Explicit Space-Time Codes that Achieve the Diversity-Multiplexing Gain Tradeoff

Petros Elia
Department of EE-Systems
University of Southern California
Los Angeles, CA 90089, USA
Email: elia@usc.edu

K. Raj Kumar
Sameer A. Pawar
P. Vijay Kumar [1]
ECE Dept., Indian Institute of Science
Bangalore, 560 012, India
Email: {raj,sameerp,vijay}@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 for the quasi-static, Rayleigh-fading MIMO channel with n_t transmit and n_r receive antennas, that there exists a fundamental tradeoff between diversity gain and multiplexing gain, referred to as the Diversity-Multiplexing Gain (D-MG) tradeoff.**

This paper presents the first explicit construction of space-time (ST) codes for an arbitrary number of transmit and/or receive antennas that achieve the D-MG tradeoff. It is shown here that ST codes constructed from cyclic-division-algebras (CDA) and satisfying a certain non-vanishing determinant (NVD) property, are optimal under the D-MG tradeoff for any n_t, n_r. Furthermore, this optimality is achieved with minimum possible value of the delay or block-length parameter $T = n_t$. 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 CDA-based constructions are also extended to provide D-MG optimal codes for all $T \geq n_t$, again for any number n_t of transmit antennas. This extension thus presents rectangular D-MG optimal space-time codes that achieve the D-MG tradeoff.

Taken together, the above constructions also extend the region of T for which the D-MG tradeoff is precisely known from $T \geq n_t + n_r - 1$ to $T \geq n_t$.

I. INTRODUCTION

Quasi-Static Channel Model: Consider the Rayleigh-fading ST channel with block length or 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 an $(n_t \times T)$ transmitted codeword matrix drawn from a ST code $\mathcal{X}$, H is the $(n_r \times n_t)$ channel matrix and W is the $(n_r \times T)$ noise matrix. The entries of H and W are assumed to be i.i.d., circularly symmetric $\mathbb{C}\mathcal{N}(0,1)$ random variables. The entries of X are drawn from a constellation whose size scales with SNR such that

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

It is assumed that H is known to the receiver but not to the transmitter.

D-MG Tradeoff: Let r be the normalized rate given by $R = r\log(\text{SNR})$. Following [1], we will refer to r as the *multiplexing gain*. Thus a ST code achieving normalized rate r has size

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

Let the *diversity gain* $d(r)$ corresponding to transmission at normalized rate r be 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, averaged over channel realizations. In [1] it is shown that for a fixed integer multiplexing gain r, and $T \geq n_t+n_r-1$, the maximum achievable diversity gain $d^*(r)$ is governed by

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

for non-integral values of r, $d^*(r)$ is obtained through

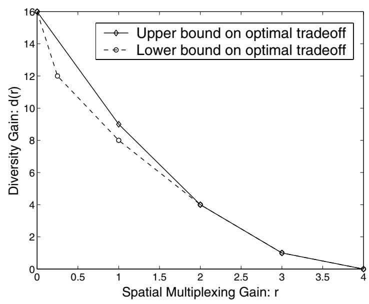

Fig. 1. *Diversity-Multiplexing Gain Tradeoff for $n_t = n_r = T = 4$*

straight-line interpolation. For $T < n_t + n_r - 1$ only upper and lower bounds on $d^*(r)$ are available.

Prior Work: The results in [1] spurred considerable research activity. Much recent progress has been made in constructing D-MG optimal codes.

Yao and Wornell [5] were the first to provide an optimal construction for the $(n_t = 2,\ n_r = 2)$ case. Subsequent optimal constructions for the (2×2) case can be found in [9],

[1]This work was carried out while P. Vijay Kumar was on leave of absence from the University of Southern California. This research is supported in part by NSF-ITR CCR-0326628, in part by the DRDO-IISc Program on Advanced Research in Mathematical Engineering and in part from Grant NSC 93-2218-E-194-012.

[8], [10]. The first code construction that is D-MG optimal for all (n_t, n_r) pairs is due to El Gamal et al. [6] who provide a lattice-based construction of space-time codes known as LAST codes that achieve the D-MG tradeoff over the i.i.d. Rayleigh fading for all n_t, n_r. This construction technique does not however, provide a closed-form expression for the codes constructed and does not yield minimum-delay codes.

In [13], 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 [13] (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. In [13] approximately universal constructions were explicitly constructed for some instances of the parallel channel.

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.

The CDA-based constructions are also extended to provide D-MG optimal codes for all $T \geq n_t$, again for any number n_t of transmit antennas. This extension thus presents rectangular D-MG optimal space-time codes that achieve the D-MG tradeoff.

Taken together, the above constructions also extend the region of T for which the D-MG tradeoff is precisely known from $T \geq n_t + n_r - 1$ to $T \geq n_t$. Further details regarding the above results may be found in the journal-submission version of the present paper [2].

II. Achieving the Optimal D-MG Tradeoff

Theorem 1: Consider a full-rank $n_t \times T$ space-time code $\mathcal{X}$ with $T \geq n_t$. Let ΔX denote the difference of any two codeword-matrices drawn from $\mathcal{X}$ and r be the spatial multiplexing gain. Define $\min_{\Delta X} \det(\Delta X \Delta X^\dagger) := SNR^{\delta}$. If the parameter δ of the space-time code $\mathcal{X}$ satisfies

$$\delta = n_t - r, \qquad 0 \leq r \leq \min\{n_t, n_r\},$$

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

Proof: We will prove the case when $n_r \geq n_t$, same proof can be easily extended to the case of $n_r < n_t$. Let $\mathcal{X}$ be a space-time code with the parameters stated in the theorem. Let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{n_t}$ and $l_1 \geq l_2 \geq \cdots \geq l_{n_t}$ be the ordered eigenvalues of $H^\dagger H$ and $\Delta X \Delta X^\dagger$ respectively and $d_E^2(\Delta X, H)$ be the squared Euclidean distance between the codeword pair corresponding to ΔX for a given channel realization. From [11], [2] we have

$$\begin{aligned} d_E^2(\Delta X, H) &\geq \sum_{i=1}^{n_t} \lambda_i l_i \\ &\geq (j+1) \prod_{i=n_t-j}^{n_t} \lambda_i^{\frac{1}{j+1}} \prod_{i=n_t-j}^{n_t} l_i^{\frac{1}{j+1}}, \quad (5) \end{aligned}$$

for each $0 \leq j \leq n_t - 1$. Set $\lambda_i = \text{SNR}^{-\alpha_i}$. This implies that $\alpha_1 \geq \ldots \geq \alpha_{n_t}$. Any channel realization is characterized by the corresponding $\underline{\alpha} = (\alpha_1, \ldots, \alpha_{n_t})$.

Since $\det(\Delta X \Delta X^\dagger) \dot{\geq} SNR^{\delta}$ and $l_i \leq Tr(\Delta X \Delta X^\dagger) = \|\Delta X\|_F^2 \dot{\leq} \text{SNR}$, we obtain,

$$\prod_{i=n_t-j}^{n_t} l_i \dot{\geq} \frac{(\text{SNR}^{\delta})}{\text{SNR}^{(n_t-j-1)}}, \ j = 0, 1, \ldots, n_t - 1. \quad (6)$$

Using the sphere bound and the fact that $\|W\|_F^2$ is a chi-squared random variable in $2n_rT$ dimensions, we obtain the codeword error probability as

$$\begin{aligned} P_e(\underline{\alpha}) &\leq Pr\left\{ ||W||^2 > \frac{d_{E,\min}^2(\underline{\alpha})}{4} \right\} \\ &= e^{-z} \sum_{k=0}^{n_rT-1} \frac{z^k}{k!} \Bigg|_{z=\frac{d_{E,\min}^2(\underline{\alpha})}{4}}, \quad (7) \end{aligned}$$

where $d_{E,\min}^2(\underline{\alpha})$ denotes the minimum squared Euclidean distance between any two distinct codewords given a particular channel realization. We can obtain a lower bound on $d_{E,\min}^2(\underline{\alpha})$ by substituting (6) in (5) and using the assumption that $\delta = n_t - r$ as,

$$d_{E,\min}^2(\underline{\alpha}) \dot{\geq} \text{SNR}^{\ \Delta_j(\underline{\alpha})}, \quad (8)$$

where $\Delta_j(\underline{\alpha}) = 1 - \frac{r}{j+1} - \sum_{i=n_t-j}^{n_t} \left[\frac{\alpha_i}{j+1}\right]$ for all $0 \leq j \leq n_t - 1$. Averaging (7) over the channel and using (8), we obtain

$$\begin{aligned} P_e &\leq \int_{\underline{\alpha}} P_e(\underline{\alpha}) p(\underline{\alpha}) d\underline{\alpha} \\ &\dot{\leq} \int_{\underline{\alpha}} e^{-\text{SNR}^{\Delta_j(\underline{\alpha})}} \sum_{k=0}^{n_rT-1} \frac{\text{SNR}^{k\Delta_j(\underline{\alpha})}}{k!} p(\underline{\alpha}) d\underline{\alpha}, \quad (9) \end{aligned}$$

where the joint probability density function (pdf) of the ordered eigenvalues λ_i of $H^\dagger H$ is given in [1],

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

for some constant K.

Notice that in (9), if $\Delta_j(\underline{\alpha}) > 0$ for some j the double exponential term $e^{-\text{SNR}^{\Delta_j(\underline{\alpha})}}$ in (9) will drive P_e to zero with increasing SNR [2]. Similarly, from the expression for $p(\underline{\alpha})$, it can be shown that (9) reduces to zero if $\alpha_i < 0$ for any i. Therefore, the codeword error probability

$$P_e \doteq \mathrm{SNR}^{-d(r)} \dot{\leq} \int_{\mathcal{B}} P_e(\underline{\alpha})p(\underline{\alpha})d\underline{\alpha}$$

where $\mathcal{B} = \{\underline{\alpha} : \alpha_i \geq 0 \ \forall\ i,\ \Delta_j \leq 0, j = 0, \ldots, n_t - 1\}$. Evaluation of the above integral leads to

$$d(r) \ \geq \ \inf_{\underline{\alpha}\in\mathcal{B}} \sum_{i=1}^{n_t}(2i-1+|n_r-n_t|)\alpha_i. \qquad (10)$$

In general, when $k-1 \leq r \leq k, k = 1, \cdots, n_t$, the infimum is obtained by setting

$$\begin{aligned} \alpha_{n_t} = \alpha_{n_t-1} = \cdots = \alpha_{n_t-k+2} &= 0, \ (\text{for k} > 1) \\ \alpha_{n_t-k+1} &= k-r \\ \alpha_{n_t-k} = \alpha_{n_t-k-1} = \cdots = \alpha_1 &= 1 \end{aligned}$$

Thus for $(k-1) \leq r \leq k$ we have that

$$\begin{aligned} d(r) \ \geq \ & \sum_{i=1}^{n_t-k}(2i-1+n_r-n_t) \\ & + [2(n_t-k+1)-1+n_r-n_t]\,(k-r) \end{aligned}$$

so the values for non-integral r are obtained by above straight line equation and at the integral values $r = k$ we have,

$$d(k) \ \geq \ (n_r-k)(n_t-k)$$

which is same as in the case of the upper bound on optimal tradeoff curve $d^*(r)$ derived in [1]. ■

It will be shown in the sequel that square CDA-based ST codes ($n_t = T$) with NVD satisfy the requirements of Theorem 1 and are therefore D-MG optimal. The construction of CDA-based ST codes with NVD is the subject of the next section.

III. CDA based square ST-code construction

We will adopt the space-time channel model

$$Y = \theta HX + W$$

with the scaling factor θ chosen to ensure

$$\mathbb{E}(\|\theta X\|_F^2) \leq T\mathrm{SNR}. \qquad (11)$$

We will initially construct square ($T = n_t = n$) ST codes based on cyclic division algebras (CDA). The square constructions achieve minimum possible delay. Details on division-algebra-based ST codes can be found in [7].

The construction of a CDA-based ST code calls for a cyclic field extension $\mathbb{L}/F$ (where $\mathbb{L}, \mathbb{F}$ 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 $\mathbb{F}$ of an element in $\mathbb{L}$ equals n. In [7], γ is chosen to be transcendental over $\mathbb{L}$, whereas in [8], γ is an algebraic integer in $\mathbb{F}$. 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 codeword matrices in the ST code $\mathcal{X}$, is bounded away from 0 even in the limit as $\mathrm{SNR} \to \infty$, $r > 0$. Such a ST code is said to have the non-vanishing determinant (NVD) property [8].

Prior to the present work, finding suitable fields $\mathbb{F}$ and $\mathbb{L}$ and non-norm element γ had only been accomplished for a few specific values of n, see [8], [12]. A general technique for constructing cyclic extensions and identifying non-norm elements that hold for all n is given in Sections VI, VII.

Our construction begins by choosing $\mathbb{F} = \mathbb{Q}(\imath)$ and an n-degree cyclic Galois extension $\mathbb{L}/\mathbb{F}$ as described in Section VI. Let $\mathcal{O}_{\mathbb{L}}$, the ring of integers of the field $\mathbb{L}$, be the integral closure of $\mathcal{O}_{\mathbb{F}}$ in $\mathbb{L}$. Let $\beta_i, i = 1, 2, \cdots, n$ be an integral basis for $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{F}}$ where $n = [\mathbb{L} : \mathbb{F}]$. If σ is the generator of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$, we introduce a symbol z such that $\ell z \ = \ z\sigma(\ell) \quad \forall \ \ \ell \in \mathbb{L}$ and $z^n = \gamma$ for a "non-norm" element γ. Set $\gamma \in \mathbb{Z}[\imath]$. The cyclic division algebra $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ is then

$$D = \mathbb{L} \oplus z\mathbb{L} \oplus \ldots \oplus z^{n-1}\mathbb{L}.$$

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 of D. The left-regular representation X of any element $x \in D$ is of the form

$$X = \begin{bmatrix} \ell_0 & \gamma\sigma(\ell_{n-1}) & \ldots & \gamma\sigma^{n-1}(\ell_1) \\ \ell_1 & \sigma(\ell_0) & \ldots & \gamma\sigma^{n-1}(\ell_2) \\ \vdots & \vdots & \vdots & \vdots \\ \ell_{n-1} & \sigma(\ell_{n-2}) & \ldots & \sigma^{n-1}(\ell_0) \end{bmatrix}, \qquad (12)$$

$\ell_i \in \mathbb{L}$. The desired space-time code $\mathcal{X}$ is obtained by restricting the elements ℓ_i appearing in (12) to be of the form

$$\ell_i \ = \ \sum_{k=1}^{n} e_{i,k}\beta_k, \quad e_{i,k} \in \mathcal{A}_{\mathrm{QAM}},$$

where $\mathcal{A}_{\mathrm{QAM}} = \{a+\imath b \mid -M+1 \leq a, b \leq M-1, a, b \ \text{ odd }\}$. Note that $|\mathcal{A}_{\mathrm{QAM}}| = M^2$ and $|e_{i,k}|^2 \leq 2(M-1)^2 \doteq M^2$. Thus $|X_{i,j}|^2 \dot{\leq} M^2$ for all i, j. From (3) and (12) $|\mathcal{X}| = \mathrm{SNR}^{nr} = (M^2)^{n^2} \Rightarrow M^2 = \mathrm{SNR}^{\frac{r}{n}}$. The energy constraint in (11) leads to

$$\theta^2 \doteq \frac{\mathrm{SNR}}{\mathbb{E}\{\|X\|_F^2\}} \doteq \frac{\mathrm{SNR}}{M^2} = \mathrm{SNR}^{1-\frac{r}{n}} \qquad (13)$$

The determinant of the difference of any two code matrices belongs to $\mathbb{F} \bigcap \mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\imath]$, see [2] for details. We therefore have,

$$\det(\Delta X \Delta X^\dagger) \ \dot{\geq} \ \mathrm{SNR}^0, \qquad (14)$$

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

IV. Optimality of the CDA construction

Theorem 2: Square space-time codes ($n_t = T$) constructed from cyclic division algebras as in Section III and having the NVD property are optimal with respect to the D-MG tradeoff for any number of receive antennas.

Proof: For the square CDA based ST constructions, we obtain from (13) and (14) that

$$\det[(\theta\Delta X)(\theta\Delta X)^\dagger] = \left(\theta^2\right)^n \det(\Delta X \Delta X^\dagger) \ \dot{\geq} \ \mathrm{SNR}^{n-r}$$

Hence the sufficient condition for D-MG optimality in Theorem 1 is satisfied. ∎

Details relating to the construction of cyclic Galois extensions and identification of a suitable non-norm element which are key to the construction of cyclic division algebras will be given in Sections VI, VII.

In the next section, we show how CDA-based constructions can be modified to provide constructions of rectangular space-time codes with $T > n_t$. While such constructions are not of minimum delay, they do extend the range of T for which D-MG optimal constructions are available. They also extend the range of T for which the D-MG tradeoff is known precisely.

V. Construction of Rectangular ($T > n_t$) ST codes

We present here two explicit constructions of D-MG optimal space-time codes which we name as the puncturing and stacking constructions respectively.

A. Puncturing Construction

Consider an $T \times T$ square D-MG optimal ST code $\mathcal{X}'_{T\times T}$ obtained as in Section III. An $n_t \times T$ ST code $\mathcal{X}$ is obtained by deleting the last $(T-n_t)$ rows of each matrix $X'_{T\times T} \in \mathcal{X}'_{T\times T}$, i.e., every $X \in \mathcal{X}$ is such that,

$$X'_{T\times T} = \left[\begin{array}{c} X_{n_t\times T} \\ Z_{(T-n_t)\times T} \end{array} \right],$$

for some $Z \in \mathbb{C}^{(T-n_t)\times T}$. In the sequel, the notation $l_k(A)$ will denote the k^{th} ordered eigenvalue of the matrix $A \in \mathbb{C}^{n\times n}$, assumed to be arranged in increasing order,

$$l_1(A) \;\leq\; l_2(A) \;\leq\; \cdots \;\leq\; l_n(A).$$

Lemma 3: [3] Let $A \in \mathbb{C}^{T\times T}$ be a Hermitian matrix, let n_t be an integer with $1 \leq n_t \leq T$, and let A_{n_t} denote any n_t-by-n_t principal submatrix of A (obtained by deleting $T-n_t$ rows and the corresponding columns from A). For each integer k such that $1 \leq k \leq n_t$ we have

$$l_k(A) \;\leq\; l_k(A_{n_t}) \;\leq\; l_{k+T-n_t}(A)$$

Theorem 4: The $n_t \times T$ space-time code $\mathcal{X}$ with $T > n_t$ derived from a D-MG optimal $T \times T$ space-time code $\mathcal{X}'_{T\times T}$ by retaining the first n_t rows, achieves the optimal D-MG tradeoff.

Proof: Let $\Delta X'$ be the difference of any two distinct codewords from the ST code $\mathcal{X}'_{T\times T}$ and ΔX be the corresponding difference matrix in ST code $\mathcal{X}$. Then

$$\Delta X^{'}\Delta X^{'\dagger} = \left[\begin{array}{c} \Delta X \\ \Delta Z \end{array} \right] \left[\Delta X^{\dagger} \Delta Z^{\dagger} \right] = \left[\begin{array}{cc} \Delta X \Delta X^{\dagger} & \Delta X \Delta Z^{\dagger} \\ \Delta Z \Delta X^{\dagger} & \Delta Z \Delta Z^{\dagger} \end{array} \right]$$

Let $l_{\max}$ be the maximum eigenvalue of $(\theta^2 \Delta X' \Delta X'^{\dagger})$. We have $l_{\max} \leq ||\theta \Delta X'||_F^2 \;\dot{\leq}\;$ SNR. Then direct application of Lemma 3 along with the fact that $\mathcal{X}'_{T\times T}$ is $T \times T$ D-MG optimal ST code gives

$$\min_{\Delta X} \det(\theta^2 \Delta X \Delta X^{\dagger}) \geq \frac{\min_{\Delta X'} \det(\theta^2 \Delta X^{'} \Delta X^{'\dagger})}{(l_{\max})^{T-n_t}} \doteq SNR^{n_t - r}$$

∎

B. Stacking Construction

Let t be the smallest factor of T which is greater than or equal to n_t. The $(n_t \times T)$ stacking ST code $\mathcal{X}$ is obtained by horizontally stacking $k = \frac{T}{t}$ punctured rectangular $(n_t \times t)$ ST codes $\mathcal{X}_i, \;\; i = 1, 2, \cdots, k$ as shown below.

$$\mathcal{X} = \left[\; \left[\mathcal{X}_1 \right]_{n_t\times t} \left[\mathcal{X}_2 \right]_{n_t\times t} \cdots \left[\mathcal{X}_k \right]_{n_t\times t} \; \right]_{n_t\times T}$$

Lemma 5: Let $A, B \in \mathbb{C}^{n\times n}$ be Hermitian. Assume that B is positive semidefinite and that the eigenvalues of A and $A+B$ are arranged in increasing order. Then

$$l_k(A) \leq l_k(A+B) \text{ for all } k = 1, 2, \ldots, n.$$

Theorem 6: The $(n_t \times T)$ type-B rectangular space-time code $\mathcal{X}$ achieves the optimal D-MG tradeoff.

Proof: Upon using Lemma 5, the proof follows along similar lines as the proof of Theorem 4 . ∎

VI. Cyclic Extensions

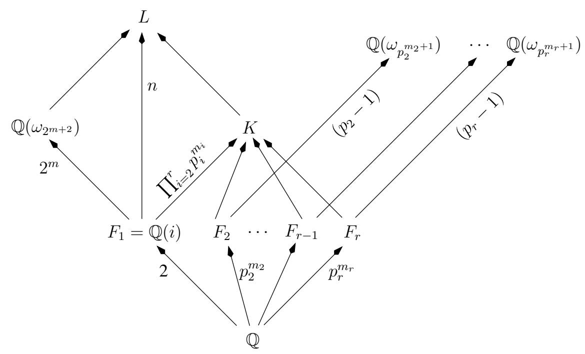

Fig. 2. Construction of cyclic extensions of $\mathbb{Q}(\imath)$ of arbitrary degree.

A systematic means of constructing cyclic Galois extensions of a number field $\mathbb{F}$, 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 $\mathbb{Q}(\omega_m)$. First, we set $\mathbb{F}_1 = \mathbb{Q}(\imath)$. Next consider $\mathbb{R}_i = \mathbb{Q}(\omega_{p_i^{m_i+1}})$, for distinct odd primes p_i, $i = 2, \cdots, r$. Then $\mathbb{R}_i/\mathbb{Q}$ is a cyclic extension of degree $\phi(p_i^{m_i+1}) = p_i^{m_i}(p_i - 1)$ [4]. It has a cyclic subgroup $H_i < G_i = Gal(\mathbb{R}_i/\mathbb{Q})$ of order $(p_i - 1)$. From Galois theory, there is a unique subfield $\mathbb{F}_i$ of $\mathbb{R}_i$ fixed by the subgroup H_i. It can be shown that $\mathbb{F}_i$ is a cyclic extension of $\mathbb{Q}$ of degree $p_i^{m_i}$ [2].

Cyclic Extensions of $\mathbb{F}_1 = \mathbb{Q}(\imath)$*:* Here we obtain cyclic extensions of $\mathbb{F}_1$ of arbitrary degree n.

Theorem 7: [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 $\mathbb{F}$ of degree n_i (where the n_i are pairwise relatively prime), then S is a cyclic extension of $\mathbb{F}$ of degree $\prod_{i=1}^{r} n_i$.

From the theorem, it follows that $\mathbb{K} = \mathbb{F}_1 \mathbb{F}_2 \ldots \mathbb{F}_r$ with $\mathbb{F}_i$ as defined above and as shown in Fig. 2, is cyclic over $\mathbb{Q}$. Consequently, $\mathbb{K}/\mathbb{F}_1$ 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 [4]. A second application of Theorem 7 shows that $\mathbb{L} = \mathbb{K}\ \mathbb{Q}(\omega_{2^{m+2}})$ 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 $\gamma \in \mathbb{F}^*$ satisfying $\gamma^i \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L}), i < n$. We make use of a theorem in [12].

Theorem 8: [12] Let $\mathbb{K}$ be a degree n Galois extension of a number field $\mathbb{F}$ and let $\mathfrak{p}$ be a prime ideal in the ring $\mathcal{O}_\mathbb{F}$ below the prime ideal $\mathfrak{P} \subset \mathcal{O}_\mathbb{K}$ 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 $\gamma^i \notin N_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ for any $i = 1, 2, \cdots, f-1$.

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

Lemma 9: [4] 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 10: [4] 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 11: (Dirichlet's theorem) Let a, m be integers such that $1 \leq a \leq m, \gcd(a, m) = 1$. Then the progression $\{a, a+m, a+2m, \ldots, a+km, \ldots\}$ contains infinite primes.

We have thus identified primes q_i such that, $f_i = [\mathbb{F}_i : \mathbb{Q}] = p_i^{m_i}$ for $i = 2, \cdots, r$. For $i = 1$, i.e., $\mathbb{F} = \mathbb{F}_1 = \mathbb{Q}(\imath)$ 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 [12]. Next, consider the following two theorems proved in [2].

Theorem 12: 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 13: Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be Galois extensions of a field $\mathbb{F}$ of degree $p_1^{n_1}$ and $p_2^{n_2}$ respectively, for distinct primes p_1, p_2. If an ideal $\mathsf{J} \in \mathcal{O}_\mathbb{F}$ has inertial degree $f_1 = p_1^{n_1}$ and $f_2 = p_2^{n_2}$ in $\mathbb{K}_1/\mathbb{F}$ and $\mathbb{K}_2/\mathbb{F}$ respectively, then its inertial degree in $\mathbb{K}_1\mathbb{K}_2$ 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 $\mathbb{K}/\mathbb{Q}(\imath)$ and then in $\mathbb{L}/\mathbb{Q}(\imath)$. 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 [14], modifications to the current methodology were presented that allow for reduced signalling complexity. Furthermore, the CDA codes presented here provided the basis for the recent generalization of the perfect space-time code constructions. Perfect space-time codes were first introduced in [15] for $n_t = 2, 3, 4, 6$, to be the D-MG optimal codes with equal power sharing among the different antennas, as well as with a signalling set that belongs in a lattice that is isometric to the multi-dimensional integers (cubic constellation). Applying these two extra conditions greatly improved the corresponding performance. Perfect codes were recently generalized in [16], for all n_t, n_r and all $T \geq n_t$.

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] Roger A. Horn and Charles R. Johnson, *Matrix analysis*, Cambridge University Press, 1999.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] P. Dayal and M. K. Varanasi,"An Optimal Two Transmit Antenna Space-Time Code and its Stacked Extensions," *Proc. Asilomar Conf. on Signals, Systems and Computers*, Monterey, CA, Nov. 2003.

[10] Genyuan Wang and Xiang-Gen Xia, "On optimal multi-layer cyclotomic space-time code design," *IEEE Trans. on Info. Theory*, pp. 1102-1135, Volume: 51, Issue: 3, March 2005.

[11] C. Kose and R. D. Wesel, "Universal space-time trellis codes," *IEEE Trans. on Info. Theory*, pp. 2717-2727, Volume 49, Oct 2003.

[12] 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.

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

[14] 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.*

[15] F. Oggier, Ghaya Rekaya, J.C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes," *Submitted to IEEE Trans. Inform. Theory*, August 2004.

[16] Petros Elia, B. A. Sethuraman and P. Vijay Kumar " Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas," *Presented at the WirelessCom 2005, International Conference on Wireless Networks, Communications, and Mobile Computing.*