Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas

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

***Abstract*— Perfect space-time codes were first introduced by Oggier et. al. as space-time codes having full rate, full diversity-gain, non-vanishing determinant for increased spectral efficiency, uniform average transmitted energy per antenna and good constellation shaping. A consequence of these conditions is the optimality of perfect codes with respect to the Zheng-Tse Diversity-Multiplexing Gain (D-MG) tradeoff, irrespective of the fading distribution of the channel coefficients. The above traits endow perfect codes with error performance that is currently unmatched. Yet perfect space-time codes have been constructed only for $2, 3, 4$ and 6 transmit antennas. We construct minimum and non-minimum delay perfect codes for all channel dimensions.**

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

I. Introduction

A. Definition of Perfect Codes

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

- *Full rate*. The code is a linear-dispersion code where the n^2 coefficients representing the message symbols are drawn from either the QAM or HEX constellations.
- *Full diversity*. For every pair X_1, X_2 of distinct code matrices, the difference matrix ΔX is non-singular.
- *Non vanishing determinant for increasing spectral efficiency*. The determinant of any difference matrix, 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 spectral efficiency.
- *Good shaping of the constellation.* This condition requires that the signalling set, obtained by code-matrix vectorization be isometric to QAM^{n^2} or HEX^{n^2}.
- *Uniform average transmitted energy per antenna*. This condition requires that the expected value of the transmitted power is uniform across antennas and across time slots.

Perfect codes are of interest as the above attributes guarantee near-optimal performance as measured by error probability.

Petros Elia and P. Vijay Kumar are with the Department of EE-Systems, University of Southern California, Los Angeles, CA 90089 ({elia,vijayk}@usc.edu). B. A. Sethuraman is with the Department of Mathematics, of the California State University Northridge, CA 91330 (al.sethuraman@csun.edu). P. Vijay Kumar is currently on leave of absence from USC at the Indian Institute of Science, Bangalore 560 012.

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.

B. New results

1) Additional properties satisfied by perfect codes: In addition to the defining properties, perfect codes also satisfy

- *Approximate universality*. This property was introduced in [19] to describe a code that is D-MG optimal [3] irrespective of channel fading statistics. Such codes exhibit high-SNR error performance that is given by the high-SNR approximation of the probability of outage of any given channel. The only known family of approximately universal codes is the family of space-time codes with non-vanishing determinant constructed from cyclic-division algebras, see [2]. Perfect codes are also approximately universal.
- *Residual approximate universality*. The truncated code resulting from deletion of a fixed subset of the rows from all code matrices in the space-time code results in a code that is also approximately universal for the correspondingly smaller number of transmit antennas.
- *Gaussian-like signalling.* This is an empirical observation and it relates to a Gaussian-like signalling set with a covariance matrix that tends to maximize mutual information for all practical ranges of SNR.
- *Information losslessness*. This property relates to having full rate as well as unitary linear dispersion matrices [21], [23], and guarantees that the mutual information is not reduced as a result of the code's structure.
- *Scalable sphere decoding complexity*. This property guarantees that as the number of receive antennas becomes smaller, the structure of the code allows for substantial reductions in sphere decoding complexity without essential loss in performance. For MISO channels, the structure of the code will allow for reduction of sphere decoding complexity, from $O(n^2)$ to $O(n)$.

2) Summary of presented contributions: In this paper we introduce explicit constructions of minimum-delay perfect space-time codes for any number n of transmit antennas and any number n_r of receive antennas. Non-minimum delay perfect codes are constructed for any delay T that is a multiple of n. The additional attributes of perfect codes listed above will also be established.

The general construction of perfect codes is provided in Section II. The additional attributes of perfect codes are established in Section III. Recent applications of perfect codes are discussed in Section IV. Examples and simulation results are provided in Section V.

II. THE GENERAL PERFECT CODE CONSTRUCTION

A. Space-Time Codes from Cyclic Division Algerbas

Division algebras are rings with identity in which every nonzero element has a multiplicative inverse. 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 subfield of D contains $\mathbb{L}$ is called a *maximal subfield* of D (Fig. 1). 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.

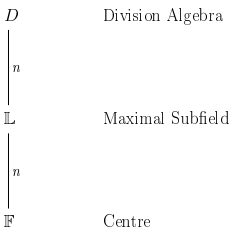

Fig. 1. Structure of a Cyclic Division Algebra

Our interest is in cyclic division algebras (CDA), 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 [35], 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

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

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

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

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 $\mathbb{L}$.

A space-time code $\mathcal{X}$ can be associated to D by selecting the set of matrices corresponding to the matrix representation of elements of a finite subset of D. Note that since these matrices are all square matrices, the resultant ST code necessarily has $T = n_t$. Set $n := n_t = T$.

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 (1), 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

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

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

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

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

Proof: See [37]. ∎

In this section, we follow [15], [16], [1] and show how a CDA-based ST code with NVD can be constructed for the case when the underlying constellation is 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 $\mathbb{F} \ = \ \mathbb{Q}(\imath)$.

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 $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. 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 $\gamma \ \in \ \mathcal{O}_{\mathbb{F}}$, $\gamma \neq 0$, be a non-norm element and $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ denote the associated CDA.

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 $\mathcal{A}_{\text{QAM}}$.

Consider the space-time code $\mathcal{X}$ comprising of matrices corresponding to the left-regular representation as in (2) of all elements d in CDA D which are of the form

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

From Lemma 1, it follows that the determinant of every such left-regular representation lies in $\mathbb{F} = \mathbb{Q}(\imath)$. But since all entries of the regular representation lie in the ring $\mathcal{O}_{\mathbb{L}}$, it follows that the determinant must moreover, lie in

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

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 and since the magnitude of any nonzero element in $\mathbb{Z}[\imath]$ is ≥ 1.

Thus the space-time codes under this setup achieve

1) full diversity
2) full-rate
3) a non-vanishing determinant.

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 uniform transmitted power and a good signal constellation. We begin by vectoring the code matrices in layer-by-layer fashion as shown below:

$$\underbrace{\begin{bmatrix} l_0 \\ \sigma(l_0) \\ \sigma^2(l_0) \\ \cdot \\ \cdot \\ \cdot \\ l_{n-1} \\ \gamma\sigma(l_{n-1}) \\ \gamma\sigma^2(l_{n-1}) \\ \vdots \end{bmatrix}}_{\underline{\text{vec}}(X)} = \underbrace{\begin{bmatrix} \Gamma_0\, G & & \\ & \vdots & \\ & & \Gamma_{n-1}G \end{bmatrix}}_{\Upsilon} \cdot \underbrace{\begin{bmatrix} f_{0,0} \\ f_{0,1} \\ f_{0,2} \\ \cdot \\ \cdot \\ \cdot \\ f_{n-1,0} \\ f_{n-1,1} \\ f_{n-1,2} \\ \vdots \end{bmatrix}}_{\underline{f}}$$

where

$$G = \begin{bmatrix} \beta_0 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \cdots & \sigma(\beta_{n-1}) \\ & \vdots & \\ \sigma^{n-1}(\beta_0) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{bmatrix}, \qquad (3)$$

and where the Γ_i, are of the form

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

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

$$U(G) \ = \ \kappa G, \qquad (4)$$

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 block-diagonal transformation matrix Υ is unitary. As a consequence we would have that,

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

where

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

From this it follows that

- the set $\{\underline{\text{vec}}(X) \mid X \in \mathcal{A}_{\text{QAM}}\}$ is isometric to the set $\mathcal{A}_{\text{QAM}}^{n_t^2}$
- hence the corresponding $2n_t^2$-dimensional real counterpart of this n_t^2-dimensional complex vector is part of an infinite lattice equivalent to $\mathbb{Z}^{2n_t^2}$
- at each time slot, on average, each antenna transmits the same amount of energy and
- any two elements of $\underline{\text{vec}}(X)$ are uncorrelated.

We proceed in the following subsections to show how a suitable unit magnitude element γ and a suitable unitary matrix G can always be found.

B. 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: (*Construction of the non-norm element for the QAM constellation*) Let $n = 2^s n_1$ where n_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}, and which has order $\text{ord}(q)|_{\mathbb{Z}_p^*} = n_1$ 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 $n_1 = 1$, we take $\mathbb{L} = \mathbb{Q}(\omega_{2^{s+2}})$ and $\gamma = \dfrac{1+2\imath}{1-2\imath}$.) Then for any choice of basis $\{\beta_i\}_{i=0}^{n-1}$ for $\mathbb{L}$ over $\mathbb{Q}(\imath)$ such that the associated matrix $U(G)$ (for some choice of scale factor $\kappa \in \mathbb{F}$) in (4) is unitary, the associated space-time code arising from equation (2) has full-diversity, full-rate, non-vanishing determinant and satisfies the additional equal power sharing constraint.

Proof: See Appendix I ∎

Proposition 3: (*Construction of the non-norm element for the HEX code*) 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 $\text{ord}(q)|_{\mathbb{Z}_p^*} = n_1$ 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 should also be congruent to 3 mod 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 $n_1 = 1$, so $s = 1$, we take $\mathbb{L} = \mathbb{Q}(\omega_3)(\imath)$, and $\gamma = \dfrac{3+\omega_3}{3+\omega_3^2}$.) Then for any choice of basis $\{\beta_i\}_{i=0}^{n-1}$ for $\mathbb{L}$ over $\mathbb{Q}(\imath)$, the associated space-time code arising from equation (2) has full-diversity, full-rate, non-vanishing determinant and satisfies the additional equal power sharing constraint.

Proof: See Appendix I ∎

Consequently, we have constructed algebraic, unit-magnitude 'non-norm' elements, valid for use in perfect codes, for any n. Some examples 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	$(3+\omega_3)/(1+3\omega_3)$ $(4+9\imath)/(9+4\imath)$

C. Finding Unitary Matrices G

The goal here is to construct proper matrices of the form

$$U(G) = \kappa G \tag{5}$$

$$G = \begin{bmatrix} \beta_0 & \cdots & \beta_{n-1} \\ \sigma(\beta_0) & \cdots & \sigma(\beta_{n-1}) \\ & \vdots & \\ \sigma^{n-1}(\beta_0) & \cdots & \sigma^{n-1}(\beta_{n-1}) \end{bmatrix}, \tag{6}$$

where

- $\mathbb{F}$ is either $\mathbb{Q}(\imath)$ or else $\mathbb{Q}(\omega_3)$,
- $\mathbb{K}$ is a cyclic, degree n extension of $\mathbb{F}$ as in Propositions 2 - 3,
- $\{\beta_i\}$ is an integral basis for $\mathbb{K}/\mathbb{F}$,
- $\kappa \in \mathbb{F}$ and
- $U(G)$ is unitary.

We adopt the approach of [10]-[14]. A matrix with integral elements such as the matrix G above can be regarded as a generator matrix for 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 (5), 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 a (guaranteed to exist) odd prime $p \equiv 1 \pmod{n_1}$
- let $\omega = \omega_p = e^{\frac{2\pi\imath}{p}}$. Let σ denote the generator of the cyclic Galois group $\mathbb{Q}(\omega)/\mathbb{Q}$.
- find primitive element r of $\mathbb{Z}_p^*$.
- for $m = \frac{p-1}{2}$, create $\alpha = \prod_{k=0}^{m-1}(1-\omega^{r^k})$ where $r^{p-1} = 1$
- Find a guaranteed to exist λ such that $\lambda(r-1) \equiv 1 \pmod{p}$ and let $z = \omega^\lambda \alpha(1-\omega)$
- For $\sigma(\omega) = \omega^r$, let $x = \sum_{k=1}^{\frac{p-1}{n_1}} \sigma^{kn_1}(z)$.

The element x is hence in the field $\mathbb{K}'$, the subfield of $\mathbb{Q}(\omega)$ fixed by σ^{n_1}, of degree n_1 over $\mathbb{Q}$. Then the matrix $U(G_{n_1})$ given below is unitary.

$$U(G_{n_1}) = \frac{1}{p}\begin{vmatrix} x & \sigma(x) & \cdots & \sigma^{n_1-2}(x) & \sigma^{n_1-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & \sigma^{n_1-1}(x) & x \\ \sigma^2(x) & \sigma^3(x) & \cdots & x & \sigma(x) \\ & \vdots & & \vdots & \\ \sigma^{n_1-1}(x) & x & \cdots & \sigma^{n_1-3}(x) & \sigma^{n_1-2}(x) \end{vmatrix} \tag{7}$$

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

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

and the rest of the circulant matrix by:

$$U(G_{n_1})(i+1,j) = U(G_{n_1})(i,j+1 \mod n_1),\ i = 0,\cdots,n_1-2.$$

Example *1:* 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 next 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]: For when the information set is QAM, then $\mathbb{F} = \mathbb{Q}(\imath)$ and we 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 $\mathbb{Q}(\imath)$. Considering that 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 $\sigma(\omega) = \omega^5$, it is the case 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 that

$Gal(\mathbb{K}/\mathbb{Q}(\imath)) =< \sigma >$. Take $\{\omega^0, \omega^1, \omega^2, \cdots, \omega^{m-1}\}$ to be the integral basis over $\mathbb{Q}(\imath)$, and set

$$U(G_{2^s}) = \frac{1}{\sqrt{m}}\left[\sigma^k(\omega^i)\right]_{i,k} = \frac{1}{\sqrt{m}}\left[\omega^{i\cdot 5^k}\right]_{i,k} \quad (8)$$

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 (8), 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 $2^s n_1$ 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 II-C.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.

III. Information theoretic interpretation and generalization of the perfect code conditions

The D-MG tradeoff [3] bounds the optimal performance of a space-time code $\mathcal{X}$ operating at rate R bpcu, corresponding to a multiplexing gain

$$r = \frac{R}{\log_2(\text{SNR})}.$$

The *diversity gain* corresponding to a given r, is defined by

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

where P_e denotes the probability of codeword error. For the Rayleigh fading channel, Zheng and Tse [3] described the optimal tradeoff between these two gains by showing that for a fixed integer multiplexing gain r, the maximum achievable diversity gain is

$$d(r) \ = \ (n-r)(n_r - r). \quad (9)$$

The function for non-integral values is obtained through straight-line interpolation.

We use this D-MG approach as a basis for interpreting and generalizing the conditions that define perfect-codes.

4) Full rate condition: Consider an $n \times T$ code $\mathcal{X}$ where each code-matrix carries m information symbols per channel use from a discrete constellation $\mathcal{A}$ such as QAM. It is then the case that

$$|\mathcal{X}| = 2^{RT} = 2^{rT\log_2 \text{SNR}} = \text{SNR}^{rT} = |\mathcal{A}|^{mT}$$

which implies that $|\mathcal{A}| \doteq \text{SNR}^{\frac{r}{m}}$. We will assume the discrete constellation $\mathcal{A}$ to be such that $\mathbb{E}_{\mathcal{A}}[|\alpha|^2] \doteq |\mathcal{A}|$. Certainly this is true of the QAM and HEX constellations. The fact that each element $X_{i,j}$ of a code matrix is a linear combination of elements of $\mathcal{A}$, gives that

$$\mathbb{E}[\|X_{i,j}\|^2] \doteq |\mathcal{A}| = \text{SNR}^{\frac{r}{m}}.$$

The SNR normalizing factor ν that guarantees that $\mathbb{E}[\|\nu X\|_F^2] \doteq \text{SNR}$ is then given by

$$\nu^2 \doteq \text{SNR}^{1-\frac{r}{m}}. \quad (10)$$

Without loss of generality we can assume that there exist two code-matrices $X_1, X_2 \in \mathcal{X}$, with each X_i mapping the information nm-tuple $\{\alpha_i, 0, 0, \cdots, 0\}$, where $\alpha_i \doteq \text{SNR}^0$. As a result, the determinant and trace of the difference matrix ΔX, is a polynomial of degree less than n over $\alpha = \alpha_1 - \alpha_2 \doteq \text{SNR}^0$, with coefficients independent of SNR, i.e.

$$\det(\Delta X \Delta X^\dagger) \doteq \text{Tr}(\Delta X \Delta X^\dagger) \doteq \text{SNR}^0$$

and thus with all its eigenvalues

$$l_i \ \doteq \ \text{SNR}^0.$$

The corresponding pairwise error probability $\text{PEP}(X_1 \to X_2)$, in the Rayleigh fading channel [4], [7], then serves as a lower bound to the codeword error probability P_e, i.e.,

$$\begin{aligned} P_e \ &\geq \ \text{PEP}(X_1 \to X_2) \ \doteq \ \frac{1}{\prod_{j=1}^{n}[1 + \frac{\theta^2}{4} l_j]^{n_r}} \\ &\doteq \ \text{SNR}^{-n_r n(1-\frac{r}{m})} \end{aligned}$$

which results in a diversity gain of

$$d(r) \ \leq n_r n\left(1 - \frac{r}{m}\right).$$

What this means is that m discrete information symbols per channel use can potentially sustain reliable communication for up to rate $R_{\max} \approx m\log_2(\text{SNR})$.

For large SNR, the outage capacity over an $n \times n_r$ Rayleigh fading channel is given by $C_{\text{out}} \ \approx \ \min\{n, n_r\}\log_2(\text{SNR})$, implying a maximum achievable multiplexing gain of $r_{\max} = \min\{n, n_r\}$. Consequently the relation between $R_{\max}$ and C_{out}, allows for the interpretation that the full rate defining condition is necessary for reliable transmission at rates close to the outage capacity of the Rayleigh fading channel, independent of the channel topology. Equivalently, given some rate R, the full rate defining condition is necessary for reliable transmission at the smallest allowable SNR

$$\text{SNR}_{\min} \doteq 2^{\frac{R}{\min(n, n_r, m)}}$$

again independent of the channel topology. Let us now re-examine the full-rate condition, in conjunction with the determinant condition.

5) Non-vanishing determinant condition: We consider the $n \times T$ truncated code $\mathcal{X}$, $T \geq n$, constructed by deleting the same $T-n$ rows from all the code-matrices $X^{'}$ of a $T \times T$ perfect code $\mathcal{X}^{'}$. We have seen that for an $n \times n$ code mapping n^2 information symbols from a discrete constellation (n information symbols per channel use), the standard n-dimensional 'folding' ($|\mathcal{X}| = |\mathcal{A}|^{n^2}$) forces a normalizing factor of $\nu^2 = \text{SNR}^{1-\frac{r}{n}}$, whereas in the truncated $n \times T$ code mapping T^2 information symbols ($\frac{T^2}{n}$ information symbols per channel use), the constellation is folded in T dimensions ($|\mathcal{X}| = |\mathcal{A}|^{T^2}$), requiring for

$$\nu^2 = \text{SNR}^{1-\frac{r}{T}}.$$

This scenario accentuates the fact that in essence, we are limited by a lower bound on the determinant of the energy-normalized difference matrix $\nu^2 \Delta X \Delta X^{\dagger}$. As a result, for the n-dimensional case, the defining condition of non-vanishing determinant for the non-normalized matrix $\Delta X \Delta X^{\dagger} \geq \text{SNR}^0$, translates to

$$\begin{aligned} \det[\nu^2 \Delta X \Delta X^{\dagger}] &\geq (\nu^2)^n \text{SNR}^0 = (\text{SNR}^{1-\frac{r}{n}})^n \\ &= \text{SNR}^{n-r} \end{aligned}$$

which, for the $n \times T$ case with T-dimensional folding, translates back to the determinant bound

$$\det(\Delta X \Delta X^{\dagger}) \geq \text{SNR}^{-\frac{r}{T}(T-n)}$$

for the non-normalized code-matrices. But from [2], [17], we see that the above determinant bound is the best that any code can attain, thus allowing us to generalize the full-rate, full-diversity and non-vanishing determinant perfect code conditions, to the general condition of having

$$\det[\nu^2 \Delta X \Delta X^{\dagger}] \dot{\geq} \text{SNR}^{n-r}, \ 0 \leq r \leq \min(n, n_r). \quad (11)$$

In regards to non-minimum delay perfect codes, let us briefly note that codes resulting from row deletion of perfect codes essentially maintain all the conditions of the original minimum-delay perfect code constructions except that now the vectorization of the code-matrices is not isometric to QAM^{T^2}. Non-minimum delay perfect codes can be constructed though for delays $T = nk$, $k \in \mathbb{Z}^+$ that are multiples of n, by the horizontal stacking construction found in [2], [17] which maintains the non-vanishing determinant property as well as the isometry of the code matrices with $\text{QAM}^{n^2 k}$.

Let us now incorporate all the perfect-code defining conditions in order to provide an information theoretic interpretation that spans both the high and the low SNR regimes.

6) Approximate universality, information losslessness and Gaussian-like signalling: We begin with:

Theorem 5: Perfect codes are both approximately universal as well as information lossless.

Proof: See Appendix IV. ∎

The code's information losslessness, shown in the proof to be the result of the CDA structure and the last two conditions, essentially allows for the code to maintain the maximum mutual information corresponding to the channel and signalling set statistics. This mutual information is empirically related to the Gaussian-like signalling set and its good covariance properties, observed in Figure 2. The expedited rate with which the

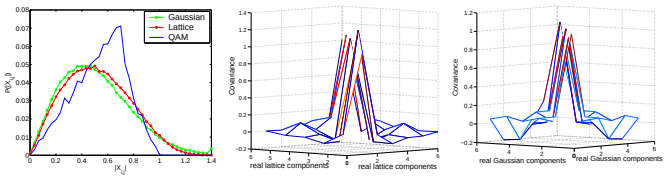

Fig. 2. Gaussian nature of the signalling set of the 3×3 perfect code, compared to QAM and random Gaussian signalling (left). Covariance of columns of perfect codes (center) compared to covariance of random Gaussian vectors (right).

signalling becomes Gaussian, relates to the high-dimensional and orthogonal nature of the lattice generator matrix which together with a unit-magnitude non-norm element, jointly allow equal magnitudes for the diagonal elements of the covariance matrix of the signalling set.

Let us now draw from the information theoretic interpretation of the defining conditions and provide variants of perfect codes that are specifically tailored for channels with a smaller number of receive antennas, and which manage to maintain good performance at a considerably reduced sphere decoding complexity.

A. Channel topology and efficient variants of perfect codes

We have seen that $n \times n$ perfect codes utilize n different layers to achieve approximate universality for all n_r. Each layer has non-vanishing product distance and maps n-elements from a discrete constellation, thus maintaining two properties that were shown in [19, Theorem 4.1] to guarantee for optimality over the statistically symmetric parallel channel, i.e. a channel with a diagonal fading coefficient matrix, as well as potentially allowing for optimality over the statistically symmetric $n \times 1$ MISO channel. To offer intuition, we observe that the sum-capacity of the n_r independent MISO channels relates to the full rate condition, whereas the achieved full diversity relates to the CDA structure and the discreteness of the powers of Γ which manage to translate the non-vanishing product distance to an overall non-vanishing determinant, and thus to keep the different layers independent and at some non-vanishing distance from each other. The full rate condition comes with a sphere decoding complexity of $O(n^2)$, but as the number of MISO channels reduces with n_r, so does the required decoding complexity. Codes over such channels can have the form

$$X = \sum_{j=0}^{n-1} \Gamma^j \left(diag(\underline{f}_j \cdot T \cdot G) \right)$$

where $T(i,j) = 1$, $i = j \in [1, .., n_r]$ and $T(i,j) = 0$ otherwise, or can have the form

$$X = \sum_{j=0}^{n_r-1} \Gamma^j \left(diag(\underline{f}_j \cdot G) \right).$$

Note here that the above codes have not been proven to be D-MG optimal.

Motivated by the down-link requirements and by the cooperative diversity uses of space-time coding in wireless networks, we will concentrate on the MISO case ($n_r = 1$), for which a D-MG optimal perfect code variant

$$\mathcal{X}_d = \{diag(\underline{x}) = diag(\underline{f} \cdot G),\ \forall \underline{f} \in \text{QAM}^n\}. \qquad (12)$$

with sphere decoding complexity of $O(n)$ was recently constructed in [50], [51] for all n, together with the code

$$\mathcal{X}_{ir} = \{X = \sum_{k=0}^{n-1} f_k \Gamma^k,\ \forall f_k \in \text{QAM-HEX}\} \qquad (13)$$

that corresponds to the center of the division algebra. With the exception of $n = 2$, $\mathcal{X}_{ir}$ has not yet been proven to be D-MG optimal. Figure 3 provides a performance comparison between the single dimensional perfect code variant with the equivalent standard perfect-code.

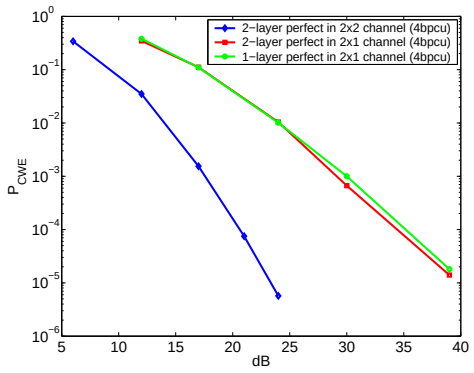

Fig. 3. For $n = 2, n_r = 1$, the single-layer perfect code variant exhibits similar error performance as the 2-layer (standard) perfect code. This changes when a second receive antenna is added.

IV. Recent developments involving perfect codes

The proposed high-dimensional perfect codes have had an impact on establishing outage-based asymptotic optimality expressions for wireless networks where independently distributed users utilize different parts of space-time schemes to relay messages for one another, hence improving the overall quality of service ([44] etc). Asymptotic optimality was explicitly achieved for the first time (see [48], [49], [50], [51]) for finite time duration networks where furthermore the assisting relays have no knowledge of the channel. This was achieved for several cooperation strategies, and for a very general network topology and statistical characterization.

V. Examples of new perfect codes and simulations

A. 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

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

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

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

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:

- The 5×5 perfect space-time code is given by

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

for

$$\Gamma = \begin{bmatrix} 0 & 0 & \cdots & 0 & \gamma \\ 1 & 0 & \cdots & 0 & 0 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \qquad (14)$$

based on $\gamma = \frac{3+2\imath}{2+3\imath}$, and circulant generator matrix G_5 defined by the first row

$$\begin{bmatrix} -0.3260 & 0.5485 & -0.4557 & -0.5969 & -0.1699 \end{bmatrix}$$

- The 7×7 perfect space-time code is given by

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

for Γ based on $\gamma = \frac{8+5\imath}{8-5\imath}$, and circulant generator matrix G_7 defined by the first row

$$\begin{bmatrix} -0.681 & 0.163 & -0.449 & 0.077 & 0.082 & 0.276 & -0.469 \end{bmatrix}$$

- The 25×25 integral restriction code

is given by

$$\mathcal{X}_{\text{ir}} = \left\{ X = \sum_{k=0}^{24} s_k \Gamma^k,\ \ s_k \in \text{QAM} \right\}$$

with $\gamma = \frac{3+2\imath}{2+3\imath}$. This code has the same sphere decoding complexity of $O(25)$ as the 5×5 standard perfect code in the example above, and is expected to have the same performance, when $n_r = 1$, as the 25×25 perfect code whose sphere decoding complexity is $O(625)$.

B. Simulations

All the simulations assume $\mathbb{C}\mathcal{N}(0,1)$ fading and thermal noise. A sphere decoder was used. We begin with Figure 4 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 (commutative 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 D-MG 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. Figures 5 and 6 show a

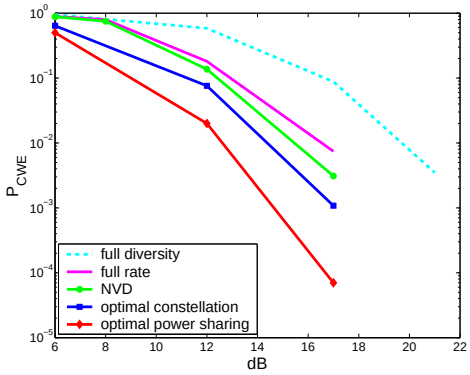

Fig. 4. Performance improvements attributed to achieving the different criteria for the perfect codes

comparison of the 2×2 unified perfect code presented here, with some perfect codes from [1] and with the Alamouti code ($n_r = 2$). The Golden code [16] performs best among all existing 2×2 perfect codes. When rates are lower, the unified perfect and the Golden code perform better than the orthogonal design whereas one of the perfect codes does not always do so. For higher rates, all considered perfect codes perform substantially better than the orthogonal design. At all rates and all SNR, the perfect code constructed here has performance very close to that of the Golden code. In Figure 7 we show the performance of the newly constructed 5-dimensional perfect code and compare that with the corresponding 5×5 single-dimensional commutative perfect code (13). As expected, the former utilizes fully the $n_r = n = 5$ channel and is thus able to transmit with a small probability of error at high rates and low SNR.

VI. Conclusion

We have explicitly constructed perfect space-time codes for any number n of transmit antennas, any number n_r of receive antennas and any delay T that is a multiple of n. Achieving all

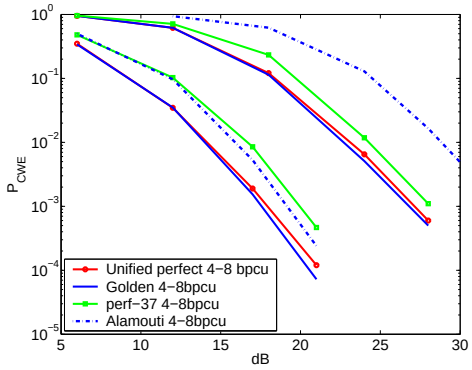

Fig. 5. Low rate comparison of the unified perfect code with two perfect codes from [1] and with the Alamouti code

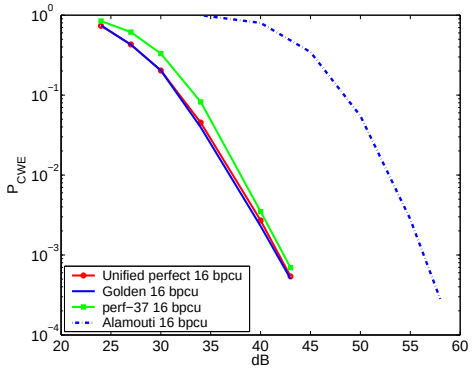

Fig. 6. High rate comparison of the unified perfect code with two perfect codes from [1] and with the Alamouti code

the defining conditions from [1], allows for perfect codes to exhibit performance that is currently unmatched. The information theoretic interpretation of the exhibited good performance both for low and high SNR, is that the defining conditions jointly endow the code with approximate universality and the ability to provide for near optimal mutual information.

High dimensional perfect codes cover a much needed requirement for near-optimal codes in multi-user cooperative diversity wireless networks, where each user acts as a transmit antenna. Specifically, perfect codes have already been used to establish the high-SNR outage region of unknown channels, and have provided the only outage-based asymptotically-optimal explicitly constructed schemes for a plethora of cooperative diversity methods and a large family of channel statistics.

Appendix I
Proof of Propositions 2 and 3

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

Lemma 6: [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 $\mathbb{Z}[\imath]$

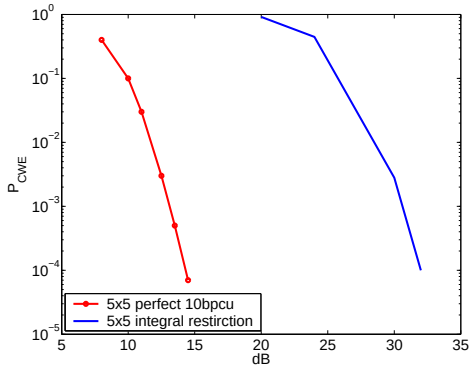

Fig. 7. Comparison of the 5×5 perfect code with the 5×5 single dimensional integral restriction code ($n_r = 5$).

($\mathbb{Z}[\omega_3]$) 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 7: [39] 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 8: (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 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 $\mathbb{L}/\mathbb{Q}(\imath)$.

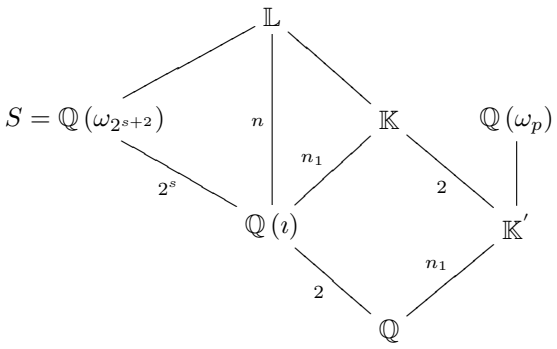

Fig. 8. Constructing a cyclic extension of $\mathbb{Q}(\imath)$ of degree $n = 2^s n_1$. The integers shown indicate the degree of the corresponding extension.

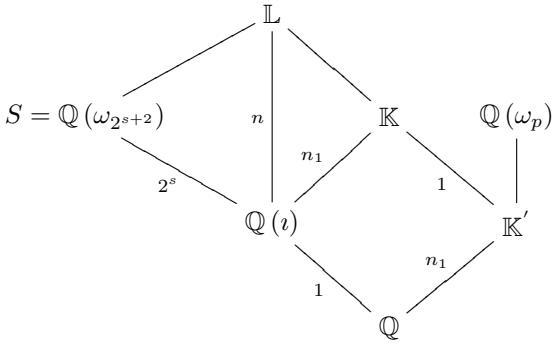

Fig. 9. Constructing a cyclic extension of $\mathbb{Q}(\imath)$ of degree $n = 2^s n_1$. The integers shown indicate the inertial degrees associated with the decomposition of either the prime ideal $q\mathbb{Z}$ or of one of its factors, over the corresponding extension.

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 $a \neq b$ (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 $\text{ord}(q)|_{\mathbb{Z}_{p^*}} = n_1$. If $s = 1$, we also require that $q \equiv 3 \pmod 4$. Assume that we have found such a p and q. The argument for the rest of the statements in this paragraph are all exactly as in the case when $\mathbb{F} = \mathbb{Q}(\imath)$: The conditions $\text{ord}(q)|_{\mathbb{Z}_{p^*}} = n_1$ 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 field $\mathbb{L}'$ is cyclic over $\mathbb{Q}$ 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 $\mathbb{L} = \mathbb{L}'(\omega_3)$, which is cyclic over $\mathbb{Q}(\omega_3)$ 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-diversity, 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 (mod 3), to m (mod p), where m is a generator of $\mathbb{Z}_{p^*}$, and (if $s = 1$) to 3 (mod 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 (mod 3) and to 3 (mod 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

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 will follow the exposition in [14] closely, retaining even the notation in [14], and show that the proofs there only use the fact that n is odd, and not that it is an odd prime.

To this end, let $n \geq 3$ be a given odd integer, and fix a prime $p \equiv 1 \pmod n$. Note that the existence of such a p is guaranteed since the sequence $\{1+dn,\ d = 1, 2, \cdots\}$, as shown by Dirichlet, 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 $\mathbb{Q}(\omega+\omega^{-1})$.

Recall that we are following the notation in [14]. Let $G = Gal(\mathbb{Q}(\omega)/\mathbb{Q})$, with generator σ, chosen so that $\sigma(\omega) = \omega^r$, where in turn, r is a generator of $\mathbb{Z}_p^*$. 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 9: 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

$$G_N G_N^T(i,j) = Tr_{\mathbb{K}/\mathbb{Q}}(\sigma^i(x)\sigma^j(x)),$$

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

Remark 1: 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 $a \mapsto v(a) = [a, \sigma(a), \ldots, \sigma^{n-1}(a)]$ (note that $\mathbb{K}$ is a real field), this Proposition says that the vectors $[v(x), v(\sigma(x), \ldots, v(\sigma^{n-1}(x))]$ 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 9

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

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 9, 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 11:

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

Proof: See Appendix III ∎

As in [14], we write

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

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 $1,\ldots,(p-1)/n$, 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 11

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 $(\bmod m)$ or through their values $(\bmod 2)$. 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
PROOF OF APPROXIMATE UNIVERSALITY AND INFORMATION LOSSLESSNESS OF PERFECT CODES (THEOREM 5)

The approximate universality part of the proof, is based on the derivation of the approximate universality conditions in [19]. It is reproduced here for completeness.

Proof: Let $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ and $l_1 \geq l_2 \geq \cdots \geq l_n$ be the ordered eigenvalues of $H^\dagger H$ and $\Delta X \Delta X^\dagger$ respectively. Irrespective of the statistics of the channel, in the high-SNR regime, the probability of no-outage at multiplexing gain r, is shown in [3] to satisfy $Pr(\text{no-outage}) \doteq Pr\left\{\sum_{i=1}^{n'}\ln(1+\text{SNR}\lambda_i) > \ln(\text{SNR}^r)\right\}$, where $n' := \min(n, n_r)$. Through the Lagrange multiplier technique we determine

$$d^2_{E,\text{worst}} = \inf_{H\notin\text{outage}}\sum_{i=1}^{n'} l_i\lambda_i$$

by writing the functional as

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

and differentiating w.r.t. λ_i, we obtain $\lambda_i = (\mu/l_i - \text{SNR}^{-1})$. We then use the Kuhn-Tucker conditions to verify that the solution $\lambda_i = (\mu/l_i - \text{SNR}^{-1})^+$ is what gives the worst possible $d^2_{E,\text{worst}}$, for μ such that

$$\sum_{i=1}^{n'}\ln(1+\text{SNR}(\mu/l_i - \text{SNR}^{-1})^+) = r\ln\text{SNR}.$$

Solving the above, we obtain that

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

Substituting this value of λ_i in $d^2_{E,\text{worst}}$ and setting $d^2_{E,\text{worst}} > \text{SNR}^\epsilon$ for some $\epsilon > 0$, we obtain a condition on the smallest n' eigenvalues of the code $\prod_{i=1}^{n'} l_i > \text{SNR}^{n'-r}$, a condition satisfied by CDA codes with non-vanishing determinant. [17].

Now moving to perfect codes, we follow the approach in [23] to show that the linear dispersion matrices are unitary. This property, together with the full rate condition, establish the information losslessness and the entire theorem.

As the code maps n^2 information elements, we consider n linear dispersion matrices $\{A_u\}_{u=1}^{n}$ of dimension $n^2 \times n$. Starting with

$$A_{n,i} = diag\left(G(i)\right)_{n\times n},\ i = 1, \cdots, n$$

where $G(i)$ represents the i^{th} row of G in (3), we recursively create

$$A_{u,i} = \Gamma^{n-u} A_{n,i}, \quad u = 1, 2, \cdots, n.$$

Finally A_u is constructed as

$$A_u \quad = \quad \left| \begin{array}{c} A_{u,0} \\ \vdots \\ A_{u,n-1} \end{array} \right|$$

It is easy to see that the unitary nature of Γ and G makes each of the A_u unitary

$$A_u^{\dagger} A_u = I_n.$$

■

REFERENCES

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

[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.

[3] 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.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communi-cation: 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, Nov.-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. Info. 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, Issue 8, pp. 2984 - 2992, Aug. 2005.

[10] B. Erez, The Galois Structure of the Trace form in Extensions of Odd Prime Degree, J. of Algebra, vol. 118, pp. 438-446, 1988.

[11] J. Boutros, E. Viterbo, C. Rastello, andJ. C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, 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. Info. Theory*, vol. 49, no. 4, pp. 1453-1467, July 1998.

[13] E. Bayer-Fluckiger, Lattices and Number Fields, Contemporary Mathematics, vol. 241, pp. 6984, 1999.

[14] E. Bayer, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$ lattice constellations for the Rayleigh fading channel," *Submitted to IEEE Trans. Inform. Theory*, April 2004.

[15] J.-C. Belfiore and G. Rekaya,"Quaternionic Lattices for Space-Time Coding," in *Proc. IEEE Information Theory Workshop.*, Paris 31 March - 4 April 2003 ITW 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)*, pp. 308, June 27-July 2, Chicago 2004.

[17] Petros Elia, K. Raj Kumar, Sameer A. Pawar, P. Vijay Kumar and Hsiao-feng Lu, "Explicit Space-Time Codes That Achieve The Diversity-Multiplexing Gain Tradeoff," *Proc. IEEE Int. Symp. Inform. Th (ISIT 2005).*

[18] Sameer A. Pawar, K. Raj Kumar, Petros 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.

[19] S. Tavildar and P. Viswanath, "Approximately universal codes over slow fading channels," *Submitted to IEEE Trans. on Information Theory*, February 2005.

[20] S. Sandhu and A. Paulraj, " Space-time block codes: A capacity perspective," *IEEE Communi Lett. , vol.4 pages. 384-386, Dec 2000*

[21] B. Hassibi and B. Hochwald, "Linear dispersion codes," *in Proc. IEEE Int. Symp. Information Theory, Washington DC, Jun. 2001, page 325*

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

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

[24] S. Galliou and J.-C. Belfiore, "A new family of full rate diverse space-time code based on Galois theory." Lausanne, Switzerland: Proc. 2002 IEEE Int. Symp. on Information Theory, 2002, p. 419.

[25] 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, Dec 2003 pp. 1957-1962*

[26] V. Shashidhar, B. Sundar Rajan, B. A. Sethuraman, "Information-lossless space-time block codes from crossed product algebras", *IEEE Transactions on Information Theory*, accepted for publication.

[27] 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/Sweden*, June 2005

[28] Petros Elia, P. Vijay Kumar, Sameer Pawar, K. Raj Kumar, B. Sundar Rajan and Hsiao-feng (Francis) Lu, "Diversity-Multiplexing Tradeoff Analysis of a few Algebraic Space-Time constructions, " *presented in Allerton-2004*.

[29] H.A.Loeliger, "Averaging arguments for lattices and linear codes, "*IEEE Trans. Inform. Theory*, Vol.IT-43, pp.1767-1773, Nov.1997

[30] 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.

[31] 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.

[32] 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.

[33] 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.

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

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

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

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

[38] R. Horn and C.R. Johnson, "Matrix Analysis," *Cambridge University Press, Cambridge, 1985.*

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

[40] Richard S. Pierce, "Associative algebras," *Graduate Texts in Mathematics, 88. Springer-Verlag, New York-Berlin, 1982.*

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

[42] A. Edelman,"Eigen Values and Condition Numbers of Random Matrices," *SIAM J. Matrix Anal. Appl.*, vol. 9 No. 4, pp. 543-560, Oct 1988.

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

[44] J. N. Laneman and G. W. Wornell, "Distributed Space-Time Coded Protocols for Exploiting Cooperative Diversity in Wireless Networks," *IEEE Trans. Inform. Theory, vol. 49, no. 10, pp. 2415-2525,* Oct. 2003.
[45] Y. Jing and B. Hassibi, "Distributed space-time coding in wireless relay networks - Part I: basic diversity results," *Submitted to IEEE Trans. on Wireless Communications,* 2004.
[46] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 3062-3080,* Dec. 2004.
[47] K. Azarian, H. El Gamal, and P. Schniter, On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels , *to appear in IEEE Transactions on Information Theory, 2005.*
[48] Petros Elia and P. Vijay Kumar, "Diversity-Multiplexing Optimality and Explicit Coding for Wireless Networks With Reduced Channel Knowledge, " *Presented at Allerton-2005*.
[49] S. Yang and J.-C. Belfiore, "Optimal Space-Time Codes for the Amplify-and-Forward Cooperative Channel, " *Presented at Allerton-2005*.
[50] Petros Elia and P. Vijay Kumar, "Approximately Universal Optimality in Wireless Networks, " *Presented at Allerton-2005*.
[51] Petros Elia and P. Vijay Kumar, "Approximately universal optimality over several dynamic and non-dynamic cooperative diversity schemes for wireless networks, " *To be submitted to IEEE Trans. Inform. Theory*.