Normalized Minimum Determinant Calculation for Multi-Block and Asymmetric Space-Time Codes

Camilla Hollanti[1] and Hsiao-feng (Francis) Lu[2]

[1]Department of Mathematics,
FIN-20014 University of Turku, Finland
[2]Department of Communication Engineering,
National Chung-Cheng University, Chia-yi, Taiwan
camilla.hollanti@utu.fi,hsiaofel@commsci1.usc.edu
http://www.math.utu.fi,http://www.comm.ccu.edu.tw

Abstract. The aim of this paper is to show the connection between certain, previously constructed multi-block and asymmetric space-time codes. The Gram determinants of the two constructions coincide, and hence the corresponding lattices share the same density. Using the notion of density, we define the normalized minimum determinant and give an implicit lower bound depending on the center of the cyclic division algebra in use. The calculation of the normalized minimum determinant is then performed in practice by using explicit code constructions.

Key words: Asymmetric space-time block codes (ASTBCs), cyclic division algebras (CDAs), dense lattices, discriminants, diversity-multiplexing tradeoff (DMT), maximal orders, multi-block, multiple-input multiple-output (MIMO) channels, nonvanishing determinant (NVD).

1 Background

Previously, different methods for constructing asymmetric [1],[2] and multi-block [3] 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+G mobile phones and DVB-H (Digital Video Broadcasting-Handhelds) user equipment, where only a very small number of antennas fits at the end user site. The best code in [1] was shown to improve upon the punctured Perfect code [2] as well as the DjABBA code [2] in the BLER performance at the data rate 4 bpcu, hence proving that the methods proposed therein come into good use.

Multi-block codes, for their part, are used when one wishes to obtain vanishing error probability in addition to the D-M tradeoff optimality. In this work, we concentrate on the minimal delay multi-block construction given in [3] and the asymmetric construction given in [1] by *Method 1*. In [4] an approach similar to Method 1 was used for the MIMO amplify-and-forward cooperative channel.

Already in [1] we stated that Method 1 can be converted to produce multi-block ST codes [3] that do achieve the DMT. Here, we shall show this explicitly and prove that maximizing the density (i.e. finding the most efficient packing in the available signal space) of asymmetric and multi-block codes arising from this method is equivalent to minimizing the discriminant of a certain order.

We define a *lattice* to be 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

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

where H indicates the complex conjugate transpose of a matrix, tr is the matrix trace (=sum of the diagonal elements), and $x_i,\ i = 1, ..., k$, form a $\mathbf{Z}$-basis of $\mathbf{L}$. The rank k of the lattice is upper bounded by $2n^2$. The Gram matrix has a positive determinant equal to the squared measure of the fundamental parallelotope $m(\mathbf{L})^2$. A change of basis does not affect the measure $m(\mathbf{L})$.

Any lattice $\mathbf{L}$ with the *nonvanishing determinant* (NVD) property [5] can be scaled, i.e. multiplied by a real constant r, either to satisfy $\det_{min}(\mathbf{L}) = 1$ or to satisfy $m(\mathbf{L}) = 1$. This is because $\det_{min}(r\mathbf{L}) = r^n \det_{min}(\mathbf{L})$ and $m(r\mathbf{L}) = r^k m(\mathbf{L})$. As the minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a lattice. Following [6], we denote by $\delta(\mathbf{L})$ the *normalized minimum determinant* of the lattice $\mathbf{L}$, i.e. here we first scale $\mathbf{L}$ to have a unit size fundamental parallelotope. Dually we denote by $\rho(\mathbf{L}) = 1/m(\mathbf{L})$ the *normalized density* of the lattice $\mathbf{L}$, when we first scale the lattice to have unit minimum determinant, and only then compute the quantity $1/m(\mathbf{L})$.

It has been shown in [7] that CDA-based square ST codes with the NVD property achieve the diversity-multiplexing tradeoff (DMT) introduced in [8]. This result also extends over multi-block space-time codes [3].

For more information on matrix representations of division algebras and their use as MIMO STBCs the reader can refer to [9]-[13], just to name a few.

2 Cyclic division algebras and orders

The theory of cyclic algebras and their representations as matrices are thoroughly considered in [9] and [14]. We are only going to recapitulate the essential facts here. For a more detailed introduction on orders, see [15].

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

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

Definition 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 (2).

Definition 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 [14, Theorem 11.12, p. 184].

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

Definition 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 $\mathcal{A}$.

Next we describe an order from where the elements are drawn in a typical CDA based MIMO space-time block code. For the proof of Proposition 2, see [15, Theorem 10.1, p. 125]. Some optimization to this can be done e.g. with the aid of ideals as in [10] or by using a maximal order [13].

Definition 4. *In any cyclic division algebra we can always choose the element $\gamma \in F^*$ determining the 2-cocycle in $H^2(E/F)$ to be an algebraic integer. We immediately see that the $\mathcal{O}_F$-module*

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

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 [16].

Proposition 2. *For any non-zero element $x \in \Lambda_{NAT}$ 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 Λ_{NAT} 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 [10] 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 a different algebra with a non-unit γ so the size of γ is not the only parameter to stare at.

Definition 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*

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

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. [15, 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.

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 [13, Lemma 7.1].

Lemma 1. *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 $\rho > 0$ be a real parameter chosen such that the minimum determinant of the lattice $\rho(x\Lambda)$ is also equal to one. Then the fundamental parallelotopes of these two lattice have the same measure*

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

3 Block diagonal asymmetric ST lattices

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

Let us consider an extension tower $F \subseteq L \subseteq E$ with the degrees $[E : L] = r, [L : F] = m$ 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 $\#\mathrm{Tx} = n = rm$.

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 $B = (b_{ij})_{1\leq i,j\leq r}$ as given in (2).

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 $\tau^k(\mathcal{B}) = (E/L, \sigma, \tau^k(\gamma)),\ k = 0, ..., m-1$ the m isomorphic copies of $\mathcal{B}$ and the respective matrix representations by

$$\tau^k(B) = (\tau^k(b_{ij}))_{1\leq i,j\leq r},\ k = 0, ..., m-1. \tag{3}$$

The next proposition shows that by using these copies as diagonal blocks we obtain an infinite lattice with nonvanishing determinant. For the proof, see [1].

Proposition 3. ***(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 lattice*

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

built from (3) has a nonvanishing determinant $\det \mathcal{C}(\Lambda) = \prod_{i=0}^{m-1} \det \tau^i(B) \in \mathbf{Z}[\delta]$. Thus, the minimum determinant is equal to one for all numbers of fading blocks m. The code rate equals $r^2m/rm = r$.

Now the natural question is how to choose a suitable division algebra. In [7] and [12] several systematic methods for constructing extensions E/L are provided. All of them make use of cyclotomic fields. In [1] we proved that, in the asymmetric scheme, maximizing the code density (i.e. minimize the volume of the fundamental parallelotope, see [13]) 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 multi-block codes from [3].

First we need the following result. For the proof, see [15, p. 223].

Lemma 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. For the proof, see [1].

Proposition 4. *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 $r = [E : L]$, $m = [L : F]$, $n = rm$, and $s = |\Im \rho|^{mr^2}$. If the order $\mathcal{C}(\Lambda)$ defined as in Proposition 3 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*

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

Corollary 1. *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 the norm of $d(\Lambda/\mathcal{O}_L)$ (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

$$d(\Lambda/\mathcal{O}_L) \geq (P_1 P_2)^{r(r-1)}, \tag{4}$$

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 [13, Theorem 3.2]).

Remark 4. Note that as opposed to [13], here we do not achieve nice, explicit lower bounds for $d(\Lambda/\mathcal{O}_L)$. That is a consequence of the fact that the center L can now be almost anything that just contains $\mathbf{Z}[i]$ or $\mathbf{Z}[\omega]$. An exact lower bound of course exists, but we have not been searching for it yet. We hope to provide this lower bound in a forthcoming paper.

Remark 5. In [13] 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 asymmetric and multi-block scheme as well.

4 Minimal delay multi-block ST codes

The nTx+rRx antenna AST code from Proposition 3 can be transformed into an rTx+rRx antenna multi-block code [3] by an evident rearrangement of the blocks:

$$\operatorname{diag}\left(B, \tau(B), \ldots, \tau^{m-1}(B)\right) \leftrightarrow \left(B, \cdots, \tau^{m-1}(B)\right). \tag{5}$$

As the Gram matrices of an AST lattice and a multi-block ST lattice coincide, Lemma 4 also holds for multi-block ST codes with the same parameters. Let the notation be as in Section 3.

Proposition 5. *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*

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

built from (3) satisfies the generalized nonvanishing determinant property (cf. [3],[11]), it is optimal with respect to the D-M tradeoff for all numbers of fading blocks m. Similarly as in Proposition 3, $\prod_{i=0}^{m-1} \det \tau^i(B) \geq 1$. The code rate equals $r^2 m/rm = r$.

Proof. For the proof, see [3].

Proposition 6. *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 $tr(diag(BB^H, .., \tau^{m-1}(B)\tau^{m-1}(B)^H)) =$
$= \sum_{i=0}^{m-1} tr(\tau^i(B)\tau^i(B)^H) = tr(\sum_{i=0}^{m-1}(\tau^i(B)\tau^i(B)^H))$.

An immediate consequence of Proposition 6 is

Corollary 2. *The lattices $\mathcal{C}(\Lambda)$ and $\mathcal{C}'(\Lambda)$ share the same density, i.e. Proposition 4 can be adapted as such to the multi-block scheme.*

5 Explicit codes

In this section we provide explicit asymmetric constructions for the important case of 4Tx + 2Rx antennas. These codes can be modified for 2×2 multi-block use (cf. (5). 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 multi-block code. However, with the aid of (5), an asymmetric code can always be transformed into a multi-block code and vice versa.

5.1 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 3 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 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. 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 basis.

5.2 Cyclotomic algebra $\mathcal{CA}$

The algebra $\mathcal{CA} = (E/L, \sigma = \tau^2 : \xi \mapsto -\xi, \gamma = 1 + s - i) = E \oplus uE$ (cf. [11], [13], [1]), 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 3, the AST code

$$\mathcal{CA}_1 \subseteq \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_1) & 0 & 0 \\ x_1 & \sigma(x_0) & 0 & 0 \\ 0 & 0 & \tau(x_0) & \tau(\gamma)\tau(\sigma(x_1)) \\ 0 & 0 & \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \middle| \, x_i \in \mathcal{O}_E \right\}$$

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 $a_1 + a_2 s + a_3\xi + a_4 s\xi$, where $a_i \in \mathbf{Z}[i]$ for all i. Hence the above code is transmitting again, 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 3). We get some energy savings as $|1 + s - i| < |2 + i|$.

5.3 Algebra $\mathcal{IA}$ – an improved maximal order

Similarly as in the two previous subsections, we obtain an rate-2 AST code $\mathcal{IA}_1$ by introducing yet another algebra $\mathcal{IA} = (E/L, \sigma = \tau^2, \gamma = \sqrt{-3})$, where $F = \mathbf{Q}(i)$, $L = \mathbf{Q}(i, \sqrt{3})$, $E = L(\sqrt{1+i})$, 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.

5.4 Algebra $\mathcal{QA}$ – an improved natural order

Let us use the multi-block 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 3 yields the following multi-block ST code with coding over 2 consecutive fading blocks:

$$\mathcal{QA}_1 \subseteq \left\{ B = \begin{pmatrix} x_0 & i\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}, \tau(B) = \begin{pmatrix} \tau(x_0) & i\tau(\sigma(x_1)) \\ \tau(x_1) & \tau(\sigma(x_0)) \end{pmatrix} \middle| \, x_i \in \mathcal{O}_E \right\}.$$

The elements x_i in the above are of the form $x_i = \sum_{j=0}^{3} a_{i,j}\zeta_5^j$, where $a_{i,j} \in \mathbf{Z}[i]$, hence the above code transmits on the average, 2 independent QAM symbols per channel use.

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

Table 1. Normalized minimum determinant δ and normalized density $\rho = 1/m(\Lambda)$ of natural and maximal orders of different algebras.

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

Example 1 *Let us calculate the normalized minimum determinant of the algebra $\mathcal{IA}$ as an example (cf. Section 1, Definitions 4, 5, and Propositions 3 and 4). The other algebras can be treated likewise. In Table 1 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 algebra $\mathcal{IA}$, for its part, has the densest maximal order. The corresponding numbers are shown* ***bold*** *in Table 1.*

For the natural order of $\mathcal{IA}$ *we have* $\det_{min}(\mathcal{C}(\Lambda_{NAT})) = 1$ *and* $\rho^{-1} = m(\mathcal{C}(\Lambda_{NAT})) = 2^{10} \cdot 3^6$, *hence* $r = 2^{-5/8} \cdot 3^{-3/8}$. *Now* $m(r\mathcal{C}(\Lambda_{NAT})) = 1$ *and the normalized minimum determinant is* $\delta = \det_{min}(r\mathcal{C}(\Lambda_{NAT})) = 2^{-5/2} \cdot 3^{-3/2} \cdot 1 \approx 0.0340$.

The maximal order of $\mathcal{IA}$ *has* $\det_{min}(\mathcal{C}(\Lambda_{MAX})) = 1$ *and* $m(\mathcal{C}(\Lambda_{MAX})) = 2^2 \cdot 3^6$, *thus* $r = 2^{-1/8} \cdot 3^{-3/8}$ *and* $\delta = \det_{min}(r\mathcal{C}(\Lambda_{MAX})) = \frac{1}{3\sqrt{2}\sqrt{3}} \approx 0.1361$.

References

1. C. Hollanti and K. Ranto, "Asymmetric Space-Time Block Codes for MIMO Systems", in *Proc. IEEE ITW 2007*, pp. 101–105, Bergen, Norway, July 2007.
2. 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, Feb.2007.
3. 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.
4. 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.
5. J.-C. Belfiore and G. Rekaya, "Quaternionic Lattices for Space-Time Coding", in *Proc. ITW 2003*, Paris, France, 2003.
6. J. Lahtonen, "Dense MIMO Matrix Lattices and Class Field Theoretic Themes in Their Construction", in *Proc. IEEE ITW 2007*, pp. 96–100, Bergen, Norway, July 2007.
7. P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, Sep. 2006.
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. 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.
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, Sep. 2006.
11. 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, Aug. 2005.
12. H.-F. Lu, P. Elia, K. R. Kumar, S. A. Pawar, 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.
13. C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "On the Densest MIMO Lattices from Cyclic Division Algebras", submitted to *IEEE Trans. Inf. Theory*, Dec. 2006. http://arxiv.org/abs/cs.IT/0703052.
14. A. A. Albert, *Structure of Algebras*, AMS, New York City 1939.
15. I. Reiner, *Maximal Orders*, Academic Press, New York 1975.
16. 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.