# Optimal Matrix Lattices for MIMO Codes from Division Algebras

Camilla Hollanti*, Jyrki Lahtonen†, Kalle Ranto†, and Roope Vehkalahti*
* TUCS Lab. of Discrete Mathematics, FIN-20014 University of Turku, Finland
Email: {cajoho, roiive}@utu.fi
† Department of Mathematics, FIN-20014 University of Turku, Finland
Email: {lahtonen, kara}@utu.fi

***Abstract*— We show why the discriminant of a maximal order within a cyclic division algebra must be minimized in order to get the densest possible matrix lattices with a prescribed non-vanishing minimal determinant. Using results from class field theory we derive a lower bound to the minimum discriminant of a maximal order with a given center and index (= the number of Tx/Rx antennas). We also give examples of division algebras achieving our bound. E.g. we construct a matrix lattice with QAM coefficients that has (inside 'large' subsets of the signal space) 2.5 times as many codewords as the celebrated Golden code of the same minimum determinant. We also give another matrix lattice with coefficients from the hexagonal lattice with an even higher density.**

## I. Introduction

We are interested in the coherent multiple input-multiple output (MIMO) case where the receiver perfectly knows the channel coefficients. For us a *lattice* is a discrete finitely generated free Abelian subgroup $\mathbf{L}$ of a real or complex finite dimensional vector space $\mathbf{V}$, called the ambient space. In the space-time setting a natural ambient space is the space $\mathcal{M}_n(\mathbf{C})$ of complex $n \times n$ matrices. We only consider full rank lattices that have a basis $x_1, x_2, \ldots, x_{2n^2}$ consisting of matrices that are linearly independent over the field of real numbers. We can form a $2n^2 \times 2n^2$ matrix $M$ having rows consisting of the real and imaginary parts of all the basis elements. It is well known that the measure, or hypervolume, $m(\mathbf{L})$ of the fundamental parallelotope of the lattice then equals the absolute value of $\det(M)$. Alternatively we may use the Gram matrix $G(\mathbf{L}) = MM^T = \left(tr(x_i x_j^H)\right)_{1 \leq i,j \leq 2n^2}$, where $H$ indicates the complex conjugate transpose of a matrix. The Gram matrix then has a positive determinant equal to $m(\mathbf{L})^2$.

From the pairwise error probability (PEP) point of view, it is well-known that 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 $\mathbf{X}-\mathbf{X}'$ taken over all distinct code matrices $\mathbf{X}, \mathbf{X}' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix $(\mathbf{X}-\mathbf{X}')(\mathbf{X}-\mathbf{X}')^H$. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$.

When a code is a subset of a lattice $\mathbf{L}$ in the ambient space $\mathcal{M}_n(\mathbf{C})$, the *rank criterion* states that any non-zero matrix in $\mathbf{L}$ must be invertible. It is widely known how the so called *Alamouti design* represents multiplication in the ring of quaternions. Matrix representations of other division algebras have been proposed as STBC codes at least in [1]–[5], and (though without explicitly saying so) [6]. The most recent work ([2]–[6]) has concentrated on adding multiplexing gain (i.e. MIMO applications) and/or combining it with a good minimum determinant. Furthermore, algebras with an imaginary quadratic field as a center yield lattices with a good minimum determinant, as the corresponding rings of integers have no short non-zero elements. This so called non-vanishing determinant property has been shown to be a sufficient condition for the resulting lattices to yield optimal diversity and multiplexing benefits [3]

In this talk we seek to make two points. The first is that in order to get the densest possible matrix lattices (with a fixed minimum determinant) one should use maximal orders rather than the so called natural orders (see the next section for precise definitions). E.g the data rates of the 2 (resp. 4 or 8) antenna codes proposed in [5] can theoretically be increased by 1.5 (resp. 6.5 or 20.5) bits per channel use without any penalty to neither minimum determinant nor transmission power by the process of finding a maximal order. The other point we seek to make is that one should be careful in choosing the cyclic division algebra. By applying relatively deep results from class field theory we derive an upper bound for the density of the matrix lattices gotten in this fashion. The bound is given in terms of the center (i.e. the alphabet) and the index (i.e. the number of antennas). The proof shows that the bound is also achieved by some (in most cases unknown) division algebra, so in this sense we completely solve the problem of determining the highest possible density of a lattice with fixed parameters. As an example we construct a code with density 2.5 times that of the Golden code [4] but same index and alphabet.

## II. Cyclic algebras, orders, Brauer groups, and discriminants

We refer the interested reader to [7] and [2] for an exposition of the theory of simple algebras, cyclic algebras, their matrix representations and their use in ST-coding. We only recall the basic definitions here. 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. $E$). In the interesting cases $F$ is an imaginary quadratic field,

either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$. We assume that $E/F$ is a cyclic field extension of degree $n$ with Galois group $Gal(E/F) = \langle\sigma\rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree $n$ ($n$ is also called the *index* of $\mathcal{A}$), 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 $A =$

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

*Definition 2.1:* The determinant (resp. trace) of the matrix $A$ above is called the *reduced norm* (resp. *reduced trace*) of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$ (resp. $tr(a)$).

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

*Example 2.1:* The division algebra $\mathcal{GA}$ used in [4] to construct the Golden code is gotten as a cyclic algebra with $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(i, \sqrt{5})$, $\gamma = i$, when the $F$-automorphism $\sigma$ 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 $\zeta$ 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 $\sigma'$ is the $F$-automorphism of $E'$ determined by $\zeta \mapsto -\zeta$ and $\gamma' = u'^2 = 5$.

Any cyclic algebra is a central simple $F$-algebra, i.e. its center is equal to $F$ and it has no nontrivial two-sided ideals. Two central simple $F$-algebras $\mathcal{A}$ and $\mathcal{B}$ are said to be similar, if there exist integers $m$ an $n$ such that the matrix algebras $\mathcal{M}_n(\mathcal{A})$ and $\mathcal{M}_m(\mathcal{B})$ are isomorphic $F$-algebras. Wedderburn's structure theorem tells us that any central simple algebra is a matrix algebra over a central simple division algebra, and it easily follows that within any similarity class there is a unique division algebra. Similarity classes of central simple algebras form a group (under tensor product over $F$), the so called Brauer group $Br(F)$ of the field $F$. If $F'$ is an extension field of $F$, and $A$ is a central simple $F$-algebra, then the tensor product $\mathcal{A}' = \mathcal{A} \otimes_F F'$ is a central simple $F'$-algebra. We refer to this algebra as the algebra gotten from $\mathcal{A}$ by *extending the scalars to* $F'$.

The next proposition due to A.A. Albert tells us when a cyclic algebra is a division algebra.

*Proposition 2.1:* The 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 $\gamma^t$ is the norm of some element in $E^*$ is $n$. ■

Let $F$ be an algebraic number field that is finite dimensional over $\mathbf{Q}$. Denote its ring of integers by $\mathcal{O}_F$. If $P$ is a prime ideal of $\mathcal{O}_F$, we denote the $P$-adic completion of $F$ by $F_P$. The division algebras over $F_P$ are easy to describe. They are all gotten as cyclic algebras of the form $A(n, r) = (E/F_P, \sigma, \pi^r)$, where $E$ is the unique unramified extension of $F_P$ of degree $n$, $\sigma$ is the Frobenius automorphism, and $\pi$ is the prime element of $F_P$. The quantity $r/n$ is called the *Hasse invariant* of this algebra. It follows immediately from Proposition 2.1 that $A(n, r)$ is a division algebra, if and only if $(r, n) = 1$. For a description of the theory of Hasse invariants we refer the reader to [8] or [10].

We next present some basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [8].

Let $R$ denote a Noetherian integral domain with a quotient field $F$, and let $\mathcal{A}$ be a finite dimensional $F$-algebra.

*Definition 2.2:* An *$R$-order* in the $F$-algebra $\mathcal{A}$ is a subring $\Lambda$ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that $\Lambda$ is a finitely generated module over $R$ and generates $\mathcal{A}$ as a linear space over $F$. An order $\Lambda$ is called *maximal*, if it isn't properly contained in another $R$-order.

*Example 2.2:* 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 order in $E$.

*Example 2.3:* 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

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E,$$

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*. It will serve as a starting point when searching for maximal orders.

*Definition 2.3:* Let $m = dim_F\mathcal{A}$. The *discriminant* of the $R$-order $\Lambda$ is the ideal $d(\Lambda/R)$ in $R$ generated by the set

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

In the interesting cases of $F = \mathbf{Q}(i)$ (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 pick a generator of the discriminant ideal, and call it the discriminant. It is easily seen that whenever $\Lambda \subseteq \Gamma$ are two $R$-orders, then $d(\Gamma)$ is a factor of $d(\Lambda)$. It turns out (cf. [8]) 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 division algebra.

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

unsurprising and probably well-known. We include them for lack of a suitable reference.

*Lemma 2.2:* Let $F = \mathbf{Q}(i), R = \mathbf{Z}[i]$, and assume that an $R$-order $\Lambda \subset (E/F, \sigma, \gamma)$ has an $R$-basis $x_1, x_2, \ldots, x_{n^2}$. Then the lattice $\Lambda$ has as a $\mathbf{Z}$-basis the set of matrices $x_1, x_2, \ldots, x_{n^2}, ix_1, ix_2, \ldots, ix_{n^2}$ and the determinant of the corresponding Gram matrix is

$$\det(G(\Lambda)) = |d(\Lambda/\mathbf{Z}[i])|^2.$$

In particular the measure of the fundamental parallelotope equals

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

*Example 2.4:* When we scale the Golden code [4] to have 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 is equal to 25. As was observed in [1] the natural order happens to be maximal in this case, so the Golden code cannot be improved upon by enlarging the order within $\mathcal{GA}$.

*Lemma 2.3:* Let $\omega = (-1 + \sqrt{-3})/2, F = \mathbf{Q}(\sqrt{-3}), R = \mathbf{Z}[\omega]$, and assume that an $R$-order $\Lambda \subset (E/F, \sigma, \gamma)$ has an $R$-basis $x_1, x_2, \ldots, x_{n^2}$. Then the lattice $\Lambda$ has as a $\mathbf{Z}$-basis the set of matrices $x_1, x_2, \ldots, x_{n^2}, \omega x_1, \omega x_2, \ldots, \omega x_{n^2}$ and the determinant of the corresponding Gram matrix is

$$\det(G(\Lambda)) = (3/4)^{n^2} |d(\Lambda/\mathbf{Z}[\omega])|^2.$$

In particular the measure of the fundamental parallelotope equals $m(\Lambda) = (\sqrt{3}/2)^{n^2} |d(\Lambda/\mathbf{Z}[\omega])|$.

So 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 we need to look for division algebras that have a maximal order with as small a discriminant as possible.

It is worth mentioning that in [9] the authors have made a similar approach in the reduced case of commutative number fields.

## III. Maximal orders with minimal discriminants

Again let $F$ be an algebraic number field that is finite dimensional over $\mathbf{Q}$, $\mathcal{O}_F$ its ring of integers, $P$ a prime ideal of $\mathcal{O}_F$ and $F_P$ the completion. In what follows we discuss the size of ideals of $\mathcal{O}_F$. By this 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.

Let us now suppose that we have a given number field $F$ and we would like to produce a division algebra $\mathcal{A}$ of a given index $n$, having $F$ as its center, and the smallest possible discriminant. In this section we are going to show that while we cannot give an explicit description of the algebra $\mathcal{A}$, we can derive an explicit formula for its discriminant.

*Theorem 3.1:* Assume that the field $F$ is totally complex and that $P_1, \ldots, P_n$ are some prime ideals of $\mathcal{O}_F$. Assume further that a sequence of rational numbers $a_1/m_{P_1}, \ldots, a_n/m_{P_n}$ satisfies

$$\sum_{i=1}^{n} \frac{a_i}{m_{P_i}} \equiv 0 \qquad (\text{mod} \quad 1),$$

$1 \leq a_i \leq m_{P_i}$ and $(a_i, m_{P_i}) = 1$.

Then there exists a central division $F$-algebra $\mathcal{A}$ that has local indices $m_{P_i}$ and index L.C.M $\{m_{P_i}\}$.

If $\Lambda$ is a maximal $\mathcal{O}_F$ order in $\mathcal{A}$, then the discriminant of $\Lambda$ is

$$d(\Lambda/\mathcal{O}_F) = \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\frac{[A:F]}{m_{P_i}}}.$$

*Proof:* We have the following exact sequence of Brauer groups

$$0 \longrightarrow B(F) \longrightarrow \oplus B(F_P) \longrightarrow \mathbf{Q}/\mathbf{Z} \tag{1}$$

which is well known from class field theory (cf e.g. [8] or the lecture notes [10]). Here the first map is gotten by mapping the similarity class of a central division $F$-algebra $\mathcal{D}$ to a sum of all the simple algebras $\mathcal{D}_P$ gotten from $\mathcal{D}$ by extending the scalars from $F$ to $F_P$, where $P$ ranges over all the prime ideals of $\mathcal{O}_F$. This exact sequence tacitly contains the piece of information that for all but finitely many primes $P$ the resulting algebra $\mathcal{D}_P$ is actually in the trivial similarity class of $F_P$-algebras, in other words $\mathcal{D}_P$ is simply a matrix algebra over $F_P$.

It is known that every element of the Brauer group $B(F_P)$ is presented by a central division $F_P$-algebra $D_P$ with Hasse invariant $a/m_P$, where $m_P = \sqrt{[\mathcal{D}_P : F_P]}$, $(a, m_P) = 1$, and $0 \leq a \leq m_P$. Also all such fractions appear as Hasse invariants of some division algebras. The last mapping in the exact sequence (1) is then gotten by adding together the Hasse invariants of the division algebras over the various completions $F_P$.

By exactness of the sequence (1) we know that there exists a central division algebra $\mathcal{A}$ over $F$ that has local indices $m_{P_i}$. From [8, Theorem 32.19] we know that $\sqrt{[\mathcal{A} : F]} = L.C.M\{m_{P_i}\}$. By [8, Theorem 32.1] the discriminant then equals

$$d(\Lambda/R) = \left( \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\kappa_{P_i}} \right)^{\sqrt{[A:F]}}, \tag{2}$$

where $\kappa_{P_i}$ is an integer called the local capacity.

A simple calculation of dimensions shows that

$$\kappa_P = \frac{\sqrt{[\mathcal{A} : F]}}{m_P}. \tag{3}$$

Substituting this into the equation 2 we get the claimed formula

$$d(\Lambda/\mathcal{O}_F) = \prod_{i=1}^{n} P_i^{(m_{P_i}-1)\frac{[A:F]}{m_{P_i}}}. \tag{4}$$

■

At this point it is clear that the discriminant $d(\Lambda)$ of a division algebra only depends on its local indices.

Now we have an optimization problem to solve. Given the center $F$ and an integer $n$ we should decide how to choose the local indices and the Hasse invariants so that the L.C.M of the local indices is $n$, the sum of the Hasse invariants is an integer and that the resulting discriminant is as small as possible.

Observe that the exponent $d(P)$ of the prime ideal $P$ in the discriminant formula

$$d(P) = (m_P - 1)\frac{[A:F]}{m_P} = n^2\left(1 - \frac{1}{m_P}\right).$$

As for the non-trivial Hasse invariants $n \geq m_P \geq 2$, we see that $n^2/2 \leq d(P) \leq n(n-1)$. Therefore the non-trivial exponents are roughly of the same size. E.g. when $n = 6$, $d(P)$ will be either 18, 24 or 30 according to whether $m_P$ is 2, 3 or 6. Not surprisingly it turns out that the optimal choice is to have only two non-zero Hasse invariants and to associate these with the two smallest prime ideals of $\mathcal{O}_F$.

*Theorem 3.2:* 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

$$(P_1P_2)^{n(n-1)}.$$

*Proof:* By Theorem 3.1 the division algebra with Hasse invariants $1/n$ and $(n-1)/n$ at the primes $P_1$ and $P_2$ has the prescribed discriminant, so we only need to show that this is the smallest possible value.

By the above discussion it is clear that in order to minimize the discriminant one cannot have more than three non-trivial Hasse invariants. This is because for prime ideals $P_1, P_2, P_3, P_4$ (listed from the smallest to the largest) we always have

$$P_1^{d(P_1)}P_2^{d(P_2)}P_3^{d(P_3)}P_4^{d(P_4)} > (P_1P_2)^{n(n-1)},$$

as the exponents $d(P_i) \geq n^2/2$ irrespective of the values of the Hasse invariants. The remaining possibility is that some combination of three Hasse invariants might yield a smaller discriminant. However, in this case either we can replace two of the Hasse invariants with the fractional part of their sum, and thus reduce the discriminant, as $d(P_3)+d(P_2) > n(n-1)$, or all the three Hasse invariants have numerators $\geq 6$ in which case $d(P_1)+d(P_2)+d(P_3) > 2n(n-1)$, and the claim follows in this case, too. ∎

We remark that the division algebra achieving our bound is by no means unique. E.g. any pair of Hasse invariants $a/n, (n-a)/n$, where $0 < a < n$, and $a$ and $n$ are coprime leads to a division algebra with the same discriminant.

*Example 3.1:* Let us consider proposition 3.2 in a situation where $n = 2$ and $F = \mathbf{Q}(i)$. The two smallest prime ideals are $(1+i)\mathcal{O}_F$ and $(2+i)\mathcal{O}_F$, so the smallest possible discriminant in this case is

$$((1+i)(2+i))^2\mathcal{O}_F.$$

Here the Hasse invariants that correspond to the primes $1+i$ and $2+i$ are $\{\frac{1}{2}, \frac{1}{2}\}$. We remark that $2+i$ here could be replaced with the other prime $2-i$ of norm five.

The Golden algebra reviewed in Example 2.1 has its non-trivial Hasse invariants corresponding to the primes $2+i$ and $2-i$, so it cannot be the algebra achieving the bound of Theorem 3.2. A clue for finding the optimal division algebra is hidden in the alternative description of the Golden algebra given in Example 2.1. It turns out that in the case $F = \mathbf{Q}(i)$, $E = \mathbf{Q}(\zeta)$ instead of using $\gamma' = 5$ as in the case of the Golden algebra we can use its prime factor $\gamma = 2+i$.

*Theorem 3.3:* The maximal orders of the cyclic division algebra $\mathcal{GA}+ = (\mathbf{Q}(\zeta)/\mathbf{Q}(i), \sigma, 2+i)$ achieve the bound of Theorem 3.2. Here $\sigma$ is the automorphism determined by $\sigma(\zeta) = -\zeta$.

*Proof:* Our algebra $\mathcal{GA}+$ is generated as a $\mathbf{Q}(i)$-algebra by the elements $\zeta$ and $u$ subject to the relations $\zeta^2 = i$, $u^2 = 2+i$, and $u\zeta = -\zeta u$. The natural order $\mathbf{Z}[\zeta] \oplus u\mathbf{Z}[\zeta]$ is not maximal. Let us use the matrix representation of $\mathcal{GA}+$ as $2\times 2$ matrices with entries in $\mathbf{Q}(\zeta)$, so elements of $\mathbf{Q}(i)$ are mapped to scalar matrices and $\zeta$ is mapped to a diagonal matrix with diagonal elements $\zeta$ and $-\zeta$. We easily see that the matrix

$$w = \begin{pmatrix} 2i-(1-i)\sqrt{2} & 2i-(1+i)\sqrt{2} \\ (1+3i)(1+\sqrt{2}+i) & 2i+(1-i)\sqrt{2} \end{pmatrix}$$

is an element of $\mathcal{GA}+$. Straightforward calculations show that $w$ satisfies the equations

$$w^2 = -i + iw \quad \text{and} \quad w\zeta = -1 + \zeta^3 - \zeta w.$$

From these relations it is obvious that the free $\mathbf{Z}[\zeta]$-module with basis elements 1 and $w$ is an order $\Lambda$. Another straightforward computation shows that $d(\Lambda/\mathbf{Z}[i]) = -8 + 6i = (1+i)^2(2+i)^2$. As this is the bound of Theorem 3.2 we may conclude that $\Lambda$ is a maximal order. ∎

By Lemma 2.2 we see that the fundamental parallelotope of the maximal order in Theorem 3.3 has measure 10. Thus this code has 2.5 times the density of the Golden code. Because of this and the close relation of the algebra $\mathcal{GA}+$ to the Golden algebra, we refer to our algebra as the "Golden+ algebra". For the benefit of anyone interested in toying with this code we give the following description for it. Let $B$ the diagonal $2\times 2$-matrix with entries $\zeta$ and $\sigma(\zeta) = -\zeta$. This code then consists of the matrices of the form

$$c_1I_2 + c_2B + c_3w + c_4Bw,$$

where the coefficients $c_1, \ldots, c_4$ are gaussian integers (i.e. $\in \mathbf{Z}[i]$). As in the case of the Golden algebra, an ideal of this maximal order may have a better shape. We also list some mostly untried optimization tricks in the concluding section.

We remark that the algebra $\mathcal{GA}+$ of Theorem 3.3 has appeared earlier in [5]. However, the authors did not consider its maximal orders.

*Example 3.2:* 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 they have norms 4 and 3 respectively. By Theorem 3.2 the minimal discriminant is $4(1-\omega)^2\mathbf{Z}[\omega]$ in this case. As the absolute value of $1-\omega$ is $\sqrt{3}$ an application of the formula in Lemma 2.3 shows that the lattice $\mathbf{L}$ of the code achieving this bound has $m(\mathbf{L}) = 27/4$. We can show that a maximal

order of the cyclic algebra $(E/F, \sigma : i \mapsto -i, \gamma = \sqrt{-3})$ where $E = \mathbf{Q}(i, \sqrt{-3})$ achieves this bound.

Again we remark that the algebra of Example 3.2 has appeared implicitly in [6], but the authors only used the natural order rather than a maximal order.

In general the problem of finding a maximal order within a division algebra is relatively difficult. An algorithm developed by Ivanyos and Rónyai (cf. [11]) can be used in some cases, but at least its MAGMA implementation runs out of memory very quickly as $n$ increases. We have developed an enhancement to their algorithm that utilizes some elementary propertis of rings cyclotomic integers. This has the severe drawback that its utility is limited to certain rather special cases, e.g. the family of algebras of index $2^\ell$ from [5].

We have carried out some very preliminary simulations with the code of Theorem 3.3. For the chosen low data rates our maximal order does offer energy vs. minimum determinant savings over the Golden code, but the block error rates are more or less the same, and unless we choose the version of the code carefully the Golden code prevails by a fraction of a dB. This is partly because we are using a less than optimal version of the code. Further optimization is necessary, but for higher data rates and signal-to-noise ratios we expect the higher density vs. minimum determinant advantage to kick in. Another possible explanation is that the singular values of the matrices in the rectangular Golden code behave better than those of our code. E.g. the basic matrices of the Golden code have singular values $0.618$ and $1.618$ whereas some basic matrices of our code have singular values $0.473$ and $2.112$. As low singular values account for many error events, this then offsets the small energy savings provided by our code at low data rates and low SNR.

We have not yet had the time to carry out any simulations with the code of Example 3.2. Similar behavior at low data rates and SNR is to be expected, as the lowest singular value of a basic matrix is $0.435$.

## IV. Concluding remarks and suggestions for further work

In the small example case above it was relatively easy to find a candidate for a cyclic division algebra that might have the optimal discriminant. The choices of the extension field and the element $\gamma$ were readily suggested by the list of ramified primes. The algorithm from [11] was then used to verify that a maximal order achieving the bound exists and could also be constructed. In the near future we hope to make this step constructive in the sense that (at least in the practical cases of a low number of antennas) we would have a recipe for constructing division algebras attaining the lower bound rather than the ad hoc methods used here. It is also clearly desirable to get a better description of the maximal orders (bearing in mind that unlike in the commutative case the maximal orders within a non-commutative division algebra are not necessarily unique).

Also at this point the 2.5 to 1 density advantage our construction enjoys over the Golden code is mostly theoretical. In a non-hypercubical lattice the problem of finding a coset of the code lattice that has a desired number of low energy matrices is somewhat difficult. It may well happen that the winning code depends on the chosen data rate - particularly at a low or mid-range SNR. The very preliminary simulations at low data rate (from 3.5 to 4.5 bpcu) that we have done so far seem to bear this out.

On the other hand we have not yet exhausted the box of optimization tools on our code. E.g. our code 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 non-unitary matrix multipliers, the geometry of our lattice will change. While we cannot turn the lattice into a rectangular one in this manner, some improvements can easily be obtained. E.g. we can distribute the transmission power more evenly between the antennas and the time slices. Overall energy savings are also available, but we have not solved the resulting optimization problem yet. Hopefully a suitably reformed version of our lattice will also allow a relatively easy description of the low energy matrices. This in turn would make the use of the sphere decoding algorithm on our lattice simpler.

## V. Acknowledgments

C. Hollanti is partially supported by the Nokia Foundation. K. Ranto is supported by the Academy of Finland, grant #108238.

## References

[1] C. Hollanti and J. Lahtonen, "A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras", accepted for presentation at IEEE ITW 2006, March 2006.

[2] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras", *IEEE Transactions on Information Theory*, vol. 49, pp. 2596–2616, October 2003.

[3] P. Elia, K. R. Kumar, P. V. Kumar, S. A. Pawar and H.-f. Lu, Explicit Space-Time Codes that Achieve the Diversity-Multiplexing Gain Trade-off, submitted to *IEEE Transactions on Information Theory*, 2004.

[4] J.-C. Belfiore, G. Rekaya, and E. Viterbo: "The Golden Code: A 2x2 Full-Rate Space-Time Code With Nonvanishing Determinants", *IEEE Transactions on Information Theory*, vol. 51, n. 4, pp. 1432-1436, Apr. 2005.

[5] Kiran T. and B. Sundar Rajan, "STBC-schemes with Non-vanishing Determinant for Certain Number of Transmit Antennas", in *Proceedings IEEE ISIT 2005*, pp. 1178–1182, September 2005.

[6] G. Wang and X.-G. Xia, "On Optimal Multi-Layer Cyclotomic Space-Time Code Designs", *IEEE Transactions on Information Theory*, vol. 51, pp. 1102–1135, March 2005.

[7] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, USA 1980.

[8] I. Reiner, *Maximal Orders*, Academic Press, NY 1975.

[9] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Algebraic Lattice Constellations: Bounds on Performance", *IEEE Transactions on Information Theory*, vol. 52, n. 1, pp. 319–327, January 2006.

[10] J. S. Milne , "Class Field Theory", Lecture notes for a course given at the University of Michigan, Ann Arbor.

[11] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in semisimple algebras over Q", *Computational Complexity 3*, pp. 245–261, 1993.