Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 23–28*

Constructing a space-time code with a small volume

Carina Alves carina@rc.unesp.br
São Paulo State Universtiy - UNESP - Rio Claro, Brasil
Jean-Claude Belfiore belfiore@telecom-paristech.fr
TELECOM-ParisTech - Comelec- Paris, France

Abstract. In this paper we introduce a new quaternion algebra and find a maximal order in this algebra which can be an interesting candidate for space-time coding due to its discriminant and the volume of the Dirichlet's polyhedron of its unit group. 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 small are better suited for decoding using the method of algebraic reduction, [1].

1 Introduction

The use of preprocessing before the search phase in decoders improves the performance of suboptimal decoders, and considerably reduces the complexity of ML decoders. We are interested here in the right preprocessing (reduction) that consists in finding a reduced basis for the lattice generated by the channel code matrix.

In [1], a new reduction approach has been proposed, called *algebraic reduction*. Its principle is to absorb part of the channel inside the codewords, by approximating normalized channel matrices by codewords. The key idea is to approximate the channel matrix with a unit of the corresponding maximal order.

Algebraic codes such that $vol(\mathcal{P})$ is small, where $\mathcal{P}$ is a compact hyperbolic polyhedron, are better suited for the method of algebraic reduction [1] 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 $vol(\mathcal{P})$ is much smaller than the volume of the polyhedron corresponding to the Golden Code algebra studied in [1].

This paper is organized as follows: in Section 2 we present introductory concepts; in Section 3 we present the Tamagawa Volume Formula. Finally, in Section 4 we present a new cyclic division algebra and generators of the group of units. Section 5 concludes the paper.

2 Cyclic algebras, orders and discriminants

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 $xe = e\sigma(x)$ for $x \in L$ 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 algebras $\mathcal{A} \otimes_K L$ and $M_n(L)$.

The next proposition tells us when a cyclic algebra is a division algebra.

Proposition 1. *[2] (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.*

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 analogy 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 $\mathcal{O}_K-$module*

$$\Lambda = \mathcal{O}_L \oplus e\mathcal{O}_L \oplus \cdots \oplus e^{n-1}\mathcal{O}_L$$

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

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

Definition 3. *Let $m = dim_K\mathcal{A}$ and $k = dim_{\mathbb{Q}}K$. The discriminant of the $\mathcal{O}_K$-order is the ideal $d(\Lambda/\mathcal{O}_K)$ in $\mathcal{O}_K$ generated by the set*

$$\{\det(tr_{\mathcal{A}/K}(x_ix_j))_{i,j=1}^m \mid (x_1, \cdots, x_m) \in \Lambda^m\}.$$

Equivalently we can compute the discriminant as

$$d(\Lambda/\mathcal{O}_K) = \det(tr(x_ix_j))_{i,j=1}^m \quad \text{and} \quad d(K/\mathbb{Q}) = \det(tr(x_ix_j))_{i,j=1}^k$$

where $\{x_1, \cdots, x_m\}$ is any $\mathcal{O}_K$-basis of Λ and $\{x_1, \cdots, x_k\}$ is an $\mathbb{Z}$-basis of $\mathcal{O}_K$, respectively.

We already saw that in the case of the Golden algebra the natural order is maximal [2]. So clearly natural orders can be maximal, but this does not always happen. Maximal orders are difficult to construct by hand. Luckily, the construction algorithm from [3] is implemented in the MAGMA software [4]. This algorithm computes a maximal order $\mathcal{O}$ for a quaternion algebra $\mathcal{A}$. In what follows, we will only consider the case of quaternion algebras, which corresponds to a space-time code with two transmit antennas.

3 Tamagawa volume formula

Algebraic reduction consists in approximating the normalized channel matrix 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 $\det(U) = 1$. For details see [1].

The quality of approximation by a unit is related to the diameter $R_{\max}$ of the fundamental polyhedron, while the speed of the algorithm depends on the cardinality r of a minimal set of generators for the group.

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 $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{C})$. Let $\mathcal{O}$ be a maximal order of $\mathcal{A}$. Then the hyperbolic volume is given by,*

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

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 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 $Vol(\mathcal{P})$ depends on a maximal order of the quaternion algebra.

[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.

4 Constructing a space-time code with a small volume

In this paper we propose to construct a quaternion algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ over $K = \mathbb{Q}(w)$, $w = (-1 + i\sqrt{3})/2$ since $|D_{\mathbb{Q}(w)}| = 3$ and $\zeta_{\mathbb{Q}(w)} = 1.285190\cdots$ 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 $\gamma = \pm 1$, $\pm w$, $\pm w^2$. Next Proposition shows that $\gamma = -w$ satisfies the norm condition for a suitable extension $L/\mathbb{Q}(w)$ which leads to a quaternion algebra of small volume.

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

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

$$a^2 - b^2(2 + w) = -w \tag{1}$$

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 (1):

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

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

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 (1)

$$\begin{aligned} a^2 - b^2(2 + w) \bmod(< 2 + w >) &= -w \bmod(< 2 + w >) \\ a^2 &= -w \bmod(< 2 + w >). \end{aligned} \tag{3}$$

We can rewrite (3) 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., (1) has no solution for a, $b \in \mathbb{Q}(w)$. □

Now we can consider the cyclic division algebra (or equivalently quaternion algebra in this case).

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

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

where $\delta = w + (w+1)\theta + (w+1)e + \theta e \quad$ and $e = \begin{pmatrix} 0 & 1 \\ -w & 0 \end{pmatrix}$.

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

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

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

Now 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 1. *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 $\mathbb{Z}[w]$-order $\mathcal{O}$, then $N_{\mathcal{A}/\mathbb{Q}(w)}(u) = \det(u)$ is a unit in $\mathbb{Z}[w]$, that is, $\det(u) \in \{1, -1, w, -w, w^2, -w^2\}$. $\mathcal{O}^1$ is the kernel of the reduced norm mapping $N = N_{\mathcal{A}/\mathbb{Q}(w)} : \mathcal{O}^* \to \{1, -1, w, -w, w^2, -w^2\}$ which is a group homomorphism, thus it is a subgroup of $\mathcal{O}$.

We have that N is surjective then $\{1, -1, w, -w, w^2, -w^2\} \cong \mathcal{O}^*/\mathcal{O}^1$, and $\mathcal{O}^1$ is a normal subgroup of index 6 of $\mathcal{O}^*$. Its cosets can be obtained by multiplying for one of the coset leaders $\{1, -1, w, -w, w^2, -w^2\}$.

So, considering the elements $g \in \mathcal{O}^1$ such that $||g||_F^2 \leq 2 + \sqrt{3}$ we need to look for elements u in $\mathcal{O}^* = \cup_{i=1}^{6} s_i \mathcal{O}^1$, $s_i \in \{1, -1, w, -w, w^2, -w^2\}$ such that $\det(u) = 1$ and $N(u) = 1$.

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 elements is the subgroup $\{\mathbf{1}, \mathbf{-1}, \mathbf{\Omega}, -\mathbf{\Omega}\}$ where $\mathbf{\Omega} = \begin{pmatrix} 0 & w \\ -w^2 & 0 \end{pmatrix}$. Finally, a set of generators for $P\mathcal{O}^1 = \mathcal{O}^1/\{\mathbf{1}, \mathbf{-1}, \mathbf{\Omega}, -\mathbf{\Omega}\}$ is displayed below.

$$u_1 = \begin{pmatrix} \frac{1}{2}(-2+\theta-\omega+\theta\omega) & \frac{1}{2}(-1-\theta-\omega) \\ \frac{1}{2}(-1-\theta\omega) & \frac{1}{2}(-2-\theta-\omega-\theta\omega) \end{pmatrix}$$
$$u_2 = \begin{pmatrix} \frac{1}{2}(-2+\theta-\omega+\theta\omega) & \frac{1}{2}(1-\theta+\omega) \\ \frac{1}{2}(1-\theta\omega) & \frac{1}{2}(-2-\theta-\omega-\theta\omega) \end{pmatrix}$$
$$u_3 = \begin{pmatrix} \frac{1}{2}(\theta-\omega+\theta\omega) & \frac{1}{2}(1-\theta-\omega) \\ \frac{1}{2}(-1-(2+\theta)\omega) & \frac{1}{2}(-\theta-\omega-\theta\omega) \end{pmatrix}$$
$$u_4 = \begin{pmatrix} \frac{1}{2}(\theta-\omega+\theta\omega) & \frac{1}{2}(-1-\theta+\omega) \\ \frac{1}{2}+\omega-\frac{\theta\omega}{2} & \frac{1}{2}(-\theta-\omega-\theta\omega) \end{pmatrix}$$
$$u_5 = \begin{pmatrix} \frac{1}{2}(-1-\theta-\omega) & \frac{1}{2}+\omega-\frac{1}{2}\theta(2+\omega) \\ \frac{1}{2}(2+\theta+\omega-\theta\omega) & \frac{1}{2}(-1+\theta-\omega) \end{pmatrix}$$
$$u_6 = \begin{pmatrix} \frac{1}{2}(-1+\theta-\omega) & \frac{1}{2}+\omega-\frac{1}{2}\theta(2+\omega) \\ \frac{1}{2}(2+\theta+\omega-\theta\omega) & \frac{1}{2}(-1-\theta-\omega) \end{pmatrix}$$

From the Dirichlet polyedron of a Kleinian group one can obtain a complete description of the latter, including generators and relations.

Due to lack of space, a set of relations among these generators and action of the generators on the vertices of the Dirichlet polyhedron will be given in a future work.

5 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, which allows a more efficient algebraic reduction of the code.

References

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

[2] 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.

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

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