Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields*

B.A. Sethuraman[1] and Frédérique Oggier[2]

[1] Department of Mathematics
California State University, Northridge
al.sethuraman@csun.edu
[2] Department of Electrical Engineering
California Institute of Technology
frederique@systems.caltech.edu

Abstract. We describe some constructions of orthonormal lattices in totally real subfields of cyclotomic fields, obtained by endowing their ring of integers with a trace form. We also describe constructions of quaternion division algebras over such fields. Orthonormal lattices and quaternion division algebras over totally real fields find use in wireless networks in ultra wideband communication, and we describe the application.

1 Introduction

1.1 Algebraic Coding for Wireless Networks

We consider the problem of designing codes for a wireless relay network with $k+2$ nodes, each of them equipped with one antenna. Communication between the source node and the sink node is done with the help of k relay nodes. Several communication protocols have been proposed in the literature, and the one we will consider [1] belongs to the family of *amplify-and-forward* protocols, where each relay node just amplifies the signal it receives from the transmitter, before forwarding it to the receiver.

This protocol [1] is composed of k phases. During phase j, the source transmits in two steps. It sends a first signal to the jth relay and the destination. While the relay forwards the signal to the destination, the source further sends a second signal to the destination. This is repeated for each j, $j = 1, \ldots, k$.

For this protocol, the code design [16,2] consists of constructing *invertible* $2k \times 2k$ codewords, defined by

$$C = \mathrm{diag}(C_1, \ldots, C_k),$$

where C_j is a 2×2 matrix, $j = 1, \ldots, k$, containing $4k$ information symbols. The block diagonal form of C reflects the sequential nature of the protocol. Division algebras [13,10] have proved useful to design such invertible codewords.

* The first author is supported in part by NSF grant DMS-0700904.

S. Boztaş and H.F. Lu (Eds.): AAECC 2007, LNCS 4851, pp. 138–147, 2007.

Codewords are usually (in narrow band systems) built over the complex field, but for ultra wideband communication, one needs to design them over the real field. Complex code constructions based on cyclic division algebras are proposed in [16]. In [2], examples of real codes are described for the case where the number of relays is at most 5. In this paper, we provide systematic code constructions for *arbitrary* number of relays, generalizing the approach in [2].

The general code design [2] consists of the following steps:

1. Choose a totally real number field F of degree k over $\mathbb{Q}$, which is cyclic, with Galois group generated by σ, and which is such that F and $\mathbb{Q}(\sqrt{5})$ are linearly disjoint over $\mathbb{Q}$. Let $\tau : \sqrt{5} \mapsto -\sqrt{5}$ be the generator of the Galois group of $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$. Then $F(\sqrt{5})$ is Galois over $\mathbb{Q}$ with Galois group $\langle\sigma\rangle \times \langle\tau\rangle$. The Galois group of $F(\sqrt{5})/F$ is hence generated by τ.
2. Furthermore, choose F such that one can find a *trace lattice* (M, b_α) (see Subsection 1.2) inside the ring of integers of F that is isometric to the standard lattice $\mathbb{Z}^k \subseteq \mathbb{R}^k$. The orthonormal structure of M allows an efficient encoding [2] of information symbols, as detailed in Steps 4 and 5 below.
3. Now consider the cyclic algebra: $\mathcal{A} = (F(\sqrt{5})/F, \tau, \gamma)$, where γ is in F^*, and choose γ such that $\mathcal{A}$ is a division algebra. This will give us invertible codewords in Steps 4 and 5 below. Note that since $\mathcal{A}$ is a cyclic algebra of degree 2, it is also the quaternion algebra
$$\mathcal{A} = (5, \gamma). \tag{1}$$
4. Denote by C_0 a codeword from $\mathcal{A}$, that is of the form
$$C_0 = \begin{pmatrix} \sqrt{\alpha\lambda} & 0 \\ 0 & \sqrt{\alpha\tau(\lambda)} \end{pmatrix} \begin{pmatrix} a + b\nu & c + d\nu \\ \gamma(c + d\tau(\nu)) & a + b\tau(\nu) \end{pmatrix}$$
where $\nu = \frac{1+\sqrt{5}}{2}$, $\alpha \in \mathcal{D}_M^{-1}$ defines the trace form b_α and $\lambda = 2/(\sqrt{5}+5)$, chosen so that $(\sqrt{\lambda}, \sqrt{\lambda}\nu)$ and $(\sqrt{\tau(\lambda)}, \sqrt{\tau(\lambda)}\tau(\nu))$ are orthonormal in $\mathbb{R}^2$. Furthermore, if $\omega_1, \ldots, \omega_k$ is an orthonormal basis for (M, b_α), then $a = \sum_{i=1}^k \omega_i s_i$, $b = \sum_{i=1}^k \omega_i s_{k+i}$, $c = \sum_{i=1}^k \omega_i s_{2k+i}$, $d = \sum_{i=1}^k \omega_i s_{3k+i}$, where $s_1, \ldots, s_{4k}$ are information symbols from $\mathbb{Q}$.
5. We now define
$$C = \mathrm{diag}(\sigma(C_0), \ldots, \sigma^{k-1}(C_0), C_0)$$
where $\sigma(C_0)$ is obtained by applying σ to every entry of C_0. Furthermore
$$\tilde{vec}(C) = P \begin{pmatrix} \begin{pmatrix} \sqrt{\lambda} & \sqrt{\lambda}\nu \\ \sqrt{\tau(\lambda)} & \sqrt{\tau(\lambda)}\tau(\nu) \end{pmatrix} \otimes G & \mathbf{0} \\ \mathbf{0} & \begin{pmatrix} \gamma\sqrt{\lambda} & \gamma\sqrt{\lambda}\nu \\ \sqrt{\tau(\lambda)} & \sqrt{\tau(\lambda)}\tau(\nu) \end{pmatrix} \otimes G \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_{4k} \end{pmatrix}$$
where $\tilde{vec}(C)$ denotes the matrix C vectorized where the zero entries are removed, P is a permutation matrix, G is the generator matrix of M. Efficient encoding (or "shaping" [2,16]) requires the matrix that multiplies the

information symbols vector to be orthonormal, for which it is sufficient[1] that G be orthonormal.

To implement these steps above for an arbitrary number of relay nodes k, we thus need to find a totally real number field F of degree k over $\mathbb{Q}$ that is cyclic with generator σ, and that is linearly disjoint from $\mathbb{Q}(\sqrt{5})$, whose ring of integers allows the construction of an orthonormal trace lattice. Furthermore, we need to find a $\gamma \in F^*$ such that the algebra $(F(\sqrt{5})/F, \tau, \gamma)$ (which is the quaternion algebra $(5, \gamma)$) is a division algebra, where τ is the map that sends $\sqrt{5}$ to $-\sqrt{5}$.

We will discuss the cases where k is a power of 2 and a power of an odd prime separately in Sections 2 and 3, and then combine the cases in Section 4.

1.2 Trace Lattices

Let F be a totally real number field of degree k over $\mathbb{Q}$, and denote by $\mathcal{O}_F$ its ring of integers. Let $\sigma_1, \ldots, \sigma_k$ be the k embeddings of F into $\mathbb{R}$, and write $\mathrm{Tr}_{F/\mathbb{Q}}$ (or Tr_F when the context is clear) for the trace from F to $\mathbb{Q}$. We call an element $x \in F$ *totally positive* if $\sigma_i(x) \geq 0$, $i = 1, \ldots, k$. Let $M \subset \mathcal{O}_F$ be an integer lattice, that is, a subgroup of the additive group of $\mathcal{O}_F$. Being a $\mathbb{Z}$-submodule of a finitely generated and free $\mathbb{Z}$-module, M will also be finitely generated and free. We will focus on those M whose rank as a free $\mathbb{Z}$-module is exactly k (called *full lattices*). We denote by $\mathcal{D}_M^{-1}$ the codifferent of M, defined by

$$\mathcal{D}_M^{-1} = \{x \in F \mid \mathrm{Tr}_F(xM) \in \mathbb{Z}\}. \tag{2}$$

Definition 1. *A* trace lattice *is an integral lattice (M, b_α), where $M \subseteq \mathcal{O}_F$ is a (full) integer lattice, α is some totally positive element in $\mathcal{D}_M^{-1}$, and $b_\alpha : M \times M \to \mathbb{Z}$ is the bilinear form given by $b_\alpha(x, y) = Tr_F(\alpha xy)$. We refer to b_α as a trace form on M. We say that the trace lattice (M, b_α) is orthonormal if there exists a basis $\{\omega_1, \ldots, \omega_k\}$ such that $b_\alpha(\omega_i, \omega_j) = \delta_{i,j}$, in which case we say that the basis above is orthonormal.*

If $\{\omega_1, \ldots, \omega_k\}$ is a $\mathbb{Z}$-basis of M, then the trace lattice (M, b_α) can be embedded isometrically in $\mathbb{R}^k$ endowed with its standard bilinear form $\langle\ ,\ \rangle$ (the "dot product") by the map $\omega_i \mapsto f(\omega_i) = \big(\sqrt{\alpha_1}\sigma_1(\omega_i), \sqrt{\alpha_2}\sigma_2(\omega_i), \ldots, \sqrt{\alpha_k}\sigma_k(\omega_i)\big)$, where $\alpha_j = \sigma_j(\alpha)$, $j = 1, \ldots, k$ (note that α is totally positive). We may collect the $f(\omega_i)$ into a matrix known as the *generator matrix* of M, given by

$$G = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \ldots & \sqrt{\alpha_k}\sigma_k(\omega_1) \\ \vdots & \vdots & \ldots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_k) & \sqrt{\alpha_2}\sigma_2(\omega_k) & \ldots & \sqrt{\alpha_k}\sigma_k(\omega_k) \end{pmatrix}. \tag{3}$$

One easily verifies that $GG^T = \{\mathrm{Tr}_F(\alpha\, \omega_i\omega_j)\}_{i,j=1}^k$, reflecting the fact that $b_\alpha(\omega_i, \omega_j) = \langle f(\omega_i), f(\omega_j)\rangle$. The basis $\{\omega_1, \ldots, \omega_k\}$ is an orthonormal basis if and only if GG^T is the identity matrix.

[1] γ should also be such that $|\gamma|^2 = 1$, which here prevents $\mathcal{A}$ to be a division algebra. This can be overcome, we refer the reader to [2, III.A.] for this discussion.

2 Totally Real Fields of Degree a Power of 2

Consider the cyclotomic field $L = \mathbb{Q}(\omega)$, where ω is the primitive 2^n-th root of unity $e^{2\pi\imath/n}$, for a positive integer $n \geq 3$. We write θ for the element $\omega + \omega^{-1}$, so that the maximal totally real subfield of L is given by $K = \mathbb{Q}(\theta)$. Note that $[L : \mathbb{Q}] = 2^{n-1}$ and $[K : \mathbb{Q}] = 2^{n-2}$. Let $k = 2^{n-2}$. We will work with the field K in this section. We will first construct an orthonormal lattice in $\mathcal{O}_K$, and then a suitable quaternion division algebra with center K.

2.1 $\mathcal{O}_K$ as an Orthonormal Lattice

We show here that $\mathcal{O}_K$ is an orthonormal lattice with respect to a suitable trace form. We have constructed this lattice after studying the $k = 2$ case presented in [2]. The existence of this lattice was sketched independently by Eva Bayer-Fluckiger and Gabriele Nebe in [5, Prop. 4.3]. We provide expanded proofs and some combinatorial remarks.

Note that $\mathcal{O}_K = \mathbb{Z}[\theta]$ (see [9, Exer. 35, Chap. 2] for instance). We write θ_j ($j = 0, 1, \ldots,$) for the element $\omega^j + \omega^{-j}$; in particular, $\theta_1 = \theta$ and $\theta_0 = 2$. Expanding each power θ^s binomially and collecting terms we find

$$\theta^s = \begin{cases} \sum_{j=0}^{\lfloor s/2 \rfloor} \binom{s}{j} \theta_{s-2j} & \text{if } s \text{ is odd,} \\ \sum_{j=0}^{(s/2)-1} \binom{s}{j} \theta_{s-2j} + \binom{s}{s/2} & \text{if } s \text{ is even.} \end{cases} \tag{4}$$

It is easy to see that the relations (4) can inductively be inverted to write θ_s as a $\mathbb{Z}$-linear combination of θ^s. It follows that 1, $\theta_1 = \theta$, $\theta_2, \ldots, \theta_{k-1}$ is also a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

We start by proving a property of the trace of the elements of the form θ_j.

Lemma 1. *For $1 \leq j < 2k$,*

$$Tr_{K/\mathbb{Q}}(\theta_j) = 0 \tag{5}$$

and for $1 \leq i, j \leq k - 1$

$$Tr_{K/\mathbb{Q}}(\theta_i \theta_j) = \begin{cases} 0 & \text{if } i \neq j \\ 2k & \text{if } i = j \end{cases} \tag{6}$$

Proof. First consider the case where j is odd. Since ω raised to any odd power is also a primitive 2^n-th root of unity, ω^j has minimal polynomial $x^k \pm \imath$ over $\mathbb{Q}(\imath)$, and consequently, ω^j has trace zero from L to $\mathbb{Q}(\imath)$. The same reasoning holds for $\omega^{-j} = (\omega^{-1})^j$ since ω^{-1} is also a primitive 2^n-th root of unity. It follows that $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\theta_j) = 0$. Since $\mathrm{Tr}_{K/\mathbb{Q}}(\theta_j) = \mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\theta_j)$, our result is proved when j is odd. (Notice that these arguments for odd j hold even if $j > 2k$.)

When j is even, we first assume that $j < k$. (This case is vacuous if $n = 3$.) If $j = 2m$, we write $2m$ as $2^e a$ for some $e \geq 1$ and odd integer a. Then ω^j is a

primitive 2^{n-e}-root of unity, and $[L : \mathbb{Q}(\omega^j)] = 2^e$. Since, by assumption, $e < n-2$, $\mathbb{Q}(\omega^j)$ strictly contains $\mathbb{Q}(\imath)$. Now, $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\omega^j) = \mathrm{Tr}_{\mathbb{Q}(\omega^j)/\mathbb{Q}(\imath)}\mathrm{Tr}_{L/\mathbb{Q}(\omega^j)}(\omega^j) = 2^e\mathrm{Tr}_{\mathbb{Q}(\omega^j)/\mathbb{Q}(\imath)}(\omega^j)$. Just as in the previous paragraph, $\mathrm{Tr}_{\mathbb{Q}(\omega^j)/\mathbb{Q}(\imath)}(\omega^j)$ is zero since the minimal polynomial of ω^j is $x^{2^{n-e-2}} \pm \imath$. Since similar arguments hold for ω^{-j}, we find $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\theta_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\theta_j) = 0$.

Now assume $k \leq j < 2k$. Note that $\omega^k = \imath$ and $\omega^{-k} = -\imath$. Thus, when $j = k$, $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\theta_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\theta_j) = \imath - \imath = 0$. For $j > k$, $\omega^j = \imath\omega^{j-k}$, and by the considerations of the previous paragraph, $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\omega^j) = \imath\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\omega^{j-k}) = 0$. Similarly, $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\omega^{-j}) = 0$, so once again, $\mathrm{Tr}_{L/\mathbb{Q}(\imath)}(\theta_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\theta_j) = 0$.

For the second assertion, note that $\theta_i\theta_j = \theta_{i+j} + \theta_{j-i}$, where we can assume without loss of generality that $j - i \geq 0$. The result immediately follows from the calculations of $\mathrm{Tr}_{K/\mathbb{Q}}(\theta_j)$ above, noting that $i + j < 2k$, and $\theta_0 = 2$.

Corollary 1. *For all x in $\mathcal{O}_K = \mathbb{Z}[\theta]$, the expression $Tr_{K/\mathbb{Q}}(1/k - \theta/2k)x$ takes values in $\mathbb{Z}$.*

Proof. Since trace is $\mathbb{Z}$-bilinear, this assertion can be checked for x coming from the basis 1, $\theta_1 = \theta$, θ_2, $\ldots$, θ_{k-1}. For such x the assertion is immediate from Lemma 1 above.

Write α for $1/k - \theta/2k$. Any element $\sigma \in Gal(K/\mathbb{Q})$ sends θ to θ_r for some odd r, so $\sigma(\theta)/2$ is a real number strictly between 1 and -1. Hence, α is totally positive, so as in Definition 1, we have the trace form $b_\alpha \colon \mathbb{Z}[\theta] \times \mathbb{Z}[\theta] \to \mathbb{Z}$ given by $b_\alpha(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(1/k - \theta/2k)xy$.

We first calculate the value of this bilinear form on the basis elements 1, $\theta_1 = \theta$, θ_2, $\ldots$, θ_{k-1}. (Note that this is really [5, Prop. 4.3], except that the authors in [5] work with the element $1/k + \theta/2k$.)

Lemma 2. *For $1 \leq j \leq i \leq k-1$, we have the formulas:*

$$b_\alpha(1, 1) = 1 \tag{7}$$

$$b_\alpha(1, \theta_i) = \begin{cases} -1 & \text{if } i = 1 \\ 0 & \text{if } i > 1 \end{cases} \tag{8}$$

$$b_\alpha(\theta_i, \theta_j) = \begin{cases} 2 & \text{if } j = i \\ -1 & \text{if } j = i + 1 \\ 0 & \text{if } j > i + 1 \end{cases} \tag{9}$$

Proof. The first two formulas arise from a direct application of the formulas in Lemma 1. For the third, we compute: $b_\alpha(\theta_i, \theta_j) = \mathrm{Tr}_{K/\mathbb{Q}}(1/k - \theta/2k)\theta_i\theta_j = (1/k)\mathrm{Tr}_{K/\mathbb{Q}}(\theta_i\theta_j) - (1/2k)\mathrm{Tr}_{K/\mathbb{Q}}(\theta\theta_i\theta_j)$. Now the formulas in Lemma 1 show that $(1/k)\mathrm{Tr}_{K/\mathbb{Q}}(\theta_i\theta_j)$ is zero except when $i = j$, in which case it is 2. As for the term $(\theta\theta_i\theta_j)$, note that like in the proof of Lemma 1, $\theta\theta_i\theta_j = \theta_1(\theta_{i+j} + \theta_{j-i}) = \theta_{i+j+1} + \theta_{i+j-1} + \theta_{j-i+1} + \theta_{j-i-1}$. When $i = j$ and when $j > i + 1$, Lemma 1 shows that $(1/2k)\mathrm{Tr}_{K/\mathbb{Q}}(\theta\theta_i\theta_j)$ is zero. When $i = j + 1$ the term $\theta_{j-i-1} = 2$ contributes $-(1/2k)2k$ to the trace. This establishes the formula. □

The lemma above immediately leads to the following (see the remark in [5] at the end of the proof of their Prop. 4.3):

Theorem 1. *The vectors* $w_0 = 1$, $w_1 = 1 + \theta_1$, $w_2 = 1 + \theta_1 + \theta_2$, ..., $w_{k-1} = 1 + \theta_1 + \theta_2 + \cdots + \theta_{k-1}$ *form an orthonormal basis for* $\mathcal{O}_K$ *with respect to the trace form* $b_\alpha(x, y)$ *described above.*

Proof. We prove this inductively. The assertion that $b_\alpha(w_0, w_0) = 1$ is just the first formula in Lemma 2 above. Now assume that we have proved that the vectors $w_0, \ldots, w_i$ are orthonormal. First, for a given $j < k$ and $l < k$, we expand w_j as $1 + \theta_1 + \cdots + \theta_j$ and using the bilinearity of b_α, we see that $b_\alpha(w_j, \theta_l) = 0$ whenever $l > j + 1$, and $b_\alpha(w_j, \theta_l) = -1$ if $l = j + 1$. From this and the induction assumption, it follows that for $j \leq i$, $b_\alpha(w_j, w_{i+1}) = b_\alpha(w_j, w_j) + b_\alpha(w_j, \theta_{j+1}) + \cdots + b_\alpha(w_j, \theta_{i+1}) = 1 - 1 = 0$. Also, $b_\alpha(w_{i+1}, w_{i+1}) = b_\alpha(w_i, w_i) + 2b_\alpha(w_i, \theta_{i+1}) + b_\alpha(\theta_{i+1}, \theta_{i+1}) = 1 - 2 + 2 = 1$. This proves the theorem. □

To compute the generator matrix for this lattice, note that the Galois group $Gal(K/\mathbb{Q})$ is generated by the action on K of $\sigma : \omega \mapsto \omega^r$, where r is some generator of the multiplicative group $(\mathbb{Z}/2^{n-1}\mathbb{Z})^*$. Thus, $\sigma(\theta_1) = \theta_r$, $\sigma(\theta_2) = \theta_{2r}$, $\sigma(1/k - \theta_1/2k) = 1/k - \theta_r/2k$ etc.

Some combinatorial remarks: There is a nice interplay between the two $\mathbb{Z}$-bases 1, θ, θ^2, ..., θ^{k-1} (consisting of powers of θ), and the basis 1, $\theta_1 = \theta$, θ_2, ..., θ_{k-1}, which leads to some interesting combinatorial considerations. For instance, we can compute the codifferent of $\mathcal{O}_K$ in terms of the two bases, and doing so, we are led to the *Hankel transform* of the binomial sequence $\binom{2n}{n}$: these have been studied by various authors ([12], [8],[15], for example) and is defined as the sequence h_n, $n = 1, 2, \cdots$, where h_n is the determinant of the $n \times n$ matrix

$$\begin{pmatrix} \binom{0}{0} & \binom{2}{1} & \cdots & \binom{2(n-1)}{n-1} \\ \binom{2}{1} & \binom{4}{2} & \cdots & \binom{2n}{n} \\ \vdots & \vdots & \vdots & \vdots \\ \binom{2(n-1)}{n-1} & \binom{2n}{n} & \cdots & \binom{4(n-1)}{2(n-1)} \end{pmatrix}. \tag{10}$$

We will be exploring this connection in [14].

In a different direction, one can check that the vectors w_i described in Theorem 1 above can be defined in terms of the powers θ^i by the following inductive scheme: $w_0 = 1$, $w_l = \sum_{s=0}^{l-1} a_s^{(l)} w_s + \theta^l$ for $l \geq 1$, where

$$a_s^{(l)} = \begin{cases} (-1)^{s+1}\binom{2t}{t-\lfloor\frac{s+1}{2}\rfloor}, & l = 2t; \\ (-1)^s\binom{2t+1}{t-\lfloor\frac{s}{2}\rfloor}, & l = 2t+1. \end{cases} \tag{11}$$

(Indeed, this is the form in which we originally discovered our lattice. The various expressions on the right side of the definition of the $a_s^{(l)}$ above are all the binomial coefficients of the form $\binom{l}{j}$, starting from the middle and and working

towards both ends, taking one alternately on each side.) Proving the orthonormality of the w_i *directly* in this form without invoking Theorem 1 above leads to the following interesting combinatorial identities:

$$1 + \sum_{s=0}^{l} \left(a_s^{(l+1)}\right)^2 = \binom{2l+2}{l+1},$$

and, for $j > i$,

$$\sum_{s=0}^{i-1} a_s^{(i)} a_s^{(j)} - a_i^{(j)} = \begin{cases} -\binom{i+j}{(i+j+1)/2-1} & \text{if } i+j \text{ is odd,} \\ \binom{i+j}{(i+j)/2} & \text{if } i+j \text{ is even.} \end{cases} \tag{12}$$

2.2 A Quaternion Division Algebra over K

We now need to build a suitable quaternion divison algebra $\mathcal{A} = (5, \gamma)$ on K (see (1)). We will prove in this subsection the following result:

Theorem 2. *The algebra $\mathcal{A} = (5, 2-\theta)$ defined over K is a division algebra.*

Proof. We need to show that $2-\theta$ is not a norm from $K(\sqrt{5})$ to K. Observe that $2-\theta = (1-\omega)(1-\omega^{-1})$. It is a standard fact that there is a unique prime ideal $\tilde{P}$ in $\mathcal{O}_L$ that lies over 2, that it has ramification index $e = [L:\mathbb{Q}] = 2^{n-1}$ and inertial degree $f = 1$, and that it is generated by both $1-\omega$ and $1-\omega^{-1}$ (see for instance [9, Chap 3, Theo. 26]; note that ω^{-1} is also a primitive 2^n-th root of unity). It follows that there is a unique prime ideal lying over 2 in $\mathcal{O}_K$, call it P, and that $P\mathcal{O}_L = \tilde{P}^2$. But $\tilde{P}^2 = (1-\omega)\mathcal{O}_L(1-\omega^{-1})\mathcal{O}_L = (2-\theta)\mathcal{O}_L$. Since $2-\theta$ is already in $\mathcal{O}_K$, it follows that $P = \tilde{P}^2 \cap \mathcal{O}_K = (2-\theta)\mathcal{O}_K$.

Now we consider how P extends to $K(\sqrt{5})$. To do this, note that the prime 2 of $\mathbb{Z}$ stays prime in the field $\mathbb{Q}(\sqrt{5})$ (see [9, Chap. 3, Theo. 25] for instance.) Call this prime of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ P', so $e(P'|2\mathbb{Z}) = 1$ and $f(P'|2\mathbb{Z}) = 2$. Now if Q is any prime of $\mathcal{O}_{K(\sqrt{5})}$ lying over P, then $e(Q|2\mathbb{Z}) = e(Q|P)e(P|2\mathbb{Z}) \geq e(P|2\mathbb{Z}) = k$, and $f(Q|2\mathbb{Z}) = f(Q|P')f(P'|2\mathbb{Z}) \geq f(P'|2\mathbb{Z}) = 2$. Since $k \cdot 2$ already equals $[K(\sqrt{5}):\mathbb{Q}]$, we find that Q is the unique prime in $K(\sqrt{5})$ lying over 2 and that $e(Q|2\mathbb{Z}) = k$ and $f(Q|2\mathbb{Z}) = 2$. In particular, this means that Q is the unique prime of $\mathcal{O}_K$ lying over P, and that $e(Q|P) = 1$ and $f(Q|P) = 2$.

Now assume that $2-\theta = N(x)$, for some $x \in K(\sqrt{5})$, where we have written N for the norm from $K(\sqrt{5})$ to K. Further writing $x = y/z$ for y and z in $\mathcal{O}_{K(\sqrt{5})}$, we find $N(z)(2-\theta) = N(y)$. Assume that the ideal $y\mathcal{O}_{K(\sqrt{5})}$ has the factorization $Q^l \cdot Q_1^{l_1} \cdots Q_r^{l_r}$ where the Q_i are primes other than Q and l and the l_i are nonnegative integers. Assume similarly that $z\mathcal{O}_{K(\sqrt{5})}$ has the factorization $Q^{l'} \cdot (Q'_1)^{l'_1} \cdots (Q'_{r'})^{l'_{r'}}$. Then the ideal $N(y)\mathcal{O}_K$ in $\mathcal{O}_K$ has the factorization $P^{2l} \cdot P_1^{f_1 l_1} \cdots P_r^{f_r l_r}$, where the f_i are the inertial degrees of the primes Q_i, and $P_i = Q_i \cap \mathcal{O}_K$. (This follows, for instance from [9, Chap 3, Exer. 14]; note that we have used the fact that $f(Q|P) = 2$.) Similarly, $N(z)\mathcal{O}_K$ in $\mathcal{O}_K$ has the factorization $P^{2l'} \cdot (P'_1)^{f'_1 l'_1} \cdots (P'_{r'})^{f'_{r'} l'_{r'}}$. But then, since the ideal $(2-\theta)\mathcal{O}_K$ is

just P, we find that the powers of P in the associated factorization of ideals $N(y)\mathcal{O}_K = PN(z)\mathcal{O}_K$ do not match up, a contradiction. Hence, $(5, 2-\theta)$ is a division algebra over K.

3 Totally Real Fields of Odd Degree

3.1 An Orthonormal Lattice in $\mathcal{O}_K$

An example of an orthonormal lattice in totally real number fields K of degree p an odd prime was given by Erez ([7]). It was later pointed out in [6] that Erez' construction works, without any modification, for any odd degree k. We quote the construction from [6] with minor changes in notation:

- Pick a (guaranteed to exist) odd prime $p \equiv 1 \pmod{k}$.
- Set $\omega = \omega_p = e^{\frac{2\pi\imath}{p}}$ and let σ denote the generator of the cyclic Galois group $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$.
- Find a primitive element r of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$.
- For $m = \frac{p-1}{2}$, create $\alpha = \prod_{j=0}^{m-1}(1-\omega^{r^j})$.
- Find a (guaranteed to exist) λ such that $\lambda(r-1) \equiv 1 \pmod{p}$ and let $z = \omega^{\lambda}\alpha(1-\omega)$.
- For $\sigma(\omega) = \omega^r$, let $x = \sum_{j=1}^{\frac{p-1}{k}} \sigma^{jk}(z)$.

The element x is hence in the field K, the subfield of $\mathbb{Q}(\omega)$ fixed by σ^k, of degree k over $\mathbb{Q}$. Then the matrix G given below is unitary:

$$G = \frac{1}{p}\begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{k-2}(x) & \sigma^{k-1}(x) \\ \sigma(x) & \sigma^2(x) & \cdots & \sigma^{k-1}(x) & x \\ \sigma^2(x) & \sigma^3(x) & \cdots & x & \sigma(x) \\ & \vdots & & \vdots & \\ \sigma^{k-1}(x) & x & \cdots & \sigma^{k-3}(x) & \sigma^{k-2}(x) \end{pmatrix}. \tag{13}$$

Note that since k divides m as well, any element fixed by σ^k is also fixed by σ^m. Thus, K is contained in the fixed field of σ^m, which is the totally real field $\mathbb{Q}(\omega + \omega^{-1})$. K is hence totally real. Also, note that since z is integral over $\mathbb{Q}$, the element x is in $\mathcal{O}_k$. The fact that this matrix above is unitary says that the elements $x, \sigma(x), \ldots, \sigma^{k-1}(x)$ form an orthonormal basis for M with respect to the trace form $b_\gamma : M \times M \to \mathbb{Z}$ given by $b_\gamma(s,t) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma st)$, where $\gamma = 1/p^2$ (see the matrix G in the remark following Definition 1).

Remark: For the field $K = \mathbb{Q}(\omega + \omega^{-1})$, where ω is a primitive p^n-th root of unity, and p is an odd prime, it would be interesting to see if, just as for $p = 2$ in Subsection 2.1, there exists a suitable trace form for which $\mathcal{O}_K$ turns out to be an orthonormal lattice. Such a trace form is known to exist if $n = 1$ [4], but this construction does not hold for $n \geq 2$. The existence of such trace forms for general p and n is open as far as we know. For the special case of $K = \mathbb{Q}(\omega_9 + \omega_9^{-1})$, where we have written ω_9 for $e^{2\pi\imath/9}$, one can check that the vectors $-(1-\theta)\theta$, $-\theta$, $-1+\theta$ (where $\theta = \omega_9 + \omega_9^{-1}$) form an orthonormal basis

for $\mathcal{O}_K$ with respect to the trace form $b_\alpha(x,y) = Tr_K(\alpha xy)$, where α is the (totally positive) element $(16-\theta-5\theta^2)/9$.

3.2 A Quaternion Division Algebra over K

To construct a quaternion division algebra $\mathcal{A} = (5,\gamma)$ over K (as described in (1)), it is sufficient to take a quaternion division algebra over $\mathbb{Q}$ and consider it as an algebra over K: this follows from the result that if D is a division algebra of index m over a field F and if L/F is a field extension of degree n relatively prime to m, then $D \otimes_F L$ remains a division algebra ([11, Chap. 13, §4, Prop.]).

For this, note, for example, that $(5,2)$ is a division algebra over $\mathbb{Q}$. For, if 2 is the norm from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}$ of an element $x = (a+b\sqrt{5})/m$, where a, b, and m are integers, then we find $2m^2 = a^2 - 5b^2$. If m is divisible by 5, so must a, and then, so must b. Hence, we can repeatedly cancel 5^2 from both sides until m is not divisible by 5. Now reducing mod 5 and noting m is not zero mod 5, we find $2 = (a/m)^2$. But this is a contradiction as 2 is not a square mod 5. Hence, we may use $(5,2)$ as our quaternion division algebra over K.

4 Totally Real Fields of Arbitrary Degree

Finally, to construct lattices and quaternion division algebras over totally real number fields of arbitrary degree, we just have to combine the constructions in the previous two sections. Given an arbitrary positive integer $k \geq 2$, write $k = 2^m k'$, where k' is odd. We may assume that $m \geq 1$ and $k' \geq 3$, else we are in the situation of the previous sections. Write K_e for the field obtained in Section 2 of degree 2^m over $\mathbb{Q}$. Write M_e for the lattice obtained in that same section, b_{α_e} for its bilinear form, and G_e for the generator matrix that defines its isometric embedding in $\mathbb{R}^{2^m}$. Similarly, write K_o for the field obtained in Section 3 of degree k', M_o for the lattice obtained in that section, b_{α_o} for its bilinear form, and G_o for the generator matrix that defines its isometric embedding in $\mathbb{R}^{k'}$. Then, since the degrees of K_e and K_o are relatively prime, the compositum $K = K_eK_o$ has degree $k = 2^m k'$ over $\mathbb{Q}$. It is totally real since both K_e and K_o are totally real. (In fact, K is Galois over $\mathbb{Q}$ with Galois group $Gal(K_e/\mathbb{Q}) \times Gal(K_o/\mathbb{Q})$.)

If $\{c_i\}$ ($c_i \in K_e$) is an orthonormal basis for M_e, and if $\{d_j\}$ ($d_j \in K_o$) is an orthonormal basis for M_o, it is easy to see that the set $\{c_id_j\}$ is $\mathbb{Z}$-linearly independent, and hence generates a free submodule N of $\mathcal{O}_K$. We have the bilinear form $b_{\alpha_e\alpha_o}$, defined on the basis by

$$\begin{aligned} &b_{\alpha_e\alpha_o}(c_id_j, c_sd_t) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_e\alpha_o c_id_jc_sd_t) = \mathrm{Tr}_{K_e/\mathbb{Q}}(\mathrm{Tr}_{K/K_e}(\alpha_e\alpha_o c_id_jc_sd_t)) \\ &= \mathrm{Tr}_{K_e/\mathbb{Q}}(\alpha_e c_ic_s \mathrm{Tr}_{K/K_e}(\alpha_o d_jd_t)) = \mathrm{Tr}_{K_e/\mathbb{Q}}(\alpha_e c_ic_s \mathrm{Tr}_{K_o/\mathbb{Q}}(\alpha_o d_jd_t)) \\ &= \mathrm{Tr}_{K_e/\mathbb{Q}}(\alpha_e c_ic_s)\mathrm{Tr}_{K_o/\mathbb{Q}}(\alpha_o d_jd_t) = b_e(c_i,c_s)b_o(d_j,d_t). \end{aligned}$$

The basis $\{c_id_j\}$ is orthonormal: $b_{\alpha_e\alpha_o}(c_id_jc_sd_t) = \delta_{(i,j),(s,t)}$. Since $Gal(K/\mathbb{Q}) \cong Gal(K_e/\mathbb{Q}) \times Gal(K_o/\mathbb{Q})$, we may write every element $\phi \in Gal(K/\mathbb{Q})$ as a product $\sigma\tau$ of elements $\sigma \in Gal(K_e/\mathbb{Q})$ and $\tau \in Gal(K_o/\mathbb{Q})$. Hence, $\phi(\alpha_e\alpha_o) =$

$\sigma(\alpha_e)\tau(\alpha_o)$, $\phi(c_i d_j) = \sigma(c_i)\tau(d_j)$, etc. Using this, it is easy to see that the orthonormal trace lattice $(N, b_{\alpha_e \alpha_o})$ embeds isometrically into $\mathbb{R}^k$ via the Kronecker product of the matrices G_e and G_o.

To obtain a quaternion division algebra over K, we simply consider the quaternion division algebra $\mathcal{A}$ obtained over K_e in Section 2 as an algebra over K. Since K is of odd degree over K_e, $\mathcal{A} \otimes_{K_e} K$ remains a division algebra by ([11, Chap. 13, §4, Prop.]).

References

1. Azarian, K., El Gamal, H., Schniter, P.: On the Achievable Diversity-Multiplexing Tradeoff in Half-Duplex Cooperative Channels. IEEE Trans. Inform. Theory 51(12), 4152–4172 (2005)
2. Abou-Rjeily, C., Daniele, N., Belfiore, J.-C.: Distributed Algebraic Space Time Codes for Ultra Wideband Communications. Kluwer Journal, Special Issue on Cooperative Diversity (2006)
3. Bayer-Fluckiger, E.: Lattices and Number Fields. Contemporary Mathematics 241, 69–84 (1999)
4. Bayer, E., Oggier, F., Viterbo, E.: New Algebraic Constructions of Rotated $\mathbb{Z}^n$ Lattice Constellations for the Rayleigh Fading Channel. IEEE Trans. Inform. Theory 50(4), 702–714 (2004)
5. Bayer-Fluckiger, E., Nebe, G.: On the Euclidean Minimum of Some Real Number Fields. J. Théo. Nombres Bordeaux 17, 437–454 (2005)
6. Elia, P., Sethuraman, B.A., Kumar, P.V.: Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas. IEEE Trans. Inform. Theory (to appear)
7. Erez, B.: The Galois structure of the Trace Form in Extensions of Odd Prime Degree. J. of Algebra 118, 438–446 (1988)
8. Layman, J.W.: Then Hankel Transform and Some of Its Properties. J. Integer Sequences 4, Article 01.1.5 (2001)
9. Marcus, D.A.: Number Fields. Universitext. Springer, NY (1977)
10. Oggier, F.E., Rekaya, G., Belfiore, J.-C., Viterbo, E.: Perfect Space-Time Block Codes. IEEE Trans. Inform. Theory 52(9), 3885–3902 (2006)
11. Pierce, R.S: Associative Algebras. GTM88. Springer, NY (1982)
12. Radoux, C.: Calcul effectif de certains determinants de Hankel. Bull. Soc. Math. Belg. 31(1), 49–55 (1979)
13. Sethuraman, B.A., Rajan, B.S., Shashidhar, V.: Full-diversity, High-Rate Space-Time Block Codes from Division Algebras. IEEE Trans. Inform. Theory 49, 2596–2616 (2003)
14. Sethuraman, B.A., Oggier, F.E.: The Hankel Transform of the Central Binomial Coefficients and Orthonormal Lattices in Cyclotomic Fields (in preparation)
15. Spivey, M.Z., Steil, L.L.: The k-Binomial Transform and the Hankel Transform. J. Integer Sequences 9, Article 06.1.1 (2006)
16. Yang, S., Belfiore, J.-C.: Optimal Space-Time Codes For The Mimo Amplify-And-Forward Cooperative Channel. IEEE Trans. Inform. Theory 53(2), 647–663 (2007)