Explicit, Minimum-Delay Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff

Petros Elia
P. Vijay Kumar
Department of EE-Systems
University of Southern California
Los Angeles, CA 90089, USA
Email: {elia,vijayk}@usc.edu

K. Raj Kumar
Sameer A. Pawar
Electr. Comm. Engineering Dept.
Indian Institute of Science
Bangalore, 560 012, India
Email: {raj,sameerp}@ece.iisc.ernet.in

Hsiao-feng Lu
Dept. of Comm. Engineering
National Chung-cheng University
160 San-Hsing, Min-Hsiung, Chia-Yi 621
Taiwan, R.O.C.
Email: francis@ccu.edu.tw

***Abstract*— In the recent landmark paper of Zheng and Tse it is shown that there exists a fundamental tradeoff between diversity gain and multiplexing gain, referred to as the Diversity-Multiplexing gain(D-MG) tradeoff.**

The present paper presents the first explicit construction of space-time (ST) codes for arbitrary number of transmit antennas that achieve the D-MG tradeoff. It is shown here that ST codes with non-vanishing determinant (NVD) constructed from cyclic-division-algebras (CDA), are optimal under the D-MG tradeoff for any number n_t, n_r of transmit and receive antennas and with minimum delay $T = n_t$. The full result shows optimality of a wider class of constructions. CDA-based ST codes with NVD have previously been constructed for restricted values of n_t. A unified construction of D-MG optimal CDA-based ST codes with NVD is given here, for any number n_t of transmit antennas.

The results also establish that for any n_t, n_r, the D-MG tradeoff at $T = n_t$ is the same as that for $T \geq n_t + n_r - 1$.

In addition, we also show that the CDA based ST constructions achieve the optimal D-MG tradeoff of a wider class of channels.

I. Introduction

Quasi-Static Channel Model: Consider the Rayleigh-fading ST channel with quasi-static interval T, n_t transmit and n_r receive antennas. The received signal matrix Y is given by

$$Y \;=\; HX + W \tag{1}$$

where X is the transmitted code matrix $(n_t \times T)$ drawn from a ST code $\mathcal{X}$, H the $(n_r \times n_t)$ channel matrix and W the $(n_r \times T)$ noise matrix. The entries of H and W are assumed to be i.i.d., circularly symmetric complex Gaussian $\mathbb{C}\mathcal{N}(0,1)$ random variables. The entries of X are drawn from a constellation whose size scales with SNR and it is ensured that

$$\mathbb{E}(\|X\|_F^2) = T \text{ SNR}. \tag{2}$$

D-MG Tradeoff: In a recent landmark paper, Zheng and Tse [1] showed that there exists a fundamental tradeoff between diversity and multiplexing gain, referred to as the D-MG tradeoff. For large SNR, the ergodic capacity of the ST channel model in (1) is given by $C \approx \min\{n_t, n_r\}\log(\text{SNR})$. The ST code $\mathcal{X}$ transmits $R = \frac{1}{T}\log(|\mathcal{X}|)$ bits per channel use. Let r be the normalized rate given by $R = r\log(\text{SNR})$. Thus a ST code achieving normalized rate r has size

$$|\mathcal{X}| \;=\; \text{SNR}^{rT}. \tag{3}$$

It follows that the maximum achievable multiplexing gain equals $r = \min\{n_t, n_r\}$. Following [1], we will refer to r as the *multiplexing gain*. The *diversity gain* corresponding to a normalized rate r is defined by

$$d(r) \;=\; -\lim_{\text{SNR}\to\infty} \frac{\log(P_e)}{\log(\text{SNR})},$$

where P_e denotes the probability of codeword error. In [1], for a fixed integer multiplexing gain r, and $T \geq n_t + n_r - 1$, the maximum achievable diversity gain $d(r)$ is shown to be

$$d(r) \;=\; (n_t - r)(n_r - r). \tag{4}$$

The plot (see Fig. 1) for non-integral values is obtained through straight-line interpolation. For $T < n_t + n_r - 1$ only upper and lower bounds on the maximum possible $d(r)$ are available [1].

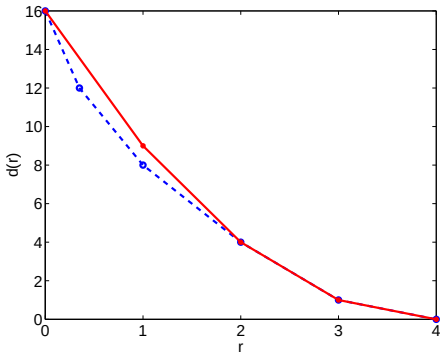

Fig. 1. *Upper and Lower Bounds on D-MG Tradeoff* $(n_t = n_r = 4)$.

Prior Work: The results in [1] spurred research activity worldwide and considerable recent progress has been made

in constructing D-MG optimal codes. These include the Yao-Wornell [4] and the Golden Code [7] constructions of D-MG optimal minimal-delay ST codes for two transmit antennas, and the Lattice-based Space-Time (LAST) codes in [5] that achieve the D-MG tradeoff for $T \geq n_t + n_r - 1$ but involve code construction from a random lattice.

In [11], a sufficient condition for D-MG optimality similar to the one presented in this paper is given, although derived using a different approach. The criterion is stated in terms of a constraint on the singular values of the codeword difference matrix. The sufficient criteria in [11] (termed as the approximate universality condition) is independent of the channel statistics in that it ensures that the error probability of any ST scheme that meets these criteria will achieve the outage curve of the respective channel. They then exhibit an explicit construction of approximately universal MIMO codes for one or two receive antennas.

We use the approximate criteria provided in [11] to show that the CDA based constructions in this paper are approximately universal in section IX.

Results: The principal result of the present paper, is to give a sufficient condition for a space-time code $\mathcal{X}$ having $n_t \leq T$ to achieve the optimal D-MG tradeoff for any number n_r of receive antennas. Space-time codes with non-vanishing determinant (NVD) constructed out of suitable CDA are instances of codes that meet the above mentioned criteria and hence achieve the D-MG tradeoff.

However, constructions for CDA-based ST codes with NVD exist in the literature only for certain restricted values of n_t. A second major contribution of the paper is a unified construction of CDA-based ST codes with NVD for any number n_t of transmit antennas.

Taken together, the two results represent an explicit construction of ST codes with minimum possible delay $T = n_t$, optimal under the D-MG tradeoff, for any number n_t, n_r of transmit and receive antennas. They also establish that for any n_t, n_r, the D-MG tradeoff at $T = n_t$ is the same as that established in [1] for $T \geq n_t + n_r - 1$.

II. Achieving the Optimal D-MG Tradeoff

Consider a maximal rank space-time code $\mathcal{X}$ with $n_t = T$ and entries drawn from an alphabet $\mathcal{A} \subseteq \mathbb{C}$. From (3), we have that $|\mathcal{X}| = SNR^{Tr}$ and from the Singleton bound that $|\mathcal{X}| = |\mathcal{A}|^T = SNR^{Tr} \Rightarrow |\mathcal{A}| = SNR^r$

Theorem 1: (Main Theorem) Consider a maximal rank $n_t \times T$ space-time code $\mathcal{X}$ $(T \geq n_t)$. Let ΔX denote the difference of any two code-matrices drawn from $\mathcal{X}$. Define $\min_{\Delta X} \det(\Delta X \Delta X^\dagger) := SNR^{\delta}$. If the minimum determinant of $\mathcal{X}$ satisfies

$$\delta = n_t - r$$

then $\mathcal{X}$ is optimal with respect to the D-MG tradeoff for any number of receive antennas.

Proof: Provided below following preliminaries. ∎

In the sequel, define $n' := \min(n_t, n_r)$. For clarity of presentation, we also set $n := n_t$.

Expression for Euclidean Distance: Let $\Delta X = X_i - X_j$ be the difference of any two signal matrices from $\mathcal{X}$. Let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ and $l_1 \geq l_2 \geq \cdots \geq l_n$ be the ordered eigenvalues of $H^\dagger H$ and $\Delta X \Delta X^\dagger$ respectively and d_E^2 be the squared Euclidean distance.

Lemma 2: (*Mismatched Eigenvalue Bound*) For a given channel realization H and a particular ΔX, the squared Euclidean distance $d_E^2 = \|H\Delta X\|_F^2$ is lower bounded by

$$d_E^2 = Tr(H\Delta X \Delta X^\dagger H^\dagger) \geq \sum_{i=1}^{n} \lambda_i l_i$$

where Tr denotes the trace function.

Proof: Omitted for lack of space, see [2]. ∎

Thus d_E^2 is lower bounded by the "mismatched" inner-product of the $\{\lambda_i\}$ and $\{l_j\}$.

Bounds on the Eigenvalues of $\Delta X \Delta X^\dagger$: In the ST codes under consideration here, the code difference matrix ΔX is always of full rank i.e., rank n. Let $Tr_{\max} := \max_{\Delta X}\{Tr(\Delta X \Delta X^\dagger)\}$ and $\det_{\min} := \min_{\Delta X}\{\det(\Delta X \Delta X^\dagger)\}$ be the maximum and minimum values of the trace and determinant of $\Delta X \Delta X^\dagger$ respectively. Define $l_i = \text{SNR}^{-\beta_i}$ $\forall$ i. We have $\det_{\min} \dot{\geq} \text{SNR}^{\delta}$, where $\dot{=}$, $\dot{\geq}$ and $\dot{\leq}$ denote exponential equality and inequalities respectively [1]. Using (2), the fact that $Tr(\Delta X \Delta X^\dagger) = \|\Delta X\|_F^2 \dot{\leq} \text{SNR}$ and that $\sum_{i=1}^{n} l_i \leq Tr_{max}$ and $\prod_{i=1}^{n} l_i \geq \det_{\min}$, leads to the following bounds for each $j = 0, 1, \cdots, n' - 1$:

$$\prod_{i=n-j}^{n} l_i \dot{\geq} \frac{(\text{SNR}^{\delta})}{\text{SNR}^{(n-j-1)}} \Rightarrow -\sum_{i=n-j}^{n} \beta_i \geq \delta - (n-j-1) \quad (5)$$

Proof of Theorem 1: For $j = 0, 1, ..., n'-1$, Lemma 2 gives

$$d_E^2 \geq \sum_{i=1}^{n} \lambda_i l_i \geq \sum_{i=n-j}^{n} \lambda_i l_i \quad (6)$$

We have thus expanded a single inequality into a set of n' inequalities. Let $\lambda_i := \text{SNR}^{-\alpha_i}$ with $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. Applying the arithmetic mean-geometric mean (AM-GM) inequality to the n' inequalities in (6), we get,

$$\begin{aligned} d_E^2 &\geq (j+1) \prod_{i=n-j}^{n} \lambda_i^{\frac{1}{j+1}} \prod_{i=n-j}^{n} l_i^{\frac{1}{j+1}} \\ &\doteq \text{SNR}^{-\frac{1}{j+1}\left[\sum_{i=n-j}^{n} \alpha_i + \sum_{i=n-j}^{n} \beta_i\right]} \end{aligned} \quad (7)$$

for $0 \leq j \leq n' - 1$. Let $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n)$. Then for a given channel realization, i.e., a given $\underline{\alpha}$, we obtain from (5) and (7), the following lower bound

$$d_{E,min}^2(\underline{\alpha}) \dot{\geq} \text{SNR}^{\,1 - \frac{n-\delta}{j+1} - \sum_{i=n-j}^{n} \left[\frac{\alpha_i}{j+1}\right]}, \quad j = 0, \cdots, n' - 1$$

By hypothesis, $r = n - \delta$ hence $d_{E,min}^2(\underline{\alpha}) \dot{\geq} \text{SNR}^{\,\Delta_j(\underline{\alpha})}$ where $\Delta_j(\underline{\alpha}) = 1 - \frac{r}{j+1} - \sum_{i=n-j}^{n} \left[\frac{\alpha_i}{j+1}\right]$.

Using the sphere bound and the fact that the square of the Frobenius norm of the noise matrix $\|W\|_F^2$ is a chi-squared

random variable in $2n_rT$ dimensions, we obtain

$$P_e(\underline{\alpha}) \quad \leq \quad e^{-\frac{d^2_{E,min}(\underline{\alpha})}{4}} \sum_{k=0}^{n_rT-1} \frac{\left[\frac{d^2_{E,min}(\underline{\alpha})}{4}\right]^k}{k!} = \Gamma(\underline{\alpha}) \text{(say)}$$

Next, the joint probability density function (pdf) of the ordered eigenvalues λ_i of $H^\dagger H$ for $n_r \geq n_t$ is given [1] by

$$p(\underline{\alpha}) = K\left[\log(\text{SNR})\right]^{n'} \prod_{i=1}^{n'} (\text{SNR})^{-(|n_r-n_t|+1)\alpha_i} \cdot \prod_{i<j} \left(\text{SNR}^{-\alpha_i} - \text{SNR}^{-\alpha_j}\right)^2 \exp\left[-\sum_{i=1}^{n'} \text{SNR}^{-\alpha_i}\right]$$

for some constant K. Averaging over the ordered eigenvalues of $H^\dagger H$ leads to $P_e \leq \int_{\underline{\alpha}} \Gamma(\underline{\alpha}) p(\underline{\alpha}) d\underline{\alpha}$.

For any $\alpha_i < 0$ and any $\Delta_j > 0$, the integrand contains a term that decays with SNR exponentially [2]. Thus at high SNR we can ignore the integral over the range of $\underline{\alpha}$ with any $\alpha_i < 0$ or any $\Delta_j > 0$. The range of integration is then restricted to $\mathcal{B} = \{\underline{\alpha} : \alpha_i \geq 0 \forall\ i\ , \Delta_j \leq 0, j = 0, \cdots, n'-1\}$ i.e.,

$$P_e \doteq \int_{\mathcal{B}} \text{SNR}^{-\sum_{i=1}^{n}(2i-1+|n_r-n_t|)\alpha_i} d\underline{\alpha} = \text{SNR}^{-d(r)}.$$

It follows that, $d(r) \geq \inf_{\underline{\alpha}\in\mathcal{B}} \sum_{i=1}^{n}(2i-1+|n_r-n_t|)\alpha_i$. It can be shown that evaluation of the above infimum at integral values $r = k$ for $k = 0, 1, \cdots, n'$ yields $d(k) \geq (n_r-k)(n-k)$ and that the values for non-integral r are obtained by straight line interpolation as with the optimal tradeoff curve $d^*(r)$ derived in [1]. □

It will be shown in the sequel that CDA-based ST codes ($n_t = T$) with NVD satisfy all the requirements of Theorem 1 and therefore are D-MG optimal. We now turn to their construction.

III. Signal Alphabet and Energy for the CDA-based space-time codes

Throughout the paper, all our constructions of ST codes will be for the case of $T = n_t := n$. For clarity of exposition, we will assume the following space-time channel model with n_t transmit and n_r receive antennas in the sequel:

$$Y = \theta HX + W.$$

X is drawn from a space-time code $\mathcal{X}$ and the entries of H and W are assumed to be i.i.d. circularly symmetric $\mathbb{CN}(0,1)$ as before. θ is chosen to ensure

$$\mathbb{E}(\|\theta X\|_F^2) = T.SNR \tag{8}$$

Signal Alphabet: Consider a base alphabet $\mathcal{A}$ that can be scaled with SNR in such a way that $|\ \mathcal{A}(\text{SNR})\ | \doteq \text{SNR}^{\frac{r}{n_t}}$. Thus for $a \in \mathcal{A}(\text{SNR})$ we have $|\ a\ |^2 \doteq \text{SNR}^{\frac{r}{n_t}}$.

Example *1: QAM Constellation*

$$\mathcal{A}_{\text{QAM}} = \{a + \imath b \ \mid -M+1 \leq a, b \leq M-1,\ a, b \text{ odd }\}$$

with M^2 elements, where $M^2 = \text{SNR}^{\frac{r}{n_t}}$.

We will call a ST code $\mathcal{X}$ *$\mathcal{A}$-linear* , if every entry X_{ij} of each code matrix X is of the form $X_{ij} = \sum_{k=1}^{m} c_{ijk}\alpha_{ijk}$, $c_{ijk} \in \mathcal{A}$, for some m, and for some fixed set of complex numbers $\{\alpha_{ijk}\}$ which do not vary with SNR. The code $\mathcal{X}$ is said to be *full-rate* if $|\ \mathcal{X}\ | = |\ \mathcal{A}\ |^{n_tT} = \text{SNR}^{rT}$. Thus, a full-rate ST code matrix X conveys $r\log(\text{SNR})$ bits of information per channel use.

Signal Energy: For an $\mathcal{A}$-linear ST code $\mathcal{X}$, we have,

$$||X||_F^2 \quad \leq \quad \sum_{i,j=1}^{n}\sum_{k=1}^{m} |\ c_{ijk}\ |^2\ |\ \alpha_{ijk}\ |^2 \dot{\leq} \text{SNR}^{\frac{r}{n}}$$

since α_{ijk} are fixed and independent of the SNR and $|c_{ijk}|^2 \dot{\leq} \text{SNR}^{\frac{r}{n}}$. From (8), it follows that a valid choice of θ^2 is

$$\theta^2 \doteq \text{SNR}^{1-\frac{r}{n}}.$$

IV. CDA based ST-code construction

Let $n \geq 2$ be an arbitrary integer. In this paper we will construct CDA-based ST codes $\mathcal{X}$ with $n_t = T = n$ that are $\mathcal{A}$-linear over the alphabet $\mathcal{A}_{QAM}$. Code matrices in the CDA-based ST code correspond to left-regular representations of elements of a subset of a division algebra. Details on division algebra based ST codes can be found in [6].

The construction of a CDA-based ST code calls for a cyclic field extension L/F (where L, F are number fields) and for a parameter γ (henceforth referred to as a "non-norm" element) such that the smallest power t of γ for which γ^t is the norm over F of an element in L equals n. In [6], γ is chosen to be transcendental over L, whereas in [7], [9], γ is an algebraic integer in F. The latter choice can potentially ensure that the magnitude of the determinant $\det(\Delta X \Delta X^\dagger)$ of the difference ΔX of any pair of distinct code matrices in the ST code $\mathcal{X}$, is bounded away from 0 even in the limit as SNR $\to \infty$. Such a ST code is said to have the non-vanishing determinant (NVD) property [7], [9].

Finding suitable fields F and L and non-norm element γ had only been accomplished for a few specific values of n_t, see [7], [9], [10]. A general technique for constructing cyclic extensions and identifying non-norm elements that hold for all n_t is given in Sections VI, VII.

In brief, our construction begins by choosing $F = \mathbb{Q}(\imath)$ and the n-degree cyclic field extension L/F as described in Section VI. For $\mathcal{O}_L$ the integral closure of $\mathbb{Z}[\imath]$ in L, we let $\beta_i, i = 1, \cdots, n$ be an integral basis for $\mathcal{O}_L/\mathbb{Z}[\imath]$. For σ the generator of the Galois group $\text{Gal}(L/F)$ we introduce a symbol z such that $\ell z = z\sigma(\ell) \quad \forall\ \ell \in L$ and $z^n = \gamma$ for a "non-norm" $\gamma \in F^*$. The cyclic division algebra $D(L/F, \sigma, \gamma)$ is then $D = L \oplus zL \oplus \ldots \oplus z^{n-1}L$. A ST code $\mathcal{X}$ can be associated to D by selecting the set of matrices corresponding to the left-regular representation of elements of a finite subset D_1 of D having the representation

$$D_1 = L_1 \oplus zL_1 \oplus \ldots \oplus z^{n-1}L_1,$$

where $L_1 = \sum_{i=1}^{n} a_i\beta_i, \quad a_i \in \mathcal{A}_{\text{QAM}} \subseteq \mathcal{O}_F = \mathbb{Z}[\imath]$. Then each code-matrix X is of the form

$$X = \begin{bmatrix} \ell_0 & \gamma\sigma(\ell_{n-1}) & \dots & \gamma\sigma^{n-1}(\ell_1) \\ \ell_1 & \sigma(\ell_0) & \dots & \gamma\sigma^{n-1}(\ell_2) \\ \vdots & \vdots & \vdots & \vdots \\ \ell_{n-1} & \sigma(\ell_{n-2}) & \dots & \sigma^{n-1}(\ell_0) \end{bmatrix} \tag{9}$$

where $\ell_i \in L_1$. Thus the elements of each code-matrix X are of the form $X_{ij} = \sum_{k=1}^{n} e_{ij,k}\alpha_{ijk}, \quad e_{ijk} \in \mathcal{A}_{\text{QAM}}, \alpha_{ijk} \in \mathbb{C}$. The alphabet of the ST code is clearly $\mathcal{A}_{\text{QAM}}$-linear and the ST code is also full-rate with respect to $\mathcal{A}_{\text{QAM}}$. The determinant of the difference of any two code matrices belongs to $F \bigcap \mathcal{O}_L = \mathcal{O}_F = \mathbb{Z}[\imath]$, see [8] for details. If ΔX denotes the difference of any two code matrices drawn from $\mathcal{X}$, we therefore have,

$$\det_{min}(\Delta X \Delta X^{\dagger}) \doteq \text{SNR}^0, \tag{10}$$

i.e. the non-vanishing determinant property holds.

V. Optimality of the CDA construction

Theorem 3: Square space-time codes ($n_t = T$) constructed from cyclic division algebras which have the non-vanishing determinant property are optimal with respect to the D-MG tradeoff for any number of receive antennas.

Proof: The parameter δ for the CDA construction is $\text{SNR}^{\delta} = \min_{\Delta X} \det[(\theta\Delta X)(\theta\Delta X)^{\dagger}] = \left(\theta^2\right)^n \det_{min}(\Delta X \Delta X^{\dagger})$ and thus from (10) we obtain that $\delta = n_t - r$.

From theorem 1, we therefore conclude that the CDA based space-time codes with NVD achieve the D-MG tradeoff for any number of receive antennas. ∎

Details regarding the construction of cyclic Galois extensions and determining non-norm elements which are key in the construction of cyclic division algebras follow.

VI. Cyclic Extensions and non-norm elements

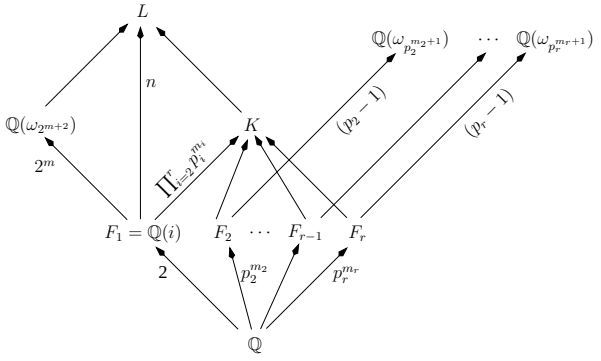

Fig. 2. Construction of cyclic extensions of $\mathbb{Q}(\imath)$ of arbitrary degree.

A systematic means of constructing cyclic Galois extensions of a number field F, of any degree $n = 2^m \prod_{i=1}^{r} p_i^{m_i}$, p_i odd prime is now given. Fig. 2 gives an overview of the method.

Cyclic Extensions of $\mathbb{Q}$: Let ω_m denote a complex, primitive m^{th} root of unity. We construct cyclic extensions over $\mathbb{Q}$ starting from cyclotomic extensions $R = \mathbb{Q}(\omega_m)$. First, we set $F_1 = \mathbb{Q}(\omega_{p_1^{m_1+1}}) = \mathbb{Q}(\imath)$. The Galois group $Gal(F_1/\mathbb{Q})$ is cyclic of degree 2. Next consider $R_i = \mathbb{Q}(\omega_{p_i^{m_i+1}})$, for distinct odd primes p_i, $i = 2, \cdots, r$. Then $R_i/\mathbb{Q}$ is a cyclic extension of degree $\phi(p_i^{m_i+1}) = p_i^{m_i}(p_i - 1)$ [3]. It has a cyclic subgroup $H_i < G_i = Gal(R_i/\mathbb{Q})$ of order $(p_i - 1)$. From Galois theory, there is a unique subfield F_i of R_i fixed by the subgroup H_i. It can be shown that F_i is a cyclic extension of $\mathbb{Q}$ of degree $p_i^{m_i}$ [2].

Cyclic Extensions of $F_1 = \mathbb{Q}(\imath)$: Here we obtain cyclic extensions of F_1 of arbitrary degree n.

Theorem 4: [2] Let $S = S_1 S_2 \cdots S_r$ be the compositum of the fields $S_1, S_2, \cdots, S_r$. If each S_i is a cyclic extension of a field F of degree n_i (where the n_i are pairwise relatively prime), then S is a cyclic extension of F of degree $\prod_{i=1}^{r} n_i$. From the theorem, it follows that $K = F_1 F_2 \dots F_r$ with F_i as defined above and as shown in Fig. 2, is cyclic over $\mathbb{Q}$. Consequently, K/F_1 is cyclic of degree $\prod_{i=2}^{r} p_i^{m_i}$. It is known that $\mathbb{Q}(\omega_{2^{m+2}})/\mathbb{Q}(\imath)$ is cyclic of degree 2^m [3]. A second application of Theorem 4 shows that $L = K\ \mathbb{Q}(\omega_{2^{m+2}})$ is a cyclic extension of arbitrary degree n over $\mathbb{Q}(\imath)$ as desired.

VII. Determining a "non-norm" element

In this section, we provide a procedure for identifying a "non-norm" element γ, i.e., an element $\gamma \in F^*$ satisfying $\gamma^i \notin N_{L/F}(L), i < n$. We make use of a theorem in [10].

Theorem 5: [10] Let K be a degree n Galois extension of a number field F and let $\mathfrak{p}$ be a prime ideal in the ring $\mathcal{O}_F$ below the prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ with norm given by $\|\mathfrak{P}\| = \|\mathfrak{p}\|^f$, where f is the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. If γ is any element of $\mathfrak{p} \setminus \mathfrak{p}^2$, then $\gamma^i \notin N_{K/F}(K)$ for any $i = 1, 2, \cdots, f-1$.

In particular, if $Gal(K/F) =< \sigma >$ with $[K : F] = n$, then the cyclic algebra $(K/F, \sigma, \gamma)$ is a division algebra if $\gamma \in \mathfrak{p} \setminus \mathfrak{p}^2$ for some prime triplet $(p; \mathfrak{p}; \mathfrak{P})$ with $f(\mathfrak{P}|\mathfrak{p}) = n$, where p is the characteristic of $\mathcal{O}_F/\mathfrak{p}$.

In order to find a "non-norm" element γ in $F\mathbb{Q}(\imath)$, it is sufficient to find a prime ideal in $\mathbb{Z}[\imath]$ whose inertial degree f in $L/\mathbb{Q}(\imath)$ is $f = [L : \mathbb{Q}(\imath)] = n$. Such an ideal is said to be inert in $L/\mathbb{Q}(\imath)$. The two lemmas below show the existence of an ideal $q_i\mathbb{Z}$ that is inert in $F_i/\mathbb{Q}$ for $i = 2, \cdots, r$.

Lemma 6: [3] Let q_i be any prime, $q_i \neq p_i$, let $f_i \geq 1$ be the smallest integer such that $q_i^{f_i} \equiv 1 \pmod{p_i^{m_i+1}}$ and let $g_i = \phi(p_i^{m_i+1})/f_i$. Then $A_i q_i = \beta_1 \cdots \beta_{g_i}$ where $\beta_1 \cdots \beta_{g_i}$ are distinct prime ideals of A_i and $N(\beta_j) = q_i^{f_i}$, all j.

Lemma 7: [3] Let p be any odd prime. Then for any $k \in \mathbb{Z}$, $\mathbb{Z}_{p^k}^*$ is cyclic of order $\phi(p^k)$. For any integer f dividing $\phi(p^k)$ there exists an $a \in \mathbb{Z}_{p^k}^*$ such that a has order f in $\mathbb{Z}_{p^k}^*$.

Dirichlet's theorem shows moreover, that the q_i can be assumed to be prime.

Theorem 8: (Dirichlet's theorem) Let a, m be integers such that $1 \leq a \leq m, \gcd(a, m) = 1$. Then the progression $\{a, a+m, a+2m, \dots, a+km, \dots\}$ contains infinite primes.

We have thus identified primes q_i such that, $f_i[F_i : \mathbb{Q}] = p_i^{m_i}$ for $i = 2, \cdots, r$. For $i = 1$, i.e., $F = F_1 = \mathbb{Q}(\imath)$ we will always use the prime $q_1 = 5$ whose inertial degree in $\mathbb{Q}(\omega_{2^{m+2}})/\mathbb{Q}$ is 2^m for all m [10]. Next, consider the following two theorems proved in [2].

Theorem 9: If $\exists$ primes $q_i \in \mathbb{Z}$ having primitive multiplicative order f_i in $\mathbb{Z}/(p_i^{m_i+1}\mathbb{Z})$ for $i = 1, 2, \cdots, r$ with all p_i being distinct primes, then $\exists$ a prime $q \in \mathbb{Z}$ which has multiplicative order f_i in $\mathbb{Z}/(p_i^{m_i+1}\mathbb{Z})$ for $i = 1, 2, \cdots, r$.

Theorem 10: Let K_1 and K_2 be Galois extensions of a field F of degree $p_1^{n_1}$ and $p_2^{n_2}$ respectively, for distinct primes p_1, p_2. If an ideal $\mathsf{J} \in \mathcal{O}_F$ has inertial degree $f_1 = p_1^{n_1}$ and $f_2 = p_2^{n_2}$ in K_1/F and K_2/F respectively, then its inertial degree in K_1K_2 is $f = f_1 f_2 = p_1^{n_1} p_2^{n_2}$.

It is now clear that we may use the q_i to obtain an inert ideal first in $K/\mathbb{Q}(\imath)$ and then in $L/\mathbb{Q}(\imath)$. Having proven the existence of 'γ' for any number of antennas we explicitly calculate γ for a few cases, shown in Table I.

TABLE I
NON-NORM ELEMENTS

n_t	2	3	4	5	6	7	8
q	5	5	5	13	5	5	5
γ	$2+\imath$	$2+\imath$	$2+\imath$	$3+2\imath$	$2+\imath$	$2+\imath$	$2+\imath$

VIII. Recent constructions of CDAs

In a recent paper [12], alternative methods are presented for constructing cyclic Galois extensions and identifying the non-norm elements, valid for all n, which result in lesser signalling complexity than the constructions presented here.

IX. Proof of approximate Universality of the CDA based ST constructions

The proof of approximate universality of the CDA based ST constructions is along the lines of [11]. For completeness, we include a proof below. The property of the CDA being approximately universal ensures that it meets the outage curve of any given channel, irrespective of the channel statistics.

Theorem 11: The ST codes derived from cyclic division algebras which have non-vanishing determinant are approximately universal.

Proof: Define the probability of outage at a rate of transmission R bits/channel use as

$$P_{\text{out}}(R) = \inf_{Q\geq 0, tr(Q)\leq n_t} Pr\left[\log\det\left(I + \frac{SNR}{n_t} HQH^\dagger\right) < R\right]$$

where Q denotes the covariance matrix of the input vector.

Irrespective of the statistics of the channel, we have from [1] that

$$\begin{aligned} Pr\left[\log\det\left(I + \frac{SNR}{n_t} HH^\dagger\right) < R\right] &\geq P_{\text{out}}(R) \\ &\geq Pr\left[\log\det\left(I + \text{SNR} HH^\dagger\right) < R\right] \end{aligned}$$

At high SNR, the bounds are tight and we obtain [1]

$$P_{\text{out}}(R) \doteq Pr\left[\log\det(I + \text{SNR} H^\dagger H) < R\right] \qquad (11)$$

For $n' = \min(n_t, n_r)$ we get

$$Pr(\text{no-outage}) = Pr\left\{\sum_{i=1}^{n'} \ln(1 + \text{SNR}\lambda_i) > \ln(\text{SNR}^r)\right\}$$

and from lemma 2, we have $d_E^2(H, \Delta X) \geq \sum_{i=1}^{n'} l_i\lambda_i$.

To determine the worst possible value for the above expression under the no-outage condition, i.e. to determine $d^2_{E,\text{worst}} = \inf_{H\notin\text{outage}} \sum_{i=1}^{n'} l_i\lambda_i$, we use the lagrange multiplier technique. Writing the functional as

$$J(\lambda_1, \ldots, \lambda_{n'}) = \sum_{i=1}^{n'} l_i\lambda_i + \mu \sum_{i=1}^{n'} \ln(1 + \text{SNR}\lambda_i) - \mu r \ln \text{SNR}$$

and differentiating w.r.t. λ_i, we obtain $\lambda_i = \left(\frac{\mu}{l_i} - \frac{1}{\text{SNR}}\right)$. We then use the Kuhn-Tucker conditions to verify that the solution $\lambda_i = \left(\mu/l_i - \text{SNR}^{-1}\right)^+$ is what gives the worst possible $d^2_{E,\text{worst}}$, for μ such that $\sum_{i=1}^{n'} \ln\left(1 + \text{SNR}\left(\mu/l_i - \text{SNR}^{-1}\right)^+\right) = r\ln\text{SNR}$ Solving the above, we obtain

$$\mu = \overbrace{\text{SNR}^{-\left(1-\frac{r}{n'}\right)}}^{\psi} \overbrace{\prod_{i=1}^{n'} l_i^{\frac{1}{n}}}^{G} \quad \text{and thus} \quad \lambda_i = \frac{\phi G}{l_i} - \frac{1}{\text{SNR}}.$$

Substituting this value of λ_i in $d^2_{E,\text{worst}}$ and setting $d^2_{E,\text{worst}} > \text{SNR}^\epsilon$ for some $\epsilon > 0$, we obtain condition on smallest n' eigenvalues of code $\prod_{i=1}^{n'} l_i > \text{SNR}^{n'-r}$.

This ensures exponential decay of P_e in the no-outage region. Since CDA ST codes satisfy the above condition on eigenvalues they are approximately universal. ■

References

[1] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. Info. Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.

[2] Petros Elia, K. Raj Kumar, Sameer A. Pawar, P. Vijay Kumar and Hsiao-feng Lu, "Explicit, Minimum-Delay Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff," *Submitted to IEEE Trans. Inform. Theory*, Sept. 2004. Available at http://ece.iisc.ernet.in/~vijay/csdpapers/explicit.pdf

[3] Paulo Ribenboim, *Classical theory of Algebraic Numbers*, New York: Springer-Verlag: Universitext, 2001.

[4] H. Yao, G.W. Wornell,"Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay," GLOBECOM 2003. IEEE , Vol. 4, 1-5 Dec. 2003 pp. 1941 - 1945.

[5] H. El Gamal, G. Caire and M.O. Damen,"Lattice Coding and Decoding Achieve the Optimal Diversity-Multilpexing Tradeoff of MIMO Channels,"*IEEE Trans. Inform. Theory*, vol. 50, pp. 968-985, June 2004.

[6] B. A. Sethuraman and B. Sundar Rajan and V. Shashidhar, "Full-diversity, High-rate, Space-Time Block Codes from Division Algebras," *IEEE Trans. Info. Theory*, vol. 49, pp. 2596-2616, Oct. 2003.

[7] J.-C. Belfiore, G. Rekaya and E.Viterbo, "The Golden code: a 2×2 full-rate space-time code with non-vanishing determinants," *Proc. IEEE Int. Symp. Inform. Th (ISIT 2004)*, pp. 308, June 27-July 2, Chicago 2004.

[8] Petros Elia, P. Vijay Kumar, Sameer Pawar, K. Raj Kumar, B. Sundar Rajan and Hsiao-feng (Francis) Lu, "Diversity-Multiplexing Tradeoff Analysis of a few Algebraic Space-Time constructions," *Proc. 42nd Allerton conf. on Comm., Control & Computing*, Sept. 2004. Available at http://ece.iisc.ernet.in/~vijay/csdpapers/DMG_bounds.pdf

[9] G. Rekaya, J.-C. Belfiore and E.Viterbo, "Algebraic 3×3, 4×4 and 6×6 space-time codes with non-vanishing determinants," *Proc. of Int. Symp. Inform. Th and its Applns. (ISITA 2004)*, Parma, Italy, Oct. 10-13,2004.

[10] Kiran.T. and B.Sundar Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *Submitted to IEEE Trans. Inform. Theory*, August 2004.

[11] S. Tavildar and P. Viswanath, "Permutation codes for the parallel fading channel: Achieving the diversity-Multiplexing tradeoff," *Proc. CISS-2004*, Feb. 2004.

[12] Hsiao-feng Lu, Petros Elia, K. Raj Kumar, Sameer A. Pawar and P. Vijay Kumar, "Space-time codes meeting the diversity-multiplexing gain tradeoff with low signalling complexity," *Submitted to the 39th Annual CISS 2005 Conference on Information Sciences and Systems*.