Higher dimensional perfect space-time coded modulation

Oggier, Frederique; Sole, Patrick

2009

Oggier, F. & Sole, P. (2009). Higher dimensional perfect space-time coded modulation. Information Theory Workshop, Sicily 2009: (pp.1-4).

<https://hdl.handle.net/10356/90920>

Higher Dimensional Perfect Space-Time Coded Modulation

Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

Patrick Solé
CNRS, I3S,
Les Algorithmes B,
2000, route des Colles
06 903 Sophia Antipolis,
France
Email: sole@unice.fr

Abstract—We address the problem of designing coset codes for use over slow block fading MIMO channel. We consider as inner code different codes built over cyclic algebras (in particular for different number of antennas), and show that two alternative approaches for the outer code are either codes on cyclic algebras over finite fields, or error correcting codes over finite fields.

I. INTRODUCTION

We consider the problem of coding over a slow block fading MIMO channel, for example in a mobile wireless setting, where the channel is assumed to be fixed over the duration of a frame. Compared to standard MIMO channels, slow fading induces a loss in diversity, which can be compensated by using concatenated coding schemes, as for example space-time trellis codes [12]. Finer concatenated schemes enable to distinguish the two main design criteria, namely the rank and determinant criteria: an inner code guarantees full diversity, while combining with an outer code brings coding gain. Any fully diverse space-time code can be used as inner code, but in this work, we will focus on codes built over cyclic division algebras [10], [7] whose algebraic structure is easier to analyze.

A. Prior work

Most attempts in the literature to obtain coded modulation schemes for algebraic space-time codes focused on having the so-called Golden code [2] as inner code. In the first attempt [3], the Golden code was concatenated with an outer trellis code, whose drawback is its high trellis complexity. Trellis coded modulation using a set partitioning of the Golden code is studied in [5], where a systematic design approach is proposed: partitions of the Golden code with increasing minimum determinant correspond to $\mathbb{Z}^8$ lattice partitions, which are labeled by using a sequence of nested binary codes. In [6], the algebraic structure of the Golden code partitions is investigated, and the authors show that they are actually dealing with matrices over the finite field $\mathbb{F}_2$, or over the finite ring $\mathbb{F}_2[i]$. The problem becomes thus the one of designing a suitable outer code over the given ring of matrices, for which only two examples are given: one repetition code of length 2, and one ad hoc construction using Reed Solomon codes.

In [8], a general code construction over $\mathcal{M}_2(\mathbb{F}_2)$ has been proposed, following a new design criterion.

B. Contribution and organization

In this paper, we introduce a general setting for considering as inner code not only the Golden code, but also higher dimensional codes built over division algebras. Our main contribution is two-fold: first we generalize the analysis of [6] by studying coset codes in higher dimensions. Second, we give a new interpretation of what those coset codes really are in terms of cyclic algebras over finite fields. This is particularly nice since it then allows us to further connect to more familiar objects, namely error correcting codes over finite fields, which generalizes the approach of [8].

This paper is organized as follows. In Section II, we recall the background on cyclic algebras. In Section III, coset codes of cyclic algebra codes are built, where we show that they are codes on matrices over finite fields, which in turn are proven to be codes over cyclic algebras over finite fields in Section IV. This representation allows us to go one step further, and relate coset codes to more traditional codes over finite fields, as explained in Section V.

II. BACKGROUND

Let us start by recalling what is the code design problem addressed.

A. Code design criterion

For a slow block fading channel, where the fading coefficients are assumed to be constant for L time blocks, the goal is to design a codebook $\mathcal{C}$ of codewords

$$\mathbf{X} = (X_1, \dots, X_L), \quad X_i \in \mathcal{S}$$

for $i = 1, \dots, L$, where $\mathcal{S}$ is a set of codewords from a fully diverse space-time codebook, such that the minimum determinant Δ_{min} of $\mathcal{C}$ given by

$$\Delta_{min} = \min_{\mathbf{X} \neq \mathbf{0}} \det(\mathbf{X}\mathbf{X}^*)$$

is maximized. For this paper, $\mathcal{S}$ will be a set of $n \times n$ perfect space-time codewords [7], [11]. These codes are not only fully diverse, they further offer a good minimum determinant, independently of the size of the signal constellation.

B. Cyclic algebras

Let us briefly recall the definition of codes built over cyclic algebras, introduced in [10], since perfect space-time codes that are of interest for this work are a subclass.

Definition 1: Let L/K be a cyclic extension of degree n , with Galois group $\text{Gal}(L/K) = \langle \sigma \rangle$, where σ is the generator of the cyclic group. Let $\mathcal{A} = (L/K, \sigma, \gamma)$ be its corresponding cyclic algebra of degree n , that is

$$\mathcal{A} = 1 \cdot L \oplus e \cdot L \oplus \dots \oplus e^{n-1} \cdot L$$

with $e \in \mathcal{A}$ such that $le = e\sigma(l)$ for all $l \in L$ and $e^n = \gamma \in K$, $\gamma \neq 0$.

Note that L/K is a priori any cyclic field extension. In this paper, we will focus on both number field extensions, as well as finite field extensions.

One can associate a matrix to any element $x \in \mathcal{A}$ using the map λ_x , the multiplication by x of an element $y \in \mathcal{A}$:

$$\begin{aligned} \lambda_x : \mathcal{A} &\rightarrow \mathcal{A} \\ y &\mapsto \lambda_x(y) = x \cdot y. \end{aligned}$$

The matrix of the multiplication by λ_x , with

$$x = x_0 + ex_1 + \dots + e^{n-1}x_{n-1},$$

is given by

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \dots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \dots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \dots & \gamma\sigma^{n-2}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \dots & \sigma^{n-1}(x_0) \end{pmatrix}. \quad (1)$$

Perfect codes [7] are codes built over cyclic division algebras, with in particular the property that their minimum determinant is lower bounded by a constant independent of the size of the signal constellation. This can be achieved by considering the subset of elements $x = x_0 + ex_1 + \dots + e^{n-1}x_{n-1}$, x_i in $\mathcal{O}_L$ instead of L , $k = 1, \dots, n$, where $\mathcal{O}_L$ denote the ring of integers of L . In other words, we consider the subset $\Lambda \subset \mathcal{A}$ given by

$$\Lambda = 1 \cdot \mathcal{O}_L \oplus e \cdot \mathcal{O}_L \oplus \dots \oplus e^{n-1} \cdot \mathcal{O}_L,$$

which is actually an order of $\mathcal{A}$, as identified in [4].

For the case of interest to us, K is typically $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity, to allow the use of either QAM or HEX symbols. Since their respective rings of integers $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ are principal ideal domains, it makes sense to speak of an $\mathcal{O}_K$ -basis for $\mathcal{O}_L$. We can now be more precise, and recall that for R a Noetherian integral domain with quotient field K , and $\mathcal{A}$ a finite dimensional K -algebra, we have the following definition.

Definition 2: An R -order in the K -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 K . An order Λ is called *maximal* if it is not properly contained in any other R -order.

n	L/K	$\mathcal{O}_L$
2	$\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$	$\mathbb{Z}[i, (1 + \sqrt{5})/2]$
3	$\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\zeta_3)$	$\mathbb{Z}[\zeta_3, \zeta_7 + \zeta_7^{-1}]$
4	$\mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i)$	$\mathbb{Z}[i, \zeta_{15} + \zeta_{15}^{-1}]$

TABLE I
ORDERS CORRESPONDING TO SOME PERFECT CODES

In the cyclic algebra $\mathcal{A}$, we can always choose the elements $0 \neq \gamma \in K$ to be an algebraic integer (we are not speaking of division algebras for now). We see that the order Λ given above is more precisely an $\mathcal{O}_K$ -order in $\mathcal{A}$.

In Table I, we can see the orders Λ corresponding to the codes from [7], for dimensions 2,3 and 4.

The table reads that for an $n \times n$ space-time block code, the cyclic field extension used to construct the cyclic algebra $\mathcal{A}$ is L/K , and the order Λ in $\mathcal{A}$ is given by $\Lambda = 1 \cdot \mathcal{O}_L \oplus e \cdot \mathcal{O}_L \oplus \dots \oplus e^{n-1} \cdot \mathcal{O}_L$.

III. COSET CODES

Let us now recall what are the codes of interest here. We are looking for a codebook $\mathcal{C}$ of codewords

$$\mathbf{X} = (X_1, \dots, X_L), \quad X_i \in \mathcal{S}$$

for $i = 1, \dots, L$, where $\mathcal{S}$ is a set of codewords from codes given for example in Table I, such that

$$\Delta_{\min} = \min_{\mathbf{X} \neq \mathbf{0}} \det(\mathbf{X}\mathbf{X}^*)$$

is maximized. It is known that choosing the blocks X_i independently does not bring coding gain. This is remedied by using outer codes, or more particularly in this setting, coset codes, as proposed in [6]. Consider the projection

$$\begin{aligned} \pi : \mathcal{S} &\rightarrow \mathcal{S}/\mathcal{I} \simeq R \\ g &\mapsto \pi(g) \end{aligned}$$

where $\mathcal{I}$ is a two-sided ideal of $\mathcal{S}$ seen as a ring, so that the quotient $\mathcal{S}/\mathcal{I} \simeq R$ is a ring. We now take a code $\tilde{\mathcal{C}}$ over R . The coset code $\mathcal{C}$ is obtained by considering $\pi^{-1}(\tilde{\mathcal{C}})$.

To be more precise, when $\mathcal{S}$ is a set of codewords coming from division algebras, we can really consider Λ , an order of the algebra as defined in Definition 2, which has a ring structure.

The $\mathcal{O}_K$ -order Λ of $\mathcal{A}$ is a free module over $\mathcal{O}_k = \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, with basis $\{b_i\}$, $i = 1, \dots, n^2$:

$$\Lambda \simeq \bigoplus_{i=1}^{n^2} \mathcal{O}_K b_i,$$

since for us $\mathcal{O}_L$ is a free $\mathcal{O}_K$ -module of rank n (say with basis β_k , $k = 1, \dots, n$):

$$\begin{aligned} \Lambda &\simeq \bigoplus_{j=1}^n e^j \mathcal{O}_L \\ &\simeq \bigoplus_{j=1}^n e^j \bigoplus_{k=1}^n \beta_k \mathcal{O}_K. \end{aligned}$$

The basis vectors $\{b_i\}$ are thus given by

$$\{e^j \beta_k\}, \quad j, k = 1, \dots, n.$$

Let $\mathfrak{a}$ be a two sided ideal of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is commutative, we have that

$$\Lambda/\mathfrak{a}\Lambda \simeq \bigoplus_{i=1}^{n^2} \mathcal{O}_K b_i / \mathfrak{a} b_i$$

is a free module over the ring $\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$, with basis $\{\pi(b_i)\}$, $i = 1, \dots, n^2$, where π is the canonical projection

$$\pi : \Lambda \rightarrow \Lambda/\mathfrak{a}\Lambda.$$

The above considerations mean the following for our setting.

Lemma 1: For $n = 2, 3, 4$ respectively, we have:

- 1) If $\Lambda = \mathbb{Z}[i, (1 + \sqrt{5})/2] + e\mathbb{Z}[i, (1 + \sqrt{5})/2]$, $\mathfrak{a} = (1 + i)$, then

$$\mathbb{Z}[i]/\mathfrak{a}\mathbb{Z}[i] \simeq \mathbb{F}_2$$

and $\Lambda/\mathfrak{a}\Lambda$ is a $\mathbb{F}_2$ -module of rank 4. In particular, we have that

$$|\Lambda/\mathfrak{a}\Lambda| = 2^4.$$

- 2) If $\Lambda = \mathbb{Z}[\zeta_3, \zeta_7 + \zeta_7^{-1}] + e\mathbb{Z}[\zeta_3, \zeta_7 + \zeta_7^{-1}] + e^2\mathbb{Z}[\zeta_3, \zeta_7 + \zeta_7^{-1}]$, $\mathfrak{a} = 2$, then

$$\mathbb{Z}[\zeta_3]/\mathfrak{a}\mathbb{Z}[\zeta_3] \simeq \mathbb{F}_2^2$$

and $\Lambda/\mathfrak{a}\Lambda$ is a $\mathbb{F}_4$ -module of rank 9. In particular, we have that

$$|\Lambda/\mathfrak{a}\Lambda| = 4^9.$$

- 3) If $\Lambda = \mathbb{Z}[i, \zeta_{15} + \zeta_{15}^{-1}] + e\mathbb{Z}[i, \zeta_{15} + \zeta_{15}^{-1}] + e^2\mathbb{Z}[i, \zeta_{15} + \zeta_{15}^{-1}] + e^3\mathbb{Z}[i, \zeta_{15} + \zeta_{15}^{-1}]$, $\mathfrak{a} = (1 + i)$, then

$$\mathbb{Z}[i]/\mathfrak{a}\mathbb{Z}[i] \simeq \mathbb{F}_2$$

and $\Lambda/\mathfrak{a}\Lambda$ is a $\mathbb{F}_2$ -module of rank 16. In particular, we have that

$$|\Lambda/\mathfrak{a}\Lambda| = 2^{16}.$$

Note that 2 is prime in $\mathbb{Z}[\zeta_3]$, while 2 splits as $2 = (1 + i)(1 - i)$ in $\mathbb{Z}[i]$.

This yields that

Proposition 1: We have

$$\begin{aligned} \Lambda/\mathfrak{a}\Lambda &\simeq \mathcal{M}_n(\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K) \\ &\simeq \begin{cases} \mathcal{M}_2(\mathbb{F}_2) & \text{for } n = 2 \\ \mathcal{M}_3(\mathbb{F}_4) & \text{for } n = 3 \\ \mathcal{M}_4(\mathbb{F}_2) & \text{for } n = 4 \end{cases} \end{aligned}$$

Proof: By the previous lemma, we already know that $\Lambda/\mathfrak{a}\Lambda$ is a $\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$ -module whose cardinality is the same as $\mathcal{M}_n(\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K)$. It is thus enough to give a ring homomorphism $\psi : \Lambda/\mathfrak{a}\Lambda \rightarrow \mathcal{M}_n(\mathcal{O}_K/\mathfrak{a}\mathcal{O}_K)$ which is one-to-one to conclude. ψ can be defined by mapping the basis vectors $\pi(e^j \beta^k)$. ■

The particular case for $n = 2$ was proved in [6]. The meaning of this proposition is that we now need to build codes on matrices over finite fields or finite rings. For the case of finite fields, we prove in the next section that an alternative way of seeing things is to ask for codes on cyclic divisions over finite fields.

IV. CYCLIC ALGEBRAS OVER FINITE FIELDS

Let $\mathbb{F}_2$ be the finite field with 2 elements, and consider the field extension $\mathbb{F}_{2^n}/\mathbb{F}_2$ of degree n , that is $\mathbb{F}_{2^n} \simeq \mathbb{F}_2(w)$ with $p(w) = 0$ and $p \in \mathbb{F}_2[X]$ is an irreducible polynomial of degree n . Its cyclic Galois group is generated by the Frobenius automorphism $\sigma : w \mapsto w^2$. We consider the cyclic algebra $\mathcal{A} = (\mathbb{F}_{2^n}/\mathbb{F}_2, \sigma, 1)$, with

$$\mathcal{A} \simeq \mathbb{F}_{2^n} \oplus \dots \mathbb{F}_{2^n} e \oplus \mathbb{F}_{2^n} e^{n-1}$$

(see Definition 1). We know by Lemma 2.16 in [9] that $\mathcal{A} \simeq \text{End}_{\mathbb{F}_2}(\mathbb{F}_{2^n})$. The isomorphism $j : \mathcal{A} \rightarrow \text{End}_{\mathbb{F}_2}(\mathbb{F}_{2^n})$ is explicitly given by $:j(a)$ is the multiplication by a for all a in $\mathbb{F}_{2^n}$, and $j(e) = \sigma$. Indeed, we have that

$$\begin{aligned} j(ea)(x) &= (j(e)j(a))(x) \\ &= j(e)(ax) \\ &= \sigma(ax) \\ &= \sigma(a)\sigma(x) \\ &= j(\sigma(a))\sigma(x) \\ &= j(\sigma(a)e)(x) \end{aligned}$$

thus $j(ea) = j(\sigma(a)e)$.

Example 1: We consider the cyclic algebra $\mathcal{A} = (\mathbb{F}_8/\mathbb{F}_2, \sigma, 1)$, where $\mathbb{F}_8 \simeq \mathbb{F}_2(w)$ with $w^3 + w + 1 = 0$ and $\sigma : w \mapsto w^2$. As a vector space, we have $\mathcal{A} \simeq \mathbb{F}_8 \oplus \mathbb{F}_8 e \oplus \mathbb{F}_8 e^2$ and multiplication is given by $ea = \sigma(a)e$ for $a \in \mathbb{F}_8$. We have that $\mathcal{A} \simeq \mathcal{M}_3(\mathbb{F}_2)$. The isomorphism is given as follows:

$$\begin{aligned} e &\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \\ a_0 + a_1 w + a_2 w^2 &\mapsto \begin{pmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 + a_2 & a_1 + a_2 \\ a_2 & a_1 & a_0 + a_2 \end{pmatrix}. \end{aligned}$$

It is a straightforward computation to check that

$$\begin{aligned} e(a_0 + a_1 w + a_2 w^2) &= \sigma(a_0 + a_1 w + a_2 w^2)e \\ &= (a + bw^2 + c(w^2 + w))e. \end{aligned}$$

Example 2: Consider now the cyclic algebra $\mathcal{A} = (\mathbb{F}_{16}/\mathbb{F}_2, \sigma, 1)$, where $\mathbb{F}_{16} \simeq \mathbb{F}_2(w)$ with $w^4 + w^2 + 1 = 0$ and $\sigma : w \mapsto w^2$. We have that $\mathcal{A} \simeq \mathcal{M}_4(\mathbb{F}_2)$. The isomorphism is given as follows:

$$\begin{aligned} e &\mapsto \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ w &\mapsto \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{aligned}$$

The above example gives us an explicit isomorphism

$$\mathcal{M}_4(\mathbb{F}_2) \simeq \mathbb{F}_{16} \oplus \mathbb{F}_{16} e \oplus \mathbb{F}_{16} e^2 \oplus \mathbb{F}_{16} e^3.$$

V. ERROR CORRECTING CODES

Let us continue our sequence of isomorphisms, and now connect codes on cyclic algebras over finite fields to classical error correcting codes.

The isomorphism

$$\mathcal{A} \simeq \mathbb{F}_{2^n} \oplus \dots \mathbb{F}_{2^n} e \oplus \mathbb{F}_{2^n} e^{n-1} \simeq \mathcal{M}_n(\mathbb{F}_2)$$

clearly induces an isomorphism of $\mathbb{F}_2$ -left vector space

$$\phi : \underbrace{\mathbb{F}_{2^n} \times \dots \times \mathbb{F}_{2^n}}_n \rightarrow \mathcal{M}_n(\mathbb{F}_2).$$

Example 3: Let $\mathbb{F}_2$ be the finite field with 2 elements, and $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ be the finite field with 4 elements, where $\omega^2 + \omega + 1 = 0$. We have a ring isomorphism (as described in the above section) given by

$$\mathcal{M}_2(\mathbb{F}_2) \simeq \mathbb{F}_2(\omega) + \mathbb{F}_2(\omega)e$$

where $e^2 = 1$ and $e\omega = \bar{\omega}e = \omega^2e$, which is explicitly given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto e, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto \omega.$$

It in turn induces an isomorphism of $\mathbb{F}_2$ left vector space

$$\phi : \mathbb{F}_4 \times \mathbb{F}_4 \rightarrow \mathcal{M}_2(\mathbb{F}_2).$$

We have that ϕ maps a pair $(a, b) \in \mathbb{F}_4 \times \mathbb{F}_4$ to a matrix in $\mathcal{M}_2(\mathbb{F}_2)$. To be completely explicit, note that for $a, b \in \mathbb{F}_2$,

$$a + \omega b \mapsto \begin{pmatrix} a & b \\ b & a + b \end{pmatrix},$$

so that

$$(a + b\omega, c + d\omega) \mapsto \begin{pmatrix} a & b \\ b & a + b \end{pmatrix} + \begin{pmatrix} c & d \\ d & c + d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2)$$

$$= \begin{pmatrix} a + d & b + c \\ b + c + d & a + b + d \end{pmatrix}. \quad (3)$$

Also, ϕ can be extended to m -tuples

$$\phi : (\mathbb{F}_{2^n} \times \dots \times \mathbb{F}_{2^n})^m \rightarrow \mathcal{M}_n(\mathbb{F}_2)^m$$

so that if $\pi(\mathcal{C})$ is a code of length m over $\mathcal{M}_n(\mathbb{F}_2)$, then $\phi^{-1}(\pi(\mathcal{C}))$ is a code of length $2m$ over $\mathbb{F}_{2^n}$.

This connection with classical codes has been introduced first in [1] for the construction of particular lattices, and recently in [8], for applications to space-time modulation in the case where the inner code is the Golden code (that is $n = 2$).

VI. CODE CONSTRUCTIONS: CURRENT AND FUTURE WORK

In this paper, what we have done is to prove different characterizations of coset codes coming from cyclic algebras. We are still left as (current and) future work to exhibit explicit families of codes, that satisfy the design criterion of maximizing the minimum determinant $\Delta_{\min}$. It was proved in [6] for $n = 2$ (that is the Golden code) that

$$\Delta_{\min} \geq \min(4\delta, d_{\min}^2 \delta), \quad \mathcal{I} = (1 + i),$$

where $d_{\min}$ is the minimum Hamming distance of the code over $\mathcal{M}_2(\mathbb{F}_2)$, and $\delta = 1/5$ is the minimum determinant of the Golden code. This result can be readily generalized. For example, for $n = 4$ (that is for the construction of 4×4 code considered here), we have that

$$\Delta_{\min} \geq \min(16\delta, d_{\min}^2 \delta), \quad \mathcal{I} = (1 + i).$$

Trivial code constructions as the repetition code proposed in [6] are of course available for $n = 4$. In order to meet the bound, we can consider the repetition code of length 4 over $\mathcal{M}_4(\mathbb{F}_2)$. Questions to address the improvement of code constructions are as follows: How to design families of codes over $\mathcal{M}_n(\mathbb{F}_2)$ with good Hamming distance? What if we further would like to get a good rate? A new bound on $\Delta_{\min}$ has been proposed in [8], based on a different distance than the Hamming distance. Can this distance be generalized to higher dimensions, and if so, what are the corresponding codes? The two approaches should be compared, and simulation results should be provided, especially since the bounds on the minimum determinant are loose. Finally, if one would like to increase the minimum determinant, all the above questions hold while this time working over finite rings rather than finite fields.

ACKNOWLEDGMENTS

The research of F. Oggier is supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

REFERENCES

- [1] C. Bachoc, "Applications of coding theory to the construction of modular lattices" *J. Comb. Th A* 78-1 (1997) 92-119.
- [2] J.-C. Belfiore, G. Rekaya, E. Viterbo, "The Golden Code: a 2×2 full-rate space-time code with non-vanishing determinants", *IEEE Trans. on Information Theory*, vol. 51, no 4, 2005
- [3] D. Champion, J.-C. Belfiore, G. Rekaya, E. Viterbo, "Partitioning the Golden Code: a framework to the design of space-time coded modulation", *Canadian Workshop on Information Theory*, 2005.
- [4] C. Hollanti, J. Lathonen, K. Ranto, R. Vekhalahiti, "On the Densest MIMO Lattices from Cyclic Division Algebras", submitted, available at arxiv.org/abs/cs.IT/0703052.
- [5] Y. Hong, E. Viterbo, J.-C. Belfiore, "Golden Space-Time trellis coded modulation", *IEEE Trans. on Information Theory*, vol. 53, no 5, 2007.
- [6] L. Luzzi, G. Rekaya-Ben Othman, J.-C. Belfiore and E. Viterbo, "Golden Space-Time Block Coded Modulation," submitted to *IEEE Transactions on Information Theory*, available on [arXiv 0805.4502](http://arXiv.org/abs/0805.4502)
- [7] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. on Information Theory*, vol. 52, no 9, 2006.
- [8] F. Oggier, P. Solé, J.-C. Belfiore, "Codes over $\mathcal{M}_2(\mathbb{F}_2)$ and applications to Golden Space-Time Coded Modulation", *ISIT 09*.
- [9] W. Scharlau, "Quadratic and Hermitian Forms", *Springer-Verlag*, 1985.
- [10] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras", *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596– 2616, October 2003.
- [11] P. Elia, B. A. Sethuraman, P. Vijay Kumar, "Perfect space-time codes for any number of antennas", *IEEE Transactions on Information Theory*, 53, November 2007.
- [12] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, 1998.