Space-time codes based on quaternion algebras of small volume

Carina Alves and Jean-Claude Belfiore

***Abstract*— We have seen in [13] a new reduction method for the decoding of 2×2 algebraic space-time codes, called algebraic reduction as been introduced. Algebraic codes such that the volume of the Dirichlet's polyhedron of its units group is small are better suited for decoding using the method of algebraic reduction. In this paper, we propose a new framework for constructing a space-time code whose algebraic reduction behaves better than the one of the Golden code.**

***Keywords*— Algebraic reduction, maximal order, cyclic division algebra, space-time codes.**

***Resumo*— Vimos em [13] um novo método de redução para a decodificação de códigos algébricos espaço-tempo 2×2, chamado redução algébrica como foi introduzido. Códigos algébricos tais que o volume do poliedro de Dirichlet do seu grupo de unidades é menor, são mais adequados para a decodificação usando o método da redução algébrica. Neste artigo, nós propomos uma nova estrutura para a construção de códigos espaço-tempo cuja redução algébrica se comporta melhor do que o código de Ouro.**

***Palavras-Chave*— Redução algébrica, ordem maximal, álgebra de divisão cíclica, códigos espaço-tempo.**

I. Introduction

Wireless communication systems may require new coding techniques to combat the effect of fading channels. This required new algebraic tools, namely division algebras. Division algebras are non-commutative algebras that naturally yield families of fully-diverse codes, thus enabling to design high rate, highly reliable space-time codes.

Up to now, the decoding of algebraic space-time codes has been performed using their lattice representation. We want to find the performance lattice reduction for the lattice generated by the channel + code matrix, [3]. It is shown in the literature 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 [13], a new reduction approach has been proposed, called *algebraic reduction*. Unlike existing decoding techniques, algebraic reduction directly exploits the multiplicative structure of the space-time code in addition to the lattice structure. Its principle is to absorb part of the channel inside the codewords, by approximating normalized channel matrices by codewords.

The algebraic reduction technique has then been extended in [13] to the multiple-input multiple output (MIMO) case for space-time block codes (STBC) based on maximal orders of division algebras. The key idea is to approximate the channel matrix by a unit of the corresponding maximal order.

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

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

For division algebras of index greater than 2, characterizing the unit group remains a difficult problem in computational algebra (see the survey [7]).

However, the situation is much better understood in the case of quaternion algebras (index 2), where the Swan algorithm can be used to find a presentation of the unit group. We focus here, exclusively on the case of 2 transmit and 2 receive antennas. Once a presentation is known, an easy-to-implement algorithm is able to find the best approximation of the channel matrix as a product of the generators [13].

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 [13] since the approximation error is then reduced. This volume is known *a priori* and only depends on the choice of the quaternion algebra. In this paper we propose to build a quaternion 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 [13].

This paper is organized as follows: in Section II we present introductory concepts; in Section III we introduce the system model and a brief idea concerning algebraic reduction; in Section IV we describe the structure of units group; in Section V we present the Tamagawa Volume Formula. Finally, in Section VI we present a new quaternion algebra and generators of the group of units. Section VII concludes the paper.

II. Cyclic algebras, orders and discriminants

A. Definitions

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

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

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

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

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

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

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 need a tool for identifying division algebras among the cyclic algebras. Next proposition tells us when a cyclic algebra is a division algebra.

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

As mentioned in the introduction, characterizing the unit group for division algebras of index greater than 2 is a difficult problem in computational algebra. However, the situation is much better understood in the case of quaternion algebras (index 2). Therefore, we focus here on the case of 2 transmit and 2 receive antennas.

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.

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

$$\Lambda = O_L \oplus eO_L \oplus \cdots \oplus e^{n-1}O_L$$

where O_L is the ring of integers of L, is a subring of the cyclic algebra $(L/K, \sigma, \gamma)$. We refer to this ring as the *natural order*.

We use the previous notation.

Definition 2: An O_K-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_K and generates $\mathcal{A}$ as a linear space over K. $\mathcal{O}$ is said to be *maximal* if it is not properly contained in any other O_K-order in $\mathcal{A}$.

Definition 3: Let $m = dim_K\mathcal{A}$. The discriminant of the O_K-order $\mathcal{O}$ is the ideal $d(\Lambda/O_K)$ in O_K generated by the set

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

where $\mathcal{B}_\mathcal{O} = \{x_1, \cdots, x_n\}$ is any $\mathcal{O}_K-$ basis of $\mathcal{O}$.

It is readily seen that whenever $\mathcal{O} \subset \Gamma$ are two O_K-orders, then $d(\Gamma/O_K)$ is a factor of $d(\mathcal{O}/O_K)$. It 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 a maximal one.

B. Finding Maximal Orders

We already saw that in the case of the Golden algebra the natural order is maximal [18]. So clearly natural orders can be maximal, but this does not always happen.

Recently, maximal orders have been proposed in [5] and [18] as new tools to construct cyclic division algebra based STBC ([17], [11]). It was shown in [18] that in order to maximize the number of codewords in the available signal space, i.e. to maximize the *code density*, one should look for cyclic division algebras having maximal orders with minimal discriminants. Luckily, the minimum determinant of the code does not change when increasing the density in this way. However, the construction of maximal orders is not obvious and involves some advanced number theory.

Maximal orders are difficult to construct by hand. Luckily, the construction algorithm from [6] is implemented in the MAGMA software [9]. This algorithm computes a maximal order $\mathcal{O}$ for a quaternion algebra $\mathcal{A}$.

III. System Model and Algebraic Reduction

A. System model

We consider a quasi-static 2×2 MIMO system employing a space-time block code. The received signal is given by

$$Y = HX + W,\ X, H, Y, W \in M_2(\mathbb{C}) \tag{1}$$

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.

B. Algebraic Reduction

In this paper we give a brief idea of the principle of algebraic reduction. For details see [13].

First of all, we normalize the received signal. In the system model (1), 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]:

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

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

IV. The structure of the group of units

In [13] an algorithm to find the nearest unit U to the normalized channel matrix H_1 with respect to the criterion (2) was described. In order to apply it, we need to understand the structure of the group of units $\mathcal{O}^1 = \{U \in \mathcal{O}^* \mid \det(U) = 1\}$ of the maximal order $\mathcal{O}$.

The search algorithm is based on the action of the group on a suitable space. We use the fact that $\mathcal{O}^1$ is a discrete subgroup of the special linear group $SL_2(\mathbb{C})$, and consider the action of $SL_2(\mathbb{C})$ on the hyperbolic 3-space $\mathbb{H}^3$ ([4],[8]).

We refer to the upper half-space model of $\mathbb{H}^3$:

$$\mathbb{H}^3 = \{(z, r) \mid z \in \mathbb{C},\, r \in \mathbb{R},\, r > 0\}. \tag{3}$$

Given a matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{C}),$$

its action on a point $P = (z, r)$ is defined as $M(z, r) = (z^*, r^*)$ with

$$\begin{cases} z^* = \dfrac{(az+b)(\overline{c}\,\overline{z}+\overline{d}) + a\overline{c}r^2}{|cz+d|^2 + |c|^2 r^2}, \\ r^* = \dfrac{r}{|cz+d|^2 + |c|^2 r^2}. \end{cases}$$

The action of M and $-M$ is the same, so there is an induced action of $PSL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{\mathbb{1}, \text{-}\mathbb{1}\}$.

All the information we will gain about the group $\mathcal{O}^1$ will thus be modulo the equivalence relation $M \sim -M$, we denote by $P\mathcal{O}^1$ its quotient with respect to this relation.

Consider the action of $PSL_2(\mathbb{C})$ on the special point $J = (0, 1) = \mathbf{j}$ which has the following nice property ([4] Proposition 1.7):

$$\forall M \in SL_2(\mathbb{C}),\, ||M||_F^2 = 2\cosh \rho(J, M(J)). \tag{4}$$

As anticipated in Section III, given the normalized channel matrix $H_1 \in SL_2(\mathbb{C})$ we want to find

$$\begin{aligned} \hat{U} &= arg \min_{U \in \mathcal{O}^1} ||UH_1^{-1}||_F^2 \\ &= \arg \min_{U \in \mathcal{O}^1} \cosh(\rho(J, UH_1^{-1}(J))) \\ &= \arg \min_{U \in \mathcal{O}^1} \rho(J, UH_1^{-1}(J)) \\ &= arg \min_{U \in \mathcal{O}^1} \rho(U^{-1}(J), H_1^{-1}(J)) \end{aligned}$$

since U is an isometry.

Remark 1: If $M \in U(2)$ is unitary, then g leaves every point of $\mathbb{H}^3$ fixed ([4] Proposition 1.1). Then by considering for example the mapping $PSL_2(\mathbb{C}) \to \mathbb{H}^3$ that sends M to $M(J)$, one can identify $\mathbb{H}^3$ with the quotient space $PSL_2(\mathbb{C})/U(2)$.

V. Tamagawa Volume Formula

Poincaré's theorem establishes a correspondence between a set of generators of the group and the isometries which map a facet of the polyhedron to another facet. All the polyhedra are isometric, and they cover the whole space $\mathbb{H}^3$, forming a tiling. We want to approach the points into $\mathbb{H}^3$ by the closer unit. Thus, when the volume is smaller the units are closer to each other and therefore the approximation is better. This volume is known *a priori* and only depends on the choice of the algebra $\mathcal{A}$.

Theorem 1: (Tamagawa Volume Formula). Let $\mathcal{A}$ be a quaternion algebra over K 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,

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

In the previous formula, ζ_K denotes the Dedekind zeta function[2] relative to the field K, D_K is the discriminant of K, $\delta_{\mathcal{O}}$ is the discriminant of $\mathcal{O}$, p varies among the primes of O_K, and $N_p = [O_K : pO_K]$, where O_K is the ring of integers of K.

We have seen in [13] that algebraic codes such that $Vol(\mathcal{P}_{\mathcal{O}^1})$ is small are better suited for the method of algebraic reduction. So, we wish to build a quaternion algebra over K, such that $|D_K|$ and ζ_K are as small as possible. Furthermore, as can be seen in Theorem 1, the calculation of $Vol(\mathcal{P}_{\mathcal{O}^1})$ depends on a maximal order of the quaternion algebra. In [13] a quaternion algebra over $K = \mathbb{Q}(i)$ was built. In this case, $|D_{\mathbb{Q}(i)}| = 4$ and $\zeta_{\mathbb{Q}(i)} = 1.50670301\cdots$.

VI. Constructing a space-time code with a small volume

A. The Maximal Order

In this paper we propose to construct a quaternion algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ over $K = \mathbb{Q}(\omega)$, where $\sigma : L \to L$ is the generator of the Galois group of L/K and $\omega = (-1+i\sqrt{3})/2$. The reason we choose $K = \mathbb{Q}(\omega)$ is because $|D_{\mathbb{Q}(\omega)}| = 3$ and $\zeta_{\mathbb{Q}(\omega)} = 1.285190\cdots$ are both smaller than the same quantities for $\mathbb{Q}(i)$. Now, according to Proposition 1, we need to choose $\gamma \in K^*$ which is not a norm of elements of any elements in L and such that $|\gamma| = 1$, which guarantees that the same average energy is transmitted from each antenna and each channel use. This limits the choice to $\gamma = \pm 1,\, \pm\omega,\, \pm\omega^2$. Next Proposition shows that $\gamma = -\omega$ satisfies the norm condition for a suitable extension $L/\mathbb{Q}(\omega)$ which leads to a quaternion algebra of small volume.

Proposition 2: Let $L = \mathbb{Q}(\omega, \theta)$, $\omega = (-1 + i\sqrt{3})/2$ and $\theta = \sqrt{2+\omega}$. Then the element $\gamma = -\omega$ is not a relative norm of any $x \in L$, i.e, $N_{L/\mathbb{Q}(\omega)}(x) \neq -\omega,\, \forall x \in L$.

Proof: See appendix. ∎

Now we can consider the cyclic division algebra (or equivalently quaternion algebra in this case) $\mathcal{A} = (L/\mathbb{Q}(\omega), \sigma, -\omega)$ over L, and we can represent all its elements by 2×2 matrices:

$$\begin{aligned} X &= \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix} + \begin{bmatrix} x_3 & 0 \\ 0 & x_4 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -\omega & 0 \end{bmatrix} \\ &= \begin{bmatrix} x_1 & x_3 \\ -\omega x_4 & x_2 \end{bmatrix}, \end{aligned}$$

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

where $x_1, x_2, x_3, x_4 \in L$.

But here, the natural order is not a maximal order. By using the MAGMA software, we compute a maximal order $\mathcal{O}$ for the quaternion algebra $\mathcal{A}$ with basis $\{1, \theta, e, \theta e\}$. This maximal order $\mathcal{O}$ can be written as

$$\mathcal{O} = \mathbb{Z}[\omega] \oplus \mathbb{Z}[\omega]\theta \oplus \mathbb{Z}[\omega]e \oplus \mathbb{Z}[\omega]\delta$$

where $\delta = \omega + (\omega+1)\theta + (\omega+1)e + \theta e$ and

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

Now we are ready to calculate the value of $\prod_{p|\delta_{\mathcal{O}}} (N_p - 1)$ which is

$$(N_{2\mathbb{Z}[\omega]} - 1) \cdot (N_{(2+\omega)\mathbb{Z}[\omega]} - 1) = 2 \cdot 3 = 6.$$

Therefore, by Theorem 1 $Vol(\mathcal{P}_{\mathcal{O}^1}) = 1.0338314$. This volume is smaller than the one of the Golden Code algebra $(4.885149838\cdots)$.

B. Units and Generators

According to the principle of algebraic reduction we need to approximate the normalized channel matrix with a unit of norm 1 of the maximal order $\mathcal{O}$ of the algebra given above.

Remark 2: The set $\mathcal{O}^1 = \{U \in \mathcal{O}^* \mid \det(U) = 1\}$ is a subgroup of $\mathcal{O}$.

In fact, if U is a unit of the $\mathbb{Z}[\omega]$-order $\mathcal{O}$, then $N_{\mathcal{A}/\mathbb{Q}(\omega)}(U) = \det(U)$ is a unit in $\mathbb{Z}[\omega]$, that is, $\det(U) \in \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$. $\mathcal{O}^1$ is the kernel of the reduced norm mapping

$$N = N_{\mathcal{A}/\mathbb{Q}(\omega)} : \mathcal{O}^* \to \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$$

which is a group homomorphism, thus it is a subgroup of $\mathcal{O}$.

We have that N is surjective since there are elements 1, $e+\omega$, δ, e, ω, $\omega(e+\omega)$ in $\mathcal{O}^*$ such that $N(1) = 1$, $N(e+\omega) = -1$, $N(\delta) = \omega$, $N(e) = -\omega$, $N(\omega) = \omega^2$, $N(\omega(e+\omega)) = -\omega^2$. So $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\} \cong \mathcal{O}^*/\mathcal{O}^1$, and $\mathcal{O}^1$ is a normal subgroup of index 6 of $\mathcal{O}^*$.

Our problem is then reduced to studying the subgroup $\mathcal{O}^1$. In particular, we need to find a presentation of this group: a set of generators S and a set of relations R among these generators. In fact, one can show that $\mathcal{O}^1$ is finitely presentable, that is it admits a presentation with S and R finite.

Here, we also have to find the unitary units which, once multiplied by any other unit will not change the Frobenius norm of that unit. In fact, they have no incidence in the approximation of the normalized channel matrix since the metric we want to minimize is the Frobenius norm. So, after some calculus we found that this set of unitary units was the subgroup $\mathcal{U} = \{\mathbb{1}, \text{-}\mathbb{1}, \mathbf{\Omega}, -\mathbf{\Omega}\}$ where

$$\mathbf{\Omega} = \begin{pmatrix} 0 & \omega \\ -\omega^2 & 0 \end{pmatrix},$$

which is not a normal subgroup of $\mathcal{O}^1$.

We know that the set $\mathcal{U}$ stabilizes $J = (0, 1)$, so we need to consider the action of $PSL_2(\mathbb{C})$ on the point PJ, $P \in SL_2(\mathbb{C})$ such that the stabilize of PJ is $\{\mathbb{1}, \text{-}\mathbb{1}\}$.

Therefore of (4) we have that

$$||UH_1^{-1}||_F^2 = 2\cosh\rho(PJ, PuP^{-1}Ph_1^{-1}P^{-1}(PJ)),$$

that is, the units U and the normalized channel matrix $H_1 \in SL_2(\mathbb{C})$ are conjugated by P.

Considering the point $PJ = (0.00002, 1.00002)$ and the algorithms implemented of [14] using MAGMA software we found a Dirichlet's polyhedron with 26 faces, 72 edges and a set minimal of generators for $P\mathcal{O}^1 = \mathcal{O}^1/\{\mathbb{1}, \text{-}\mathbb{1}\}$ is $\{u, g_1, g_2\}$ where,

$$u = \begin{pmatrix} 0 & \omega \\ -\omega^2 & 0 \end{pmatrix} \quad \text{(unitary unit)}$$

$$g_1 = \begin{pmatrix} -1 - \frac{\theta}{2} - \frac{\omega}{2} - \frac{\theta\omega}{2} & -\frac{1}{2} + \frac{\theta}{2} \\ -1 - \omega + \frac{\theta\omega}{2} - \frac{\omega^2}{2} & -1 + \frac{\theta}{2} - \frac{\omega}{2} + \frac{\theta\omega}{2} \end{pmatrix}$$

$$g_2 = \begin{pmatrix} -\frac{\theta}{2} - \frac{\omega}{2} - \frac{\theta\omega}{2} & \frac{1}{2} + \frac{\theta}{2} - \omega \\ -\omega + \frac{\theta\omega}{2} + \frac{\omega^2}{2} & \frac{\theta}{2} - \frac{\omega}{2} + \frac{\theta\omega}{2} \end{pmatrix}$$

A set of relations among these generators, vertices and action of the generators on the vertices of the Dirichlet polyhedron will be given in a long paper.

C. Simulation result

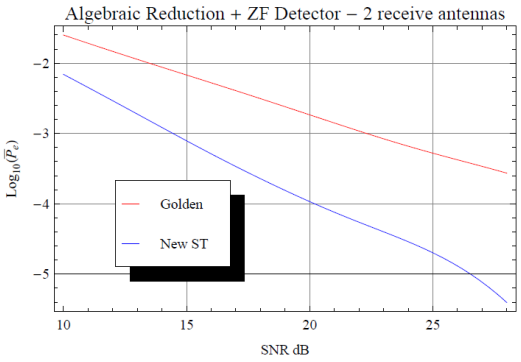

Fig. 1. Performance of algebraic reduction followed by ZF decoder using infinite lattice.

Figure 1 shows the performance of algebraic reduction followed by ZF decoder using infinite lattice by comparing the Golden code and the New code. One can see that there is a significant gain compared to the Golden code.

VII. Conclusion

In this paper we have introduced a new cyclic division algebra based on quaternion algebras and have found a maximal order in this algebra which can be an interesting candidate for space-time coding. For this new algebra, $Vol(\mathcal{P})$ is much smaller than the volume of the polyhedron corresponding to the Golden Code algebra. Algebraic codes such that $Vol(\mathcal{P})$ is smaller are better suited for decoding using the method of algebraic reduction. Our simulation results show that in this case there is a significant gain compared to the Golden

code. The quality of approximation by a unit is related to the maximum radius $R_{\max}$ of the fundamental polyhedron, while The speed of the algorithm depends on the cardinality r of a minimal set of generators for the group. Finding good space-time codes from quaternion algebras such that r and $R_{\max}$ is small is an interesting open problem.

APPENDIX

Proof Proposition 2:

Let $x = a + b\sqrt{2+w} \in L$ with $a, b \in \mathbb{Q}(w)$ then we must show that

$$\begin{aligned} N_{L/\mathbb{Q}(w)}(x) &= (a + b\sqrt{2+w})(a - b\sqrt{2+w}) \\ &= a^2 - b^2(2+w) \neq -w, \end{aligned}$$

i.e., that

$$a^2 - b^2(2+w) = -w \tag{5}$$

has no solution for $a, b \in \mathbb{Q}(w)$. We can lift this equation in the $(2+w)$-adic field $K_{<2+w>}$.

Taking the valuations, $\nu = \nu_{<2+w>}$, in both sides of (5):

$$\nu(a^2 - b^2(2+w)) = \nu(-w) = 0, \tag{6}$$

since w is an unity in $\mathbb{Q}(w)$.

Using the properties of valuation we have that

$$\nu(a^2 - b^2(2+w)) \geq \min\{2\nu(a), 2\nu(b)+1\}.$$

As $2\nu(a) \neq 2\nu(b)+1$ since $2\nu(a)$ is even and $2\nu(b)$ is odd, we have

$$\nu(a^2 - b^2(2+w)) = \min\{2\nu(a), 2\nu(b)+1\} \overset{(6)}{=} 0.$$

So if

$$\min\{2\nu(a), 2\nu(b)+1\} = 2\nu(a),$$

then $\nu(a) = 0$, so $a \in \mathcal{O}_{K_{<2+w>}}$ is a integer as well as b since $2\nu(b)+1 > 0$. The other case is impossible since $2\nu(b)+1$ is odd.

Thus from (5)

$$\begin{aligned} a^2 - b^2(2+w) \bmod(<2+w>) &= -w \bmod(<2+w>) \\ a^2 &= -w \bmod(2+w). \end{aligned} \tag{7}$$

We can rewrite (7) as

$$a^2 \equiv [-(2+w) + 3 - 1] \bmod(<2+w>).$$

Since we have $\mathcal{O}_{K_{<2+w>}} / <2+w> \mathcal{O}_{K_{<2+w>}} \simeq \mathbb{F}_3$,

$$a^2 = -1 \bmod(<2+w>) \text{ in } \mathbb{F}_3.$$

We conclude that -1 should be a square in $\mathbb{F}_3$, which is a contradiction. So $a^2 = -1$ has no solution in $K_{<2+w>}$, but $\mathbb{Q}(w) \subset K_{<2+w>}$ then a^2 has no solution in $\mathbb{Q}(w)$, i.e., (5) has no solution for a, $b \in \mathbb{Q}(w)$.

REFERENCES

[1] J.-C. Belfiore, G. Rekaya and E. Viterbo, *The golden code: a 2 × 2 full-rate space-time code with non-vanishing determinants*, IEEE Trans. Inform. Theory, 51 (2005), 1432-1436.

[2] C. Corrales, E. Jespers, G. Leal, A. del Rio, *Presentations of the unit group of an order in a non-split quaternion algebra*, Advances in Mathematics, 186 n.2 (2004) 498-524.

[3] M. O. Damen, A. Chkeif, and J.-C. Belfiore, *Lattice code decoder for space-time codes*, IEEE Communications Letters, Volume 4, Issue 5, May 2000, Page(s):161 - 163

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

[5] C. Hollanti, J. Lahtonen, an H.-f.(F.) Lu, *Maximal Orders in the Design of Dense Space-Time Lattice Codes*, IEEE Trans. Inform. Theory, 54 (2008).

[6] G. Ivanyos and L. Rónyai, *On the complexity of finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Computat. Complexity, vol. 3, pp. 245-261, 1993.

[7] E. Kleinert, *Units of Classical Orders: A Survey*, L'Enseignement Mathematique, 40 (1994), 205-248.

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

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

[10] A.D. Murugan, H. El Gamal, M. O. Damen, G. Caire, *A unified framework for tree search decoding: rediscovering the sequential decoder*, IEEE Trans. Inform. Theory, vol 52 n. 3, 2006.

[11] F. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo,*Perfect space-time block codes*, IEEE Trans. Inform. Theory, 52 (2006), 3885-3902.

[12] F. Oggier and E. Viterbo. *Algebraic number theory and code design for Rayleigh fading channels.* Foundations and Trends in Communications and Information Theory, vol. 1, 2004.

[13] G.R.-B. Othman, L. Luzzi and J.-C. Belfiore, *Algebraic Reduction for the Golden Code, Advances in Mathematics of Communications*, vol. 6, n. 1, 2012, 1-26.

[14] A. Page, *Computing arithmetic Kleinian groups*,Submitted on 1 Jun 2012. Available: http://www.eleves.ens.fr/home/page/index-en.html

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

[16] G. Rekaya, J.-C. Belfiore and E. Viterbo, *A very efficient lattice reduction tool on fast fading channels*, in Proceedings of ISITA 2004, (2004), Parma, Italy.

[17] B. A. Sethuraman, B. Sundar Rajan and V. Shashidar, *Full-diversity, high-rate space-time block codes from division algebras*, IEEE Trans. Inform. Theory, 49 (2003), 2596-2616.

[18] R. Vehkalahti, C. Hollanti, J. Lahtonen and K. Ranto,*On the Densest MIMO Lattices from Cyclic Division Algebras*, IEEE Trans. Inform. Theory, 55 (2009) 3751-3780.