Asymmetric Space-Time Block Codes for MIMO Systems

Camilla Hollanti
Lab. of Discrete Math. for Inf. Tech.
Turku Centre for Computer Science
Joukahaisenkatu 3-5 B, FIN-20520 Turku, Finland
Email: cajoho@utu.fi

Kalle Ranto
Department of Mathematics
FIN-20014 University of Turku, Finland
Email: kara@utu.fi

***Abstract*— In this paper, the need for the construction of asymmetric space-time block codes (ASTBCs) is discussed, mostly concentrating on the case of four transmitting and two receiving antennas for simplicity. Above the trivial puncturing method, i.e. switching off the extra layers in the symmetric multiple input-multiple output (MIMO) setting, a more sophisticated yet simple asymmetric construction method is proposed. This method can be converted to produce multi-block space-time codes that achieve the diversity-multiplexing (D-M) tradeoff. It is also shown that maximizing the density of the newly proposed codes is equivalent to minimizing the discriminant of a certain order. The use of the general method is then demonstrated by building explicit, sphere decodable codes using different cyclic division algebras (CDAs). We verify by computer simulations that the newly proposed method can compete with the puncturing method, and in some cases outperforms it. Our conquering construction exploiting maximal orders improves even upon the punctured perfect code and the DjABBA code.**

I. Background

In this work, we are interested in the coherent MIMO case where the receiver perfectly knows the channel coefficients. A *lattice* is a discrete finitely generated free abelian subgroup $\mathbf{L}$ 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 $G(\mathbf{L}) = \left(\Re tr(x_i x_j^H)\right)_{1 \leq i,j \leq t}$, where H indicates the complex conjugate transpose of a matrix, tr is the matrix trace (=sum of the diagonal elements), and $x_i,\ i = 1, ..., t$, form a $\mathbf{Z}$-basis of $\mathbf{L}$. The Gram matrix has a positive determinant equal to the squared measure of the fundamental parallelotope $m(\mathbf{L})^2$.

From the pairwise error probability point of view, the performance of a space-time code is dependent on *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 $X, X' \in \mathcal{C}$. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix $(X - X')(X - X')^H$. 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 when the spectral efficiency approaches infinity, the ST code is said to have the *nonvanishing determinant* (NVD) property [1]. For non-zero square matrices, being full-rank coincides with being invertible.

The very first STBC for two transmit antennas was the *Alamouti code* 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 proposed as STBCs at least in [2]-[7]. The most recent work has concentrated on adding multiplexing gain, i.e. MIMO applications, and/or combining it with a good minimum determinant. It has been shown in [5] that CDA-based square ST codes with the NVD property achieve the diversity-multiplexing (D-M) tradeoff introduced in [8]. This result also extends over multi-block space-time codes [9].

The codes proposed in this paper are not fully multiplexing nor full-rate[1] due to the modified application requirements. This follows from the fact that the number of Rx antennas will be strictly less than the number of Tx antennas. We call this situation *asymmetric* as opposed to the symmetric case of #Tx antennas = #Rx antennas. The construction method proposed in this paper can be converted to produce multi-block ST codes that do achieve the diversity-multiplexing tradeoff. We shall show that maximizing the density (i.e. finding the most efficient packing in the available signal space) of codes arising from this method is equivalent to minimizing the discriminant of a certain order.

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. A typical example is a cellular phone downlink with two receivers exploiting polarization. Due to the limited size of 3+G mobile phones and DVB-H (Digital Video Broadcasting-Handhelds) user equipment, only a very small number of antennas fits at the end user site. For this kind of an application, the minimum delay MIMO constructions arising from the theory of cyclic division algebras (see e.g. [3]) have to be modified. For simplicity, we will mostly concentrate on the 4Tx+2Rx 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 Gaussian numbers in

[1]Full-rate, or rate-optimal, means that the code rate equals the decoding delay. The code rate is defined as the ratio of the number of transmitted symbols to the decoding delay.

1-4244-1199-8/07/$25.00

four time slots, i.e. four in each time slot. Now, however, the reduced number of Rx antennas limits the transmission down to two Gaussian numbers per each time slot.

We have come up with two different types of solutions to this problem. Both solutions take advantage of cyclic division algebras and yield rate r codes with a nonvanishing determinant. Let us denote by $n = rm$ the number of transmitters in the usual symmetric CDA based MIMO system and suppose we want to construct a code for nTx+rRx antennas. One idea is to first pick an index r division algebra with a center that is $2m$-dimensional over $\mathbf{Q}$, form isomorphic copies of it and then use them as $r \times r$ diagonal blocks in an $n \times n$ code matrix. Another possibility is to take the symmetric $n \times n$ MIMO code, but choose the elements in the matrix from an intermediate field of degree $2r$ over $\mathbf{Q}$ instead of the maximal subfield. In this paper we will cover the first method. The other method will be treated in more detail in a forthcoming paper.

III. Cyclic division algebras and orders

The theory of cyclic algebras and their representations as matrices are thoroughly considered in [2] and [10]. We are only going to recapitulate the essential facts here. For a more detailed introduction on orders, see [11].

In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). The rings of algebraic integers are denoted by $\mathcal{O}_F$ and $\mathcal{O}_E$ respectively. Let E/F be a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$, where σ is the generator of the cyclic group. 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 it determines the number of transmitters), that is

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

with $u \in \mathcal{A}$ such that $eu = u\sigma(e)$ for all $e \in E$ and $u^n = \gamma \in F^*$. An element $x = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $A =$

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

Definition 3.1: An algebra $\mathcal{A}$ is called *simple* if it has no nontrivial ideals. A cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ is *central* if its center $Z(\mathcal{A}) = \{x \in \mathcal{A} \mid xx' = x'x \text{ for all } x' \in \mathcal{A}\} = F$.

All algebras considered here are finite dimensional associative central simple algebras over a field. From now on, we identify the element x of an algebra with its standard matrix representation defined above in (1).

Definition 3.2: The determinant of the matrix A is called the *reduced norm* of the element $x \in \mathcal{A}$ and is denoted by $nr(x)$.

Remark 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.

In the following we give a condition when an algebra is a division algebra, i.e. each of its non-zero elements has a multiplicative inverse. For the proof, see [10, Theorem 11.12, p. 184].

Proposition 3.1: An algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of index 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 in E^* is n.

Let R denote a Noetherian integral domain with a quotient field F, 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.

As usual, an R-order in $\mathcal{A}$ is said to be *maximal*, if it is not properly contained in any other R-order in $\mathcal{A}$.

The next proposition describes an order from where the elements are drawn in a typical CDA based MIMO space-time block code. For the proof, see [11, Theorem 10.1, p. 125]. Some optimization to this can be done e.g. with the aid of ideals as in [3].

Proposition 3.2: Let us define the $\mathcal{O}_F$ order

$$\Lambda_{\mathcal{A}} = \{x_0 + \cdots + u^{n-1}x_{n-1} \mid x_i \in \mathcal{O}_E\}$$

$\subseteq \mathcal{A} = (E/F, \sigma, \gamma)$. Later on this order will be referred to as the *natural order*. For any non-zero element $x \in \Lambda_{\mathcal{A}}$ its reduced norm $nr(x)$ 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 or a cyclotomic field, then the minimum determinant of the lattice $\Lambda_{\mathcal{A}}$ is nonvanishing and equal to one. More generally, if x is an element of an R-order Λ, then $nr(x) \in R$.

Remark 2: Note that if $\gamma \in F^*$ is not an algebraic integer, then an order 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. One of the motifs underlying the perfect codes [3] is the requirement that the variable γ should have a unit modulus. Relaxing this restriction on the size of γ will lead to an antenna power imbalance in both space and time domains. The measure of the fundamental parallelotope varies with different algebras. Hence, one has to keep in mind that on the other hand, an algebra with a unit γ may still admit larger average energy than an algebra with a non-unit γ so the size of γ is not the only parameter to stare at.

Definition 3.4: 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

$$\{\det tr(x_i x_j)_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}.$$

In the interesting cases of $F = \mathbf{Q}(i)$, $i = \sqrt{-1}$ (resp. $F = \mathbf{Q}(\sqrt{-3})$) the ring $R = \mathbf{Z}[i]$ (resp. $R = \mathbf{Z}[\omega]$, $\omega = (-1 + \sqrt{-3})/2$) 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 compute the discriminant as $d(\Lambda/R) = \det tr(x_i x_j)_{i,j=1}^m$, where $\{x_1, \ldots, x_m\}$ is any R-basis of Λ.

Remark 3: 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. [11, Theorem 25.3]) that all the maximal orders of a division algebra share the same discriminant. 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 the maximal one.

Let us now define some specific index 4 cyclic division algebras that will be later on used in the explicit code constructions. We denote by ζ_n the primitive nth root of unity.

A. Perfect algebra

In [3] the authors presented the so-called perfect codes that satisfy certain, quite strict, design criteria and hence perform very well in computer simulations. The underlying algebra in their 4×4 construction is the cyclic division algebra $\mathcal{PA} = (E/F, \tau, \gamma)$ with $E = \mathbf{Q}(\theta, i)$, $F = \mathbf{Q}(i)$, $u^4 = \gamma = i$, $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos(2\pi/15)$, and $\tau(\theta) = \theta^2 - 2$. The corresponding perfect code is

$$PC = \{ax \mid x \in \Lambda_{\mathcal{PA}} \text{ (cf. Prop. 3.2)},\ a = 1 - 3i + i\theta^2\},$$

where $\mathcal{I} = \langle a \rangle$ is an ideal of $\mathcal{O}_E$.

Moreover, a change of basis given by

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

is required for obtaining an orthogonal basis.

B. Cyclotomic algebra and a new isomorphic algebra

The AST codes obtained from the perfect algebra will be compared with the ones within the algebra $\mathcal{CA} = (E/F, \tau, \gamma)$ with $E = \mathbf{Q}(\xi = \zeta_{16})$, $F = \mathbf{Q}(i)$, $u^4 = \gamma = 2 + i$, and $\tau(\xi) = i\xi$.

This algebra has appeared earlier in at least [4] and [7].

Now let us denote by t the first quadrant fourth root of $2 + i$. The algebra $\mathcal{CA}$ is isomorphic to the algebra $\mathcal{NA} = (\mathbf{Q}(t)/\mathbf{Q}(i), t \mapsto it, i)$ with a unit γ [7]. Even though γ is a unit and hence the energy evenly spread, one has to realize that the fact that $\left|\sqrt[4]{2+i}\right| > |\zeta_\ell| = 1$ may hostilely affect to the average code energy (cf. Remark 2). We return to this example in Section IV.

IV. Constructing Asymmetric ST lattices

A straightforward way to obtain AST lattices would be just to switch off the extra layers in a symmetric MIMO setting. In the case of 4Tx+2Rx antennas this would mean that in (1) we set e.g. $x_1 = x_3 = 0$ in order to transmit a limited number of 8 Gaussian numbers that can be received with only two receivers in four time slots. In what follows we present another – in some cases significantly better – method for constructing AST lattices.

Let us consider an extension tower with the degrees $[E : L] = r, [L : F] = m$ and with the Galois groups $\mathrm{Gal}(E/F) = \langle \tau \rangle$, $\mathrm{Gal}(E/L) = \langle \sigma = \tau^m \rangle$. Let $\mathcal{B} = (E/L, \sigma, \gamma) = E + \cdots + u^{r-1}E$ be an index r division algebra, where the center L is fixed by $\sigma = \tau^m$. We denote by #Tx $= n = rm$.

Note that if one has a symmetric, index $n = rm$ 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 $b = x_0 + \cdots + u^{r-1}x_{r-1},\ x_i \in E,\ i = 0, ..., r-1$ of the algebra $\mathcal{B}$ has a representation as an $r \times r$ matrix $B = (b_{ij})_{1 \le i,j \le r}$ as given in (1). However, we can afford an $n \times n$ packing as we are using n transmitters. This can be achieved by using the isomorphism τ. Let us denote by $\tau^k(\mathcal{B}) = (E/F, \sigma, \tau^k(\gamma)),\ k = 0, ..., m-1$ the m isomorphic copies of $\mathcal{B}$ and the respective matrix representations by

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

Proposition 4.1: (**Method 1**) Let $b \in \Lambda \subseteq \mathcal{B}$ and $F = \mathbf{Q}(\delta)$, where $\delta \in \{i, \omega\}$. Assume $\gamma \in \mathcal{O}_L$. The lattice

$$\mathcal{C}(\Lambda) = \left\{ M = \text{diag}\left(B, \tau(B), \ldots, \tau^{m-1}(B)\right) \right\}$$

built from (2) has a nonvanishing determinant $\det \mathcal{C}(\Lambda) \in \mathbf{Z}[\delta]$. Thus, the minimum determinant is equal to one. The code rate equals $r^2 m/rm = r$.

Proof: According to Definition 3.2 and Proposition 3.2,

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

and hence $|\det M| \ge 1$. ∎

Now the natural question is how to choose a suitable division algebra. In [5] and [6] several systematic methods for constructing extensions E/L are provided. All of them make use of cyclotomic fields. In what follows we show how to maximize the code density (i.e. minimize the volume of the fundamental parallelotope, see [7]) with a given minimum determinant by minimizing a certain discriminant. Another question worth asking is how to do this in practice.

We need the following result. For the proof, see [11, p. 223].

Lemma 4.2: Suppose $\Lambda \subseteq \mathcal{A} = (E/L, \tau, \gamma)$ is an $\mathcal{O}_F$-order and that $F \subseteq L$. The discriminants then satisfy

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

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

The definition of the discriminant closely resembles that of the Gram matrix of a lattice, so the following results are rather unsurprising.

Lemma 4.3: Assume that F is an imaginary quadratic number field and that $\{1, \rho\}$ forms a $\mathbf{Z}$-basis of its ring of integers $\mathcal{O}_F$. Let $r = [E : L]$, $m = [L : F]$, and $n = rm$. If the order $\mathcal{C}(\Lambda)$ defined as in Proposition 4.1 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

$$m(\mathcal{C}(\Lambda)) = |\Im\rho|^{mr^2}|d(\Lambda/\mathcal{O}_F)|.$$

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 $n \times n$ complex matrix. We flatten it out into a $4 \times 4n^2$ matrix $L(A)$ by first forming a vector of length n^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 rows we can easily verify the identities $L(A)L(B)^H =$

$$\text{diag}\left(tr(AB^H), \tau(tr(AB^H)), tr(A^HB), \tau(tr(A^HB))\right) \quad (3)$$

and $L(A)L(B^T)^T =$

$$\text{diag}\left(tr(AB), \tau(tr(AB)), tr(AB)^*, \tau(tr(AB))^*\right). \quad (4)$$

Next let $\mathcal{X} = \{x_1, x_2, \ldots, x_{r^2}\}$ be an $\mathcal{O}_L$-basis for Λ. We form the $4r^2 \times 4r^2$ matrix $L(\mathcal{X})$ by stacking the matrices $L(x_i)_{4\times 4r^2}$ 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 (4) the matrix $M = L(\mathcal{X})R(\mathcal{X})$ consists of four by four blocks of the form $L(x_i)L(x_j^T)^T =$

$$\text{diag}\left(tr(x_ix_j), \tau(tr(x_ix_j)), tr(x_ix_j)^*, \tau(tr(x_ix_j))^*\right).$$

Clearly $\det R(\mathcal{X})R(\mathcal{X})^H = \pm \det L(\mathcal{X})L(\mathcal{X})^H$ and $\det M = |d(\Lambda/\mathcal{O}_L)|^2|\tau(d(\Lambda/\mathcal{O}_L))|^2$. Thus,

$$|\det L(\mathcal{X})L(\mathcal{X})^H|^{1/2} = |d(\Lambda/\mathcal{O}_L)||\tau(d(\Lambda/\mathcal{O}_L))|. \quad (5)$$

Next we turn our attention to the Gram matrix. Let $\{1, \theta, ..., \theta^3\}$ 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

$$d(\mathcal{O}_F/\mathbf{Z}) = \det D(\rho)^2 \text{ and } d(\mathcal{O}_L/\mathbf{Z}) = \det D(\theta)^2, \quad (6)$$

where $D(\rho) = \begin{pmatrix} 1 & 1 \\ \rho & \rho^* \end{pmatrix}$ 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

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

together with (3) it follows that for any two $n \times n$ matrices A and B we have $\frac{1}{2}\left(D(\theta)L(A)\right)\left(D(\theta)L(B)\right)^H =$

$$\begin{pmatrix} \Re(tr(AB^H)) & \cdots & \Re(tr(A(\theta^3B)^H) \\ \vdots & & \vdots \\ \Re(tr(\theta^3AB^H)) & \cdots & \Re(tr(\theta^3A(\theta^3B)^H)) \end{pmatrix}.$$

Therefore, if we denote by $D^{[r]}$ the $4r^2 \times 4r^2$ matrix having r^2 copies of $D(\theta)$ along the diagonal and zeros elsewhere, we get $G(\mathcal{C}(\Lambda)) = \frac{1}{2}\left(D^{[r]}L(\mathcal{X})\right)\left(D^{[r]}L(\mathcal{X})\right)^H$. Thus, $m(\mathcal{C}(\Lambda)) = \sqrt{\det G(\mathcal{C}(\Lambda))} = \left|\det L(\mathcal{X})L(\mathcal{X})^H\right|^{1/2} \cdot (\frac{1}{4})^{r^2}\left|\det D(\theta)\right|^{r^2}$.

As $(\frac{1}{2})^{2r^2}\left|\det D(\theta)\right|^{r^2} = \left|d(\mathcal{O}_L/\mathcal{O}_F)\right|^{r^2}\left|\Im\rho\right|^{2r^2}$ by (6) and Lemma 4.2, Equation (5) now gives us the claim when we still note (again by Lemma 4.2) that $d(\mathcal{O}_L/\mathcal{O}_F)^{r^2}d(\Lambda/\mathcal{O}_L)\tau(d(\Lambda/\mathcal{O}_L)) = d(\Lambda/\mathcal{O}_F)$. ■

Corollary 4.4: In the case $F = \mathbf{Q}(i)$ we get $m(\mathcal{C}(\Lambda)) = |d(\Lambda/\mathbf{Z}[i])|$. For $F = \mathbf{Q}(\omega)$ the volume equals $m(\mathcal{C}(\Lambda)) = (\frac{\sqrt{3}}{2})^{mr^2}|d(\Lambda/\mathbf{Z}[\omega])|$.

Now we can conclude that the extensions $E/L, L/F$ and the order $\Lambda \subseteq \mathcal{B}$ should be chosen such 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 $d(\Lambda/\mathcal{O}_L)$ (cf. Remark 3). 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

$$d(\Lambda/\mathcal{O}_L) \geq (P_1P_2)^{r(r-1)}, \quad (7)$$

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 [7, Theorem 3.2]). In [7] we have studied the use of maximal orders in the design of dense, symmetric, CDA based MIMO STBCs in more detail. The same ideas can be adapted to the asymmetric scheme as well.

Remark 4: The nTx+rRx antenna AST code from Proposition 4.1 can be transformed into an rTx+rRx antenna multi-block code [9] by an evident rearrangement of the blocks:

$$\text{diag}\left(B, \tau(B), \ldots, \tau^{m-1}(B)\right) \leftrightarrow \begin{pmatrix} B & \cdots & \tau^{m-1}(B) \end{pmatrix}.$$

As the Gram matrices of an AST lattice and a multi-block ST lattice coincide, Lemma 4.3 also holds for multi-block ST codes with the same parameters.

Remark 5: (**Method 2**) Another way to construct AST lattices would be as follows. Let $\mathcal{A} = (E/F, \tau, \gamma)$ be an index n division algebra and $[E : L] = m,\ [L : F] = r$. If in the matrix (1) the elements x_i are restricted to belong to L (rather than to E), we obtain a division algebra $\mathcal{A}'$ with the center $F[u^r]$. Obviously also the algebra $\mathcal{A}'$ is a division algebra as it is contained in $\mathcal{A}$. This construction also yields rate r codes for nTx+rRx antennas with a nonvanishing determinant.

V. Explicit AST codes

In this section we provide explicit constructions for the important case of 4Tx + 2Rx antennas.

For $\mathcal{PA}$ (cf. Section III-A) we have the nested sequence of fields $F \subseteq L \subseteq E$ with $L = \mathbf{Q}(i, \sqrt{5})$. As $\tau(\sqrt{5}) = -\sqrt{5}$, the field L is fixed by $\sigma = \tau^2$. By embedding the algebra $(E/L, \sigma, i)$ as in Proposition 4.1 we obtain the AST code $\mathcal{PA}_1 \subseteq$

$$\left\{ \begin{pmatrix} x_0 & i\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & i\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \;\middle|\; x_i \in \mathcal{O}_E \right\}.$$

As the center is now L with $[L:\mathbf{Q}(i)]=2$ and $\mathcal{O}_L=\mathbf{Z}[i,\mu=(1+\sqrt{5})/2]$, the elements x_i in the matrix are of the form $a_1+a_2\mu+a_3\theta+a_4\mu\theta$, where $a_i\in\mathbf{Z}[i]$ for all i. Hence, the code rate is $8/4=2$.

The algebra $\mathcal{CA}$ (cf. Section III-B), for its part, has the nested sequence of fields $F\subseteq L\subseteq E$ with $L=\mathbf{Q}(s=\zeta_8)$. As $\tau(s)=-s$, the field L is fixed by $\sigma=\tau^2$. Again by embedding the algebra $(E/L,\sigma:\xi\mapsto-\xi,\gamma=1+s-i)$ as in Proposition 4.1, the AST code $\mathcal{CA}_1\subseteq$

$$\left\{\left(\begin{array}{cccc} x_0 & \gamma\sigma(x_1) & 0 & 0\\ x_1 & \sigma(x_0) & 0 & 0\\ 0 & 0 & \tau(x_0) & \tau(\gamma)\tau(\sigma(x_1))\\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{array}\right)\;\middle|\; x_i\in\mathcal{O}_E\right\}$$

is obtained. The center is L with $[L:\mathbf{Q}(i)]=2$ and $\mathcal{O}_L=\mathbf{Z}[s]$. The elements x_i in the matrix are of the form $a_1+a_2s+a_3\xi+a_4s\xi$, where $a_i\in\mathbf{Z}[i]$ for all i, and so the code rate is 2. Note that we have chosen here a suitable non-norm element γ from $\mathcal{O}_L$ instead of $\mathcal{O}_F$ (cf. Section III-B). We get some energy savings as $|1+s-i|<|2+i|$.

Example 5.1: For our example algebras over $\mathbf{Q}(i)$ we have (cf. Propositions 3.2, 4.1, and 4.3) $m(\mathcal{C}(\Lambda_{\mathcal{PA}}))=3^4\cdot5^6$, $m(\mathcal{C}(\Lambda_{\mathcal{CA}}))=2^{16}\cdot3^2$, and $m(\mathcal{C}(\Lambda_{\mathcal{NA}}))=2^{16}\cdot5^3$. The two smallest prime ideal norms of $\mathcal{O}_{\mathbf{Q}(i,\sqrt{5})}$, $\mathcal{O}_{\mathbf{Q}(s)}$, and $\mathcal{O}_{\mathbf{Q}(\sqrt{2+i})}$ are 4 and 5, 2 and 9, and 2 and 5, respectively. The maximal orders of the respective algebras have fundamental parallelotopes of measures $5^6, 2^9\cdot3^2$, and $2^9\cdot5^3$. Thus we see that $\mathcal{PA}$ is the only algebra among these that does not achieve the discriminant bound that would give the measure $2^2\cdot5^5$ instead of 5^6 (cf. (7)). The algebra $\mathcal{CA}$ can be expected to have the best performance as it has the smallest measure. This is also backed up by computer simulations, see Fig. 1.

VI. Simulation results

In Figure 1, the different construction methods are denoted by subscripts: $0=$ Puncturing method, $1=$ Method 1 (cf. V), and $2=$ Method 2 (cf. Remark 5).

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 ($x_1=x_3=0$, cf. (1)) Perfect code $\mathcal{PA}_0$ and the code $\mathcal{PA}_1$, for which we used the ideal given in III-A.

The codes $\mathcal{CA}_1$, $\mathcal{PA}_2$, $\mathcal{PA}_1$, and $\mathcal{PA}_0$ perform more or less equally. The code $\mathcal{CA}_2$ loses to 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 $\mathcal{CA}_2$. The codes $\mathcal{NA}_0,\mathcal{NA}_1,\mathcal{NA}_2$ are in the respective order between the codes $\mathcal{CA}_0$ and $\mathcal{CA}_2$. They are not shown in Figure 1 in order not to make it too crowded. Due to the careful optimization carried out in [3] the code $\mathcal{PA}_1$ performs equally to the code $\mathcal{CA}_1$ despite of its lower density. Probably for the same reason, it appears to be irrelevant which construction method is used for $\mathcal{PA}$, whereas the same is not true at all for the other algebras.

The code $\mathcal{CA}_1$ MAX gotten by combining Method 1 with the use of a maximal order [7] triumphs over all the other codes. It outperforms the next best code by approximately $0.6-1$ dB. In [12] 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 - or at the worst ties with it. A suitably modified (more details will follow in a forthcoming paper) sphere decoder was used for decoding the lattices.

It seems that the best construction method depends on the very algebra that is in use. Figure 1 shows that the puncturing method is not always the first choice, hence proving the point of new construction methods. Actually, for the algebras $\mathcal{CA}$ and $\mathcal{NA}$ puncturing yields the worst performance.

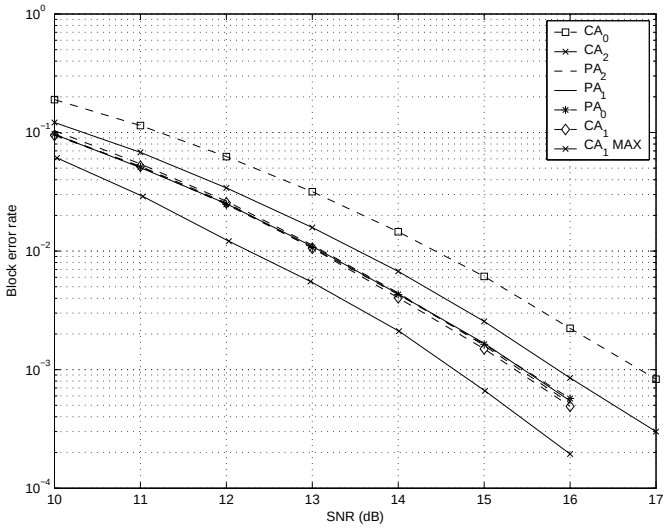

Fig. 1. Block error rates at 4 bpcu.

References

[1] J.-C. Belfiore and G. Rekaya, "Quaternionic Lattices for Space-Time Coding", in *Proc. ITW 2003*, Paris, France, 2003.

[2] 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, October 2003.

[3] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[4] Kiran. T 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, August 2005.

[5] 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, September 2006.

[6] 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 Signalling Complexity", in *Proc. CISS 2005*, Baltimore MD, March 2005.

[7] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "On the Densest MIMO Lattices from Cyclic Division Algebras", submitted to *IEEE Trans. Inf. Theory*, December 2006. http://arxiv.org/abs/cs.IT/0703052.

[8] 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.

[9] H.-f. (F.) Lu, "Explicit Constructions of Multi-Block Space-Time Codes that Achieve the Diversity-Multiplexing Tradeoff", in *Proc. IEEE ISIT 2006*, pp. 1149–1153, Seattle, 2006.

[10] A. A. Albert, *Structure of Algebras*, AMS, New York City 1939.

[11] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.

[12] 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 WSA 2007*, Vienna, Austria, February 2007.