Perfect Space-Time Codes for Any Number of Antennas

Petros Elia, B. A. Sethuraman and P. Vijay Kumar

***Abstract*— In a recent paper, perfect $(n \times n)$ space-time codes were introduced as the class of linear dispersion space-time codes having full rate, non-vanishing determinant, a signal constellation isomorphic to either the rectangular or hexagonal lattices in $2n^2$ dimensions and uniform average transmitted energy per antenna. Consequence of these conditions include optimality of perfect codes with respect to the Zheng-Tse Diversity-Multiplexing Gain tradeoff (DMT), as well as excellent low-SNR performance. Yet perfect space-time codes have been constructed only for $2, 3, 4$ and 6 transmit antennas.**

In this paper, we construct perfect codes for all channel dimensions, present some additional attributes of this class of space-time codes and extend the notion of a perfect code to the rectangular case.

***Index Terms*— perfect space-time codes, diversity-multiplexing tradeoff, division algebras, MIMO.**

I. Introduction

Consider the quasi-static, Rayleigh fading, space-time (ST) MIMO channel with quasi-static interval T, n_t transmit and n_r receive antennas. The $(n_r \times T)$ received signal matrix Y is given by

$$Y \;=\; \theta H X + W \tag{1}$$

where X is a $(n_t \times T)$ code matrix drawn from a ST code $\mathcal{X}$, H the $(n_r \times n_t)$ channel matrix and W represents additive noise. The entries of W are assumed to be i.i.d., circularly symmetric, complex Gaussian $\mathbb{CN}(0,1)$ random variables. The real scalar θ ensures that the energy constraint

$$\theta^2 ||X||_F^2 \;\le\; T \text{ SNR}, \quad \text{all } X \in \mathcal{X}, \tag{2}$$

is met.

Let

$$\mathcal{Z} \;=\; \{\theta X \mid X \in \mathcal{X}\},$$

denote the normalized (for SNR) version of the ST code $\mathcal{X}$. For the most part, our interest is in square space-time codes, i.e., space time codes $\mathcal{X}$ where $T = n_t$ in which case we will use the symbol $n = n_t = T$ to denote their common dimension.

A ST code is said to meet the *rank criterion* if the difference $\Delta X = X_1 - X_2$ of every pair of distinct code matrices, X_1, X_2 has rank equal to $\min\{n_t, T\}$. A ST code $\mathcal{X}$ is said to be a *linear dispersion code* over a constellation $\mathcal{A}$ if every code matrix X has a unique expansion of the form

$$X \;=\; \sum_{k=1}^{K} a_k \Lambda_k, \quad a_k \in \mathcal{A},$$

where the matrices Λ_k are fixed and independent of the message and where conversely, every matrix of the form on the right is a code matrix. A linear-dispersion code over a constellation $\mathcal{A}$ is said to be *full-rate* over the constellation $\mathcal{A}$ if $K \;=\; n_t T$.

A. Diversity-Multiplexing Gain Tradeoff

Multiple transmit and receive antennas have the potential of increasing reliability of communication as well as permitting communication at higher rates. In a recent landmark paper, Zheng and Tse [3] showed that there is a fundamental tradeoff between diversity and multiplexing gain, referred to as the diversity-multiplexing gain tradeoff (DMT). The space-time code $\mathcal{X}$ transmits

$$R \;=\; \frac{1}{T}\log(|\ \mathcal{X}\ |)$$

bits per channel use. The normalized rate parameter r given by $R = r\log(\text{SNR})$ is called the multiplexing gain. The diversity gain $d(r)$ corresponding to multiplexing gain r is then 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. We adopt the exponential equality notation of [3] under which this relationship can equivalently be expressed by

$$P_e \doteq \text{SNR}^{-d(r)}.$$

A principal result in [3] is the proof that for a fixed integer multiplexing gain r, and $T \ge n_t + n_r - 1$, the maximum achievable diversity gain $d(r)$ in the case of Rayleigh fading, i.e., when the entries of the channel matrix H are i.i.d and drawn from a $\mathbb{CN}(0,1)$ distribution, is governed by

$$d(r) \;=\; (n_t - r)(n_r - r). \tag{3}$$

The value of $d(r)$ for non-integral values of r is obtained through straight-line interpolation. The plot in Fig. 1 is for the

Petros Elia is with Forschungszentrum Telekommunikation Wien, 1220, Vienna (elia@ftw.at). P. Vijay Kumar is with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, 560012, on leave of absence from EE-Systems, University of Southern California, Los Angeles, CA 90089 (vijayk@usc.edu). B. A. Sethuraman is with the Department of Mathematics, of the California State University Northridge, CA 91330 (al.sethuraman@csun.edu). Part of this work was carried out while Petros Elia was at the University of Southern California.

This paper was presented in part at the *International Conference on Wireless Networks, Communications, and Mobile Computing (WirelessCom 2005)*, Maui, Hawaii, June 13-16. This research is supported in part by NSF-ITR CCR-0326628 and in part by the DRDO-IISc Program on Advanced Research in Mathematical Engineering.

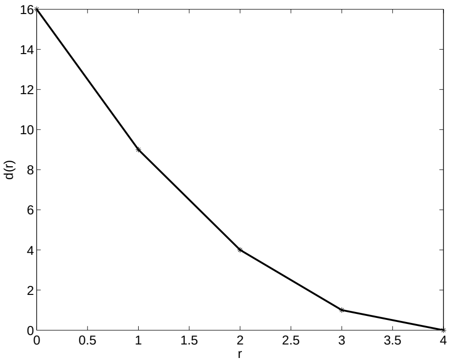

Fig. 1. *The DMT in the case of* 4 *transmit and* 4 *receive antennas.*

case $n_r = n_t = T = 4$. It has been shown in [2] that space-time codes from cyclic division algebras (CDA) with a certain non-vanishing determinant (NVD) property, achieve the DMT with minimum possible value $T = n_t$ of delay parameter T.

Perfect codes, described in detail below, are a subclass of space-time codes with the NVD property whose construction is based on CDAs and whose vectorized code matrices are associated with the cubic lattice in $2n_tT$-dimensional Euclidean space. In [19], the authors present constructions of CDA-based ST codes with the NVD property in which the constellation of code matrices in $2n_tT$-dimensional Euclidean signal-space is more energy efficient. In [20], the authors show that in order to construct CDA-based space-time codes with a prescribed NVD property whose vectorized code matrices form the densest possible lattice, it is necessary to minimize the discriminant of a maximal order (see [20] for a definition) within a CDA. A lower bound to the value of this discriminant is provided as well as example constructions achieving this lower bound. See [23], [22], [21] for more recent results in this direction.

B. Perfect Codes

In [1, Definition 1], perfect codes are defined as $n \times n$ space-time codes that satisfy the following conditions.

- P1 *Full rate*: the code is a full-rate linear-dispersion code using n^2 information symbols either QAM or HEX;
- P2 *Non vanishing determinant*: the minimum determinant of the infinite code is non zero (so that in particular the code meets the rank criterion)
- P3 *Good constellation shaping*. the energy required to send the linear combination of the information symbols on each layer is similar to the energy used for sending the symbols themselves (we do not increase the energy of the system in encoding the information symbols);
- P4 *Uniform average transmitted energy*. it induces uniform average transmitted energy per antenna in all time slots, i.e., all the coded symbols in the code matrix have the same average energy.

Perfect codes are of interest as the above attributes guarantee excellent performance as measured by error probability. We extend the definition of perfect codes here to include rectangular $(n_t \times T)$ codes by replacing properties P1, P2 above by the slight modifications:

- P1 *Full rate*. The code is a full-rate linear-dispersion code where the (n_tT) coefficients representing the message symbols are drawn from either the QAM or HEX constellations.
- P2 *Non vanishing determinant*: For every pair X_1, X_2 of distinct code matrices, the determinant $\det(\Delta X \Delta X^\dagger)$, $\Delta X = X_1 - X_2$, prior to SNR normalization (this is explained in greater detail below), is lower bounded by a constant that is greater than zero and independent of the code size.

Properties P3, P4 remain the same. In all of our constructions, we will meet property P3 by ensuring that the signalling set, obtained by code-matrix vectorization, is isometric to either QAM$^{n^2}$ or else HEX$^{n^2}$.

It can be shown that properties $P1$ through $P4$ imply that when perfect codes are operated over a Rayleigh-fading channel, they are optimal with respect to the DMT of this channel. DMT optimality of a space-time code ensures good performance at large values of SNR. The known constructions of perfect codes exhibit in addition, excellent low-SNR performance as well.

C. Results

In the construction of perfect codes in [1], the authors restrict their choice of a so-called non-norm element γ to the ring of integers lying in a certain algebraic number field. This restriction was a key factor preventing the authors of [1] from generalizing their construction of perfect codes to values of n_t other than $2, 3, 4$ and 6. While a restriction to the ring of integers results in better performance, the defining properties of a perfect code $P1$ through $P4$ can be satisfied even without this requirement. Choosing the non-norm element γ suitably within the larger number field containing the ring of algebraic integers, and observing, with proof, that a key construction in [14] of unitary matrices for the prime case holds in a more general situation, permitted us to extend the construction of perfect codes to any value of the integer n_t.

Thus in this paper explicit constructions of perfect space-time codes for any number n_t of transmit antennas and any number n_r of receive antennas are provided. Rectangular perfect codes are constructed for any delay T that is a multiple of n_t. In addition, the following additional attributes of perfect codes are established:

- *Approximate universality*: i.e., the property that perfect codes achieve the diversity-multiplexing gain tradeoff (DMT) for any statistical description of the channel fading coefficients h_{ij}
- *Residual approximate universality*: by which we mean that perfect codes have the property that if certain rows of each space-time code matrix are deleted, then the resultant code is approximately universal for the correspondingly lesser number of transmit antennas
- *Information losslessness*: this concept was introduced in [29]. Our codes are information lossless over the class of rotationally invariant [38] ST channels.

Section II provides background on space-time codes constructed from cyclic division algebras. The general construction of perfect codes is provided in Section III. Examples and simulation results are also to be found here. Rectangular versions of perfect codes are constructed in Section IV. Additional attributes of perfect codes are established in Section V. Many proofs can be found in the appendices. A summary of mathematical notation employed appears in Appendix IV.

II. Space-Time Codes from Cyclic Division Algebras

A. Division Algebras

Division algebras are rings with identity in which every nonzero element has a multiplicative inverse. Thus unlike in the case of fields, multiplication of two elements is not necessarily commutative. The center $\mathbb{F}$ of any division algebra D, i.e., the subset comprising of all elements in D that commute with every element of D, is a field. The division algebra is a vector space over the center $\mathbb{F}$ of dimension n^2 for some integer n. A field $\mathbb{L}$ such that $\mathbb{F} \subset \mathbb{L} \subset D$ and such that no proper subfield of D contains $\mathbb{L}$ is called a *maximal subfield* of D (Fig. 2). Every division algebra is also a vector space over a maximal subfield and the dimension of this vector space is the same for all maximal subfields and equal to n. This common dimension n is known as the *index* of the division algebra. We will be interested only in the case when the index is finite.

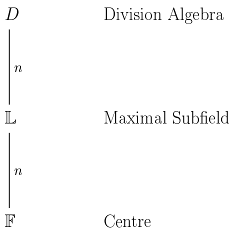

Fig. 2. Structure of a Cyclic Division Algebra

B. Cyclic Division Algebras

Our interest is in cyclic division algebras, i.e., division algebras in which the center $\mathbb{F}$ and a maximum subfield $\mathbb{L}$ are such that $\mathbb{L}/\mathbb{F}$ is a cyclic (Galois) extension. CDAs have a simple characterization that aids in their construction, see [45], Proposition 11 of [8], or Theorem 1 of [15].

Let $\mathbb{F}$, $\mathbb{L}$ be number fields, with $\mathbb{L}$ a finite, cyclic Galois extension of $\mathbb{F}$ of degree n. Let σ denote the generator of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Let z be an indeterminate satisfying

$$\ell z \;=\; z\sigma(\ell) \quad \forall \;\; \ell \in \mathbb{L} \qquad \text{and} \qquad z^n = \gamma,$$

for some non-norm element $\gamma \in \mathbb{F}^*$, by which we mean some element γ having the property that the smallest positive integer t for which γ^t is the relative norm $N_{\mathbb{L}/\mathbb{F}}(u)$ of some element u in $\mathbb{L}^*$, is n (by S^* we denote the group of units of some set S). Then a CDA $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ with index n, center $\mathbb{F}$ and maximal subfield $\mathbb{L}$ is the set of all elements of the form

$$\sum_{i=0}^{n-1} z^i \ell_i, \quad \ell_i \in \mathbb{L}. \tag{4}$$

Moreover it is known that every CDA has this structure. It can be verified that D is a right vector space (i.e., scalars multiply vectors from the right) over the maximal subfield $\mathbb{L}$.

C. Matrix Representation

The matrix corresponding to an element $d \in D$ corresponds to the left multiplication by the element d in the division algebra. Let λ_d denote this operation, $\lambda_d : D \to D$, defined by

$$\lambda_d(e) = de, \;\forall\; e \in D.$$

It can be verified that λ_d is a $\mathbb{L}$-linear transformation of D. From (4), a natural choice of basis for the right-vector space D over $\mathbb{L}$ is $\{1, z, z^2, \ldots, z^{n-1}\}$. A typical element in the division algebra D is $d = \ell_0 + z\ell_1 + \cdots + z^{n-1}\ell_{n-1}$, where the $\ell_i \in \mathbb{L}$. By considering the effect of multiplying $d \times 1$, $d \times z$, $\ldots$, $d \times z^{n-1}$, one can show that the $\mathbb{L}$-linear transformation λ_d under this basis has the matrix representation

$$\begin{bmatrix} \ell_0 & \gamma\sigma(\ell_{n-1}) & \gamma\sigma^2(\ell_{n-2}) & \ldots & \gamma\sigma^{n-1}(\ell_1) \\ \ell_1 & \sigma(\ell_0) & \gamma\sigma^2(\ell_{n-1}) & \ldots & \gamma\sigma^{n-1}(\ell_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \ell_{n-1} & \sigma(\ell_{n-2}) & \sigma^2(\ell_{n-3}) & \ldots & \sigma^{n-1}(\ell_0) \end{bmatrix}, \tag{5}$$

known as the left regular representation of d.

A set of such matrices, obtained by choosing a finite subset of elements in D constitutes the CDA-based ST code $\mathcal{X}$. The non-commutativity of the CDA endows the codeword matrices (and their differences) with a key determinant property.

Lemma 1: Let A denote the $(n \times n)$ matrix that is the left-regular representation of the element

$$\psi \;=\; \sum_{i=0}^{n-1} \ell_i z^i, \;\; \ell_i \in \mathbb{L}.$$

Then $\det(A) \in \mathbb{F}$.

Proof: See [47], [2]. ■

III. PERFECT CODE CONSTRUCTION FOR GENERAL n

A. QAM and HEX Constellations

In this section, we follow [15], [16], [1] and show how a CDA-based ST code with NVD can be constructed, that is a linear-dispersion code over the QAM constellation. The construction is also extended to the case of the HEX constellation. The QAM and HEX constellations are given respectively by

$$\begin{aligned} \mathcal{A}_{\text{QAM}} &= \{a + \imath b \;\mid\; |a|, |b| \leq (M-1), \;a, b \;\text{ odd}\}, \\ \mathcal{A}_{\text{HEX}} &= \{a + \omega_3 b \mid\; |a|, |b| \leq (M-1), \;a, b \;\text{ odd}\}. \end{aligned}$$

The $\mathcal{A}_{\text{QAM}}$ constellation has the property that

$$u \in \mathcal{A}_{\text{QAM}} \;\Rightarrow \mid u \mid^2 \leq 2M^2.$$

Since

$$\mathcal{A}_{\text{QAM}} \;\subseteq\; \mathbb{Q}(\imath)$$

it is natural to consider CDA with center $\mathbb{F} \;=\; \mathbb{Q}(\imath)$.

B. Canonical construction of a CDA-based space-time code

Let $\mathbb{F} = \mathbb{Q}(\imath)$, $\mathbb{L}$ be a n-degree cyclic Galois extension $\mathbb{L}/\mathbb{F}$ of $\mathbb{F}$ and let σ be the generator of the Galois group $\text{Gal}(\mathbb{L}/\mathbb{F})$. Let $\mathcal{O}_{\mathbb{F}}, \mathcal{O}_{\mathbb{L}}$ denote the ring of algebraic integers in $\mathbb{F}, \mathbb{L}$ respectively. It is known that $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\imath]$. Let $\gamma \in \mathbb{F}$, $|\gamma| = 1$, be a non-norm element of unit magnitude and $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ denote the associated CDA. Note that we do not insist that $\gamma \in \mathcal{O}_{\mathbb{F}}$.

Let $\{\beta_1, \ldots, \beta_n\}$ form an integral basis for $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{F}}$ and define the set

$$\mathcal{A}_{\text{QAM}}(\beta_1, \beta_2, \ldots, \beta_n) \ = \ \left\{ \sum_i a_i \beta_i \mid a_i \in \mathcal{A}_{\text{QAM}} \right\}.$$

Thus $\mathcal{A}_{\text{QAM}}(\beta_1, \beta_2, \ldots, \beta_n)$ is the set of all linear combinations of the basis elements β_i with coefficients lying in $\mathcal{A}_{\text{QAM}}$.

For the discussion in the next two subsections, Section III-C, III-D, we will presuppose the existence of such a canonical cyclic division algebra. In Sections III-E, III-F, III-G we discuss selection of the non-norm element as well as of the integral basis $\{\beta_1, \beta_2, \cdots, \beta_n\}$, we will explain how the desired cyclic algebra is actually to be constructed.

Consider the space-time code $\mathcal{X}$ comprising of matrices corresponding to the left-regular representation as in (5) of all elements d in CDA D which are of the form

$$d = \sum_{i=0}^{n-1} z^i \ell_i \ , \quad \ell_i \in \mathcal{A}_{\text{QAM}}(\beta_1, \beta_2, \ldots, \beta_n).$$

C. Full-rate property

The space-time codes under this setup are linear-dispersion ST codes as can be seen from the expansion below

$$X = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_{ij} \ \Gamma^i \ \text{diag}\big(\beta_j, \sigma(\beta_j), \cdots, \sigma^{n-1}(\beta_j)\big) \tag{6}$$

where $f_{ij} \in \mathcal{A}_{\text{QAM}}$ and where the cyclic-shift-and-multiply-at-end-by-γ matrix Γ is given by

$$\Gamma \ = \ \begin{bmatrix} 0 & 0 & \cdots & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} . \tag{7}$$

Note that by taking the sum on j inside, we can write

$$X = \sum_{i=0}^{n-1} \ \Gamma^i \ \text{diag}\big(\ell_i, \sigma(\ell_i), \cdots, \sigma^{n-1}(\ell_i)\big) \tag{8}$$

where

$$\ell_i \ = \ \sum_{j=0}^{n-1} f_{ij} \beta_j,$$

and this is the expansion of the code matrix in terms of its n "threads" or "layers". The full rate property holds since we are in effect transmitting n QAM symbols per channel use.

Example *1:* When $n = 3$, 9 QAM symbols are transmitted:

$$\begin{bmatrix} \ell_0 & \gamma\sigma(\ell_2) & \gamma\sigma^2(\ell_1) \\ \ell_1 & \sigma(\ell_0) & \gamma\sigma^2(\ell_2) \\ \ell_2 & \sigma(\ell_1) & \sigma^2(\ell_0) \end{bmatrix} =$$

$$\sum_{i=1}^{3} f_{0,i} \begin{bmatrix} \beta_i & & \\ & \sigma(\beta_i) & \\ & & \sigma^2(\beta_i) \end{bmatrix} +$$

$$\sum_{i=1}^{3} f_{1,i} \begin{bmatrix} & & \gamma\sigma^2(\beta_i) \\ \beta_i & & \\ & \sigma(\beta_i) & \end{bmatrix} +$$

$$\sum_{i=1}^{3} f_{2,i} \begin{bmatrix} & \gamma\sigma(\beta_i) & \\ & & \gamma\sigma^2(\beta_i) \\ \beta_i & & \end{bmatrix} =$$

$$\begin{bmatrix} \ell_0 & & \\ & \sigma(\ell_0) & \\ & & \sigma^2(\ell_0) \end{bmatrix} + \begin{bmatrix} & & \gamma\sigma^2(\ell_1) \\ \ell_1 & & \\ & \sigma(\ell_1) & \end{bmatrix} +$$

$$\begin{bmatrix} & \gamma\sigma(\ell_2) & \\ & & \gamma\sigma^2(\ell_2) \\ \ell_2 & & \end{bmatrix}$$

and the last three matrices are the 3 threads/layers.

D. Non-vanishing determinant property

From Lemma 1, it follows that the determinant of every such left-regular representation lies in $\mathbb{F} = \mathbb{Q}(\imath)$. Let $\gamma = \frac{a}{b}$, where $a, b \in \mathbb{Z}[\imath]$. By scaling every entry in columns $2, 3, \ldots, n$ of every code matrix in the space-time code $\mathcal{X}$ by the element b in $\mathbb{Z}[\imath]$ if necessary, we can ensure that every entry in the scaled matrix lies in $\mathcal{O}_{\mathbb{L}}$. We do not need to scale the entries in the first column since γ does not appear in the first column of any code matrix. It follows that the determinant of the scaled matrix lies in

$$\mathcal{O}_{\mathbb{L}} \cap \mathbb{F} \ = \ \mathcal{O}_{\mathbb{F}} \ = \ \mathbb{Z}[\imath].$$

Consequently, the determinant of the unscaled matrix lies in the set $\frac{1}{b^{n-1}}\mathbb{Z}[\imath]$ and in this set, the magnitude of every element is bounded below by $\frac{1}{|b|^{n-1}}$. The NVD property of the ST code constructed now follows since the difference of any two elements in the CDA is also an element of the CDA. This is regardless of the size M^2 of the QAM constellation.

We have thus shown that this construction of space-time codes is endowed with properties P1, P2.

E. Constellation Shaping and Uniform Energy Property

We next show how a proper choice of non-norm element γ and of integral basis $\{\beta_1, \beta_2, \cdots, \beta_n\}$ for $\mathcal{O}_{\mathbb{L}}/\mathcal{O}_{\mathbb{F}}$, will endow the ST code with good signal constellation (Property P3) and uniform transmitted power (Property P4). As shown above, each code matrix X may be regarded as being built up of n layers, with the ith layer, $0 \leq i \leq n-1$ comprising of the elements that are a function of the ith symbol ℓ_i. We begin by rearranging the entries of the code matrix X in a layer-by-layer fashion to form a vector $\underline{\text{lay}}(X)$ as shown below.

$$\underbrace{\begin{bmatrix} l_0 \\ \sigma(l_0) \\ \sigma^2(l_0) \\ \cdot \\ \cdot \\ \cdot \\ l_{n-1} \\ \gamma\sigma(l_{n-1}) \\ \gamma\sigma^2(l_{n-1}) \\ \vdots \end{bmatrix}}_{\underline{\mathrm{lay}}(X)} \tag{9}$$

$$= \underbrace{\begin{bmatrix} B_0\,G & & \\ & \ddots & \\ & & B_{n-1}G \end{bmatrix}}_{\Upsilon} \cdot \underbrace{\begin{bmatrix} f_{0,0} \\ f_{0,1} \\ f_{0,2} \\ \cdot \\ \cdot \\ \cdot \\ f_{n-1,0} \\ f_{n-1,1} \\ f_{n-1,2} \\ \vdots \end{bmatrix}}_{\underline{f}} \tag{10}$$

where

$$G = \begin{bmatrix} \beta_0 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \cdots & \sigma(\beta_{n-1}) \\ & \vdots & \\ \sigma^{n-1}(\beta_0) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{bmatrix}, \tag{11}$$

and where the B_i, are of the form

$$B_i \ = \ \mathrm{diag}(\underbrace{1, 1, \ldots, 1}_{n-i \text{ entries}}, \underbrace{\gamma, \gamma, \ldots, \gamma}_{i \text{ entries}}).$$

Suppose next that it were possible to choose an integral basis $\{\beta_1, \beta_2, \cdots, \beta_n\}$ such that the normalized matrix

$$U(G) \ = \ \kappa G, \tag{12}$$

where the scale factor κ lies in $\mathbb{F}$, is unitary and if in addition it were possible to choose the non-norm element γ to have unit magnitude, i.e., chosen such that $|\gamma| = 1$.

We would then have that the scaled block-diagonal transformation matrix $\kappa\Upsilon$ is unitary. As a consequence we would have that,

$$\begin{aligned} \mathbb{E}(\underline{\mathrm{lay}}(X)\underline{\mathrm{lay}}(X)^\dagger) &= \Upsilon\mathbb{E}(\underline{f}\underline{f}^\dagger)\Upsilon^\dagger \\ &= \frac{1}{\kappa^2}\mathcal{E}I \end{aligned}$$

where

$$\mathcal{E} \ = \ \frac{1}{|\mathcal{A}_{\mathrm{QAM}}|}\sum_{u \in \mathcal{A}_{\mathrm{QAM}}} |u|^2 = \frac{2(M^2-1)}{3}$$

From this it follows that

- the set $\{\underline{\mathrm{lay}}(X) \mid X \in \mathcal{A}_{\mathrm{QAM}}\}$ is isometric to the set $\mathcal{A}_{\mathrm{QAM}}^{n_t^2}$ which is the constellation shaping desired
- at each time slot, on average, each antenna transmits the same amount of energy.

To reiterate, a sufficient condition for the uniform constellation and equal energy properties to hold is that the matrix $U(G)$ is unitary and the element γ have magnitude 1. In the subsections to follow, we show how a suitable unit magnitude element γ and a suitable unitary matrix $U(G)$ can always be found.

F. Finding a unit-magnitude, non-norm element γ

Let us denote the l^{th} primitive root of unity by ω_l, i.e. $\omega_l = e^{2\pi\imath/l}$. Let k^* denote the complex conjugate of $k \in \mathbb{C}$.

Proposition 2 (non-norm element: QAM case): Let $n = 2^s n_1$ where $n_1 > 1$ is odd. Then there exists a prime p congruent to 1 mod n_1. Furthermore, there exists a prime q that is congruent to 5 mod 2^{s+2} such that the element $q \pmod p$ of $\mathbb{Z}_p$ has multiplicative order n_1 and which factors in $\mathbb{Z}[\imath]$ as $q = \pi_1\pi_1^*$ for a suitable prime $\pi_1 \in \mathbb{Z}[\imath]$. Let $\mathbb{K}'$ be the unique subfield of $\mathbb{Q}(\omega_p)$ of degree n_1 over $\mathbb{Q}$. Let $\mathbb{K}$ be the composite of $\mathbb{K}'$ and $\mathbb{Q}(\imath)$ and let $\mathbb{L} = \mathbb{K} \cdot \mathbb{Q}(\omega_{2^{s+2}})$. Then $\mathbb{L}$ is a cyclic extension of $\mathbb{Q}(\imath)$, and the element

$$\gamma = \frac{\pi_1}{\pi_1^*}$$

is an (algebraic) unit-magnitude element that is a non-norm element for the extension $\mathbb{L}/\mathbb{Q}(\imath)$. When $n = 2^s$, i.e., $n_1 = 1$, we can take $\mathbb{L} = \mathbb{Q}(\omega_{2^{s+2}})$ and $\gamma = \dfrac{1+2\imath}{1-2\imath}$.

Proof: See Appendix I ■

Proposition 3 (non-norm element: HEX case): Let $n = 2^s n_1,\ s \in \{0, 1\}$, where n_1 is odd. Then there exists a prime $p > 3$ congruent to 1 mod n_1. Furthermore, there exists a prime q that is congruent to 1 mod 3 and which has order $\mathrm{ord}(q)|_{\mathbb{Z}_p^*} = n_1$ and splits in $\mathbb{Z}[\omega_3]$ as $q = \pi_1\pi_1^*$ for a suitable prime $\pi_1 \in \mathbb{Z}[\omega_3]$. If $s = 1$ then q can be chosen to equal $3 \pmod 4$. The fields $\mathbb{Q}(\omega_p)$ and $\mathbb{Q}(\omega_3)$ are linearly disjoint over $\mathbb{Q}$. Let $\mathbb{K}$ be the unique subfield of $\mathbb{Q}(\omega_3)(\omega_p)$ of degree n_1 over $\mathbb{Q}(\omega_3)$ and let $\mathbb{L} = \mathbb{K} \cdot \mathbb{Q}(\omega_{2^{s+1}})$. Then $\mathbb{L}$ is a cyclic extension of $\mathbb{Q}(\omega_3)$, and the element

$$\gamma = \frac{\pi_1}{\pi_1^*}$$

is an (algebraic) unit-magnitude element that is a non-norm element for the extension $\mathbb{L}/\mathbb{Q}(\omega_3)$. When $n_1 = 1$, then $s = 1$ and we can take $\mathbb{L} = \mathbb{Q}(\omega_3)(\imath)$ and $\gamma = \dfrac{3+\omega_3}{3+\omega_3^2}$.

Proof: See Appendix I ■

Some example non-norm elements identified in this way are given in Table I.

TABLE I
NON-NORM ELEMENTS

No. of Antennas	Non-norm 'γ'
2	$(2+\imath)/(1+2\imath)$ $(1+4\imath)/(1-4\imath)$
3	$(3+\omega_3)/(3+\omega_3^*)$ $(1+9\omega_3)/(9+\omega_3)$
4	$(2+\imath)/(2-\imath)$
5	$(3+2\imath)/(3-2\imath)$
6	$(3+7\omega_3)/(3+7\omega_3^*)$
7	$(8+5\imath)/(5+8\imath)$
8	$(2+\imath)/(1+2\imath)$
9	$(3+\omega_3)/(1+3\omega_3)$ $(4+9\imath)/(9+4\imath)$

Remark 1: As we shall see, perfect codes can be constructed using rational-valued γ, i..e, $\gamma \in \mathbb{F} \setminus \mathcal{O}_{\mathbb{F}}$. For the limited situations $(n = 2, 3, 4, 6)$ where perfect codes can also be constructed using an algebraic integer $\gamma \in \mathcal{O}_{\mathbb{F}}$, the use of an algebraic integer yields a larger value of non-vanishing determinant which makes for better error-probability performance.

G. Finding Unitary Matrices G

The goal here is to construct unitary matrices $U(G)$ of the form

$$U(G) \;=\; \kappa G, \tag{13}$$

$$G \;=\; \begin{bmatrix} \beta_0 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \cdots & \sigma(\beta_{n-1}) \\ & \vdots & \\ \sigma^{n-1}(\beta_0) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{bmatrix} ,\tag{14}$$

where

- $\mathbb{F}$ is either $\mathbb{Q}(\imath)$ or else $\mathbb{Q}(\omega_3)$,
- $\mathbb{K}$ is a cyclic, degree-n extension of $\mathbb{F}$ with σ as the generator of the Galois group, as in Propositions 2, 3,
- $\{\beta_i\}$ is an integral basis for $\mathbb{K}/\mathbb{F}$,
- and the scalar κ belongs to $\mathbb{F}$.

We follow the approach adopted in [10]-[14] and regard the matrix G as the generator matrix of the lattice $\{\underline{\lambda}^T G \mid \underline{\lambda} \in \mathbb{Z}^n\}$.

We will first construct unitary matrices $U(G)$ of the form in (13), for the cases when $n = n_1$ is odd and $n = 2^s$ respectively. The Kronecker product of the resulting matrices will turn out to yield a unitary matrix $U(G)$ for the general case $n = 2^s n_1$. Without loss of generality, we will restrict our attention to the QAM case, corresponding to $\mathbb{F} = \mathbb{Q}(\imath)$.

1) Case $n = n_1$ is odd. : Recently, the authors in [14], Section V, give a detailed exposition of a previous result in [10] of an explicit construction of unitary matrices for the case $n = p$, p an odd prime. As we show below, the same construction carries over to the more general case of $n = n_1$, n_1 an odd integer.

- pick an odd prime $p \equiv 1 \pmod{n_1}$ (by a theorem of Dirichlet, (see Theorem 10), this can always be done)
- let $\omega = \omega_p = e^{\frac{2\pi\imath}{p}}$. Let σ denote the generator of the cyclic Galois group $\mathbb{Q}(\omega)/\mathbb{Q}$.
- let r be a primitive element of the field $\mathbb{Z}_p^*$.
- set $m = \frac{p-1}{2}$, and $\alpha = \prod_{k=0}^{m-1}(1-\omega^{r^k})$
- let λ be such that $\lambda(r-1) \equiv 1 \pmod{p}$ and set $z = \omega^\lambda \alpha (1-\omega)$
- Let the automorphism σ be defined by $\sigma(\omega) = \omega^r$, and set $x = \sum_{k=1}^{\frac{p-1}{n_1}} \sigma^{kn_1}(z)$.

The element x lies in the subfield $\mathbb{K}'$ of $\mathbb{Q}(\omega)$ fixed by the subgroup $< \sigma^{n_1} >$ generated by σ^{n_1}. This subfield $\mathbb{K}'$ is a degree-n_1 extension of $\mathbb{Q}$. Then the matrix $U(G_{n_1})$ given below is unitary.

$$U(G_{n_1}) \;=\; \tag{15}$$
$$\frac{1}{p}\begin{bmatrix} x & \sigma(x) & \cdots & \sigma^{n_1-2}(x) & \sigma^{n_1-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & \sigma^{n_1-1}(x) & x \\ \sigma^2(x) & \sigma^3(x) & \cdots & x & \sigma(x) \\ & \vdots & & \vdots & \\ \sigma^{n_1-1}(x) & x & \cdots & \sigma^{n_1-3}(x) & \sigma^{n_1-2}(x) \end{bmatrix}$$

Since $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\imath)$ are linearly disjoint over $\mathbb{Q}$, the field $\mathbb{K} = \mathbb{K}'(\imath)$ will be cyclic over $\mathbb{Q}(\imath)$, and the elements x, $\sigma(x), \ldots, \sigma^{n_1-1}(x)$ will be an integral basis for $\mathbb{K}/\mathbb{Q}(\imath)$.

Proof: See Appendix II. ■

More specifically the first row of $U(G_{n_1})$ is given by

$$U(G_{n_1})(0,j) = \frac{1}{p}\omega^\lambda \alpha \sum_{k=1}^{\frac{p-1}{n_1}} (-1)^{n_1 k + j}(1-\omega^{r^{n_1 k + j}})$$

for $j = 0, .., n_1 - 1$ and the rest of the circulant matrix by:

$$U(G_{n_1})(i+1, j) = U(G_{n_1})(i, j+1 \mod n_1),$$

for $i = 0, \cdots, n_1 - 2$.

Example 2: The first row of the 9-dimensional $U(G_9)$ is $\frac{1}{19}\Big(-2.831\ 7.298\ -1.435\ 4.149\ -8.688\ -8.451\ -6.414\ \ 5.355\ \ -7.983\Big)$ and every successive row is obtained by a single left cyclic shift of the previous row. The matrix was obtained by setting $n_1 = 9,\ p = 19,\ r = 3$ and $\lambda = 10$.

Similarly the first row of the 15-dimensional $U(G_{15})$ is $\frac{1}{31}\Big(-2.242\ 6.361\ -10.78\ -8.071\ 7.253\ -9.45\ 1.127\ -3.334\ 8.806\ -4.391\ 10.442\ 5.404\ -11.12\ -11.004\ -9.989\ \Big)$ obtained by setting $n_1 = 15,\ p = 31,\ r = 3$ and $\lambda = 16$.

2) Case $n = 2^s$ [12]: We once again set $\mathbb{F} = \mathbb{Q}(\imath)$ and consider $\mathbb{K} = \mathbb{Q}(\omega_{m'})$ where $m' = 2^{s+2}$ and $\omega_{m'} = \omega = e^{2\pi\imath/m'}$ the m'^{th} primitive root of unity. $\mathbb{Q}(\omega)$ is a cyclic Galois extension over $\mathbb{Q}(\imath)$. Since the order of 5 in $\mathbb{Z}_{m'}^* \tilde{=} Gal(\mathbb{K}/\mathbb{Q})$ is $m = 2^s = \frac{\phi(m')}{2}$, we see that for $\sigma \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ such that $\sigma(\omega) = \omega^5$, we have that $\sigma(\imath) = \sigma(\omega^{2^s}) = \omega^{2^s 5}\omega^{(1+4)2^s} = \omega^{2^s}\omega^{2^{s+2}} = \omega^{2^s} = \imath$ which gives us $Gal(\mathbb{K}/\mathbb{Q}(\imath)) =< \sigma >$. Take

$\{\omega^0, \omega^1, \omega^2, \cdots, \omega^{m-1}\}$ to be the integral basis over $\mathbb{Q}(\imath)$, and set

$$U(G_{2^s}) = \frac{1}{\sqrt{m}}\Big[\sigma^k(\omega^i)\Big]_{i,k} = \frac{1}{\sqrt{m}}\Big[\omega^{i\cdot 5^k}\Big]_{i,k} \tag{16}$$

Now for $r_i = [1 \ \omega^{5^i} \ \omega^{5^i 2} \ \omega^{5^i 3} \ \cdots \ \omega^{5^i(n-1)}]$, $i = 0, 1, \cdots, m-1$, being the i^{th} row of $\sqrt{m}U(G_{2^s})^T$ in (16), we have that $r_i r_j^\dagger = \sum_{k=0}^{m-1} \omega^{5^i k}\omega^{5^j k} \sum_{k=0}^{m-1} \omega^{k(5^i - 5^j)}$. Since 5 has order $\frac{m'}{4} = \frac{\phi(m')}{2}$ in $\mathbb{Z}_{m'}^{*}$, then $5^i \neq 5^j \ \forall i \neq j, \ i,j = 0, 1, \cdots, \frac{m'}{4} - 1$. This combines with the fact that $k(5^i - 5^j) = k5^j(5^{i-j} - 1) \equiv 0 \pmod 4$ so that each summand pairs with another summand in the summation so that their ratio is ω^4. This symmetry, the fact that $\frac{m'}{2} \equiv 0 \pmod 4$ and the fact that $\omega^{5^i} + (\omega^{5^i})^{\frac{m'}{2}} = 0$, means that each summand ω^{5^i} has another summand as its additive inverse. Together with the fact that the complex conjugate of ω is ω^{-1}, results in $r_i r_j^\dagger = m\delta_{i,j}$ and in the desired unitary property $U(G_{2^s})U(G_{2^s})^\dagger = I$.

3) The General Case $n = 2^s n_1$: We will need the following lemma:

Lemma 4: Let $\mathbb{L}$ be the compositum of l Galois extensions $\mathbb{K}_i$ over $\mathbb{Q}$ of co-prime degrees n_i. Assuming that there exist unitary matrices $U(G_{n_i})$ for all $i = 1, 2, \cdots, l$ then the Kronecker product of these matrices is a $(n \times n)$ unitary matrix $U(G_n)$ of the desired form for $n = \prod_{i=1}^{l} n_i$.

In particular when $n = 2^s n_1$ and $\mathbb{F} = \mathbb{Q}(\imath)$, we can use the Kronecker product of the matrices constructed separately for the case $n = n_1$ odd and $n = 2^s$.

For the case $\mathbb{F} = \mathbb{Q}(\omega_3)$, for $n = n_1$ odd we again use the $n_1 \times n_1$ unitary matrix $U(G_{n_1})$ from Section III-G.1, and for $n = 2n_1$, n_1 odd, the unitary matrix $U(G_n)$ can be taken to be the Kronecker product of $U(G_{n_1})$ and the matrix $U(G_2) = \frac{1}{\sqrt{2}}\begin{vmatrix} 1 & \imath \\ 1 & -\imath \end{vmatrix}$.

This concludes the unified construction of minimum-delay perfect codes. We summarize the results in the form of a proposition:

Proposition 5 (Perfect Codes over QAM): Let $n = 2^s n_1 > 1$ be given, n_1 odd. Let $\mathbb{F} = \mathbb{Q}(\imath)$, let $\mathbb{L}/\mathbb{F}$ be a cyclic Galois extension of $\mathbb{F}$ with σ as the generator of the Galois group. Let $\gamma \in \mathbb{F}^{*}$ be a non-norm element in the extension $\mathbb{L}/\mathbb{F}$ constructed as discussed in Section III-F. Let $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ be a CDA of index n corresponding to this choice of $\mathbb{L}/\mathbb{F}$, γ and σ. Let $\mathcal{B} = \{\beta_1, \beta_2, \cdots, \beta_n\}$ be an integral basis for $\mathcal{O}_{\mathbb{L}}/\mathbb{Z}[\imath]$ as discussed in Section III-G. Let $\mathcal{X}$ be the $(n \times n)$ ST code constructed from $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ the integral basis $\mathcal{B}$ and alphabet $\mathcal{A}_{\text{QAM}}$ as discussed in Section III-G.

Then $\mathcal{X}$ satisfies the 4 defining properties P1-P4 and is hence a perfect code.

A similar proposition can be stated to cover the case of the HEX constellation.

H. Examples of new perfect codes and simulations

1) Examples of new perfect codes: • A 2×2 perfect code can be chosen to have code-matrices which prior to SNR normalization, are of the form

$$\begin{aligned} X &= \frac{1}{\sqrt{2}}\begin{vmatrix} f_{0,0} + f_{0,1}\omega_8^3 & \gamma(f_{1,0} + f_{1,1}\sigma(\omega_8^3)) \\ f_{1,0} + f_{1,1}\omega_8^3 & f_{0,0} + f_{0,1}\sigma(\omega_8^3) \end{vmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{vmatrix} f_{0,0} + f_{0,1}\omega_8^3 & \gamma(f_{1,0} + f_{1,1}\omega_8^7) \\ f_{1,0} + f_{1,1}\omega_8^3 & f_{0,0} + f_{0,1}\omega_8^7 \end{vmatrix} \end{aligned}$$

where $f_{i,j}$ are from the desired QAM constellation, $\omega_8 := e^{\frac{2\pi\imath}{8}}$ and $\gamma = \frac{2+\imath}{1+2\imath}$. Matrices map $n^2 = 4$ information elements from QAM. Furthermore the signalling set, in the form of the layer-by-layer vectorization of the code-matrices, before SNR normalization, comes from the lattice

$$\Lambda = \Big\{[f_{0,0} \ f_{0,1} \ f_{1,0} \ f_{1,1}]R_v \ \mid \\ [f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1}] \in \text{QAM}^{n^2}\Big\}$$

where

$$R_v = \frac{1}{\sqrt{2}}\begin{vmatrix} 1 & 1 & 0 & 0 \\ \omega_8^3 & \omega_8^7 & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & \omega_8^3 & \gamma\omega_8^7 \end{vmatrix}$$

satisfying the defining condition of

$$R_v R_v^\dagger = I_4.$$

We find the smallest possible determinant, prior to SNR normalization, to be

$$\det(\Delta X \Delta X^\dagger)_{\min} = \frac{1}{20}$$

which is larger than some previously constructed 2×2 perfect codes. The code's performance improves if the existing $G = \begin{vmatrix} 1 & 1 \\ \omega_8^3 & \omega_8^7 \end{vmatrix}$ is substituted with $G_2 = \begin{vmatrix} 0.5257 & 0.8507 \\ 0.8507 & -0.5257 \end{vmatrix}$ taken from [14].

Other examples:

- In the case of the 5×5 perfect space-time code, the γ element is given in Table I to be $\gamma = \frac{3+2\imath}{2+3\imath}$. Furthermore, the 5×5 unitary circulant lattice generator matrix G_5, it self defined by its first row:

$$\begin{bmatrix} -0.32601867960931 \\ 0.54852873198059 \\ -0.45573414065529 \\ -0.59688478766687 \\ -0.16989112404934 \end{bmatrix}^T$$

  To obtain G_5 we used the approach in Section III-G.1, setting parameters $n_1 = 5, p = 11, w = e^{2\pi\imath/11}, r = 2, m = 5, \lambda = 1$. To obtain the code, one can either use the vectorized form described in (9), or the linear-dispersion form ([30])

$$\mathcal{X} = \Big\{ X = \sum_{j=0}^{4} \Gamma^j \big(diag(\underline{f}_j \cdot G_5)\big), \ \ \underline{f}_j \in \text{QAM}^5 \Big\}$$

- In the case of the 7×7 perfect space-time code, the γ element is given in Table I to be $\gamma = \frac{8+5\imath}{8-5\imath}$. Furthermore, the 7×7 unitary circulant lattice generator matrix G_7 has the first row equal to:

$$\begin{bmatrix} -0.68093653331388 \\ 0.16310251780907 \\ -0.44885286628634 \\ 0.07738152540498 \\ 0.08232156822109 \\ 0.27555479527388 \\ -0.46857099000493 \end{bmatrix}^T$$

To obtain G_7 we again used the approach in Section III-G.1, setting parameters $n_1 = 7, p = 29, w = e^{2\pi\imath/29}, r = 2, m = 14, \lambda = 1$. As before, the code follows either in the vectorized form (9), or the linear-dispersion form.

$$\mathcal{X} = \left\{ X = \sum_{j=0}^{6} \Gamma^j \big(diag\big(\underline{f}_j \cdot G_7\big)\big), \quad \underline{f}_j \in \text{QAM}^7 \right\}.$$

2) Simulations: All the simulations assume $\mathbb{C}\mathcal{N}(0,1)$ fading and additive noise. We begin with Figure 3 to indicate the performance improvement as the different defining conditions are satisfied one-by-one. The first curve from the top corresponds to satisfying the full-diversity condition (single-dimensional CDA code - orthogonal design). The second curve now includes the full-rate condition (random, full-rate, linear-dispersion codes). The third curve corresponds to the family of DMT optimal but not information lossless CDA codes presented in [2], which achieve the first three criteria of full-diversity, full-rate, and non-vanishing determinant. The performance transition from the CDA codes to perfect codes is described by the next two curves. Figure 4 provides a comparison of the 2×2 perfect code presented here, with some perfect codes from [1]. Figure 5 shows the performance of the newly constructed 5-dimensional perfect code and compares it with the corresponding 5×5, 5-layer, symmetric TAST code ([34]) with full diversity rotation matrix and transcendental Diophantine numbers.

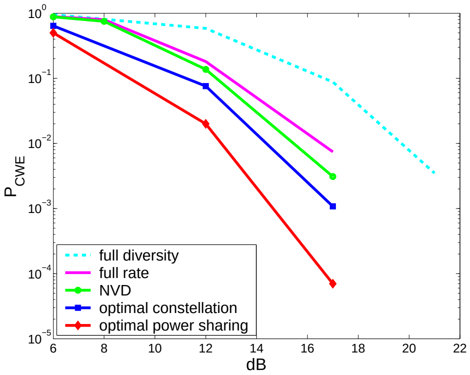

Fig. 3. Performance improvements attributed to achieving the different criteria for the perfect codes.

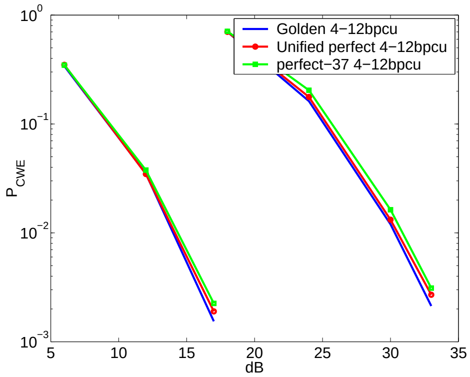

Fig. 4. Comparison of the unified perfect code with two codes, the Golden code and a second previously constructed perfect code. There are 2 receive antennas and sphere decoding is employed.

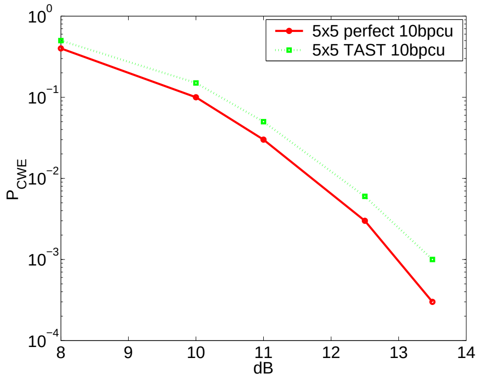

Fig. 5. Comparison of the 5×5 perfect code with the 5×5 TAST code. There exist 5 receive antennas, the rate is at 10 bpcu, and decoding is done using modulo-Λ (sphere) encoding and MMSE-GDFE lattice decoding ([39]).

IV. Rectangular Perfect Code Construction

In this section, we show how perfect codes can be constructed for the case when the number of channel uses T is a multiple of the number n_t of transmit antennas. Thus the corresponding perfect codes in this case are rectangular.

Proposition 6 (Rectangular Perfect Codes over QAM): Let

$$n,\ n_1,\ \mathbb{F},\ \mathbb{L},\ \sigma,\ \gamma,\ \mathcal{B},\ \mathcal{O}_{\mathbb{L}},\ D(\mathbb{L}/\mathbb{F},\sigma,\gamma),\ \mathcal{X}$$

be as in Proposition 5. Then the m-fold Cartesian product $\mathcal{X}^m$

$$\mathcal{X}^m \quad = \quad \underbrace{\mathcal{X} \times \mathcal{X} \times \cdots \times \mathcal{X}}_{\text{m copies}}$$

satisfies the 4 defining properties P1-P4 and is hence a perfect code.

Proof: It is not hard to verify that the Cartesian product satisfies properties P1, P3 and P4. It remains to verify the non-vanishing determinant property, P2. Consider the difference

$$\begin{aligned} \Delta X \quad &= \quad [X_1^{(1)}\ X_1^{(2)} \dots X_1^{(m)}] \ - \\ &\quad\quad\ [X_2^{(1)}\ X_2^{(2)} \dots X_2^{(m)}] \\ &= \quad [\Delta X^{(1)}\ \Delta X^{(2)} \dots\ \Delta X^{(m)}] \end{aligned}$$

between any two distinct code matrices in the product code $\mathcal{X}$. At least one of the $\Delta X^{(k)}$, say, $\Delta X^{(k_0)}$ must be nonzero. Next, let us write

$$\Delta X \Delta X^{\dagger} = [\Delta X^{(k_0)}][\Delta X^{(k_0)}]^{\dagger} \tag{17}$$

$$+ \sum_{k=1, k\neq k_0}^{m} [\Delta X^{(k)}][\Delta X^{(k)}]^{\dagger} \tag{18}$$

$$= A + B \tag{19}$$

where $A = [\Delta X^{(k_0)}][\Delta X^{(k_0)}]^{\dagger}$ and

$$B = \sum_{k=1, k\neq k_0}^{m} [\Delta X^{(k)}][\Delta X^{(k)}]^{\dagger}.$$

Let

$$\mu_1^{(A)} \leq \mu_2^{(A)} \leq \cdots \leq \mu_{n_t}^{(A)} \qquad \text{and}$$
$$\mu_1^{(A+B)} \leq \mu_2^{(A+B)} \leq \cdots \leq \mu_{n_t}^{(A+B)}$$

denote the ordered eigenvalues of the Hermitian matrices $A, A+B$ respectively. Then from a theorem of Weyl (see Theorem 4.3.1 of [50]), we have that

$$\mu_i^{(A+B)} \geq \mu_i^{(A)}, \quad 1 \leq i \leq n_t.$$

As a result, we have that

$$\begin{aligned} \det([A+B]) &\geq \det(A) \\ &\dot{\geq} \text{SNR}^0. \end{aligned}$$

Thus the non-vanishing determinant property, Property P2, is also met.

■

V. Additional Attributes of Perfect Codes

A. *Information losslessness*

The ergodic capacity C of the Rayleigh space-time channel

$$\underline{y} = H\underline{x} + \underline{w}$$

is given by, see [38]

$$C = \log\det(I + \frac{\rho}{n} HH^{\dagger}),$$

where SNR is now defined as ρ.

Let $\mathcal{Z}$ be a linear dispersion space time code where each $(n_t \times T)$ code matrix $Z \in \mathcal{Z}$ has an expansion of the form

$$Z = \sum_{i=1}^{k} f_k F_k,$$

in which the information-bearing symbols $\{f_k\}$ are chosen from some alphabet $\mathcal{A}$. Let

$$\begin{aligned} \underline{f} &= [f_1 \ f_2 \ \cdots f_k]^T \\ R_f &= \mathbb{E}(\underline{f}\underline{f}^{\dagger}). \end{aligned}$$

The maximum amount $C^{'}$ of information per channel use that can be transferred across the ST channel using this ST code is given by

$$C^{'} = \max_{R_f \quad \text{Tr}(R_f) \leq T\rho} I(Y; \sum_k f_k F_k \mid H).$$

In [29], a code is defined to be information lossless if the structure imposed by the dispersion matrices F_k, does not result in a reduction of the achievable mutual information. This comparison takes place under the assumption that the information symbols in $\underline{f}$ are drawn randomly from a Gaussian distribution, and that the corresponding covariance matrix is a scaled identity matrix. Without any loss of generality, we proceed and for our setting we set

$$R_f = \rho^{\frac{r}{n}} I_{n^2}.$$

In accordance with the above, we will assume Gaussian $\underline{f}$ and will say that a space-time code $\mathcal{Z}$ is information lossless over the Rayleigh channel if $C^{'} = C$. We now show that the structure of the perfect ST codes allows for this property.

Firstly, perfect ST codes are linear dispersion codes having parameters $n_t = T = n$, $k = n^2$. Given an $(m \times n)$ matrix A having columns $\underline{a}_i$, i.e.,

$$A = \left[\begin{array}{cccc} \underline{a}_1 & \underline{a}_2 & \cdots & \underline{a}_n \end{array} \right],$$

we will use $\text{vec}(A)$ to denote the vectorized version of the matrix, i.e.,

$$\text{vec}(A) = \left[\begin{array}{c} \underline{a}_1 \\ \underline{a}_2 \\ \vdots \\ \underline{a}_n \end{array} \right].$$

Let

$$\mathcal{H} = \text{diag}(\underbrace{H, H, \ldots, H}_{\text{n times}}).$$

Next note that if

$$Y = \theta H X + W,$$

then

$$\begin{aligned} \text{vec}(Y) &= \text{vec}(\theta H X) + \text{vec}(W) \\ &= \mathcal{H}\text{vec}(\theta X) + \text{vec}(W). \end{aligned}$$

In the case of a perfect code $\mathcal{Z}$, the vector $\text{vec}(X)$ is related via a permutation matrix P to the layered vector $\underline{\text{lay}}(X)$ introduced earlier, so that we have

$$\begin{aligned} \text{vec}(Y) &= \mathcal{H} \ P \ \underline{\text{lay}}(\theta X) + \text{vec}(W) \\ &= \mathcal{H} \ P \ \Upsilon \left(\theta \underline{f}\right) + \text{vec}(W) \end{aligned}$$

We note that $\kappa P \Upsilon$ is a unitary matrix since both $P, \kappa\Upsilon$ are unitary. The maximum mutual information $C^{'}$ that can be transferred using the perfect code is given by

$$C^{'} = \max_{R_f, \quad \text{Tr}(R_f) \leq n\rho} \frac{1}{n} \log\det(I + \theta^2 \mathcal{H} P \Upsilon R_f \Upsilon^{\dagger} P^{\dagger} \mathcal{H}^{\dagger}).$$

Clearly we have the upper bound

$$C^{'} \leq C.$$

We also know that the matrix $\kappa P \Upsilon$ is unitary. Combining the two gives us that

$$C^{'} \geq \frac{1}{n} \log\det(I + \frac{\theta^2 \rho^{\frac{r}{n}}}{\kappa^2} \mathcal{H}\mathcal{H}^{\dagger}).$$

The constant θ was chosen to meet the SNR requirement and hence it must be that

$$\begin{aligned} n\rho &= \mathbb{E}(\mathrm{Tr}(\theta^2 XX^\dagger)) \\ &= \mathbb{E}(\mathrm{Tr}(\theta^2 P\Upsilon R_f \Upsilon^\dagger P^\dagger)) \\ &= n^2 \frac{\theta^2 \rho^{\frac{r}{n}}}{\kappa^2} \end{aligned}$$

i.e.,

$$\begin{aligned} \frac{\theta^2 \rho^{\frac{r}{n}}}{\kappa^2} &= \frac{\rho}{n} \\ C^{'} &\geq \frac{1}{n}\log\det(I + \frac{\rho}{n}\mathcal{H}\mathcal{H}^\dagger) \\ &\geq C \end{aligned}$$

and it follows that $C^{'} = C$. This establishes that the structure of perfect codes allows for information losslessness over the Rayleigh fading channel. This proof extends to rotationally-invariant channels H, i.e., channels H such that H, HQ_1 and Q_2H for Q_1, Q_2 unitary, have the same statistics.

B. Approximate Universality

Theorem 7 (Approximate Universality [26]): An $(n_t \times T)$ space-time code $\mathcal{X}$ is approximately universal iff the ordered, squared-singular values $\{\ell_i\}_{i=1}^{n_t}$ of every difference matrix $\Delta X = X_1 - X_2$, $X_1, X_2 \in \mathcal{X}$, $X_1 \neq X_2$ satisfy

$$\prod_{i=1}^{m} \ell_i \ \dot{\geq}\ \rho^{m-r}$$

where $m = \min\{n_t, n_r\}$. The singular values are assumed to be ordered in increasing order, i.e.,

$$\ell_1 \leq \ell_2 \leq \cdots \leq \ell_{n_t}.$$

We now show that perfect codes over the QAM constellation are approximately universal. The proof in the case of the HEX constellation is similar and will be omitted.

Consider a perfect code over a QAM constellation of size M^2. Since an $(n_t \times n_t)$ perfect code is full rate, it must be that

$$\begin{aligned} [M^2]^{n_t^2} &= \rho^{rn_t} \\ \Rightarrow M^2 &= \rho^{\frac{r}{n_t}}. \end{aligned}$$

Each code matrix Z in the perfect code is of the form

$$Z = \theta X.$$

Since each element transmits the same energy on the average, it must be that

$$\theta^2 \doteq \rho^{1-\frac{r}{n_t}}.$$

Consider the case when $n_r \geq n_t$. In this case, $m = n_t$ and we have

$$\begin{aligned} \prod_{i=1}^{n_t} \ell_i &\doteq \rho^0 \theta^{n_t(1-\frac{r}{n_t})} \\ &= \rho^{n_t - r}, \end{aligned}$$

so that perfect codes are approximately universal in this case. For the case when $n_r < n_t$, $m = n_r$. Note that

$$\begin{aligned} \ell_i &\ \dot{\leq}\ \mathrm{Tr}(\theta^2 \Delta X \Delta X^\dagger) \\ &\doteq \rho, \end{aligned}$$

so that

$$\ell_i \ \dot{\leq}\ \rho.$$

It follows that

$$\begin{aligned} \prod_{i=1}^{m} \ell_i &\ \dot{\geq}\ \frac{\rho^{n_t - r}}{\rho^{n_t - m}} \\ &= \rho^{m-r}, \end{aligned}$$

which shows that perfect codes are approximately universal even in this case.

C. Residual approximate universality

This property states that if certain rows of a perfect code are deleted, then the row-deleted code is approximately universal for the appropriately reduced number of transmit antennas.

This observation follows from the results in [2]. For the sake of completeness, we provide a proof.

Let $\mathcal{Z}$ be an $(n_t \times n_t)$ perfect ST code. Next, let $\mathcal{Z}_n$ be the $(n \times n_t)$ rectangular ST code obtained by deleting a particular set of $(n_t - n)$ rows from every code matrix $Z \in \mathcal{Z}$. Then the $(n \times n_t)$ ST code $\mathcal{Z}_R$ is approximately universal for n transmit antennas.

We first observe that $\Delta Z_n \Delta Z_n^\dagger$ is a $(n \times n)$ principal submatrix of $\Delta Z \Delta Z^\dagger$. Let

$$\mu_1 \leq \mu_2 \leq \cdots \leq \mu_n \tag{20}$$
$$\ell_1 \leq \ell_2 \leq \cdots \leq \ell_n \leq \cdots \leq \ell_{n_t} \tag{21}$$

be the ordered eigenvalues of $\Delta Z_n \Delta Z_n^\dagger$ and $\Delta Z \Delta Z^\dagger$ respectively. By the inclusion principle of Hermitian matrices, (see Theorem 4.3.15 of [50]) the smallest eigenvalues of $\Delta Z_R \Delta Z_R^\dagger$ dominate the corresponding smallest eigenvalues of $\Delta Z_S \Delta Z_S^\dagger$, i.e.,

$$\mu_k \geq \ell_k, \quad 1 \leq k \leq n.$$

Since $||\Delta Z||_F^2 \ \dot{\leq}\ \rho$, it follows that every eigenvalue ℓ_k of $\Delta Z \Delta Z^\dagger$ is bounded above by ρ. If the ST code $\mathcal{Z}$ is designed to operate at rate $r\log(\rho)$ bits per channel use, then we have

$$\begin{aligned} \det(\Delta Z_n \Delta Z_n^\dagger) &\ \dot{\geq}\ \frac{\mathrm{SNR}^{n_t - r}}{\mathrm{SNR}^{n_t - n}} \\ &= \mathrm{SNR}^{n-r} \end{aligned}$$

and it follows that the row-deleted code is also clearly approximately universal.

VI. Conclusion

We have explicitly constructed perfect space-time codes for any number n_t of transmit antennas, any number n_r of receive antennas and any delay T that is a multiple of n. In addition we have identified some additional properties satisfied by perfect codes, which make for good error probability performance.

Appendix I
Proof of Propositions 2 and 3

We first recall three results that relate to identifying a "non-norm" element γ.

Lemma 8: [9] Let $\mathbb{L}$ 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 $\mathfrak{P} \subset \mathcal{O}_{\mathbb{L}}$ 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 $\gamma^i \notin N_{\mathbb{L}/\mathbb{F}}(\mathbb{L})$ for any $i = 1, 2, \cdots, f-1$.

Thus, in order to find a "non-norm" element γ in $\mathbb{F} = \mathbb{Q}(\imath)$ ($\mathbb{F} = \mathbb{Q}(\omega_3)$), it is sufficient to find a prime ideal in $\mathbb{Z}[\imath]$ ($\mathbb{Z}[\omega_3]$) whose inertial degree f in $\mathbb{L}/\mathbb{F}$ is $f = [\mathbb{L} : \mathbb{F}] = n$. Such an ideal is said to be inert in $\mathbb{L}/\mathbb{F}$.

Lemma 9: [48] Let p be any odd prime. Then for any integer k, $\mathbb{Z}^{*}_{p^k}$ 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 $\mathbb{Z}^{*}_{p^k}$.

Theorem 10: (Dirichlet's theorem) Let a, m be integers such that $1 \leq a \leq m, \gcd(a,m) = 1$. Then the arithmetic progression $\{a, a+m, a+2m, \ldots, a+km, \ldots\}$ contains infinitely many primes.

We now discuss separately, the cases when $\mathbb{F} = \mathbb{Q}(\imath)$ and $\mathbb{F} = \mathbb{Q}(\omega_3)$.

a) Unit-magnitude, non-norm elements for $\mathbb{F} = \mathbb{Q}(\imath)$: Let

$$n = 2^s n_1$$

where n_1 is odd. Assume first that $n_1 > 1$. Let p be the smallest odd prime p such that $n_1 \mid (p-1)$. Such a prime is guaranteed to exist by Dirichlet's theorem applied to the progression

$$1, 1+n_1, \ldots, 1+kn_1, \ldots,$$

The cyclic group $\mathbb{Z}^{*}_{p}$ contains an element whose order equals $(p-1)$. Let a denote this element. Our first goal is to find a prime q such that

$$\begin{aligned} q &= 5 \pmod{2^{s+2}} \\ q &= a \pmod{p}. \end{aligned}$$

Note that

$$q = 1 \pmod{4}\ .$$

Since $(2^{s+2}, p) = 1$, we can, by the Chinese Remainder Theorem, find an integer b such that

$$\begin{aligned} b &= 5 \pmod{2^{s+2}} \\ b &= a \pmod{p}. \end{aligned}$$

Note that such an integer b is relatively prime to $2^{s+2}p$. Consider the arithmetic progression

$$b + l(2^{s+2}p), \quad l = 0, 1, 2, \ldots$$

By Dirichlet's theorem, this arithmetic progression is guaranteed to contain a prime q having the desired properties. Now let us verify that this leads to a CDA.

Let $\mathbb{K}^{'}$ be the subfield of $\mathbb{Q}(\omega_p)$ that is a cyclic extension of $\mathbb{Q}$ of degree n_1. Let $\mathbb{K}$ be the compositum of $\mathbb{K}^{'}$ and $\mathbb{Q}(\imath)$ and let $\mathbb{L}$ be the compositum of the fields $\mathbb{K}$ and $\mathbb{Q}(\omega_{2^{s+2}})$. Note that $\mathbb{L}$ is cyclic over $\mathbb{Q}(\imath)$, since it is a composite of the cyclic extension $\mathbb{Q}(\omega_{2^{s+2}})/\mathbb{Q}(\imath)$ of degree 2^s and the cyclic extension $\mathbb{K}/\mathbb{Q}(\imath)$ of degree n_1 (note that 2^s and n_1 are relatively prime). Next consider the decomposition of the prime ideal (q) in the extension $\mathbb{L}/\mathbb{Q}$.

Since $q = 1 \pmod 4$ we have that in the extension $\mathbb{Q}(\omega_{2^{s+2}})/\mathbb{Q}$, q has inertial degree equal to 2^s. Since q has order $(p-1)$ in $\mathbb{Z}_p$ it follows that q remains inert in $\mathbb{Q}(\omega_p)/\mathbb{Q}$. Since $q = 5 \pmod{2^{s+2}}$ and 5 has order 2^s in $\mathbb{Z}_{2^{s+2}}$, it follows that in the extension $\mathbb{Q}(\omega_{2^{s+2}})/\mathbb{Q}$, q splits completely in $\mathbb{Q}(\imath)/\mathbb{Q}$ but remains inert thereafter.

Let q split in $\mathbb{Q}(\imath)/\mathbb{Q}$ according to

$$q = \pi_1 \pi_1^*$$

where $\pi_1 = (a + \imath b)$ and $\pi_1^* = (a - \imath b)$. Now by using the fact that in a field tower $[\mathbb{E} : \mathbb{K} : \mathbb{F}]$ of field extensions, $f_{\mathbb{E}/\mathbb{F}} = f_{\mathbb{E}/\mathbb{K}} f_{\mathbb{K}/\mathbb{F}}$, $g_{\mathbb{E}/\mathbb{F}} = g_{\mathbb{E}/\mathbb{K}} g_{\mathbb{K}/\mathbb{F}}$, $[\mathbb{E} : \mathbb{F}] = f_{\mathbb{E}/\mathbb{F}}\ g_{\mathbb{E}/\mathbb{F}}$, it follows that π_1 remains inert in the extension $\mathbb{L}/\mathbb{Q}(\imath)$.

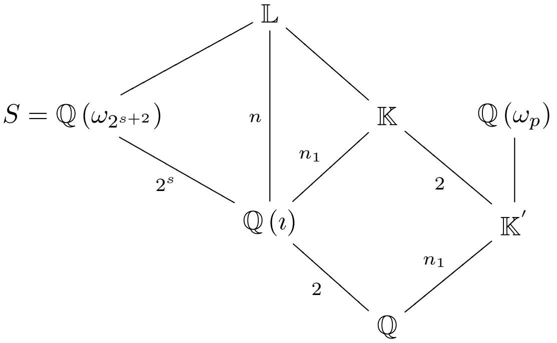

Fig. 6. Constructing a cyclic extension of $\mathbb{Q}(\imath)$ of degree $n = 2^s n_1$. The integers shown indicate the degree of the corresponding extension.

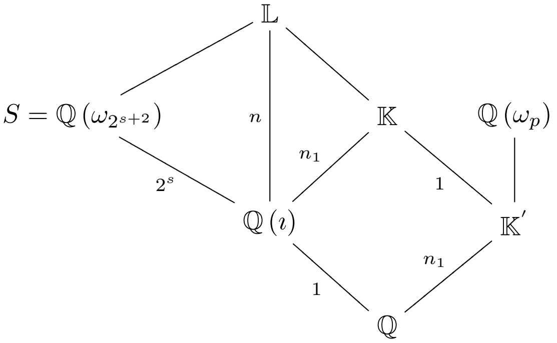

Fig. 7. Constructing a cyclic extension of $\mathbb{Q}(\imath)$ of degree $n = 2^s n_1$. The integers shown indicate the inertial degrees associated with the decomposition of either the prime ideal $q\mathbb{Z}$ or of one of its factors, over the corresponding extension.

To now find a non-norm element of unit magnitude, we note that since the units of $\mathbb{Z}[\imath]$ belong to the set $\{\pm 1,\ \pm \imath\}$, the associates of

$$\pi_1 \;=\; a + \imath b \quad \text{belong to the set}$$

$$\{a + \imath b,\quad -a - \imath b,\quad \imath(a + \imath b),\quad -\imath(a + \imath b)\}.$$

It follows that since $ab \neq 0$, and since $a \neq \pm b$ (or else q would not be prime), $a - \imath b$ does not belong to the set of associates of $a + \imath b$. Our goal now is to show that

$$\gamma \ = \ \frac{\pi_1}{\pi_1^*}$$

is a non-norm element, i.e., that the smallest exponent k for which γ^k is the norm of an element in $\mathbb{L}$, is n. This is the case since if

$$\gamma^k \ = \ N_{\mathbb{L}/\mathbb{F}}(\ell) \quad \text{some } \ell \in \mathbb{L}$$

then

$$\pi_1^k \ = \ (\pi_1^*)^k \prod_{l=0}^{n-1} \sigma^l(\ell)$$

where σ is the generator of the cyclic Galois group of $\mathbb{L}/\mathbb{F}$. For $\ell = \frac{a}{b}$, $a, b \in \mathcal{O}_{\mathbb{L}}$, we have, in terms of ideals of $\mathcal{O}_{\mathbb{L}}$,

$$(\pi_1)^k \prod_{l=0}^{n-1} (\sigma^l(b)) \ = \ (\pi_1^*)^k \prod_{l=0}^{n-1} (\sigma^l(a)).$$

Since the primes π_1 and π_1^* are relatively prime, π_1 must divide $\sigma^l(a)$ for some l. But since $\sigma(\pi_1) = \pi_1$ we have that if (π_1) divides $(\sigma^l(x))$ for some l and $x \in \mathcal{O}_{\mathbb{L}}$, it must divide $(\sigma^l(x))$, for all l. This in turn implies that the power of (π_1) in the prime decomposition of $(\pi_1)^k \prod_{l=0}^{n-1}(\sigma^l(b))$ is $k \mod n$ whereas the power of (π_1) in the prime decomposition of $(\pi_1^*)^k \prod_{l=0}^{n-1}(\sigma^l(a))$ is a multiple of n and it follows that γ is a non-norm element. Equivalently k must be a multiple of n.

When $n_1 = 1$, it is sufficient to take q to equal 5, and $\mathbb{L} = \mathbb{Q}(\omega_{2^{s+2}})$. The prime 5 splits in $\mathbb{Q}(\imath)$ as $(1+2\imath)(1-2\imath)$ and then each of $(1+2\imath)$ and $(1-2\imath)$ remain inert in the extension $\mathbb{L}/\mathbb{Q}(\imath)$. The element

$$\gamma = \frac{1+2\imath}{1-2\imath}$$

is then a non-norm element for this extension, for the same reasons as above. This concludes the proof of Proposition 2. □

b) Unit-magnitude, non-norm elements for $\mathbb{F} = \mathbb{Q}(\omega_3)$: Let $n = 2^s n_1$, $s \in \{0,1\}$ where n_1 is odd. The proof is similar to when $\mathbb{F} = \mathbb{Q}(\imath)$. Assume first that $n_1 > 1$. We find a prime $p \equiv 1 \pmod{n_1}$, $p > 3$ and a prime $q \in \mathbb{Z}$, $q \equiv 1 \pmod 3$, with $\text{ord}(q) = n_1$, when $q \pmod p$ is considered as an element of $\mathbb{Z}_p^*$. If $s = 1$, we also require that $q \equiv 3 \pmod 4$. Assume that we have found such a p and q. The arguments for the rest of the statements in this paragraph are all exactly as in the case when $\mathbb{F} = \mathbb{Q}(\imath)$: The conditions $\text{ord}(q \pmod p) = n_1$ in $\mathbb{Z}_p^*$ and $q \equiv 3 \pmod 4$ (if $s = 1$) guarantee that the prime q remains inert in the ring of integers $\mathcal{O}_{\mathbb{L}'}$ of the cyclotomic field $\mathbb{L}' = \mathbb{K}(\omega_{2^{s+1}})$, where $\mathbb{K}$ is the unique subfield of degree n_1 in the extension $\mathbb{Q}(\omega_p)/\mathbb{Q}$. The extension $\mathbb{L}'/\mathbb{Q}$ is cyclic of degree $2^s n_1$.

Since $q \equiv 1 \pmod 3$, the prime q splits into two distinct primes π_1, π_2 in $\mathbb{Z}[\omega_3]$ which are conjugates of each other. Let $\mathbb{L} = \mathbb{L}'(\omega_3)$, then $\mathbb{L}/\mathbb{Q}(\omega_3)$ can be verified to be cyclic of degree $2^s n_1$. Then π_1 will remain inert in the extension $\mathbb{L}/\mathbb{Q}(\omega_3)$. The element $\gamma = \frac{\pi_1}{\pi_2} = \frac{\pi_1}{\pi_1^*}$ will then be a unit-magnitude (algebraic) non-norm element for the extension $\mathbb{L}/\mathbb{Q}(\omega_3)$, and the codes constructed with this data will then be perfect, i.e. be full-rate, have non-vanishing determinant, and of course, will satisfy the equal power-sharing constraint as γ is of unit-magnitude.

What is left is to find p and q. The prime p is found using Dirichlet as in the case where $\mathbb{F} = \mathbb{Q}(\imath)$. To find q, first find an integer b that is simultaneously congruent to $1 \pmod 3$, to $m \pmod p$, where m is a generator of $\mathbb{Z}_{p*}$, and (if $s = 1$) to $3 \pmod 4$. This is possible by the Chinese Remainder Theorem. Next, find the prime q by applying Dirichlet's theorem to the arithmetic sequence $b + l(3p)$, $l = 0, 1, 2, \ldots$ if $s = 0$ and the sequence $b + l(12p)$, $l = 0, 1, 2, \ldots$ if $s = 1$.

When $n_1 = 1$ (so $s = 1$), we take $\mathbb{L}$ to be $\mathbb{Q}(\omega_3)(\imath)$, and the prime q to be 7. Since q is congruent to $1 \pmod 3$ and to $3 \pmod 4$, q splits into $3 + \omega_3$ and $3 + \omega_3^2$ in $\mathbb{Q}(\omega_3)$ but remains inert in the extension $\mathbb{Q}(\imath)/\mathbb{Q}$. It follows that each of $3 + \omega_3$ and $3 + \omega_3^2$ remain inert in the extension $\mathbb{L}/\mathbb{Q}(\omega_3)$. The element

$$\gamma = \frac{3+\omega_3}{3+\omega_3^2}$$

will then be a non-norm element for this extension, for the same reasons as above. This concludes the proof of Proposition 3. □

Appendix II
Orthogonal Lattices in $\mathcal{O}_{\mathbb{K}}$, Where $\mathbb{K}/\mathbb{Q}$ is Cyclic Galois of Odd Degree

For simplicity, in this section, we write n in place of n_1 and $\mathbb{K}$ in place of $\mathbb{K}'$.

We here show that the construction in [10] (of which a detailed exposition has been provided in [14, Section 5]) of lattices that belong in a cyclic Galois extension $\mathbb{K}$ of *prime* degree q over $\mathbb{Q}$, actually gives without any modification orthogonal lattices *for any odd degree n*. We follow the exposition in [14] closely, and show that the proofs there only require that n be odd, and that the assumption that n be an odd prime is unnecessary.

To this end, let $n \geq 3$ be a given odd integer, and fix a prime $p \equiv 1 \pmod n$. Note that such a prime p can always be found since by Dirichlet's theorem, Theorem 10, the sequence $\{1 + dn,\ d = 1, 2, \cdots\}$ contains infinitely many primes. Let ω be a primitive p-th root of unity. Thus, $\mathbb{Q}(\omega)$ is cyclic of degree $p-1$ over $\mathbb{Q}$, and contains the real subfield $\mathbb{Q}(\omega + \omega^{-1})$ which is cyclic of degree $(p-1)/2$ over $\mathbb{Q}$. Since n divides $p - 1$, there is a unique field $\mathbb{K}$ contained in $\mathbb{Q}(\omega)$ which is cyclic of degree n over $\mathbb{Q}$. This is the field we will work with. Note that since n is odd, n divides $(p-1)/2$ as well, so $\mathbb{K}$ is contained in the real subfield $\mathbb{Q}(\omega + \omega^{-1})$.

Let $G = \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, with generator σ, chosen so that $\sigma(\omega) = \omega^r$, where in turn, r is a generator of $\mathbb{Z}_p^{\circledast}$. We let $m = \frac{p-1}{2}$, and observe that $r^m \equiv -1 \pmod p$. We also choose λ so that $\lambda(r-1) \equiv 1 \pmod p$.

We define α by $\alpha = \prod_{k=0}^{m-1}(1 - \omega^{r^k})$. The following result is just a combination of Lemmas 3 and 4 of [14], and since they have to do purely with the cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ and have nothing to do with n, their proofs remain valid:

Lemma 11: The following equalities hold:

1) $\sigma(\alpha) = -\omega^{p-1}\alpha$
2) $\sigma(\omega^{\lambda}\alpha) = -\omega^{\lambda}\alpha$
3) $(\omega^{\lambda}\alpha)^2 = (-1)^m p$

We now define $z = \omega^{\lambda}\alpha(1-\omega) \in \mathcal{O}_{\mathbb{Q}(\omega)}$, and

$$x = Tr_{\mathbb{Q}(\omega)/\mathbb{K}}(z) = \sum_{j=1}^{(p-1)/n} \sigma^{jn}(z).$$

Note that x is in $\mathcal{O}_{\mathbb{K}}$, as z is in $\mathcal{O}_{\mathbb{Q}(\omega)}$. Observing that

$$[G_nG_n^T](i,j) \;=\; Tr_{\mathbb{K}/\mathbb{Q}}(\sigma^i(x)\sigma^j(x)), \;\;\; 0 \le i,j \le (n-1),$$

we are interested in $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x))$. The following, which is Proposition 2 of [14], gives us the key to constructing the orthogonal lattice.

Proposition 12: $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = p^2\delta_{0,t}$, for $t = 0,\dots,n-1$.

Remark 2: Note that $Tr_{\mathbb{K}/\mathbb{Q}}(\sigma^i(x)\sigma^j(x)) = Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^{j-i}(x))$. Thus, if we embed $\mathcal{O}_{\mathbb{K}}$ in $\mathbb{R}^n$ via $a \mapsto v(a) = [a, \sigma(a), \dots, \sigma^{n-1}(a)]$ (note that $\mathbb{K}$ is a real field), this Proposition says that the vectors $[v(x), v(\sigma(x), \dots, v(\sigma^{n-1}(x))]$ are orthogonal to one another.

Proof: For n being odd, we have

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) &= \sum_{a=0}^{n-1}\sigma^a(x\sigma^t(x)) \\ &= \sum_{a=0}^{n-1}\sum_{c,j=1}^{(p-1)/n} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \end{aligned}$$

and from Lemma 11

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = \sum_{a=0}^{n-1}\sum_{c,j=1}^{(p-1)/n} &(-1)^{a+cn}\omega^{\lambda}\alpha(1-\omega^{r^{a+cn}}) \\ &\cdot (-1)^{a+t+jn}\omega^{\lambda}\alpha(1-\omega^{r^{a+t+jn}}) \end{aligned}$$

We observe that since n is odd, $(-1)^{cn} = (-1)^c$ and $(-1)^{jn} = (-1)^j$. Moreover, $(-1)^a(-1)^a = 1$, and $(-1)^t$ is common to the sums above. By Lemma 11, we may replace $(\omega^{\lambda})^2$ by $(-1)^m p$. Thus we find, after rearranging the sums, that

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = (-1)^t(-1)^m p &\sum_{c=1}^{(p-1)/n}(-1)^c \cdot \\ \cdot \Bigg[\sum_{a=0}^{n-1}\sum_{j=1}^{(p-1)/n} &(-1)^j(1-\omega^{r^{a+cn}}) \\ - \sum_{a=0}^{n-1}\sum_{j=1}^{(p-1)/n} (-1)^j(&\omega^{r^{a+t+jn}} - \omega^{r^{a+cn}+r^{a+t+jn}})\Bigg] \end{aligned}$$

Now the term $\sum_{j=1}^{(p-1)/n}(-1)^j(1-\omega^{r^{a+cn}})$ can be rewritten as $(1-\omega^{r^{a+cn}})\sum_{j=1}^{(p-1)/n}(-1)^j$. Since n is odd, $(p-1)/n$ is even, and hence, there are as many positive as negative terms in the expression $\sum_{j=1}^{(p-1)/n}(-1)^j$, and thus, the sum becomes zero. Similarly, the term $\sum_{c=1}^{(p-1)/n}(-1)^c\sum_{a=0}^{n-1}(-\sum_{j=1}^{(p-1)/n}(-1)^j(\omega^{r^{a+t+jn}})$ becomes zero: this is because the terms in $\sum_{a=0}^{n-1}(-\sum_{j=1}^{(p-1)/n}(-1)^j(\omega^{r^{a+t+jn}})$ are independent of c, while the term $\sum_{c=1}^{(p-1)/n}(-1)^c = 0$ as $(p-1)/n$ is even and there as many positive as negative terms. We thus find

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = (-1)^{t+m}p &\sum_{c=1}^{(p-1)/n}(-1)^c \cdot \\ &\cdot \sum_{a=0}^{n-1}\sum_{j=1}^{(p-1)/n}(-1)^j\omega^{r^{a+cn}+r^{a+t+jn}} \end{aligned}$$

We now have the following:

Lemma 13:

$$\begin{aligned} &\sum_{c=1}^{(p-1)/n}(-1)^c\sum_{a=0}^{n-1}\sum_{j=1}^{(p-1)/n}(-1)^j\omega^{r^{a+cn}+r^{a+t+jn}} \\ &\quad = \sum_{d=1}^{(p-1)/n}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{(p-1)/n}\omega^{r^{a+nd+nk}+r^{a+t+nk}} \\ &\quad\quad = \sum_{d=1}^{(p-1)/n}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{(p-1)/n}\omega^{r^{a+kn}(r^{nd}+r^t)} \end{aligned}$$

Proof: See Appendix III ■

As in [14], we write

$$\begin{aligned} &\sum_{d=1}^{(p-1)/n}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{(p-1)/n}\omega^{r^{a+kn}(r^{nd}+r^t)} \\ &\qquad\qquad = \sum_{d=1}^{(p-1)/n}(-1)^d\sum_{s=1}^{(p-1)}\omega_{d,t}^s \end{aligned}$$

where $\omega_{d,t} = \omega^{(r^{nd}+r^t)}$, and of course,

$$\sum_{s=1}^{(p-1)}\omega_{d,t}^s = \begin{cases} p-1 & \text{if } \omega_{d,t} = 1, \\ -1 & \text{otherwise} \end{cases}$$

To determine when $\omega_{d,t} = 1$, note that this happens (as in [14]) when $t = nd - m + k_1(p-1)$. Since n is odd, n divides m, so n must divide t. This forces $t = 0$.

We now have $\omega_{d,t} = 1$ implies $r^{nd} \equiv -1 \pmod{p}$, and writing -1 as r^m, yields $nd - m = l(p-1)$ for some l. This then gives $d = (p-1)(2l+1)/2n$, which we may write as $(2l+1)$ times $(p-1)/2n$ (note again that since n is odd, n divides $(p-1)/2$). Since d varies in the range $1,\dots,(p-1)/n$, we find that l must be zero, that is, $d = (p-1)/2n$. Thus, $\omega_{d,t} = 1$ precisely when $t = 0$ and $d = (p-1)/2n$.

In particular, when $t \neq 0$ then $\omega_{d,t} \neq 1$ and we have that

$$\begin{aligned} Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) &= (-1)^{t+m}p\sum_{d=1}^{(p-1)/n}(-1)^d\sum_{s=1}^{(p-1)}\omega_{d,t}^s \\ &= (-1)^{t+m}p\sum_{d=1}^{(p-1)/n}(-1)^d(-1) \end{aligned}$$

Once again, since n is odd, $(p-1)/n$ is even, so the term $\sum_{d=1}^{(p-1)/n}(-1)^d = 0$. Thus, for $t \neq 0$, $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = 0$.

When $t=0$, we find

$$Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = (-1)^m p \sum_{d=1,d\neq(p-1)/2n}^{(p-1)/n} \Big[(-1)^d(-1) + (-1)^m p(-1)^{(p-1)/2n}(p-1)\Big]$$

and the right side then yields $p+p(p-1)=p^2$. To see this last fact, consider first the case where $(p-1)/2$ is even (i.e., $p \equiv 1 \bmod 4$). Then, since n is odd, $(p-1)/2n$ is also even. The sum $\sum_{d=1,d\neq(p-1)/2n}^{(p-1)/n}(-1)^d$ equals $\sum_{d=1}^{(p-1)/n}(-1)^d - (-1)^{(p-1)/2n}$, and we have already seen that, again because n is odd, $\sum_{d=1}^{(p-1)/n}(-1)^d = 0$. Thus the right hand side in the equation above for $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x))$ indeed yields p^2 in this case. We can similarly deal with the case when $(p-1)/2$ is odd (i.e., $p \equiv 3 \bmod 4$), to find that in both cases, indeed $Tr_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = p^2$ when $t=0$. This proves the Proposition. ■

Appendix III
Proof of Lemma 13

We wish to prove:

$$\sum_{c=1}^{\frac{p-1}{n}}(-1)^c \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j \omega^{r^{a+cn}+r^{a+t+jn}} = \sum_{d=1}^{\frac{p-1}{n}}(-1)^d \sum_{a=0}^{n-1}\sum_{k=1}^{\frac{p-1}{n}} \omega^{(r^{nd}+r^t)r^{a+nk}}$$

Set $m = \frac{p-1}{n}$ and denote $\mathbb{Z}/m\mathbb{Z}$ by $\mathbb{Z}_m$. In the above equation, the dependence on c,j,d,k is only through their values (mod m) or through their values (mod 2). If we assume $2|m$, which follows from the assumption that n is odd, we can then treat c,j,d,k as elements of $\mathbb{Z}_m$. We thus have

$$\begin{aligned}\sum_{c=1}^{\frac{p-1}{n}}(-1)^c \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(-1)^j \omega^{r^{a+cn}+r^{a+t+jn}} &= \sum_{c\in\mathbb{Z}_m}(-1)^c \sum_{a=0}^{n-1}\sum_{k\in\mathbb{Z}_m}(-1)^k \omega^{r^{a+cn}+r^{a+t+kn}} \\ &= \sum_{c\in\mathbb{Z}_m}\sum_{k\in\mathbb{Z}_m}(-1)^{c+k}\sum_{a=0}^{n-1}\omega^{r^{a+cn}+r^{a+t+kn}}.\end{aligned}$$

We now make the change of variables: $c = d+k \pmod m$ which implies, since $2|m$, that $c = d+k \pmod 2$ and hence $d = c-k = c+k \pmod 2$. As the pair (c,k) varies over all of $(\mathbb{Z}_m \times \mathbb{Z}_m)$, so does the pair (d,k). We thus have

$$\begin{aligned}\sum_{c\in\mathbb{Z}_m}\sum_{k\in\mathbb{Z}_m}(-1)^{c+k}\sum_{a=0}^{n-1}\omega^{r^{a+cn}+r^{a+t+kn}} &= \sum_{d\in\mathbb{Z}_m}(-1)^d\sum_{a=0}^{n-1}\sum_{k\in\mathbb{Z}_m}\omega^{r^{a+(d+k)n}+r^{a+t+kn}} \\ &= \sum_{d\in\mathbb{Z}_m}(-1)^d\sum_{a=0}^{n-1}\sum_{k\in\mathbb{Z}_m}\omega^{(r^{nd}+r^t)(r^{a+nk})} \\ &= \sum_{d=1}^{\frac{p-1}{n}}(-1)^d\sum_{a=0}^{n-1}\sum_{k=1}^{\frac{p-1}{n}}\omega^{(r^{nd}+r^t)r^{a+nk}}.\end{aligned}$$

□

Appendix IV
Mathematical Notation

$\mathbb{Z}$ denotes the rational integers, $\mathbb{Q}$ denotes the rational numbers, and $\mathbb{Z}[\imath]$ denotes the Gaussian integers. For integers a,b, then $a \bmod b$, is the value of a modulo b. $\mathbb{Z}_b$ denotes the integers modulo b. Two integers are co-prime if their greatest common denominator (gcd) is one. S^* denotes the units of some ring S, i.e., the set of elements in S having an inverse in S. $S_1 \setminus S_2$, denotes the elements that are in set S_1 but not in set S_2. $\phi(\cdot)$ denotes Euler's totient function. For G a finite group, the order $\text{ord}(g)|_G$ of an element $g \in G$, describes the smallest power, say m, of g such that $g^m = 1$.

A field $\mathbb{F}$ is a commutative ring where each element except 0 has a multiplicative inverse. A field $\mathbb{L}$ is an extension field of $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{L}$. This extension is denoted as $\mathbb{L}/\mathbb{F}$ and it has degree $[\mathbb{L} : \mathbb{F}]$ equal to the dimension of $\mathbb{L}$ as a vector space over $\mathbb{F}$. A number field is a field that is a finite degree extension of $\mathbb{Q}$. Cyclotomic extensions are extensions of the rationals of the form $\mathbb{Q}(\omega_m)/\mathbb{Q}$ where $\omega_m = \exp\left(\frac{\imath 2\pi}{m}\right)$ for some integer $m \geq 3$. The degree of this extension equals $\phi(m)$.

If $\mathbb{L}$ is an extension of $\mathbb{F}$, then $l \in \mathbb{L}$ is said to be algebraic over $\mathbb{F}$ if l is the zero of some nonzero polynomial with coefficients in $\mathbb{F}$. The compositum of two finite dimensional number fields $\mathbb{F}_1, \mathbb{F}_2$ is the set of all sums of products of elements, one from $\mathbb{F}_1$ and the other from$\mathbb{F}_2$. This set is a field. For l an algebraic element over $\mathbb{F}$, then $\mathbb{F}(l)$ is a field extension consisting of sums of products of the form $f \cdot l^k,\ f \in \mathbb{F}, k \in \mathbb{Z}$.

A number-field element $l \in \mathbb{L}$ is said to be an algebraic integer if l is the zero of a monic polynomial with coefficients in $\mathbb{Z}$. The set of all algebraic integers in $\mathbb{L}$ forms a ring, known as the ring of algebraic integers, and is denoted $\mathcal{O}_{\mathbb{L}}$. If $[\mathbb{L} : \mathbb{F}]$ is a finite extension of number fields, then the ring of integers $\mathcal{O}_{\mathbb{L}}$ of $\mathbb{L}$ is precisely the collection of all elements in $\mathbb{L}$ that are the zeros of monic polynomials with coefficients in $\mathcal{O}_{\mathbb{F}}$.

An integral basis for an extension $\mathbb{L}/\mathbb{F}$ of number fields is a vector-space basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ such that $\alpha_i \in \mathcal{O}_{\mathbb{L}}$, all i, and such that every element $x \in \mathcal{O}_{\mathbb{L}}$ can be expressed as $x = \sum_{i=1}^n c_i\alpha_i,\ \ c_i \in \mathcal{O}_{\mathbb{F}}$. $x|y$ denotes the fact that integer x divides integer y.

The Galois group of $\mathbb{E}/\mathbb{F}$ is defined as the set of all automorphisms σ of $\mathbb{E}$ that fix every element of $\mathbb{F}$, i.e.,

$$\begin{aligned}\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \;=\; & \{\sigma : \mathbb{E} \rightarrow \mathbb{E} \mid \sigma \quad \text{is an automorphism of } \mathbb{E} \\ & \text{and } \sigma(f) = f, \text{ all } f \in \mathbb{F}\ \}.\end{aligned}$$

This set forms a group under the composition operator. The size of the Galois group of the extension $\mathbb{E}/\mathbb{F}$ is always $\leq [\mathbb{E} : \mathbb{F}]$. The extension is said to be Galois if equality holds. An Abelian (cyclic) extension $\mathbb{E}/\mathbb{F}$ is a Galois extension in which the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is cyclic, by which we mean that $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is generated by an automorphism σ, i.e.,

$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \;= < \sigma > =\; \{\sigma^0,\ \sigma,\ \cdots, \sigma^{n-1}\}, \qquad (22)$$

where $n = [\mathbb{E} : \mathbb{F}]$. In a cyclic Galois extension $\mathbb{E}/\mathbb{F}$, the "relative norm" $N_{\mathbb{E}/\mathbb{F}}(x)$ of an element $x \in \mathbb{E}$ is given by $N_{\mathbb{E}/\mathbb{F}}(x) = \prod_{i=0}^{n-1} \sigma^i(x)$ and it can be shown that $N_{\mathbb{E}/\mathbb{F}}(x) \in \mathbb{F}$. The "relative trace" $Tr_{\mathbb{E}/\mathbb{F}}(x)$ is given by $Tr_{\mathbb{E}/\mathbb{F}}(x) = \sum_{i=0}^{n-1} \sigma^i(x) \in \mathbb{F}$.

An ideal I of the ring of integers $\mathcal{O}_{\mathbb{F}}$ is an additive subgroup which is closed under multiplication by any element of $\mathcal{O}_{\mathbb{F}}$. In number fields, every ideal I of $\mathcal{O}_{\mathbb{F}}$ has a unique factorization as the products of powers of prime ideals. Let $\mathbb{L}$ be a finite Galois extension of $\mathbb{F}$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{\mathbb{F}}$, then the ideal $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ of $\mathcal{O}_{\mathbb{L}}$ has a unique factorization of the form

$$\mathfrak{p}\ \mathcal{O}_{\mathbb{L}} \;=\; \prod_{i=1}^{g} \beta_i^e, \qquad (23)$$

for distinct prime ideals β_i of $\mathcal{O}_{\mathbb{L}}$. The exponent e is called the ramification index of β_i over $\mathfrak{p}$ and written $e(\beta_i/\mathfrak{p})$. This number is the same for all β_i. We will also loosely refer to $e(\beta_i/\mathfrak{p})$ as the ramification index of $\mathfrak{p}$ or the ramification index of β_i.

REFERENCES

[1] F. Oggier, G. Rekaya, J. C. Belfiore, E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.

[2] P. Elia, K. Raj Kumar, S. A. Pawar, P. Vijay Kumar, and H-F. Lu, "Explicit, minimum-delay space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.

[3] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[5] S. Alamouti,"A transmitter diversity scheme for wireless communications, "*IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451–1458, Oct. 1998.

[6] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Dec. 1999.

[7] J.-C. Guey, M. P. Fitz, M. R. Bell, and W.-Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," *Proc. IEEE VTC'96, 2000*, pp. 136–140.

[8] B. A. Sethuraman and B. Sundar Rajan and V. Shashidhar, "Full-diversity, high-rate, space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596–2616, Oct. 2003.

[9] Kiran.T. and B.Sundar Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2984–2992, Aug. 2005.

[10] B. Erez, "The Galois structure of the trace form in extensions of odd prime degree," *Journal of Algebra*, vol. 118, pp. 438–446, 1988.

[11] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.

[12] J. Boutros, E. Viterbo, "Signal space diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel" *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 1453-1467, Jul. 1998.

[13] E. Bayer-Fluckiger, "Lattices and Number Fields," *Contemporary Mathematics*, vol. 241, pp. 69–84, 1999.

[14] E. Bayer, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$ lattice constellations for the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 50, no. 4, pp. 702–714, Apr. 2004.

[15] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," *Proc. IEEE Information Theory Workshop (ITW 2003)*, Paris, Apr. 2003.

[16] 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).*

[17] P. Elia, K. Raj Kumar, S. A. Pawar, P. Vijay Kumar and H-F. Lu, "Explicit space-time codes that achieve the diversity-multiplexing gain tradeoff," *Proc. IEEE Int. Symp. Inform. Th. (ISIT 2005).*

[18] P. Elia, B. A. Sethuraman and P. Vijay Kumar, "Perfect space-time codes with minimum and non-minimum delay for any number of antennas," *Proc. WirelessCom 2005, International Conference on Wireless Networks, Communications, and Mobile Computing*, Maui, Hawaii, Jun. 13-16, 2005.

[19] K. Raj Kumar and G. Caire, "Construction of structured LaST codes," *Proc. IEEE Int. Symp. Inform. Th. (ISIT 2006).*

[20] C. Hollanti, J. Lahtonen, K. Ranto and R. Vehkalahti, "On the densest MIMO lattices from cyclic division algebras," submitted to the *IEEE Trans. Inform. Theory*. Available at arXiv:cs.IT/0703052v1, Mar. 12, 2007.

[21] C. Hollanti and K. Ranto, "Asymmetric Space-Time Block Codes for MIMO Systems," Proceedings of the *IEEE Trans. Inform. Theory Workshop*, Jul. 1-6, 2007, Bergen, Norway.

[22] J. Lahtonen, "Dense MIMO Matrix Lattices and Class Field Theoretic Themes in Their Construction," Proceedings of the *IEEE Trans. Inform. Theory Workshop*, Jul. 1-6, 2007, Bergen, Norway.

[23] R. Vehkalahti, "Constructing optimal division algebras for space-time coding," Proceedings of the *IEEE Trans. Inform. Theory Workshop*, Jul. 1-6, 2007, Bergen, Norway.

[24] S. Yang, J.-C. Belfiore and G. Rekaya-Ben Othman, "Perfect space-time block codes for parallel MIMO channels," *Proc. IEEE Int. Symp. Inform. Th (ISIT 2006).*

[25] S. A. Pawar, K. Raj Kumar, P. Elia, B. A. Sethuraman and P. Vijay Kumar, "Minimum-delay space-time codes achieving the DMD tradeoff of the MIMO-ARQ channel," *Submitted to IEEE Trans. Inform. Theory*, Oct. 2005.

[26] S. Tavildar and P. Viswanath, "Approximately universal codes over slow-fading channels," *IEEE Trans. Inform. Theory*, vol. 52, no. 7, pp. 3233–3258, Jul. 2006.

[27] S. Sandhu and A. Paulraj, "Space-time block codes: A capacity perspective," *IEEE Commun. Lett.*, vol. 4, pp. 384–386, Dec. 2000.

[28] B. Hassibi and B. Hochwald, "Linear dispersion codes," *Proc. IEEE Int. Symp. Inform. Th. (ISIT 2001).*

[29] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inform. Theory*, vol. 48, pp. 753-761, Mar. 2002.

[30] B. Hassibi and B.M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inform. Theory*, vol.48, no.7, Jul. 2002, pages 1804-24.

[31] S. Galliou and J.-C. Belfiore, "A new family of full rate diverse space-time code based on Galois theory," *Proc. IEEE Int. Symp. Inform. Th. (ISIT 2002).*

[32] V. Shashidhar, B. Sundar Rajan, B. A. Sethuraman, "STBCs using capacity achieving designs from cyclic division algebras", *IGLOBECOM 2003 - IEEE Global Telecommunications Conference,* vol. 22, no. 1, pp. 1957–1962, Dec 2003.

[33] V. Shashidhar, B. Sundar Rajan, B. A. Sethuraman, "Information-lossless space-time block codes from crossed product algebras", *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3913–3935, Sept 2006.

[34] H. El Gamal and M.O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, no.5, pp. 1097–1119, May 2003.

[35] C. Pietsch and J. Lindner, "On the construction of capacity achieving full diversity space-time block codes," *in Proc. IEEE 61st Semiannual Vehicular Technology Conference (VTC)*, Stockholm, Jun. 2005.

[36] P. Elia, P. Vijay Kumar, S. Pawar, K. Raj Kumar, B. Sundar Rajan and H-F. Lu, “Diversity-multiplexing tradeoff analysis of a few algebraic space-time constructions, ” *presented in Allerton-2004*.

[37] H. A. Loeliger, “Averaging arguments for lattices and linear codes,” *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 1767–1773, Nov. 1997.

[38] B. Hassibi and B. M. Hochwald, “High-rate codes that are linear in space and time,” *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 1804–1824, Jul. 2002.

[39] 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, no. 6, pp. 968–985, Jun. 2004.

[40] 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.

[41] H. Yao, G.W. Wornell,“Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay,” GLOBECOM’03.IEEE, vol. 4, pp. 1941–1945, Dec. 2003.

[42] Genyuan Wang and Xiang-Gen Xia, “On optimal multi-layer cyclotomic space-time code designs,” *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1102–1135, Mar. 2005.

[43] C. Köse and R. D. Wesel, “Universal space-time trellis codes,” *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2717–2727, Oct. 2003.

[44] A. Edelman,“Eigen values and condition numbers of random matrices,” *SIAM J. Matrix Anal. Appl.*, vol. 9, no. 4, pp. 543–560, Oct. 1988.

[45] A. A. Albert, *Structure of Algebras*, Providence, R. I.: Coll. Publ., vol. 24, Amer. Math. Soc., 1961.

[46] D. A. Marcus, *Number Fields* (Universitext), New York: Springer Verlag, 1977.

[47] W. Scharlau, *Quadratic & Hermitian Forms, (Grundlehren Der Mathematischen Wissenchaften Series, vol. 270)*: Springer-Verlag, 1984.

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

[49] Richard S. Pierce, *Associative algebras,* Graduate Texts in Mathematics, New York–Berlin: Springer-Verlag, 1982.

[50] R. A. Horn and C. R. Johnson, *Matrix analysis*, Cambridge University Press, 1999.

[51] G. H. Hardy, *Orders of infinity,* Cambridge Tracts in Mathematics and mathematical physics, no. 12, 1924.

[52] A. Dembo, O. Zeitouni, *Large Deviations Techniques and Applications*, New York: 2nd edition, Springer-Verlag, 1998.

Petros Elia received the B.Sc. degree in electrical engineering from the Illinois Institute of Technology, Chicago, and the M.Sc. and Ph.D. Degrees in electrical engineering from the University of Southern California, Los Angeles in 2006. He is currently with Forschungszentrum Telekommunikation Wien, in Vienna. His current research interests include applications of information theory, large deviations and discrete/continuous mathematics, for analyzing communication, coding and resource-allocation methods in delay limited wireless networks.

B.A Sethuraman is with the Department of Mathematics at California State University Northridge. He got his bachelor’s degree in mechanical engineering at the Indian Institute of Technology, Chennai, India, and then switched fields and got his Ph.D. in mathematics at the University of California at San Diego. His research interests are in algebra and algebraic geometry, in which he has published extensively, won several research grants, and written textbooks.

Lately he has had the privilege of helping develop new applications of algebra to wireless communication in collaboration with engineers; in particular, his suggestion that division algebras embedded in matrices are the correct mathematical objects for use in MIMO applications has firmly taken root, and codes based on division algebras now come close to achieving the fundamental limits of outage-limited communications.

P. Vijay Kumar P. Vijay Kumar is with the Department of Electrical Communication Engineering at the Indian Institute of Science, Bangalore, on leave of absence from the University of Southern California (USC). He obtained his B.Tech and M. Tech from IIT and his Ph.D. from USC. His current research interests include space-time codes for point-to-point and cooperative-relay-network communication, code design for CDMA and distributed signal processing algorithms for sensor networks. He was Technical Program Co-Chair of the 2007 IEEE Information Theory Workshop held at Bergen Norway and General Co-Chair of the 2007 Applied Algebra, Algebraic Algorithms and Error-Correcting Codes Symposium (AAECC-17), Bangalore India. He was an invited plenary speaker at the 1992 IEEE Second International Symposium on Spread-Spectrum Techniques and Applications, Yokohama, Japan. A CDMA pseudorandom sequence family introduced in a 1996 paper co-authored by him is now part of the 3rd Generation W-CDMA Standard. He received the USC School-of-Engineering Senior Research Award as well as the 1995 IEEE Information Theory Society’s Prize Paper Award for co-authoring a 1994 paper that provided a solution to a long-standing mystery in coding theory. He is a Fellow of the IEEE.