Advances in Mathematics of Communications
Volume 00, No. 0, 2013, 1–25

doi:

ALGEBRAIC SPACE-TIME CODES BASED ON DIVISION ALGEBRAS WITH A UNITARY INVOLUTION

Abstract. In this paper, we focus on the design of unitary space-time codes achieving full diversity using division algebras, and on the systematic computation of their minimum determinant. We also give examples of such codes with high minimum determinant. Division algebras allow to obtain higher rates than known constructions based on finite groups.

Grégory Berhuy

Université Joseph Fourier
Institut Fourier
100 rue des maths
BP 74, F-38402 Saint Martin d'Hères Cedex, France

Introduction

The problem addressed in the design of space-time codes in the coherent case (that is, in the case where the receiver knows the properties of the channel) can be summarized as follows: find a set $\mathcal{C}$ of complex $n \times n$ matrices such that the **minimum determinant**

$$\delta_{min}(\mathcal{C}) = \inf_{X \neq X' \in \mathcal{C}} |\det(X - X')|^2$$

is maximal. Of course, the first step is to ensure that $\delta_{min}(\mathcal{C})$ is not zero. When this is the case, we will say that $\mathcal{C}$ is **fully diverse**. One natural way to achieve this is to use division algebras. Indeed, any division algebra D whose center k is a subfield of $\mathbb{C}$ may be identified to a subring of a matrix algebra $\mathrm{M}_n(\mathbb{C})$. In particular, $D^\times$ may be identified to a subgroup of $\mathrm{GL}_n(\mathbb{C})$, and taking $\mathcal{C}$ to be a subset of D yields a fully diverse algebraic space-time code.

The use of division algebras for space-time coding started with the seminal work by B. A. Sethuraman and B. Sundar Rajan [13]. Number fields and cyclic algebras were discussed, which have been a favourite tool for space-time design. Some surveys are by now available [9, 12], and we refer the interested reader to them for further details. Other algebras have also been explored, such as crossed product algebras [1] or non-associative algebras [11]. Recently, the optimality of algebraic codes obtained by Oggier et al. on cyclic algebras or crossed product algebras has been established ([3]; see also [15]). Notice that the two surveys mentioned above focus on the coherent case.

2010 *Mathematics Subject Classification:* Primary:12E15 ; Secondary: 11T71,16W10.
Key words and phrases: Skew fields, algebras with involution, unitary involutions, algebraic coding, space-time codes.

In the non-coherent case, the problem has a different flavour: the minimum determinant still needs to be maximized, but the elements of the code $\mathcal{C}$ must be complex unitary matrices [4, 5]. We will say that $\mathcal{C}$ is a **unitary code**.

The question of designing good unitary codes is far from being solved. The two main difficulties arising in the non-coherent case are the following:

(a) fully diverse families of unitary matrices are hard to find;

(b) contrary to the coherent case, no systematic way to compute or even estimate $\delta_{min}(\mathcal{C})$ is known.

Question (a) has been addressed in [14] using unitary representations of finite fixed-point free groups. Later on, Oggier proposed somme approach using cyclic algebras with a unitary involution ([10, 7]). We refer the reader to [8] for a survey of known results.

In this paper, we will give a method to construct unitary codes using division algebras carrying a unitary involution, generalizing in particular the work done by Oggier and Lequeu, and show how to compute the minimum determinant of such codes. The advantage of this approach compared to the group-theoretic approach is that division algebras allow to obtain higher rates (the rate corresponds, roughly speaking, to the cardinality of the code).

Notice that in the literature, the quantity which is asked to be maximal is not the minimum determinant, but the so-called **diversity product** $\zeta(\mathcal{C})$, defined by

$$\zeta(\mathcal{C}) = \frac{1}{2} \inf_{X \neq X' \in \mathcal{C}} |\det(X - X')|^{\frac{1}{n}},$$

where n is the size of the matrices. In other words, we have

$$\zeta(\mathcal{C}) = \frac{1}{2} \delta_{min}(\mathcal{C})^{\frac{1}{2n}}.$$

The two optimization problems being obviously equivalent, we will focus essentially on the computation of the minimum determinant.

The structure of this paper is as follows. In Section 1, we recall some basic definitions on central simple algebras with unitary involutions, and provide some examples. In Section 2, we will provide a systematic way to construct unitary space-time codes using algebras with unitary involutions. Finally, in Section 3, we will explain how to compute the minimum determinant of these codes and provide examples.

1. Algebras with unitary involutions: definitions and examples

In this section, k is a field, and A is a central simple k-algebra. To simplify the exposition, we will assume that $\mathrm{char}(k) \neq 2$. We will collect here some basic definitions and results on unitary involutions. We will assume that the reader is familiar with the theory of central simple algebras. We let the reader refer to [6] for the missing details and proofs concerning central simple k-algebras with involutions.

Definition 1.1. An **involution** on A is a ring anti-automorphism of A of order at most 2.

In other words, an involution is a map $\sigma : A \longrightarrow A$ satisfying for all $x, y \in A$:

1. $\sigma(x+y) = \sigma(x) + \sigma(y)$;
2. $\sigma(1) = 1$;
3. $\sigma(xy) = \sigma(y)\sigma(x)$;
4. $\sigma(\sigma(x)) = x$.

For example, the transposition is an involution on $\mathrm{M}_n(k)$. Notice that Id_A is never an involution unless A is commutative, which implies that $A = k$. Therefore, if $A \neq k$, an involution on A has order 2.

It is easy to check that for every $\lambda \in k$, we have $\sigma(\lambda) \in k$. Hence $\sigma_{|_k}$ is an automorphism of order at most 2 of k.

We set

$$k_0 = \{\lambda \in k | \sigma(\lambda) = \lambda\}.$$

We say that σ is an **involution of the first kind** if $\sigma_{|_k} = \mathrm{Id}_k$, that is if $k = k_0$, and an **involution of the second kind (or unitary)** otherwise. In the latter case, k/k_0 is a quadratic field extension, and $\sigma_{|_k}$ is the unique non-trivial k_0-automorphism of k/k_0. Conversely, if k/k_0 is a quadratic field extension, we will say that a unitary involution σ on a central simple k-algebra A is a k/k_0-**involution** if $\sigma_{|_k}$ is the unique non-trivial k_0-automorphism of k.

An element $x \in A$ is called **symmetric** if $\sigma(x) = x$, and **skew-symmetric** if $\sigma(x) = -x$. We denote by $\mathrm{Sym}(A, \sigma)$ the set of symmetric elements of A, and by $\mathrm{Skew}(A, \sigma)$ the set of skew-symmetric elements of A. Both have a natural structure of a k_0-vector space. We also set

$$\mathrm{Sym}(A, \sigma)^\times = \mathrm{Sym}(A, \sigma) \cap A^\times \text{ and } \mathrm{Skew}(A, \sigma)^\times = \mathrm{Skew}(A, \sigma) \cap A^\times.$$

We say that two central simple k-algebras with involutions (A, σ) and (A', σ') are **isomorphic** if there exists an isomorphism of k-algebras $f : A \xrightarrow{\sim} A'$ such that

$$\sigma' \circ f = f \circ \sigma.$$

In this case, one may verify that σ and σ' are involutions of the same kind. Moreover, f then induces isomorphisms of k_0-vector spaces

$$\mathrm{Sym}(A, \sigma) \simeq \mathrm{Sym}(A', \sigma') \text{ and } \mathrm{Skew}(A, \sigma) \simeq \mathrm{Skew}(A', \sigma').$$

One may show that, if σ, σ' are two k/k_0-involutions of the second kind, there exists $u \in \mathrm{Sym}(A, \sigma)^\times$, which is unique up to multiplication by an element of $k_0^\times$, such that $\sigma' = \mathrm{Int}(u) \circ \sigma$, where

$$\mathrm{Int}(u)\colon \begin{array}{l} B \longrightarrow B \\ b \longmapsto ubu^{-1}. \end{array}$$

Example 1.2. Let k/k_0 be a quadratic field extension, and let $^-$ be its non-trivial k_0-automorphism. If $n \geq 1$, the map

$$\begin{array}{c} \mathrm{M}_n(k) \longrightarrow \mathrm{M}_n(k) \\ M = (a_{ij}) \longmapsto M^* = (\overline{a}_{ji}) \end{array}$$

is a unitary involution on $\mathrm{M}_n(k)$. The result mentioned above then shows that every k/k_0-involution on $\mathrm{M}_n(k)$ has the form

$$\sigma_H = \mathrm{Int}(H) \circ {}^*,$$

where $H \in \mathrm{GL}_n(k)$ satisfies $H^* = H$.

We now would like to give a family of examples which will be useful in the sequel. First, we recall the notion of a crossed-product algebra.

Definition 1.3. Let L/k be a finite Galois extension, with Galois group G. The group G acts by k-algebra automorphisms on L by

$$\begin{aligned} L\times G &\longrightarrow L \\ (\lambda,\sigma) &\longmapsto \lambda^\sigma=\sigma^{-1}(\lambda). \end{aligned}$$

Let us consider a 2-**cocycle** of G with values in L, that is a map

$$\xi\colon \begin{array}{c} G\times G\longrightarrow L^\times \\ (\sigma,\rho)\longmapsto \xi_{\sigma,\rho} \end{array}$$

satisfying

$$\xi_{\sigma,\mathrm{Id}}=\xi_{\mathrm{Id},\rho}=1 \ \text{ for all } \sigma,\rho\in G,$$

and

$$\xi_{\sigma,\rho\nu}\xi_{\rho,\nu}=\xi_{\sigma\rho,\nu}\xi_{\sigma,\rho}^{\nu} \ \text{ for all } \sigma,\rho,\nu\in G.$$

The **crossed-product algebra** $(\xi,L/k,G)$ is the k-algebra with generators $(f_\sigma)_{\sigma\in G}$ satisfying

$$(\xi,L/k,G)=\bigoplus_{\sigma\in G} f_\sigma L$$

and subject to the relations

$$f_{\mathrm{Id}}f_\sigma=f_\sigma f_{\mathrm{Id}}=f_\sigma,\ \lambda f_\sigma=f_\sigma\lambda^\sigma,\ f_\sigma f_\rho=f_{\sigma\rho}\xi_{\sigma,\rho}$$

for all $\sigma,\rho\in G,\lambda\in L$.

Notice for later use that f_{Id} is the unit element of $(\xi,L/k,G)$, and that f_σ is invertible for all $\sigma\in G$.

This is a central simple k-algebra of degree n (see [2, Lemma VI.1.7], for example).

Example 1.4. Let $\gamma\in k^\times$, let L/k be a cyclic extension of degree n, and let σ be a generator of its Galois group. Setting

$$\xi^\gamma_{\sigma^i,\sigma^j}=\begin{cases} 1 & \text{if} \quad i+j<n \\ \gamma & \text{if} \quad i+j\geq n \end{cases}$$

defines a 2-cocycle, and the corresponding crossed-product is simply the k-algebra $(\gamma,L/k,\sigma)=\bigoplus\limits_{i=0}^{n-1} e^iL$ generated by one element e subject to the relations

$$e^n=\gamma,\lambda e=e\lambda^\sigma \text{ for all } \lambda\in L.$$

The k-algebra $(\gamma,L/k,\sigma)$ is called a **cyclic** k-algebra.

Example 1.5. Let L/k be a biquadratic extension with Galois group $G=\langle\sigma,\tau\rangle$, let $a,b,u\in L^\times$ satisfy

$$a^\sigma=a,b^\tau=b,uu^\sigma=\frac{a}{a^\tau},uu^\tau=\frac{b^\sigma}{b},$$

and let $\xi^{a,b,u}:G\times G\longrightarrow L^\times$ be defined by

$$\xi^{a,b,u}_{\mathrm{Id},\mathrm{Id}}=1,\xi^{a,b,u}_{\mathrm{Id},\sigma}=1,\xi^{a,b,u}_{\mathrm{Id},\tau}=1,\xi^{a,b,u}_{\mathrm{Id},\sigma\tau}=1,$$

$$\xi^{a,b,u}_{\sigma,\mathrm{Id}}=1,\xi^{a,b,u}_{\sigma,\sigma}=a,\xi^{a,b,u}_{\sigma,\tau}=1,\xi^{a,b,u}_{\sigma,\sigma\tau}=a^\tau,$$

$$\xi^{a,b,u}_{\tau,\mathrm{Id}} = 1, \xi^{a,b,u}_{\tau,\sigma} = u, \xi^{a,b,u}_{\tau,\tau} = b, \xi^{a,b,u}_{\tau,\sigma\tau} = \frac{b^\sigma}{u},$$
$$\xi^{a,b,u}_{\sigma\tau,\mathrm{Id}} = 1, \xi^{a,b,u}_{\sigma\tau,\sigma} = \frac{a}{u^\sigma}, \xi^{a,b,u}_{\sigma\tau,\tau} = b, \xi^{a,b,u}_{\sigma\tau,\sigma\tau} = abu^\tau.$$

A lengthy case-by-case verification shows that $\xi^{a,b,u}$ is a 2-cocycle. It is easy to check that the corresponding crossed-product algebra is nothing but the k-algebra generated by two elements e and f satisfying

$$(a, b, u, L/k) = L \oplus eL \oplus fL \oplus efL,$$

subject to the relations

$$\lambda e = e\lambda^\sigma, \lambda f = f\lambda^\tau, e^2 = a, f^2 = b, fe = efu.$$

The following result provides the family of examples we are aiming for, and generalizes the construction of a unitary involution of a cyclic algebra proposed in [10].

Lemma 1.6. *Let k/k_0 be a quadratic field extension, and denote by $\bar{\ }$ its non-trivial k_0-automorphism. Let L/k be a finite Galois extension with Galois group G. Assume that there exists a ring automorphism $\alpha : L \longrightarrow L$ satisfying the following conditions:*

1. $\alpha^2 = \mathrm{Id}_L$;
2. $\alpha \circ \sigma = \sigma \circ \alpha$ *for all* $\sigma \in G$;
3. $\alpha(\lambda) = \overline{\lambda}$ *for all* $\lambda \in k$.

Let $\xi : G\times G \longrightarrow L^\times$ be a 2-cocycle satisfying $(\alpha\circ\xi)\xi = 1$, and let $B = (\xi, L/k, G)$ be the corresponding crossed-product algebra. Then there is a unique unitary involution τ on B satisfying

$$\tau(f_\sigma) = f_\sigma^{-1} \text{ for all } \sigma \in G \text{ and } \tau_{|_L} = \alpha.$$

Moreover, if M_b is the matrix of left multiplication by b in the L-basis $(f_\sigma)_{\sigma\in G}$, then we have

$$M_{\tau(b)} = M_b^\sharp \text{ for all } b \in B,$$

where $\sharp$ is the unitary involution on $\mathrm{M}_n(L)$ defined by

$$\mathrm{M}_n(L) \longrightarrow \mathrm{M}_n(L)$$
$$M = (m_{\sigma\rho})_{\sigma,\rho\in G} \longmapsto M^\sharp = (\alpha(m_{\rho\sigma})_{\sigma,\rho\in G}).$$

Proof. Assume that an involution τ satisfying the properties of the lemma exists. Using the fact that τ is an anti-automorphism, we get that

$$\tau\big(\sum_{\sigma\in G} f_\sigma\lambda_\sigma\big) = \sum_{\sigma\in G} \alpha(\lambda_\sigma)f_\sigma^{-1} \text{ for all } \lambda_\sigma \in L, \sigma \in G.$$

This proves the uniqueness of τ. We now have to prove that the map τ defined by the formula above is indeed a unitary involution on B. Clearly, τ is additive, and for all $x \in k$, we have

$$\tau(x) = \alpha(x) = \overline{x}.$$

We now check that we have

$$\tau(xy) = \tau(y)\tau(x) \text{ for all } x, y \in B.$$

The usual distributivity argument shows that it is enough to prove it for $x = f_\sigma\lambda, y = f_\rho\mu, \sigma,\rho\in G, \lambda,\mu\in L$. We have

$$\tau(f_\sigma\lambda f_\rho\mu)=\tau(f_{\sigma\rho}\xi_{\sigma,\rho}\lambda^\rho\mu)=\alpha(\xi_{\sigma,\rho})\alpha(\lambda^\rho)\alpha(\mu)f_{\sigma\rho}^{-1}.$$

On the other hand, we have

$$\tau(f_\rho\mu)\tau(f_\sigma\lambda)=\alpha(\mu)f_\rho^{-1}\alpha(\lambda)f_\sigma^{-1}.$$

From the relation $\lambda f_\sigma = f_\sigma\lambda^\sigma$, we get

$$f_\sigma^{-1}\lambda=\lambda^\sigma f_\sigma^{-1}.$$

Therefore, we get

$$\begin{array}{rcl}\tau(f_\rho\mu)\tau(f_\sigma\lambda) & = & \alpha(\mu)(\alpha(\lambda))^\rho f_\rho^{-1}f_\sigma^{-1}\\ & = & \alpha(\mu)(\alpha(\lambda))^\rho(f_\sigma f_\rho)^{-1}\\ & = & \alpha(\mu)(\alpha(\lambda))^\rho(f_{\sigma\rho}\xi_{\sigma,\rho})^{-1}\\ & = & \alpha(\mu)(\alpha(\lambda))^\rho\xi_{\sigma,\rho}^{-1}f_{\sigma\rho}^{-1}.\end{array}$$

Since α commutes with the elements of G and $\alpha(\xi_{\sigma,\rho})=\xi_{\sigma,\rho}^{-1}$ by assumption, we get the desired equality. It remains to prove that $\tau^2=\mathrm{Id}_B$. Since τ is an antiautomorphism of rings, τ^2 is an automorphism of rings. Hence to prove that τ^2 is the identity map, it is enough to check that $\tau^2(f_\sigma)=f_\sigma$ for all $\sigma\in G$ and that $\tau^2_{|_L}=\mathrm{Id}_L$, which is clear from the definition of τ.

We finally prove the last assertion. We will index the entries of a matrix with coefficients in L with the elements of G. Let $b\in B$. If $M_b=(m_{\sigma,\rho})_{\sigma,\rho\in G}$, we have to check that $M_{\tau(b)}=(\alpha(m_{\rho,\sigma}))_{\sigma,\rho\in G}$. Let us write

$$b=\sum_{\sigma\in G}f_\sigma\lambda_\sigma.$$

For all $\rho\in G$, we have

$$\begin{array}{rcl}bf_\rho & = & \displaystyle\sum_{\sigma\in G}f_\sigma\lambda_\sigma f_\rho\\ & = & \displaystyle\sum_{\sigma\in G}f_\sigma f_\rho\lambda_\sigma^\rho\\ & = & \displaystyle\sum_{\sigma\in G}f_{\sigma\rho}\xi_{\sigma,\rho}\lambda_\sigma^\rho\\ & = & \displaystyle\sum_{\sigma\in G}f_\sigma\xi_{\sigma\rho^{-1},\rho}\lambda^\rho_{\sigma\rho^{-1}},\end{array}$$

so we have

$$M_b=(\xi_{\sigma\rho^{-1},\rho}\lambda^\rho_{\sigma\rho^{-1}})_{\sigma,\rho\in G}.$$

Now from the equality $f_\sigma f_{\sigma^{-1}\rho}=f_\rho\xi_{\sigma,\sigma^{-1}\rho}$, we get

$$f_\sigma^{-1}f_\rho=f_{\sigma^{-1}\rho}\xi^{-1}_{\sigma,\sigma^{-1}\rho}.$$

Therefore, we have

$$\begin{array}{rcl}\tau(b)f_\rho & = & \sum_{\sigma\in G}\alpha(\lambda_\sigma)f_\sigma^{-1}f_\rho \\ & = & \sum_{\sigma\in G}\alpha(\lambda_\sigma)f_{\sigma^{-1}\rho}\xi^{-1}_{\sigma,\sigma^{-1}\rho} \\ & = & \sum_{\sigma\in G}f_{\sigma^{-1}\rho}(\alpha(\lambda_\sigma))^{\sigma^{-1}\rho}\xi^{-1}_{\sigma,\sigma^{-1}\rho} \\ & = & \sum_{\sigma\in G}f_\sigma\alpha(\lambda_{\rho\sigma^{-1}})^\sigma\xi^{-1}_{\rho\sigma^{-1},\sigma},\end{array}$$

the last equality being obtained by performing the change of variables $\sigma\leftrightarrow\sigma^{-1}\rho$. Using again that α commutes with the elements of G and $\alpha(\xi_{\rho\sigma^{-1},\sigma})=\xi^{-1}_{\rho\sigma^{-1},\sigma}$, we get

$$\tau(b)f_\rho=\sum_{\sigma\in G}f_\sigma\alpha(\lambda^\sigma_{\rho\sigma^{-1}}\xi_{\rho\sigma^{-1},\sigma}).$$

Thus we get

$$M_{\tau(b)}=(\alpha(\lambda^\sigma_{\rho\sigma^{-1}}\xi_{\rho\sigma^{-1},\sigma}))_{\sigma,\rho\in G}=M_b^\sharp,$$

and this concludes the proof. □

Remark 1.7. The description of the involution τ in the lemma above may be made more explicit. As explained in the proof, we have

$$\tau\big(\sum_{\sigma\in G}f_\sigma\lambda_\sigma\big)=\sum_{\sigma\in G}\alpha(\lambda_\sigma)f_\sigma^{-1}\text{ for all }\lambda_\sigma\in L,\sigma\in G.$$

Now we have $f_\sigma f_{\sigma^{-1}}=\xi_{\sigma,\sigma^{-1}}$, and therefore

$$f_\sigma^{-1}=f_{\sigma^{-1}}\xi^{-1}_{\sigma,\sigma^{-1}}\text{ for all }\sigma\in G.$$

Thus, we get

$$\alpha(\lambda_\sigma)f_\sigma^{-1}=f_{\sigma^{-1}}\alpha(\lambda_\sigma)^{\sigma^{-1}}\xi^{-1}_{\sigma,\sigma^{-1}}\text{ for all }\sigma\in G,$$

and performing the change of variables $\sigma\leftrightarrow\sigma^{-1}$ yields

$$\tau\big(\sum_{\sigma\in G}f_\sigma\lambda_\sigma\big)=\sum_{\sigma\in G}f_\sigma\alpha(\lambda_{\sigma^{-1}})^\sigma\xi^{-1}_{\sigma^{-1},\sigma}\text{ for all }\lambda_\sigma\in L,\sigma\in G.$$

Since α commutes with σ and $\alpha(\xi_{\sigma^{-1},\sigma})\xi_{\sigma^{-1},\sigma}=1$ by assumption, we finally get that

$$\tau\big(\sum_{\sigma\in G}f_\sigma\lambda_\sigma\big)=\sum_{\sigma\in G}f_\sigma\alpha(\lambda^\sigma_{\sigma^{-1}}\xi_{\sigma^{-1},\sigma})\text{ for all }\lambda_\sigma\in L,\sigma\in G.$$

Example 1.8. Assume that k_0 is a number field. Let L/k be a finite Galois extension of k with Galois group G, and assume that complex conjugation induces a k_0-automorphism α of L which commutes with elements of $\mathrm{Gal}(L/k)$. This automorphism satisfies the conditions of Lemma 1.6. In particular, if $\xi: G\times G\longrightarrow L^\times$ is a 2-cocycle satisfying

$$|\xi_{\rho,\rho'}|^2=1\text{ for all }\rho,\rho'\in G,$$

then $B=(\xi,L/k,\sigma)$ carries a unitary involution τ such that τ restricts to complex conjugation on L and $\tau(f_\sigma)=f_\sigma^{-1}$ for all $\sigma\in G$.

For example, if $B = (\gamma, L/k, \sigma)$ is a cyclic k-algebra of degree n such that $|\gamma|^2 = 1$, then the unitary involution τ on B given by the previous lemma is defined by

$$\tau : \begin{array}{c} B \longrightarrow B \\ \displaystyle\sum_{i=0}^{n-1} e^i \lambda_i \longmapsto \overline{\lambda}_0 + \sum_{i=1}^{n-1} e^i \, \overline{\gamma \lambda_{n-i}^{\sigma^i}}, \end{array} ,$$

as it may easily be seen by direct computations, or by using the remark above.

We recover in this way the involution obtained by Oggier and Lequeu [10].

2. Algebras with involutions and space-time coding

As briefly explained in the introduction, we would like to find a set $\mathcal{C}$ of $n \times n$ **unitary** matrices such that the **minimum determinant**

$$\delta_{min}(\mathcal{C}) = \inf_{\mathbf{U} \neq \mathbf{U}' \in \mathcal{C}} |\det(\mathbf{U} - \mathbf{U}')|^2$$

is maximal.

As this has been done for the coherent case, we are going to use the theory of division algebras to construct unitary codes.

We now explain how we are going to proceed. First, we need a definition. Let k/k_0 be a quadratic field extension of number fields, whose non-trivial automorphism is given by the complex conjugation. Let (B, τ) be a central simple k-algebra with a unitary k/k_0-involution.

Notice that, if L is any subfield of $\mathbb{C}$ containing k and $^-$ denotes the complex conjugation, the map $\tau \otimes {}^-$ is a unitary involution on $B \otimes_k L$. Thus the following definition makes sense.

Definition 2.1. We say that (B, τ) is **positive definite** if there exists a subfield L of $\mathbb{C}$ such that there exists an isomorphism of L-algebras with involutions

$$\varphi : (B \otimes_k L, \tau \otimes {}^-) \xrightarrow{\sim} (\mathrm{M}_n(L), {}^*),$$

that is, if there exists an isomorphism of L-algebras $\varphi : B \otimes_k L \xrightarrow{\sim} \mathrm{M}_n(L)$ such that

$$\varphi \circ (\tau \otimes {}^-) = {}^* \circ \varphi.$$

Example 2.2. The standard conjugate transpose involution on $\mathrm{M}_n(\mathbb{C})$ is positive definite.

Remark 2.3. Notice that since the elements $b \otimes 1$ span $B \otimes_k L$ as an L-vector space, the elements $\varphi(b \otimes 1)$ span $\mathrm{M}_n(L)$ as an L-vector space, where $b \in B$. Hence, an isomorphism $\varphi : B \otimes_k L \xrightarrow{\sim} \mathrm{M}_n(L)$ induces an isomorphism

$$\varphi : (B \otimes_k L, \tau \otimes {}^-) \xrightarrow{\sim} (\mathrm{M}_n(L), {}^*)$$

if and only if

$$\varphi(\tau(b) \otimes 1) = \varphi(b \otimes 1)^* \quad \text{for all } b \in B.$$

In view of this definition, it does not seem to be very easy to check whether or not a given unitary involution is positive definite. In fact, one may show that τ is positive definite if and only if a certain hermitian form attached to (B,τ) is positive definite. Since we will not need this criterion for our purpose, we postpone the statement and the proof of this criterion in the appendix.

Assume that τ is positive definite, and set $\mathbf{U}_b = \varphi(b\otimes 1)$ for all $b\in B$. Then the equality above may be rewritten as

$$\mathbf{U}_b^* = \mathbf{U}_{\tau(b)} \text{ for all } b\in B.$$

We may now prove an easy lemma.

Lemma 2.4. *The map*

$$\begin{aligned} B &\longrightarrow \mathrm{M}_n(\mathbb{C}) \\ b &\longmapsto \mathbf{U}_b \end{aligned}$$

is an injective morphism of k-algebras. Moreover, the induced group morphism

$$\begin{aligned} B^\times &\longrightarrow \mathrm{GL}_n(\mathbb{C}) \\ b &\longmapsto \mathbf{U}_b \end{aligned}$$

is injective.

Proof. Clearly, $\mathbf{U}_1 = I_n$. Let $b, b'\in B$. Since φ is a morphism of L-algebras, we have

$$\mathbf{U}_b\mathbf{U}_{b'} = \varphi(b\otimes 1)\varphi(b'\otimes 1) = \varphi(bb'\otimes 1) = \mathbf{U}_{bb'}.$$

Similarly, one shows that $\mathbf{U}_b + \mathbf{U}_{b'} = \mathbf{U}_{b+b'}$, and $\lambda\mathbf{U}_b = \mathbf{U}_{\lambda b}$ for all $\lambda\in k$.

Moreover, $\mathbf{U}_b = I_n$ if and only if $b=1$, since φ and the canonical map $B\longrightarrow B\otimes_k L$ are injective. This concludes the proof. □

Let us come back to the previous considerations. For all $b\in B$, we have

$$\mathbf{U}_b\mathbf{U}_b^* = \mathbf{U}_b\mathbf{U}_{\tau(b)} = \mathbf{U}_{b\tau(b)}.$$

In particular, $\mathbf{U}_b$ is unitary if and only if $b\tau(b)=1$. This motivates the following definition.

Definition 2.5. Let k/k_0 be any quadratic field extension, and let (B,τ) be a central simple k-algebra with an arbitrary unitary k/k_0-involution. We say that $b\in B$ is **unitary** (with respect to τ) if $b\tau(b)=1$.

The set of unitary elements is easily seen to be a subgroup of $B^\times$, that we denote by $\mathbf{U}(B,\tau)$.

Example 2.6. If k is a number field, $B=\mathrm{M}_n(k)$ and τ is the conjugate transpose of matrices, a unitary element with respect to τ is nothing but a unitary matrix.

The previous results may then be summarized as follows.

Lemma 2.7. *Let k/k_0 be a quadratic extension of number fields, whose non-trivial automorphism is the complex conjugation, and let (B,τ) be a central simple k-algebra with a positive definite unitary k/k_0-involution. The map*

$$\begin{aligned} B &\longrightarrow \mathrm{M}_n(\mathbb{C}) \\ b &\longmapsto \mathbf{U}_b \end{aligned}$$

induces an injective group morphism

$$\begin{aligned}\mathbf{U}(B,\tau) &\longrightarrow \mathbf{U}_n(\mathbb{C})\\ b &\longmapsto \mathbf{U}_b.\end{aligned}$$

Let (B,τ) be a central simple k-algebra with a positive definite unitary k/k_0-involution. Keeping the previous notation, for any subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$, we get a unitary space-time code

$$\mathcal{C}_{\mathcal{G}} = \{\mathbf{U}_b = \varphi(b\otimes 1) \mid b \in \mathcal{G}\}.$$

Hence, the main idea here is to take our unitary code $\mathcal{C}$ to be a finite subset of some $\mathcal{C}_{\mathcal{G}}$, where $\mathcal{G}$ is a subgroup of $\mathbf{U}(B,\tau)$. In this case, if B is division, we will have $\delta_{min}(\mathcal{C}) > 0$ (i.e. the code is fully diverse), and

$$\delta_{min}(\mathcal{C}) \geq \delta_{min}(\mathcal{C}_{\mathcal{G}}).$$

Of course, we still need to find a way to estimate $\delta_{min}(\mathcal{C}_{\mathcal{G}})$. This problem will be examined in the next section.

Example 2.8. Assume that B has a maximal subfield $L \subset \mathbb{C}$, and that τ is positive definite. In this case, it is well-known that we have a unique isomorphism of L-algebras $\varphi : B \otimes_k L \overset{\sim}{\longrightarrow} \mathrm{M}_n(L)$ satisfying

$$\varphi(b\otimes 1) = M_b \ \text{ for all } b \in B,$$

where M_b is the matrix of left multiplication by b with respect to a fixed L-basis of $B \otimes_k L$. In this case, for every $b \in \mathbf{U}(B,\tau)$, we will have $\mathbf{U}_b = M_b$, and thus, for any subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$, we will get

$$\mathcal{C}_{\mathcal{G}} = \{\mathbf{U}_b = M_b \mid b \in \mathcal{G}\}.$$

Thus, the difficulty now is to find examples of division algebras B carrying a positive definite unitary involution τ. Lemma 1.6 provides such examples.

Example 2.9. Let k/k_0 be a quadratic extension of number fields, and L/k be a Galois extension of number fields with Galois group G, such that complex conjugation induces a k_0-automorphism of L which commutes with the elements of G.

Let $B = (\xi, L/k, G)$ be a crossed-product algebra of degree n, where ξ is a 2-cocycle satisfying $|\xi_{\sigma,\rho}|^2 = 1$ for all $\sigma, \rho \in G$.

By Lemma 1.6, there exists a unique unitary involution τ on B such that

$$M_{\tau(b)} = M_b^* \ \text{ for all } b \in B,$$

where M_b is the matrix of left multiplication by b in the L-basis $(f_\sigma)_{\sigma\in G}$. By Remark 2.3 and the previous example, τ is positive definite.

Hence, for any subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$, we have

$$\mathcal{C}_{\mathcal{G}} = \{\mathbf{U}_b = M_b \mid b \in \mathcal{G}\}.$$

It is about time to show how to find classes of unitary elements in a division algebra with a unitary involution (B,τ) by looking at elements of norm 1 in some subfields of B. The following result has been proven is [10] in the case where B is a cyclic division k-algebra, but the result and its proof still hold in the general case (see also [2, Lemma IX.5.12]).

Lemma 2.10. *Let k be an arbitrary field, and let (B, τ) be a division k-algebra with a k/k_0-involution. Then for every $x \in B$, the following conditions are equivalent:*

1. *x is unitary with respect to τ;*
2. *there exists a subfield M of B containing x, such that τ restricts to a non-trivial k_0-automorphism of M and $N_{M/M^{\langle\tau\rangle}}(x) = 1$;*
3. *there exist a subfield M of B containing x and $u \in M^\times$, such that τ restricts to a non-trivial k_0-automorphism of M and $x = u\tau(u)^{-1}$.*

Example 2.11. Let $k = \mathbb{Q}(j)$, where $j = \zeta_3 = -\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i$, and $L = \mathbb{Q}(j)(\zeta_7 + \zeta_7^{-1})$. We have $\mathrm{Gal}(L/\mathbb{Q}(j)) = \langle\sigma\rangle$, where

$$\sigma : \begin{array}{c} L \longrightarrow L \\ \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2}. \end{array}$$

Consider the cyclic division algebra $B = (j, L/\mathbb{Q}(j), \sigma)$. Since $|j|^2 = 1$, by Example 1.8, there exists a positive definite unitary involution τ on B given by

$$\tau : \begin{array}{c} B \longrightarrow B \\ \lambda_0 + e\lambda_1 + e^2\lambda_2 \longmapsto \overline{\lambda_0} + ej^2\overline{\lambda_2^{\sigma}} + e^2j^2\overline{\lambda_1^{\sigma^2}}. \end{array}$$

Example 2.9 shows that the left multiplication matrix of any unitary element is a unitary matrix. Following the method explained above, we look for subfields M of B which are stable by τ. The first obvious subfield of B one can think of is L. The restriction of τ on L is the complex conjugation. In this case, unitary elements contained in L are elements of the form $z\overline{z}^{-1}, z \in L^\times$.

Let us consider now the subfield generated by e. Since $1, e, e^2$ are linearly independent over L, they are also linearly independent over k. Therefore $[k(e) : k] \geq 3$, and since $e^3 = \gamma$, we have $[k(e) : k] \leq 3$. Thus $k(e)$ is a subfield of B of degree 3 over k, and the minimal polynomial of e over k is $X^3 - j$. Thus we have an isomorphism

$$k(e) \cong_{\mathbb{Q}} \mathbb{Q}(\zeta_9),$$

where ζ_9 is a primitive 9^{th}-root of 1, this isomorphism mapping e onto ζ_9. Since $\tau(e) = e^{-1}$, the previous isomorphism maps $\tau(e)$ onto $\zeta_9^{-1} = \overline{\zeta}_9$. In other words, we have an isomorphism of k-algebras with involution

$$(k(e), \tau_{|k(e)}) \cong_k (\mathbb{Q}(\zeta_9), ^{-}).$$

It follows that unitary elements in $k(e)$ are mapped onto elements of the form $u\overline{u}^{-1}, u \in \mathbb{Q}(\zeta_9)^\times$ by this isomorphism.

Take for example the element $u = 1 + j + \zeta_9 + \zeta_9^2 j \in \mathbb{Q}(\zeta_9)$. This element corresponds to the element $y = (1 + j) + e + e^2 j \in k(e)$, and the element $\overline{u}$ corresponds to the element $\tau(y)$. Set $\mathbf{Y} = M_y$. Then we have

$$\mathbf{Y} = \begin{pmatrix} 1+j & j^2 & j \\ 1 & 1+j & j^2 \\ j & 1 & 1+j \end{pmatrix}.$$

Now we also have

$$M_{\tau(y)} = \begin{pmatrix} -j & 1 & j^2 \\ j & -j & 1 \\ j^2 & j & -j \end{pmatrix},$$

which can be checked to be $\mathbf{Y}^*$. Then the element $b = y\tau(y)^{-1}$ is unitary, and its multiplication matrix $\mathbf{U}_b = \mathbf{Y}(\mathbf{Y}^*)^{-1}$ is a unitary matrix, as we may check directly by computation.

3. The minimum determinant of a unitary code

Let us summarize what we have done in the previous section. Let k/k_0 be a quadratic extension of number fields, whose non-trivial automorphism is given by complex conjugation. Let (B,τ) be a central simple k-algebra of degree n with a positive definite unitary k/k_0-involution, let L/k be a splitting field of B ($L \subset \mathbb{C}$) and let

$$\varphi : B \otimes_k L \xrightarrow{\sim} \mathrm{M}_n(L)$$

be an isomorphism of L-algebras such that

$$\varphi(\tau(b) \otimes 1) = \varphi(b \otimes 1)^* \text{ for all } b \in B.$$

For any subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$, the set

$$\mathcal{C}_{\mathcal{G}} = \{\mathbf{U}_b = \varphi(b \otimes 1) \mid b \in \mathcal{G}\}$$

is a unitary algebraic code, which is fully diverse as soon as B is a division algebra.

As explained in the introduction, we would like to find a good estimation of the minimum determinant of our unitary code $\mathcal{C}_{\mathcal{G}}$. The first step is, as in the coherent case, to find a more tractable expression of it. This is given by the next lemma.

Lemma 3.1. *Let k be a number field, let (B,τ) be a central simple k-algebra with a positive definite unitary involution, and let $\mathcal{G}$ be a subgroup of $\mathbf{U}(B,\tau)$. Then we have*

$$\delta_{min}(\mathcal{C}_{\mathcal{G}}) = \inf_{b \in \mathcal{G}\setminus\{1\}} |\mathrm{Nrd}_B(1-b)|^2.$$

Proof. For all $b, b' \in \mathbf{U}(B,\tau), b \neq b'$, using Lemma 2.7, we get

$$\mathbf{U}_b - \mathbf{U}_{b'} = \mathbf{U}_b(I_n - \mathbf{U}_b^{-1}\mathbf{U}_{b'}) = \mathbf{U}_b(I_n - \mathbf{U}_{b^{-1}b'}).$$

Now, if b and b' run through all elements of $\mathcal{G}$, $b^{-1}b'$ runs through all elements of $\mathcal{G} \setminus \{1\}$. Since the determinant of a unitary matrix is a complex number of modulus 1, we finally get that

$$\delta_{min}(\mathcal{C}_{\mathcal{G}}) = \inf_{b \in \mathcal{G}\setminus\{1\}} |\det(I_n - \mathbf{U}_b)|^2.$$

Now we have

$$I_n - \mathbf{U}_b = I_n - \varphi(b \otimes 1) = \varphi((1-b) \otimes 1),$$

and therefore

$$\det(I_n - \mathbf{U}_b) = \det(\varphi((1-b) \otimes 1)) \text{ for all } b \in \mathcal{G} \setminus \{1\}.$$

Thus, this equality may be rewritten as

$$\det(I_n - \mathbf{U}_b) = \mathrm{Nrd}_B(1-b) \text{ for all } b \in \mathcal{G} \setminus \{1\},$$

and therefore

$$\delta_{min}(\mathcal{C}_{\mathcal{G}}) = \inf_{b\in\mathcal{G}\setminus\{1\}} |\mathrm{Nrd}_B(1-b)|^2.$$

This concludes the proof. □

Example 3.2. Let us keep the notation of Example 2.11. One may take the subgroup $G = \langle b\rangle$ of $\mathbf{U}(B,\tau)$ generated by b, and consider the unitary code $\mathcal{C}_G$. We then get an infinite unitary code. One way to see this is as follows: after computations, we get

$$\det(\mathbf{U}_b) = \frac{11}{38} - i\frac{21\sqrt{3}}{38}.$$

Hence, we have $\det(\mathbf{U}_b) = e^{i\theta}$, with $\cos(\theta) = \dfrac{11}{38}$. But one may show by induction that $\cos(2m\theta) \neq 1$ for all $m \geq 1$. In particular, $m\theta$ is never a rational multiple of 2π. It follows that $\mathbf{U}_b^m \neq I_3$ for all $m \geq 1$, which is equivalent to saying that G is infinite. However, the minimum determinant of such a code is 0, as shown in the next proposition.

Proposition 3.3. *If $\mathcal{G}$ is a subgroup of $\mathbf{U}(B,\tau)$ containing an element of infinite order, then $\delta_{min}(\mathcal{C}_{\mathcal{G}}) = 0$.*

Proof. Let $b \in \mathcal{G}$ be an element of infinite order. Since $\mathcal{H} = \langle b\rangle \subset \mathcal{G}$, we have

$$0 \leq \delta_{min}(\mathcal{C}_{\mathcal{G}}) \leq \delta_{min}(\mathcal{C}_{\mathcal{H}}).$$

Hence, it is enough to prove that $\delta_{min}(\mathcal{C}_{\mathcal{H}}) = 0$. Notice that, by assumption on b, the corresponding matrix $\mathbf{U}_b$ has infinite order, since the map

$$\begin{aligned}\mathbf{U}(B,\tau) &\longrightarrow \mathbf{U}_n(\mathbb{C})\\ b &\longmapsto \mathbf{U}_b\end{aligned}$$

is an injective group morphism by Lemma 2.7. Since $\mathbf{U}_b$ is unitary, it can be diagonalized and all its eigenvalues have modulus 1.

Let $e^{i\theta_j}, j = 1,\ldots,n$ be the (not necessarily distinct) eigenvalues of $\mathbf{U}_b$. For all $m \in \mathbb{Z}$, the matrix $I_n - \mathbf{U}_b^m$ is similar to the diagonal matrix whose diagonal entries are

$$1 - e^{im\theta_j} = -2i\sin(\frac{m\theta_j}{2})e^{i\frac{m\theta_j}{2}}, j = 1,\ldots,n.$$

It follows easily that

$$\delta_{min}(\mathcal{C}_{\mathcal{H}}) = 4^n \inf_{m\geq 1}\prod_{j=1}^{n}\sin^2(\frac{m\theta_j}{2}).$$

Now, since $\mathbf{U}_b$ has infinite order, at least one θ_j is not a rational multiple of 2π. For this θ_j, the sequence $(\sin(\frac{m\theta_j}{2}))_{m\geq 1}$ is dense in $[-1,1]$, so we may find an increasing sequence of integers $(\alpha_m)_{m\geq 1}$ such that $\lim\limits_{m}\sin(\dfrac{\alpha_m\theta_j}{2}) = 0$. This implies that $\delta_{min}(\mathcal{C}_{\mathcal{H}}) = 0$, and this concludes the proof. □

We now prove a result which will allow us to compute the minimum determinant in terms of norms of cyclotomic extensions.

If $n \geq 1$ is an integer, we denote by ϕ_n the n^{th} cyclotomic polynomial.

Proposition 3.4. *Let k be a number field, and let D be an arbitrary central division k-algebra of degree n. If $D^\times$ has an element d of order m, the following properties hold:*

1. *the minimal polynomial $\mu_{d,\mathbb{Q}}$ over $\mathbb{Q}$ is ϕ_m and $k(d)\cong_k k(\zeta_m)$, where $\zeta_m\in\mathbb{C}$ is some primitive m^{th}-root of 1;*
2. *$[k(\zeta_m):k]\mid n$ and either $\zeta_m\in k$ or $D\otimes_k k(\zeta_m)$ is not a division algebra;*
3. *$\dfrac{\varphi(m)}{gcd(\varphi(m),[k:\mathbb{Q}])}\mid n$. In particular, $\varphi(m)\mid n[k:\mathbb{Q}]$;*
4. *we have the equalities*

$$\begin{aligned}\mathrm{Nrd}_D(1-d) &= N_{k(\zeta_m)/k}(1-\zeta_m)^{\frac{n}{[k(\zeta_m):k]}}\\ &= (\mu_{\zeta_m,k}(1))^{\frac{n}{[k(\zeta_m):k]}}.\end{aligned}$$

Moreover, if D has prime degree and property (2) holds, then $D^\times$ has an element of order m.

Proof. Let $d\in D^\times$ be an element of order m, so we have $d^m=1$. Hence $\mu_{d,\mathbb{Q}}$ divides X^m-1, and therefore $\mu_{d,\mathbb{Q}}$ is a cyclotomic polynomial ϕ_r, for some $r\mid m$. Since $\phi_r\mid X^r-1$, we have $d^r-1=0$, and therefore $m\mid r$. Hence $r=m$ and $\mu_{d,\mathbb{Q}}=\phi_m$. Now $\mu_{d,k}\mid\mu_{d,\mathbb{Q}}$, so there exists $\zeta_m\in\mathbb{C}$, a primitive m^{th}-root of 1, such that $\mu_{d,k}(\zeta_m)=0$. Elementary Galois theory then shows that we have an isomorphism of k-algebras

$$k(d)\cong_k k(\zeta_m),$$

which maps d onto ζ_m. This proves (1). Notice for later use that such an isomorphism preserves degrees and norms. Therefore, $k(\zeta_m)$ is isomorphic to a subfield of D. In particular, $[k(\zeta_m):k]\mid n$. If $\zeta_m\notin k$, $k(\zeta_m)/k$ has degree at least 2, and it is well-known that $D\otimes_k k(\zeta_m)$ is not a division algebra (see [2, Proposition V.3.2] for example). Now assume that D has prime degree, and that $[k(\zeta_m):k]\mid n$. If $\zeta_m\in k$, then $\zeta_m\in D^\times$ has order m. If $D\otimes_k k(\zeta_m)$ is not a division algebra, then $k(\zeta_m)/k$ is an extension of degree at least 2 dividing n. Since D has prime degree, this implies that $k(\zeta_m)$ is isomorphic to a subfield of D. Such an isomorphism maps ζ_m onto an element $d\in D^\times$ of order m. This proves (2) and the last part of the proposition.

Now let $t=gcd(\varphi(m),[k:\mathbb{Q}])$, and write $[k:\mathbb{Q}]=rt$ and $\varphi(m)=st$, with $gcd(r,s)=1$. We have to prove that $s\mid n$. From the equalities

$$[k(\zeta_m):\mathbb{Q}]=[k(\zeta_m):k][k:\mathbb{Q}]=[k(\zeta_m):\mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m):\mathbb{Q}],$$

we get that $[k(\zeta_m):k]r=[k(\zeta_m):\mathbb{Q}(\zeta_m)]s$. In particular, we have $s\mid[k(\zeta_m):k]$. Since $[k(\zeta_m):k]=[k(d):k]$, and $[k(d):k]\mid n$, we get (3).

It remains to prove (4). Let M be a maximal subfield of D containing d. Then it contains $1-d$, and we have

$$\mathrm{Nrd}_D(1-d)=N_{M/k}(1-d)=N_{k(d)/k}(1-d)^{\frac{n}{[k(d):k]}}.$$

Thus, we have

$$\mathrm{Nrd}_D(1-d)=N_{k(\zeta_m)/k}(1-\zeta_m)^{\frac{n}{[k(\zeta_m):k]}}.$$

Now notice that $k(\zeta_m)=k(1-\zeta_m)$, and that

$$\mu_{1-\zeta_m,k}(X)=(-1)^{[k(\zeta_m):k]}\mu_{\zeta_m,k}(1-X).$$

It follows immediately that $N_{k(\zeta_m)/k}(1-\zeta_m)=\mu_{\zeta_m,k}(1)$, and this proves (4). This concludes the proof. $\square$

Corollary 3.5. *Let k be a number field, and let D be a central division k-algebra of degree n. Then any subgroup of $D^\times$ is either finite or has an element of infinite order.*

Proof. Let $\mathcal{G}$ be a subgroup of $D^\times$. Assume that every element of $\mathcal{G}$ has finite order. By the previous proposition, if $g \in \mathcal{G}$ has order m, then $\varphi(m) \mid n[k:\mathbb{Q}]$. This implies that m may take only finitely many values. In particular, the least common multiple of the orders of the elements of $\mathcal{G}$ is finite, that is $\mathcal{G}$ has finite exponent. Now if L is a maximal subfield of D, the injective k-algebra morphism

$$\varphi_{D,L} : D \hookrightarrow \mathrm{M}_n(L)$$

induces an injective group morphism $D^\times \hookrightarrow \mathrm{GL}_n(L)$. It follows that $\mathcal{G}$ is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{C})$ of finite exponent. By a celebrated theorem of Burnside, this implies that $\mathcal{G}$ is finite. □

We now summarize our results on the minimum determinant of unitary codes in the following theorem.

Theorem 3.6. *Let $\mathcal{G}$ be a subgroup of $\mathbf{U}(B,\tau)$, and assume that B is a division k-algebra of degree n. Then $\mathcal{G}$ is either finite or has an element of infinite order. Moreover, the following properties hold:*

1. *If $\mathcal{G}$ has an element of infinite order, then $\delta_{min}(\mathcal{C}_G) = 0$;*
2. *If $\mathcal{G}$ is finite, we have*

$$\begin{aligned}\delta_{min}(\mathcal{C}_\mathcal{G}) &= \inf_{b\in\mathcal{G}\setminus\{1\}} |N_{k(\zeta_{m_b})/k}(1-\zeta_{m_b})|^{\frac{2n}{[k(\zeta_{m_b}):k]}} \\ &= \inf_{b\in\mathcal{G}\setminus\{1\}} |\mu_{\zeta_{m_b},k}(1)|^{\frac{2n}{[k(\zeta_{m_b}):k]}},\end{aligned}$$

where m_b is the order of b.

Proof. This follows from Proposition 3.3, Proposition 3.4 and Corollary 3.5, since a subgroup of $\mathbf{U}(B,\tau)$ is a subgroup of $B^\times$. □

Remark 3.7. If $b \in \mathcal{G}$ has finite order m_b, Proposition 3.4 shows that that $\mathrm{Nrd}_B(1-b)$ only depends on m_b. In particular, $\delta_{min}(\mathcal{C}_\mathcal{G})$ only depends on the orders of the elements of $\mathcal{G}$, and not on the group itself. Therefore, to compute the minimum determinant, one may proceed as follows:

1. compute the set of values $S = \{m_b \mid b \in \mathcal{G} \setminus \{1\}\}$;
2. choose a subset $\mathcal{S}$ of $\mathcal{G}$ such that each element of S is obtained by a unique element of $\mathcal{S}$;
3. the observation above shows that we have

$$\begin{aligned}\delta_{min}(\mathcal{C}_\mathcal{G}) &= \inf_{b\in\mathcal{S}} |\mathrm{Nrd}_B(1-b)|^2 \\ &= \inf_{b\in\mathcal{S}} |\det(I_n - \mathbf{U}_b)|^2 \\ &= \inf_{b\in\mathcal{S}} |N_{k(\zeta_{m_b})/k}(1-\zeta_{m_b})|^{\frac{2n}{[k(\zeta_{m_b}):k]}} \\ &= \inf_{b\in\mathcal{S}} |\mu_{\zeta_{m_b},k}(1)|^{\frac{2n}{[k(\zeta_{m_b}):k]}}.\end{aligned}$$

As a first application, we compute the exact value of the minimum determinant of a code presented in [7].

Example 3.8. Let $B = (j, \mathbb{Q}(\zeta_{21})/K, \sigma)$, where $K = \mathbb{Q}(j, \sqrt{-7})$ and $\sigma : \zeta_{21} \longmapsto \zeta_{21}^4$. One may show that B is a division algebra. Let e be the generator of this cyclic k-algebra. Then Oggier considers the unitary code

$$\mathcal{C} = \{E^r D^s \mid r = 0, \ldots, 8, s = 0, \ldots, 6\},$$

where E and D are the left multiplication matrix of e and ζ_{21} respectively.

In fact, $\mathcal{C}$ is simply the unitary code $\mathcal{C}_{\mathcal{G}}$, where $\mathcal{G}$ is the group of order 63, generated by e and ζ_{21}. The possible values for the order of an element of $\mathcal{G}$ are $1, 3, 7, 9, 21, 63$. Notice that $\mathcal{G}$ is not abelian, hence not cyclic, so $\mathcal{G}$ has no elements of order 63. We also look only at non-trivial elements of $\mathcal{G}$, so we may also discard 1. One may also check that $\mathcal{G}$ has no element of order 9. By considering $\zeta_{21}^7, \zeta_{21}^3$ and ζ_{21}, we see that the other possible values are obtained.

The remark above shows that it is enough to compute $|\det(I_3 - D^m)|^2$ for $m = 1, 3, 7$. Here, the minimum is obtained for $m = 1$, so

$$\delta_{min}(\mathcal{C}_G) = |\det(I_3 - D)|^2 \approx 0.21.$$

Computing $\mu_{\zeta_{21},K}$ shows that the exact value is $\dfrac{5 - \sqrt{21}}{2}$.

Notice that we may extend this code by considering the group

$$\mathcal{G}' = \langle e, \zeta_{21}, -j\rangle = \langle e, \zeta_{21}, -1\rangle.$$

It is easy to check that $\mathcal{G}' \simeq \mathcal{G} \times \{\pm 1\}$, so that

$$\mathcal{C}_{\mathcal{G}'} = \{\pm \mathbf{U} \mid \mathbf{U} \in \mathcal{C}_{\mathcal{G}}\}.$$

Hence the orders of non-trivial elements of $\mathcal{G}$ are now

$$2, 3, 6, 7, 14, 21, 42,$$

and $-1, -\zeta_{21}^7, -\zeta_{21}^3$ and $-\zeta_{21}$ are elements of order $2, 6, 14$ and 42 respectively. One may compute that

$$\delta_{min}(\mathcal{C}_{\mathcal{G}'}) = |\det(I_3 + D^2)|^2 = \frac{23 - 5\sqrt{21}}{2} \approx 0.04.$$

Remark 3.9. Let $\mathcal{G}$ be a finite subgroup of $\mathbf{U}(B, \tau)$. One way to get a group $\mathcal{G}$ whose cardinality is as large as possible is to ensure that G contains all the roots of unity lying in k. However, we will often get a small minimum determinant, as we proceed to show now.

Indeed, Theorem 3.6 shows in particular that, if $\zeta_m \in k$, then we have

$$\delta_{min}(\mathcal{C}_{\mathcal{G}}) \leq |1 - \zeta_m|^{2n},$$

for any finite subgroup $\mathcal{G}$ of $\mathbf{U}(B, \tau)$ (where n is the degree of B over k), that is

$$\delta_{min}(\mathcal{C}_{\mathcal{G}}) \leq (2\sin(\frac{\pi}{m}))^{2n}.$$

Hence, the diversity product satisfies

$$\zeta(\mathcal{C}_{\mathcal{G}}) \leq \sin(\frac{\pi}{m}).$$

Now, if $m \geq 7$, this shows that

$$\zeta(\mathcal{C}_{\mathcal{G}}) \leq \sin(\frac{\pi}{7}) < 0.44.$$

The upper bound above also shows that $\zeta(\mathcal{C}_\mathcal{G})$ will tend to be very small if the base field k contains roots of 1 of large order.

The next lemma, used together with the previous proposition, allows us to compute the minimum determinant of a unitary code $\mathcal{C}_\mathcal{G}$ when $k/\mathbb{Q}$ is a totally imaginary quadratic extension.

Lemma 3.10. *Let $k/\mathbb{Q}$ be a totally imaginary quadratic extension, and let $m \geq 2$. Then we have*

$$|N_{k(\zeta_m)/k}(1-\zeta_m)|^2 = \begin{cases} p & \text{if } m = p^r, r \geq 1 \text{ and } k \subset \mathbb{Q}(\zeta_m) \\ p^2 & \text{if } m = p^r, r \geq 1 \text{ and } k \not\subset \mathbb{Q}(\zeta_m) \\ 1 & \text{otherwise .} \end{cases}$$

Proof. Since $k/\mathbb{Q}$ is a totally quadratic imaginary extension, we have

$$|N_{k(\zeta_m)/k}(1-\zeta_m)|^2 = N_{k(\zeta_m)/\mathbb{Q}}(1-\zeta_m) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1-\zeta_m)^{[k(\zeta_m):\mathbb{Q}(\zeta_m)]}.$$

Therefore, we have

$$|N_{k(\zeta_m)/k}(1-\zeta_m)|^2 = \begin{cases} N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1-\zeta_m) \text{ if } k \subset \mathbb{Q}(\zeta_m) \\ N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1-\zeta_m)^2 \text{ if } k \not\subset \mathbb{Q}(\zeta_m). \end{cases}$$

Notice now that $\mu_{1-\zeta_m,\mathbb{Q}}(X) = (-1)^{\varphi(m)}\phi_m(1-X)$. It follows that we have

$$N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1-\zeta_m) = \phi_m(1).$$

If p is a prime number, we have the well-known relations

$$\phi_m(X^p) = \begin{cases} \phi_{mp} & \text{if } p \mid m \\ \phi_{mp}\phi_m & \text{otherwise.} \end{cases}$$

It follows easily that $\phi_m(1) = p$ if $m = p^r, r \geq 1$ and $\phi_m(1) = 1$ otherwise. This concludes the proof. ☐

Remarks 3.11. Assume that $k/\mathbb{Q}$ is a totally imaginary quadratic extension. Let $\mathcal{G}$ be a subgroup of $\mathbf{U}(B,\tau)$, and assume that B is a division k-algebra of degree n.

1. It follows from Theorem 3.6 that if $\mathcal{G}$ contains an element of order m we have
$$\varphi(m) \mid 2n \text{ if } k \subset \mathbb{Q}(\zeta_m)$$
and
$$\varphi(m) \mid n \text{ if } k \not\subset \mathbb{Q}(\zeta_m).$$
2. If $\mathcal{G}$ is finite and contains an element whose order is not a prime power, then we have
$$\delta_{min}(\mathcal{C}_\mathcal{G}) = 1,$$
that is
$$\zeta(\mathcal{C}_\mathcal{G}) = \frac{1}{2}.$$
Indeed, this is an immediate consequence of Theorem 3.6 and Lemma 3.10.

If we want to find subgroups $\mathcal{G}$ of $\mathbf{U}(B,\tau)$ such that $\delta_{min}(\mathcal{C}_\mathcal{G}) > 0$, Theorem 3.6 says that all elements of $\mathcal{G}$ need to have finite (multiplicative) order. Such elements may be found as follows: choose a subfield M of B which is stable by τ, and look for unitary elements among 'roots of 1 in M', that is elements $b \in M$ such that $\mu_{b,\mathbb{Q}} = \phi_m$ for some $m \geq 1$. Moreover, a list of possible values for m may be found using points (2) and (3) of Proposition 3.4.

However, the product of elements of finite order is not necessarily an element of finite order. Hence, once we found several unitary elements of finite order, we are still not ensured that the group they generate only has elements of finite order. The next lemma shows how to avoid this problem.

Lemma 3.12. *Assume that $k/\mathbb{Q}$ is a totally quadratic imaginary extension. Let Λ be a subring of B which is also a free $\mathcal{O}_k$-module of finite rank, where $\mathcal{O}_k$ is the ring of integers of k. Then $\mathbf{U}(B,\tau)\cap\Lambda^\times$ is finite.*

Proof. Let $n=\deg(B)$. By Lemma 2.7, the map

$$\psi\colon \begin{array}{rcl} \mathbf{U}(B,\tau) & \longrightarrow & \mathbf{U}_n(\mathbb{C}) \\ b & \longmapsto & \mathbf{U}_b \end{array}$$

is an injective group morphism. Therefore, $\psi(\Lambda)$ is also a free $\mathcal{O}_k$-module of finite rank. Since $k/\mathbb{Q}$ is quadratic imaginary, $\mathcal{O}_k$ is a full $\mathbb{Z}$-lattice of the $\mathbb{R}$-vector space $\mathbb{C}\simeq_{\mathbb{R}}\mathbb{R}^2$. Thus, $\psi(\Lambda)$ is a full $\mathbb{Z}$-lattice of $\mathrm{M}_n(\mathbb{C})\simeq_{\mathbb{R}}\mathbb{R}^{2n^2}$. It follows that $\mathbf{U}_n(\mathbb{C})\cap\psi(\Lambda)$ is finite, since $\mathbf{U}_n(\mathbb{C})$ is compact. Consequently, $\psi(\mathbf{U}(B,\tau)\cap\Lambda^\times)\subset \mathbf{U}_n(\mathbb{C})\cap\psi(\Lambda)$ is finite, and therefore so is $\mathbf{U}(B,\tau)\cap\Lambda^\times$. This concludes the proof. $\square$

Remark 3.13. Such a subring Λ always exists. One may even assume that Λ contains a k-basis of B. For example, let $e_1=1_B,e_2,\ldots,e_{n^2}$ be a k-basis of B containing 1_B. For all $1\leq i,j\leq n^2$, there exist $m_{ij}\in\mathbb{Z}$ such that

$$m_{ij}e_ie_j\in\sum_{i=1}^{n^2}e_i\mathcal{O}_k.$$

Let m be the least common multiple of the $m'_{ij}s$. Then we have

$$me_ie_j\in\sum_{i=1}^{n^2}e_i\mathcal{O}_k \text{ for } 1\leq i,j\leq n^2.$$

Let $\Lambda=1_B\mathcal{O}_k\oplus me_2\mathcal{O}_k\oplus\cdots\oplus me_{n^2}\mathcal{O}_k$. By construction, Λ is a subring of B, which contains a k-basis of B, and which a free $\mathcal{O}_k$-module of finite rank.

Example 3.14. We will use here the notation introduced in Example 1.5. Let $k=\mathbb{Q}(i)$, and consider the central simple k-algebra

$$B=(\zeta_8,\frac{1+2i}{\sqrt{5}},i,k(\sqrt{2},\sqrt{5})/k,\sigma,\rho),$$

where σ and ρ are defined in a unique way by

$$\sigma(\sqrt{2})=\sqrt{2},\sigma(\sqrt{5})=-\sqrt{5} \text{ and } \rho(\sqrt{2})=-\sqrt{2},\rho(\sqrt{5})=\sqrt{5}.$$

As shown in [1], this is a division k-algebra. By Example 1.5, the values of the cocycle corresponding to the algebra $(a,b,u,L/k,\sigma,\rho)$ will have modulus 1 if and only if a,b and u have modulus 1. All these conditions are fulfilled here, so by Lemma 1.6, there is an involution τ on B such that $\tau_{|L}$ is the complex conjugation, $\tau(e)=e^{-1}$, and $\tau(f)=f^{-1}$, where e,f are the generators of B.

The elements e and f are unitary and e has finite order. However, f has infinite order. Since $\sqrt{5}$ and f commute, $M=k(f,\sqrt{5})$ is a subfield of B which is stable by τ. Let $\alpha \in \mathbb{C}$ such that $\alpha^2 = \dfrac{1+2i}{\sqrt{5}}$. Notice that $(\alpha\overline{\alpha})^2 = 1$, and thus $\alpha\overline{\alpha} = 1$. We then have an isomorphism of k-algebras

$$M \cong_k k(\alpha, \sqrt{5})$$

which maps f onto α and $\sqrt{5}$ onto $\sqrt{5}$. Since $\tau(f) = f^{-1}$ is mapped onto $\alpha^{-1} = \overline{\alpha}$, it easily follows that we have an isomorphism of k-algebras with involution

$$(M, \tau_{|M}) \cong_k (k(\alpha, \sqrt{5}), ^{-}).$$

Set $\theta = \dfrac{1+\sqrt{5}}{2}$. One may check that the element

$$\zeta = -\frac{\theta}{2} + \alpha(\frac{1}{2} + i\frac{1-\theta}{2})$$

satisfies $\zeta^5 = i$, that is ζ is a primitive 20^{th}-root of 1. In particular, $\zeta\overline{\zeta} = 1$. Using the isomorphism above, this yields an element

$$z = -\frac{\theta}{2} + f(\frac{1}{2} + i\frac{1-\theta}{2}) \in B,$$

which is unitary and which has order 20.

Straightforward computations show that

$$e^{16} = 1, z^{20} = 1 \text{ and } ze = ez^{-3}.$$

It follows easily that the ring $\Lambda = \mathcal{O}_k[e, z]$ is finitely generated as an $\mathcal{O}_k$-module, hence as an abelian group. One may show that

$$\mathcal{G} = \mathbf{U}(B, \tau) \cap \Lambda^\times = \{e^\ell z^m \mid \ell = 0, \ldots, 3, m = 0, \ldots, 19\},$$

is a group of order 80. Therefore, the unitary code $\mathcal{C}_\mathcal{G}$ consists of 80 matrices. If $E = \mathbf{U}_e, Z = \mathbf{U}_z$, we have

$$E = \begin{pmatrix} 0 & \zeta_8 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\zeta_8 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

and

$$Z = \begin{pmatrix} -i\frac{\theta}{2} & 0 & \frac{1}{2} + i\frac{\theta-1}{2} & 0 \\ 0 & i\frac{\theta-1}{2} & 0 & -\frac{\theta}{2} - \frac{i}{2} \\ \frac{1}{2} - i\frac{\theta-1}{2} & 0 & -i\frac{\theta}{2} & 0 \\ 0 & -\frac{\theta}{2} + \frac{i}{2} & 0 & i\frac{\theta-1}{2} \end{pmatrix}.$$

In other words,

$$\mathcal{C}_\mathcal{G} = \{E^\ell Z^m \mid \ell = 0, \ldots, 3, m = 0, \ldots, 19\}.$$

By Remark 3.11 (2), $\zeta(\mathcal{C}_\mathcal{G}) = \dfrac{1}{2}$.

Let us give another example.

Example 3.15. Let $k = \mathbb{Q}(j)$, and let $L = k(\zeta_7)$. Then L/k is a cyclic extension of degree 6, a generator σ of $\mathrm{Gal}(L/k)$ being given by

$$\sigma\colon \begin{aligned} L &\longrightarrow L \\ \zeta_7 &\longmapsto \zeta_7^3. \end{aligned}$$

Consider the cyclic k-algebra $B = (-j, k(\zeta_7)/k, \sigma)$. One may show that B is a division k-algebra (see [2, Example IX.5.28] for a proof). Since B fulfills all the assumptions of Lemma 1.6, we may consider the unitary involution τ described in this lemma.

If e is the canonical generator of B, then e is a unitary element of order 36. Moreover, $z = \zeta_7$ is a unitary element of order 7. It follows from the equality $ze = ez^\sigma = ez^3$ that the subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$ generated by e and z is a finite group of order $36{\cdot}7 = 252$. Theorem 3.6 and Lemma 3.10 then show that $\zeta(\mathcal{C}_\mathcal{G}) = \dfrac{1}{2}$.

In other words, the unitary code

$$\mathcal{C}_\mathcal{G} = \{E^\ell Z^m \mid \ell = 0,\ldots,35, m = 0,\ldots,6\}$$

consists of 252 unitary matrices and satisfies $\delta_{min}(\mathcal{C}_\mathcal{G}) = 1$, where

$$E = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -j \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} \zeta_7^{-2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_7^4 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_7^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_7^{-4} & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_7^{-1} \end{pmatrix}.$$

One may also obtain a code with a better diversity product by considering a restricted number of matrices. Indeed, let us consider the subgroup $\mathcal{H}$ of $\mathbf{U}(B,\tau)$ generated by e^4 and z. Then $\mathcal{H}$ is a semidirect product of the cyclic group $\langle e^4\rangle$ of order 9 and of the cyclic group $\langle z\rangle$ of order 7. Straightforward arguments then show that the orders of non-trivial elements of $\mathcal{H}$ are $3, 7$ or 9. By Lemma 3.10, the unitary code

$$\mathcal{C}_\mathcal{H} = \{E^{4\ell} Z^m \mid \ell = 0,\ldots,8, m = 0,\ldots,6\}$$

has 63 elements and satisfies $\delta_{min}(\mathcal{C}_\mathcal{H}) = 3$, that is $\zeta(\mathcal{C}_\mathcal{H}) \approx 0.55$.

Notice that the method using fixed-point free groups in [14] does not provide an example of group constellations for $n = 6$, and provides a non-group constellation $\mathcal{C}$ of 72 matrices with diversity product equal to $\dfrac{1}{2}$.

In this section, we mainly focused on the computation of infinite unitary codes built using a subgroup $\mathcal{G}$ of $\mathbf{U}(B,\tau)$. Theorem 3.6 thus tells us that we have to exclude elements of infinite order to ensure that $\delta_{min}(\mathcal{C}_\mathcal{G}) > 0$. However, in practice, we only need finite subsets $\mathcal{C}$ of $\mathcal{C}_\mathcal{G}$. Therefore, we may use these elements to extend further the codes obtained using the techniques developed above, and we are not restricted to consider only finite groups.

Example 3.16. Let us keep the notation of Example 3.14, and consider the code

$$\mathcal{C}_r = \{E^\ell Z^m F^t \mid \ell = 0,\ldots,3, m = 0,\ldots,19, t = 0,\ldots,r\},$$

where F is the multiplication matrix of the element f. Notice that F is a unitary matrix of infinite order, since f is a unitary element of infinite order. The unitary code $\mathcal{C}_r$ has $80(r+1)$ elements, and one may compute that

$$\zeta(\mathcal{C}_1) \approx 0.41, \zeta(\mathcal{C}_2) \approx 0.33, \zeta(\mathcal{C}_3) \approx 0.27, \zeta(\mathcal{C}_4) \approx 0.22.$$

Notice that the method using fixed-point free groups in [14] yields a non-group constellation $\mathcal{C}$ of 289 matrices with diversity product approximatively equal to 0.31.

APPENDIX: POSITIVE DEFINITE UNITARY INVOLUTIONS.

As promised, we give in this appendix an explicit criterion to decide whether or not a given unitary involution is positive definite. First, we need a lemma. All the fields here have characteristic different from 2.

Lemma 3.17. *Let k/k_0 be a quadratic extension of arbitrary fields, let $^-$ be its non-trivial k_0-automorphism, and let (B,τ) be a central simple k-algebra with a unitary k/k_0 involution. Then we have*

$$\mathrm{Trd}_B(\tau(b)) = \overline{\mathrm{Trd}_B(b)} \quad \textit{for all } b \in B,$$

where Trd_B is the reduced trace.

Proof. Let L/k be a splitting field of B, so we have an isomorphism of L-algebras

$$\varphi : B \otimes_k L \xrightarrow{\sim} \mathrm{M}_n(L).$$

Set $\tau' = \varphi \circ (\tau \otimes ^-) \circ \varphi^{-1}$. It is easy to check that τ' is a unitary involution of $\mathrm{M}_n(L)$. By Example 1.2, there exists an invertible hermitian matrix $H \in \mathrm{M}_n(L)$ such that $\tau' = \mathrm{Int}(H)\circ^*$. In other words, we have

$$(\mathrm{Int}(H)\circ^*) \circ \varphi = \varphi \circ (\tau \otimes ^-).$$

Thus, for all $b \in B$, we get

$$H\varphi(b \otimes 1)^* H^{-1} = \varphi(\tau(b) \otimes 1).$$

By definition of the reduced trace, we have $\mathrm{Trd}_B(\tau(b)) = \mathrm{tr}(\varphi(\tau(b)\otimes 1))$. Therefore, we get

$$\mathrm{Trd}_B(\tau(b)) = \mathrm{tr}(H\varphi(b\otimes 1)^* H^{-1}) = \mathrm{tr}(\varphi(b \otimes 1)^*) = \overline{\mathrm{tr}(\varphi(b\otimes 1))} = \overline{\mathrm{Trd}_B(b)}.$$

This concludes the proof. □

Notice now that for all $b \in B$, $\tau(b)b$ is τ-symmetric. In view of this lemma, the map

$$T_{(B,\tau)} \colon \begin{array}{l} B \times B \longrightarrow k \\ (b, b') \longmapsto \mathrm{Trd}_B(\tau(b)b'). \end{array}$$

is a hermitian form on B with respect to $(k, ^-)$.

Let L/k be a field extension, and let $\alpha : L \longrightarrow L$ be a ring automorphism of L extending $^-$. In particular, $\alpha \neq \mathrm{Id}_L$. If L_0 denotes the subfield of L fixed by α, then L_0 contains k_0 and L/L_0 is a quadratic extension.

If $h : V \times V \longrightarrow k$ is a hermitian form on a finite dimensional k-vector space V with respect to $(k, ^-)$, we denote by $h_{(L,\alpha)}$ the unique hermitian form on $V \otimes_k L$ with respect to (L,α) satisfying

$$h_{(L,\alpha)}(v_1 \otimes \lambda_1, v_2 \otimes \lambda_2) = \alpha(\lambda_1)\lambda_2 h(v_1, v_2) \text{ for all } v_1, v_2 \in V, \lambda_1, \lambda_2 \in L.$$

We then have the following lemma.

Lemma 3.18. *Let (B,τ) and (B',τ') be two central simple k-algebras with a unitary k/k_0 involution, let L/k be a field extension, and let $\alpha : L \longrightarrow L$ be a ring automorphism of L extending $^-$. Then the following properties hold :*

(1) *if $(B,\tau) \cong_k (B',\tau')$, then $T_{(B,\tau)} \cong_k T_{(B',\tau')}$;*

(2) *the map* $\tau \otimes \alpha$ *is a unitary* L/L_0*-involution on* $B \otimes_k L$*, and we have*

$$T_{(B\otimes_k L,\tau\otimes\alpha)} \cong_L (T_{(B,\tau)})_{(L,\alpha)}$$

(3) *Let* $B = \mathrm{M}_n(k)$ *and let* $\tau = \mathrm{Int}(H)\circ^*$*, for some invertible hermitian matrix* $H \in \mathrm{M}_n(k)$*. Finally, let* h_H *be the hermitian form on* k^n *defined by*

$$h_H\colon \begin{array}{c} k^n \times k^n \longrightarrow k \\ (X,Y) \longmapsto X^*HY \end{array}$$

If $h_H \cong_k \langle \lambda_1,\ldots,\lambda_n\rangle, \lambda_i \in k_0^\times$*, then*

$$T_{(B,\tau)} \cong_k \langle 1, \lambda_1\lambda_2^{-1},\ldots,\lambda_j\lambda_i^{-1},\ldots\rangle.$$

Proof.

(1) Let $\varphi : B \xrightarrow{\sim} B'$ be an isomorphism of k-algebras such that $\varphi\circ\tau = \tau'\circ\varphi$. Then for all $b_1, b_2 \in B$, we have

$$\begin{array}{rcl} T_{(B',\tau')}(\varphi(b_1),\varphi(b_2)) & = & \mathrm{Trd}_{B'}(\tau'(\varphi(b_1))\varphi(b_2)) \\ & = & \mathrm{Trd}_{B'}(\varphi(\tau(b_1))\varphi(b_2)) \\ & = & \mathrm{Trd}_{B'}(\varphi(\tau(b_1)b_2)) \\ & = & \mathrm{Trd}_{B}(\tau(b_1)b_2) \\ & = & T_{(B,\tau)}(b_1,b_2). \end{array}$$

In other words, φ induces an isomorphism of hermitian forms

$$T_{(B,\tau)} \cong_k T_{(B',\tau')}.$$

(2) The first part is clear. For all $b_1, b_2 \in B$, we have

$$\begin{array}{rcl} T_{(B\otimes_k L,\tau\otimes\alpha)}(b_1\otimes 1, b_2\otimes 1) & = & \mathrm{Trd}_{B\otimes_k L}((\tau(b_1)\otimes 1)(b_2\otimes 1)) \\ & = & \mathrm{Trd}_{B\otimes_k L}(\tau(b_1)b_2\otimes 1) \\ & = & \mathrm{Trd}_{B}(\tau(b_1)b_2) \\ & = & (T_{(B,\tau)})_{(L,\alpha)}(b_1\otimes 1, b_2\otimes 1). \end{array}$$

Since for $b \in B$ the elements $b\otimes 1$ span $B\otimes_k L$ as an L-vector space, this yields the desired result.

(3) Let $(X_1,\ldots,X_n)$ be an h_H-orthogonal basis of k^n, and let $P \in \mathrm{GL}_n(k)$ be the matrix whose columns are $X_1,\ldots,X_n$. The matrix $D = P^*HP$ is a diagonal invertible matrix (with diagonal entries lying in $k_0^\times$). For all $M \in \mathrm{M}_n(k)$, easy computations show that we have

$$T_{(B,\tau)}(\mathrm{Int}((P^*)^{-1})(M)) = \mathrm{Trd}_B(DM^*D^{-1}M) = T_{(B,\mathrm{Int}(D)\circ^*)}(M).$$

Hence, we have an isomorphism of hermitian forms $T_{(B,\tau)} \cong_k T_{(B,\mathrm{Int}(D)\circ^*)}$, and we thus may assume that $H = D$. Now if $\lambda_1,\ldots,\lambda_n \in k_0^\times$ are the diagonal entries of D and $M = (a_{ij})$, we have

$$T_{(B,\mathrm{Int}(D)\circ^*)}(M) = \mathrm{tr}(DM^*D^{-1}M) = \sum_{i,j}\lambda_i\lambda_j^{-1}\overline{a}_{ji}a_{ji} = \sum_{i,j}\lambda_j\lambda_i^{-1}\overline{a}_{ij}a_{ij}.$$

Therefore, the canonical isomorphism $k^{n^2} \cong_k \mathrm{M}_n(k)$ induces an isomorphism of hermitian forms

$$T_{(B,\mathrm{Int}(D)\circ^*)} \cong_k \langle 1, \lambda_1\lambda_2^{-1},\ldots,\lambda_j\lambda_i^{-1},\ldots\rangle.$$

This concludes the proof. □

We are now ready to state and prove the desired criterion.

Theorem 3.19. *Assume that k/k_0 is a quadratic extension of number fields, whose non-trivial k_0-automorphism is the complex conjugation. In particular, $k_0 \subset \mathbb{R}$. Let (B, τ) be a central simple k-algebra with a unitary k/k_0-involution. Then τ is positive definite if and only if T_τ is a positive definite hermitian form, that is if and only if*

$$\mathrm{Trd}_B(\tau(b)b) > 0 \quad \text{for all } b \in B \setminus \{0\}.$$

Proof. Assume first that τ is positive definite, so that there exists L/k ($L \subset \mathbb{C}$) such that

$$(B \otimes_k L, \tau \otimes ^-) \cong_L (\mathrm{M}_n(L), ^*).$$

By Lemma 3.18, we have

$$(T_{(B,\tau)})_{(L,^-)} \cong_L T_{(B\otimes_k L, \tau\otimes^-)} \cong_L T_{(\mathrm{M}_n(L),^*)} \cong_L \langle 1, \ldots, 1\rangle.$$

It follows that for all non-zero $x \in B \otimes_k L$, we have

$$(T_{(B,\tau)})_{(L,^-)}(x, x) > 0.$$

In particular, for all non-zero $b \in B$, we get

$$(T_{(B,\tau)})_{(L,^-)}(b \otimes 1, b \otimes 1) = T_{(B,\tau)}(b, b) = \mathrm{Trd}_B(\tau(b)b) > 0.$$

Conversely, assume that $\mathrm{Trd}_B(\tau(b)b) > 0$ for all $b \in B \setminus \{0\}$ and take $L = \mathbb{C}$. The assumption means that $T_{(B,\tau)}$ is a positive definite hermitian form. Then $(T_{(B,\tau)})_{(\mathbb{C},^-)}$ is also positive definite, and thus $T_{(B\otimes_k L,\tau\otimes^-)}$ is positive definite by the second point of the previous lemma.

Now, let us fix an isomorphism of $\mathbb{C}$-algebras $\varphi : B \otimes_k \mathbb{C} \xrightarrow{\sim} \mathrm{M}_n(\mathbb{C})$. The map $\tau' = \varphi \circ (\tau \otimes ^-) \circ \varphi^{-1}$ is easily seen to be a unitary $\mathbb{C}/\mathbb{R}$-involution on $\mathrm{M}_n(\mathbb{C})$, so $\tau' = \mathrm{Int}(H)\circ^*$ for some invertible hermitian matrix H by Example 1.2. By definition of τ', we have

$$(B \otimes_k \mathbb{C}, \tau \otimes ^-) \cong_{\mathbb{C}} (\mathrm{M}_n(\mathbb{C}), \mathrm{Int}(H)\circ^*).$$

By Lemma 3.18, we get that

$$T_{(B\otimes_k\mathbb{C},\tau\otimes^-)} \cong_{\mathbb{C}} \langle 1, \lambda_1\lambda_2^{-1}, \ldots \lambda_j\lambda_i^{-1}, \ldots\rangle,$$

where $\langle \lambda_1, \ldots, \lambda_n\rangle$ is a diagonalization of the hermitian form over $\mathbb{C}^n$ represented by H. Now, since $T_{(B\otimes_k\mathbb{C},\tau\otimes^-)}$ is positive definite, it easily follows that $\lambda_1, \ldots, \lambda_n$ have the same sign. Replacing H by $-H$ if necessary, one may assume that $\lambda_i > 0$ for all i. In this case, it follows that H is a positive definite hermitian matrix, and thus $H = PP^*$ for some $P \in \mathrm{GL}_n(\mathbb{C})$. Now, for all $M \in \mathrm{M}_n(\mathbb{C})$, we get

$$(\mathrm{Int}(P^{-1}) \circ \tau')(M) = P^{-1}PP^*M^*(P^*)^{-1}P^{-1}P = (P^{-1}MP)^* = (\mathrm{Int}(P^{-1})(M))^*.$$

This means that $\mathrm{Int}(P^{-1})$ induces an isomorphism $(\mathrm{M}_n(\mathbb{C}), \mathrm{Int}(H)\circ^*) \cong_{\mathbb{C}} (\mathrm{M}_n(\mathbb{C}), ^*)$, and therefore

$$(B \otimes_k \mathbb{C}, \tau \otimes ^-) \cong_{\mathbb{C}} (\mathrm{M}_n(\mathbb{C}), \mathrm{Int}(H)\circ^*) \cong_{\mathbb{C}} (\mathrm{M}_n(\mathbb{C}), ^*).$$

Hence τ is positive definite, and this concludes the proof. □

Acknowledgements

We would like to thank the anonymous referee for his/her careful reading and his/her pertinent comments and suggestions, which helped us to improve significantely a previous version of this paper.

References

[1] G. Berhuy and F. Oggier. Space-time codes from crossed product algebras of degree 4. *Proceedings of Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci*, 4851:90–99, 2007.

[2] G. Berhuy and F. Oggier. *An introduction to central simple simple algebras and their applications to wireless communications*, volume 191 of *Mathematical Surveys and Monographs*. A.M.S., Providence, Rhode Island, 2013.

[3] G. Berhuy and R. Slessor. Optimality of codes based on crossed product algebras. 2010. Preprint. Available from http://www-fourier.ujf-grenoble.fr/~berhuy/Berhuy-Slessor-2209.pdf.

[4] B. Hochwald and W. Sweldens. Differential unitary space time modulation. *IEEE Trans. Commun.*, 48:2041–2052, December 2000.

[5] B. Hughes. Differential space-time modulation. *IEEE Trans. Inform. Theory*, 46:2567–2078, November 2000.

[6] M.A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The Book of Involutions*, volume 44 of *Amer. Math. Soc. Coll. Pub.* A.M.S, 1998.

[7] F. Oggier. Cyclic algebras for noncoherent differential space-time coding. *IEEE Transactions on Information Theory*, 53 (9):3053–3065, 2007.

[8] F. Oggier. A survey of algebraic unitary codes. *International Workshop on Coding and Cryptology*, 5757:171–187, 2009.

[9] F. Oggier, J.-C. Belfiore, and Viterbo E. *Cyclic Division Algebras: A Tool for Space-Time Coding*. Now Publishers Inc., Hanover, MA, USA, 2007.

[10] F. Oggier and L. Lequeu. Families of unitary matrices achieving full diversity. *International Symposium on Information Theory*, pages 1173–1177, 2005.

[11] S. Pumpluen and T. Unger. Space-time block codes from nonassociative division algebras. *Advances in Mathematics of Communications*, 5(3):449–471, 2011.

[12] B. A. Sethuraman. Division algebras and wireless communication. *Notices of the AMS*, 57(11):1432–1439, December 2010.

[13] B.A. Sethuraman, B. Sundar Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Trans. Information Theory*, 49, 2003.

[14] A. Shokrollahi, B. Hassibi, B.M. Hochwald, and W. Sweldens. Representation theory for high-rate multiple-antenna code design. *IEEE Trans. Information Theory*, 47(6):2335–2367, September 2001.

[15] R. Slessor. *Performance of codes based on crossed product algebras*. PhD thesis, School of Mathematics, University of Southampton, May 2011. Available from http://eprints.soton.ac.uk/197309/3.hasCoversheetVersion/Thesis_--_Richard_Slessor.pdf.