A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras

Camilla Hollanti
TUCS Lab. of Discrete Mathematics
University of Turku
FIN-20014 Turku, Finland
Email: cajoho@utu.fi

Jyrki Lahtonen
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
Email: lahtonen@utu.fi

***Abstract*— A means to construct dense, full-diversity STBCs from maximal orders in central simple algebras is introduced for the first time. As an example we construct an efficient ST lattice code with non-vanishing determinant for four transmit antenna MISO application. Also a general algorithm for testing the maximality of a given order is presented. By using a maximal order instead of just the ring of algebraic integers, the size of the code increases without losses in the minimum determinant. The usage of a proper ideal of a maximal order further improves the code, as the minimum determinant increases. Simulations in a quasi-static Rayleigh fading channel show that our lattice outperforms the DAST-lattice due to the properties described above.**

I. Introduction

We are interested in the coherent multiple input-single output (MISO) case where the receiver perfectly knows the channel coefficients. The received signal is

$$\mathbf{y_{1\times n}} = \mathbf{h_{1\times k}}\mathbf{X_{k\times n}} + \mathbf{n_{1\times n}},$$

where $\mathbf{X}$ is the transmitted codeword taken from the Space-Time Block Code (STBC) $\mathcal{C}$, $\mathbf{h}$ is the Rayleigh fading channel response and the components of the noise vector $\mathbf{n}$ are i.i.d. complex Gaussian random variables.

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. The receiver, however, (recall that we work in the MISO setting) sees vector lattices instead of matrix lattices. When the channel state is $\mathbf{h}$, the receiver expects to see the lattice $\mathbf{hL}$.

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 $(\mathbf{X}-\mathbf{X}')(\mathbf{X}-\mathbf{X}')^H$, where ^{H} denotes the Hermitian transpose. 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. This follows from the fact that the difference of any two matrices from $\mathbf{L}$ is again in $\mathbf{L}$.

It is widely known how the so called *Alamouti design* represents 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 STBC codes at least in [1],[2],[3],[4], and (though without explicitly saying so) [5]. The most recent work ([3],[4] and [5]) has concentrated on adding multiplexing gain (i.e. MIMO applications) and/or combining it with a good minimum determinant. We do not seek any multiplexing gains, but want to improve upon e.g. the DAST-lattices introduced in [2] by using not only non-commutative division algebras, but the maximal orders within them. The usage of division algebras has been of the utmost interest in the recent study, as they naturally produce families of linear, full-rank codes. By choosing the elements in the code matrices from a maximal order instead of just picking them from the ring of algebraic integers – albeit in some cases these may collapse – the size of the code can be increased without losses in the minimum determinant. By further requiring the elements to belong to a proper ideal of a maximal order the minimum determinant increases and hence, after scaling, denser lattices are produced.

II. Lattice construction

The set $\{a_1 + a_2 i + a_3 j + a_4 k |\ a_i \in \mathbf{R}\ \forall i\}$, where $i^2 = j^2 = k^2 = -1,\ ij = k$, is recalled as the ring of Hamiltonian quaternions. We shall use extension rings of the Gaussian integers $\mathcal{G} = \{a + bi | a, b \in \mathbf{Z}\}$ inside a given division algebra as they nicely fit with the popular 16-QAM and QPSK alphabets. Let $\xi = e^{\pi i/4} = (1+i)/\sqrt{2}$ be a primitive 8^{th} root of unity. Our main example is the division algebra $\mathbf{H} = \mathbf{Q}(\xi) \oplus \mathbf{Q}(\xi)j$. As $zj = jz^*$ for all complex numbers z, and as the field $\mathbf{Q}(\xi)$ is stable under the usual complex conjugation $(^*)$, the set $\mathbf{H}$ is a subskewfield of the quaternions.

As always, multiplication from the left by a non-zero element of the division algebra $\mathcal{A}$ is an invertible $\mathbf{Q}(i)$-linear mapping with $\mathbf{Q}(i)$ acting from the right. Therefore its matrix with respect to a chosen $\mathbf{Q}(i)$-basis $\mathcal{B}$ of $\mathcal{A}$ is also invertible. The division algebra $\mathbf{H}$ has the set $\mathcal{B}_H = \{1, \xi, j, j\xi\}$ as a

natural $\mathbf{Q}(i)$-basis. Thus we immediately arrive (see also [1]) at the following matrix representation of the division algebra $\mathbf{H}$.

Proposition 2.1: Let the variables c_1, c_2, c_3, c_4 range over all the elements of $\mathbf{Q}(i)$. The division algebra $\mathbf{H}$ can be identified via an isomorphism ϕ with the following ring of matrices $\mathbf{H} =$

$$\left\{ M = M(c_1, c_2, c_3, c_4) = \begin{pmatrix} c_1 & ic_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & ic_4^* & -c_3^* \\ c_3 & ic_4 & c_1^* & c_2^* \\ c_4 & c_3 & -ic_2^* & c_1^* \end{pmatrix} \right\}.$$

In particular the determinants of these matrices are non-zero whenever at least one of the coefficients c_1, c_2, c_3, c_4 is non-zero. ∎

In order to get STBC-lattices and useful bounds for the minimum determinant we need to identify suitable subrings R of the algebra $\mathbf{H}$. We shall do this by placing certain restrictions for the elements c_1, c_2, c_3, c_4. Later on, in section III, we shall show that one of these restrictions produces a maximal order.

The $\mathcal{G}$-module spanned by our earlier basis $\mathcal{B}_H$ is a ring $\mathcal{L}$ of the required type. We call this ring the ring of Lipschitz' integers of $\mathbf{H}$. The ring $\phi(\mathcal{L})$ consists of those matrices of $\mathbf{H}$ that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. However, $\mathcal{L}$ is not maximal among the rings satisfying our requirements. The ring of Hurwitz' integral quaternions also has an extension of the prescribed type inside $\mathbf{H}$. This ring, denoted by $\mathcal{H}$, is the right $\mathcal{G}$-module generated by the basis $\mathcal{B}_{Hur} = \{\rho, \rho\xi, j, j\xi\}$, where $\rho = (1 + i + j + k)/2$. For future use we express the ring $\mathcal{H}$ in terms of the basis $\mathcal{B}_H$ of Proposition 2.1. It is not difficult to show that the quaternion $q = c_1 + \xi c_2 + jc_3 + j\xi c_4$ is an element of $\mathcal{H}$, if and only if the coefficients $c_t, t = 1, 2, 3, 4$ satisfy the requirements $(1 + i)c_t \in \mathcal{G}$ for all t and $c_1 + c_3, c_2 + c_4 \in \mathcal{G}$. As the ideal generated by $1 + i$ is of index two in $\mathcal{G}$, we see that $\mathcal{L}$ is an additive subgroup of index four in $\mathcal{H}$. We summarize these findings in Proposition 2.2. The bound on the minimum determinant is a consequence of the fact that all the elements of $\mathcal{G}$ have norm at least 1.

Proposition 2.2: The following rings of matrices form STBC-lattices of minimum determinant 1.

$$\mathbf{L}_{\mathcal{L}} = \{M(c_1, c_2, c_3, c_4) | c_1, c_2, c_3, c_4 \in \mathcal{G}\},$$

$$\mathbf{L}_{\mathcal{H}} = \{M(c_1, c_2, c_3, c_4) | c_1, c_2, c_3, c_4 \in \frac{1+i}{2}\mathcal{G}, \; c_1 + c_3 \in \mathcal{G}, c_2 + c_4 \in \mathcal{G}\}.$$ ∎

Remark 2.1: The lattice $\mathbf{L}_{\mathcal{L}}$ is a more developed case from the so-called *quasi-orthogonal* STBC suggested e.g. in [6]. The matrix of $\mathbf{L}_{\mathcal{L}}$ can be found as an example also in [3], but no optimization has been done there by using, for example, maximal orders as we shall do here.

A drawback of the lattice $\mathbf{L}_{\mathcal{L}}$ is that in the ambient space of the transmitter it is isometric to the rectangular lattice $\mathbf{Z}^8$. The rectangular shape does carry the advantage that the sets of information carrying coefficients of the basic matrices are simple and all identical (this is useful in e.g. sphere decoding), but this shape is very wasteful in terms of transmission power. Geometrically denser sublattices of $\mathbf{Z}^8$, e.g. the diamond lattice E_8 are well known (cf. e.g. [7]). However, we must be careful when picking the copies of the sublattices, as it is the minimum determinant we want to keep an eye on.

The units of the ring $\mathbf{L}_{\mathcal{L}}$ are exactly the non-zero matrices, whose determinants have the minimal absolute value one. Thus an intuitive way to find a sublattice with a better minimum determinant is to take the lattice $\phi(\mathcal{I})$, where $\mathcal{I} \subset R$ is a proper ideal. This idea has appeared in [1] and [4]. Even earlier, ideals of rings of algebraic integers were used in [8] to produce dense lattices.

The diamond lattice E_8 can be described in terms of the Gaussian integers as follows (cf. [9]):

$$E_8 = \frac{1}{1+i}\{(c_1, c_2, c_3, c_4) \in \mathcal{G}^4 | c_1 + \mathcal{I} = c_t + \mathcal{I}, \; t = 2, 3, 4, \; \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}.$$

By our identification of quadruples $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ and elements of $\mathbf{H}$ it is readily verified that $\Lambda = (1 + i)E_8$ has $\{2, (1 + i) + (1 + i)\xi, (1 + i)\xi + (1 + i)j, 1 + \xi + j + j\xi\} \subseteq \mathcal{L}$ as a $\mathcal{G}$-basis, whence the set $\{1 + i, 1 + \xi, \xi + j, \rho + \rho\xi\} \subseteq \mathcal{H}$ is a $\mathcal{G}$-basis for E_8. By another simple computation we see that $E_8 = \mathcal{H}(1 + \xi)$, i.e. E_8 is the left ideal of the ring $\mathcal{H}$ generated by $1 + \xi$.

Proposition 2.3: The lattice

$$\mathbf{L}_{E_8} = \{M(c_1, c_2, c_3, c_4) \in \mathbf{L}_{\mathcal{L}} | \; c_1 + \mathcal{I} = c_t + \mathcal{I}, \; t = 2, 3, 4, \; \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}$$

is an index 16 sublattice of $\mathbf{L}_{\mathcal{L}}$. Furthermore, the minimum determinant of $\mathbf{L}_{E_8}$ is 64.

Proof: Let $M_I = M(1, 1, 0, 0)$ be the matrix $\phi(1 + \xi)$ under the isomorphism of Proposition 2.1. We see that $\det(M_I M_I^*) = 4$. By the preceding discussion any matrix A of the lattice $\mathbf{L}_{E_8}$ is of the form $A = MM_I(1 + i)$, where M is a matrix from $\mathbf{L}_{\mathcal{H}}$. Thus, $\det AA^* = 16 \det(M_I M_I^*) \det(MM^*)$ and the claim on the minimum determinant follows from Proposition 2.2. We see that the coefficient c_1 can be chosen arbitrarily within $\mathcal{G}$. The coefficients c_2 and c_3 then must belong to the coset $c_1 + \mathcal{I}$, and c_4 must be chosen such that $c_1 + c_2 + c_3 + c_4 \in 2\mathcal{G} = \mathcal{I}^2$. As $\mathcal{I}$ is of index two in $\mathcal{G}$, we see that the index of $\mathbf{L}_{E_8}$ in $\mathbf{L}_{\mathcal{L}}$ is 16 as claimed. ∎

III. Cyclic algebras and orders

The theory of cyclic algebras and their representations as matrices are thoroughly considered in [3]. We are only going to recapitulate the essential facts here.

In the following, we consider number field extensions E/F, where F denotes the base field. F^* (resp. E^*) denotes the set of non-zero elements of F (resp. E). Let E/F be a cyclic field extension of degree n with Galois group $Gal(E/F) =$

$\langle\sigma\rangle$, where σ is the generator of the cyclic group. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n, that is

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

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

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

Let us compute the third column as an example:

$$\begin{aligned} u^2 \mapsto au^2 &= x_0u^2 + ux_1u^2 + \cdots + u^{n-1}x_{n-1}u^2 \\ &= u\sigma(x_0)u + u^2\sigma(x_1)u + \cdots + \gamma\sigma(x_{n-1})u \\ &= u^2\sigma^2(x_0) + u^3\sigma^2(x_1) + \cdots + u\gamma\sigma^2(x_{n-1}), \end{aligned}$$

and hence for the third column we get the vector $(\gamma\sigma^2(x_{n-2}), \gamma\sigma^2(x_{n-1}), \sigma^2(x_0), \ldots, \sigma^2(x_{n-3}))^T$.

Definition 3.1: An algebra $\mathcal{A}$ is called *simple*, if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is *central* if its centre $Z(A) = \{a \in \mathcal{A} | aa' = a'a \ \forall a' \in \mathcal{A}\} = F$.

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

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

In the preceding section we have attested that the algebra $\mathbf{H}$ is a division algebra. The next proposition provides us with a sufficient condition when an algebra is indeed a division algebra.

Proposition 3.1: The algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if the smallest factor $t \in \mathbf{Z}$ of n such that γ^t is the norm of some element in E^* is n. ∎

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [10].

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, a Λ-order in $\mathcal{A}$ is said to be *maximal*, if it is not properly contained in any other Λ-order in $\mathcal{A}$. If the integral closure $\overline{R}$ of R in $\mathcal{A}$ happens to be an R-order in $\mathcal{A}$, then $\overline{R}$ is automatically the unique maximal R-order in $\mathcal{A}$.

Let us illustrate the above definition by the following example.

Example 3.1: (a) Orders always exist: If M is a full R-lattice in $\mathcal{A}$, i.e. $FM = \mathcal{A}$, then the *left order* of M defined as $\mathcal{O}_l(M) = \{x \in \mathcal{A} | xM \subseteq M\}$ is an R-order in $\mathcal{A}$. The right order is defined in an analogous way.

(b) If $\mathcal{A} = \mathcal{M}_n(F)$, the algebra of all $n \times n$ matrices over F, then $\Lambda = \mathcal{M}_n(R)$ is an R-order in $\mathcal{A}$.

Hereafter, F will be an algebraic number field and R a Dedekind ring with F as a field of fractions.

Proposition 3.2: Let $\mathcal{A}$ be a finite dimensional semisimple algebra over F and Λ be a $\mathbf{Z}$-order in $\mathcal{A}$. Let $\mathcal{O}_F$ stand for the ring of algebraic integers of F. Then $\Gamma = \mathcal{O}_F\Lambda$ is a $\mathcal{O}_F$-order containing Λ. As a consequence, a maximal $\mathbf{Z}$-order in $\mathcal{A}$ is a maximal $\mathcal{O}_F$-order as well. ∎

In Section IV some facts from the local theory of orders are required. Let us first define the ring $\mathbf{Z}_p$.

Definition 3.4: For a rational prime p let $\mathbf{Z}_p$ denote the ring

$$\mathbf{Z}_p = \{\frac{r}{s} \in \mathbf{Q} \mid r, s \in \mathbf{Z}, \ gcd(p, s) = 1\}.$$

$\mathbf{Z}_p$ is a discrete valuation ring with the unique maximal ideal $p\mathbf{Z}_p$. If Λ is a $\mathbf{Z}$-order we use the notation $\Lambda_p = \mathbf{Z}_p\Lambda$.

Definition 3.5: Let S denote an arbitrary ring with identity. The *Jacobson radical* of S is the set $Rad(S) =$

$$\{x \in S | xM = (0) \text{ for all simple left S-modules } M\}.$$

Definition 3.6: Let $m = dim_F\mathcal{A}$. The discriminant of the R-order Λ is the ideal $d(\Lambda)$ in R generated by the set

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

It is clear that if $\Lambda \subseteq \Gamma$ then $d(\Gamma)|d(\Lambda)$. Moreover, we have an equality if and only if $d(\Gamma) = d(\Lambda)$.

Proposition 3.3: Let Λ be an R-order and $\{a_1, ..., a_m\} \subseteq \Lambda$ be an F-basis of $\mathcal{A}$. Then the principal ideal generated by the nonzero determinant $d = det(tr(a_ia_j))_{i,j=1}^m$ is contained in the discriminant. Let Γ be any order containing Λ. Then $d\Gamma \subseteq R\{a_1, ..., a_m\} \subseteq \Lambda$. □

The following proposition gives us a useful tool to find the maximal orders within a given algebra.

Proposition 3.4: Let Λ be an R-order in $\mathcal{A}$. For each $a \in \Lambda$ we have $nr(a) \in R, \ tr(a) \in R$. ∎

Proposition 3.5: Let Γ be a subring of $\mathcal{A}$ containing R such that $F\Gamma = \mathcal{A}$, and suppose that each $a \in \Gamma$ is integral over R. Then Γ is an R-order in $\mathcal{A}$. Conversely, every R-order in $\mathcal{A}$ has these properties. ∎

Corollary 3.6: Every R-order in $\mathcal{A}$ is contained in a maximal R-order in $\mathcal{A}$. There exists at least one maximal R-order in $\mathcal{A}$. ∎

Proposition 3.7: Let $\mathcal{A}$ be a simple algebra over F and M a finitely generated $\mathcal{O}_F$-module such that $FM = \mathcal{A}$. Then there exists an element $s \in \mathcal{O}_F \setminus \{0\}$ such that $s \cdot 1 \in M$. Moreover, $\mathcal{O}_l(M) = \{b \in s^{-1}M | \ bM \leq M\} \leq s^{-1}M$. ∎

Proposition 3.8: The prime ideals $\mathcal{P}$ of a maximal order Λ and the prime ideals P of R are in one-to-one correspondence, given by $P = R \cap \mathcal{P},\ \mathcal{P} \supseteq P\Lambda$.

(i) The ideals of Λ are exactly the products of prime ideals.

(ii) For a prime ideal P of R there exists a unique natural number m_P such that $P\Lambda = \mathcal{P}^{m_P}$. The numbers m_P are divisors of n and, except for finitely many prime ideals P of R, $m_P = 1$.

(iii) $d(\Lambda)$ is independent of the choice of the maximal order Λ. Moreover, $m_P > 1$ implies that $P|d(\Lambda)$. ■

Proposition 3.9: Let P be a prime ideal of R and Γ be an R-order such that Γ_P is not a maximal R_P-order. Then there exists an ideal $\mathcal{I} \geq P\Gamma$ of Γ for which $\mathcal{O}_l(\mathcal{I}) > \Gamma$. ■

Remark 3.2: The algebra $\mathbf{H}$ can also be viewed as a cyclic division algebra. As it is a subring of the Hamiltonian quaternions, its center consists of the intersection $\mathbf{H} \cap \mathbf{R} = \mathbf{Q}(\sqrt{2})$. Also $\mathbf{Q}(\xi)$ is an example of a splitting field of $\mathbf{H}$. In the notation above we have an obvious isomorphism

$$\mathbf{H} \simeq (\mathbf{Q}(\xi)/\mathbf{Q}(\sqrt{2}), \sigma, -1),$$

where σ is the usual complex conjugation.

Next we prove that the lattice $\mathbf{L}_{E_8} = \mathcal{H}(1+\xi)$ is optimal within the cyclic division algebra $\mathbf{H}$ in the sense that it corresponds to a proper ideal of a maximal order in $\mathbf{H}$.

Proposition 3.10: The ring

$$\mathcal{H} = \{q = c_1 + \xi c_2 + jc_3 + j\xi c_4 \mid c_1, \ldots, c_4 \in \mathbf{Q}(i),$$
$$(1+i)c_t \in \mathbf{Z}[i]\ \forall t, c_1 + c_3, c_2 + c_4 \in \mathbf{Z}[i]\}$$

is a maximal $\mathbf{Z}$-order of the division algebra $\mathbf{H}$.

Proof: Clearly the $\mathbf{Q}$-span of $\mathcal{H}$ is the whole algebra $\mathbf{H}$, and we have seen that $\mathcal{H}$ is a ring, so it is an order of $\mathbf{H}$. Furthermore, if Λ is any order of $\mathbf{H}$, then so is $\Lambda[\sqrt{2}] = \Lambda \cdot \mathbf{Z}[\sqrt{2}]$, as the element $\sqrt{2}$ is in the center of $\mathbf{H}$ (cf. Proposition 3.2). Therefore it suffices to show that $\mathcal{H}$ is a maximal $\mathbf{Z}[\sqrt{2}]$-order. In what follows, we will call rational numbers in the coset $(1/2) + \mathbf{Z}$ half-integers. Assume for contradiction that we could extend the order $\mathcal{H}$ into a larger order $R = \mathcal{H}[q]$ by adjoining the quaternion $q = a_1 + a_2 j$, where the coefficients $a_t = m_{t,0} + m_{t,1}\xi + m_{t,2}\xi^2 + m_{t,3}\xi^3, \quad m_{t,\ell} \in \mathbf{Q}$ for all t, ℓ are elements of the field $\mathbf{Q}(\xi)$. As $\xi - \xi^3 = \sqrt{2}$, and $\overline{\xi} = -\xi^3$, we see that

$$tr(q) = a_1 + \overline{a_1} = 2m_{1,0} + \sqrt{2}(m_{1,1} - m_{1,3}).$$

By Proposition 3.4 this must be an element of $\mathbf{Z}[\sqrt{2}]$, so we may conclude that $m_{1,0}$ must be an integer or a half-integer, and that $m_{1,1} - m_{1,3}$ must be an integer. Similarly

$$tr(q\xi) = -2m_{1,3} + \sqrt{2}(m_{1,0} - m_{1,2})$$

must be an element of $\mathbf{Z}[\sqrt{2}]$. We may thus conclude that all the coefficients $m_{1,\ell},\ \ell = 0,1,2,3$ are integers or half-integers, and that the pairs $m_{1,0}, m_{1,2}$ (resp. $m_{1,1}, m_{1,3}$) must be of the same type, i.e. either both are integers or both are half-integers. A similar study of $tr(qj)$ and $tr(qj\xi)$ shows that the same conclusions also hold for the coefficients $m_{2,\ell},\ \ell = 0,1,2,3$. Because $\mathbf{Z}[\xi] \subseteq \mathcal{H}$, replacing q with any quaternion of the form $q - \omega$, where $\omega \in \mathbf{Z}[\xi]$ will not change the resulting order R. Thus we may assume that the coefficients $m_{1,\ell},\ \ell = 0,1,2,3$ all belong to the set $\{0, 1/2\}$. Similarly, if need be, replacing q with $q - \omega' j$ for some $\omega' \in \mathbf{Z}[\xi]$ allows us to assume that the coefficients $m_{2,\ell},\ \ell = 0,1,2,3$ also all belong to the set $\{0, 1/2\}$. Further replacements of q by $q - \rho$ or $q - \rho\xi$ then permit us to restrict ourselves to the case $m_{2,\ell} = 0$, for all $\ell = 0,1,2,3$. If we are to get a proper extension of $\mathcal{H}$, we are left with the cases $q = (1+i)/2$, $q = \xi(1+i)/2$ and $q = (1+\xi)(1+i)/2$. We immediately see that none of these have reduced norms in $\mathbf{Z}[\sqrt{2}]$, so we have arrived at a contradiction. ■

IV. General algorithm for testing the maximality

The possibilities of the ad hoc methods in the proof of Proposition 3.10 are somewhat limited. It is clearly desirable to have algorithms for constructing and identifying maximal orders.

In the following we shortly describe how the maximality of a given order can be proved in general. A more detailed version of the algorithm can be found in [11]. An algorithm for constructing a maximal order is presented in [12]. Some of the methods therein are implemented in the Magma software [13].

Suppose we are given a central simple algebra $\mathcal{A}$ over F and a finitely generated $\mathcal{O}_F$-order $\Lambda \leq \mathcal{A}$. Let k be a multiple of $d(\Lambda)$ (c.f. Definition 3.6). The following algorithm depicts how the maximality of Λ can be tested (in polynomial time [11] if the discriminant is small).

As the input the algorithm requires two lists. The first list consists of the prime ideals P of $\mathcal{O}_F$ which divide k. The ideals $\mathcal{P}$ of Λ which contain $P\Lambda$ together constitute the second list. Now Λ_P is a maximal $(\mathcal{O}_F)_P$-order if P is not contained in the first list (c.f. Propositions 3.3 and 3.8). We are left with the task of verifying the local maximality at the prime ideals P of the first list. By Propositions 3.8 and 3.9 it then suffices to repeat the algorithm below at each P.

STEP 1 Is there exactly one prime ideal $\mathcal{P}$ of Λ in the second list such that $P\Lambda \leq \mathcal{P}$?

"NO": QUIT, Λ is not maximal.

STEP 2 Is there an integer $t,\ 1 \leq t \leq n$ such that $P\Lambda = \mathcal{P}^t$?

"NO": QUIT, Λ is not maximal.

STEP 3 Does the equality $\{\mathcal{J} |\ \mathcal{J} \supseteq P\Lambda$ ideal of $\Lambda\} = \{\mathcal{P}^i |\ 0 \leq i \leq t\}$ hold?

"NO": QUIT, Λ is not maximal.

STEP 4 Is the left order $\mathcal{O}_l(\mathcal{P}^i) = \Lambda$ for every ideal $\mathcal{P}^i,\ 0 \leq i \leq t$?

"YES": QUIT, Λ is maximal at P.
"NO": QUIT, Λ is not maximal.

If, in the end, Λ turns out to be maximal at each P on the list, then Λ is a maximal $\mathcal{O}_F$-order.

Let us now exemplify the above algorithm.

Example 4.1: In any cyclic algebra where the element γ determining the 2-cocycle in $H^2(E/F)$ happens to be an algebraic integer, we have the following "natural" order

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

where $\mathcal{O}$ is the ring of integers of the field E (= the unique maximal order in E). In the so called Golden Division Algebra (GDA) [4], i.e. the cyclic algebra $(E/F, \sigma, \gamma)$ gotten from the data $E = \mathbf{Q}(i, \sqrt{5})$, $F = Q(i)$, $\gamma = i$, $n = 2$, $\sigma(\sqrt{5}) = -\sqrt{5}$, the natural order Λ is already maximal. As a $\mathbf{Z}[i]$-order Λ has discriminant $25 = 5^2$. Hence the first list consists of the Gaussian primes $2 \pm i$. We only consider the prime $P = 2 + i$, the prime $2 - i$ can be treated similarly. Let $\tau = (1 + \sqrt{5})/2$. The set $\{1, u, \tau, u\tau\}$ is a $\mathbf{Z}[i]$-basis for Λ. Let $\mathbb{F}_q$ denote the finite field of q elements. As $u^2 = -2$ in $\Lambda/P\Lambda$, u defines a field $K = \mathbb{F}_{25}$ and hence, any nontrivial ideal $\mathcal{I}$ of $\Lambda/P\Lambda$ is a vector space over K and the intersection $\mathcal{I} \cap K$ is trivial. The ideal $R = K(\tau + 2)$ is easily seen to be nilpotent and as $dim_{\mathbb{F}_5}(\Lambda/P\Lambda) = 4$, R is the only nontrivial and the only maximal ideal in $\Lambda/P\Lambda$ and thus

$$R = Rad(\Lambda/P\Lambda) = \mathbb{F}_5(\tau + 2) \oplus \mathbb{F}_5 u(\tau + 2).$$

From these facts we can conclude that the second list is $\{P\Lambda, \mathcal{P} = \langle \sqrt{5}, P\Lambda \rangle, \Lambda\}$ (note that $\sqrt{5} = 2(\tau + 2)$) with $\mathcal{P}$ being the unique prime ideal. For more details concerning the computation of the prime ideals in a ring, see [11]. The algorithm now proceeds as follows.

STEP 1 This is now clear as we saw that $\mathcal{P}$ is the only prime ideal in the second list.

STEP 2 We claim that $\mathcal{P}^2 = P\Lambda$. The inclusion $\mathcal{P}^2 \subseteq P\Lambda$ is immediate, so it suffices to prove the reverse inclusion, i.e. $2 + i \in \mathcal{P}^2$. Obviously the squares $(2 + i)^2$, $\sqrt{5}^2 \in \mathcal{P}^2$. The ring $\mathcal{G}$ is a Euclidean domain, hence we have the extended Euclidean algorithm available for calculating gcds. This algorithm produces two Gaussian integers $a,\ b$ such that $a \cdot (2 + i)^2 + b \cdot 5 = 2 + i$ in $\mathcal{G}$. As both summands in the left belong to $\mathcal{P}^2$, we infer that $2 + i$ is also in $\mathcal{P}^2$.

STEP 3 $\mathcal{P}^0 = \Lambda,\ \mathcal{P}^1 = \mathcal{P},\ \mathcal{P}^2 = P\Lambda$.

STEP 4 We have to show that $\mathcal{O}_l(M) = \Lambda$ for all $M \in \{P\Lambda, \mathcal{P}, \Lambda\}$. Note that $\mathcal{O}_l(\mathcal{P}^i) \geq \Lambda$, $1 \leq i \leq t$. By the Proposition 3.7 $\mathcal{O}_l(\Lambda) \subseteq 1^{-1}\Lambda$ as $1 \in \Lambda$. Again according to the Proposition 3.7 $\mathcal{O}_l(M) \subseteq (2+i)^{-1}M$ since we notice that $2 + i \in M\ \forall M$. For the case $M = P\Lambda$ it is now obvious that $\mathcal{O}_l(M) \subseteq \Lambda$. The case $M = \mathcal{P}$ remains. We only have to show that if $X = p + ru + s\sqrt{5} + tu\sqrt{5} \in \mathcal{O}_l(M),\ p, r, s, t \in \mathbf{Q}(i)$, then $2 + i$ does not divide the denominators of p, r, s, t. By considering the elements $X\sqrt{5}$, $X(2+i) \in \mathcal{P}$ we see that this is indeed true, and consequently Λ is maximal at P.

We can now conclude that the natural order of the GDA is already maximal.

V. Simulation results

In order to compare the lattices $\mathbf{L}_{\mathcal{L}}$, $\mathbf{L}_{\mathcal{H}}$, and $\mathbf{L}_{E_8}$ we scale them to the same minimum determinant. When a real scaling factor ρ is used the minimum determinant is multiplied by ρ^2. As all the lattices have rank 8, the fundamental volume is then multiplied by ρ^8. Let us choose the units so that the fundamental volume of $\mathbf{L}_{\mathcal{L}}$ is $m(\mathbf{L}_{\mathcal{L}}) = 1$. Then after scaling $m(\mathbf{L}_{E_8}) = 1/4$. As the density of a lattice is inversely proportional to the fundamental volume, we thus expect the codes constructed within the lattice $\mathbf{L}_{E_8}$ to outperform the codes of the same size within $\mathbf{L}_{\mathcal{L}}$.

Simulations at the rate 2 bits/s/Hz show that the lattice $\mathbf{L}_{E_8}$ wins approximately by 1 dB over the lattice $\mathbf{L}_{\mathcal{L}}$, and by 2 dB over the DAST-lattice.

VI. Conclusions

In this paper, we present new constructions of rate one, full diversity, and energy efficient 4×4 space-time codes arising from the theory of cyclic algebras and maximal orders. By using a maximal order instead of the ring of algebraic integers one can increase the size of the code without losses in the minimum determinant. By choosing a proper ideal of a maximal order, one can further improve the code as the minimum determinant increases. Comparisons with the DAST-code show that our codes provide lower energy and block error rates due to their good minimum determinant and high density.

VII. Acknowledgements

We are indebted to professor Lajos Rónyai for bringing this algorithm to our notice and for explaining it to us in detail.

This research was supported in part by a grant from the Nokia Foundation.

References

[1] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Dense Full-Diversity Matrix Lattices for Four Antenna MISO Channel", in *Proceedings IEEE ISIT 2005*, pp. 1290–1294, September 2005.

[2] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal Algebraic Space-Time Block Codes", *IEEE Transactions on Information Theory*, vol. 48, pp. 628–636, March 2002.

[3] 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.

[4] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: A 2x2 Full-Rate Space-Time Code with Non-Vanishing Determinants", in *Proceedings IEEE ISIT 2004*, Chicago, p. 308, June 27 - July 2, 2004.

[5] 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.

[6] H. Jafarkhani, "A Quasi-Orthogonal Space-Time Block Code", in *Proceedings IEEE WCNC*, vol. 1, pp. 42–45, September 2000.

[7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der mathematischen Wissenschaften #290, Springer-Verlag, NY 1988.

[8] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels", *IEEE Transactions on Information Theory*, vol. 42, pp. 502–518, March 1996.

[9] D. Allcock, "New Complex- and Quaternion-Hyperbolic Reflection Groups", *Duke Mathematical Journal*, vol. 103, pp. 303–333, June 2000.

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

[11] L. Rónyai, "Algorithmic Properties of Maximal Orders in Simple Algebras Over Q", *Computational Complexity 2*, pp. 225–243, 1992.

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

[13] Web page: http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.