Construction of E_8 as a left ideal of the Silver algebra

Carina Alves and Jean-Claude Belfiore

***Abstract*— Silver code was originally discovered in [1-4] for 2×2 multiple-input multiple-output (MIMO) channels. This code can be constructed algebraically from a particular cyclic division algebra, *Silver algebra*. Space-Time Block Codes (STBC) based on an order of a cyclic division algebra of index 2 such that the volume of the Dirichlet's polyhedron of the group of units is small, are better suited for decoding using the method of algebraic reduction since the approximation error is smaller [16]. In this paper we propose a new construction of E_8-lattice from Silver algebra and whose algebraic reduction behaves better than the one of the Golden code.**

***Keywords*— Algebraic reduction, algebraic lattices, cyclic division algebra, space-time codes.**

***Resumo*— O Silver code foi descoberto em [1-4] para canais MIMO com 2 antenas transmissoras e 2 antenas receptoras. Este código pode ser construído algebricamente através de uma determinada álgebra de divisão cíclica, *Silver álgebra*. Códigos espaço-tempo baseados em uma ordem de uma álgebra de divisão cíclica de índice 2, tal que o volume do poliedro de Dirichlet do grupo das unidades é menor, são mais adequados para a decodificação utilizando o método de redução algébrica, uma vez que o erro de aproximação é menor [16]. Neste artigo, nós propomos uma nova construção do reticulado E_8 a partir da Silver álgebra e cuja redução algébrica se comporta melhor do que o Golden code.**

I. Introduction

Signal constellations having a lattice structure have been studied as meaningful tools for transmitting data over both Gaussian and single-antenna Rayleigh fading channels [10].

More recently, the need for higher data transmission has led to consider communication channels using multiple antennas at both transmitter and receiver ends (MIMO stands for multiple input/ multiple output channel).

In the case of Minimum Delay Space-Time code (codewords are now square matrices), maximizing the minimum rank requires that all nonzero codewords are invertible. Recently cyclic division algebras have been introduced in the context of coherent Space-Time coding. These are non-commutative algebras which naturally yield families of invertible matrices, or in other words, linear codes that fulfill the rank criterion.

A 2×2 perfect space-time code for 2×2 MIMO has been proposed in [1], [2], [3], [4] that offers full rate and full diversity. Recently, this code has been named as *Silver code* in [9] and it has normalized minimum determinant $1/\sqrt{7}$, slightly lower than Golden code, but it allows reduced-complexity maximum likelihood decoding [5-6]. It is shown in the literatures that lattice reduction makes decoding easier. Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm is the most widely used due to its polynomial average complexity. In [16], a new reduction approach has been proposed, called *algebraic reduction*.

Algebraic codes such that the volume of the Dirichlet's polyhedron of its units group, $Vol(\mathcal{P}_{\mathcal{O}_1})$, is small are better suited for decoding using the method of algebraic reduction [16] since the approximation error is then reduced.

In this paper we propose to construct the densest lattice 8-dimensional, namely E_8-lattice from a maximal order of the Silver algebra such that $Vol(\mathcal{P}_{\mathcal{O}_1})$ is much smaller than the volume of the polyhedron corresponding to the Golden code algebra studied in [16]. We show some comparisons in terms of the normalized minimum determinant.

This paper is organized as follows: in Section II we present introductory concepts; in Section III we introduce the system model, space-time block codes and lattices; in Section IV we present the Silver algebra; in Section V we present a new construction of E_8 from Silver algebra; in Section VI we present a brief idea concerning algebraic reduction. Finally in Section VII we compute the volume of the Dirichlet polyhedron for the group of units. Section VIII concludes the paper.

II. Cyclic algebras, orders and discriminants

A. Definitions

We consider number field extension $\mathbb{L}/\mathbb{F}$ where $\mathbb{F}$ denotes the base field and $\mathbb{L}^*$ (resp. $\mathbb{F}^*$) denotes the set of the non-zero elements of $\mathbb{L}$ (resp. $\mathbb{F}$).

Let $\mathbb{L}/\mathbb{F}$ be a Galois extension of degree n such that its Galois group $G = Gal(\mathbb{L}/\mathbb{F})$ is cyclic, with generator σ. Choose a element $\gamma \in \mathbb{F}^*$. We construct a non commutative algebra, denoted by $\mathcal{A} = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$, as follows:

$$\mathcal{A} = \mathbb{L} \oplus e\mathbb{L} \oplus e^2\mathbb{L} \oplus \cdots \oplus e^{n-1}\mathbb{L}$$

where $e \in \mathcal{A}$ is an auxiliary generating element subject to the relations

$$xe = e\sigma(x) \text{ for } x \in \mathbb{L} \text{ and } e^n = \gamma.$$

Recall that $\oplus$ denotes a direct sum. Such an algebra is called a *cyclic algebra*. It is a right vector space over $\mathbb{L}$, and as such has dimension $(\mathcal{A} : \mathbb{L}) = n$.

Cyclic algebras naturally provide families of matrices thanks to an explicit isomorphism between the *split* algebra $\mathcal{A} \otimes_{\mathbb{F}} \mathbb{L}$ ($\otimes$ denotes a tensor product) and the algebra $\mathcal{M}_n(\mathbb{L})$, the n-dimensional matrices with coefficients in $\mathbb{L}$.

Carina Alves, Department of Mathematics, Sao Paulo State University, UNESP/Rio Claro-SP, Brazil, carina@rc.unesp.br

Acknowledgements: To FAPESP for financial support 2013/14723-4.

Jean-Claude Belfiore, Department COMELEC, TELECOM-ParisTech, Paris, France, belfiore@telecom-paristech.fr

An element $x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1} \in \mathcal{A}$ has the following standard representation as a matrix

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

We call this representation the *left regular representation*.

Next proposition tells us when a cyclic algebra is a division algebra.

Proposition 1: [18] (Norm Condition): The cyclic algebra $\mathcal{A} = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ of degree n is a division algebra if and only if $\gamma^{n/p}$ is not the norm of some element of $\mathbb{L}^*$ for any prime divisor p of n.

Due to the above proposition, the element γ is often referred to as the *non-norm element*.

The minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a code. In order to get a good lower bound to the minimum determinant it is natural exploit fully the multiplicative structure of the cyclic division algebra, and go with the so-called orders within the algebra.

Definition 1: Suppose that $\mathbb{L}/\mathbb{F}$ is a cyclic extension of algebraic number fields. Let $\mathcal{A} = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ be a cyclic division algebra and let $\gamma \in O_{\mathbb{F}}^*$ be an algebraic integer of $\mathbb{F}$. The $O_{\mathbb{F}}$-module

$$\Lambda = O_{\mathbb{L}} \oplus eO_{\mathbb{L}} \oplus \cdots \oplus e^{n-1}O_{\mathbb{L}}$$

where $O_{\mathbb{L}}$ is the ring of integers of $\mathbb{L}$, is a subring of the cyclic algebra $(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$. We refer to this ring as the *natural order*. Note also that if γ is not an algebraic integer, then $\mathbb{L}$ fails to be closed under multiplication.

The most important algebraic object for the design of lattice codes from algebraic number fields is the ring of algebraic integers. In division algebras, the analogous of this concept is what is called a maximal order. It is showed in [18] that in order to maximize the minimum determinant we have to use maximal orders.

We use the previous notation.

Definition 2: An $O_{\mathbb{F}}$-order $\mathcal{O}$ in $\mathcal{A}$ is a subring of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that $\mathcal{O}$ is a finitely generated module over $O_{\mathbb{F}}$ and generates $\mathcal{A}$ as a linear space over $\mathbb{F}$. $\mathcal{O}$ is said to be *maximal* if it is not properly contained in any other $O_{\mathbb{F}}$-order in $\mathcal{A}$.

Definition 3: Let $m = \dim_{\mathbb{F}} \mathcal{A}$. The discriminant of the $O_{\mathbb{F}}$-order Γ is the ideal $d(\Gamma/O_{\mathbb{F}})$ in $O_{\mathbb{F}}$ generated by the set

$$\{\det(\mathrm{Tr}_{\mathcal{A}/\mathbb{F}}(x_i x_j))_{i,j=1}^m \mid (x_1, \cdots, x_m) \in \mathcal{B}_\Gamma,\, i,j = 1, \cdots, m\}$$

where $\mathcal{B}_\Gamma = \{x_1, \cdots, x_n\}$ is any $O_{\mathbb{F}}$- basis of Γ.

It is readily seen that whenever $\Gamma \subset \mathcal{O}$ are two $O_{\mathbb{F}}$-orders, then $d(\mathcal{O}/O_{\mathbb{F}})$ is a factor of $d(\Gamma/O_{\mathbb{F}})$. It turns out (cf. [17, 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 a maximal one.

III. Space-time block codes and lattices

A. Connection between Space-time block codes and lattices

A lattice is a discrete finitely generated free Abelian subgroup of a real or complex finite-dimensional vector space V, called the ambient space.

Consider a system with n_t transmit antennas and n_r receive antennas. The complex baseband channel, within a single fading block of T symbol durations, can be expressed as:

$$Y_{n_r \times T} = H_{n_r \times n_t} X_{n_t \times T} + W_{n_r \times T}. \qquad (1)$$

The entries of H are i.i.d. complex Gaussian random variables with zero mean and variance per real dimension equal to $\frac{1}{2}$, and W is the Gaussian noise with i.i.d. entries of zero mean and variance N_0. Channel matrix H is supposed to be perfectly known at the receiver. X denotes the transmitted codeword.

The subscripts indicate the corresponding matrix dimensions and will be omitted for simplicity.

Consider the column-wise matrix vectorization function $vec(\cdot)$ which also separates real $\Re(\cdot)$ and imaginary $\Im(\cdot)$ parts as

$$\begin{aligned} vec(Y) = (&\Re(y_{11}), \Im(y_{11}), \cdots, \Re(y_{n_r 1}), \Im(y_{n_r 1}), \cdots, \\ &\cdots, \Re(y_{1T}), \Im(y_{1T}), \cdots, \Re(y_{n_r T}), \Im(y_{n_r T}))^T \end{aligned} \qquad (2)$$

and the complex-to-real matrix conversion $ri(\cdot)$ which replaces each complex entry of a matrix $H = (h_{ij})$ with a 2×2 real matrix

$$\begin{pmatrix} \Re(h_{ij}) & -\Im(h_{ij}) \\ \Im(h_{ij}) & \Re(h_{ij}) \end{pmatrix}.$$

The MIMO channel $Y = HX + W$ can be rewritten as a $2n_tT$ real vector channel $y = \mathcal{H}x + w$, where $y, \mathcal{H}, x$ and w are given by

$$vec(Y) = \begin{pmatrix} ri(H) & & 0 \\ & \ddots & \\ 0 & & ri(H) \end{pmatrix} \times vec(X) + vec(W).$$

The codewords in a STBC correspond to points x in the $N = 2n_tT$ dimensional Euclidean space $\mathbb{R}^N$. When the STBC is a linear infinite code the points x form a lattice Λ defined by some generator matrix R, so that we identify the code with the lattice

$$\mathcal{C}_\infty = \Lambda = \{x = Ru : u \in \mathbb{Z}^N\}.$$

A finite code $\mathcal{C} \subseteq \mathcal{C}_\infty$ corresponds to a finite constellation carved from the infinite lattice Λ.

When $n_t = n_r = T = n$ we can reliably encode at most $k = n^2$ information symbols. In this case Λ is said to have full rank. Full-rank lattices yield full-rate space-time codes with the maximum multiplexing gain.

B. System model

We consider a quasi-static 2×2 MIMO system employing a space-time block code (STBC). The received signal is given in (1). We are interested in STBCs that are subsets of a principal ideal of a maximal order $\mathcal{O}$ in a cyclic division algebra $\mathcal{A}$ of index 2 over $\mathbb{F}$ (a quaternion algebra).

C. Determinant of lattices constructed from left ideals

Let $\Lambda_{\mathcal{I}}$ be the $\mathbb{Z}$-lattice obtained from a left ideal $\mathcal{I}$ of a maximal order $\mathcal{O}$. The following result gives the value of its determinant.

Lemma 1: Let $\mathbb{F}$ be an imaginary quadratic field and let $\mathcal{I}$ be a left ideal of a maximal order $\mathcal{O}$ of a cyclic division algebra $\mathcal{A}$ of index 2 over $\mathbb{F}$, with discriminant $\delta_{\mathcal{O}}$. Then

$$\det(\Lambda_{\mathcal{I}}) = (\Im(\theta))^8 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4 \quad (3)$$

where $\{1, \theta\}$ is a basis of $O_{\mathbb{F}}$, $nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I})$ denotes the reduced norm of $\mathcal{I}$ and $\Im(\theta)$ denotes the imaginary part of θ.

Proof: From [18, Lemma 5.1], we know that, if Γ is a free $O_{\mathbb{F}}$-module of rank 4, then

$$\sqrt{\det(\Lambda_\Gamma)} = (\Im(\theta))^4 \cdot |d(\Gamma/O_{\mathbb{F}})|$$

where Λ_Γ is the lattice obtained from Γ and $d(\Gamma/O_{\mathbb{F}})$ is the discriminant of Γ. Now equation (3) can be easily derived since

$$|d(\Gamma/O_{\mathbb{F}})|^2 = N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{A}/\mathbb{F}}(\mathcal{I}))^4.$$

■

D. E_8-lattice

The E_8-lattice has a number of desirable properties. It is the best-known lattice in eight dimensions, in the sense of having the densest packing, highest kissing number and being the best quantizer [11]. It also has an efficient decoding algorithm. The lattice generator matrix is triangular, which makes it suitable for encoding. In addition, the E_8-lattice points are either integers or half-integers; for implementations, this may be more suitable than writing arbitrary values to memory.

E_8 is also suited to communicating binary data since, by construction A, we have

$$\frac{1}{\sqrt{2}} E_8/\mathbb{Z}^8 \simeq (8,4)_{\mathbb{F}_2}$$

where $(8,4)_{\mathbb{F}_2}$ is the extended binary Hamming code of length 8 and dimension 4.

We propose here a new construction of E_8-lattice from Silver algebra $\mathcal{SA}$ (see V).

IV. Silver Algebra

We use the algebraic structure of the Silver algebra to construct the E_8-lattice. For this algebra, $Vol(\mathcal{P}_{\mathcal{O}_1})$ is much smaller than the one of the Golden code algebra.

The Silver algebra [9] is given by, $\mathcal{SA} = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ where $\mathbb{F} = \mathbb{Q}(\sqrt{-7})$ is the center, $\mathbb{L} = \mathbb{F}(i)$ is the maximal subfield, $\gamma = -1$ is the non-norm element and σ is the generator of the Galois group of $\mathbb{L}/\mathbb{F}$ given by,

$$\sigma : \begin{cases} i \to -i \\ \sqrt{7} \to -\sqrt{7} \end{cases}$$

The ring of integers of $\mathbb{L}$ is $O_{\mathbb{L}} = \mathbb{Z}[i, \theta]$, where $\theta = \frac{1+\sqrt{-7}}{2}$. The minimal polynomial of θ is $x^2 - x + 2$.

A tipical element ℓ in the Silver algebra is of the form, $\ell = \ell_0 + e\ell_1$ where $\ell_0, \ell_1 \in \mathbb{L}$ and $e^2 = -1$. The matrix representation of ℓ is given by,

$$X_\ell = \begin{pmatrix} \ell_0 & -\sigma(\ell_1) \\ \ell_1 & \sigma(\ell_0) \end{pmatrix}.$$

Here, the natural order is not maximal order. By using the MAGMA software, we compute a maximal order $\mathcal{O}$ for the Silver code algebra with basis $\{1, i, e, ie\}$. This maximal order $\mathcal{O}$ can be written as

$$\mathcal{O} = \mathbb{Z}[\theta] \oplus i\mathbb{Z}[\theta] \oplus e\mathbb{Z}[\theta] \oplus \left(\frac{1+i+e+ie}{2}\right)\mathbb{Z}[\theta],$$

where

$$e = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The Silver code is given by the set of all matrices of the form,

$$X = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix}$$

where,

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = U \begin{pmatrix} x_3 \\ x_4 \end{pmatrix},$$

and U is a unitary matrix given by,

$$U = \frac{1}{\sqrt{7}} \begin{pmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{pmatrix}.$$

Here $\{x_i\}_{i=1}^4$ are the information symbols drawn from a subset of the Gaussian integers $\mathbb{Z}[i]$. The complex conjugation is denoted by $(\cdot)^*$. It is showed in [9] that the Silver code is a subset of the Silver algebra.

V. Construction of E_8-lattice

Let $\Lambda_{\mathcal{I}}$ be a lattice, where $\mathcal{I}$ is a left ideal of a maximal order $\mathcal{O}$ of $\mathcal{SA}$. A necessary (but not sufficient) condition for $\Lambda_{\mathcal{I}}$ to be isomorphic to $\sqrt{c}E_8$, a scaled version of E_8, is that $\det(\Lambda_{\mathcal{I}}) = c^8$, c an integer. In order to fulfill this condition (see Lemma 1), we need that

$$D_{\mathbb{F}}^4 \cdot N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) \cdot N_{\mathbb{F}/\mathbb{Q}}(nr_{\mathcal{SA}/\mathbb{F}}(\mathcal{I}))^4 = c^8. \quad (4)$$

In this case, $|D_{\mathbb{F}}| = 7$ and $N_{\mathbb{F}/\mathbb{Q}}(\delta_{\mathcal{O}}) = 2^8$. In order to find a left ideal $\mathcal{I}$ of a maximal order $\mathcal{O}$ from $\mathcal{SA}$ with reduced norm 14, we will consider subfields $\mathbb{K}$ of $\mathcal{SA}$.

Subfields of $\mathcal{SA}$ are of the form

$$\mathbb{K} = \mathbb{F}\left(\sqrt{-x_1^2 - x_2^2 - x_3^2}\right).$$

This ideal $\mathcal{I}$ will be the product of two prime ideals $\mathcal{I}_1$ and $\mathcal{I}_2$ in $\mathcal{O}$ with respective absolute norm 7 and 2. So, it is enough to find ideals J_1, $J_2 \in O_{\mathbb{K}}$ such that

$$\begin{cases} 7 = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(J_1)) \\ 2 = N_{\mathbb{F}/\mathbb{Q}}(N_{\mathbb{K}/\mathbb{F}}(J_2)) \end{cases}$$

Thus to construct $\mathcal{I}_1$ we consider $\mathbb{K} = \mathbb{Q}(\sqrt{-7}, \sqrt{-3})$ $(x_1 = x_2 = x_3 = 1)$. In this case J_1 is generated by

$$1/2(2 - 2\omega - \theta),$$

$\omega = \sqrt{-3}$ and $\theta = (1+\sqrt{-7})/2$. After embedding J_1 in $\mathcal{SA}$ and we get a left ideal $\mathcal{I}_1$, generated by

$$(1+\theta) - \theta\left(\frac{1}{2}(1+i+e+ie)\right).$$

Now to construct $\mathcal{I}_2$ we consider $\mathbb{K} = \mathbb{Q}(\sqrt{-7}, \sqrt{-1})$ ($x_1 = 1$ and $x_2 = x_3 = 0$). In this case J_2 is generated by

$$-1 + (-1+\theta)\omega,$$

$\omega = \sqrt{-1}$. After embedding J_2 in $\mathcal{SA}$ and we get a left ideal $\mathcal{I}_2$, generated by

$$-1 + (-1+\theta)i.$$

The left ideal $\mathcal{I} = \mathcal{I}_1\mathcal{I}_2$ then gives a $\mathbb{Z}$-lattice with Gram matrix (after rescaling),

$$G(\Lambda_{\mathcal{I}}) = \begin{pmatrix} 6 & 3 & 0 & -6 & 0 & -3 & 3 & -5 \\ 3 & 12 & 6 & 0 & 3 & 0 & 8 & 6 \\ 0 & 6 & 6 & 3 & 0 & 4 & 3 & 5 \\ -6 & 0 & 3 & 12 & -4 & 0 & -2 & 6 \\ 0 & 3 & 0 & -4 & 6 & 3 & 3 & 4 \\ -3 & 0 & 4 & 0 & 3 & 12 & -1 & 6 \\ 3 & 8 & 3 & -2 & 3 & -1 & 6 & 3 \\ -5 & 6 & 5 & 6 & 4 & 6 & 3 & 12 \end{pmatrix}.$$

This matrix has determinant 1 and all diagonal terms are even integers. So, lattice $\Lambda_{\mathcal{I}}$ is the only even unimodular lattice in dimension 8, E_8. By computer we have verified that the normalized minimum determinant is $\sqrt{2/7}$.

The Golden code also gives the E_8-lattice and the normalized minimum determinant is $1/\sqrt{5}$ [8], while the Silver code gives the $\mathbb{Z}^8$-lattice and the normalized minimum determinant is $1/\sqrt{7}$ [9]. So in terms of the normalized minimum determinant, our code is better than the Silver code and the Golden code.

VI. Algebraic Reduction

In this paper we give a brief idea of the principle of algebraic reduction. For details see [16].

First of all, we normalize the received signal. In the system model (1), the channel matrix H has nonzero determinant with probability 1, and so the system can be rewritten as

$$H = \sqrt{\det(H)}H_1,\ H_1 \in SL_2(\mathbb{C}).$$

Therefore the system is equivalent to

$$Y_1 = \frac{Y}{\sqrt{\det(H)}} = H_1X + W_1.$$

Algebraic reduction consists in approximating the normalized channel matrix H_1 with a unit U of norm 1 of the maximal order $\mathcal{O}$ of the algebra of the considered STBC, that is an element U of $\mathcal{O}$ such that $\det(U) = 1$.

In the general case, the approximation is not perfect, i.e., $H_1 \neq U$, so we must take into account the approximation error E, i.e., $H_1 = EU$.

We have seen that ideally the error term E should be unitary in order to have optimality for the Zero Forcing (ZF) decoder, so we should choose the unit U in such a way that $E = H_1U^{-1}$ is quasi-orthogonal. This requires that Frobenius norm $||E^{-1}||_F^2$ should be minimized[1]:

$$\hat{U} = \underset{\substack{U\in\mathcal{O}\\ \det(U)=1}}{\operatorname{argmin}} \quad ||UH_1^{-1}||_F^2. \tag{5}$$

VII. Computing the volume of the Dirichlet polyhedron for the group of units

In [16] an algebraic reduction technique has been introduced to decode space-time block codes (STBC) based on maximal orders of quaternion algebras. The key idea is to approximate the normalized channel matrix by a unit of the corresponding maximal order, with reduced norm 1. An algorithm to find the nearest unit to the normalized channel matrix was described. The search algorithm is based on the action of $SL_2(\mathbb{C})$ on the 3-dimensional hyperbolic space $\mathbb{H}^3$ [12], [14].

In [16], it has been shown that codes based on quaternion algebras such that the volume of the Dirichlet's polyhedron of its group of unit is small are better suited for algebraic reduction. This volume is known *a priori* and only depends on the choice of the quaternion algebra. Quaternion algebras can be seen as special cases of cyclic algebras.

Theorem 1: [14] (Tamagawa Volume Formula). Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{F}$ such that $\mathcal{A}\otimes_{\mathbb{Q}}\mathbb{R} \cong \mathcal{M}_2(\mathbb{C})$. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$. Then the hyperbolic volume is given by,

$$Vol(\mathcal{P}_{\mathcal{O}^1}) = \frac{1}{4\pi^2}\zeta_{\mathbb{F}}(2)|D_{\mathbb{F}}|^{3/2}\prod_{p|\delta_{\mathcal{O}}}(N_p - 1).$$

where $\mathcal{O}^1 = \{U \in \mathcal{O}^* \mid \det(U) = 1\}$, $\zeta_{\mathbb{F}}$ denotes the Dedekind zeta function[2] relative to the field $\mathbb{F}$, $D_{\mathbb{F}}$ is the discriminant of $\mathbb{F}$, $\delta_{\mathcal{O}}$ is the discriminant of $\mathcal{O}$, p varies among the primes of $O_{\mathbb{F}}$, and $N_p = [O_{\mathbb{F}} : pO_{\mathbb{F}}]$.

In the case of the Golden Code algebra [16], $|D_{\mathbb{Q}(i)}| = 4$, $\zeta_{\mathbb{Q}(i)} = 1.50670301\cdots$ and $Vol(\mathcal{P}_{\mathcal{O}^1}) = 4.885149838\cdots$. In the case of Silver code algebra, $|D_{\mathbb{Q}(\theta)}| = 7$, $\zeta_{\mathbb{Q}(\theta)} = 1.8948414\cdots$, $\delta_{\mathcal{O}} = 2^4$ and $N_p - 1 = 1$ and therefore $Vol(\mathcal{P}_{\mathcal{O}^1}) = 0.88891\cdots$, much smaller than the Golden Code algebra. Therefore the algebraic reduction behaves better when is applied to the Silver algebra than the one of Golden Code.

VIII. Conclusions

In this paper we showed that an ideal of some maximal order of the Silver algebra is well-suited for the algebraic reduction method since the volume of the Dirichlet polyhedron of its group of units is much smaller than the volume of the polyhedron corresponding to the Golden code algebra. This offers the advantage of reduced complexity decoding. Moreover, this left ideal, as a lattice, is also equivalent to E_8, which make this space-time code as dense as possible.

[1] Remark that since $\det(E) = 1$, $||E||_F^2 = ||E^{-1}||_F^2$.

[2] The Dedekind zeta function is defined as $\zeta_{\mathbb{F}}(s) = \sum_I([O_{\mathbb{F}} : I])^{-s}$, where I varies among the proper ideals of $O_{\mathbb{F}}$.

REFERENCES

[1] O. Tirkkonen and A. Hottinen, “Square-matrix Embeddable Space-Time Block Codes for Complex Signal Constellations” *IEEE Trans. on Information Theory*, v.48, n.2, pp.389–395, February 2002.

[2] O. Tirkkonen amd R. Kashaev, “Combined Information an Performance Optimization of Linear MIMO Modulations”, *Proc IEEE Int. Symp. Inform. Theory (ISIT 2002)*, Lausanne, Switzerland, June 2002.

[3] A. Hottinen and O. Tirkkonen, “Precoder Designs for High Rate Space-Time Block Codes”, *in Proc Conf. on Information Sciences and Systems*, Princeton, NJ, March 2004.

[4] A. Hottinen, O. Tirkkonen and R. Wichmann, *Multi Antenna Transciever Techniques for 3G and Beyound*, John Wiley and Sons Ltd., 2003.

[5] J. Paredes, A.B. Gershman, and M. G. Alkhanari, “A 2×2 space-time code with non-vanishing determinants and fast maximum likelihood decoding,” *in Proc IEEE ICASSP* 2007, Honolulu, Hawaii, USA, pp. 877-880, April 2007.

[6] E. Biglieri, Y. Hong, and E. Viterbo, “On fast-decodable space-time block codes,” *IEEE Trans. Information Theory*, v. 55, n. 2, February 2009.

[7] M. Samuel and M. P. Fitz, “Reducing the Detection Complexity by using 2×2 Multi-Srata Space-Time Codes”, *Proc IEEE Int. Symp. Inform. Theory* (ISIT 2007), Nice, France, June 2007.

[8] J.-C. Belfiore, G. Rekaya and E. Viterbo “ The Golden Code: A 2×2 Full Rate Space-Time Code with Non-vanishing Determinant property,” *IEEE Trans. Inform. Theory*, v. 51, n. 4, April 2005.

[9] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, and E. Viterbo, “On the Algebraic Structure of the Silver Code,” *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[10] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore, Good lattice constellations for both Rayleigh fading and Gaussian channels, *IEEE Trans. Inform. Theory*, v.42, n.2, pp. 502–517, 2006.

[11] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups,* Springer-Verlag, 1988.

[12] J. Elstrodt, F. Grunewald, J. Mennicke, *Groups Acting on Hyperbolic Space*, Springer, 1998.

[13] C. Hollanti, J. Lahtonen, H.-f.(F.) Lu, “Maximal Orders in the Design of Dense Space-Time Lattice Codes,” *IEEE Trans. Inform. Theory*, v. 54, n.10, pp. 4493–4510, 2008.

[14] C. Maclachlan, A. W. Reid, *The Arithmetic of Hyperbolic 3-Manifolds*, Springer, 2003.

[15] MAGMA Computational Algebra System, Univ. Sydney, Sydney, Australia [Online]. Available: http://magma.maths.usyd.edu.au/

[16] L. Luzzi, G. R-B. Othman, J-C. Belfiore, “Algebraic Reduction for the Golden Code,” *Advances in Mathematics of Communications,* v.6, n.1, pp. 1–26, 2012.

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

[18] R. Vehkalahti, C. Hollanti, J. Lahtonen, K. Ranto, “On the Densest MIMO Lattices from Cyclic Division Algebras,” *IEEE Trans. Inform. Theory,* v.55, n.8, 3751–3780, 2009.