C}} |\det(\mathbf{B}(\mathbf{c}, \mathbf{c}'))|^{2/n} \\ = \min_{\mathbf{c}, \mathbf{c}' \in \mathcal{C}} \left| N_{K/F} \left( \sum_{i=0}^{n-1} (f_i - f'_i) \alpha^i \right) \right|^{2/n}, \quad (16)$$

where  $\mathbf{B}(\mathbf{c}, \mathbf{c}') = \mathbf{J}(\mathbf{c}, \mathbf{c}')^H \mathbf{J}(\mathbf{c}, \mathbf{c}')$ ,  $\mathbf{J}(\mathbf{c}, \mathbf{c}')$  is the code difference matrix of  $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ ,  $N_{K/F}(a)$  denotes the norm of element  $a$  from  $K$  to  $F$ , and  $\mathbf{c} = \sum_{i=0}^{n-1} f_i \mathbf{M}^i$ ,  $\mathbf{c}' = \sum_{i=0}^{n-1} f'_i \mathbf{M}^i$  with  $f_i$  and  $f'_i$  from  $F$ .

If we restrict  $p(x)$  to be of the form  $x^n - \gamma$ , where  $\gamma \in F^*$  (non-zero elements of  $F$ ), then from eqn.(15) the matrix corresponding to  $\lambda_k$  is of the form

$$\begin{bmatrix} f_0 & \gamma f_{n-1} & \gamma f_{n-2} & \dots & \gamma f_1 \\ f_1 & f_0 & \gamma f_{n-1} & \dots & \gamma f_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \dots & f_0 \end{bmatrix}. \quad (17)$$

For  $\gamma = \omega_L^b$ , where  $\omega_L$  is  $e^{j2\pi/L}$  and  $b$  is some integer,  $x^n - \omega_L^b$  is irreducible over  $F$ , if  $L$  and  $b$  are relative primes and if the set of prime factors of  $L$  forms a subset of the set of prime factors of  $n$  [8]. In other words, if prime factorizations of  $L$  and  $n$  are  $p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$  and  $p_1^{\beta_1} p_2^{\beta_2} \dots p_{k'}^{\beta_{k'}}$  respectively for some  $\delta_i$  and  $\beta_i$  values, then the above polynomial is irreducible if  $\{p_1, p_2, \dots, p_k\} \subseteq \{p_1, p_2, \dots, p_{k'}\}$ . This generates Cyclotomic Field Extensions over  $F$ . We use code constructions relying on the polynomial  $x^n - \omega_L^b$  in our example constructions.

## REFERENCES

- [1] S. Sugiura, S. Chen and L. Hanzo, "Coherent and differential space-time shift keying: A dispersion matrix approach," *IEEE Transactions on Communications*, vol. 58, no. 11, pp. 3219–3230, 2010.
- [2] S. Sugiura, S. Chen and L. Hanzo, "Generalized space-time shift keying designed for flexible diversity-, multiplexing- and complexity- tradeoffs," *IEEE Transactions on Communications*, accepted for publication.
- [3] R. Mesleh, H. Haas, C. Ahn, and S. Yun "Spatial modulation - a new low complexity spectral efficiency enhancing technique," in *Proc. First International Conf. Commun. Netw., Beijing, China.*, pp. 1-5, Oct. 2006.
- [4] R. Mesleh, H. Haas, S. Sinanovic, C. Ahn, and S. Yun "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228-2242, 2008.
- [5] J. Jeganathan, A. Ghrayeb, "Space shift keying modulation for MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3692–3703, 2009.
- [6] S. Sandhu, R. Nabar, D. Gore and A. Paulraj, "Introduction to Space-Time codes," <http://www.stanford.edu/group/sarg/sandhu062503.pdf>.
- [7] V. Shashidhar, K. Subrahmanyam, R. Chandrasekharan, B. S. Rajan, and B. A. Sethuraman, "High-rate, full-diversity STBCs from field extensions," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, June 29 to July 4, p. 126, 2003.
- [8] B. A. Sethuraman, B. Sundar Rajan, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2596–2616, 2003.
- [9] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," *IEEE Transactions on Information Theory*, vol. 48, pp. 1804–1824, July 2002.
- [10] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744-765, 1998.
- [11] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Spatial modulation: optimal detection and performance analysis," *IEEE Commun. Lett.*, vol. 12, no. 8, pp. 545-547, 2008.