Construction Methods for Asymmetric and Multiblock Space–Time Codes

Camilla Hollanti and Hsiao-Feng (Francis) Lu, *Member, IEEE*

***Abstract*—In this paper, the need for the construction of asymmetric and multiblock space–time codes is discussed. Above the trivial puncturing method, i.e., switching off the extra layers in the symmetric multiple-input multiple-output (MIMO) setting, two more sophisticated asymmetric construction methods are proposed. The first method, called the block diagonal method (BDM), can be converted to produce multiblock space–time codes that achieve the diversity–multiplexing tradeoff (DMT). It is also shown that maximizing the density of the newly proposed block diagonal asymmetric space–time (AST) codes is equivalent to minimizing the discriminant of a certain order, a result that also holds as such for the multiblock codes. An implicit lower bound for the density is provided and made explicit for an important special case that contains e.g., the systems equipped with $4\mathrm{Tx}$ $+2\mathrm{Rx}$ antennas. Further, an explicit scheme achieving the bound is given. Another method proposed here is the Smart Puncturing Method (SPM) that generalizes the subfield construction method proposed in earlier work by Hollanti and Ranto and applies to any number of transmitting and lesser receiving antennas. The use of the general methods is demonstrated by building explicit, sphere decodable codes using different cyclic division algebras (CDAs). Computer simulations verify that the newly proposed methods can compete with the trivial puncturing method, and in some cases clearly outperform it. The conquering construction exploiting maximal orders improves upon the punctured perfect code and the DjABBA code as well as the Icosian code. Also extensive DMT analysis is provided.**

***Index Terms*—Asymmetric space–time block codes (ASTBCs), cyclic division algebras (CDAs), dense lattices, discriminants, diversity–multiplexing tradeoff (DMT), maximal orders, multiblock codes, multiple-input multiple-output (MIMO) channels, normalized minimum determinant.**

I. Introduction

MULTIPLE-antenna wireless communication promises very high data rates, in particular when we have perfect channel state information (CSI) available at the receiver. In [1], the design criteria for such systems were developed, and further on the evolution of space–time (ST) codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch and especially on the so-called asymmetric and multiblock space–time codes. We are interested in the coherent multiple-input multiple-output (MIMO) case where the receiver perfectly knows the channel coefficients. The received signal is

$$Y = HX + N$$

where X is the transmitted codeword taken from the space–time block code (STBC) $\mathcal{C}$, H is the Rayleigh-fading channel response matrix and the elements of the noise matrix N are independent and identically distributed (i.i.d.) complex Gaussian random variables. Throughout the paper, n_t (respectively, n_r) denotes the number of transmitting (respectively, receiving) antennas #Tx (respectively, #Rx).

From the pairwise error probability (PEP) point of view [2], the performance of a space–time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X-X'$ taken over all distinct code matrices $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. For non-zero square matrices, being full-rank coincides with being invertible. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix $(X - X')(X - X')^{\dagger}$, where $\dagger$ indicates the complex conjugate transpose of a matrix. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$. If it is bounded away from zero even in the limit as the spectral efficiency approaches infinity, the ST code is said to have the *nonvanishing determinant* (NVD) property [3]. Note that the minimum determinant defined here is actually the square of the minimum determinant of a lattice defined below.

Definition 1.1: The *data rate* R in bits per channel use (bpcu) is given by

$$R = \frac{1}{T}\log_2(|\mathcal{C}|)$$

where $|\mathcal{C}|$ is the size of the code, and T is the block length.

Here, the *code rate* is defined as the ratio of the number of transmitted information symbols (complex, e.g., QAM symbols) to the decoding delay (equivalently, block length) of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. If this ratio is equal to the delay, the code is said to have *full rate*.

The very first STBC for two transmit antennas was the *Alamouti code* [4] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e., the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been

Manuscript received December 26, 2007; revised October 24, 2008. Current version published February 25, 2009. The work of C. Hollanti is supported in part by the Finnish Cultural Foundation, the Finnish Academy of Science, and the Foundation of the Rolf Nevanlinna Institute, Finland. The material in this paper was presented in part at the IEEE Information Theory Workshop, Bergen, Norway, July 2007, and at the IEEE International Symposium on Information Theory, Toronto, ON, Canada, July 2008.

C. Hollanti was with the Laboratory of Discrete Mathematics for Information Technology, Turku Centre for Computer Science, Finland. She is now with the Department of Mathematics, FI-20014 University of Turku, Finland (e-mail: cajoho@utu.fi).

H.-F. Lu is with Department of Communications Engineering, National Chiao Tung University, Hsinchu 300, Taiwan (e-mail:francis@cc.nctu.edu.tw).

Communicated by E. Viterbo, Associate Editor for Coding Techniques.

Color version of Figure 2 is available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2008.2011449

proposed as STBCs in various papers, e.g., [5]–[18] to name just a few. Major amount of the work in recent years has concentrated on adding multiplexing gain and/or combining it with a good minimum determinant, so that the resulting constructions can achieve the so-called diversity–multiplexing tradeoff (DMT) in [19]. It has been shown in [15] that cyclic division algebra (CDA) based square ST codes with the NVD property achieve the DMT. This result also extends over multiblock space–time codes [20]. The codes proposed in [17] all fall into this category (as do many other codes too) and are in that sense optimal. One of the goals of this paper is to generalize some of the results of [17] to the asymmetric and multiblock case.

After a cyclic division algebra has been chosen, the next step is to choose a corresponding lattice, or what amounts to the same thing, to choose an order within the algebra. Most authors, including [10] and [15], have gone with the so-called natural order (see the next section for a definition). One of the points the authors wanted to emphasize in [17] was to use maximal orders instead. The idea is that one can sometimes use several cosets of the natural order and hence transmit at a higher rate without sacrificing anything in terms of the minimum determinant or the coding gain. So the study of maximal orders is clearly motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available. The standard matrix representation of the natural order results in codes that have a so-called threaded layered structure [21]. When a maximal order is used, the code will then also extend "between layers". Earlier, maximal orders have been successfully used in the construction of MISO and symmetric MIMO lattices, see [5], [22], [17]. For more information on matrix representations of division algebras and their use as MIMO STBCs the reader can refer to [23], [7].

Recently, different methods for constructing asymmetric [24], [25] and multiblock [20] space–time codes have been proposed. *Asymmetric* codes are targeted at the code design for downlink transmission where the number of Rx antennas is strictly less than the number of Tx antennas. Typical examples of such situations are $3+\mathrm{G}$ mobile phones and DVB-H (Digital Video Broadcasting-Handheld) user equipment, where only a very small number of antennas fits at the end user site. Multi-block codes, for their part, are called for when one wishes to obtain vanishing error probability in addition to the DMT optimality.

Remark 1.1: We want to note that in this paper the emphasis is purely on the construction of sphere decodable asymmetric schemes having a minimum delay, and hence we do not intend to compete with the symmetric schemes that will naturally have a higher rate. The problem of constructing minimum-delay symmetric schemes has been efficiently solved already, see e.g., [10], [17]. However, unless at least n_t receiving antennas is used, such codes cannot be decoded by using simple decoding methods such as a sphere decoder, and this is the very reason why we now consider the construction of sphere decodable codes for n_r receiving antennas, n_r being strictly less than the number of transmitters n_t.

We define a *lattice* to be a discrete finitely generated free abelian subgroup L of a real or complex finite dimensional vector space, called the ambient space. In the space–time (ST) setting a natural ambient space is the space $\mathcal{M}_n(\mathbf{C})$ of complex $n\times n$ matrices. The *Gram matrix* is defined as

$$G(L)=\left(\Re\mathrm{tr}\left(x_i x_j^\dagger\right)\right)_{1\le i,j\le k} \tag{1}$$

where tr is the matrix trace (=sum of the diagonal elements), and $x_i\in\mathcal{M}_n(\mathbf{C}), i=1,\ldots,k$, form a $\mathbf{Z}$-basis of L. The rank k of the lattice is upper bounded by $2n^2$. Note that we really need to take the real part of the trace in the Gram matrix, as the matrices $x_i x_j^\dagger$ are not necessary real as themselves for $i\neq j$. The Gram matrix has a positive determinant equal to the squared measure of the fundamental parallelotope $m(L)^2$. A change of basis does not affect the measure $m(L)$.

Any lattice L with the NVD property [8] can be scaled, i.e., multiplied by a real constant t, either to satisfy $\det_{\min}(L)=\min_{M\in L\setminus\{0\}}\det(M)=1$ or to satisfy $m(L)=1$. This is because $\det_{\min}(tL)=t^n\det_{\min}(L)$ and $m(tL)=t^k m(L)$. As the minimum determinant determines the asymptotic pairwise error probability, this gives rise to natural numerical measures for the quality of a lattice.

Definition 1.2: Following [26], we shall denote by $\delta(L)$ the *normalized minimum determinant* of the lattice L, i.e., here we first scale L to have a unit size fundamental parallelotope. Dually we denote by $\rho(L)=1/m(L)$ the *normalized density* of the lattice L, when we first scale the lattice to have unit minimum determinant, and only then compute the quantity $1/m(L)$. In other words, we define

$$\delta(L)=\frac{\det_{\min}(L)}{m(L)^{n/k}}$$

$$\rho(L)=\frac{(\det_{\min}(L))^{k/n}}{m(L)}.$$

When comparing the minimum determinants of different codes, one should always use the normalized minimum determinant. To avoid confusion let us mention that from now on, when we talk about minimum determinant we always mean $\det_{\min}(L)$ and not its square as in the traditional definition of minimum determinant (see above). The squared normalized minimum determinant $\delta(L)^2$ can be righteously identified with the coding gain. According to the above definition, maximizing the coding gain, i.e., the normalized minimum determinant, is equivalent to maximizing the (normalized) density of the code. Formally, we get the following proposition.

Proposition 1.1: The coding gain of a lattice L equals

$$\delta(L)^2=\rho(L)^{2n/k}.$$

Hence, increasing the density is equivalent to increasing the coding gain.

Given that maximal orders provide the best codes in terms of minimum determinant versus average power we are left with the question: Which division algebra should we use? To continue the analogy from the theory of error-correcting codes we want to find the codes with the highest possible density. That is, with the smallest fundamental parallelotope. In [17] we developed

the required tools for parameterizing cyclic division algebras with a given center and index. Also an achievable lower bound for the measure of the fundamental parallelotope was derived.

One aim in this paper is to generalize the notions and results from [17] to the *asymmetric scheme* where the number of receiving antennas is strictly less than the number of transmitting antennas. As the main contributions, we

- propose new methods for constructing asymmetric space–time codes, one of which is applicable for any number of transmitting and receiving antennas ($\#\mathrm{Rx} < \#\mathrm{Tx}$);
- prove that similarly to the symmetric scheme, maximizing the density (i.e., finding the most efficient packing in the available signal space) of codes arising from the so-called block diagonal method is equivalent to minimizing the discriminant of an order. With the aid of this observation we generalize the density bound from [17] to the asymmetric scheme;
- derive an explicit density upper bound for the $4\mathrm{Tx} + 2\mathrm{Rx}$ case;
- provide an explicit $4\mathrm{Tx} + 2\mathrm{Rx}$ construction achieving our density bound;
- give a table comparing the normalized minimum determinants and densities of different block diagonal AST codes;
- show that the block diagonal method can be converted to produce multiblock ST codes [20] that achieve the DMT, and that the density bound is also applicable as such to these multiblock codes;
- provide extensive DMT alalysis of the proposed codes;
- demonstrate by simulations that by using the newly proposed methods we can outperform the punctured Perfect code and the DjABBA code [25] as well as the Icosian code [27] in BLER performance.

The paper is organized as follows. In Section II we will shortly motivate this research and describe our solutions to the stated problems. In Section III, various algebraic notions related to cyclic algebras, orders, and discriminants are introduced. If the reader is familiar with the standard symmetric cyclic division algebra based space–time codes, this introductory section can safely be skipped. Furthermore, it is shown that maximizing the density of the code, i.e., minimizing the fundamental parallelotope is equivalent to minimizing the discriminant. This leads us to Section IV, where we recall the achievable lower bound from [17] for the discriminant in the symmetric case. In Section V we describe the block diagonal construction method for asymmetric ST lattices. We generalize the density bound from [17] to the block diagonal AST codes in Section V-A, and show in Section V-B that it also holds as such to the multiblock codes [20]. Also explicit example codes are given in Section V-C accompanied with a table comparing their densities and normalized minimum determinants. Further, in Section V-D we derive an explicit, achievable density bound for the $4\mathrm{Tx} + 2\mathrm{Rx}$ case and show that it is achieved by one of the proposed constructions. The smart puncturing method is described in Section VI, and finally some simulation results and DMT analysis are provided in Sections VII and VIII, respectively. Section IX contains the conclusions.

II. Motivation and Problem Statement

In some applications the number of Rx antennas is required to be strictly less than the number of Tx antennas. Typical examples are $3 + \mathrm{G}$ mobile phones and DVB-H (Digital Video Broadcasting-Handheld) user equipment, where only a very small number of antennas fits at the end user site. One may also think of downlink transmissions in wireless networks, where one can usually fit more antennas in the access point than in a laptop. For such application, the symmetric, minimum-delay MIMO constructions arising from the theory of cyclic division algebras (see e.g., [10]) have to be modified. For simplicity, the concrete examples given here concentrate on the $4\mathrm{Tx}+2\mathrm{Rx}$ antenna case: if we could afford four Rx antennas, the task would be easy—just to use the 4×4 minimum-delay, rate-optimal CDA-based construction transmitting 16 (complex, usually QAM/HEX) information symbols in four time slots, i.e., four in each time slot. Now, however, the reduced number of Rx antennas limits the transmission down to two symbols per each time slot (cf. Definition 1.1) if we wish to enable efficient decoding such as sphere decoding.

We have come up with two different types of solutions to this problem. Both solutions take advantage of cyclic division algebras and yield rate n_r codes with a non-vanishing determinant. Let us denote by $n_t = n_r m$ the number of transmitters in the usual symmetric CDA-based MIMO system and suppose we want to construct a code for $n_t\mathrm{Tx} + n_r\mathrm{Rx}$ antennas. In the *Block Diagonal Method* (BDM) the idea is to first pick an index n_r division algebra with a center that is 2 m-dimensional over $\mathbf{Q}$, form isomorphic copies of it and then use them as $n_r \times n_r$ diagonal blocks in an $n_t \times n_t$ code matrix. Another possibility is to take the symmetric $n_t \times n_t$ MIMO code, but choose the elements in the matrix from an intermediate field of degree $2n_r$ over $\mathbf{Q}$ instead of the maximal subfield. This method can be generalized to *any number of transmitters and receivers* ($\#\mathrm{Rx} < \#\mathrm{Tx}$) by performing so called *Smart Puncturing Method* (SPM) instead of restricting the elements to belong to some fixed subfield. In practice, this means that we puncture at an arbitrary level, i.e., set a required number of QAM/HEX coeffiecients of basis elements to zero. These methods shall be explained in greater detail in Sections V and VI accompanied with illuminating examples.

In this paper, we will thoroughly analyze (in class field theoretic terms) the block diagonal method. The smart puncturing method will be treated in more detail in a forthcoming paper.

III. Cyclic Algebras, Orders, and Discriminants

We refer the interested reader to [23] and [7] for a detailed exposition of the theory of simple algebras, cyclic algebras, their matrix representations and their use in ST-coding. We only recall the basic definitions and notations here. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (respectively, E^*) denotes the set of the nonzero elements of F (respectively, E). In the interesting cases F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$ corresponding to the QAM and HEX alphabets, respectively. We assume that E/F is a cyclic field extension of degree n with the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be

the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathcal{A}$, and in practice $n_t = n$), that is

$$\mathcal{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E$$

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $A =:$

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

We refer to this as the standard matrix representation of $\mathcal{A}$. Observe that some variations are possible here. E.g., one may move the coefficients γ from the upper triangle to the lower triangle by conjugating this matrix with a suitable diagonal matrix. Similarly, one may arrange to have the first row to contain the "pure" coefficients $x_0, \ldots, x_{n-1}$. Such changes do not affect the minimum determinant nor the density of the resulting lattices.

In practice, some restrictions to the elements $x_i \in E$ and γ have to be made, see Definition 3.4 and the comment below. If we denote the integral basis of E/F by $\{e_0, e_1, \ldots, e_{n-1}\}$, then the elements x_i, $i = 0, \ldots, n-1$ in the above matrix are restricted to take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathcal{O}_F$ for all $k = 0, \ldots, n-1$. Hence n information symbols are transmitted per channel use, i.e., the design has rate n. In literature this is often referred to as having a *full rate*.

Definition 3.1: The determinant of the matrix A above is called the *reduced norm* of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$.

Remark 3.1: The connection between the usual norm map $N_{\mathcal{A}/F}(a)$ and the reduced norm $nr(a)$ of an element $a \in \mathcal{A}$ is $N_{\mathcal{A}/F}(a) = (nr(a))^n$, where n is the degree of E/F.

Definition 3.2: An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is *central* if its center $Z(\mathcal{A}) = \{a \in \mathcal{A} \,|\, aa' = a'a \; \forall a' \in \mathcal{A}\} = F$.

All algebras considered in this paper are central simple.

A division algebra may be represented as a cyclic algebra in many ways as demonstrated by the following example.

Example 3.1: The division algebra $\mathcal{GA}$ used in [3] to construct the Golden code is a cyclic algebra with $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(i, \sqrt{5})$, $\gamma = i$, when the F-automorphism σ is determined by $\sigma(\sqrt{5}) = -\sqrt{5}$. We also note that in addition to this representation $\mathcal{GA}$ can be given another construction as a cyclic algebra. As now $u^2 = i$ we immediately see that $F(u)$ is a subfield of $\mathcal{GA}$ that is isomorphic to the eighth cyclotomic field $E' = \mathbf{Q}(\zeta)$, where $\zeta = (1+i)/\sqrt{2}$. The relation $u\sqrt{5} = -\sqrt{5}u$ read differently means that we can view u as the complex number ζ and $\sqrt{5}$ as the auxiliary generator, call it $u' = \sqrt{5}$. We thus see that the cyclic algebra

$$E' \oplus u'E' = (E'/F, \sigma', \gamma')$$

is isomorphic to the Golden algebra. Here σ' is the F-automorphism of E' determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

The element γ is often called a *non-norm element* due to Theorem 3.2 by A. A. Albert [28, Theorem 11.12, p. 184]. It provides us with a condition of when a cyclic algebra is a division algebra. The original result was stated for $t = 1, 2, \ldots, n-1$, but can be simplified after the next lemma.

Lemma 3.1: Let $\gamma \in F^*$ and E/F be as above. Consider the set S of exponents $t \in \mathbf{Z}$ such that γ^t is a norm of an element of E. Then

$$S = k\mathbf{Z}$$

for some $k \,|\, n$.

Proof: The mapping $f : t \mapsto \gamma^t$ is a homomorphism of groups from $(\mathbf{Z}, +)$ to $(F^*, \cdot)$. Because $H = N_{E/F}(E^*)$ is a subgroup of F^*, and $S = f^{-1}(H)$, we immediately see that S is a subgroup of $(\mathbf{Z}, +)$. From basic algebra it now follows that S is cyclic, i.e., $S = k\mathbf{Z}$ for some $k \in \mathbf{Z}$. On the other hand, as $\gamma \in F^*$ we get that $\gamma^n = N_{E/F}(\gamma)$, and hence $n \in S$. Therefore $k \,|\, n$. □

Proposition 3.2 (Norm Condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Proof: We are to prove the equivalence of two conditions, the original stating that γ^t is not a norm for any t in the range $1, 2, \ldots, n-1$, and the relaxed version stating the same for those t in the same range that are also divisors of n. One implication is clear, and the other follows from the above lemma. Namely, if there are integers t in the range $1, 2, \ldots, n-1$ such that γ^t happens to be a norm, then the lemma tells us that the smallest such t must be a divisor of n. □

Remark 3.2: We can even relax the above conditions for t. The proof of the previous lemma shows that actually it suffices to check that $\gamma^{n/p}$ is not a norm for any prime divisor p of n. For example, when $n = 8$, it suffices to check that γ^4 is not a norm.

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [29].

Let R denote a Noetherian integral domain with a quotient field F (e.g., $R = \mathbf{Z}[i]$ and $F = \mathbf{Q}(i)$), and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 3.3: An *R-order* in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over R and generates $\mathcal{A}$ as a linear space over F. An order Λ is called *maximal*, if it is not properly contained in any other R-order.

In the rest of the paper, Λ will always denote an order and can be treated as an algebraic lattice. Let us illustrate the above definition by concrete examples.

Example 3.2:

(a) Orders always exist: If M is a *full* R-lattice in $\mathcal{A}$, i.e., $FM = \mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M) =$

$\{x \in \mathcal{A} \,|\, xM \subseteq M\}$ is an R-order in $\mathcal{A}$. The right order is defined in an analogous way.
(b) If R is the ring of integers $\mathcal{O}_F$ of the number field F, then the ring of integers $\mathcal{O}_E$ of the extension field E is the unique maximal R-order in E. For example, in the case of the cyclotomic field $E = \mathbf{Q}(\zeta)$, where $\zeta = \exp(2\pi i/k)$ is a primitive root of unity of order k the maximal order is $\mathcal{O}_E = \mathbf{Z}[\zeta]$.
(c) The set of integral elements does not form a ring in the non-commutative case. As an easy counter-example one can use the ring of Lipschitz quaternions

$$\mathcal{L} = \{q = a + bi + cj + dk \in \mathbb{H} \,|\, a, b, c, d \in \mathbf{Z}, \; i^2 = j^2 = k^2 = -1, ij = k\}$$

a subring of the Hamiltonian quaternions $\mathbb{H}$ used for the construction of the Alamouti code. For instance, consider the polynomial $f(x) = x^2 + 1$ having integral coefficients. The element $t = \frac{3i+4j}{5}$ is one of the (infinitely many) roots of the polynomial $f(x)$, and hence may be called integral. However, if we try to adjoin t to the ring $\mathcal{L}$, we end up with a set that will also contain the element it. The reduced trace $\mathrm{tr}(it) \in \mathbf{Q}$ is not an integer, hence we cannot have an order that would contain both the Lipschitz quaternions and t.

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g., [29, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO-lattices. We identify an order (or its subsets) with its standard matrix representation.

Proposition 3.3: Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $\mathrm{nr}(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.

Definition 3.4: In any cyclic algebra we can always choose the element $\gamma \in F^*$ to be an algebraic integer. We immediately see that the $\mathcal{O}_F$-module

$$\Lambda_{\mathrm{NAT}} = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E$$

where $\mathcal{O}_E$ is the ring of integers, is an $\mathcal{O}_F$-order in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to this $\mathcal{O}_F$-order as the *natural order*. An alternative appellation would be *layered order*, as the corresponding MIMO-lattice of this order has the layered structure described in [21].

Remark 3.3: We want the reader to note that in any central simple algebra a maximal $\mathbf{Z}$-order is a maximal $\mathcal{O}_F$-order as well. Note also that if γ is not an algebraic integer, then Λ fails to be closed under multiplication. This may adversely affect the minimum determinant of the resulting matrix lattice, as elements not belonging to an order may have non-integral (and hence small) norms.

Definition 3.5: Let $m = \dim_F \mathcal{A}$. The *discriminant* of the R-order Λ is the ideal $d(\Lambda/R)$ in R generated by the set

$$\left\{ \det(\mathrm{tr}(x_i x_j))_{i,j=1}^m \,\middle|\, (x_1, \ldots, x_m) \in \Lambda^m \right\}.$$

In the interesting cases of $F = \mathbf{Q}(i)$ (respectively, $F = \mathbf{Q}(\sqrt{-3})$) the ring $R = \mathbf{Z}[i]$ (respectively, $R = \mathbf{Z}[\omega]$, $\omega = (-1 + \sqrt{-3})/2$) is a Euclidean domain, so in these cases (as well as in the case $R = \mathbf{Z}$) it makes sense to speak of the discriminant as an element of R rather than as an ideal. We simply pick a generator of the discriminant ideal, and call it the discriminant. Equivalently we can compute the discriminant as

$$d(\Lambda/R) = \det(\mathrm{tr}(x_i x_j))_{i,j=1}^m$$

where $\{x_1, \ldots, x_m\}$ is any R-basis of Λ.

Remark 3.4: It is readily seen that whenever $\Lambda \subseteq \Gamma$ are two R-orders, then $d(\Gamma/R)$ is a factor of $d(\Lambda/R)$. It also turns out (cf. [29, Theorem 25.3]) that all the maximal orders of a division algebra share the same discriminant that we will refer to as the discriminant of the division algebra. In this sense a maximal order has the smallest possible discriminant among all orders within a given division algebra, as all the orders are contained in some maximal order.

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following result proved in [17] is unsurprising and immediately generalizes to the asymmetric scheme as well as was shown in [24].

Lemma 3.4: Assume that F is an imaginary quadratic number field and that 1 and ν form a $\mathbf{Z}$-basis of its ring of integers R. Assume further that the order Λ is a free R-module (an assumption automatically satisfied, when R is a principal ideal domain). Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |\Im\nu|^{n^2} |d(\Lambda/R)|.$$

In the respective cases $F = \mathbf{Q}(i)$ and $F = \mathbf{Q}(\sqrt{-3})$ we have $\nu = i$ and $\nu = (-1+\sqrt{-3})/2$, respectively, so we immediately get the following two corollaries.

Corollary 3.5: Let $F = \mathbf{Q}(i), R = \mathbf{Z}[i]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = |d(\Lambda/\mathbf{Z}[i])|.$$

Example 3.3: When we scale the Golden code [3](cf. Example 3.1) to have a unit minimum determinant, all the 8 elements of its $\mathbf{Z}$-basis will have length $5^{1/4}$ and the measure of the fundamental parallelotope is thus 25. In view of all of the above this is also a consequence of the fact that the $\mathbf{Z}[i]$-discriminant of the natural order of the Golden algebra $\mathcal{GA}$ is equal to 25. As was observed in [30] the natural order happens to be maximal in this case, so the Golden code cannot be improved upon by enlarging the order within $\mathcal{GA}$.

Corollary 3.6: Let $\omega = (-1 + \sqrt{-3})/2$, $F = \mathbf{Q}(\omega)$, $R = \mathbf{Z}[\omega]$, and assume that $\Lambda \subset (E/F, \sigma, \gamma)$ is an R-order. Then the measure of the fundamental parallelotope equals

$$m(\Lambda) = (\sqrt{3}/2)^{n^2} |d(\Lambda/\mathbf{Z}[\omega])|.$$

The upshot in [17] was that in both cases maximizing the density of the code, i.e., minimizing the fundamental parallelotope,

is equivalent to minimizing the discriminant. Thus, in order to get the densest MIMO-codes one needs to look for division algebras that have a maximal order with as small a discriminant as possible.

For an easy reference we also include the following result [17] that is a relatively easy consequence of the definitions.

Lemma 3.7: Let E/F be as above, assume that γ is an algebraic integer of F, and let Λ be the natural order of Definition 3.4. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then

$$d(\Lambda/\mathcal{O}_F) = d(\mathcal{O}_E/\mathcal{O}_F)^n \gamma^{n(n-1)}.$$

To conclude the section, we include the following simple but interesting result on maximal orders explaining why using a principal one-sided (left or right) ideal instead of the entire order will not change the density of the code. For the proof, see [17, Lemma 7.1]

Lemma 3.8: Let Λ be a maximal order in a cyclic division algebra over an imaginary quadratic number field. Assume that the minimum determinant of the lattice Λ is equal to one. Let $x \in \Lambda$ be any non-zero element. Let $\mu > 0$ be a real parameter chosen so that the minimum determinant of the lattice $\mu(x\Lambda)$ is also equal to one. Then the fundamental parallelotopes of these two lattice have the same measure

$$m(\Lambda) = m(\mu(x\Lambda)).$$

IV. The Discriminant Bound

In this section, we recall some more material from [17] to be used later on in Section V.

Again let F be an algebraic number field that is finite dimensional over $\mathbf{Q}$ and $\mathcal{O}_F$ its ring of integers. In what follows by the size of ideals of $\mathcal{O}_F$ we mean that ideals are ordered by the absolute values of their norms to $\mathbf{Q}$, so e.g., in the case $\mathcal{O}_F = \mathbf{Z}[i]$ we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3 as they have norms 5 and 9, respectively.

Theorem 4.1: [17, Discriminant bound] Assume that F is a totally complex number field, and that P_1 and P_2 are the two smallest prime ideals in $\mathcal{O}_F$. Then the smallest possible discriminant of all central division algebras over F of index n is

$$(P_1 P_2)^{n(n-1)}.$$

We remark that the division algebra achieving this bound is by no means unique.

Example 4.1: The smallest primes of the ring $\mathbf{Z}[i]$ are $1+i$ and $2 \pm i$. They have norms 2 and 5, respectively. The smallest primes of the ring $\mathbf{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 3.5 and 3.6 we have arrived at the following bounds.

Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq 10^{n(n-1)/2}.$$

Let Λ be an order of a central division algebra of index n over the field $\mathbf{Q}(\omega)$, $\omega = (-1+\sqrt{-3})/2$. Then the measure of a fundamental parallelotope of the corresponding lattice

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}.$$

Example 4.2: Let $F = \mathbf{Q}(\sqrt{-3})$, so $\mathcal{O}_F = \mathbf{Z}[\omega]$. In this case the two smallest prime ideals are generated by 2 and $1-\omega$ and as noted above they have norms 4 and 3, respectively. By Theorem 4.1 the minimal discriminant is $4(1-\omega)^2$ when $n=2$. As the absolute value of $1-\omega$ is $\sqrt{3}$ an application of the formula in Corollary 3.6 shows that the lattice L of the code achieving this bound has $m(L) = 27/4$. In [22] we showed that a maximal order of the cyclic algebra $(E/F, \sigma(i) = -i, \gamma = \sqrt{-3})$, where $E = \mathbf{Q}(i, \sqrt{-3})$, achieves this bound.

For more information on finding maximal orders and their discriminants, see [17]. In practice maximal orders can easily be computed with the aid of the (unfortunately commercial) MAGMA software [31], or in small cases by hand following [32] (see also [33], [34]). The computation and decoding of maximal order will be treated in more detail in a forthcoming paper by Hollanti and Ranto [35].

We conclude this section by a couple of remarks[1] related to the use of outer codes and our choice to consider only codes having a minimum delay.

Remark 4.1: While the concatenation of the maximal-order space–time code as the inner code and the conventional error correction code as the outer code is beyond the scope of this work, it is expected that such concatenation will result in a smaller multiplexing gain as the outer code has rate less than 1. However, the error performance will be significantly improved due to the use of additional error correction techniques. On the other hand, we must point out that since 1) the inner maximal-order code makes use of sphere decoding, which is a hard-decision based decoding, and 2) such inner decoder cannot provide soft information for the input of output decoder, it is technically impossible to use either low-density parity check (LDPC) code or turbo code as the outer code as these codes requires a soft-input–soft-output (SISO) decoder in order to deliver the promised near-capacity performance. Nevertheless, some conclusion can be easily drawn. From simulation we have already seen that, in the symmetric case, the maximal order code outperforms the perfect code, meaning that the former has lower error probability than the latter; the overall error probability of the concatenated maximal-order code after incorporating the outer decoder must be even lower than that of the concatenated perfect code, simply because the BER curve of the outer decoder is monotonically decreasing in SNR, and such conclusion holds for all outer codes.

Remark 4.2: In this paper the focus is on square matrices, i.e., on codes having a minimum delay. If longer delay is allowed, then the optimal DMT can be achieved at least in some special

[1]The remarks are invoked by the comments of the anonymous reviewers of this paper. We thank all the reviewers for the careful reading of our paper. Also complexity issues were brought up by one of the reviewers, hence a short discussion on the decoding complexity has been added in the simulation results section.

cases. The authors of the present paper have submitted a separate work related to this subject, see [41]. Increasing the delay requires lattices with a higher dimension, so also the decoding process will get more complex.

V. Constructing Asymmetric and Multiblock Space–Time Codes by the Block Diagonal Method (BDM)

A straightforward way to obtain AST lattices would be just to "switch off the extra layers" (following [25] and [24]) in a symmetric MIMO setting, i.e., by trivial puncturing. In the case of $4\mathrm{Tx} + 2\mathrm{Rx}$ antennas this would mean that in the standard matrix representation we set e.g., $x_1 = x_3 = 0$ in order to transmit a limited number of symbols that can be received with only two receivers. In this and the following section we present two more sophisticated methods for constructing AST lattices that still admit efficient sphere decoding.

A. Block Diagonal Asymmetric ST Lattices

In this section, we recall *Method 1* from [24]. Let us rename this method as *Block Diagonal Method* (BDM).

Let us consider an extension tower $F \subseteq L \subseteq E$ with the degrees $[E:L] = n_r, [L:F] = m$ and with the Galois groups $\mathrm{Gal}(E/F) = \langle \tau \rangle$, $\mathrm{Gal}(E/L) = \langle \sigma = \tau^m \rangle$. Let

$$\mathcal{B} = (E/L, \sigma, \gamma) = E \oplus uE \oplus \cdots \oplus u^{n_r-1}E$$

be an index n_r division algebra, where the center L is fixed by $\sigma = \tau^m$. We denote by $\#\mathrm{Tx} = n_t = n_r m$.

Note that if one has a symmetric, index $n_t = n_r m$ CDA-based STBC, the algebra $\mathcal{B}$ can be constructed by just picking a suitable intermediate field $L \subseteq E$ of a right degree as the new center.

An element $b = x_0 + \cdots + u^{n_r-1}x_{n_r-1}$, $x_i \in E$, $i = 0, \ldots, n_r - 1$ of the algebra $\mathcal{B}$ has the standard representation as an $n_r \times n_r$ matrix $B = (b_{ij})_{1 \le i,j \le n_r}$ as given in Section III.

However, we can afford an $n_t \times n_t$ packing as we are using n_t transmitting antennas. This can be achieved by using the isomorphism τ. Let us denote by $\tau^k(\mathcal{B}) = (E/L, \sigma, \tau^k(\gamma))$, $k = 0, \ldots, m-1$ the m isomorphic copies of $\mathcal{B}$ and the respective matrix representations by

$$\tau^k(B) = (\tau^k(b_{ij}))_{1 \le i,j \le n_r},\ k = 0, \ldots, m-1. \tag{2}$$

The next proposition shows that by using these copies as diagonal blocks we obtain an infinite lattice with non-vanishing determinant.

Proposition 5.1 (BDM): Let $b \in \Lambda \subseteq \mathcal{B}$ and $F = \mathbf{Q}(\delta)$, where $\delta \in \{i, \omega\}$. Assume $\gamma \in \mathcal{O}_L$. The block diagonal lattice

$$\mathcal{C}(\Lambda) = \left\{ M = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \right\}$$

built from (2) has a nonvanishing determinant $\det(M) = \prod_{i=0}^{m-1} \det(\tau^i(B)) \in \mathbf{Z}[\delta]$. Thus, the minimum determinant is equal to one for all m. The code rate equals $n_r^2 m / n_r m = n_r$.

Proof: According to Definition 3.1 and Proposition 3.3

$$\begin{aligned} \det(M) &= \prod_{i=0}^{m-1} \det(\tau^i(B)) = \prod_{i=0}^{m-1} nr(\tau^i(b)) \\ &= \prod_{i=0}^{m-1} \tau^i(nr(b))) = N_{L/F}(nr(b)) \in \mathbf{Z}[\delta] \end{aligned}$$

and hence $|\det(M)| \ge 1$. □

Remark 5.1: In [36] an approach similar to the BDM was used for the MIMO amplify-and-forward cooperative channel.

Now the natural question is how to choose a suitable division algebra. In [15] and [16] several systematic methods for constructing extensions E/L are provided. All of them make use of cyclotomic fields. Next we will show that also in the asymmetric scheme, maximizing the code density (i.e., minimize the volume of the fundamental parallelotope, see [17]) with a given minimum determinant is equivalent to minimizing a certain discriminant. In the next section we shall show that this also holds for the multiblock codes from [20].

First we need the following result. For the proof, see [29, p. 223].

Lemma 5.2: Suppose $\Lambda \subseteq \mathcal{A} = (E/L, \tau, \gamma)$ is an $\mathcal{O}_F$-order and that $F \subseteq L$. The discriminants then satisfy

$$d(\Lambda/\mathcal{O}_F) = N_{L/F}(d(\Lambda/\mathcal{O}_L)) d(\mathcal{O}_L/\mathcal{O}_F)^{\dim_L \mathcal{A}}.$$

The same naturally holds in the commutative case when we replace $\mathcal{A}$ with E.

As a generalization to Lemma 3.4, we prove the following proposition.

Proposition 5.3: Assume that F is an imaginary quadratic number field and that $\{1, \nu\}$ forms a $\mathbf{Z}$-basis of its ring of integers $\mathcal{O}_F$. Let $n_r = [E:L], m = [L:F]$, $n_t = n_r m$, and $s = |\Im \nu|^{m n_r^2}$. If the order $\mathcal{C}(\Lambda)$ defined as in Proposition 5.1 is a free $\mathcal{O}_F$-module (which is always the case if $\mathcal{O}_F$ is a principal ideal domain), then the measure of the fundamental parallelotope equals

$$\begin{aligned} m(\mathcal{C}(\Lambda)) &= s|d(\Lambda/\mathcal{O}_F)| && (3) \\ &= s|d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} N_{L/F} d(\Lambda/\mathcal{O}_L)| && (4) \\ &= s|d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} \prod_{i=0}^{m-1} \tau^i(d(\Lambda/\mathcal{O}_L))|. && (5) \end{aligned}$$

Proof: In order to keep the notation simple let us assume $m = 2$. The proof directly generalizes to an arbitrary m. Let $A = (a_{ij})$ be an $n_t \times n_t$ complex matrix. We flatten it out into a $4 \times 4n_t^2$ matrix $L(A)$ by first forming a vector of length n_t^2 out of the entries (e.g., row by row) and then replacing a complex number z by a diagonal four by four matrix with entries $z, \tau(z), z^*$, and $\tau(z)^*$ (z^* is the usual complex conjugate of z). If A and B are two square matrices with n_t rows we can easily verify the identities as shown in (6) and (7) at the top of the following page.

Next let $\mathcal{X} = \{x_1, x_2, \ldots, x_{n_r^2}\}$ be an $\mathcal{O}_L$-basis for Λ. We form the $4n_r^2 \times 4n_r^2$ matrix $L(\mathcal{X})$ by stacking the matrices

$$L(A)L(B)^\dagger = \begin{pmatrix} \mathrm{tr}(AB^\dagger) & 0 & 0 & 0 \\ 0 & \tau(\mathrm{tr}(AB^\dagger)) & 0 & 0 \\ 0 & 0 & \mathrm{tr}(A^\dagger B) & 0 \\ 0 & 0 & 0 & \tau(\mathrm{tr}(A^\dagger B)) \end{pmatrix} \tag{6}$$

and

$$L(A)L(B^T)^T = \begin{pmatrix} \mathrm{tr}(AB) & 0 & 0 & 0 \\ 0 & \tau(\mathrm{tr}(AB)) & 0 & 0 \\ 0 & 0 & \mathrm{tr}(AB)^* & 0 \\ 0 & 0 & 0 & \tau(\mathrm{tr}(AB))^* \end{pmatrix}. \tag{7}$$

$L(x_i)_{4\times 4r^2}$ on top of each other. Similarly we get $R(\mathcal{X})$ by using the matrices $L(x_i^T)^T$ as column blocks. Then by (7) the matrix

$$M = L(\mathcal{X})R(\mathcal{X})$$

consists of four by four blocks of the form

$$L(x_i)L\left(x_j^T\right)^T = \mathrm{diag}(\mathrm{tr}(x_ix_j), \tau(\mathrm{tr}(x_ix_j)), \mathrm{tr}(x_ix_j)^*, \tau(\mathrm{tr}(x_ix_j))^*).$$

Clearly

$$\det R(\mathcal{X})R(\mathcal{X})^\dagger = \pm \det L(\mathcal{X})L(\mathcal{X})^\dagger$$

and

$$\det M = |d(\Lambda/\mathcal{O}_L)|^2 |\tau(d(\Lambda/\mathcal{O}_L))|^2.$$

Thus

$$|\det L(\mathcal{X})L(\mathcal{X})^\dagger|^{1/2} = |d(\Lambda/\mathcal{O}_L)||\tau(d(\Lambda/\mathcal{O}_L))|. \tag{8}$$

Next, we turn our attention to the Gram matrix. Let $\{1, \theta, \ldots, \theta^3\}$ be a $\mathbf{Z}$-basis for $\mathcal{O}_L$. Then by our assumptions the set $\mathcal{X} \cup \theta\mathcal{X} \cup \cdots \cup \theta^3\mathcal{X}$ is a $\mathbf{Z}$-basis for Λ. From the theory of algebraic numbers we know that

$$d(\mathcal{O}_F/\mathbf{Z}) = \det D(\nu)^2 \text{ and } d(\mathcal{O}_L/\mathbf{Z}) = \det D(\theta)^2 \tag{9}$$

where $D(\nu) = \left(\begin{smallmatrix} 1 & 1 \\ \nu & \nu^* \end{smallmatrix}\right)$ and

$$D(\theta) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \theta & \tau(\theta) & \theta^* & \tau(\theta)^* \\ \theta^2 & \tau(\theta^2) & (\theta^2)^* & \tau(\theta^2)^* \\ \theta^3 & \tau(\theta^3) & (\theta^3)^* & \tau(\theta^3)^* \end{pmatrix}.$$

From the identities $\Re(xy^*) = (xy^* + x^*y)/2$ and

$$D(\theta)L(x) = \begin{pmatrix} x & \tau(x) & x^* & \tau(x)^* \\ \vdots & & & \vdots \\ \theta^3 x & \tau(\theta^3 x) & (\theta^3 x)^* & \tau(\theta^3 x)^* \end{pmatrix}$$

together with (6) it follows that for any two $n_t \times n_t$ matrices A and B we have

$$\frac{1}{2}(D(\theta)L(A))(D(\theta)L(B))^\dagger = \begin{pmatrix} \Re(\mathrm{tr}(AB^\dagger)) & \cdots & \Re(\mathrm{tr}(A(\theta^3 B)^\dagger) \\ \vdots & & \vdots \\ \Re(\mathrm{tr}(\theta^3 AB^\dagger)) & \cdots & \Re(\mathrm{tr}(\theta^3 A(\theta^3 B)^\dagger)) \end{pmatrix}.$$

Therefore, if we denote by $D^{[n_r]}$ the $4n_r^2 \times 4n_r^2$ matrix having n_r^2 copies of $D(\theta)$ along the diagonal and zeros elsewhere, we get

$$G(\mathcal{C}(\Lambda)) = \frac{1}{2}\left(D^{[n_r]}L(\mathcal{X})\right)\left(D^{[n_r]}L(\mathcal{X})\right)^\dagger.$$

Thus

$$m(\mathcal{C}(\Lambda)) = \sqrt{\det G(\mathcal{C}(\Lambda))} = |\det L(\mathcal{X})L(\mathcal{X})^\dagger|^{1/2} \cdot \left(\frac{1}{4}\right)^{n_r^2} |\det D(\theta)|^{n_r^2}.$$

As

$$\left(\frac{1}{2}\right)^{2n_r^2} |\det D(\theta)|^{n_r^2} = |d(\mathcal{O}_L/\mathcal{O}_F)|^{n_r^2} |\Im\nu|^{2n_r^2}$$

by (9) and Lemma 5.2, (8) now gives us the claim when we still note (again by Lemma 5.2) that

$$d(\mathcal{O}_L/\mathcal{O}_F)^{n_r^2} d(\Lambda/\mathcal{O}_L)\tau(d(\Lambda/\mathcal{O}_L)) = d(\Lambda/\mathcal{O}_F). \tag{10}$$

□

Corollary 5.4: In the case $F = \mathbf{Q}(i)$ the volume equals

$$m(\mathcal{C}(\Lambda)) = |d(\Lambda/\mathbf{Z}[i])|.$$

Corollary 5.5: In the case $F = \mathbf{Q}(\omega)$, we get

$$m(\mathcal{C}(\Lambda)) = \left(\frac{\sqrt{3}}{2}\right)^{mn_r^2} |d(\Lambda/\mathbf{Z}[\omega])|.$$

Now we can conclude (cf. (4)) that the extensions $E/L, L/F$ and the order $\Lambda \subseteq \mathcal{B}$ should be chosen in such a way that the discriminants $d(\mathcal{O}_L/\mathcal{O}_F)$ and $d(\Lambda/\mathcal{O}_L)$ are as small as possible. By choosing a maximal order within a given division algebra we can minimize the norm of $d(\Lambda/\mathcal{O}_L)$ (cf. Remark 3.4). As in practice an imaginary quadratic number field F is contained in L, we know that L is totally complex. In that case the fact that

$$d(\Lambda/\mathcal{O}_L) \geq (P_1P_2)^{n_r(n_r-1)} \tag{11}$$

where P_1 and P_2 are prime ideals $\in \mathcal{O}_L$ with the smallest norms (to $\mathbf{Q}$) helps us in picking a good algebra (for the proof, see [17, Theorem 3.2]). Note that optimization with respect to $d(\mathcal{O}_L/\mathcal{O}_F)$ may result in a loss in $d(\Lambda/\mathcal{O}_L)$ and vice versa.

Keeping the above notation, we have now arrived at the following theorem.

Theorem 5.6 (Density Bound for Lattices From BDM): For the density of the lattice $\mathcal{C}(\Lambda), \Lambda \subseteq \mathcal{A}$ it holds that

$$\rho = \frac{1}{m(\mathcal{C}(\Lambda))} \leq s^{-1}|d(\mathcal{O}_L/\mathcal{O}_F)|^{-n_r^2}|N_{L/F}(P_1P_2)|^{n_r(1-n_r)}. \quad (12)$$

Remark 5.2: Note that as opposed to Example 4.1 (cf. [17]), here we do not automatically achieve nice, explicit lower bounds for $m(\mathcal{C}(\Lambda))$. That is a consequence of the fact that the center L can now be any field containing $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$, and thus determining the smallest ideals P_1 and P_2 or even the minimal $d(\mathcal{O}_L/\mathcal{O}_F)$ is not at all straightforward. An exact lower bound is hard to derive in the general case as the calculation of minimal number field discriminants is known to be a tricky problem. The reader may ponder over the fact that tables for minimal discriminants do exist in literature (though only for certain degrees, see e.g., [37]) so why not use them. We want to emphasize that these tables cannot be adapted here, as the fields in question do not necessarily contain the desired subfield $\mathbf{Q}(i)$ or $\mathbf{Q}(\omega)$. However, in the smallest (and perhaps the most practical) case of $4\mathrm{Tx}+2\mathrm{Rx}$ antennas we are able to give an explicit and even achievable upper bound for the density. We believe that the best one can do in the other cases is to take advantage of known bounds of more general nature such as Odlyzko's bound [38].

B. Minimum-Delay Multiblock ST Codes

The $n_t\mathrm{Tx}+n_r\mathrm{Rx}$ antenna AST code from Proposition 5.1 can be transformed into an $n_r\mathrm{Tx}+n_r\mathrm{Rx}$ antenna multiblock code [20] by an evident rearrangement of the blocks:

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \tau(B) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{m-1}(B) \end{pmatrix} \leftrightarrow (\, B \quad \cdots \quad \tau^{m-1}(B)\,). \quad (13)$$

As the Gram matrices of an AST lattice and a multiblock ST lattice coincide, Lemma 5.3 also holds for multiblock ST codes with the same parameters. Let the notation be as in Section V-A.

Proposition 5.7: Let $b \in \Lambda \subseteq \mathcal{B}$ and $F = \mathbf{Q}(\delta)$, where $\delta \in \{i, \omega\}$. Assume $\gamma \in \mathcal{O}_L$. As the lattice

$$\mathcal{C}'(\Lambda) = \{M = (B, \tau(B), \ldots, \tau^{m-1}(B))\}$$

built from (2) satisfies the generalized non-vanishing determinant property (cf. [20], [12]), it is optimal with respect to the DMT for all numbers of fading blocks m. Similarly as in Proposition 5.1,

$$\left|\prod_{i=0}^{m-1} \det(\tau^i(B))\right| \geq 1.$$

The code rate equals $n_r^2 m/n_r m = n_r$.

Proof: For the proof, see [20]. □

Proposition 5.8: The Gram determinants (cf. (1)) of the lattices $\mathcal{C}(\Lambda)$ and $\mathcal{C}'(\Lambda)$ coincide:

$$\det G(\mathcal{C}(\Lambda)) = \det G(\mathcal{C}'(\Lambda)).$$

Proof: This is obvious, as

$$\begin{aligned} &\mathrm{tr}(\mathrm{diag}(BB^\dagger, .., \tau^{m-1}(B)\tau^{m-1}(B)^\dagger)) \\ &= \sum_{i=0}^{m-1} \mathrm{tr}(\tau^i(B)\tau^i(B)^\dagger) \\ &= \mathrm{tr}(\sum_{i=0}^{m-1} (\tau^i(B)\tau^i(B)^\dagger)). \end{aligned}$$ □

An immediate consequence of Proposition 5.8 is as follows.

Corollary 5.9: The lattices $\mathcal{C}(\Lambda)$ and $\mathcal{C}'(\Lambda)$ share the same density, i.e., Proposition 5.3 can be adapted as such to the multiblock scheme.

C. Explicit Codes Using BDM

In this section we provide explicit asymmetric constructions for the important case of $4\mathrm{Tx}+2\mathrm{Rx}$ antennas. These codes can be modified for 2×2 multiblock use (cf. (13). The primitive nth root of unity will be denoted by ζ_n. The first three examples are given in terms of an asymmetric construction, whereas the last one is described as a multiblock code. However, with the aid of (13), an asymmetric code can always be transformed into a multiblock code and vice versa.

1) Perfect Algebra $\mathcal{PA}$: Let us consider an algebra with the same maximal subfield that was used for the 4×4 Perfect code in [10]. We have the nested sequence of fields $F \subseteq L \subseteq E$, where $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(\sqrt{5}, i)$, and $E = \mathbf{Q}(\theta, i)$ with $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos(2\pi/15)$. We denote this algebra by $\mathcal{PA} = (E/L, \sigma = \tau^2, \gamma) = E \oplus uE$, where $u^2 = \gamma = i$ and $\tau(\theta) = \theta^2 - 2$. As $\tau(\sqrt{5}) = -\sqrt{5}$, the field L is indeed fixed by $\sigma = \tau^2$. By embedding the algebra $\mathcal{PA}$ as in Proposition 5.1 we obtain the AST code

$$\mathcal{PA}_1 \subseteq \left\{ \begin{pmatrix} x_0 & i\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & i\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \right\}$$

where $x_i \in \mathcal{O}_E$. As the center is L with $[L : \mathbf{Q}(i)] = 2$ and $\mathcal{O}_L = \mathbf{Z}[i, \pi = (1+\sqrt{5})/2]$, the elements x_k in the matrix are of the form $x_k = a_{k,0} + a_{k,1}\pi + a_{k,2}\theta + a_{k,3}\pi\theta$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code transmits, on the average, 2 independent QAM symbols per channel use.

We can further improve the performance by taking the elements x_i from the ideal $a\mathcal{O}_E$, where $a = 1 - 3i + i\theta^2 \in \mathcal{O}_E$. Moreover, a change of basis given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{pmatrix}$$

guarantees an orthogonal lattice.

2) Cyclotomic Algebra $\mathcal{CA}$: The algebra $\mathcal{CA} = (E/L, \sigma = \tau^2 : \xi \mapsto -\xi, \gamma = 1 + s - i) = E \oplus uE$ (cf. [12], [22], [24]), for its part, has the nested sequence of fields $F \subseteq L \subseteq E$ with $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(s = \zeta_8)$, and $E = \mathbf{Q}(\xi = \zeta_{16})$. As we have

$\tau : \xi \mapsto i\xi, s \mapsto -s$, the field L is fixed by $\sigma = \tau^2$. Again by embedding the algebra $\mathcal{CA}$ as in Proposition 5.1, the AST code

$$\mathcal{CA}_1 \subseteq \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & \tau(\gamma)\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \right\}$$

with $x_i \in \mathcal{O}_E$ is obtained. The center is L with $[L : \mathbf{Q}(i)] = 2$ and $\mathcal{O}_L = \mathbf{Z}[s]$. The elements x_k in the matrix are of the form $x_k = \sum_{j=0}^{3} a_{k,j}\xi^j$, where $a_{k,j} \in \mathbf{Z}[i]$, hence the above code transmits on the average, 2 independent QAM symbols per channel use.

Note that we have chosen here a suitable non-norm element γ from $\mathcal{O}_L$ instead of $\mathcal{O}_F$ (cf. Section V.A). We get some energy savings as $|1 + s - i| < |2 + i|$.

The code $\mathcal{CA}_1$ can be made perfect (see [11]) by forcing γ to be unit, i.e., we can choose $\gamma = \frac{2+i}{2-i}$. The loss in the minimum determinant is compensated by an improvement in performance. We denote the perfect version of the code by $\mathcal{CA}_1$ PERF.

By doing this, we need not sacrifice the NVD property: Let $X = (X_1\ X_2\ X_3\ X_4)^T \in \mathcal{CA}_1$ PERF. If we denote by M the matrix where we have multiplied the matrix rows containing γ by $2 - i$, that is

$$M = ((2-i)X_1\ X_2\ (2-i)X_3\ X_4)^T \in \mathcal{CA}_1$$

then we have

$$|\det(M)| = |(2-i)^2 \det(X)| \geq 1$$

and hence

$$|\det(X)| \geq \frac{1}{5} > 0.$$

Note also that this is only possible because of the *additive* structure of the code. Taking powers of the elements $X \in \mathcal{CA}_1$ PERF into the code would result in a vanishing determinant (cf. Remark 3.3).

3) Algebra $\mathcal{IA}$—an Improved Maximal Order: Similarly as in the two previous subsections, we obtain a rate-2 AST code $\mathcal{IA}_1$ by introducing yet another algebra $\mathcal{IA} = (E/L, \sigma = \tau^2, \gamma = \sqrt{-3})$, where $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(i, \sqrt{3})$, $E = L(a = \sqrt{1+i})$, and $\tau : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{1+i} \mapsto -\sqrt{1+i}$. Among our example algebras, $\mathcal{IA}$ has the densest maximal order. In Section V-D we will show that its maximal order is also the densest in general, when $F = \mathbf{Q}(i)$ and $m = n_r = 2$.

Let us now describe the code explicitly. If we order the $\mathbf{Z}$-basis of the natural order of $\mathcal{IA}$ as

$$\{e_i\}_{1\leq i\leq 16} = \{1, u, i, \gamma, a, ui, u\gamma, ua, i\gamma, ia, a\gamma, ui\gamma, uia, ua\gamma, ia\gamma, uia\gamma\},$$

then (according to the MAGMA software [31]) the maximal order $\Lambda_{\mathrm{MAX}} \subseteq \mathcal{IA}$ has a $\mathbf{Z}$-basis

$$\left\{ \begin{array}{l} \frac{1}{2}(e_1 + e_2 + e_3 + e_6), \\ \frac{1}{2}(e_2 + e_6 + e_9 + e_{12} + e_{14} + e_{16}) \\ \frac{1}{2}(e_3 + e_6 + e_7 + e_9 + e_{14} + e_{15}) \\ \frac{1}{2}(e_4 + e_6 + e_7 + e_9 + e_{12}) \\ \frac{1}{2}(e_5 + e_8 + e_{10} + e_{13}),\ e_6,\ e_7 \\ \frac{1}{2}(e_8 + e_{13} + e_{15} + e_{16}),\ e_9 \\ \frac{1}{2}(e_{10} + e_{13} + e_{14} + e_{15}), \\ \frac{1}{2}(e_{11} + e_{14} + e_{15} + e_{16}) \\ e_{12},\ e_{13},\ e_{14},\ e_{15},\ e_{16} \end{array} \right\}.$$

Now the codebook $\mathcal{C} \subseteq \Lambda_{\mathrm{MAX}}$ of an arbitrary size can be produced as

$$\mathcal{C} \subseteq \{M \in \Lambda_{\mathrm{MAX}} \,|\, \|M\| \leq E\}$$

where $\|\cdot\|$ denotes the Frobenius norm (corresponds to the squared Euclidean norm of the vectorized matrix, i.e., the sum of the squares of all the matrix elements), and E is some desired energy limit.

4) Algebra $\mathcal{QA}$—An Improved Natural Order: Let us use the multiblock notation for a change. Here we consider another tower of number fields $F \subset L \subset E$, where $E = \mathbf{Q}(\zeta_5, i)$, $F = \mathbf{Q}(i)$, and where $L = \mathbf{Q}(\theta, i)$ with $\theta = \zeta_5 + \zeta_5^{-1}$. Clearly, we have $\mathrm{Gal}(E/F) = \langle\tau\rangle$, $\tau(\zeta_5) = \zeta_5^2$, and $\tau(\theta) = \theta^2 - 2$. Thus we obtain the CDA $\mathcal{QA} = (E/L, \sigma = \tau^2, \gamma) = E \oplus uE$, and $\gamma = u^2 = i$ is a non-norm element. Embedding the algebra $\mathcal{QA}$ as in Proposition 5.1 yields the following multiblock ST code with coding over 2 consecutive fading blocks:

$$\mathcal{QA}_1 \subseteq \{(B\ \tau(B)) \,|\, x_i \in \mathcal{O}_E\}$$

where

$$B = \begin{pmatrix} x_0 & i\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}$$

and

$$\tau(B) = \begin{pmatrix} \tau(x_0) & i\tau(\sigma(x_1)) \\ \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix}.$$

The elements x_k in the above are of the form $x_k = \sum_{j=0}^{3} a_{k,j}\zeta_5^j$, where $a_{k,j} \in \mathbf{Z}[i]$, hence the above code transmits on the average, two independent QAM symbols per channel use.

Among our example algebras, $\mathcal{QA}$ has the densest natural order.

Example 5.1: Let us calculate the normalized minimum determinant of the algebra $\mathcal{IA}$ as an example (cf. Section I, Definitions 3.4, 3.5, and Propositions 5.1,5.3). The other algebras can be treated likewise. In Table I we have listed the normalized minimum determinants δ and densities ρ of the natural and maximal orders of the algebras $\mathcal{PA}, \mathcal{CA}, \mathcal{IA}$, and $\mathcal{QA}$. Note that for $\mathcal{QA}$ these two actually coincide. We can conclude that among the natural orders, that of the algebra $\mathcal{QA}$ has the largest normalized minimum determinant, i.e., the highest density. The

TABLE I
NORMALIZED MINIMUM DETERMINANT δ AND NORMALIZED DENSITY $\rho = 1/m(\Lambda)$ OF NATURAL AND MAXIMAL ORDERS OF DIFFERENT ALGEBRAS

	$\mathcal{QA}$	$\mathcal{CA}$	$\mathcal{IA}$	$\mathcal{PA}$
	$\mathbf{\Lambda_{NAT}}$	Λ_{NAT}	Λ_{NAT}	Λ_{NAT}
δ	$\mathbf{0.0894}$	0.0361	0.0340	0.0298
ρ	$5^{-6} = 6.4 \cdot 10^{-5}$	$2^{-16} \cdot 3^{-2} = 1.7 \cdot 10^{-6}$	$2^{-10} \cdot 3^{-6} = 1.4 \cdot 10^{-6}$	$3^{-4} \cdot 5^{-6} = 7.9 \cdot 10^{-7}$
	$\mathcal{IA}$	$\mathcal{CA}$	$\mathcal{QA}$	$\mathcal{PA}$
	$\mathbf{\Lambda_{MAX}}$	Λ_{MAX}	Λ_{MAX}	Λ_{MAX}
δ	$\mathbf{0.1361}$	0.1214	0.0894	0.0894
ρ	$\mathbf{2^{-2} \cdot 3^{-6} = 3.4 \cdot 10^{-4}}$	$2^{-9} \cdot 3^{-2} = 2.2 \cdot 10^{-4}$	$5^{-6} = 6.4 \cdot 10^{-5}$	$5^{-6} = 6.4 \cdot 10^{-5}$

algebra $\mathcal{IA}$, for its part, has the densest maximal order. The corresponding numbers are shown **bold** in Table I.

For the natural order of $\mathcal{IA}$ we have $\det_{\min}(\mathcal{C}(\Lambda_{\rm NAT})) = 1$ and $\rho^{-1} = m(\mathcal{C}(\Lambda_{\rm NAT})) = 2^{10} \cdot 3^6$, hence $t = 2^{-5/8} \cdot 3^{-3/8}$. Now $m(t\mathcal{C}(\Lambda_{\rm NAT})) = 1$ and the normalized minimum determinant is $\delta = \det_{\min}(t\mathcal{C}(\Lambda_{\rm NAT})) = 2^{-5/2} \cdot 3^{-3/2} \cdot 1 \approx 0.0340$. The maximal order of $\mathcal{IA}$ has $\det_{\min}(\mathcal{C}(\Lambda_{\rm MAX})) = 1$ and $m(\mathcal{C}(\Lambda_{\rm MAX})) = 2^2 \cdot 3^6$, thus $t = 2^{-1/8} \cdot 3^{-3/8}$ and $\delta = \det_{\min}(t\mathcal{C}(\Lambda_{\rm MAX})) = \frac{1}{3\sqrt{2}\sqrt{3}} \approx 0.1361$.

D. An Explicit Density Upper Bound for the Lattices $\mathcal{C}(\Lambda)$ With $F = \mathbf{Q}(i)$ and $n_t = 4$

As shown in Example 5.1, for the maximal order Λ of $\mathcal{IA}$ we have

$$\begin{aligned} m(\mathcal{C}(\Lambda)) &= d(\mathcal{O}_L/\mathcal{O}_F)^{\dim_L \mathcal{IA}} N_{L/F}(d(\Lambda/\mathcal{O}_L)) \\ &= d(\mathcal{O}_L/\mathcal{O}_F)^4 N_{L/F}\left(P_1^2 P_2^2\right) \\ &= 3^4 \cdot 2^2 \cdot 3^2 = 2916 \end{aligned}$$

where P_1 and P_2 are the norm wise smallest ideals of $\mathcal{O}_L$. In what follows, we will show that when $F = \mathbf{Q}(i)$ and $m = n_r = 2$ we cannot go below this, i.e., the maximal order of $\mathcal{IA}$ has optimal density.

Let us now assume that we would have such an extension $L/\mathbf{Q}(i)$ that the corresponding lattice would have $m(\Lambda) < 2916$. If the prime $1+i$ splits, this would mean that $d(\mathcal{O}_L/\mathbf{Z}[i]) < \sqrt{27} \approx 5.196$. If $1+i$ does not split, then the discriminant should be even smaller so this is a sufficient upper bound for $d(\mathcal{O}_L/\mathbf{Z}[i])$.

Let $\alpha \in \mathcal{O}_L$ such that $\{1, \alpha\}$ is an integral basis for $L/\mathbf{Q}(i)$. Now this degree two extension has a minimal polynomial of the form $f_\alpha(x) = x^2 + bx + c$, where $b, c \in \mathbf{Z}[i]$, and the discriminant

$$d(\mathcal{O}_L/\mathcal{O}_F) = b^2 - 4c \in \mathbf{Z}[i].$$

Note that a minimal polynomial of the form $x^2 + c$ is out of the question, as then $|d(\mathcal{O}_L/\mathcal{O}_F)| = 4|c| \geq 4\sqrt{2} > 5.196$. Furthermore, $d(\mathcal{O}_L/\mathcal{O}_F)$ cannot be a square, as then it would trivially follow that $\alpha \in \mathbf{Q}(i)$ and $L = \mathbf{Q}(i)$. Now we are left with the choices $d(\mathcal{O}_L/\mathcal{O}_F) \in \{1+i, (1+i)^3, 2+i, (1+i)(2+i), (1+i)^2(2+i), 3(1+i), 3, 2+3i, (1+i)(2+3i), 4+i\}$ or the obvious translates with the same absolute value.

Let us treat in detail the cases $d(\mathcal{O}_L/\mathcal{O}_F) = (1+i)^j$, $j = 1, 3$ to set an example. As the prime $1+i$ ramifies in this extension, we know that the smallest ideal is $P_1 \in \mathcal{O}_L$ above $1+i$ and $N(P_1) = 1+i$. The second ideal P_2 would depend on the behavior of the primes $2+i$ and 3. However, as $d(\mathcal{O}_L/\mathcal{O}_F) = b^2 - 4c = (r+si)^2 - 4(t+ui) = (r^2 - s^2 - 4t) + (2rs - 4u)i = (1+i)^j$, $r, s, t, u \in \mathbf{Z}$, it immediately follows that neither of $j = 1, 3$ fit into the equation.

The other cases are equally straightforward. In the case $d(\mathcal{O}_L/\mathcal{O}_F) = \pm 3$ we note that we end up into an isomorphic extension $L/\mathbf{Q}(i) \simeq \mathbf{Q}(\zeta_{12}) \simeq \mathbf{Q}(i, \sqrt{3})/\mathbf{Q}(i)$ that we already have. For $d(\mathcal{O}_L/\mathcal{O}_F) = 1 + 4i$ it would require that $1+i$ splits which is not the case.

We have now proved the following proposition. For the notation, cf. Proposition 5.1.

Proposition 5.10 (Density Bound for $n_t = 4$, $F = \mathbf{Q}(i)$): Let $m = n_r = 2$, i.e., $n_t = 4$. For the density of the lattice $\mathcal{C}(\Lambda)$ it holds that

$$\rho = 1/m(\mathcal{C}(\Lambda)) \leq \frac{1}{2^2 \cdot 3^6} \approx 0.00034. \tag{14}$$

The lower bound is achieved, e.g., by the maximal order of the algebra $\mathcal{IA}$, see Table I. □

VI. CONSTRUCTING AST LATTICES BY THE SMART PUNCTURING METHOD (SPM)

Another way to construct AST lattices would be as follows (cf. [24]). Let $\mathcal{A} = (E/F, \tau, \gamma)$ be an index n_t division algebra and $[E : L] = m$, $[L : F] = n_r$. If in the standard matrix representation the elements x_i are restricted to belong to L (rather than to E), we obtain another division algebra $\mathcal{A}'$. Obviously also the algebra $\mathcal{A}'$ is a division algebra as it is contained in $\mathcal{A}$. This construction also yields rate n_r codes for $n_t\mathrm{Tx} + n_r\mathrm{Rx}$ antennas with a nonvanishing determinant. As L is fixed by $\sigma = \tau^{n_r}$ we have

$$\begin{aligned} l u^{n_r} &= u\tau(l)u^{n_r - 1} = \cdots = u^{n_r}\tau^{n_r}(l) \\ &= u^{n_r}\sigma(l) = u^{n_r} l \end{aligned}$$

for all $l \in L$. Thus, the center F of $\mathcal{A}$ is extended by the element u^{n_r}.

Proposition 6.1: Let $\mathcal{O}_L$ be the ring of algebraic integers of L and $F = \mathbf{Q}(i)$. The lattice

$$\mathcal{C}_2 = \left\{ \begin{pmatrix} x_0 & \gamma\tau(x_3) & \cdots & \gamma\tau^{n_t-1}(x_1) \\ x_1 & \tau(x_0) & \cdots & \gamma\tau^{n_t-1}(x_2) \\ \vdots & & & \vdots \\ x_{n_t-1} & \tau(x_{n_t-2}) & \cdots & \tau^{n_t-1}(x_0) \end{pmatrix} \right\}$$

$x_i \in \mathcal{O}_L$ has a non-vanishing determinant $\det(\mathcal{C}_2) \in \mathbf{Z}[i]$. Thus, the minimum determinant is equal to one.

Proof: This immediately follows from the way of construction. □

As we consider the construction of Proposition 6.1 only for natural orders, we denote it by $\mathcal{C}_2$ as opposed to the notation $\mathcal{C}_1(\Lambda)$ where we needed to specify the order in use. The above

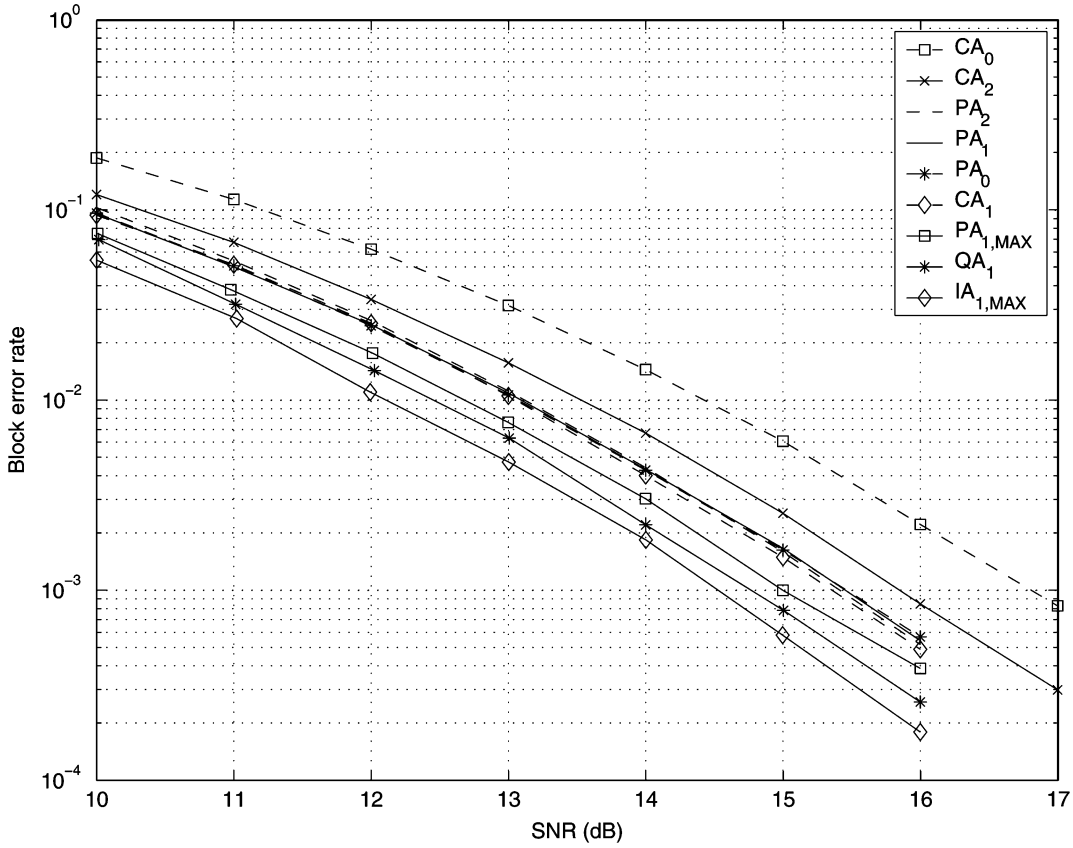

Fig. 1. Block error rates at 4 bpcu.

subfield construction method [24] can be generalized so that it applies to any number of receiving antennas $\#\mathrm{Rx} < \#\mathrm{Tx}$. The idea is that instead of restricting the elements x_i to belong to a subfield, we can puncture at *any* level. By this we mean that we can set an arbitrary number of the QAM/HEX coefficients equal to zero. More formally, let us denote

$$x_j = \sum_{k=0}^{n_t-1} a_{k,j} e_j \in \mathcal{O}_E \quad (j = 0, \ldots, n_t - 1)$$

where $a_{k,j} \in \mathbf{Z}[\delta]$ and $e_0, \ldots, e_{n_t-1}$ is an integral basis of E/F. If we wish to use n_r receiving antennas, we set any $n_t - n_r$ of the coefficients $a_{k,j}$ to zero for each x_j. Nevertheless, to enable efficient decoding one should choose the same set of indices k at where to puncture for each x_j. We call this the *Smart Puncturing Method* (SPM).

For instance, one option is to define $a_{k,j} = 0$ for $n_r \leq k \leq n_t - 1$, that is

$$x_j = \sum_{k=0}^{n_r-1} a_{k,j} e_j$$

for $j = 0, \ldots, n_t - 1$.

A. Explicit Codes Using SPM

Let us now use the SPM for constructing AST codes. To simplify the notation, we use the subfield construction as a special case of SPM. To set an example, we write down the constructions for the algebras $\mathcal{PA}$ and $\mathcal{CA}$, the other algebras can be treated similarly.

1) Algebra $\mathcal{PA}$: By using the algebra $\mathcal{PA}$ (cf. Section V-C1) and the subfield Construction 6.1, we get

$$\mathcal{PA}_2 \subseteq \left\{ \begin{pmatrix} x_0 & i\tau(x_3) & ix_2 & i\tau(x_1) \\ x_1 & \tau(x_0) & ix_3 & i\tau(x_2) \\ x_2 & \tau(x_1) & x_0 & i\tau(x_3) \\ x_3 & \tau(x_2) & x_1 & \tau(x_0) \end{pmatrix} \middle| \; x_i \in \mathcal{O}_L \right\}.$$

Each of the elements x_k is of the form $x_k = a_{k,0} + a_{k,1}\pi$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code rate is again equal to two.

2) Algebra $\mathcal{CA}$: Let us then construct a code using $\mathcal{CA}$ (cf. Section V-C2) and 6.1. This time we have

$$\mathcal{CA}_2 \subseteq \left\{ \begin{pmatrix} x_0 & \gamma\tau(x_3) & \gamma x_2 & \gamma\tau(x_1) \\ x_1 & \tau(x_0) & \gamma x_3 & \gamma\tau(x_2) \\ x_2 & \tau(x_1) & x_0 & \gamma\tau(x_3) \\ x_3 & \tau(x_2) & x_1 & \tau(x_0) \end{pmatrix} \middle| \; x_i \in \mathcal{O}_L \right\}$$

with $\gamma = 2 + i$.

Each of the elements x_k is of the form $a_{k,0} + a_{k,1}s$, where $a_{k,j} \in \mathbf{Z}[i]$. Thus, the code rate equals two.

Again we could also use a unit non-norm element $\gamma = \frac{2+i}{2-i}$.

VII. Simulation Results

In Fig. 1, the different construction methods are denoted by subscripts: $0 =$ Trivial Puncturing Method, $1 =$ Block Diagonal Method (cf. Section V\-C), and $2 =$ Subfield Construction Method (cf. Section VI-A).

The use of a maximal order instead of the natural order will be indicated by 'MAX', e.g., we write $\mathcal{IA}_{1,\mathrm{MAX}}$ for the code

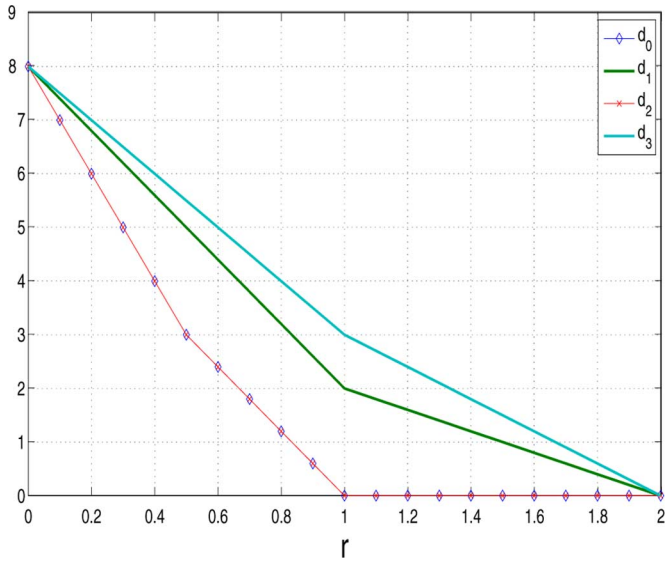

Fig. 2. DMT for $n_t = 4$, $n_r = 2$, and $m = 2$.

designed using the BDM and a maximal order of the algebra $\mathcal{IA}$.

First of all, we have to admit that we have not carried out optimization as much as would have been possible. For example, the use of ideals has not been taken advantage of, except in the case of the punctured Perfect code $\mathcal{PA}_0$ and the code $\mathcal{PA}_1$, for which we used the ideal given in Section V-C1. Still, the simulation results are indeed very satisfactory.

The codes $\mathcal{CA}_1$, $\mathcal{PA}_2$, $\mathcal{PA}_1$, and $\mathcal{PA}_0$ perform more or less equally. The code $\mathcal{CA}_2$ is beaten by these by 0.2–0.7 dB, depending on the SNR. Next comes $\mathcal{CA}_0(x_1 = x_3 = 0)$, losing still by 0.7–1 dB to $\mathcal{CA}_2$. Despite of its lower density, the code $\mathcal{PA}_1$ performs equally well as the code $\mathcal{CA}_1$, possibly because of the careful optimization of $\mathcal{PA}_1$ carried out in [10] such that it falls into the category of *information lossless* (IL) codes (see [40] for the definition) and has a good (orthogonal) lattice *shaping*. Probably for the same reason, it appears to be irrelevant to which construction method is used for $\mathcal{PA}$, whereas the same is not true at all for the other algebras. Thus, the simulation results of the $\mathcal{PA}$ codes suggest that having a good shaping is also important at low SNR regime and it is better that the code has this property.

Do note that information losslessness is a property defined for linear dispersion (LD) codes and as such does not concern the maximal order codes (they are not linear dispersion codes when optimally used). Orthogonal shaping, for its part, has many other justifications than that of yielding information lossless codes. As mentioned earlier, orthogonal (or hexagonal) shaping enables simple bit labeling and usually makes the decoding less complex. Hence, in addition to density (maximization of the normalized minimum determinant), it is preferable to have orthogonal or nearly orthogonal shaping. In our simulations we did not do lattice reduction or use any other methods to simplify the decoding, as we feel that these concepts should be treated in a paper of their own.

To summarize the above, by orthogonal shaping one can compensate somewhat the lower density. That is, if we have two equally dense codes, then one might prefer the one that is closer to being orthogonal. But do note that by using orthogonal codes only, one cannot achieve the excellent performance provided by the maximal order codes as is clearly shown by the simulations. Also the data rate used in Fig. 1 is very much in favor of $\mathcal{PA}$ as its shape fits perfectly with the constellation. At a different data rate (e.g., at 5 bpcu), however, the performance of $\mathcal{PA}$ can be expected to get worse as compared to the maximal order codes as then the orthogonal shape does not help that much and the density has more impact. Similar phenomenon was experienced when comparing the Golden code with the Golden+ code [17]: At the rate 4 bpcu that is ideal for the Golden code it could not be beaten, but immediately when taking a bigger data rate the difference became clear and the denser Golden+ code was shown to outperform the Golden code.

The code $\mathcal{IA}_{1,\mathrm{MAX}}$ obtained by combining BDM with the use of a maximal order (cf. Section V-C3 and [22]) triumphs over all the other codes. It outperforms the next best code $\mathcal{QA}_1$ by approximately 0.3 dB and $\mathcal{PA}_{1,\mathrm{MAX}}$ by 0.5 dB. In [25] the authors show that the DjABBA code wins the punctured Perfect code by 0.5 dB or less in the BER performance at the rate 4 bpcu. The same holds for the BLER performance and thus our code improves even upon the DjABBA code. Also the Icosian code for $4\mathrm{Tx}+2\mathrm{Rx}$ antennas exploiting the Icosian ring (which also happens to be a maximal order) loses to $\mathcal{IA}_{1,\mathrm{MAX}}$ by 0.7–1 dB. The curves depicting the DjABBA code, the Icosian code and the perfect version of $\mathcal{CA}_1$ are not shown in the picture in order to keep it readable. The perfect version of the code $\mathcal{CA}_{1,\mathrm{PERF}}$ performs almost equally to $\mathcal{PA}_{1,\mathrm{MAX}}$ being just slightly better.

Remark 7.1: There are some practical problems related to maximal order codes in general. Using maximal orders or more generally highly skewed lattices can make the bit labeling less obvious and the decoding process more complex even when the same decoding procedure is used. E.g., comparing the number of points in the search tree visited by a sphere decoder shows that usually a skewed lattice causes more visits than an orthogonal one. So these are purely properties the system designer can choose to use or not to use, depending on the situation. Nevertheless, the decoding complexity can be significantly reduced by using sphere encoding together with some suboptimal decoding techniques getting very close to the maximal-likelihood (ML) performance, see [42] for the promising results.

Here, a suitably modified (more details will follow in a forthcoming paper, see [35]) sphere decoder was used for decoding the lattices. Briefly, the sphere decoder performs an additional energy check, checking that the decoded codeword is valid and within the desired energy sphere. This step is required because of the spherical shape used for the constellation. The codebook can be formed beforehand, so it has to be carried out only once. Alternatively, maintaining a codebook can be overcome by using sphere encoding as mentioned above. The maximal order codes can be also used as linear dispersion codes, but then the full advantage of the density of maximal orders is not achieved. If used as LD codes, no additional steps are needed for decoding.

The DMT analysis (Section III) tells us that asymptotically BDM should outperform the other constructions methods, but

we want to emphasize that, as suggested by Fig. 1, at the low SNR this is not necessarily the case. Indeed it seems that at the low SNRs, the best construction method depends on the very algebra (and especially on its density) that is in use. Fig. 1 also shows that the trivial puncturing method used by other authors [25] is not always the first choice (as again implied by the DMT analysis too, see Section III), hence proving the point of new construction methods. Actually, for the algebra $\mathcal{CA}$ puncturing actually yields the worst performance.

VIII. Diversity–Multiplexing Tradeoff Analyses

Diversity–multiplexing tradeoff (DMT) analyses of several constructions of asymmetric space–time codes will be given in this section. We try to make this section self contained. In a MIMO communication system with n_t transmit and n_r receive antennas, under the quasi-static MIMO Rayleigh block fading channel model, it is known that the ergodic MIMO channel capacity C equals [39]

$$C = \min\{n_t, n_r\}\log_2 \mathsf{SNR} + O(1) \text{ bits/channel use} \quad (15)$$

at high SNR regime.

Let R denote that data rate of a space–time code $\mathcal{X}$ defined in Definition 1.1, and let r denote the *normalized rate* of $\mathcal{X}$, also known as the *multiplexing gain* [19], given by

$$r := \frac{R}{\log_2 \mathsf{SNR}}. \quad (16)$$

From (15) it can be seen that the maximum achievable multiplexing gain equals $\min\{n_t, n_r\}$. Given the code $\mathcal{X}$ with multiplexing gain r, we say $\mathcal{X}$ achieves *diversity gain* $d(r)$ if at high SNR regime, the codeword error probability of $\mathcal{X}$ is on the order of

$$P_e(r) \doteq \mathsf{SNR}^{-d(r)}. \quad (17)$$

By $\doteq$ we mean the exponential equality [19], i.e., we say the function $f(\mathsf{SNR}) \doteq \mathsf{SNR}^b$ if and only if

$$\lim_{\mathsf{SNR}\to\infty} \frac{\log f(\mathsf{SNR})}{\log \mathsf{SNR}} = b. \quad (18)$$

The notations of $\dot{\geq}$ and $\dot{\leq}$ are defined similarly.

Zheng and Tse [19] showed that there exists a fundamental tradeoff between the multiplexing and the diversity gains, referred to as the *diversity–multiplexing tradeoff* (DMT). For the cases when $T \geq n_t + n_r - 1$ and when the code $\mathcal{X}$ spans over m independent block fading channels, the DMT asserts that the maximum possible diversity gain $d^*(r)$ for any space–time coding scheme with multiplexing gain r is a piecewise linear function connecting the points $(k, d^*(k))$, $k = 0, 1, \ldots, \min\{n_t, n_r\}$, and

$$d^*(k) = m(n_t - k)(n_r - k). \quad (19)$$

Furthermore, it has been shown in [20] using explicit constructions that the tradeoff (19) holds whenever $T \geq n_t$. On the other hand, if $T < n_t$, only upper and lower bounds on $d^*(r)$ are available in [19].

A. DMT for the Trivial Puncturing Construction

Let $\mathfrak{D}_0$ denote the cyclic division algebra $(E/F, \sigma, \gamma)$ where $[E:F] = n_t$ and E/F is cyclic Galois. Let $F = \mathbf{Q}(i)$ and let $\mathcal{D}_0$ be the corresponding $(n_t \times n_t)$ cyclic algebra

$$\mathcal{D}_0 = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_t-1}) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma(x_{n_t-2}) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\}$$

where $x_i \in E$. The puncturing construction $\mathcal{X}_0$ is thus obtained by setting $x_{n_r} = \cdots = x_{n_t-1} = 0$ in $\mathcal{D}_0$ and by restricting the elements $x_0, \ldots, x_{n_r-1}$ to be of form

$$x_i = \sum_{j=0}^{n_t-1} a_{i,j} e_i, \qquad a_{i,j} \in \mathcal{A}_0,\ i = 0, \ldots, n_r - 1$$

where $\mathcal{A}_0 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \ldots, e_{n_t-1}\}$ is an integral basis for E/F.

Remark 8.1: If $|\gamma| = 1$, it does not matter which ones of the coefficients x_i we set equal to zero. However, if $|\gamma| > 1$, then we should choose the indices for which $x_i = 0$ in such a way that the overall energy is minimized. It can be easily verified that the above puncturing method, i.e., $x_{n_r} = \cdots = x_{n_t-1} = 0$, is the most efficient in energy.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_0| = |\mathcal{A}_0|^{n_t n_r} \doteq \mathsf{SNR}^{n_t r} \quad (20)$$

hence

$$|\mathcal{A}_0| = \mathsf{SNR}^{\frac{r}{n_r}}. \quad (21)$$

Given the transmitted code matrix $X_0 \in \mathcal{X}_0$, the received signal matrix Y_0 at the receiver end is

$$Y_0 = \theta_0 H X_0 + W \quad (22)$$

where we set

$$\theta_0^2 = \mathsf{SNR}^{1-\frac{r}{n_r}} \quad (23)$$

to ensure the power constraint $\frac{1}{n_t}\mathbb{E}\|X_0\|^2 \leq \mathsf{SNR}$. Let $\lambda_1 \leq \cdots \lambda_{n_r}$ be the ordered eigenvalues of $HH^\dagger$, and for any $X_0 \neq X_0' \in \mathcal{X}_0$, let $\delta_1 \geq \cdots \geq \delta_{n_t}$ be the ordered eigenvalues of $\Delta X_0 \Delta X_0^\dagger$, where $\Delta X_0 = X_0 - X_0'$. Then given H, the squared Euclidean distance between $\theta_0 H X_0$ and $\theta_0 H X_0'$ is

$$\begin{aligned} d_E^2(X_0, X_0') &:= \theta_0^2 \|H\Delta X_0\|^2 \geq \theta_0^2 \sum_{i=1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\geq \theta_0^2 \sum_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\dot{\geq} \theta_0^2 \left(\prod_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \right)^{\frac{1}{k}} \end{aligned}$$

for $k = 1, 2, \ldots, n_r$. In particular

$$\begin{aligned} \prod_{i=n_r-k+1}^{n_r} \delta_{n_t-n_r+i} &\geq \frac{1}{\prod_{i=1}^{n_t-k}\delta_i} \dot{\geq} \|\Delta X_0\|^{-2(n_t-k)} \\ &\doteq \mathsf{SNR}^{-\frac{r(n_t-k)}{n_r}}. \end{aligned}$$

Combining the two results above and setting $\alpha_i = -\log_{\mathrm{SNR}} \lambda_i$ we have $d_E^2(X_0, X_0') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$E_k = 1 - \frac{r}{n_r} - \frac{1}{k} \sum_{i=n_r-k+1}^{n_r} \alpha_i - \frac{r(n_t-k)}{kn_r} = \frac{1}{k}\left[\sum_{i=n_r-k+1}^{n_r} (1-\alpha_i) - mr\right].$$

Now we see the DMT for the puncturing construction is lower bounded by

$$d_0(r) \geq \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_r} (2i - 1 + n_r(m-1))\alpha_i \qquad (24)$$

and the right-hand side is given by the lines connecting the points $(n_t - mr)(n_r - mr)$ for integral values of mr.

B. DMT for the Block Diagonal Construction

Let E/F be cyclic Galois with $[E:F] = n_t$, $\mathrm{Gal}(E/F) = \langle \tau \rangle$ and $F = \mathbf{Q}(i)$. Let $L \subset E$ be such that $[E:L] = n_r$ and $[L:F] = m$ with $\mathrm{Gal}(E/L) = \langle \sigma \rangle$ where $\sigma = \tau^m$. It should be noted that we have assumed $n_t = mn_r$. Let $\mathfrak{D}_1$ be the cyclic division algebra $(E/L, \sigma, \gamma)$ and let $\mathcal{D}_1$ be the corresponding $(n_r \times n_r)$ algebra

$$\mathcal{D}_1 = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_r-1}) & \cdots & \gamma\sigma^{n_r-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_r-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_r-1} & \sigma(x_{n_r-2}) & \cdots & \sigma^{n_r-1}(x_0) \end{pmatrix} \right\}$$

$x_i \in E$. The block diagonal construction $\mathcal{X}_1$ is

$$\mathcal{X}_1 = \{\mathrm{diag}(X_1, \tau(X_1), \ldots, \tau^{m-1}(X_1))\}, \qquad (25)$$

where $X_1 \in \mathcal{D}_1$ with $x_i = \sum_{j=0}^{n_t-1} a_{i,j} e_i, a_{i,j} \in \mathcal{A}_1$. $\mathcal{A}_1 \subset \mathbf{Z}[i]$ denotes the underlying base-alphabet and $\{e_0, \ldots, e_{n_t-1}\}$ is an integral basis for E/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_1| = |\mathcal{A}_1|^{n_t n_r} \doteq \mathsf{SNR}^{n_t r} \qquad (26)$$

hence

$$|\mathcal{A}_1| = \mathsf{SNR}^{\frac{r}{n_r}}. \qquad (27)$$

Given the transmitted code matrix

$$\mathrm{diag}(X, \tau(X), \ldots, \tau^{m-1}(X)) \in \mathcal{X}_1$$

the received signal matrix Y_1 at the receiver end is

$$Y = \theta_1 H \mathrm{diag}(X, \tau(X), \ldots, \tau^{m-1}(X)) + W \qquad (28)$$

where we set

$$\theta_1^2 = \mathsf{SNR}^{1-\frac{r}{n_r}} \qquad (29)$$

to ensure the power constraint. On the other hand, we may partition the matrices Y, H, and W into

$$Y = [Y_0 Y_1 \cdots Y_{m-1}], H = [H_0 H_1 \cdots H_{m-1}]$$
$$W = [W_0 W_1 \cdots W_{m-1}]$$

and rewrite (28) as

$$Y_i = \theta_1 H_i \tau^i(X) + W_i$$

for $i = 0, 1, \ldots, m-1$. Let

$$\lambda_{i,1} \leq \cdots \leq \lambda_{i,n_r}$$

be the ordered eigenvalues of $H_i H_i^\dagger$, and for any

$$\mathrm{diag}(X, \tau(X), \ldots, \tau^{m-1}(X)) \neq \mathrm{diag}(X', \tau(X'), \ldots, \tau^{m-1}(X')) \in \mathcal{X}_1$$

let

$$\delta_{i,1} \geq \cdots \geq \delta_{i,n_r}$$

be the ordered eigenvalues of $\Delta X_i \Delta X_i^\dagger$, where $\Delta X_i = \tau^i(X - X')$. We will reorder and reindex the set of eigenvalues $\{\lambda_{i,j}\}$ and $\{\delta_{i,j}\}$ such that $\lambda_1 \leq \lambda_2 \cdots \leq \lambda_{n_t}$ and $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_{n_t}$. Thus the squared Euclidean distance between the two noise-free received signal matrices can be lower bounded by

$$d_E^2(X, X') = \theta_1^2 \sum_{i=0}^{m-1} \|H_i \Delta X_i\|^2 \geq \theta_1^2 \sum_{i=1}^{n_t} \lambda_i \delta_i \geq \theta_1^2 \sum_{i=n_t-k+1}^{n_t} \lambda_i \delta_i \dot{\geq} \theta_1^2 \left(\prod_{i=n_t-k+1}^{n_t} \lambda_i \delta_i \right)^{\frac{1}{k}}.$$

Moreover

$$\prod_{i=n_t-k+1}^{n_t} \delta_i \geq \frac{1}{\prod_{i=1}^{n_t-k} \delta_i} \dot{\geq} \left(\sum_{i=0}^{m-1} \|\Delta X_i\|^2 \right)^{-(n_t-k)} \doteq \mathsf{SNR}^{-\frac{r(n_t-k)}{n_r}}.$$

Combining the two results above and setting $\alpha_i = -\log_{\mathrm{SNR}} \lambda_i$ we have $d_E^2(X, X') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$E_k = 1 - \frac{r}{n_r} - \frac{1}{k} \sum_{i=n_t-k+1}^{n_t} \alpha_i - \frac{r(n_t-k)}{kn_r} = \frac{1}{k}\left(\sum_{i=n_t-k+1}^{n_t} (1-\alpha_i) - rm \right).$$

Now we see the DMT for the block-diagonal construction is given by

$$d_1(r) = \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_t} (2i-1)\alpha_i \qquad (30)$$

and is obtained by the lines connecting the points $(n_t - mr)(n_r - r)$ for integral values of r.

C. DMT for the Subfield Construction

The DMT derived here for the subfield construction also holds for the more general codes designed using the smart puncturing method.

Let E/F be a cyclic Galois extension with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ and $[E:F] = n_t$, and $F = \mathbf{Q}(i)$. Let $\mathfrak{D}_2$ be the cyclic division algebra $(E/F, \sigma, \gamma)$ and let

$$\mathcal{D}_2 = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n_t-1}) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma(x_{n_t-2}) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\}$$

where $x_i \in L$, $L \subset E$ and $[L:F] = n_r$. The subfield construction $\mathcal{X}_2$ is thus obtained by restricting the elements $x_0, \ldots, x_{n_t-1}$ to be of form

$$x_i = \sum_{j=0}^{n_r-1} a_{i,j} e_i, \quad a_{i,j} \in \mathcal{A}_2, \quad i = 0, \ldots, n_t - 1$$

where $\mathcal{A}_2 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \ldots, e_{n_r-1}\}$ is an integral basis for L/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_2| = |\mathcal{A}_2|^{n_t n_r} \doteq \mathsf{SNR}^{n_t r} \tag{31}$$

hence

$$|\mathcal{A}_2| = \mathsf{SNR}^{\frac{r}{n_r}}. \tag{32}$$

Given the transmitted code matrix $X_2 \in \mathcal{X}_2$, the received signal matrix Y_2 at the receiver end is

$$Y_2 = \theta_2 H X_2 + W \tag{33}$$

where we set

$$\theta_2^2 = \mathsf{SNR}^{1-\frac{r}{n_r}} \tag{34}$$

to ensure the power constraint. Now we see the DMT for this construction has the same lower bound as that for the puncturing construction, hence

$$d_2(r) \geq \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_r} (2i - 1 + n_r(m-1))\alpha_i \tag{35}$$

and the right-hand-side is obtained by the lines connecting the points $(n_t - mr)(n_r - mr)$ for integral values of mr.

D. DMT for the Original CDA Construction

Let E/F be a cyclic Galois extension with $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ and $[E:F] = n_t$, and $F = \mathbf{Q}(i)$. Let $\mathfrak{D}_3$ be the cyclic division algebra $(E/F, \sigma, \gamma)$ and let

$$\mathcal{D}_3 = \left\{ \begin{pmatrix} x_0 & \gamma\sigma\left(x_{n_t-1}\right) & \cdots & \gamma\sigma^{n_t-1}(x_1) \\ x_1 & \sigma(x_0) & \cdots & \gamma\sigma^{n_t-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ x_{n_t-1} & \sigma\left(x_{n_t-2}\right) & \cdots & \sigma^{n_t-1}(x_0) \end{pmatrix} \right\}$$

$x_i \in E$. The original construction $\mathcal{X}_3$ (cf. e.g., [15]) is obtained by restricting the elements $x_0, \ldots, x_{n_t-1}$ to be of form

$$x_i = \sum_{j=0}^{n_t-1} a_{i,j} e_i, \quad a_{i,j} \in \mathcal{A}_3, \quad i = 0, \ldots, n_t - 1$$

where $\mathcal{A}_3 \subset \mathbf{Z}[i]$ is the underlying base-alphabet and where $\{e_0, \ldots, e_{n_t-1}\}$ is an integral basis for E/F.

To achieve multiplexing gain at value r, we require

$$|\mathcal{X}_3| = |\mathcal{A}_3|^{n_t n_t} \doteq \mathsf{SNR}^{n_t r} \tag{36}$$

hence

$$|\mathcal{A}_3| = \mathsf{SNR}^{\frac{r}{n_t}}. \tag{37}$$

Given the transmitted code matrix $X_3 \in \mathcal{X}_3$, the received signal matrix Y_3 at the receiver end is

$$Y_3 = \theta_3 H X_3 + W \tag{38}$$

where we set

$$\theta_3^2 = \mathsf{SNR}^{1-\frac{r}{n_t}} \tag{39}$$

to ensure the power constraint. Let $\lambda_1 \leq \cdots \lambda_{n_r}$ be the ordered eigenvalues of $HH^\dagger$, and for any $X_3 \neq X_3' \in \mathcal{X}_3$, let $\delta_1 \geq \cdots \geq \delta_{n_t}$ be the ordered eigenvalues of $\Delta X_3 \Delta X_3^\dagger$, where $\Delta X_3 = X_3 - X_3'$. Then given H, the squared Euclidean distance between $\theta_3 H X_3$ and $\theta_3 H X_3'$ is

$$\begin{aligned} d_E^2(X_0, X_0') := \theta_3^2 \|H \Delta X_3\|^2 &\geq \theta_3^2 \sum_{i=1}^{n_r} \lambda_i \delta_{n_t - n_r + i} \\ &\geq \theta_3^2 \sum_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \\ &\dot{\geq} \theta_3^2 \left(\prod_{i=n_r-k+1}^{n_r} \lambda_i \delta_{n_t-n_r+i} \right)^{\frac{1}{k}}. \end{aligned}$$

for $k = 1, 2, \ldots, n_r$. In particular,

$$\begin{aligned} \prod_{i=n_r-k+1}^{n_r} \delta_{n_t-n_r+i} &\geq \frac{1}{\prod_{i=1}^{n_t-k} \delta_i} \dot{\geq} \|\Delta X_0\|^{-2(n_t-k)} \\ &\doteq \mathsf{SNR}^{-\frac{r(n_t-k)}{n_t}}. \end{aligned}$$

Combining the two results above and setting $\alpha_i = -\log_{\mathrm{SNR}} \lambda_i$ we have $d_E^2(X_3, X_3') \dot{\geq} \mathsf{SNR}^{E_k}$ and

$$\begin{aligned} E_k &= 1 - \frac{r}{n_t} - \frac{1}{k} \sum_{i=n_r-k+1}^{n_r} \alpha_i - \frac{r(n_t-k)}{k n_t} \\ &= \frac{1}{k} \left[\sum_{i=n_r-k+1}^{n_r} (1 - \alpha_i) - r \right]. \end{aligned}$$

Now we see the DMT for the CDA construction is given by

$$d_3(r) = \inf_{\alpha_i : E_k < 0} \sum_{i=1}^{n_r} (2i - 1 + n_r(m-1))\alpha_i \tag{40}$$

and the right-hand side is obtained by the lines connecting the points $(n_t - r)(n_r - r)$ for integral values of r.

Remark 8.2: One might ponder why not use the original symmetric construction with a smaller constellation as it is DMT optimal. In principle, AST codes can indeed be designed just by using the standard CDA-based MIMO code with a smaller constellation. Nevertheless, this destroys the lattice structure and causes exponential complexity at the receiver.

IX. Concluding Remarks and Suggestions for Further Work

We have introduced new construction methods for asymmetric space–time codes based on cyclic division algebras and their orders. Part of the results were reviewed from [24] and [17]. One of the methods, the so-called smart puncturing method, is suitable for an arbitrary number of transmitting antennas and lesser receiving antennas.

The density bound from [17] was generalized to the block diagonal asymmetric case and made explicit for the $4\mathrm{Tx} + 2\mathrm{Rx}$ antenna case when building upon $\mathbf{Q}(i)$. Also a construction achieving this bound was provided. It was noted that in the more general case, the most reasonable way to derive density bounds is with the aid of Odlyzko bound as the computation of minimal discriminants is in general a hard problem.

We proved the connection between the block diagonal asymmetric and multiblock codes, hence showing that the density results hold as such in the multiblock case.

We have not yet exhausted the box of optimization tools on our code. For example, the codes can be pre- and postmultiplied by any complex matrix of determinant one without affecting neither its density nor its good minimum product distance. In particular, if we use nonunitary matrix multipliers, the geometry of the lattice will change. While we cannot always turn the lattice into a rectangular one in this manner, some energy savings and perhaps also shaping gains are available. The simulations were carried out by using a suitably modified sphere decoder (on which more details in a forthcoming paper [35]). It was shown that the newly proposed codes outperform in block error performance the punctured Perfect code, the DjABBA code as well as the Icosian code, all aimed at transmission with four transmitting and two receiving antennas.

Also extensive DMT analysis was provided, showing that amongst the previously and newly proposed methods, the BDM is the best way to construct asymmetric codes in this respect.

Acknowledgment

The authors would like to thank Professor P. Vijay Kumar (Indian Institute of Science, Bangalore, India) for bringing the perfect version of the code $\mathcal{CA}_1$ to our notice. They are also indebted to Dr. J. Lahtonen (University of Turku, Finland) for the helpful discussions during the revision process of this paper. Dr. R. Vehkalahti (University of Turku, Finland) is gratefully acknowledged for his help in Section V-C3.

References

[1] 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," in *Proc. IEEE Veh. Technol. Conf.*, 1996, pp. 136–140, Also. in *IEEE Trans. Commun.*, vol. 47, pp. 527–537, Apr. 1999.

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

[3] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden code: A 2×2 full-rate space-time code with non-vanishing determinant," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432–1436, Apr. 2005.

[4] S. M. Alamouti, "A simple transmit diversity technique for wireless communication," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 1451–1458, Oct. 1998.

[5] C. Hollanti and J. Lahtonen, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4493–4510, Oct. 2008.

[6] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, pp. 628–636, Mar. 2002.

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

[8] J.-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. ITW 2003*, Paris, France, Mar. 31–Apr. 4 2003.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Algebraic 3×3, 4×4 and 6×6 space-time codes with non-vanishing determinants," in *Proc. IEEE ISITA 2004*, Parma, Italy, Oct. 10–13, 2004.

[10] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, Sept. 2006.

[11] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space-time codes for any number of antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853–3868, Nov. 2007.

[12] T. Kiran and B. S. Rajan, "STBC-schemes with non-vanishing determinant for certain number of transmit antennas," *IEEE Trans. Inf. Theory*, vol. 51, pp. 2984–2992, Aug. 2005.

[13] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "STBCs using capacity achieving designs from crossed-product division algebras," in *Proc. IEEE ICC 2004*, Paris, France, June 20–24, 2004, pp. 827–831.

[14] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "Information-lossless STBCs from crossed-product algebras," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, Sep. 2006.

[15] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, Sep. 2006.

[16] H.-F. Lu, P. Elia, S. A. Pawar, K. R. Kumar, and P. V. Kumar, "Space-time codes meeting the diversity-multiplexing gain tradeoff with low signaling complexity," in *Proc. CISS 2005*, Baltimore, MD, Mar. 2005.

[17] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "On the densest MIMO lattices from cyclic division algebras," *IEEE Trans. Inf. Theory* [Online]. Available: http://arxiv.org/abs/cs.IT/0703052

[18] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1102–1135, Mar. 2005.

[19] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[20] H.-f. (F.) Lu, "Explicit constructions of multiblock space-time codes that achieve the diversity-multiplexing tradeoff," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.

[21] H. El Gamal and A. R. Hammons, Jr., "A new approach to layered space-time coding and signal processing," *IEEE Trans. Inf. Theory*, vol. 47, pp. 2321–2334, Sep. 2001.

[22] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal matrix lattices for MIMO codes from division algebras," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2006)*, Seattle, Jul. 2006, pp. 783–787.

[23] N. Jacobson, *Basic Algebra II*. San Francisco, CA: Freeman, 1980.

[24] C. Hollanti and K. Ranto, "Asymmetric space-time block codes for MIMO systems," in *Proc. IEEE ITW 2007*, Bergen, Norway, July 2007, pp. 101–105.

[25] A. Hottinen, Y. Hong, E. Viterbo, C. Mehlführer, and C. F. Mecklenbräuker, "A comparison of high rate algebraic and non-orthogonal STBCs," in *Proc. ITG/IEEE Workshop Smart Antennas WSA 2007*, Vienna, Austria, Feb. 2007.

[26] J. Lahtonen, "Dense MIMO matrix lattices and class field theoretic themes in their construction," in *Proc. IEEE ITW 2007*, Bergen, Norway, Jul. 2007, pp. 96–100.

[27] J. Liu and A. R. Calderbank, "The Icosian code and the E_8 lattice: A new 4×4 space-time code with non-vanishing determinant," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2006)*, Seattle, WA, Jul. 2006, pp. 1006–1010.
[28] A. A. Albert, *Structure of Algebras*. New York: American Mathematical Society, 1939.
[29] I. Reiner, *Maximal Orders*. New York: Academic, 1975.
[30] C. Hollanti and J. Lahtonen, "A new tool: Constructing STBCs from maximal orders in central simple algebras," in *Proc. IEEE ITW 2006*, Punta del Este, Mar. 13–17, 2006, pp. 322–326.
[31] [Online]. Available: http://magma.maths.usyd.edu.au/magma/html-help/text835.htm#8121 Web page
[32] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in semisimple algebras over Q," *Comput. Complex.*, vol. 3, pp. 245–261, 1993.
[33] L. Rónyai, "Algorithmic properties of maximal orders in simple algebras over Q," *Comput. Complex.*, vol. 2, pp. 225–243, 1992.
[34] L. Rónyai, "Computing the structure of finite algebras," *J. Symb. Comput.*, vol. 9, pp. 355–373, 1990.
[35] C. Hollanti and K. Ranto, "Maximal orders in space-time coding: Construction and decoding," in *Proc. 2008 Int. Symp. Inf. Theory Its Appl. (ISITA)*, New Zealand, Dec. 2008, to be published.
[36] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 647–663, Feb. 2007.
[37] H. Cohen, F. Diaz y Diaz, and M. Olivier, "A table of totally complex number fields of small discriminants," in *Proc. Third Int. Symp. Algorithmic Number Theory*, 1998, pp. 381–391.
[38] A. M. Odlyzko, "Lower bounds for discriminants in number fields II," *Tohoku Math. J.*, no. 29, pp. 209–216, 1977.
[39] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, Nov.–Dec. 1999.
[40] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753–760, Mar. 2002.
[41] H.-F. Lu and C. Hollanti, "Optimal diversity multiplexing tradeoff and code constructions of constrained asymmetric MIMO systems," *IEEE Trans. Inf. Theory*, May 2008, submitted for publication.
[42] K. R. Kumar and G. Caire, "Space-time codes from structured lattices," *IEEE Trans. Inf. Theory* Apr. 2008 [Online]. Available: http://www.citebase.org/abstract?id=oai:arXiv.org:0804.1811, submitted for publication

Camilla Hollanti received the M.S. degree in pure mathematics from the University of Turku, Finland, in 2003 and the Ph.D. degree in discrete mathematics from the University of Turku/Turku Centre for Computer Science in January 2009.

Since June 2004, she has been with the Department of Mathematics, University of Turku, Finland. In 2005, she visited the Department of Algebra at Charles' University, Prague, Czech Republic, for six months. Her research is in the area of applications of algebraic number theory and class field theory in lattice space–time coding.

Ms. Hollanti is a recipient of several grants from various foundations, including the Finnish Cultural Foundation research grant in 2007 and the Finnish Academy of Science research grant in 2008. She received the prize for the best presentation in the EWM 2007 conference of European Women in Mathematics that took place in Cambridge, U.K., in September 2007.

Hsiao-Feng (Francis) Lu (S'98–M'04) received the B.S. degree from Tatung University, Taipei, Taiwan, in 1993, and the M.S.E.E. and Ph.D. degrees from the University of Southern California (USC), Los Angeles, in 1999 and 2003, respectively, all in electrical engineering.

He was a Postdoctoral Research Fellow at University of Waterloo, ON, Canada, during 2003–2004. In February 2004, he joined the faculty of the Department of Communications Engineering, National Chung-Cheng University, Chiayi, Taiwan, and was promoted to Associate Professor in August 2007. Since August 2008, he has been with the Department of Communications Engineering, National Chiao Tung University, Hsinchu, Taiwan. His research is in the area of space–time codes, MIMO systems, error correcting codes, wireless communication, optical fiber communication, and multiuser detection.

Dr. Lu is a recipient of several research awards, including the 2006 IEEE Information Society Taipei Chapter and IEEE Communications Society Taipei/Tainan Chapter Best Paper Award for Young Scholars, the 2007 Wu Da You Memorial award from Taiwan National Science Council, the 2007 IEEE Communication Society Asia Pacific Outstanding Young Researchers Award, and the 2008 Academia Sinica Research Award for Junior Research Investigators.