On the Existence of Perfect Space-Time Codes

Grégory Berhuy, Frédérique Oggier

Abstract

Perfect space-time codes are codes for the coherent MIMO channel. They have been called so since they satisfy a large number of design criteria that makes their performances outmatch many other codes. In this correspondence, we discuss the existence of such codes.

Index Terms

Central simple algebras, Coherent MIMO channel, Perfect space-time codes.

I. PRELIMINARIES

Perfect space-time codes are $n \times n$ codes for the coherent MIMO channel, introduced in [6]. They have been called so since they satisfy a large number of design criteria. In order to maximize the throughput, they are *full rate* in the sense that the n^2 degrees of freedom are used to transmit n^2 information symbols. They are *fully-diverse* [9], and furthermore have a lower bound on their minimum determinant, which has been shown [4] to be a sufficient condition to achieve the diversity-multiplexing trade-off of Zheng-Tse [10]. They are *energy efficient* since encoding the information symbols into the layers of the space-time codeword does not increase the energy of the system. Finally, similar average transmit energy per antenna is required. In [6], perfect codes have been built algebraically using cyclic division algebras. In this work, they were claimed to exist only in dimensions 2, 3, 4 and 6. In [5], the authors claim to have perfect codes for any dimension. The goal of this correspondance is to give a formal proof (missing in [6]) that perfect codes as presented in [6] indeed exist only in dimensions 2, 3, 4 and 6. This apparent contradiction comes from the fact that the definition of perfect space-time codes used in [5] and [6] slightly differ.

Grégory Berhuy is with the School of Mathematics, University of Southampton, England.

Frédérique Oggier is with the California Institute of Technology, 91125 Pasadena, CA.

Emails: G.W.Berhuy@soton.ac.uk, frederique@systems.caltech.edu

This work was supported in part by the Nuffield Newly Appointed Lecturers Scheme 2006 NAL/32706 and by the Swiss National Science Foundation grant PBEL2-110209.

The organization of this correspondence is as follows. Since the goal is to give a missing proof, we let the reader refer to [6] for background on space-time coding. In Section II, we give the mathematical background necessary to understand the proof, while Section III contains the proof itself.

II. A Short Introduction to Central Simple Algebras

Central division algebras naturally appear in the context of space-time coding since their elements may always be represented as invertible matrices with coefficients in a suitable field. These particular algebras belong to a broader class of algebras, namely the central simple algebras.

In the sequel, we start by recalling what is a K-algebra and the basic related definitions. We then define the concept of central simple algebras. Finally, we introduce the definition of *Brauer group*.

A. K-algebras

All the rings will have a unit element, with an associative multiplication law.

Definition 1: Let A be a ring. The *center of* A, denoted by $Z(A)$, is the subset of A defined as

$$Z(A) = \{a \in A \mid aa' = a'a \text{ for all } a \in A\}.$$

This is a commutative subring of A.

For example, if K is a field and denote by $M_n(K)$ the $n \times n$ matrices with coefficients in K. Then $Z(M_n(K)) = \{\lambda \cdot I_n, \lambda \in K\}$ for all $n \geq 1$.

Definition 2: Let A be a ring with unit element 1_A, and denote by '+' and '·' the operations on A. We define a new multiplication law on A, denoted by $*$, as follows:

$$a * b = b \cdot a, \text{ for all } a, b, \in A.$$

It is easy to check that the operations $+$ and $*$, together with the unit element 1_A, endows the **set** A with a ring structure. We denote by A^{op} this new ring.

For example, if A is a commutative ring, then $A = A^{op}$.

Definition 3: Let K be a field. A ring A is called a K*-algebra* if K is isomorphic to a subring of $Z(A)$.

A *homomorphism* (resp. *isomorphism*) of K-algebras $A \to B$ is a ring homomorphism (resp. isomorphism) which is also K-linear.

For example, if L/K is a field extension, then L is a K-algebra. Another example is given by $M_n(K)$ for all $n \geq 1$, or $\mathrm{End}_K(V)$, the set of K-linear endomorphisms of V, for a finite dimensional K-vector space V. The choice of a K-basis of V induces an isomorphism of K-algebras $\mathrm{End}_K(V) \cong M_n(K)$, where $n = \dim_K(V)$.

Notice that if A is K-algebra, so is A^{op}, since $Z(A^{op}) = Z(A)$ by definition.

From now on, all the K-algebras will be finite-dimensional as a K-vector space. We will also always consider K as included in A.

We now introduce the concept of tensor product of K-algebras.

Definition 4: Let A, B be two K-algebras. The *tensor product* of A, B is the K-vector space generated by the elements $a \otimes b, a \in A, b \in B$ and submitted to the following relations, for all $a, a' \in A$, $b, b' \in B$ and $\lambda \in K$:

1) $a \otimes \lambda b = \lambda a \otimes b = \lambda(a \otimes b)$, $\lambda \in K$,
2) $(a + a') \otimes b = a \otimes b + a' \otimes b$ and $a \otimes (b + b') = a \otimes b + a \otimes b'$,
3) $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$.

One can easily check that $A \otimes_K B$ is a ring containing K in its center, that is a K-algebra.

If $A = M_n(K)$ and $B = M_m(K)$, then one can show that $A \otimes_K B \cong M_{nm}(K)$, and under this isomorphism , the generator $M \otimes N$ corresponds to the Kronecker product of the matrices M and N.

The tensor product operation $\otimes$ is associative and commutative, in the sense that we have canonical isomorphisms of K-algebras:

1) $A \otimes_K B \cong B \otimes_K A$
2) $(A \otimes_K B) \otimes_K C \cong A \otimes_K (B \otimes_K C)$

Note that if A is a K-algebra and L/K is a field extension, then $L \otimes_K A$ is not only a K-algebra, but also a L-algebra. Indeed, the set $\{\mu \otimes 1, \mu \in L\}$ is a subring of $Z(L \otimes_K A)$ which is isomorphic to L (this follows from the definition of the multiplication law on $L \otimes_K A$ and from the fact that L is commutative).

Note for later use that we have $\dim_L(L \otimes_K A) = \dim_K(A)$.

B. Central simple algebras

Definition 5: A *central simple K-algebra* is a K-algebra satisfying the two following conditions:

1) A is *simple*, that is the only two-sided ideals of A are (0) and A itself,
2) $Z(A) = K$.

A standard example of central simple K-algebra is the K-algebra $M_n(K)$ for all n. One can show that if A and B are central simple K-algebras, so is $A \otimes_K B$ (see [8, p. 288] for example).

Another example is given by central division K-algebras:

Definition 6: A *central division K-algebra* is a K-algebra D satisfying the two following conditions:

1) Every non-zero element of D is invertible in D,

2) $Z(D) = K$.

A central division K-algebra is a particular central simple K-algebra, since condition 1) easily implies that D has no two-sided ideals, except from (0) and D.

We now cite a theorem which will explain the interest of central division K-algebras for space-time coding.

Theorem 2.1: Let K be a field, and let A be a K-algebra. The following conditions are equivalent:

1) A is a central simple K-algebra.

2) There exists a central division K-algebra D and an integer $r \geq 1$ such that $A \cong M_r(D)$ as a K-algebra. The K-algebra D is unique up to K-isomorphism.

3) There exists a finite Galois extension L/K and an integer $n \geq 1$ such that $L \otimes_K A \cong M_n(L)$ as a L-algebra.

Proof: See [1, §5,§10]. ■

Part 2) of this result is known as Wedderburn's theorem.

It follows from the previous result that if A is a central simple K-algebra, then A can be viewed as a subring of $M_n(L)$ for some field extension L as follows: if $h : L \otimes_K A \to M_n(L)$ is an isomorphism of L-algebras, then the map $a \in A \mapsto h(1 \otimes a) \in M_n(L)$ is an injective ring homomorphism. In particular, it maps an invertible element of A to an invertible matrix.

Hence, if D is a central division K-algebra and $D \hookrightarrow M_n(L)$ is an injective ring homomorphism constructed as previously, then **every** non zero-element of D is mapped to an invertible matrix. It is this property of division algebras that made them popular for space-time coding.

The last part of the theorem, together with the equality $\dim_L(L \otimes_K A) = \dim_K(A)$, shows that the dimension of a central simple K-algebra over K is always the square of an integer. Therefore the following definition makes sense:

Definition 7: Let A be a central simple K-algebra. The *degree* of A, denoted by $\deg(A)$, is the integer defined by

$$\deg(A) = \sqrt{\dim_K(A)}.$$

Let A be a central simple K-algebra. By Wedderburn's theorem, we can write $A \cong M_r(D)$, where D is a central division K-algebra, unique up to K-isomorphism, for some integer $r \geq 1$. In particular, $\deg(D)$ only depends on the isomorphism class of D and A.

Definition 8: The *index* of A, denoted by $\text{ind}(A)$, is defined by

$$\text{ind}(A) = \deg(D).$$

Notice that if $A \cong M_r(D)$, we have by definition

$$\deg(A) = r \, \text{ind}(A)$$

C. The Brauer group

Definition 9: We say that two central simple K-algebras A, B are *Brauer equivalent* if they correspond to the same division K-algebra D, namely $A \cong M_r(D)$ and $B \cong M_s(D)$, for some integers r, s. We write $A \sim B$.

One can check that this is indeed an equivalence relation on the set of central simple K-algebras. The equivalence class of A is denoted by $[A]$. The set of equivalence classes is denoted by $\text{Br}(K)$.

We define an addition on the set $\text{Br}(K)$ as follows:

$$[A] + [B] := [A \otimes_K B].$$

One can show that this operation is well-defined. Moreover, it is commutative and associative (this follows from the properties of $\otimes$).

Note that the class $[K]$ is a neutral element for '+' since $A \otimes_K K \cong A$. We will denote it simply by 0. For any $[A] \in \text{Br}(K)$, one can show that the opposite $-[A]$ is the class $[A^{op}]$. Hence the operation '+' endows $\text{Br}(K)$ with a structure of abelian group (see [8, p. 290]).

This group is called the *Brauer group* of K, honoring Richard Brauer who made the first systematic study of what would appear to be a fundamental invariant. Note also for later use that for all n, we have $[M_n(K)] = 0$ in $\text{Br}(K)$.

Definition 10: The *exponent* of A is the order of the class $[A]$ in the Brauer group $\text{Br}(K)$.

The following theorem gives a relationship among the three invariants of a central simple algebra that are the exponent, the index and the degree.

Theorem 2.2: For any central simple K-algebra, we have

$$\exp(A) | \, \text{ind}(A) | \deg(A).$$

If moreover K is a number field, then $\exp(A) = \text{ind}(A)$.

Proof: For a proof of the first statement, see [3, p. 66]. For the second one, see [2]. ∎

III. Cyclic algebras and perfect codes

Perfect space-time codes have been built using cyclic division algebras. Cyclic algebras, as recalled below, are a particular class of central simple algebras. After having presented the results we need about cyclic algebras, we recall the definition of a perfect space-time code, and give the proof that they exist only in dimension 2, 3, 4, and 6.

A. Cyclic algebras

Let us recall the definition of a cyclic algebra.

Definition 11: If L/K is a cyclic extension of degree n, and if σ is a generator of the Galois group, for any $\gamma \in K^{\times}$, we can define a K-algebra denoted by $\mathcal{A} = (\gamma, L/K, \sigma)$ as follows: consider the vector space

$$L \oplus eL \oplus \cdots e^{n-1}L,$$

and define a product by the relations:

$$e^n = \gamma, \lambda e = e\sigma(\lambda).$$

Then $\mathcal{A} = (\gamma, L/K, \sigma)$ is called *a cyclic algebra*.

Cyclic algebras naturally provide families of matrices thanks to an explicit isomorphism h between $L \otimes_K \mathcal{A}$ and $M_n(L)$. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + \ldots + e^{n-1}x_{n-1},\ x_i \in L \text{ for all } i,$$

it is enough to give $h(1 \otimes x_i)$ and $h(1 \otimes e)$. We have that

$$h : L \otimes_K \mathcal{A} \cong M_n(L) \tag{1}$$

is given by

$$1 \otimes x_i \mapsto \begin{pmatrix} x_i & 0 & & 0 \\ 0 & \sigma(x_i) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & \sigma^{n-1}(x_i) \end{pmatrix} \text{ for all } i,\ 1 \otimes e \mapsto \begin{pmatrix} 0 & 0 & 0 & & \gamma \\ 1 & 0 & 0 & & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & & \ddots & & \\ 0 & & & 1 & 0 \end{pmatrix}.$$

Thus the matrix of $h(1 \otimes x)$ is easily checked to be

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

The map h is easily seen to be indeed an isomorphism of L-algebras. Therefore, Theorem 2.1 implies:

Proposition 3.1: The algebra $\mathcal{A} = (\gamma, L/K, \sigma)$ is a central simple K-algebra of degree n.

One can prove the following result:

Proposition 3.2: 1) We have $(1, L/K, \sigma) \cong M_n(K)$, where $n = [L : K]$.

In others words, $[(1, L/K, \sigma)] = 0$ in the Brauer group.

2) $[(\gamma, L/K, \sigma)] + [(\gamma', L/K, \sigma)] = [(\gamma\gamma', L/K, \sigma)]$ in the Brauer group.

Proof:

1) The proof [8, p. 318] consists in showing that the map

$$j : (1, L/K, \sigma) \to \text{End}_K(L)$$

defined by $j(\lambda) =$ left multiplication by λ, for $\lambda \in L$, and $j(e) = \sigma$ is an isomorphism. There is then a known isomorphism between $\text{End}_K(L)$, the K-linear endomorphisms of K, and $M_n(K)$. The translation in terms of the Brauer group is given by the fact that $[M_n(K)] = 0$, as pointed out before.

2) See [8, p. 319].

■

The following corollary will play a fundamental role in the final proof.

Corollary 3.3: Let K be a number field, and let $\mathcal{A} = (\gamma, L/K, \sigma)$. If γ is a m^{th}-root of 1, then $\text{ind}(\mathcal{A})|m$.

Proof: The second point of the previous proposition applied several times shows that, in the Brauer group,

$$m[\mathcal{A}] = [(\gamma^m, L/K, \sigma)].$$

Since $\gamma^m = 1$ by assumption, the first point of the proposition shows that $m[\mathcal{A}] = 0$ in the Brauer group. Hence $\exp(\mathcal{A})|m$ by definition. Since K is a number field, by Theorem 2.2, $\text{ind}(\mathcal{A}) = \exp(\mathcal{A})$ and we are done. ■

In [8], the definition of a cyclic algebra is slightly different ($\mathcal{A}$ is defined as a right vector space over L), but it is easy to check that all the results above are still true with our definition.

B. Existence of Perfect Space-Time Codes

Perfect $n \times n$ space-time codes are linear dispersion codes for the coherent MIMO channel that satisfy the following design criteria. They are full rate: the n^2 degrees of freedom are used to transmit n^2 information symbols. They have a non-vanishing determinant: prior to SNR normalization, the minimum determinant of the codebook $\mathcal{C}$

$$\min_{\mathbf{X}_i \neq \mathbf{X}_j \in \mathcal{C}} |\det(\mathbf{X}_i - \mathbf{X}_j)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2$$

is lower bounded by a constant. In particular, the code is fully-diverse. A shaping constraint is imposed at the encoder: the information symbols are encoded into the layers of the space-time code without changing the energy at the transmitter. Finally, uniform average energy per antenna is required.

The existing codes that satisfy all these properties are built using cyclic division algebras $\mathcal{A} = (\gamma, L/K, \sigma)$, where L/K has base field $K = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$ respectively, where ζ_3 denotes a primitive 3^{rd} rooth of unity. Codewords are of the form given in (2). The choice of $K = \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$ allows to transmit QAM or HEX constellations resp.

As noticed in [6], in order to obtain both uniform average energy per antenna and efficient energy encoding at the transmitter, γ is asked to satisfy $|\gamma|^2 = 1$. There are now two possibilities in choosing γ:

1) either $\gamma \in \mathbb{Z}[i]$, $\mathbb{Z}[\zeta_3]$ resp., in which case γ has to be a 4th, resp., 6th root of unity,
2) or $\gamma \in \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$ resp., but then, γ will have a denominator in $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_3]$ resp.

This is here that the work of [6] and [5] differ. In [5], the authors choose $\gamma = \gamma_1/\gamma_2 \in \mathbb{Q}(i)$, resp. $\mathbb{Q}(\zeta_3)$, while in [6], γ is chosen to be a root of unity (both choices of γ are such that the resulting cyclic algebra is a division algebra). Let us discuss briefly here how the choice of γ influences the minimum determinant of the code (that is, its coding gain). Let $\mathbf{X}$ be a codeword of the form (2), but where the coefficients $x_0, \ldots, x_{n-1}$ are chosen in $\mathcal{O}_L$, and furthermore γ is chosen to be in $\mathcal{O}_K = \mathbb{Z}[i]$, resp. $\mathbb{Z}[\zeta_3]$. Then $\det(\mathbf{X}) \in \mathcal{O}_K$ [6]. The minimum determinant is thus lower bounded by 1. If $\gamma \in \mathbb{Q}(i)$, $\mathbb{Q}(\zeta_3)$ resp., then a lower bound can be computed as follows: write $\mathbf{X}$ as

$$\frac{1}{\gamma_2^{n-1}} \tilde{\mathbf{X}},$$

where all the coefficients of $\tilde{\mathbf{X}}$ are in $\mathcal{O}_L$. The minimum determinant of $\tilde{\mathbf{X}}$ is again 1, but the minimum determinant of $\mathbf{X}$ is now

$$\frac{1}{|\gamma_2|^{2(n-1)}}.$$

In order to maximize the minimum determinant, in [6], γ is chosen to be a root of unity. Under this assumption, we now show that perfect space-time codes exist only in dimension 2, 3, 4, and 6.

Theorem 3.4: Perfect space-time codes only exist in dimension 2, 3, 4 and 6.

Proof: By definition, γ has to be a 4^{th} or 6^{th} root of 1, hence the index of the cyclic algebra used to build the code is $1, 2, 3, 4$ or 6 by Corollary 3.3. Since we want $\mathcal{A}$ to be a division algebra, we need $\deg(\mathcal{A}) = \mathrm{ind}(\mathcal{A})$. Indeed, if $\mathcal{A} = M_r(D)$, for a central division K-algebra D, then by definition we have $\deg(\mathcal{A}) = r\,\mathrm{ind}(\mathcal{A})$. Hence $\mathcal{A}$ will be a division algebra if and only if $r = 1$, that is $\deg(\mathcal{A}) = \mathrm{ind}(\mathcal{A})$. Moreover, since we want $n \geq 2$, the only possible values for n are $2, 3, 4$ or 6, and we are done. ■

IV. Conclusion

In this correspondence, we proved that the so-called perfect codes only exist in dimension 2, 3, 4 and 6, when perfect codes are defined as in [6], with the parameter γ chosen to be a root of unity. Doing so, we give a missing proof in [6].

Acknowledgment

The authors would like to thank Prof. E. Viterbo for his careful reading of a preliminary version of this paper.

References

[1] N. Bourbaki, *Eléments de mathématiques, Algèbre, Ch.8*, Masson, Paris.

[2] J.W.S. Cassels and A. Frohlich, *Algebraic Number Theory*, Academic Press, London and New York, 1967.

[3] P.K. Draxl, *Skew fields*, LMS Lecture Note Series **81**, Cambridge University Press, 1983.

[4] P. Elia, K. Raj Kumar, S. A. Pawar, P. Vijay Kumar and H.-F. Lu, "Explicit, Minimum-Delay Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff," Submitted to *IEEE Trans. Inform. Theory*, Sept. 2004.

[5] P. Elia, B. A. Sethuraman and P. Vijay Kumar, "Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas," Proc. WirelessCom 2005, International Conference on Wireless Networks, Communications, and Mobile Computing.

[6] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes", to appear in the *IEEE Trans. on Information Theory*, September 2006.

[7] S. Lang, *Algebra*, Addison-Wesley publishing company, 1971.

[8] W. Scharlau, *Quadratic and Hermitian Forms*, Grundleheren der math. Wiss **270**, Berlin, Heidelberg, Springer Verlag, 1985.

[9] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication : Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, March 1998.

[10] L. Zheng, D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. on Information Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.