Optimality of codes based on crossed product algebras

Grégory Berhuy, Richard Slessor

OPTIMALITY OF CODES BASED ON CROSSED PRODUCT ALGEBRAS

GRÉGORY BERHUY, RICHARD SLESSOR

Abstract. In this paper, we explain how to construct reliable codes for wireless communication channels using crossed product division algebras, and we prove the optimality of the codes already constructed on cyclic algebras and biquadratic crossed products.

Contents

Introduction

Within the last few years we have seen a notable increase in the use of wireless communication, which has led to the need for higher data rates. In view of this multiple antenna communication systems have

been investigated, which can provide very high data rates particularly when there is perfect channel state information (CSI) at the receiver. The design criteria of such codes established in [6] led to the development of **space-time codes**[16], specifically **space-time trellis codes** (STTCs). In this paper we will be concerned with another class of space-time codes called **space-time block codes** (STBCs) [15]. A STBC $\mathcal{C}$ consists of a set of $N \times T$ ($N \geq T$) matrices with entries in $\mathbb{C}$.

In [16] the pairwise probability of error of a space-time code is derived, i.e., the probability of receiving a message and decoding it incorrectly. This bound led the authors to develop two design criteria: the **rank criterion** and the **determinant criterion**. The rank criterion states that in order to maximise the **diversity gain** we require the difference of any two distinct matrices $X, X' \in \mathcal{C}$ to be full rank. A code satisfying this property is called **fully diverse**. Once the rank criterion has been satisfied, the determinant criterion states that in order to maximise the **coding gain**, the determinant of $(X - X')\overline{(X - X')}^t$, taken over all pairs of distinct codewords in $\mathcal{C}$, must be maximised.

Finding codes that are fully diverse led to an interest in constructing codes from division algebras [13], in particular cyclic division algebras. This work generated a lot of interest and in [14] constructions of codes based on crossed product algebras were given that included the codes given in [13] as a subset. An approach based on cyclic division algebras, which differs from [13] was given in [10]. This paper introduced **perfect** codes (PSTBCs). These codes satisfy a large number of properties including a shaping constraint that is related to the cubic lattice. In the paper the authors give examples of perfect codes in dimensions $2, 3, 4$ and 6.

Codes from non-cyclic division algebras have also been investigated. In [2] the authors consider biquadratic crossed product algebras and construct a code with good performance in dimension 4.

In [3] it is shown that PSTBCs only exist in these dimensions, although by relaxing the definition slightly PSTBCs can exist for any number of antennas [4]. We will concentrate on the former case. The optimality of perfect codes has been studied and in [8] it is shown that the golden code, a PSTBC of dimension 2 presented in [1], is optimal with respect to the coding gain.

In this paper we will prove the optimality of the perfect codes of dimension 4 and 6, as well as the optimality of the biquadratic code presented in [2]. We will also generalise bounds on the minimum determinant of codes based on cyclic division algebras to the case of codes based on crossed product algebras.

This paper is organised as follows. In Section 1 some basic aspects of coding theory and the wireless channel are introduced as well as the bound on the pairwise probability of error. It then explains how division algebras can be used to give fully diverse codes and gives a description of codes based on crossed product algebras. The section also introduces the energy constraint and its link with the cubic lattice. This leads to Section 2 which introduces complex ideal lattices and gives results that will be necessary in deciding when it is possible to construct the cubic lattice. Bounds on the minimum determinant of codes based on crossed product algebras are also derived. Section 3 is then concerned with proving the optimality of the PSTBCs of dimension 4 and 6 given in [10]. Finally in Section 4 we prove that the code constructed in [2] is optimal.

1. From codes to crossed product algebras

1.1. **Modelling a communication channel.** Consider the following communication problem. A **transmitter**, which is equipped with one antenna, wishes to transmit some information to a **receiver**, also equipped with one antenna, over a wireless channel. The signal that the transmitter wants to send can be modelled by a vector

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n.$$

At time t, $t = 1, \ldots, n$ the transmit antenna sends x_t, which will reach the receive antenna via different paths, that may include several reflections (this is due to the nature of the wireless environment). Furthermore, x_t will be affected by some noise, coming from different interferences it may experience. Thus what the receiver will get is a modified signal denoted by y_t, where

$$y_t = h_t x_t + v_t, \ t = 1, \ldots, n.$$

The coefficients h_t and v_t are assumed to be complex Gaussian random variables, and they model respectively **fading** (coming from the signal propagation through multipaths) and **noise**.

The wireless channel from the transmitter to the receiver during n time slots can thus be modelled as follows:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{v},$$

where $\mathbf{y}$ is the received vector, and $\mathbf{H}$ is a diagonal $n \times n$ matrix called the **fading matrix** or **channel matrix**. The vector $\mathbf{v}$ contains the noise. Both $\mathbf{H}$ and $\mathbf{v}$ are assumed to have as coefficients complex Gaussian random variables, all of them being independent and identically distributed.

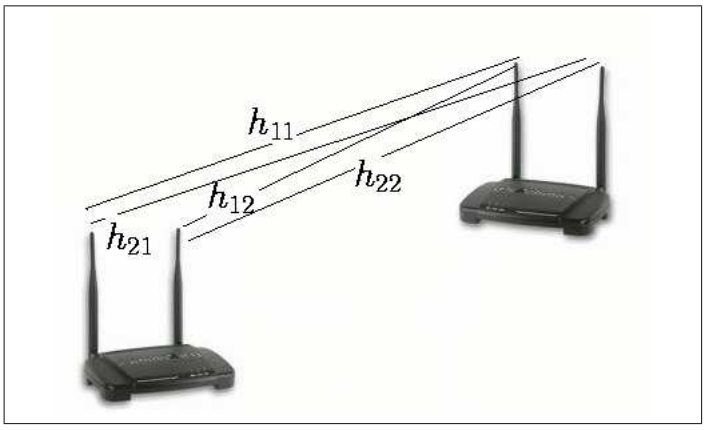

FIGURE 1. A channel with two antennas at both the transmitter and receiver.

In order to be able to transmit more and more data in the wireless environment, systems having multiple antennas at both transmitter and receiver have been introduced. They are commonly called Multiple Input Multiple Output (MIMO) systems or channels.

Let us first consider a channel with two transmit and two receive antennas (see Fig. 1). At time t, the first and second antennas respectively send x_{1t} and x_{2t}. Both these signals will be received by the two receive antennas, and will follow a different path to access each of them. The signals y_{1t}, y_{2t} sensed by each receive antenna are

$$\begin{aligned} y_{1t} &= h_{11}x_{1t} + h_{12}x_{2t} + v_{1t} \\ y_{2t} &= h_{21}x_{1t} + h_{22}x_{2t} + v_{2t} \end{aligned}$$

where h_{ij} denote the fading from the jth transmit antenna to the ith receive antenna, and v_{it} denotes the noise at the ith receive antenna at time t.

Note that in the above equations, the fading coefficients h_{ij} should depend on t. However, it is reasonable to assume that the environment does not change so fast, and that there is a period of time T during which the channel (that is h_{ij}) remains constant. This period T is called a **coherence interval**.

For example, let us assume here that the channel stays approximately constant over a period of length $T = 2$, and the transmission starts at time $t = 1$.

The first and second antennas transmit respectively x_{11} and x_{21} at time $t = 1$. At the other end, the first and second antennas receive respectively the signals y_{11} and y_{21}, each of them being the sum of the

two transmitted signals with fading and some noise, that is

$$\begin{aligned} y_{11} &= h_{11}x_{11} + h_{12}x_{21} + v_{11} \\ y_{21} &= h_{21}x_{11} + h_{22}x_{21} + v_{21}. \end{aligned}$$

Similarly, the transmit antennas send respectively x_{12} and x_{22} at time $t = 1$, and the two receive antennas get y_{12} and y_{22}. Since the channel remains constant over a period of length $T = 2$, the fading coefficients remain the same, and we have

$$\begin{aligned} y_{12} &= h_{11}x_{12} + h_{12}x_{22} + v_{12} \\ y_{22} &= h_{21}x_{12} + h_{22}x_{22} + v_{22}. \end{aligned}$$

This can be written in a matrix equation as

$$\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} + \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}.$$

This model can be generalised to the case where we have M transmit antennas and N receive antennas. At time t, the M antennas each send one signal. Those M signals can be collected and written as a vector $\mathbf{x}_t = \begin{pmatrix} x_{1t} \\ \vdots \\ x_{mt} \end{pmatrix}$. Each x_{jt} will be received by all the N antennas. Thus x_{jt} follows n different paths, each corresponding to a given fading denoted by h_{ij}, $i = 1, \ldots, n$ to reach its N destinations. Now, each receive antenna will sense a signal, which is the sum of noisy and faded copies of the signals transmitted by all antennas.

Let us now consider T instances of the transmission, where T is the coherence time interval, during which the channel is assumed to be constant. The model for transmission with multiple antennas over a coherence time T can be summarised as follows:

$$\mathbf{Y}_{N\times T} = \mathbf{H}_{N\times M}\mathbf{X}_{M\times T} + \mathbf{V}_{N\times T}, \tag{1.1}$$

where all matrices have coefficients in $\mathbb{C}$, and their dimensions are written as subscript. Each column of the matrix $\mathbf{X}$ contains the vector $\mathbf{x}_t$ sent at time t. The matrices $\mathbf{H}$ and $\mathbf{V}$ are random matrices whose coefficients are complex Gaussian random variables. They are independent and identically distributed.

It is clear from the model that the transmitted signal $\mathbf{X}$ will be modified during transmission, both attenuated by the fading, and affected by the noise. Actually, the fading a priori makes the signal even more vulnerable to noise. However, whatever data the transmitter and receiver want to share, they would like it to be communicated reliably, i.e., they want the whole message to be recovered completely from $\mathbf{Y}$ at the receiver, despite the fading and noise. It is here that **coding** comes into play. The idea behind coding is to send as signal $\mathbf{X}$ not the data

itself, but a function of the data, which typically adds redundancy. In MIMO communication, coding typically exploits the fact that fading actually provides different paths from transmitter to receiver, since a receiver with N antennas may get up to N faded copies of each transmitted signal. **Coding** thus consists of designing **codewords**, that are here the matrices $\mathbf{X}$, as a function of the data to be sent, in such a way as to protect the data encoded inside. The set of codewords is called a **codebook**. A typical communication scheme can thus be seen as follows: a set of **information symbols**, that is, the data to be sent, is the input of an **encoder**. The encoder maps the information symbols to a codeword $\mathbf{X}$, which is sent over the channel by M antennas. The receiver obtains $\mathbf{Y} = \mathbf{HX} + \mathbf{V}$. It is the role of a **decoder** to recover the information symbols from $\mathbf{Y}$.

In a multiple antenna setting, the data is encoded during **time** (we consider a time interval of T slots) and **space** (since we have M antennas). Thus, codes for multiple antenna systems are often called **space-time codes**.

In a traditional coding setting, where transmission takes place over a wire, there is no fading. Thus, a transmitted signal $\mathbf{x}$ will only be affected by noise (which we assume Gaussian). Geometrically, the transmitted signal $\mathbf{x}$ can be seen as a point in an n-dimensional space, and the received signal $\mathbf{y}$ as another point, within a ball centered at $\mathbf{x}$ of radius given by the variance of the noise. In this case, the decoder, which knows all the possible codewords, can compute $\|\mathbf{x} - \mathbf{y}\|^2$ for all possible $\mathbf{x}$ in the codebook and decide that its estimate $\hat{\mathbf{x}}$ of $\mathbf{y}$ is given by the vector which minimises $\|\mathbf{x} - \mathbf{y}\|^2$. If the codewords are designed such that there is only one codeword in a ball of radius equal to the variance of the noise, then the decoder will always get the right estimate. The situation is different in the case of fading.

Let us for now assume that the receiver has the knowledge of the channel $\mathbf{H}$. This is called the **coherent** case. The **non-coherent** case considers the scenario when the receiver does not know the channel, and will not be discussed in this paper. A decoding rule is obtained as follows. Let $\mathcal{C}$ denote the codebook. The receiver knows $\mathbf{Y} = \mathbf{HX} + \mathbf{V}$, the codebook, and an estimate of $\mathbf{H}$. It thus computes the "faded" codebook $\{\mathbf{HX} \mid \mathbf{X} \in \mathcal{C}\}$ by multiplying every codeword by $\mathbf{H}$. It then chooses as the decoded codeword the one which minimises the distance between $\mathbf{HX}$ and $\mathbf{Y}$. We thus have that the decoded codeword $\hat{\mathbf{X}}$ is given by

$$\hat{\mathbf{X}} = \min_{\mathbf{X} \in \mathcal{C}} \|\mathbf{HX} - \mathbf{Y}\|^2,$$

where the norm is the Frobenius norm:

$$\|(m_{ij})_{i,j}\|^2 = \sum_{i,j} |m_{ij}|^2.$$

An error will occur if the decoded codeword $\hat{\mathbf{X}}$ is different from the transmitted codeword $\mathbf{X}$. A way of formalising the reliability of a channel is thus to compute its **pairwise probability of error**, namely, the probability of sending $\mathbf{X}$ and decoding erroneously $\hat{\mathbf{X}} \neq \mathbf{X}$. We write such probability $\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}})$.

Let us assume from now on that $M = N = T$, and let us call this common value n. Therefore we get an equality

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{V} \in \mathrm{M}_n(\mathbb{C}) \tag{1.2}$$

In this case, one can show that we have

$$\mathbb{P}(\mathbf{X} \to \hat{\mathbf{X}}) \leq \frac{\kappa}{\delta_{min}(\mathcal{C})^n},$$

where

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

The real number $\delta_{min}(\mathcal{C})$ is called the **minimum determinant** of the code $\mathcal{C}$.

The quantity κ is a function depending on the minimum determinant and on the signal-to-noise ratio (SNR). This function is a decreasing function of the SNR which converges to zero when SNR goes to infinity, and the speed of convergence is an increasing function of the minimum determinant. In other words, a large minimum determinant will ensure that we will have a small probability error for a SNR which is not too large (meaning that we will not need too much power during transmission to cover the noise). We refer the reader to [16] for more details.

1.2. **Algebra based codes.** It follows from the results of the previous section that a code $\mathcal{C}$ will have a better performance if we design the codebook in such a way that the minimum determinant is as large as possible. Of course, the first step is to ensure that $\delta_{min}(\mathcal{C}) > 0$. The main difficulty comes from the non-linearity of the determinant. The idea is then to choose $\mathcal{C}$ to be a (large) finite subset of a subring D of $\mathrm{M}_n(\mathbb{C})$, which is also a division ring. In this case, the difference of two distinct codewords will lie in $D^\times \subset \mathrm{GL}_n(\mathbb{C})$. But how to find explicitly such a division ring?

This is where (central) simple K-algebras come into play. Assume that A is a simple finite dimensional K-algebra, and let L/K be a field extension such that L is a K-subalgebra of A (in particular L/K has finite degree). The product law induces on A the structure of a finite dimensional right L-vector space of dimension r. In particular, if we denote by $M_a \in \mathrm{M}_r(L)$ the matrix of left multiplication by $a \in A$

in a fixed basis of the right L-vector space A, we get a K-algebra homomorphism

$$\varphi\colon \begin{array}{c} A \longrightarrow \mathrm{M}_r(L) \subset \mathrm{M}_r(\mathbb{C}) \\ a \longmapsto M_a \end{array},$$

which is injective since A is simple.

In particular, if A is a division K-algebra, $\varphi(A)$ is a subring of $\mathrm{M}_r(\mathbb{C})$ which has the required properties, and we may take our codebook $\mathcal{C}$ to be a finite subset of $\mathcal{C}_{A,L} = \{M_a \mid a \in A\} \subset \mathrm{M}_r(\mathbb{C})$.

The previous way of encoding will introduce enough redundancy to prevent the loss of too much information during transmission. However we cannot introduce too much redundancy either, since sending an information symbol has an energy cost. One goal is of course to encode as much information as possible in a single matrix without losing too much information after transmission. The **rate** of a code $\mathcal{C} \subset \mathrm{M}_r(\mathbb{C})$ is the ratio of information symbols per coefficients sent. Of course, it is in our best interest to design codes with high rates.

Let us compute the rate $r(\mathcal{C})$ of a code $\mathcal{C} \subset \mathcal{C}_{A,L}$. The information symbols that we would like to transmit are elements of K, which may be used to define elements of A. Each element of a may then carry $\dim_K(A)$ information symbols. However, an $r \times r$ matrix may contain r^2 information symbols, so we have

$$r(\mathcal{C}) = \frac{\dim_K(A)}{r^2},$$

where $r = \dim_L(A)$. Now since $\dim_K(A) = \dim_L(A)[L : K] = r[L : K]$, this rewrites as

$$r(\mathcal{C}) = \frac{[L : K]^2}{\dim_K(A)},$$

so we should choose L/K such that $[L : K]$ is as large as possible. If A is a **central** simple K-algebra, it is known that $[L : K] \leq \deg(A)$. In particular, if A is a central division K-algebra, we may choose for L a maximal commutative subfield of A to obtain a code with a rate equal to 1, which is the maximal possible value in this case.

Now let us have a closer look at $\delta_{min}(\mathcal{C})$. One major problem is that $\mathcal{C}$ may have in practical applications a large number of elements. Thus, it could turn out that $\delta_{min}(\mathcal{C})$ is very close to 0 if $\mathcal{C}$ is not chosen carefully, simply because $\mathcal{C}_{A,L}$ contains matrices of arbitrary small determinant. Therefore the idea is to force the values of the determinant to be discrete, for example by choosing elements $a \in A$ in an order Λ of A.

The next results will provide a way to achieve this. We first introduce some notation. Let K be a number field, and let A be a central simple K-algebra of degree n having a maximal commutative subfield L/K.

Finally, let $e_1, \ldots, e_n$ be an L-basis of A. For any ideal I of the ring of integers $\mathcal{O}_L$ of L, we set

$$\Lambda_{A,I} = e_1 I \oplus \cdots \oplus e_n I \text{ and } \mathcal{C}_{A,I} = \{M_a \mid a \in \Lambda_{A,I}\}.$$

Notice that $\Lambda_{A,I}$ and $\mathcal{C}_{A,I}$ are additive groups, and therefore we have

$$\delta_{min}(\mathcal{C}_{A,I}) = \inf\{|\det(M_a)|^2 \mid a \in \Lambda_{A,I}, a \neq 0\}.$$

Moreover, if $\mathcal{C} \subset \mathcal{C}_{A,I}$, the difference of two distinct codewords is a non-zero element of $\mathcal{C}_{A,I}$, so we get

$$\delta_{min}(\mathcal{C}) \geq \delta_{min}(\mathcal{C}_{A,I}).$$

Remark 1.3. Keeping the previous notation, we have an L-algebra isomorphism

$$f\colon \begin{array}{c} A \otimes_k L \xrightarrow{\sim} \mathrm{End}_L(A) \\ a \otimes \lambda \longmapsto (z \mapsto az\lambda), \end{array}$$

where A is considered as a right L-vector space. Therefore, we have

$$\mathrm{Nrd}_A(a) = \det(f(a \otimes 1)) = \det(M_a),$$

by definition of the reduced norm. In particular, $\det(M_a) \in K$ for all $a \in A$.

We then have the following result:

Proposition 1.4. *Let K be a number field which is closed under complex conjugation. Let $K_0 = K \cap \mathbb{R}$. Keeping the notation above, there exists a natural integer $c > 0$ such that we have*

$$|\det(M_a)|^2 \in \frac{1}{c}\mathcal{O}_{K_0} \text{ for all } a \in \Lambda_{A,I}.$$

Proof. Since every element $x \in L$ may be written as $x = \dfrac{y}{s}$ for some $y \in \mathcal{O}_L$ and $s \in \mathbb{Z}$, the set

$$\{m \in \mathbb{Z} \mid mM_{e_i} \in \mathrm{M}_n(\mathcal{O}_L) \text{ for } i = 1, \ldots, n\}$$

is a non-zero ideal of $\mathbb{Z}$, hence generated by a unique positive integer $r \geq 1$. We deduce that, for every $a = e_1 a_1 + \ldots + e_n a_n \in \Lambda_{A,I}$, we have

$$rM_a = rM_{e_1} a_1 + \ldots + rM_{e_n} a_n \in \mathrm{M}_n(\mathcal{O}_L).$$

Since $\det(M_a) \in K$ by Remark 1.3, we have $\det(rM_a) = r^n \det(M_a) \in \mathcal{O}_L \cap K = \mathcal{O}_K$, and we obtain that

$$\det(M_a) \in \frac{1}{r^n}\mathcal{O}_K.$$

Hence for all $a \in \Lambda_{A,I}$, there exists $x \in \mathcal{O}_K$ such that

$$\det(M_a) = \frac{x}{r^n}.$$

By assumption, complex conjugation induces an automorphism of K. Therefore, $|x|^2 = x\overline{x} \in \mathcal{O}_K$. Hence $|x|^2 \in \mathcal{O}_K \cap \mathbb{R} = \mathcal{O}_{K_0}$. Thus

$$|\det(M_a)|^2 = \frac{|x|^2}{r^{2n}} \in \frac{1}{r^{2n}}\mathcal{O}_{K_0} \text{ for all } a \in A.$$

Setting $c = r^{2n}$ then yields the conclusion. □

Corollary 1.5. *Let $\mathcal{C}$ be a finite subset of $\mathcal{C}_{A,I}$, where A is a central division K-algebra. If $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-d}), d > 0$, then there exists a natural integer $c > 0$ such that*

$$\delta_{min}(\mathcal{C}) \geq \frac{1}{c}.$$

Proof. The previous proposition shows that we have

$$c|\det(M_a)|^2 \in \mathcal{O}_{K_0} \text{ for all } a \in \Lambda_{A,I},$$

for some natural integer $c > 0$. The assumption on the ground field implies that $\mathcal{O}_{K_0} = \mathbb{Z}$. Assume now that $a \neq 0$. Since A is division, $\det(M_a) \neq 0$ and therefore $c|\det(M_a)|^2$ is a positive integer. Hence

$$|\det(M_a)|^2 \geq \frac{1}{c} \text{ for all } a \in \Lambda_{a,L}, a \neq 0.$$

Thus we get

$$\delta_{min}(\mathcal{C}) \geq \delta_{min}(\mathcal{C}_{A,I}) \geq \frac{1}{c},$$

and this concludes the proof. □

The conclusion of the previous corollary is not true anymore if we drop the assumption on K. For example, if $K = K_0 = \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_{K_0}$ contains elements of arbitrary small absolute value. However in practice, a signal is represented by an element of $\mathbb{Q}(i)$ or $\mathbb{Q}(j)$, where $j = e^{2i\pi/3}$ (see [5] for more details). We will assume therefore in the sequel that $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$, which both satisfy the assumptions of the previous corollary. Notice that in this case, $\mathcal{O}_K$ is a principal ideal domain, and any ideal I of $\mathcal{O}_L$ has an $\mathcal{O}_K$-basis $\omega_1, \ldots, \omega_n$.

Now that we have found a way to ensure that $\delta_{min}(\mathcal{C})$ is not too close to 0, we examine another constraint related to encoding, called **shaping**.

An element $X \in \mathcal{C}$ represents some information which is already encoded. In fact, if we write

$$X = M_a, a = e_1a_1 + \ldots + e_na_n, a_i \in I$$

the real information which is transmitted is represented by the elements $a_{ij} \in \mathcal{O}_K$ defined by

$$a_i = \sum_{j=1}^{n} a_{ij}\omega_j, i = 1, \ldots, n.$$

Sending the n^2 information symbols a_{ij} has an energy cost, which is represented by the real number

$$\sum_{i,j} |a_{ij}|^2.$$

Now sending $X = (x_{ij}) \in \mathrm{M}_n(L)$ will have an energy cost equal to

$$\sum_{i,j} |x_{ij}|^2.$$

Energy constraint: Encoding the information symbols a_{ij} into the matrix $X = M_a$ needs to preserve the energy cost.

We refer the reader willing to know more about shaping constraints to [9].

Notice that, once an L-basis of A and an $\mathcal{O}_K$-basis are fixed, if $\mathbf{x}$ and $\mathbf{a}$ are the two vectors whose coordinates are the x_{ij}'s and the a_{ij}'s respectively, one may write

$$\mathbf{x} = M\mathbf{a},$$

for some $M \in \mathrm{M}_{n^2}(L)$ which does not depend on a. The energy constraint then states

$$\overline{M}^t M = \mathrm{I}_{n^2}.$$

Of course, in order to deal with this constraint, we first need examples of central simple K-algebras for which we can find an explicit maximal commutative subfield, and an explicit L-basis. A good family of such examples is given by the family of crossed product K-algebras.

1.3. **Codes based on crossed product K-algebras.** Let L/K be a Galois field extension of degree n, with Galois group G. If $\sigma \in G$ and $\lambda \in L$, we set

$$\lambda^\sigma = \sigma^{-1}(\lambda).$$

Let $\xi : G \times G \to L^\times$ be a map satisfying the cocyclicity conditions, namely

$$\xi_{\mathrm{Id},\tau} = \xi_{\sigma,\mathrm{Id}} = 1, \xi_{\sigma,\tau\rho}\xi_{\tau,\rho} = \xi_{\sigma\tau,\rho}\xi^\rho_{\sigma,\tau} \text{ for all } \sigma,\tau,\rho \in G.$$

The crossed product K-algebra $(\xi, L/K, G)$ is the K-algebra generated as a right L-vector space by elements $(e_\sigma)_{\sigma\in G}$ subject to the relations

$$e_\sigma e_\tau = e_{\sigma\tau}\xi_{\sigma,\tau}, \lambda e_\sigma = e_\sigma \lambda^\sigma \text{ for all } \sigma,\tau \in G, \lambda \in L.$$

One can show that $(\xi, L/K, G)$ is a central simple K-algebra of degree n, with maximal commutative subfield L.

In particular, we get an injective K-algebra homomorphism

$$\varphi\colon \begin{array}{c} A \longrightarrow \mathrm{M}_n(L) \\ a \longmapsto M_a \end{array}$$

associated to this particular K-algebra. In order to derive explicitly the energy constraint associated to this K-algebra, we first need to compute the multiplication matrix of an element $a \in A$.

Lemma 1.6. *Let $A = (\xi, L/K, G)$, and let $a = \sum_{\sigma\in G} e_\sigma a_\sigma$. Then the matrix M_a of left multiplication by a, relative to the L-basis $(e_\sigma)_{\sigma\in G}$ is*

$$M_a = (\xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau}.$$

Proof. For all $\tau \in G$, we have

$$\begin{aligned} ae_\tau &= \sum_{\sigma\in G} e_\sigma a_\sigma e_\tau \\ &= \sum_{\sigma\in G} e_\sigma e_\tau a^\tau_\sigma \\ &= \sum_{\sigma\in G} e_{\sigma\tau}\xi_{\sigma,\tau} a^\tau_\sigma \\ &= \sum_{\sigma\in G} e_\sigma \xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}} \end{aligned}$$

This concludes the proof. □

We now derive the energy constraint we are looking for. Since any ideal of $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $n = |G|$, we will index any $\mathcal{O}_K$-basis of I with the elements of G.

Let $A = (\xi, L/K, G)$ and let I be an ideal of $\mathcal{O}_L$. If we choose an $\mathcal{O}_K$-basis $(\omega_\sigma)_{\sigma\in G}$ of I, we will (temporarily) encode n^2 information symbols $(a_{\sigma,\tau})_{\sigma,\tau\in G}$ into the matrix $M_a \in \mathcal{C}_{A,I}$, where

$$a = \sum_{\sigma\in G} e_\sigma (\sum_{\tau\in G} a_{\sigma,\tau}\omega_\tau).$$

Proposition 1.7. *With this way of encoding, the energy constraint is satisfied if and only if the two following conditions are fulfilled:*

(1) $|\xi_{\sigma,\tau}|^2 = 1$ *for all* $\sigma, \tau \in G$

(2) *The matrix $W = (\omega^\sigma_\tau)_{\sigma,\tau}$ is unitary.*

Proof. For $\sigma \in G$, set $a_\sigma = \sum_{\tau\in G} a_{\sigma,\tau}\omega_\tau$. We would like to have

$$\sum_{\sigma,\tau\in G} |a_{\sigma,\tau}|^2 = \sum_{\sigma,\tau\in G} |\xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}}|^2 = \sum_{\sigma,\tau\in G} |\xi_{\sigma,\tau} a^\tau_\sigma|^2$$

for all $a_{\sigma,\tau} \in \mathcal{O}_K$. For $\sigma \in G$, we consider the two column vectors of L^n

$$X_\sigma = (\xi_{\sigma,\rho} a_\sigma^\rho)_{\rho\in G}, A_\sigma = (a_{\sigma,\rho})_{\rho\in G}.$$

Let D_σ be the diagonal matrix of $\mathrm{M}_n(L)$ whose non-zero entry at column ρ is $\xi_{\sigma,\rho}$. Since $a_{\sigma,\tau} \in K$, we have

$$\xi_{\sigma,\tau} a_\sigma^\tau = \sum_{\rho\in G} \xi_{\sigma,\tau} a_{\sigma,\rho}^\tau \omega_\rho^\tau = \sum_{\rho\in G} \xi_{\sigma,\tau} a_{\sigma,\rho} \omega_\rho^\tau.$$

Now if $W = (\omega_\rho^\tau)_{\tau,\rho}$, then $D_\sigma W = (\xi_{\sigma,\tau}\omega_\rho^\tau)_{\tau,\rho}$, and therefore we get

$$X_\sigma = D_\sigma W A_\sigma \text{ for all } \sigma \in G.$$

Let $\mathbf{x}$ and $\mathbf{a}$ be the block column vectors defined by

$$\mathbf{x} = \begin{pmatrix} \vdots \\ X_\sigma \\ \vdots \end{pmatrix}, \mathbf{a} = \begin{pmatrix} \vdots \\ A_\sigma \\ \vdots \end{pmatrix},$$

and let $M \in \mathrm{M}_{n^2}(L)$ be the block diagonal matrix

$$M = \begin{pmatrix} \ddots & & \\ & D_\sigma W & \\ & & \ddots \end{pmatrix}.$$

Then we have $\mathbf{x} = M\mathbf{a}$. Since $\mathbf{x}$ contains all the entries of M_a and $\mathbf{a}$ contains all the information symbols, fulfilling the energy constraint is equivalent to ask for M to be unitary. It is equivalent to say that $D_\sigma W$ is unitary for all $\sigma \in G$. Since $D_{\mathrm{Id}} = I_n$, it is equivalent to ask for W to be unitary and for D_σ to be unitary for all $\sigma \in G$. In view of the definition of D_σ, this is equivalent to conditions (1) and (2). □

Finding an $\mathcal{O}_K$-basis of I satisfying condition (2) is not easy. In order to simplify the problem, we will make the extra assumption that complex conjugation induces a $\mathbb{Q}$-automorphism on L, which commutes with every element of $\mathrm{Gal}(L/K)$.

In this case, it is easy to check that $\overline{W}^t W = (\mathrm{Tr}_{L/K}(\overline{\omega}_\sigma \omega_\tau))_{\sigma,\tau}$. Hence, we may find an $\mathcal{O}_K$-basis of I for which encoding is energy-preserving if and only if the hermitian $\mathcal{O}_K$-lattice

$$\begin{aligned} I \times I &\longrightarrow \mathcal{O}_K \\ (x, y) &\longmapsto \mathrm{Tr}_{L/K}(\overline{x}y) \end{aligned}$$

is isomorphic to the cubic lattice $\mathcal{O}_K^n$ (see next section for the definition of a hermitian $\mathcal{O}_K$-lattice).

This has very few chances to happen, so we now modify the encoding process as follows. Let $\lambda \in L^\times$ satisfying the following conditions:

(a) $\overline{\lambda} = \lambda$.

(b) λ^σ is a positive real number for all $\sigma \in G$.

(c) $\mathrm{Tr}_{L/K}(\lambda \overline{x} y) \in \mathcal{O}_K$ for all $x, y \in I$.

Notice that in this case, $N_{L/K}(\lambda)$ and $\mathrm{Tr}_{L/K}(\lambda)$ are positive real numbers.

Let $D_\lambda \in \mathrm{M}_n(\mathbb{R})$ be the diagonal matrix whose diagonal entries are the real numbers $\sqrt{\lambda^\sigma}, \sigma \in G$. If $(\omega_\sigma)_{\sigma \in G}$ is an $\mathcal{O}_K$-basis of I, we will encode n^2 information symbols $(a_{\sigma,\tau})_{\sigma,\tau \in G}$ into the matrix

$$M_a D_\lambda = (\sqrt{\lambda^\tau} \xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau},$$

where $a_\sigma = \sum_{\tau \in G} a_{\sigma,\tau} \omega_\tau$ for all $\sigma \in G$.

The reader will check that this new way of encoding simply replaces W by $W_\lambda = D_\lambda W$ in the proof of the previous proposition. Now $\overline{W}^t_\lambda W_\lambda = (\mathrm{Tr}_{L/K}(\lambda \overline{\omega}_\sigma \omega_\tau))_{\sigma,\tau}$.

Hence we may find an $\mathcal{O}_K$-basis of I for which encoding is energy-preserving if and only if the hermitian $\mathcal{O}_K$-lattice

$$\begin{aligned} I \times I &\longrightarrow \mathcal{O}_K \\ (x, y) &\longmapsto \mathrm{Tr}_{L/K}(\lambda \overline{x} y) \end{aligned}$$

is isomorphic to the cubic lattice $\mathcal{O}_K^n$.

We then set

$$\mathcal{C}_{A,\lambda,I} = \{M_a D_\lambda \mid a \in \Lambda_{A,I}\}.$$

Clearly, we have $\delta_{min}(\mathcal{C}_{A,\lambda,I}) = N_{L/K}(\lambda) \delta_{min}(\mathcal{C}_{A,I})$, and therefore is bounded by a positive constant in view of Corollary 1.5 if A is a division K-algebra.

At this point, we would like to summarise what we have done so far.

Let $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$. Let L/K be a Galois extension with Galois group G satisfying the following conditions:

(1) Complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with every element of G.

(2) There exists $\lambda \in L^\times$ and I an ideal of $\mathcal{O}_L$ satisfying the following conditions:

(a) $\overline{\lambda} = \lambda$, that is $\lambda \in \mathbb{R}$

(b) λ^σ is a positive real number for all $\sigma \in G$

(c) $\mathrm{Tr}_{L/K}(\lambda \overline{x} y) \in \mathcal{O}_K$ for all $x, y \in I$

(d) The hermitian $\mathcal{O}_K$-lattice

$$h_\lambda : \begin{array}{l} I \times I \longrightarrow \mathcal{O}_K \\ (x,y) \longmapsto \mathrm{Tr}_{L/K}(\lambda \overline{x} y) \end{array}$$

is isomorphic to the cubic lattice $\mathcal{O}_K^n$.

Then for any orthonormal $\mathcal{O}_K$-basis $(\omega_\sigma)_{\sigma\in G}$ of (I, h_λ), and for any crossed product division K-algebra $A = (\xi, L/K, G)$ such that

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

the encoding map

$$\begin{array}{c} \mathcal{O}_K^n \longrightarrow \mathcal{C}_{A,\lambda,I} \\ (a_{\sigma,\tau})_{\sigma,\tau\in G} \longmapsto (\sqrt{\lambda^\tau}\xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau}, \end{array}$$

where $a_\sigma = \sum_{\tau\in G} a_{\sigma,\tau}\omega_\tau$ for all $\sigma \in G$, is energy-preserving. Moreover, $\delta_{min}(\mathcal{C}_{A,\lambda,I})$ is bounded by a positive constant.

Notice that the conditions above also imply that other coding constraints are fulfilled. We will not go into details and let the reader refer to [9].

The next steps are to give necessary conditions for the lattice h_λ to be isomorphic to the cubic lattice, and to compute (or at least estimate) $\delta_{min}(\mathcal{C}_{A,\lambda,I})$ in terms of the data, in order to choose A and I such that $\delta_{min}(\mathcal{C}_{A,\lambda,I})$ is as large as possible.

2. Ideal lattices

2.1. **Generalities on hermitian lattices.** In this section, we recall some basic definitions on hermitian lattices and introduce some invariants that we will need later on.

Definition 2.1. Let $K/\mathbb{Q}$ be a totally imaginary quadratic field extension with non-trivial automorphism $K \to K$, $u \mapsto \bar{u}$ (which is nothing but complex conjugation). A **hermitian $\mathcal{O}_K$-lattice** is a pair (M, h), where M is a free $\mathcal{O}_K$-module and $h : M \times M \to \mathcal{O}_K$ is a hermitian form with respect to $^-$.

We say that two hermitian $\mathcal{O}_K$-lattices (M, h) and (M', h') are **isomorphic** if there is an isomorphism of $\mathcal{O}_K$-modules $f : M \xrightarrow{\sim} M'$ such that

$$h'(f(x), f(y)) = h(x, y) \text{ for all } x, y \in M.$$

A hermitian lattice (M, h) is **positive definite** if $h(x, x) > 0$ for all $x \in M, x \neq 0$. This property only depends on the isomorphism class of (M, h).

Example 2.2. Let $n \geq 1$ be an integer. The **cubic lattice** of rank n is the hermitian $\mathcal{O}_K$-lattice on $\mathcal{O}_K^n$ given by

$$h_0 : \begin{array}{c} \mathcal{O}_K^n \times \mathcal{O}_K^n \longrightarrow \mathcal{O}_K \\ (x, y) \longmapsto \overline{x}^t y. \end{array}$$

Therefore, a hermitian $\mathcal{O}_K$-lattice (M, h) is isomorphic to the cubic lattice if and only if M has an orthonormal basis with respect to the hermitian form h. In this case, it is positive definite.

Lemma 2.3. *Let (M, h) be a hermitian $\mathcal{O}_K$-lattice. Let $\mathbf{e}$ be an $\mathcal{O}_K$-basis of M. Then $\mathrm{Mat}(h, \mathbf{e}) \in \mathbb{Z}$ and does not depend on the choice of $\mathbf{e}$.*

Proof. The matrix $H = \mathrm{Mat}(h, \mathbf{e})$ is a hermitian matrix, i.e., $H = \bar{H}^t$, which implies

$$\det(H) = \det(\overline{H}) = \overline{\det(H)}.$$

Therefore the determinant of H also lies in $\mathbb{R}$. Hence $\det(H) \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$, since $K/\mathbb{Q}$ is a totally imaginary quadratic field extension.

Let $\mathbf{e}'$ be another basis of M, and let P denote the corresponding base change matrix. If $H' = \mathrm{Mat}(h, \mathbf{e}')$, then we have $H' = \overline{P}^t H P$, and therefore

$$\det(H') = N_{K/\mathbb{Q}}(\det(P)) \det(H).$$

Since $P \in \mathrm{GL}_n(\mathcal{O}_K)$, $\det(P)$ is a unit of $\mathcal{O}_K$, and thus $N_{K/\mathbb{Q}}(\det(P)) = 1$, since $K/\mathbb{Q}$ is a totally imaginary quadratic field extension. This completes the proof. □

Definition 2.4. The **determinant** of the lattice (M, h), denoted by $\det(M, h)$, is the determinant of any representative matrix of h. It only depends on the isomorphism class of (M, h).

Example 2.5. Assume that (M, h) is isomorphic to the cubic lattice. Then $\det(M, h) = 1$, since there exists an orthonormal $\mathcal{O}_K$-basis, that is a basis for which the corresponding representative matrix is the identity matrix.

Remark 2.6. If (M, h) is positive definite, then $\det(M, h)$ is positive.

We now introduce the signature of a hermitian $\mathcal{O}_K$-lattice (M, h). Extending scalars to K gives rise to a hermitian form on $V = M \otimes_{\mathcal{O}_K} K$ over K, that we will still denote by h. Considering V as a $\mathbb{Q}$-vector space, we then get a quadratic form

$$q_h : \begin{array}{c} V \longrightarrow \mathbb{Q} \\ v \longmapsto h(v, v). \end{array}$$

It is well-known that the hermitian form $h : V \times V \to K$ may be diagonalised, i.e.,

$$h \simeq \langle a_1, \ldots, a_n \rangle, a_i \in \mathbb{Q}^\times$$

and that in this case, we have

$$q_h \simeq \langle 1, d\rangle \otimes \langle a_1, \ldots, a_n\rangle,$$

where $K = \mathbb{Q}(\sqrt{-d}), d > 0$.

Thus, the following definition makes sense:

Definition 2.7. [12] The **signature** of a hermitian $\mathcal{O}_K$-lattice (M, h) is defined as

$$\mathrm{sign}(M, h) = \frac{1}{2}\mathrm{sign}(q_h) \in \mathbb{Z}.$$

Notice that we also have

$$\mathrm{sign}(M, h) = \sharp\{i \mid a_i > 0\} - \sharp\{i \mid a_i < 0\},$$

for any diagonalisation

$$h \simeq \langle a_1, \ldots, a_n\rangle, a_i \in \mathbb{Q}^\times.$$

It only depends on the isomorphism class of (M, h).

Remark 2.8. It follows from the definition of the signature that (M, h) is positive definite if and only if $\mathrm{sign}(M, h) = \mathrm{rk}(M)$.

If (M, h) is a hermitian $\mathcal{O}_K$-lattice, we have $h(x, x) \in \mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$ for all $x \in M$. Thus, we may define the minimal distance of a hermitian $\mathcal{O}_K$-lattice (M, h) as follows:

Definition 2.9. Let (M, h) be a hermitian $\mathcal{O}_K$-lattice. The **minimal distance** of (M, h) is the non-negative integer $d(M, h)$ defined by

$$d(M, h) = \min_{x\in M, x\neq 0} |h(x, x)|.$$

Once again, two isomorphic hermitian $\mathcal{O}_K$-lattices will have the same minimal distance.

Example 2.10. If (M, h) is isomorphic to the cubic lattice, then $d(M, h) = 1$.

2.2. **Complex ideal lattices.** We now study the hermitian lattices introduced at the end of the first section. We first recall the definition of the codifferent ideal of a finite extension of number fields.

Definition 2.11. The **codifferent ideal** of an extension L/K of number fields is the fractional ideal

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \subset \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L\}.$$

Lemma 2.12. *Let L/K be a finite extension of number fields. Assume that L is closed under complex conjugation, and let $L_0 = L \cap \mathbb{R}$. Then for any ideal I of $\mathcal{O}_L$ and any $\lambda \in L_0^\times$, we have*

$$\mathrm{Tr}_{L/K}(\lambda \overline{x} y) \in \mathcal{O}_K \text{ for all } x, y \in I \iff \lambda \overline{I} I \subset \mathcal{D}_{L/K}^{-1}.$$

Proof. Assume that $\lambda\bar{I}I \subset \mathcal{D}_{L/K}^{-1}$. Then for all $x, y \in I$ we have $\lambda\overline{x}y \in \mathcal{D}_{L/K}^{-1}$ by assumption and therefore

$$\mathrm{Tr}_{L/K}(\lambda\bar{x}y) = \mathrm{Tr}_{L/K}(\lambda\bar{x}y \cdot 1_K) \subset \mathcal{O}_K \text{ for all } x, y \in I.$$

Conversely, assume that $\mathrm{Tr}_{L/K}(\lambda\overline{x}y) \in \mathcal{O}_K$ for all $x, y \in I$. Since $\lambda\bar{I}I$ is generated as an additive group by elements of the form $\lambda\overline{x}_1x_2, x_i \in I$, it is enough to check that $\mathrm{Tr}_{L/K}(\lambda\overline{x}_1x_2y) \in \mathcal{O}_K$ for all $x_1, x_2 \in I, y \in \mathcal{O}_L$, which is clear from the assumption. This concludes the proof. □

We now assume for the rest of this paper that $\mathcal{O}_K$ is a principal ideal domain, and that L/K is a finite field extension of degree n, which is closed under complex conjugation. We will denote by L_0 the maximal real subfield of L, that is $L_0 = L \cap \mathbb{R}$. In this case, L_0 and K are linearly disjoint over $\mathbb{Q}$, and any K-embedding of L into $\mathbb{C}$ is the canonical extension of a $\mathbb{Q}$-embedding of L_0 into $\mathbb{C}$. In particular, for every $\lambda \in L_0$, we have

$$N_{L/K}(\lambda) = N_{L_0/\mathbb{Q}}(\lambda) \in \mathbb{Q}.$$

Notice also that, since $\mathcal{O}_K$ is a principal ideal domain, any ideal I of $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank n. In particular, the following definition makes sense.

Definition 2.13. Let L/K be an extension of number fields where L is closed under complex conjugation. A **complex ideal lattice on** L/K is a pair (I, h_λ), where I is an ideal of $\mathcal{O}_L$ with $\lambda \in L_0^\times$ satisfying $\lambda\bar{I}I \subset \mathcal{D}_{L/K}^{-1}$ and h_λ is the hermitian $\mathcal{O}_K$-lattice

$$h_\lambda \colon \begin{array}{l} I \times I \longrightarrow \mathcal{O}_K \\ (x, y) \longmapsto \mathrm{Tr}_{L/K}(\lambda\overline{x}y). \end{array}$$

The rest of this paragraph is devoted to the computation of the invariants introduced above for a given complex ideal lattice. We start with a definition.

Definition 2.14. The **relative discriminant** of L/K, denoted by $d_{L/K}$, is the determinant of $(\mathcal{O}_L, h_0)$. In other words,

$$d_{L/K} = \det(\mathrm{Tr}_{L/K}(\overline{w}_i w_j)) \in \mathbb{Z}$$

for any $\mathcal{O}_K$-basis $w_1, \ldots, w_n$ of $\mathcal{O}_L$.

We will assume until the end of the paper that complex conjugation commutes with all the K-embeddings of L into $\mathbb{C}$.

We are now ready to state our first result.

Proposition 2.15. *Let (I, h_λ) be an ideal lattice on L/K. Then*

$$\det(I, h_\lambda) = N_{L/K}(\lambda) N_{L/\mathbb{Q}}(I) d_{L/K}.$$

Proof. Since $\mathcal{O}_K$ is a principal ideal domain, there exists an $\mathcal{O}_K$-basis $\mathbf{w} = (w_1, \ldots, w_n)$ of $\mathcal{O}_L$ and elements $q_1, \ldots, q_n \in O_K$ such that $\mathbf{w}' = (q_1 w_1, \ldots, q_n w_n)$ is an $\mathcal{O}_K$-basis of I. Let $\sigma_1, \ldots, \sigma_n$ be the n K-embeddings of L into $\mathbb{C}$. Since complex conjugation commutes with $\sigma_1, \ldots, \sigma_n$, we have

$$\mathrm{Mat}(h_\lambda, \mathbf{w}') = \overline{W'}^t \mathcal{L} W',$$

where

$$W' = (q_j w_j^{\sigma_i})_{i,j} \text{ and } \mathcal{L} = \begin{pmatrix} \lambda^{\sigma_1} & & \\ & \ddots & \\ & & \lambda^{\sigma_n} \end{pmatrix}.$$

Clearly, $\det(\mathcal{L}) = N_{L/K}(\lambda)$ and $\det(W') = q_1 \ldots q_n \det(W)$, where $W = (w_j^{\sigma_i})_{i,j}$. Therefore, we get

$$\det(I, h_\lambda) = N_{L/K}(\lambda)\overline{q_1 \cdots q_n} \cdot q_1 \cdots q_n \det(\overline{W}^t) \det(W).$$

If $I = \mathcal{O}_L$ and $\lambda = 1$, we get $d_{L/K} = \det(\overline{W}^t) \det(W)$, and therefore

$$\det(I, h_\lambda) = N_{L/K}(\lambda)\overline{q_1 \cdots q_n} \cdot q_1 \cdots q_n d_{L/K}.$$

Therefore, it remains to show that $N_{L/\mathbb{Q}}(I) = \overline{q_1 \cdots q_n} \cdot q_1 \cdots q_n$. Recall that $N_{L/\mathbb{Q}}(I)$ is by definition the number of elements of $\mathcal{O}_L/I$. Notice now that we have an isomorphism of $\mathcal{O}_K$-modules

$$\mathcal{O}_L/I \simeq \mathcal{O}_K/q_1\mathcal{O}_K \times \cdots \times \mathcal{O}_K/q_n\mathcal{O}_K.$$

Thus, it remains to show that for a given $q \in \mathcal{O}_K, q \neq 0$, the group $\mathcal{O}_K/q\mathcal{O}_K$ has $\overline{q}q$ elements. But the number of elements of $\mathcal{O}_K/q\mathcal{O}_K$ is by definition $N_{K/\mathbb{Q}}(q\mathcal{O}_K)$, which is nothing but $\overline{q}q$. This completes the proof. □

Remark 2.16. The proof above also shows that $d_{L/K} > 0$.

Indeed, this follows from the equalities

$$d_{L/K} = \det(\overline{W}^t) \det(W) = \overline{\det(W)} \det(W) > 0.$$

We now relate $d_{L/K}$ to the norm of the codifferent ideal. We first recall a few definitions from number theory.

Definition 2.17. Let L/K be a finite extension of number fields. The **different ideal** $\mathcal{D}_{L/K}$ of L/K is the inverse of the fractional ideal $\mathcal{D}_{L/K}^{-1}$. This is an ideal of $\mathcal{O}_L$. The **discriminant ideal** of L/K is the ideal of $\mathcal{O}_K$ defined by

$$\mathfrak{d}_{L/K} = \mathcal{N}_{L/K}(\mathcal{D}_{L/K}).$$

Lemma 2.18. *We have* $d_{L/K} = \sqrt{N_{L/\mathbb{Q}}(\mathcal{D}_{L/K})} = \sqrt{N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})}$.

Proof. It is well-known that $\mathfrak{d}_{L/K}$ is the ideal generated by the elements $\det(\mathrm{Tr}_{L/K}(x_i x_j))$, where $x_1, \dots, x_n$ run through the K-bases of L consisting of elements of $\mathcal{O}_L$. Since $\mathcal{O}_K$ is a principal ideal domain, $\mathfrak{d}_{L/K}$ is actually generated by $\det(\mathrm{Tr}_{L/K}(w_i w_j))$, where $w_1, \dots, w_n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. We then have

$$N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) = N_{K/\mathbb{Q}}(\det(\mathrm{Tr}_{L/K}(w_i w_j))).$$

Now if $W = (w_j^{\sigma_i})$, we have $\det(\mathrm{Tr}_{L/K}(w_i w_j)) = \det(W^t W) = \det(W)^2$, and therefore

$$N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) = N_{K/\mathbb{Q}}(\det(W))^2 = (\overline{\det(W)}\det(W))^2 = d_{L/K}^2.$$

Since $d_{L/K} > 0$ by Remark 2.16, we are done. □

Corollary 2.19. *Let $K \subset M \subset L$ be a tower of field extensions. Then we have*

$$(d_{L/K})^2 = N_{M/\mathbb{Q}}(\mathfrak{d}_{L/M}) \cdot (d_{M/K})^{2\cdot[L:M]}$$

In particular, $d_{M/K}^{[L:M]} \mid d_{L/K}$.

Proof. By the previous lemma, we have $(d_{L/K})^2 = N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$. Moreover, we have $\mathfrak{d}_{L/K} = \mathcal{N}_{M/K}(\mathfrak{d}_{L/M}) \cdot \mathfrak{d}_{M/K}^{[L:M]}$. Putting this into our equation we get

$$(d_{L/K})^2 = N_{M/\mathbb{Q}}(\mathfrak{d}_{L/M}) \cdot N_{K/\mathbb{Q}}(\mathfrak{d}_{M/K})^{[L:M]} = N_{M/\mathbb{Q}}(\mathfrak{d}_{L/M}) \cdot d_{M/K}^{2[L:M]}.$$

This completes the proof. □

Corollary 2.20. *Let (I, h_λ) be a complex ideal lattice on L/K. Then $\det(I, h_\lambda) = \pm 1$ if and only if $\lambda \overline{I} I = \mathcal{D}_{L/K}^{-1}$.*

Proof. Since we have $\lambda \overline{I} I \subset \mathcal{D}_{L/K}^{-1}$ by definition of a complex ideal lattice on L/K, we will have $\lambda \overline{I} I = \mathcal{D}_{L/K}^{-1}$ if and only if $N_{L/\mathbb{Q}}(\lambda \overline{I} I) = N_{L/\mathbb{Q}}(\mathcal{D}_{L/K}^{-1})$, that is

$$N_{L/\mathbb{Q}}(\lambda \overline{I} I) N_{L/\mathbb{Q}}(\mathcal{D}_{L/K}) = 1.$$

Since complex conjugation is an automorphism of $L/\mathbb{Q}$, we have

$$N_{L/\mathbb{Q}}(\overline{I}) = N_{L/\mathbb{Q}}(I).$$

Moreover, we have

$$N_{L/\mathbb{Q}}(\lambda) = N_{K/\mathbb{Q}}(N_{L/K}(\lambda)) = N_{L/K}(\lambda)^2,$$

since $N_{L/K}(\lambda) \in \mathbb{Q}$. Using Lemma 2.18, the condition above rewrites as

$$(N_{L/K}(\lambda) N_{L/\mathbb{Q}}(I) d_{L/K})^2 = 1,$$

that is $\det(I, h_\lambda)^2 = 1$ by Proposition 2.15. This completes the proof. □

Remark 2.21. In particular, if (I, h_λ) is positive definite, we have $\det(I, h_\lambda) = 1$ if and only if $\lambda \overline{I} I = \mathcal{D}_{L/K}^{-1}$, since $\det(I, h_\lambda) > 0$ in this case.

We now compute the signature of a complex ideal lattice.

Proposition 2.22. *Let (I, h_λ) be a complex ideal lattice on L/K, and let $X(L) = \mathrm{Hom}_K(L, \mathbb{C})$. Then we have*

$$\mathrm{sign}(I, h_\lambda) = \sharp\{\sigma \in X(L) \mid \sigma(\lambda) > 0\} - \sharp\{\sigma \in X(L) \mid \sigma(\lambda) < 0\}.$$

In particular, (I, h_λ) is positive definite if and only if $\sigma(\lambda) > 0$ for every K-embedding $\sigma : L \to \mathbb{C}$.

Proof. We define two quadratic forms q_{λ,L_0} and $q'_{\lambda,L}$ by

$$q_{\lambda,L_0}: \begin{array}{l} L_0 \longrightarrow \mathbb{Q} \\ x \longmapsto \mathrm{Tr}_{L_0/\mathbb{Q}}(\lambda x^2) \end{array}$$

and

$$q'_{\lambda,L}: \begin{array}{l} L \longrightarrow \mathbb{Q} \\ x \longmapsto \mathrm{Tr}_{L/\mathbb{Q}}(\lambda \overline{x} x). \end{array}$$

Since $\lambda \overline{x} x \in L_0$ for all $x \in L$, we have

$$\mathrm{Tr}_{L/K}(\lambda \overline{x} x) = \mathrm{Tr}_{L_0/\mathbb{Q}}(\lambda \overline{x} x) \in \mathbb{Q}$$

and therefore

$$q_{h_\lambda}(x) = \mathrm{Tr}_{L/K}(\lambda \overline{x} x) = \frac{1}{2}\mathrm{Tr}_{L/\mathbb{Q}}(\lambda \overline{x} x) = \frac{1}{2} q'_{\lambda,L}(x)$$

for all $x \in L$. Hence, we have

$$\mathrm{sign}(I, h_\lambda) = \frac{1}{2}\mathrm{sign}(q'_{\lambda,L}).$$

Easy computations show that

$$q'_{\lambda,L} \simeq \langle 1, d \rangle \otimes q_{\lambda,L_0},$$

where $K = \mathbb{Q}(\sqrt{-d})$ and therefore

$$\mathrm{sign}(I, h_\lambda) = \mathrm{sign}(q_{\lambda,L_0}).$$

Set $X'(L_0) = \mathrm{Hom}_{\mathbb{Q}}(L_0, \mathbb{C})$. By [12, Proof of Theorem 3.4.5], we get

$$\mathrm{sign}(I, h_\lambda) = \sharp\{\tau \in X'(L_0) \mid \tau(\lambda) > 0\} - \sharp\{\tau \in X'(L_0) \mid \tau(\lambda) < 0\}.$$

Taking into account that every K-embedding of L into $\mathbb{C}$ is extended from a $\mathbb{Q}$-embedding of L_0 into $\mathbb{C}$, we have the desired result. □

We now give an estimation of the minimal distance of a complex ideal lattice.

Proposition 2.23. *Let (I, h_λ) be a positive definite complex ideal lattice. Then we have*

$$d(I, h_\lambda) \geq n[N_{L/K}(\lambda)N_{L/\mathbb{Q}}(I)]^{1/n}.$$

In particular, if $\det(I, h_\lambda) = 1$*, we have*

$$d(I, h_\lambda) \geq n \cdot d_{L/K}^{-1/n}.$$

Proof. By Proposition 2.22, $\sigma(\lambda)$ is a positive real number for every embedding $\sigma : L \to \mathbb{C}$. Since σ commutes with complex conjugation, $\sigma(\lambda\overline{x}x) = \sigma(\lambda)\overline{\sigma(x)}\sigma(x)$ is a positive real number for all $x \in L$. In particular, the inequality of the arithmetic and geometric means implies that

$$\frac{1}{n}\mathrm{Tr}_{L/K}(\lambda\overline{x}x) \geq N_{L/K}(\lambda\overline{x}x)^{1/n} \text{ for all } x \in I.$$

Now for all $x \in I$, we have $\lambda\overline{x}x\mathcal{O}_L \subset \lambda\overline{I}I$, and therefore

$$N_{L/\mathbb{Q}}(\lambda)N_{L/\mathbb{Q}}(I)^2 \mid N_{L/\mathbb{Q}}(\lambda\overline{x}x\mathcal{O}_L) = N_{L/\mathbb{Q}}(\lambda\overline{x}x).$$

In particular, if $x \neq 0$, we get

$$N_{L/\mathbb{Q}}(\lambda\overline{x}x) \geq N_{L/\mathbb{Q}}(\lambda)N_{L/\mathbb{Q}}(I)^2.$$

Now since $\lambda\overline{x}x \in L_0$, we have $N_{L/K}(\lambda\overline{x}x) \in \mathbb{Q}$ and thus $N_{L/\mathbb{Q}}(\lambda\overline{x}x) = N_{L/K}(\lambda\overline{x}x)^2$. For the same reason, $N_{L/\mathbb{Q}}(\lambda) = N_{L/K}(\lambda)^2$, and we get

$$N_{L/K}(\lambda\overline{x}x) \geq N_{L/K}(\lambda)N_{L/\mathbb{Q}}(I),$$

taking into account that $N_{L/K}(\lambda)$ and $N_{L/K}(\lambda\overline{x}x)$ are positive. We finally get

$$\mathrm{Tr}_{L/K}(\lambda\overline{x}x) \geq n[N_{L/K}(\lambda)N_{L/\mathbb{Q}}(I)]^{1/n} \text{ for all } x \in I, x \neq 0,$$

which proves the first part of the proposition. The second part follows from Proposition 2.15. □

Since the cubic lattice has a minimal distance equal to 1, we get:

Corollary 2.24. *If the cubic lattice is isomorphic to a complex ideal lattice on L/K, then $d_{L/K} \geq n^n$.*

2.3. **Minimum determinant of a crossed product based code.** We would now like to apply the results of the previous paragraph to give an estimation of the minimum determinant of a crossed product based code. Let us recall some notation from the first section.

Let $A = (\xi, L/K, G)$ be a crossed product K-algebra of degree n, such that $|\xi_{\sigma,\tau}|^2 = 1$ for all $\sigma, \tau \in G$, and let (I, h_λ) be an ideal lattice on L/K which is isomorphic to the cubic lattice, with orthonormal basis $(w_\sigma)_{\sigma\in G}$.

Let $\Lambda_{A,I} = \bigoplus_{\sigma\in G} e_\sigma I$, and let D_λ be the diagonal matrix whose entries are the real numbers $\sqrt{\lambda^\sigma}, \sigma \in G$. For all $a = \sum_{\sigma\in G} e_\sigma a_\sigma \in \Lambda_{A,I}$, we denote by M_a the matrix of left multiplication by a in the L-basis $(e_\sigma)_{\sigma\in G}$ of A and we set $\mathbf{X}_a = M_a D_\lambda$. In other words, we have

$$M_a = (\xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau} \text{ and } \mathbf{X}_a = (\sqrt{\lambda^\tau}\xi_{\sigma\tau^{-1},\tau} a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau}.$$

We finally set

$$\mathcal{C}_{A,\lambda,I} = \{\mathbf{X}_a \mid a \in \Lambda_{A,I}\}.$$

By the results of Section 1, the encoding map

$$a = \sum_{\sigma\in G} e_\sigma (\sum_{\tau\in G} a_{\sigma,\tau}\omega_\tau) \mapsto \mathbf{X}_a$$

is energy-preserving.

We would like to evaluate the performance of our code. In order to do this, we have to estimate $\delta_{min}(\mathcal{C}_{A,\lambda,I}) = \inf_{a\neq 0} |\det(\mathbf{X}_a)|^2$. Let us introduce some notation first. The set

$$\mathcal{E}^{(\tau)}_\xi = \{c \in \mathcal{O}_K \mid c\xi_{\sigma\tau^{-1},\tau} \in \mathcal{O}_L \text{ for all } \sigma \in G\}$$

is an ideal of $\mathcal{O}_K$. We will denote by $\Delta^{(\tau)}_\xi$ the norm of this ideal. Equivalently, we have

$$\Delta^{(\tau)}_\xi = N_{K/\mathbb{Q}}(c^{(\tau)}_\xi) = |c^{(\tau)}_\xi|^2,$$

for any generator $c^{(\tau)}_\xi$ of $\mathcal{E}^{(\tau)}_\xi$. Notice that by the definition of a cocycle, we have $\Delta^{(\mathrm{Id})}_\xi = 1$.

By definition, we have

$$\Delta^{(\tau)}_\xi = 1 \iff \xi_{\sigma\tau^{-1},\tau} \in \mathcal{O}_L \text{ for all } \sigma \in G.$$

We then set

$$\Delta_\xi = \prod_{\sigma\in G} \Delta^{(\sigma)}_\xi.$$

We then have

$$\Delta_\xi = 1 \iff \xi_{\sigma,\tau} \in \mathcal{O}_L \text{ for all } \sigma,\tau \in G.$$

Finally, we set

$$N_{min}(I) = \min_{x\in I\setminus\{0\}} |N_{L/\mathbb{Q}}(x)|.$$

Notice that $N_{min}(I) = N_{L/\mathbb{Q}}(I)$ if I is a principal ideal. In general, equality does not hold.

Proposition 2.25. *Assume that A is a division K-algebra. With the previous notation, we have*

$$\frac{1}{\Delta_\xi d_{L/K}} \leq \delta_{min}(\mathcal{C}_{A,\lambda,I}) \leq N_{L/K}(\lambda)N_{min}(I).$$

If moreover $\Delta_\xi = 1$ and I is principal, we have

$$\delta_{min}(\mathcal{C}_{A,\lambda,I}) = \frac{1}{d_{L/K}}.$$

Proof. Let $x \in I, x \neq 0$ with minimal absolute norm. Then we have

$$\mathbf{X}_{e_{\mathrm{Id}}x} = M_{e_{\mathrm{Id}}x}D_\lambda = xM_{e_{\mathrm{Id}}}D_\lambda = xD_\lambda.$$

It follows that

$$\det(\mathbf{X}_{e_{\mathrm{Id}}x}) = \prod_{\tau\in G} x^\tau\sqrt{\lambda^\tau} = N_{L/K}(x)\sqrt{N_{L/K}(\lambda)},$$

and therefore $|\det(\mathbf{X}_{e_{\mathrm{Id}}x})|^2 = N_{L/\mathbb{Q}}(x)N_{L/K}(\lambda) = N_{min}(I)N_{L/K}(\lambda)$, since we have

$$|N_{L/K}(x)|^2 = N_{K/\mathbb{Q}}(N_{L/K}(x)) = N_{L/\mathbb{Q}}(x).$$

The upper bound then follows from the definition of $\delta_{min}(\mathcal{C}_{A,\lambda,I})$.

Now let $\mathbf{X}_a = M_aD_\lambda \in \mathcal{C}_{A,\lambda,I}$. To establish the lower bound, notice that

$$|\det(\mathbf{X}_a)|^2 = |\det(M_a)|^2 N_{L/K}(\lambda).$$

Recall that we have $\det(M_a) = \mathrm{Nrd}_A(a) \in K$. Now let $c_\xi^{(\tau)}$ be a generator of $\mathcal{E}_\xi^{(\tau)}$, let C be the invertible diagonal matrix whose diagonal entry at column τ is $c_\xi^{(\tau)}$, and let $M'_a = M_aC$. By definition of $c_\xi^{(\tau)}$, we have $M'_a = (c_\xi^{(\tau)}\xi_{\sigma\tau^{-1},\tau}a^\tau_{\sigma\tau^{-1}})_{\sigma,\tau} \in \mathrm{M}_n(\mathcal{O}_L)$. Thus $\det(M'_a) \in \mathcal{O}_L \cap K = \mathcal{O}_K$ and $|\det(M'_a)|^2 \in \mathbb{Z}$.

Since each coefficient in the τ^{th}-column of M'_a lies in I^τ, the definition of the determinant and the previous observation show that we have $\det(M'_a) \in (\prod_{\tau\in G} I^\tau) \cap \mathcal{O}_K = \mathcal{N}_{L/K}(I)$. It follows that

$$|\det(M'_a)|^2 \in \overline{\mathcal{N}_{L/K}(I)}\mathcal{N}_{L/K}(I) \cap \mathbb{Z} = \mathcal{N}_{L/\mathbb{Q}}(I) = N_{L/\mathbb{Q}}(I)\mathbb{Z}.$$

Now we have

$$|\det(\mathbf{X}_a)|^2 = |\det(M'_aC^{-1}D_\lambda)|^2 = \frac{1}{\Delta_\xi}N_{L/K}(\lambda)|\det(M'_a)|^2,$$

and thus

$$|\det(\mathbf{X}_a)|^2 \in \frac{1}{\Delta_\xi}N_{L/K}(\lambda)N_{L/\mathbb{Q}}(I)\mathbb{Z}.$$

Since $\det(\mathbf{X}_a) \neq 0$ if $a \neq 0$, we get

$$|\det(\mathbf{X}_a)|^2 \geq \frac{1}{\Delta_\xi} N_{L/K}(\lambda) N_{L/\mathbb{Q}}(I) \text{ for all } a \in \Lambda_{A,I}, a \neq 0.$$

Using Proposition 2.15 and the definition of the minimum determinant, we get the desired lower bound.

Finally, if I is a principal ideal, then $N_{min}(I) = N_{L/\mathbb{Q}}(I)$. Using Proposition 2.15 again, we see that the two bounds are equal whenever $\Delta_\xi = 1$ and I is principal. □

Remark 2.26. Notice that if $x \in I, x \neq 0$ is an element with minimal norm, then the first isomorphism theorem applied to the surjective morphism $\mathcal{O}_L/x\mathcal{O}_L \to \mathcal{O}_L/I$ shows that $N_{min}(I) = N_{L/\mathbb{Q}}(I)[I : x\mathcal{O}_L]$. Hence the equation in the previous proposition may be rewritten as

$$\frac{1}{\Delta_\xi d_{L/K}} \leq \delta_{min}(\mathcal{C}_{A,\lambda,I}) \leq \frac{[I : x\mathcal{O}_L]}{d_{L/K}}.$$

This shows that maximising $\delta_{min}(\mathcal{C}_{A,\lambda,I})$ is essentially equivalent to minimising $d_{L/K}$. The lower bound also shows that it is in our interest to choose the cocycle values to be algebraic integers whenever it is possible.

3. Optimality of codes based on cyclic K-algebras

In [10] examples of codes with good performance were given for $n = 4$ and $n = 6$ that are based on a specific type of crossed product K-algebra, namely cyclic K-algebras. In this section, we will establish the optimality of these codes.

3.1. **Preliminaries.** First, let us recall the definition of a cyclic K-algebra. Let L/K be a cyclic Galois extension of degree n with Galois group G generated by σ, and let $\gamma \in K^\times$.

The map

$$\xi^\gamma : \begin{array}{c} G \times G \longrightarrow L^\times \\ (\sigma^i, \sigma^j) \longmapsto \begin{cases} 1 & \text{if } i+j < n \\ \gamma & \text{if } i+j \geq n \end{cases} \end{array}$$

is a 2-cocycle.

We denote by $(\gamma, L/K, \sigma)$ the corresponding crossed product. Such a K-algebra is called a **cyclic K-algebra**. This K-algebra is generated by a single element $e(= e_\sigma)$ subject to the relations

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

Codes based on cyclic division K-algebras that satisfy the conditions discussed at the beginning of this paper are called **Perfect Space**

Time Block Codes (PSTBC). It has been shown that if $\gamma \in \mathcal{O}_K$, then these codes only exist in dimension $2, 3, 4$ and 6 [3]. If the condition that $\gamma \in \mathcal{O}_K$ is dropped then perfect codes exist for any dimension [4]. The case of the optimal PSTBC in dimension 2 has been addressed in [8]. In this section we deal with the dimension 4 and 6 cases.

In order to study the optimality of these codes, we will need to study the ramification of some Kummer extensions of K.

Let $L = K(\sqrt[n]{d})$ be a Kummer extension of $K \supset \mu_n$ of degree n. After multiplying by a suitable n^{th}-power of an element of K, we may assume that $d \in \mathcal{O}_K$ and that $0 \leq v_\pi(d) \leq n-1$ for every prime element π of $\mathcal{O}_K$.

The following result is well-known.

Lemma 3.1. *The prime elements π of K which eventually ramify are those dividing d or n. Every prime $\pi \mid d$ ramifies and if $v_\pi(d)$ and n are relatively prime, then π totally ramifies.*

If furthermore $\pi \nmid n$, then π totally ramifies if and only if $v_\pi(d)$ and n are relatively prime.

We continue these preliminaries by giving a necessary and sufficient condition on d to have complex conjugation commuting with the Galois group of L/K.

Lemma 3.2. *Let $L = K(\sqrt[n]{d})$ be a Kummer extension of K of degree n. Then complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with $\mathrm{Gal}(L/K)$ if and only if $\overline{d}d \in K^{\times n}$.*

Proof. Let $\zeta_n \in K$ be a primitive n^{th}-root of 1. Then a generator σ of $\mathrm{Gal}(L/K)$ is given by

$$\sigma\colon \begin{array}{ccc} L & \longrightarrow & L \\ \alpha & \longmapsto & \zeta_n \alpha, \end{array}$$

where $\alpha = \sqrt[n]{d}$. Assume first that complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with $\mathrm{Gal}(L/K)$. Then $\overline{\alpha} \in L$, and we have

$$\sigma(\overline{\alpha}\alpha) = \overline{\sigma(\alpha)}\sigma(\alpha) = \overline{\alpha}\alpha,$$

since $\overline{\zeta}_n \zeta_n = 1$. Thus $\overline{\alpha}\alpha \in K^\times$. Now we have

$$(\overline{\alpha}\alpha)^n = \overline{\alpha^n}\alpha^n = \overline{d}d,$$

so $\overline{d}d \in K^{\times n}$. Conversely, assume that $\overline{d}d \in K^{\times n}$. Then we have

$$(\overline{\alpha}\alpha)^n = \overline{d}d = c^n \text{ for some } c \in K^\times,$$

and therefore $\overline{\alpha} = \dfrac{c\zeta'}{\alpha}$ for some $\zeta' \in \mu_n$. In particular, $\overline{\alpha} \in L$ and complex conjugation is therefore a $\mathbb{Q}$-automorphism of L. Moreover, we have

$$\sigma(\overline{\alpha}) = \frac{c\zeta'}{\zeta_n \alpha} = \overline{\zeta}_n \frac{c\zeta'}{\alpha} = \overline{\zeta_n \alpha},$$

that is $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$. Hence complex conjugation commutes with σ and hence with $\mathrm{Gal}(L/K)$. This completes the proof. □

We finish this section by computing Δ_{ξ^γ}.

Assume that $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$. Write $\gamma = \dfrac{\gamma_1}{\gamma_2}$, where $\gamma_1, \gamma_2 \in \mathcal{O}_K$ are relatively prime. For all $1 \leq j \leq n-1$, we have

$$\xi^\gamma_{\sigma^{j-1}(\sigma^j)^{-1},\sigma^j} = \xi^\gamma_{\sigma^{n-1},\sigma^j} = \gamma.$$

This implies easily that $\mathcal{E}^{(\sigma^j)}_{\xi^\gamma} = (\gamma_2)$. We then have $\Delta^{\sigma^j}_{\xi^\gamma} = |\gamma_2|^2$, and therefore

$$\Delta_{\xi^\gamma} = |\gamma_2|^{2(n-1)}.$$

Thus, if $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a codebook built on a cyclic division K-algebra $A = (\gamma, L/K, \sigma)$, then by Proposition 2.25 and the considerations of the previous paragraph, we have

$$\frac{1}{\delta_{min}(\mathcal{C})} \leq |\gamma_2|^{2(n-1)} d_{L/K}.$$

3.2. **The case $n = 4$.** In [10], Oggier et al. constructed a suitable code on the cyclic division $\mathbb{Q}(i)$-algebra

$$(i, \mathbb{Q}(i)(\zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i), \sigma).$$

The cyclic extension $\mathbb{Q}(i)(\zeta_{15}+\zeta_{15}^{-1})/\mathbb{Q}(i)$ has relative discriminant 1125 as we will see later on. Hence for any $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$, we get

$$\frac{1}{\delta_{min}(\mathcal{C})} \leq 1125.$$

We will show here that this bound is optimal, in the following sense:

Theorem 3.3. *If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a PSTBC built on a cyclic division K-algebra $A = (\gamma, L/K, \sigma)$ of degree 4, then we have*

$$|\gamma_2|^6 d_{L/K} \geq 1125.$$

We will need several intermediate results. Assume that we may build a PSTBC on a cyclic division K-algebra $A = (\gamma, L/K, \sigma)$, where $K = \mathbb{Q}(i)$ or $\mathbb{Q}(j)$, such that $|\gamma_2|^6 d_{L/K} < 1125$. We would like to notice first that the case $K = \mathbb{Q}(i)$ and $\gamma = i$ is the only one worth considering.

Assume that $|\gamma_2|^6 d_{L/K} < 1125$. Since we need the existence of an ideal trace lattice on L isomorphic to the cubic lattice structure, we have

$d_{L/K} \geq 4^4$ by Corollary 2.24. Taking into account that $|\gamma|^2$ is a positive integer, we get easily from the previous inequality that$|\gamma_2|^2 = 1$. Since $K/\mathbb{Q}$ is quadratic imaginary, this implies that γ_2 is a unit, so $\gamma \in \mathcal{O}_K$. Now $|\gamma|^2 = 1$, and thus γ is also a unit of $\mathcal{O}_K$.

Now if $K = \mathbb{Q}(j)$, then by the previous point $\gamma = \pm 1, \pm j, \pm j^2$, so $\gamma^6 = 1$. In particular, we have

$$6[A] = [(\gamma^6, L/K, \sigma)] = [(1, L/K, \sigma)] = 0 \in \mathrm{Br}(K).$$

Since A has degree 4, we also have $4[A] = 0$ and so $2[A] = 0$. Hence A has exponent 1 or 2, and since K is a number field, it implies that A has index 1 or 2. Thus, A is not a division K-algebra.

Assume now that $K = \mathbb{Q}(i)$. In this case, $\gamma = \pm 1, \pm i$. Since the index of A equals its exponent, A will be a division K-algebra if and only if $2[A] \neq 0$. Now if $L = K(\sqrt[4]{d})$, we have $2[A] = [(\gamma, d)]$. Since -1 is a square in K, we have $(\gamma, d) \simeq (-\gamma, d)$, and $(\gamma, L/K, \sigma)$ is then a division K-algebra if and only if $(-\gamma, L/K, \sigma)$ is. Hence, it is enough to consider the two cases $\gamma = 1, i$. The first case has to be discarded since it yields the split K-algebra $\mathrm{M}_4(K)$.

Therefore, we may assume without loss of generality that $K = \mathbb{Q}(i)$ and $A = (i, L/K, \sigma)$. In this case, we are reduced to show that there is no PSTBC on a cyclic division K-algebra $(i, L/K, \sigma)$ satisfying $d_{L/K} < 1125$.

We now assume once and for all that $K = \mathbb{Q}(i)$ and that $L = K(\sqrt[4]{d})$, where $d \in \mathcal{O}_K$ is not divisible by any 4^{th}-power of an element of $\mathcal{O}_K$.

We denote by $S_3, S_1, \overline{S}_1$ the following subsets of $\mathcal{O}_K$:

$$S_3 = \{p \equiv 3[4], p \text{ prime number } \}$$

$$S_1 = \{\pi = a + bi \mid 0 < a < b, p_\pi = a^2 + b^2, p_\pi \text{ prime number } \}$$

$$\overline{S}_1 = \{\overline{\pi} \mid \pi \in S_1\}.$$

Then any prime element of $\mathcal{O}_K$ is associate either to $1 - i$ or to exactly one element of S_3, S_1 or $\overline{S}_1$.

Decomposing d into a product of a unit and of prime elements and using Lemma 3.2 then immediately gives the following result:

Lemma 3.4. *Let $L = K(\sqrt[4]{d})$. Then complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with $\mathrm{Gal}(L/K)$ if and only if all the following conditions are satisfied:*

(1) $v_{1-i}(d) = 0$.
(2) $v_p(d) = 0$ *or* 2, *for all* $p \in S_3$.
(3) $(v_\pi(d), v_{\overline{\pi}}(d)) = (1,3), (2,2)$ *or* $(3,1)$ *for all* $\pi \in S_1$ *dividing* d.

We will assume from now on that the conditions above are satisfied. In this case, we have the following estimation of the relative discriminant.

Lemma 3.5. *The odd part of* $d_{L/K}$ *is*

$$(\prod_{\substack{p \in S_3 \\ p|d}} p)^2 (\prod_{\substack{\pi \in S_1 \\ v_\pi(d) = 1,3}} p_\pi)^3 (\prod_{\substack{\pi \in S_1 \\ v_\pi(d) = 2}} p_\pi)^2.$$

Proof. Let $p \in S_3$ dividing d. By Lemma 3.4, $v_p(d) = 2$, so p ramifies but does not totally ramify by Lemma 3.1. Hence

$$(p) = \mathfrak{P}_0^2 \text{ or } \mathfrak{P}_1^2\mathfrak{P}_2^2 \text{ in } \mathcal{O}_L,$$

where $\mathfrak{P}_1, \mathfrak{P}_2$ form an orbit under the action of $\mathrm{Gal}(L/K)$. Now since p is odd, p tamely ramifies, and thus $v_{\mathfrak{P}_i}(\mathcal{D}_{L/K}) = 2 - 1 = 1$.

If $(p) = \mathfrak{P}_0^2$, we have $N_{L/\mathbb{Q}}(\mathfrak{P}_0) = p^4$ and by Lemma 2.18, $v_p(d_{L/K}) = 2$.

If $(p) = \mathfrak{P}_1^2\mathfrak{P}_2^2$, we have $N_{L/\mathbb{Q}}(\mathfrak{P}_i) = p^2$ and by Lemma 2.18, we also get $v_p(d_{L/K}) = 2$ in this case as well.

Assume now that $\pi \in S_1$ divides d with an odd valuation. Then $\overline{\pi}$ also divides d with an odd valuation by Lemma 3.4. In this case, π and $\overline{\pi}$ totally ramify by Lemma 3.1. We then have $(\pi) = \mathfrak{P}^4$ and $(\overline{\pi}) = \overline{\mathfrak{P}}^4$. Thus $N_{L/\mathbb{Q}}(\mathfrak{P}) = N_{L/\mathbb{Q}}(\overline{\mathfrak{P}}) = p_\pi$. Once again π and $\overline{\pi}$ are tamely ramified, and reasoning as before shows that $v_{p_\pi}(d) = 3$. Finally, assume that $v_\pi(d_{L/K}) = 2$ and so $v_{\overline{\pi}}(d) = 2$ by Lemma 3.4. By Lemma 3.1, π and $\overline{\pi}$ ramify but do not totally ramify. We then have

$$(\pi) = \mathfrak{P}_0^2 \text{ and } (\overline{\pi}) = \overline{\mathfrak{P}}_0^2$$

or

$$(\pi) = \mathfrak{P}_1^2\mathfrak{P}_2^2 \text{ and } (\overline{\pi}) = \overline{\mathfrak{P}}_1^2\overline{\mathfrak{P}}_2^2$$

In the first case we have $N_{L/\mathbb{Q}}(\mathfrak{P}_0) = N_{L/\mathbb{Q}}(\overline{\mathfrak{P}_0}) = p_\pi^2$. In the second case we have $N_{L/\mathbb{Q}}(\mathfrak{P}_i) = N_{L/\mathbb{Q}}(\overline{\mathfrak{P}_i}) = p_\pi$. We now finish the proof as before. □

Example 3.6. The cyclic extension $\mathbb{Q}(i)(\zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i)$ has relative discriminant 1125. Indeed, the only prime elements which ramify here are the prime elements lying above 3 and 5, and we may apply the previous lemma to conclude.

We now give an explicit criterion to decide whether or not A is a division K-algebra.

Lemma 3.7. *The cyclic K-algebra $A = (i, L/K, \sigma)$ is a division K-algebra if and only if there exists a prime element $\pi \in S_1$ dividing d with an odd valuation such that $p_\pi \equiv 5[8]$.*

Proof. As already pointed out, A is a division K-algebra if and only if the quaternion K-algebra (i, d) does not split. In view of the previous lemma, d is congruent to $u\pi_1\overline{\pi}_1 \cdots \pi_r\overline{\pi}_r$ modulo squares, where u is a unit and $\pi_1, \ldots, \pi_r$ are the elements of S_1 dividing d with an odd valuation. Thus, we have

$$(i, d) \simeq (i, u\pi_1\overline{\pi}_1 \cdots \pi_r\overline{\pi}_r), u = \pm 1, \pm i.$$

This implies that if $p \in S_3$, or if $\pi \in S_1$ divides d with an even valuation, the Hasse symbols $(i, d)_p, (i, d)_\pi$ and $(i, d)_{\overline{\pi}}$ are trivial. If $\pi \in S_1$ divides d with an odd valuation, the Hasse symbol is the image of $i^{(p_\pi - 1)/2}$ in $\mathbb{F}_{p_\pi}^\times$. Since $i^4 = 1$, it is equal to 1 if $p_\pi \equiv 1[8]$ and to -1 if $p_\pi \equiv 5[8]$.

We are now ready to conclude. If d is divisible by a prime element $\pi \in S_1$ with an odd valuation such that $p_\pi \equiv 5[8]$, then the Hasse symbol $(i, d)_\pi$ is not trivial, so (i, d) does not split and A is a division K-algebra in this case. If d is not divisible by a prime element satisfying the previous conditions, then all Hasse symbols $(i, d)_{\pi'}, \pi' \neq 1 - i$ are trivial. The remaining Hasse symbol is then trivial by the product formula, hence (i, d) splits and A is not a division K-algebra. □

We may now finish the proof of Theorem 3.3. Assume that we may build a suitable code on a cyclic division K-algebra $A = (i, L/K, \sigma)$ with $d_{L/K} < 1125$. By Lemma 3.7, there exists $\pi \in S_1$ dividing d with an odd valuation such that $p_\pi \equiv 5[8]$. In particular, $p_\pi \geq 5$. Then by Lemma 3.5, we have $p_\pi^3 \mid d_{L/K}$. Thus, we necessarily have $\pi = 1 + 2i$ and $125 \mid d_{L/K}$ (Otherwise, we would have $p_\pi \geq 13$ and $d_{L/K} \geq 13^3 > 1125$). Now if $\pi' \in S_1, \pi' \neq 1 + 2i$ divides d, we would have $125 \cdot p_{\pi'}^2 \mid d_{L/K}$, and thus $p_{\pi'}^2 \leq 9$, which is a contradiction since $p_{\pi'} \geq 5$. Similarly, if $p \in S_3$ divides d, we have $125 \cdot p^2 \mid d_{L/K}$ and thus necessarily $p = 3$.

Hence the only possible prime divisors for d are $1 - i, 3$ and $1 \pm 2i$. Noticing that conjugate values of d generate the same field extension, we see that the remaining possibilities for d are

$$d = u \cdot 3^m(1 + 2i)(1 - 2i)^3, m = 0, 2, u = \pm 1, \pm i.$$

Using PARI GP [17] to compute the relative discriminants of the corresponding extensions, we see that the only possibility to have $d_{L/K} < 1125$ is

$$d = (1 + 2i)(1 - 2i)^3.$$

In this case, $d_{L/K} = 125 < 4^4$. Hence, using Corollary 2.24, we see that no complex ideal lattice on L/K will be isomorphic to the cubic lattice, and this completes the proof.

3.3. **The case** $n = 6$**.** If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a codebook built on a cyclic division K-algebra $A = (\gamma, L/K, \sigma)$, then this time we have

$$\frac{1}{\delta_{min}(\mathcal{C})} \leq |\gamma_2|^{10} d_{L/K},$$

where we have written $\gamma = \dfrac{\gamma_1}{\gamma_2}$ with $\gamma_1, \gamma_2 \in \mathcal{O}_K$ relatively prime.

In [10], Oggier et al. constructed a PSTBC on the cyclic division $\mathbb{Q}(j)$-algebra

$$(-j, \mathbb{Q}(j)(\zeta_{28} + \zeta_{28}^{-1})/\mathbb{Q}(j), \sigma).$$

The cyclic extension $\mathbb{Q}(j)(\zeta_{28} + \zeta_{28}^{-1})/\mathbb{Q}(j)$ has relative discriminant $2^6 \cdot 7^5$. Hence for any $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$, we get

$$\frac{1}{\delta_{min}(\mathcal{C})} \leq 2^6 \cdot 7^5.$$

Once again, this bound is optimal:

Theorem 3.8. *If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is a PSTBC built on a cyclic division K-algebra $A = (\gamma, L/K, \sigma)$ of degree 6, then we have*

$$|\gamma_2|^{10} d_{L/K} \geq 2^6 \cdot 7^5.$$

Arguing as in the previous section, we see that we may assume without loss of generality that $K = \mathbb{Q}(j)$ and $A = (-j, L/K, \sigma)$. In this case, we are reduced to show that there is no PSTBC on A such that $d_{L/K} < 2^6 \cdot 7^5$.

We now assume that $K = \mathbb{Q}(j)$ and that $L = K(\sqrt[6]{d})$, where $d \in \mathcal{O}_K$ is not divisible by any 6^{th}-power of an element of $\mathcal{O}_K$.

We denote by $T_2, T_1, \overline{T}_1$ the following subsets of $\mathcal{O}_K$:

$$T_2 = \{p \equiv 2[3], p > 2 \text{ prime number } \}$$

$$T_1 = \{\pi = a + bj \mid 0 < a < b, p_\pi = a^2 + b^2 - ab, p_\pi \equiv 1[3], p_\pi \text{ prime } \}$$

$$\overline{T}_1 = \{\overline{\pi} \mid \pi \in T_1\}.$$

Then any prime element of $\mathcal{O}_K$ is associate either to $1 - j$, 2 or to exactly one element of T_2, T_1 or $\overline{T}_1$.

We then have:

Lemma 3.9. *Let $L = K(\sqrt[6]{d})$. Then complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with $\mathrm{Gal}(L/K)$ if and only if all the following conditions are satisfied:*

(1) $v_{1-j}(d) = 0$.
(2) $v_p(d) = 0$ *or* 3, *for all* $p \in T_2$ *or* $p = 2$.
(3) $(v_\pi(d), v_{\overline{\pi}}(d)) = (1,5), (2,4), (3,3), (4,2)$ *or* $(5,1)$ *for all* $\pi \in T_1$ *dividing* d.

We will assume from now on that the conditions above are satisfied. In this case, we have the following estimation of the relative discriminant.

Lemma 3.10. *The prime-to-6 part of $d_{L/K}$ is*

$$\Big(\prod_{\substack{p \in T_2 \\ p|d}} p\Big)^3 \Big(\prod_{\substack{\pi \in T_1 \\ v_\pi(d) = 1,5}} p_\pi\Big)^5 \Big(\prod_{\substack{\pi \in T_1 \\ v_\pi(d) = 3}} p_\pi\Big)^3 \Big(\prod_{\substack{\pi \in T_1 \\ v_\pi(d) = 2,4}} p_\pi\Big)^4.$$

Moreover, the following holds:

(1) *If 2 ramifies in L/K, then $v_2(d_{L/K}) \geq 6$*
(2) *If $1-j$ ramifies in L/K, then $v_3(d_{L/K}) \geq 4$.*

Proof. Let $p \in T_2$ dividing d. By Lemma 3.9, $v_p(d) = 3$, so p ramifies but does not totally ramify by Lemma 3.1. Moreover, p tamely ramifies since p is prime to 6. Write $d = d'p^3$ with $d' \in \mathcal{O}_K, p \nmid d'$. Then p totally ramifies in $K_2 = K(\sqrt{d}) = K(\sqrt{d'p})$ by the same lemma, so we may write

$$(p) = \mathfrak{p}_0^2,$$

for some ideal $\mathfrak{p}_0$ of $\mathcal{O}_{K_2}$. Since L/K_2 is a Galois extension of prime degree 3 , either $\mathfrak{p}_0$ is totally ramified, inert or totally split. Since $\mathfrak{p}_0$ cannot be totally ramified (otherwise p would be totally ramified), we finally have

$$(p)\mathcal{O}_L = \mathfrak{p}_0^2 \text{ or } \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2 \text{ in } \mathcal{O}_L,$$

where $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ form an orbit under the action of $\mathrm{Gal}(L/K_2)$.

If $(p) = \mathfrak{p}_0^2$, we have $N_{L/\mathbb{Q}}(\mathfrak{p}_0) = p^6$, and since $v_{\mathfrak{p}_0}(\mathcal{D}_{L/K}) = 1$, we get $v_p(d_{L/K}) = 3$.

If $(p) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$, we have $N_{L/\mathbb{Q}}(\mathfrak{p}_i) = p^2$, and since $v_{\mathfrak{p}_i}(\mathcal{D}_{L/K}) = 1$, we also get $v_p(d_{L/K}) = 3$ in this case.

Now, let $\pi \in T_1$ such that $v_\pi(d) = 1$ or 5. Then $v_{\overline{\pi}}(d) = 5$ or 1 respectively. By Lemma 3.1, π and $\overline{\pi}$ totally ramify, so we have

$$(\pi) = \mathfrak{p}^6 \text{ and } (\overline{\pi}) = \overline{\mathfrak{p}}^6 \text{ in } \mathcal{O}_L,$$

with $N_{L/\mathbb{Q}}(\mathfrak{p}) = p_\pi$. We then have $v_{\mathfrak{p}}(\mathcal{D}_{L/K}) = 5 = v_{\overline{\mathfrak{p}}}(\mathcal{D}_{L/K})$ and thus $v_{p_\pi}(d_{L/K}) = 5$.

Let $\pi \in T_1$ such that $v_\pi(d) = 3$. Then we also have $v_{\overline{\pi}}(d) = 3$. Reasoning as above, we see that we have

$$(\pi) = \mathfrak{p}_0^2 \text{ or } \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2 \text{ in } \mathcal{O}_L,$$

and similarly for $(\overline{\pi})$, so that $v_{p_\pi}(d_{L/K}) = 3$.

Finally, let $\pi \in T_1$ such that $v_\pi(d) = 2$ or 4, and set $K_3 = K(\sqrt[3]{d})$. In this case, we have

$$(\pi) = \mathfrak{p}_0^3 \text{ or } \mathfrak{p}_1^3\mathfrak{p}_2^3 \text{ in } \mathcal{O}_L,$$

where $\mathfrak{p}_1, \mathfrak{p}_2$ form an orbit under the action of $\mathrm{Gal}(L/K_3)$. One may check as before that in both cases, we have $v_{p_\pi}(d_{L/K}) = 4$.

We now examine the case of the wildly ramified primes. Let us start with $1 - j$. Since $1 - j$ does not divide d or 2, it does not ramify in K_2. Then it necessarily totally ramifies in K_3, so we have

$$(1 - j) = \mathfrak{p}_0^3 \text{ in } \mathcal{O}_{K_3},$$

where $N_{K_3/\mathbb{Q}}(\mathfrak{p}_0) = 3$. Now since $1 - j$ wildly ramifies, $v_{\mathfrak{p}_0}(\mathcal{D}_{K_3/K}) \geq 3$. Therefore, 3^3 divides $N_{K_3/\mathbb{Q}}(\mathcal{D}_{K_3/K}) = d_{K_3/K}^2$. Since $d_{K_3/K}$ is an integer, we get that $3^2 \mid d_{K_3/K}$. By Corollary 2.19, we get $3^4 \mid d_{L/K}$.

Assume now that 2 ramifies in L/K. Since $v_2(d) = 0$ or 3, it does not ramify in K_3, hence it totally ramifies in K_2. We then have

$$(2) = \mathfrak{p}_0^2 \text{ in } \mathcal{O}_{K_2},$$

so that $N_{K_2/\mathbb{Q}}(\mathfrak{p}_0) = 2^2$. Since 2 wildly ramifies, $v_{\mathfrak{p}_0}(\mathcal{D}_{K_2/K}) \geq 2$, and we get as before that $2^4 \mid d_{K_2/K}^2$. Hence $2^2 \mid d_{K_2/K}$, and by Corollary 2.19, we get $2^6 \mid d_{L/K}$. □

As before we now give an explicit criterion to decide whether or not A is a division K-algebra.

Lemma 3.11. *The cyclic K-algebra $A = (-j, L/K, \sigma)$ is a division K-algebra if and only if there exist (not necessarily distinct) prime elements $\pi, \pi' \in T_1$ such that $v_\pi(d)$ is odd, $v_{\pi'}(d)$ is prime to 3 and satisfying the following conditions:*

(1) $p_\pi \equiv 7[12]$.

(2) $p_{\pi'} \equiv 4$ *or* $7[9]$.

Proof. Since K is a number field, the index of A equals the exponent of A. Thus A will be a division K-algebra if and only if $2[A] \neq 0$ and $3[A] \neq 0$. Notice that A is nothing but the symbol K-algebra $\{-j, d\}_6$. Hence $3[A] = [(-j, d)]$ and $2[A] = [\{-j, d\}_3]$. Since $(-j, d)$

and $\{-j,d\}_3$ have prime degrees, we conclude that A will be a division K-algebra if and only if $A_2=(-j,d)$ and $A_3=\{-j,d\}_3$ are not split.

Using Lemma 3.9 and properties of quaternion K-algebras, we see that we have

$$A_2=(-j,u2^m\pi_1\overline{\pi}_1\dots\pi_r\overline{\pi}_r p_1\cdots p_s),$$

where u is a unit, $m=0$ or 1, $\pi_1,\dots,\pi_r\in T_1$ and $p_1,\dots,p_s\in T_2$ are prime elements dividing d with an odd valuation.

It follows in particular that if $\pi\neq\pi_i,p_j$, then the corresponding Hasse symbol is trivial. If $\pi=p\in T_2$, then the number of elements of the residue field $\kappa(\pi)$ is $q_\pi=p^2$. The corresponding Hasse symbol is then equal to

$$\overline{-j}^{\frac{p^2-1}{2}}\in\kappa(\pi)^\times.$$

Since $p\equiv 2[3]$ and p is odd, we have $p\equiv 5[6]$, so p^2-1 is a multiple of 12. Since $(-j)^6=1$, we deduce that the Hasse symbol is trivial in this case as well.

Assume now that $\pi\in T_1$. In this case $q_\pi=p_\pi$, and the corresponding Hasse symbol is then equal to

$$\overline{-j}^{\frac{p_\pi-1}{2}}\in\kappa(\pi)^\times.$$

This Hasse symbol will then be trivial if and only if $6\mid\frac{p_\pi-1}{2}$, that is $p_\pi\equiv 1[12]$. In other words, since $p_\pi\equiv 1[3]$ and p_π is odd, the Hasse symbol will be non-trivial if and only if $p_\pi\equiv 7[12]$. Notice also that the Hasse symbols corresponding to π and $\overline{\pi}$ are equal.

It follows from our computations above that if no prime element $\pi\in T_1$ such that $p_\pi\equiv 7[12]$ divides d with an odd valuation, then all the Hasse symbols of A_2 are trivial, except maybe for the Hasse symbol corresponding to 2. By the product formula, this last symbol is also trivial, and A_2 is split in this case. If however such a π exists, then A_2 has at least one non-trivial Hasse symbol, and is therefore not split.

Thus A_2 is not split if and only if there exists $\pi\in T_1$ such that $p_\pi\equiv 7[12]$ dividing d with an odd valuation.

Using Lemma 3.9 and properties of symbol K-algebras, we see that we have

$$A_3=\{j,u\pi_1\overline{\pi}_1^2\dots\pi_r\overline{\pi}_r^2\pi_1'^2\overline{\pi'}_1\cdots\pi_s'^2\overline{\pi'}_s\}_3,$$

where u is a unit and $\pi_1,\dots,\pi_r,\pi_1',\dots,\pi_s'\in T_1$ are prime elements dividing d with a valuation prime to 3.

The Hasse symbol corresponding to each of these prime elements has the form $\overline{j}^{m\frac{p_\pi-1}{3}}$, where $m=1$ or 2. This symbol is then trivial if and only if $p_\pi\equiv 1[9]$. In other words, the corresponding Hasse symbol is not trivial if and only if $p_\pi\equiv 4,7[9]$.

Reasoning as above, we see that A_3 is not split if and only if there exists $\pi \in T_1$ such that $p_\pi \equiv 4, 7[9]$ dividing d with a valuation prime to 3. This concludes the proof. □

Assume now that we may build an energy-preserving code on a cyclic division K-algebra $A = (-j, L/K, \sigma)$, where $d_{L/K} < 2^6 \cdot 7^5$.

Let $\pi \in T_1$ divide d with an odd valuation, such that $p_\pi \equiv 7[12]$ (such a π exists by the previous result). If $p_\pi > 7$, then $p_\pi \geq 19$. In this case, Lemma 3.10 implies that $19^3 \mid d_{L/K}$. Now let $\pi' \in T_1$ divide d with a valuation which is prime to 3, such that $p_{\pi'} \equiv 4, 7[9]$. We then have $p_{\pi'} \geq 7$ and thus Lemma 3.10 implies that $7^4 \mid d_{L/K}$. Hence $7^4 \cdot 19^3 \mid d_{L/K}$, which is a contradiction since $7^4 \cdot 19^3 > 2^6 \cdot 7^5$.

Therefore, $p_\pi = 7$. We then get $7^3 \mid d_{L/K}$. If $p_{\pi'} > 7$, we have $p_{\pi'} \geq 13$ and thus $7^3 \cdot 13^4 \mid d_{L/K}$, which is again a contradiction. Hence $p_{\pi'} = 7$.

Hence we have proved that $\pi = \pi' = 2 + 3j$. Moreover, since $2 + 3j$ divides $d_{L/K}$ with an odd valuation, which is also prime to 3, then $v_{2+3j}(d_{L/K}) = 1$ or 5, and thus $7^5 \mid d_{L/K}$.

Assume that $p \in T_2$ ramifies in L/K. Since $p \equiv 2[3]$, we have $p \geq 5$, and by Lemma 3.10, we get $5^3 \mid d_{L/K}$. We then get a contradiction, since $5^3 \cdot 7^5 > 2^6 \cdot 7^5$. If $\pi'' \in T_1 \cup \overline{T}_1, \pi'' \nmid 7$ ramifies in L/K, we have $p_{\pi''} \geq 13$ since $p_{\pi''} \equiv 1[3]$. In this case, we obtain that $13^3 \mid d_{L/K}$, which again yields a contradiction. Notice that $1 - j$ and 2 do not ramify in L/K either, since otherwise we would have $3^4 \cdot 7^5 \mid d_{L/K}$ or $2^6 \cdot 7^5 \mid d_{L/K}$, which is a contradiction.

The computations above shows that $d_{L/K} = 7^5 < 6^6$, so we may not construct the cubic lattice as a complex ideal lattice on L/K by Corollary 2.24.

This proves Theorem 3.8.

4. Optimality of codes based on biquadratic crossed products

Let L/K be a biquadratic extension, and fix two generators σ, τ of $G = \mathrm{Gal}(L/K)$. Then any G-crossed product is isomorphic to the K-algebra $(a, b, u, L/K, \sigma, \tau)$, for some $a, b, u \in L^\times$, which is generated by two elements e and f subject to the relations

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

Notice that these relations imply that $(abu^\tau)^{\sigma\tau} = abu^\tau$.

A K-basis of this K-algebra is given by $1, e, f, ef$. A triple (a, b, u) satisfying the conditions above will be called (σ, τ)**-admissible**.

The corresponding cocycle is the map $\xi : G \times G \to L^\times$ defined by

$$\begin{aligned}\xi_{\mathrm{Id},\mathrm{Id}} = 1, \xi_{\mathrm{Id},\sigma} = 1, \xi_{\mathrm{Id},\tau} = 1, \xi_{\mathrm{Id},\sigma\tau} = 1,\\ \xi_{\sigma,\mathrm{Id}} = 1, \xi_{\sigma,\sigma} = a, \xi_{\sigma,\tau} = 1, \xi_{\sigma,\sigma\tau} = a^\tau,\\ \xi_{\tau,\mathrm{Id}} = 1, \xi_{\tau,\sigma} = u, \xi_{\tau,\tau} = b, \xi_{\tau,\sigma\tau} = bu^\tau,\\ \xi_{\sigma\tau,\mathrm{Id}} = 1, \xi_{\sigma\tau,\sigma} = a^\tau u, \xi_{\sigma\tau,\tau} = b, \xi_{\sigma\tau,\sigma\tau} = abu^\tau.\end{aligned}$$

It follows that the cocycle values all have modulus 1 if and only if $|a|^2 = |b|^2 = |u|^2 = 1$, provided that complex conjugation commutes with the elements of G.

Lemma 4.1. *The multiplication matrix* $\mathbf{X}$ *of* $x = x_1 + ex_\sigma + fx_\tau + efx_{\sigma\tau}$ *in the* K*-algebra* $(a, b, u, L/K, \sigma, \tau)$ *is given by*

$$\begin{pmatrix} x_1 & ax_\sigma^\sigma & bx_\tau^\tau & abu^\tau x_{\sigma\tau}^{\sigma\tau} \\ x_\sigma & x_1^\sigma & bx_{\sigma\tau}^\tau & bu^\tau x_\tau^{\sigma\tau} \\ x_\tau & a^\tau u x_{\sigma\tau}^\sigma & x_1^\tau & a^\tau x_\sigma^{\sigma\tau} \\ x_{\sigma\tau} & u x_\tau^\sigma & x_\sigma^\tau & x_1^{\sigma\tau} \end{pmatrix}.$$

In [2], Oggier and the first author constructed a suitable code on the division $\mathbb{Q}(i)$-algebra

$$A = (\zeta_8, \frac{1+2i}{\sqrt{5}}, i, \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})/\mathbb{Q}(i), \sigma, \tau),$$

where

$$\begin{aligned}\sigma(\sqrt{2}) = \sqrt{2}, \sigma(\sqrt{5}) = -\sqrt{5}\\ \tau(\sqrt{2}) = -\sqrt{2}, \tau(\sqrt{5}) = \sqrt{5}\end{aligned}$$

The biquadratic extension $L = \mathbb{Q}(i)(\sqrt{2}, \sqrt{5})$ of $\mathbb{Q}(i)$ has relative discriminant 400, as we will see later on.

Let us compute Δ_ξ in this case. Clearly we have

$$\Delta_\xi^{(\mathrm{Id})} = \Delta_\xi^{(\sigma)} = 1.$$

Moreover, we have

$$\mathcal{E}_\xi^{(\tau)} = \mathcal{E}_\xi^{(\sigma\tau)} = \{c \in \mathbb{Z}[i] \mid cb \in \mathcal{O}_L\}.$$

We claim that $\Delta_\xi^{(\tau)} = 5$. Notice that $1 - 2i \in \mathcal{E}_\xi^{(\tau)}$ since $(1-2i)b = \sqrt{5}$. Hence $\Delta_\xi^{(\tau)}$ divides $|1-2i|^2 = 5$. Since $b \notin \mathcal{O}_L$ (its minimal polynomial over $\mathbb{Q}$ is $X^4 - \frac{6}{5}X^2 + 1 \notin \mathbb{Z}[X]$), we have $\Delta_\xi^{(\tau)} \neq 1$ and therefore $\Delta_\xi^{(\tau)} = 5$. Thus we also have $\Delta_\xi^{(\sigma\tau)} = 5$ and $\Delta_\xi = 25$.

In particular, Proposition 2.25 shows that the minimum determinant of any code $\mathcal{C}$ built on this division $\mathbb{Q}(i)$-algebra satisfies

$$\delta_{min}(\mathcal{C}) \geq \frac{1}{10000}.$$

Remark 4.2. Notice that in [2], the better bound $\frac{1}{2500}$ was announced. This bound is not correct, since it was obtained by writing $b = \frac{\sqrt{1+2i}}{\sqrt{1-2i}}$, and taking the denominator outside the multiplication matrix. However, the conclusion that the determinant of the remaining matrix was an element of $\mathcal{O}_K$ was not correct, since $\sqrt{1+2i} \notin \mathcal{O}_L$.

We will show in this section that the bound obtained above is optimal, in the following sense:

Theorem 4.3. *Let $K = \mathbb{Q}(i)$. If $\mathcal{C} \subset \mathcal{C}_{A,\lambda,I}$ is an energy-preserving code built on a biquadratic crossed product division K-algebra $A = (a, b, u, L/K, \sigma, \tau)$, then we have*

$$d_{L/K}\Delta_\xi \geq 10000.$$

We will assume in the sequel that $K = \mathbb{Q}(i)$. We start with the study of the ramification of biquadratic extensions of K.

Lemma 4.4. *Let $F = K(\sqrt{d})$. Then complex conjugation induces a $\mathbb{Q}$-automorphism of L which commutes with $\mathrm{Gal}(F/K)$ if and only if all the following conditions are satisfied:*

(1) $v_{1-i}(d) = 0$.
(2) $v_p(d) = 0$ *or* 1, *for all* $p \in S_3$.
(3) $v_\pi(d) = v_{\overline{\pi}}(d) = 1$ *for all* $\pi \in S_1$ *dividing* d.

Let $L = K(\sqrt{d}, \sqrt{d'})$ be a biquadratic extension, whose Galois group commutes with complex conjugation. Then d and d' have the form m or mi, where m is a squarefree odd integer (apply twice the previous lemma). Moreover, we have $4mi = 2m(1+i)^2$, so we may in fact assume that d and d' are squarefree integers. Since -1 is a square, we may also assume that d and d' are positive.

We will then assume from now on that $L = K(\sqrt{d}, \sqrt{d'})$, where d and d' are squarefree positive integers.

Notice for later use that if π is an irreducible element lying above the prime number p dividing d and d', then $p \mid d$ and $p \mid d'$ (This is clear if π is a prime number, and if $p \equiv 1[4]$, it follows from the fact that $\overline{\pi}$ also divides d and d').

Proposition 4.5. *Let $L = K(\sqrt{d}, \sqrt{d'})$, where d and d' are squarefree positive integers. Then the following properties hold:*

(1) *The odd part of* $d_{L/K}$ *is* $\prod_p p^2$*, where* p *runs through the odd prime numbers that divide* d *or* d'*.*
(2) *The element* $1-i$ *ramifies in* L *if and only if* d *or* d' *is even. In this case,* $2^4 \mid d_{L/K}$*.*

Proof. Let p be an odd prime integer and let π be an irreducible element lying above p. Assume that p does not divide d and d'. Then $\pi \nmid d$ and $\pi \nmid d'$ (this comes from Lemma 4.4) , and thus π does not ramify in $K(\sqrt{d})$ and $K(\sqrt{d'})$. Therefore, π does not ramify in L. Assume now that $p \mid d$ for example. Replacing d' by $\dfrac{dd'}{p^2}$ if necessary, one may assume that $p \nmid d'$, so that π does not ramify in $M' = K(\sqrt{d'})$. Since π divides d, it totally ramifies in $M = K(\sqrt{d})$. Write $(\pi) = \mathfrak{p}^2$. Since π does not ramify in M', $\mathfrak{p}$ does not ramify in L/M. Hence π ramifies but does not totally ramify in L.

We then either have $(\pi) = \mathfrak{P}_0^2$ or $(\pi) = \mathfrak{P}_1^2\mathfrak{P}_2^2$ in $\mathcal{O}_L$. Reasoning as in the proof of Lemma 3.10, we may show that $v_p(d_{L/K}) = 2$.

We now study the ramification of $1-i$ in $M = K(\sqrt{d})$.

Assume first that d is odd. If $d \equiv 1[4]$ (resp. $d \equiv 3[4]$), then $x = 1$ (resp. $x = i$) is a solution of the equation $x^2 \equiv d \mod 4\mathcal{O}_K$. Hence $1-i$ does not ramify in $K(\sqrt{d})$.

If now d is even, then the equation $x^2 \equiv d \mod 4\mathcal{O}_K$ has no solution. Assume to the contrary that $x \in \mathcal{O}_K$ is a solution. Since $d = 2m$, m odd, we have $d \equiv 2[4]$, so $x^2 \equiv 2 \mod 4\mathcal{O}_K$. Writing $x = a+bi, a, b \in \mathbb{Z}$ and comparing real parts show that $a^2 - b^2 \equiv 2[4]$. But $a^2 - b^2$ is always congruent to 0 or ± 1 modulo 4, hence we have a contradiction. Thus $1-i$ totally ramifies in M in this case.

It follows as before that $1-i$ ramifies in L if and only if d or d' is even. It remains to prove that $2^4 \mid d_{L/K}$ in this case. Assume for example that d is even, so that $1-i$ totally ramifies in M. By [7, Theorem 1], a $\mathbb{Z}$-basis of $\mathcal{O}_M$ is

$$1, i, \sqrt{d}, \frac{1-i}{2}\sqrt{d}.$$

Now let $\mathfrak{P}$ be the unique prime ideal of $\mathcal{O}_M$ lying above $1-i$, and consider the third ramification group of M/K

$$\begin{aligned} G_3 &= \{\rho \in \mathrm{Gal}(M/K) \mid \rho(\alpha) \equiv \alpha \mod \mathfrak{P}^4 \text{ for all } \alpha \in \mathcal{O}_M\} \\ &= \{\rho \in \mathrm{Gal}(M/K) \mid \rho(\alpha) \equiv \alpha \mod 2\mathcal{O}_M \text{ for all } \alpha \in \mathcal{O}_M\} \end{aligned}$$

Now any $\alpha \in \mathcal{O}_M$ has the form $\alpha = \alpha_1 + \alpha_2 i + \alpha_3\sqrt{d} + \alpha_4\dfrac{1-i}{2}\sqrt{d}$, where $\alpha_i \in \mathbb{Z}$. If ι is the unique non-trivial automorphism of M/K, we

have

$$\iota(\alpha) - \alpha = -2(\alpha_3\sqrt{d} + \alpha_4\frac{1-i}{2}\sqrt{d}) \in 2\mathcal{O}_M.$$

Therefore G_3 is non-trivial, which implies that

$$v_{\mathfrak{P}}(\mathcal{D}_{K(\sqrt{d})/K}) = \sum_{i\geq 0}(|G_i| - 1) \geq 4,$$

since the ramification groups form a decreasing sequence. This then gives as usual $2^4|d^2_{M/K}$, which by Proposition 2.19 implies that $2^4|d_{L/K}$. □

Example 4.6. Let $L = K(\sqrt{2}, \sqrt{5})$. In this case, the only prime ideals which ramify in L are those generated by the prime elements $1-i, 1+2i$ and $1-2i$. Set $M = K(\sqrt{2})$ and $M' = K(\sqrt{5})$. Notice that 2 remains inert in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ and then totally ramifies $M/\mathbb{Q}(\sqrt{5})$. It follows easily that $1-i$ is inert in M/K. In particular, $\mathfrak{d}_{L/M}$ is not divisible by any prime ideal lying above $1-i$. Proposition 2.19 then implies that $v_2(d_{L/K}) = v_2(d^2_{M/K})$.

As pointed in the proof of the previous proposition, $1, i, \sqrt{2}, \frac{1-i}{2}\sqrt{2}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_M$. One may then check that $\iota(\zeta_8)-\zeta_8 \notin (1-i)^5\mathcal{O}_M$, where ι is the unique non-trivial automorphism of M/K. Thus the fourth ramification group of M/K is trivial. Hence $v_{\mathfrak{P}}(\mathcal{D}_{K(\sqrt{d})/K}) = 4$, and it follows that $v_2(d_{L/K}) = v_2(d^2_{M/K}) = 4$. We then get $d_{L/K} = 2^4 5^2 = 400$.

The following lemma shows that the existence of an energy-preserving code built on a G-crossed product does not depend on the choice of the two generators of G.

Lemma 4.7. *Let L/K be a biquadratic extension, and let σ, τ be two generators of the Galois group of L/K. If (a, b, u) is (σ, τ)-admissible, then (a, abu^τ, u) is $(\sigma, \sigma\tau)$-admissible, (abu^τ, b, u^τ) is $(\sigma\tau, \tau)$-admissible and we have*

$$(a, b, u, L/K, \sigma, \tau) \simeq (a, abu^\tau, u, L/K, \sigma, \sigma\tau) \simeq (abu^\tau, b, u^\tau, L/K, \sigma\tau, \tau).$$

Proof. The first part may be obtained by easy (but slightly tedious) computations. If e, f are the generators of the first K-algebra, the isomorphisms with the second and the third one are obtained by taking e, ef and ef, f as new sets of generators. □

In particular, if any of these three K-algebras is division, so are the other two. Moreover, if complex conjugation commutes with the elements of G, we have

$$\begin{aligned} |a|^2 = |b|^2 = |u|^2 = 1 \quad &\iff \quad |a|^2 = |abu^\tau|^2 = |u|^2 = 1 \\ &\iff \quad |abu^\tau|^2 = |b|^2 = |u^\tau|^2 = 1. \end{aligned}$$

It follows that if one may build an energy-preserving code on a G-crossed product K-algebra for a particular choice of generators, one may also build a suitable code for another choice of generators.

From now on, if $L = K(\sqrt{d}, \sqrt{d'})$, we set

$$\sigma(\sqrt{d}) = \sqrt{d}, \sigma(\sqrt{d'}) = -\sqrt{d'}$$
$$\tau(\sqrt{d}) = -\sqrt{d}, \tau(\sqrt{d'}) = \sqrt{d'}$$

Proposition 4.8. *Let $A = (a, b, u, L/K, \sigma, \tau)$. Assume that A is a division K-algebra. Then d or d' is divisible by an irreducible element π lying above a prime $p \equiv 1[4]$.*

Proof. Let M be any quadratic subfield of L. Since M is a quadratic K-subalgebra of A, A_M is not a division K-algebra. (If A is not division, this is clear, and if A is division, see [11, Corollary 13.4] for example). In particular, A_M has index at most 2 and $2[A]_M = 0 \in \mathrm{Br}(M)$. Hence $2[A]$ is split by any quadratic subfield of L.

It follows that any field extension K'/K in which at least one of the elements d, d' or dd' is a square splits $2[A]$. Indeed, in this case, K' contains at least one quadratic subfield M of L, and since M splits $2[A]$, so does K'.

Assume that d and d' are only divisible by prime elements $p \equiv 3[4]$ and eventually by 2, and let us prove that $2[A] = 0$ in this case, showing that A is not a division K-algebra.

Let $\pi \neq 1 - i$ be an irreducible element of $\mathcal{O}_K$. We are going to prove that $2[A]$ splits over K_π.

If π is lying above the prime number p and π divides d and d', then p divides d and d'. Thus replacing d by $\dfrac{dd'}{p^2}$ if necessary, we may assume that $\pi \nmid d$. Assume first that $\pi \nmid d$ and $\pi \nmid d'$. If d or d' is a square modulo $\pi\mathcal{O}_K$, since π does not lie above 2, applying Hensel's lemma shows that d or d' is a square in K_π. If d and d' are not squares modulo $\pi\mathcal{O}_K$, they both represent the unique non-trivial square class of the finite field $\mathcal{O}_K/\pi\mathcal{O}_K$, hence dd' is a (non-zero) square modulo $\pi\mathcal{O}_K$. Once again, we may use Hensel's lemma to conclude.

Assume now that $\pi \nmid d$ and $\pi \mid d'$. We are going to show that d is a square in K_π. Since $\pi \mid d'$, then by assumption $\pi = p$, where p is a prime number which is congruent to 3 modulo 4.

If $d \in \mathbb{Z}$ is a square modulo $p\mathbb{Z}$, then d is a square modulo $p\mathcal{O}_K$. If d is not a square modulo $p\mathbb{Z}$, then d represents the unique non-trivial square-class modulo $p\mathbb{Z}$, which is the class of -1, since $p \equiv 3[4]$. Hence $-d$ is a square modulo $p\mathbb{Z}$, hence a square modulo $p\mathcal{O}_K$. Then

$d = i^2(-d)$ is a square modulo $p\mathcal{O}_K$. As before, Hensel's lemma implies that d is a square in the corresponding completion of K in both cases.

Therefore, $2[A]$ splits over K_π for all $\pi \neq 1 - i$. By the Brauer-Hasse-Noether's theorem, $2[A]$ splits at all completions of K, and thus $2[A] = 0$. □

Lemma 4.9. *Let $F = K(\sqrt{\Delta})$, where Δ is a square free positive integer. Let $x \in \mathcal{O}_F$ such that $|x|^2 = 1$. Then x is a root of 1.*

More precisely:

(1) *If $\Delta \neq 2$ or 3, then x is a 4th root of 1.*
(2) *If $\Delta = 2$, x is an 8th root of 1.*
(3) *If $\Delta = 3$, x is a 4th root of 1 or a 6th root of 1.*

Proof. Since F is stable by conjugation, we have $\overline{x} \in \mathcal{O}_F$. Hence $x \in \mathcal{O}_F^\times$. Since $F/\mathbb{Q}$ is totally imaginary, Dirichlet's unit theorem shows that $x = \zeta\varepsilon_F^r, r \in \mathbb{Z}$, where $\varepsilon_F \in \mathcal{O}_F^\times$ is a fundamental unit and $\zeta \in L$ is a root of 1. Since $|\varepsilon_F| > 1$ and $|x| = 1$, we get $r = 0$, so x is a root of 1. Write $x = e^{\frac{2ik\pi}{\ell}}, gcd(k, \ell) = 1$. Then $\mathbb{Q}(x) = \mathbb{Q}(\zeta_\ell) \subset F$. Since $[F : \mathbb{Q}] = 4$, it implies that $\varphi(\ell) \leq 4$, so we get $\ell = 1, 2, 3, 4, 5, 6$ or 8. If $\ell = 5$, we get $\mathbb{Q}(\zeta_5) = F$, which is impossible as the Galois group of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is cyclic, while the Galois group of $F/\mathbb{Q}$ is the Klein group. This implies that x is a m-th root of 1, with $m = 6$ or 8 in any case.

If $\ell = 1, 2$ or 4, we get that x is in fact a 4th root of 1.

If $\ell = 3$ or 6, x is in both cases a 6th root of 1. Moreover, we get $\mathbb{Q}(j) = \mathbb{Q}(i\sqrt{3}) \subset F$, so $\mathbb{Q}(i\sqrt{3})$ is one of the three quadratic subfields of F. The only possibility is that $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(i\sqrt{\Delta})$, and since Δ is positive and squarefree, we get $\Delta = 3$. Finally, if $\ell = 8$, we get $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}) = F$. Comparing quadratic subfields shows that $\Delta = 2$. This concludes the proof. □

Lemma 4.10. *Assume that $A = (a, b, u, L/K, \sigma, \tau)$ is a division K-algebra. Then the elements a, b and abu^τ do not lie in K. Moreover, if one may build an energy-preserving code on A, then at most one of these elements lies in $\mathcal{O}_L$.*

Proof. If $a \in K$, the elements e and $\sqrt{d'}$ generate a K-subalgebra of A which is isomorphic to the quaternion K-algebra $A_1 = (a, d')$. Since A has degree 4, the centraliser A_2 of A_1 in A has degree 2. Now as A_2 is central simple, the centraliser theorem shows that $A \simeq A_1 \otimes_K A_2$. Since A_1 and A_2 have degree 2, we get $2[A] = 2[A_1] + 2[A_2] = 0 \in \mathrm{Br}(K)$. Hence A is not a division K-algebra. If $b \in K$ or $abu^\tau \in K$, similar arguments show that A is not a division K-algebra in these two cases (consider the elements f and $\sqrt{d}$ for the first case, and the elements ef and $\sqrt{dd'}$ for the second one).

Recall now that $a \in K(\sqrt{d}), b \in K(\sqrt{d'})$ and $abu^\tau \in K(\sqrt{dd'})$. Hence a, b and abu^τ all lie in a different quadratic subfield of L. Assume that one may build an energy-preserving code on the division K-algebra A, so a, b and u (hence abu^τ) have modulus 1.

Assume that two of the elements above lie in $\mathcal{O}_L$. Then they are units of the ring of integers of the quadratic subfield of L they belong to. If one of them is a 4th root of 1, then A is not a division K-algebra by the previous point, which is a contradiction. Since they lie in a different quadratic subfield of F, Lemma 4.9 implies that $L = K(\sqrt{2}, \sqrt{3})$. However, $d_{L/K} < 256$ in this case, contradicting the existence of a code built on A by Corollary 2.24. This completes the proof. □

Proposition 4.11. *Assume that there exists an energy-preserving code on the division K-algebra $A = (a, b, u, L/K, \sigma, \tau)$ with $d_{L/K}\Delta_\xi < 10000$. Then we have $256 \leq d_{L/K} < 2500$, and L is one of the three following extensions:*

$$K(\sqrt{2}, \sqrt{5}), K(\sqrt{5}, \sqrt{7}), K(\sqrt{3}, \sqrt{13}),$$

whose relative discriminants are respectively equal to $400, 1125$ *and* 1521.

Proof. By the previous lemma, at least two elements among a, b and abu^τ do not lie in $\mathcal{O}_L$. Assume first that $a \notin \mathcal{O}_L$. By examining the multiplication matrix given in Lemma 4.1, we deduce that the ideals $\mathcal{E}_\xi^{(\sigma)}$ and $\mathcal{E}_\xi^{(\sigma\tau)}$ are proper ideals of $\mathcal{O}_K$. Hence $\Delta_\xi^{(\sigma)} \geq 2$ and $\Delta_\xi^{(\sigma\tau)} \geq 2$. If $a \in \mathcal{O}_L$, then $b \notin \mathcal{O}_L$ and $abu^\tau \notin \mathcal{O}_L$ and we get $\Delta_\xi^{(\tau)} \geq 2$ and $\Delta_\xi^{(\sigma\tau)} \geq 2$ in a similar way. In both cases, we then obtain $\Delta_\xi \geq 4$, and thus $d_{L/K} < 2500$. The lower bound follows from Corollary 2.24.

Let us prove the second part of the proposition. Replacing d' by $\dfrac{dd'}{4}$ if necessary, one may assume that d' is odd. Assume first that d is even. Then $2^4 \mid d_{L/K}$ by Proposition 4.5. Since A is a division K-algebra, d or d' is divisible by a prime $p \equiv 1[4]$, and thus $p^2 \mid d_{L/K}$ by the same proposition. If d or d' were divisible by an odd prime number $\ell \neq p$, we would have in the same way $\ell^2 \mid d_{L/K}$ and thus

$$d_{L/K} \geq 2^4 p^2 \ell^2 \geq 2^4 5^2 3^2 > 2500,$$

hence a contradiction. Thus p is the only odd prime divisor of d and d'. It follows easily that $L = K(\sqrt{2}, \sqrt{p})$. The upper bound on $d_{L/K}$ immediately implies that $p = 5$. Hence $L = K(\sqrt{2}, \sqrt{5})$ and $d_{L/K} = 400$ by Example 4.6.

Assume now that d is odd. Let $p \equiv 1[4]$ be a prime number dividing d or d'. We may assume without loss of generality that $p \mid d$ and $p \nmid d'$. Since d' is an odd positive integer, it has another odd prime divisor

ℓ. Assume that d or d' is divisible by a prime number $q \neq p, \ell$. Since $q \neq \ell$, one of them is necessarily ≥ 5. Since $p \geq 5$, we get

$$d_{L/K} \geq p^2 q^2 \ell^2 \geq 5^4 3^2 > 2500,$$

which is a contradiction. Thus d and d' are only divisible by p and ℓ, so $L = K(\sqrt{p}, \sqrt{\ell})$ and $d_{L/K} = p^2\ell^2$. Since $\ell \geq 3$, the upper bound on $d_{L/K}$ shows that $p = 5$ or 13. If $p = 5$, we get that $\ell = 3$ or 7. The first possibility has to be discarded since $3^2 5^2 < 256$. Hence $L = K(\sqrt{5}, \sqrt{7})$ and $d_{L/K} = 1125$. If $p = 13$, then necessarily $\ell = 3$. In this case, $L = K(\sqrt{3}, \sqrt{13})$ and $d_{L/K} = 1521$. □

Lemma 4.12. *Let F/K be a quadratic extension such that complex conjugation is a $\mathbb{Q}$-automorphism of F which commutes with* $\mathrm{Gal}(F/K)$. *Assume that there is only one prime ideal of $\mathcal{O}_F$ lying above 2. Let $x \in F^\times, x \notin \mathcal{O}_F$ satisfying $|x|^2 = 1$ and let $\delta \in \mathcal{O}_K$ such that $\delta x \in \mathcal{O}_F$. Then $|\delta|^2 \geq 5$.*

Proof. Write $F_0 = F \cap \mathbb{R} = \mathbb{Q}(\sqrt{\Delta}), \Delta > 0$. Since $x \notin \mathcal{O}_F$, δ is not a unit of $\mathcal{O}_K$, and thus $|\delta|^2 \neq 1$. Moreover, the equation $|\delta|^2 = 3$ has no solution in $\mathcal{O}_K$, so we need to prove that $|\delta|^2 \neq 2, 4$.

Assume to the contrary that $|\delta|^2 = 2$ or 4, and set $y = \delta x \in \mathcal{O}_F$. By assumption, we have $|y|^2 = |\delta|^2$. This rewrites as $N_{F/\mathbb{Q}(\sqrt{\Delta})}(y) = N_{F/\mathbb{Q}(\sqrt{\Delta})}(\delta) = 2$ or 4. In particular, $N_{F/\mathbb{Q}}(y)$ and $N_{F/\mathbb{Q}}(\delta)$ are equal to the same power of 2. Hence the prime ideals of $\mathcal{O}_F$ dividing $\delta\mathcal{O}_F$ and $y\mathcal{O}_F$ all lie above 2. The assumption then implies that $\delta\mathcal{O}_F$ and $y\mathcal{O}_F$ are powers of the same prime ideal, and since they have same absolute norms, we get that $y\mathcal{O}_F = \delta\mathcal{O}_F$. It follows that there exists $v \in \mathcal{O}_F^\times$ such that $y = \delta v$, that is $\delta x = \delta v$. Thus $x = v \in \mathcal{O}_F$, which is a contradiction. □

We are finally ready to prove Theorem 4.3. Assume that there exists an energy-preserving code on the division K-algebra $(a, b, u, L/K, \sigma, \tau)$ with $d_{L/K}\Delta_\xi < 10000$. By Proposition 4.11, we have, up to a change of generators

$$L = K(\sqrt{5}, \sqrt{10}), K(\sqrt{5}, \sqrt{7}), \text{ or } K(\sqrt{13}, \sqrt{39}).$$

In each case, $L = K(\sqrt{p}, \sqrt{\Delta})$, where p is a prime number satisfying $p \equiv 5[8]$, and $\Delta \geq 7$. Notice for later use that there is only one prime ideal lying above 2 in $\mathcal{O}_{K(\sqrt{p})}$. Indeed, 2 is inert in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ by assumption on p, and then totally ramifies in $K(\sqrt{p})/\mathbb{Q}(\sqrt{p})$.

If $\rho \in G$ has order 2, we will denote by z_ρ the element among a, b and abu^τ which belongs to $L^{\langle\rho\rangle}$.

Let $\rho, \rho' \in G$ such that $L^{\langle\rho\rangle} = K(\sqrt{p})$ and $L^{\langle\rho'\rangle} = K(\sqrt{\Delta})$. Assume z_ρ is a unit. Then $z_\rho \in K$ by Lemma 4.9, and thus A is not a division

K-algebra by Lemma 4.10. Hence z_ρ is not a unit and by Lemma 4.12, we get that $\Delta_\xi^{(\rho)} \geq 5$.

If $\Delta = 10$, then $1 - i$ totally ramifies in $L^{\langle\rho'\rangle}/K$, so 2 totally ramifies in $L^{\langle\rho'\rangle}/\mathbb{Q}$, and the same reasoning shows that $\Delta_\xi^{(\rho')} \geq 5$. If $\Delta = 7$ or 39, one may show as above that $z_{\rho'}$ is not a unit, and then $\Delta_\xi^{(\rho')} \geq 2$. In all cases, we then get that

$$d_{L/K}\Delta_\xi \geq d_{L/K}\Delta_\xi^{(\rho)}\Delta_\xi^{(\rho')} \geq 10000,$$

hence a contradiction. This concludes the proof.

Remark 4.13. Similar arguments show that the bound 10000 is also optimal if $K = \mathbb{Q}(j)$.

References

[1] J.-C. Belfiore, G. Rekaya, and E. Viterbo. The Golden code: a 2×2 full-rate space-time code with nonvanishing determinants. *IEEE Trans. Inform. Theory*, 51(4):1432–1436, 2005.

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

[3] G. Berhuy and F. Oggier. On the existence of perfect space-time codes. *IEEE Transactions on Information Theory*, 55(5):2078 – 2082, 2009.

[4] P. Elia, B. A. Sethuraman, and P. V. Kumar. Perfect space-time codes for any number of antennas. *IEEE Trans. Inform. Theory*, 53(11):3853–3868, 2007.

[5] Jr. Forney, G., R. Gallager, G. Lang, F. Longstaff, and S. Qureshi. Efficient modulation for band-limited channels. *Selected Areas in Communications, IEEE Journal on*, 2(5):632 – 647, sep. 1984.

[6] J.-C. Guey, M.P. Fitz, M.R. Bell, and W.-Y. Kuo. Signal design for transmitter diversity wireless communication systems over rayleigh fading channels. *Communications, IEEE Transactions on*, 47(4):527 –537, apr. 1999.

[7] J. G. Huard, B. K. Spearman, and K. S. Williams. Integral bases for quartic fields with quadratic subfields. *J. Number Theory*, 51(1):87–102, 1995.

[8] F. Oggier. On the optimality of the golden code. In *IEEE Information Theory Workshop (ITW'06)*, 2006.

[9] F. Oggier, J.-C. Belfiore, and E. Viterbo. Cyclic division algebras: A tool for space-time coding. *Found. Trends Commun. Inf. Theory*, 4(1):1–95, 2007.

[10] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo. Perfect space-time block codes. *IEEE Trans. Inform. Theory*, 52(9):3885–3902, 2006.

[11] R.S. Pierce. *Associative Algebras*. Springer Verlag, 1982.

[12] W. Scharlau. *Quadratic and Hermitian Forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[13] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar. Full-diversity, high-rate space-time block codes from division algebras. *IEEE Trans. Inform. Theory*, 49(10):2596–2616, 2003. Special issue on space-time transmission, reception, coding and signal processing.

[14] V. Shashidhar, B. Sundar Rajan, and B. A. Sethuraman. Information-lossless space-time block codes from crossed-product algebras. *IEEE Trans. Inform. Theory*, 52(9):3913–3935, 2006.
[15] V. Tarokh, H. Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Inform. Theory*, 45:1456–1467, 1999.
[16] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communication: performance criterion and code construction. *IEEE Trans. Inform. Theory*, 44(2):744–765, 1998.
[17] The PARI Group, Bordeaux. *PARI/GP, version* `2.3.3`, 2005. available from `http://pari.math.u-bordeaux.fr/`.

Grégory Berhuy
Université Joseph Fourier
Institut Fourier
100 rue des Maths, BP 62
F-38402 Saint Martin d'Hères

Email: berhuy@ujf-grenoble.fr

Richard Slessor
University of Southampton
School of Mathematics
Highfield
SO17 1BJ Southampton
United Kingdom

Email: R.Slessor@soton.ac.uk