

Natural orders for asymmetric space–time coding: minimizing the discriminant

Amaro Barreal ·
Capi Corrales Rodríguez ·
Camilla Hollanti

the date of receipt and acceptance should be inserted later

Abstract Algebraic space–time coding — a powerful technique developed in the context of multiple-input multiple-output (MIMO) wireless communications — has profited tremendously from tools from Class Field Theory and, more concretely, the theory of central simple algebras and their orders. During the last decade, the study of space–time codes for practical applications, and more recently for future generation (5G+) wireless systems, has provided a practical motivation for the consideration of many interesting mathematical problems. One such problem is the explicit computation of orders of central simple algebras with small discriminants. In this article, we consider the most interesting asymmetric MIMO channel setups and, for each treated case, we provide explicit pairs of fields and a corresponding non-norm element giving rise to a cyclic division algebra whose natural order has the minimum possible discriminant.

Keywords Central Simple Algebras · Division Algebras · Discriminant · Natural Orders · MIMO · Space–Time Coding.

1 Introduction

The existing contemporary communications systems can be abstractly characterized by the conceptual seven-layer Open Systems Interconnection model. The lowest (or first) layer, known as the *physical layer*, aims to describe the

A. Barreal
Department of Mathematics and Systems Analysis, Aalto University, Finland
Tel.: +358-50-5935194
E-mail: amaro.barreal@aalto.fi

C. Corrales Rodríguez
Faculty of Mathematical Sciences, Complutense University of Madrid, Spain

C. Hollanti
Department of Mathematics and Systems Analysis, Aalto University, Finland

communication process over an actual physical medium. Due to the increasing demand for flexibility, information exchange nowadays often occurs via antennas at the transmitting and receiving end of a wireless medium, *e.g.*, using mobile phones or tablets for data transmission and reception. An electromagnetic signal transmitted over a wireless channel is however prone to interference, fading, and environmental effects caused by, *e.g.*, surrounding buildings, trees, and vehicles, making reliable wireless communications a challenging technological problem.

With the advances in communications engineering, it was soon noticed that increasing the number of spatially separated transmit and receive antennas, as well as adding redundancy by repeatedly transmitting the same information encoded over multiple time instances¹, can dramatically improve the transmission quality. A code representing both diversity over time and space is thus called a *space–time code*. Let us consider a channel with n_t and n_r antennas at its transmitting and receiving end, respectively, and assume that transmission occurs over T consecutive time instances. If $n_t = n_r$, the channel is called *symmetric*, and otherwise asymmetric, which more precisely typically refers to the case $n_r < n_t$. For the time being, a space–time code \mathcal{X} will just be a finite collection of complex matrices in $\text{Mat}(n_t \times T, \mathbb{C})$. The channel equation in this multiple-input multiple-output (MIMO) setting is given by

$$Y_{n_r \times T} = H_{n_r \times n_t} X_{n_t \times T} + N_{n_r \times T}, \quad (1)$$

where Y is the received matrix, and $X = [x_{ij}]_{i,j} \in \mathcal{X}$ is the *space–time code* matrix. In the above equation, we adopt the Rayleigh fading channel model, *i.e.*, the entries of the random *channel matrix* $H = [h_{ij}]_{i,j}$ are complex variables with identically distributed real and imaginary parts,

$$\Re(h_{ij}), \Im(h_{ij}) \sim \mathcal{N}(0, \sigma_h^2),$$

yielding a Rayleigh distributed envelope

$$|h_{ij}| = \sqrt{\Re(h_{ij})^2 + \Im(h_{ij})^2} \sim \text{Ray}(\sigma_h)$$

with scale parameter σ_h . We assume further that the channel remains static during the entire transmission of the codeword matrix X , and then changes independently of its previous state. The additive noise² is modeled by the *noise matrix* N , whose entries are independent, identically distributed complex Gaussian random variables with zero mean.

Let us briefly discuss what constitutes a "good" code. Consider a space–time code \mathcal{X} , and let X, X' be code matrices ranging over \mathcal{X} . Two basic design criteria can be derived in order to minimize the probability of error [1].

- i) The *diversity gain* of a code is the asymptotic slope of the error probability curve with respect to the signal-to-noise ratio (SNR) in a log – log scale,

¹ 'Time instances' are commonly referred to as *channel uses*.

² The noise is a combination of thermal noise and noise caused by the signal impulse.

and relates to the minimum rank $\text{rank}(X - X')$ over all pairs of distinct code matrices $(X, X') \in \mathcal{X}^2$. The minimum rank of \mathcal{X} should satisfy

$$\min_{X \neq X'} \text{rank}(X - X') = \min\{n_t, T\},$$

in which case \mathcal{X} is called a *full-diversity* code.

- ii) The *coding gain* measures the difference in SNR required for two different codes to achieve the same error probability. For a full-diversity code this is proportional to the determinant

$$\det((X - X')(X - X')^\dagger).$$

We define the *minimum determinant* of a code \mathcal{X} as the infimum

$$\Delta_{\min}(\mathcal{X}) := \inf_{X \neq X'} \det((X - X')(X - X')^\dagger)$$

as the code size increases, $|\mathcal{X}| \rightarrow \infty$. If $\Delta_{\min}(\mathcal{X}) > 0$, the space–time code is said to have the *nonvanishing determinant* property [2]. In other words, a nonvanishing determinant guarantees that the minimum determinant is bounded from below by a positive constant even in the limit, and hence the error probability will not blow up when increasing the code size.

In 2003, the usefulness of central simple algebras to construct space–time codes meeting both of the above criteria was established in [3]; especially of (cyclic) division algebras, for which the property of being division immediately implies full diversity. Thereupon the construction of space–time codes started to rely on cleverly designed algebraic structures, leading to the construction of multiple extraordinary codes, such as the celebrated Golden code [4], or general Perfect codes [5,6]. It was later shown in [2] that in a cyclic division algebra based code, achieving the nonvanishing determinant property can be ensured by restricting the entries of the codewords to certain subrings of the algebra alongside with a smart choice for the base field, and that ensuring nonvanishing determinants is enough to achieve the optimal trade-off between diversity and multiplexing.

Further investigation carried out in [7,8] showed that codes constructed from orders, in particular *maximal orders*, of cyclic division algebras performed exceptionally well. The main observation is that the discriminant of the order is directly related to the offered coding gain, and should be as small as possible in order to maximize the coding gain.

Maximal orders were then the obvious candidates, as they maximize the normalised density of the corresponding lattice and hence also maximize the coding gain. Unfortunately, they are in general very difficult to compute and may result in highly skewed lattices making the bit labeling a delicate problem on its own. Therefore, *natural orders* with a simpler structure have become a more frequent choice as they provide a good compromise between the two common extremes: using maximal orders to optimize coding gain, on the one hand, and restricting to orthogonal lattices to simplify bit labeling, encoding, and decoding, on the other.

However, the current explicit constructions are typically limited to the symmetric case, while the asymmetric case remains largely open. The main goal of this article is to fill this gap, though our interest is not to analyze the performance of explicit codes. Instead, we focus on the algebraic setup and provide lower bounds for the smallest possible discriminants of natural orders for the considered setups, and give explicit field extensions and corresponding cyclic division algebras meeting the lower bounds.

This article is structured as follows. In Section 2 we will shortly introduce MIMO space–time coding and the construction of space–time codes using representations of orders in central simple algebras. Section 3 contains the main results of this article. We will consider the most interesting asymmetric MIMO channel setups and fix $F = \mathbb{Q}$ or $F = \mathbb{Q}(i)$ as the base field to guarantee the nonvanishing determinant property³. For each considered setup (F, n_t, n_r) , we will find an explicit field extension $F \subset L \subset E$ and an explicit L -central cyclic division algebra over E , such that the norm of the discriminant of its natural order is minimal. This will translate into the largest possible determinant (see (5) and [8, 9] for the proof) and thus provide us with the maximal coding gain one can achieve by using a natural order.

2 Space–time codes from orders in central simple algebras

From now on, and for the sake of simplicity, we set the number n_t of transmit antennas equal to the number T of time slots used for transmission and shortly denote $n := n_t = T$. Thus, the considered codewords will be square matrices.

2.1 Space–time lattice codes

Very simplistically defined, a space–time code is a finite set of complex matrices. However, in order to avoid accumulation points at the receiver, in practical implementations it is convenient to impose an additional discrete structure on the code, such as a lattice structure. We define a *space–time code* to be a finite subset of a *lattice*

$$A = \left\{ \sum_{i=1}^k z_i B_i \mid z_i \in \mathbb{Z} \right\} \subset \text{Mat}(n, \mathbb{C}),$$

where $\{B_1, \dots, B_k\} \subset \text{Mat}(n, \mathbb{C})$ is a *lattice basis*. We recall that a lattice in $\text{Mat}(n, \mathbb{C})$ is *full* if $\text{rank}(A) := k = 2n^2$. We call a space–time lattice code *symmetric*, if its underlying lattice is full, and *asymmetric*⁴ otherwise.

³ From a mathematical point of view, any imaginary quadratic number field would give a nonvanishing determinant, but the choice $\mathbb{Q}(i)$ matches with the quadrature amplitude modulation (QAM) commonly used in engineering.

⁴ This definition relates to the fact that a symmetric code carries the maximum amount of information (*i.e.*, dimensions) that can be transmitted over a symmetric channel without causing accumulation points at the receiving end. In an asymmetric channel, a symmetric

Due to linearity, given a lattice $\Lambda \subset \text{Mat}(n, \mathbb{C})$ and $X, X' \in \Lambda$,

$$\Delta_{\min}(\Lambda) := \inf_{X \neq X'} \det((X - X')(X - X')^\dagger) = \inf_{X \in \Lambda \setminus \{0\}} |\det(X)|^2.$$

This implies that any lattice Λ satisfying the nonvanishing determinant property can be scaled so that $\Delta_{\min}(\Lambda)$ achieves any wanted nonzero value. Consequently, a meaningful comparison of different lattices requires some kind of normalization. To this end, consider the Gram matrix of Λ ,

$$G_\Lambda := \left[\Re \left(\text{Tr} \left(B_i B_j^\dagger \right) \right) \right]_{1 \leq i, j \leq k},$$

where Tr denotes the matrix trace. The volume $\nu(\Lambda)$ of Λ is related to the Gram matrix as $\nu(\Lambda)^2 = \det(G_\Lambda)$.

- i) The *normalized minimum determinant* [8] of Λ is the minimum determinant of Λ after scaling it to have a unit size fundamental parallelopete, that is,

$$\delta(\Lambda) = \frac{\Delta_{\min}(\Lambda)}{\nu(\Lambda)^{\frac{n}{k}}}.$$

- ii) The *normalized density* [8] of Λ is

$$\mu(\Lambda) = \frac{\Delta_{\min}(\Lambda)^{\frac{k}{n}}}{\nu(\Lambda)}. \quad (2)$$

We get the immediate relation $\delta(\Lambda) = \mu(\Lambda)^{\frac{n}{k}}$, from which it follows that in order to maximize the coding gain it suffices to maximize the density of the lattice. Maximizing the density, for its part, translates into a certain *discriminant minimization problem* [8, 9], as we shall see in Section 2.3 (cf. (5)). This observation is crucial and will be the main motivation underlying Section 3.

2.2 Central simple algebras and orders

We recall that a finite dimensional algebra over a number field L is an *L-central simple algebra*, if its center is precisely L and it has no nontrivial ideals. An algebra is said to be *division* if all of its nonzero elements have a multiplicative inverse. By [3, Prop. 1], as long as the underlying algebraic structure of a space–time code is a division algebra, the full-diversity property of the code will be guaranteed. It turns out that if L is an algebraic number field, then every L -central simple algebra is a *cyclic algebra* [10, Thm. 32.20].

code will result in accumulation points, and hence asymmetric codes, *i.e.*, non-full lattices are called for. See [9] for more details.

Let E/L be a cyclic extension of number fields of degree n with respective rings of integers \mathcal{O}_E and \mathcal{O}_L , and cyclic Galois group $\text{Gal}(E/L) = \langle \sigma \rangle$. We fix a nonzero element $\gamma \in L^\times$ and consider the right E -vector space

$$\mathcal{C} := (E/L, \sigma, \gamma) = \bigoplus_{i=0}^{n-1} u^i E,$$

with left multiplication defined by $xu = u\sigma(x)$ for all $x \in E$, and $u^n = \gamma$. The triple \mathcal{C} is referred to as a *cyclic algebra* of *index* n .

The obvious choice of lattices in \mathcal{C} will be its *orders*. We recall that if $R \subset L$ is a Dedekind ring, an R -order in \mathcal{C} is a subring $\mathcal{O} \subset \mathcal{C}$ which shares the same identity as \mathcal{C} , is a finitely generated R -module, and generates \mathcal{C} as a linear space over L . Furthermore, an order is *maximal* if it not properly contained in any other R -order of \mathcal{C} . Of special interest in this article is the \mathcal{O}_L -module

$$\mathcal{O}_{\text{nat}} := \bigoplus_{i=0}^{n-1} u^i \mathcal{O}_E,$$

which we refer to as the *natural order* of \mathcal{C} .

Throughout the paper, we will denote the relative field norm map of the extension E/L by $\text{Nm}_{E/L}$ and the absolute norm map by $\text{Nm}_E = \text{Nm}_{E/\mathbb{Q}}$. The restriction of this map to orders may be specified in the notation as $\text{Nm}_{\mathcal{O}_E/\mathcal{O}_L}$ and $\text{Nm}_{\mathcal{O}_E} = \text{Nm}_{\mathcal{O}_E/\mathbb{Z}}$.

If the element γ fails to be an algebraic integer, then \mathcal{O}_{nat} will not be closed under multiplication. Furthermore, a necessary and sufficient condition for an index- n cyclic algebra $(E/L, \sigma, \gamma)$ to be division is that

$$\gamma^{n/p} \notin \text{Nm}_{E/L}(E^\times) \quad (3)$$

for all primes $p \mid n$. This is a simple extension of a well-known result due to A. Albert, for more details and a proof see [8, Prop. 3.6]. In what follows we will refer to such a non-zero element $\gamma \in \mathcal{O}_L$ as a *non-norm element* for E/L .

Remark 1 We recall that given a Dedekind ring $R \subset L$ and an R -order \mathcal{O} with basis $\{x_1, \dots, x_n^2\}$ over R , the R -discriminant of \mathcal{O} is the ideal

$$\text{disc}(\mathcal{O}/R) = \left(\det \left(\text{tr}_{\mathcal{C}/L}(x_i x_j)_{i,j=1}^n \right) \right),$$

where $\text{tr}(\cdot)$ denotes the reduced trace, which will be defined in (4).

While the ring of algebraic integers is the unique maximal order in an algebraic number field, an L -central simple division algebra may contain several maximal orders. They all share the same discriminant [10, Thm. 25.3], known as the discriminant $d_{\mathcal{C}}$ of the algebra \mathcal{C} . Given two \mathcal{O}_L -orders Γ_1, Γ_2 , it is clear that if $\Gamma_1 \subseteq \Gamma_2$, then $\text{disc}(\Gamma_2/\mathcal{O}_L) \mid \text{disc}(\Gamma_1/\mathcal{O}_L)$. Consequently, $d_{\mathcal{C}} \mid \text{disc}(\Gamma/\mathcal{O}_L)$ for every \mathcal{O}_L -order Γ in \mathcal{C} , and the ideal norm $\text{Nm}_{\mathcal{O}_L}(d_{\mathcal{C}})$ is the smallest possible among all \mathcal{O}_L -orders of \mathcal{C} .

2.3 Algebraic space–time codes from representations of orders

Let $\mathcal{C} = (E/L, \sigma, \gamma)$ be a cyclic division algebra of index n . We fix compatible embeddings of L and E into \mathbb{C} , and identify L and E with their images under these embeddings. The E -linear transformation of \mathcal{C} given by left multiplication by an element $c \in \mathcal{C}$ results in an L -algebra homomorphism $\rho : \mathcal{C} \rightarrow \text{Mat}(n, E)$, to which we refer to as the *maximal representation*. An element $c = c_0 + uc_1 + \cdots + u^{n-1}c_{n-1} \in \mathcal{C}$ can be identified via ρ with the matrix

$$\rho(c) = \begin{bmatrix} c_0 & \gamma\sigma(c_{n-1}) & \gamma\sigma^2(c_{n-2}) & \cdots & \gamma\sigma^{n-1}(c_1) \\ c_1 & \sigma(c_0) & \gamma\sigma^2(c_{n-1}) & \cdots & \gamma\sigma^{n-1}(c_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & \sigma(c_{n-2}) & \sigma^2(c_{n-3}) & \cdots & \sigma^{n-1}(c_0) \end{bmatrix}. \quad (4)$$

The determinant $\text{nr}_{\mathcal{C}/L}(c) := \det(\rho(c))$ and trace $\text{tr}_{\mathcal{C}/L}(c) := \text{Tr}(\rho(c))$ define the *reduced norm* and *reduced trace* of $c \in \mathcal{C}$, respectively. We may shortly denote $\text{nr} = \text{nr}_{\mathcal{C}/L}$ and $\text{tr} = \text{tr}_{\mathcal{C}/L}$, when there is no danger of confusion.

Next, given an order \mathcal{O} in \mathcal{C} , we may use the maximal representation to define an injective map $\rho : \mathcal{O} \hookrightarrow \text{Mat}(n, E) \subset \text{Mat}(n, \mathbb{C})$. If the center L of the algebra is quadratic imaginary and \mathcal{O} admits an \mathcal{O}_L basis, then $\rho(\mathcal{O})$ is a lattice, and any finite subset \mathcal{X} of $\rho(\mathcal{O})$ will be a space–time lattice code, in the literature often referred to as *algebraic space–time code*.

Remark 2 Due to the algebra being division, the above matrices will be invertible, and hence any algebraic space–time code constructed in this way will have full diversity. Moreover, if $c \in \mathcal{O} \setminus \{0\}$, we have $\text{nr}(c) \in \mathcal{O}_L \setminus \{0\}$ [10, Thm. 10.1], guaranteeing nonvanishing determinants for $L = \mathbb{Q}$ or quadratic imaginary.

We now relate the minimum determinant of a code to the density of the underlying lattice $\rho(\mathcal{O})$, which is the main motivation for choosing orders with small discriminant. If the center L of the cyclic algebra is quadratic imaginary and the considered order \mathcal{O} admits an \mathcal{O}_L -basis, the volume $\nu(\rho(\mathcal{O}))$ of the lattice relates to the discriminant of the order as [8]

$$\nu(\rho(\mathcal{O})) = c(L, n) |\text{disc}(\mathcal{O}/\mathcal{O}_L)|, \quad (5)$$

where $c(L, n)$ is a constant which depends on the center and $[E : L]$. Thus, for fixed minimum determinant, the density of the code (cf. (2)) – and consequently the coding gain – is maximized by minimizing the discriminant of the order.

Example 1 Let E/L be a quadratic real extension of number fields with Galois group $\text{Gal}(E/L) = \langle \sigma \rangle$. Let L be of class number 1 and $\mathcal{O}_L, \mathcal{O}_E = \mathcal{O}_L[\omega]$ the respective rings of integers. We choose $\gamma \in \mathcal{O}_L \setminus \{0\}$ such that $\gamma \notin \text{Nm}_{E/L}(E^\times)$, and define the cyclic division algebra

$$\mathcal{C} = (E/L, \sigma, \gamma) = E \oplus uE,$$

where $u^2 = \gamma$. We consider the natural order \mathcal{O}_{nat} of \mathcal{C} and construct an algebraic space–time code as a finite subset

$$\mathcal{X} \subset \left\{ \begin{bmatrix} x_1 + x_2\omega & \gamma(x_3 + x_4\sigma(\omega)) \\ x_3 + x_4\omega & x_1 + x_2\sigma(\omega) \end{bmatrix} \middle| x_i \in \mathcal{O}_L \right\} = \rho(\mathcal{O}_{\text{nat}}).$$

The choice of fields $(E, L) = (\mathbb{Q}(i, \sqrt{5}), \mathbb{Q}(i))$ and element $\gamma = i$ gives rise to the Golden algebra and to the well-known *Golden code* [5].

The above example relates to the symmetric scenario, *i.e.*, it has an underlying lattice that is full. Full lattices can be efficiently decoded when $n_r = n_t$, and the same lattice codes can also be employed when $n_r > n_t$. There is no simple optimal decoding method for symmetric codes, however, when $n_r < n_t$ ⁵.

Building upon symmetric codes, we now briefly introduce *block diagonal asymmetric* space–time codes [9], better suited for the asymmetric scenario. Let $F \subset L \subset E$ be a tower of field extensions with extension degrees $[E : L] = n_r$, $[L : F] = n$, and $[E : F] = n_t = n_r n$, and with Galois groups $\text{Gal}(E/F) = \langle \tau \rangle$ and $\text{Gal}(E/L) = \langle \sigma \rangle = \langle \tau^n \rangle$. We fix a non-norm element $\gamma \in \mathcal{O}_L \setminus \{0\}$, and consider the cyclic division algebra

$$\mathcal{C} = (E/L, \sigma, \gamma) = \bigoplus_{i=0}^{n_r-1} u^i E.$$

Given any order \mathcal{O} in \mathcal{C} , we identify each element $c \in \mathcal{O}$ with its maximal representation $\rho(c)$ and construct the following infinite block-diagonal lattice achieving the nonvanishing determinant property, provided that the base field F is either \mathbb{Q} or quadratic imaginary [9]:

$$\mathcal{L}(\mathcal{O}) = \left\{ \begin{bmatrix} \rho(c) & 0 & \cdots & 0 \\ 0 & \tau(\rho(c)) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \tau^{n-1}(\rho(c)) \end{bmatrix} \in \text{Mat}(n_t, \mathbb{C}) \middle| c \in \mathcal{O} \right\}.$$

Remark 3 The *code rate* [9] of a space–time code carved out from $\mathcal{L}(\mathcal{O})$ in (complex) symbols per channel use is

$$R = \begin{cases} nn_r^2/nn_r = n_r & \text{if } F \text{ is quadratic imaginary,} \\ nn_r^2/2nn_r = n_r/2 & \text{if } F = \mathbb{Q}. \end{cases}$$

We point out that n_r is the maximum code rate that allows for avoiding accumulation points at the receiving end with n_r receive antennas.

In summary, in order to construct an algebraic space–time code, we first choose a central simple algebra over a suitable base field and then look for a dense lattice in it. This amounts to selecting an adequate order in the algebra. As motivated earlier, we will opt for natural orders as a compromise between simplicity and maximal coding gain.

⁵ Having too few receive antennas will cause the lattice to collapse resulting in accumulation points, since the received signal now has dimension $2n_r n_t < 2n_t^2$. Hence, partial brute-force decoding of high complexity has to be carried out.

3 Natural orders with minimal discriminant

As an illustration of the general algebraic setup, consider the tower of extensions depicted in Figure 1. In order to get the nonvanishing determinant

$$\mathcal{C} = (E/L, \sigma, \gamma) = \bigoplus_{i=0}^{n_r-1} u^i E$$

$$\begin{array}{c} | \\ n_r \\ E \\ | \\ n_r \\ L \\ | \\ n \\ F = \mathbb{Q}(\sqrt{d}) \end{array}$$

Fig. 1 Tower of Field Extensions.

property, we fix the base field $F \in \{\mathbb{Q}, \mathbb{Q}(i)\}$, as well as the extension degrees $n = [L : F]$ and $n_r = [E : L]$. With these parameters fixed, our goal is to find an explicit field extension E/L with $\text{Gal}(E/L) = \langle \sigma \rangle$ and a non-norm element $\gamma \in \mathcal{O}_L \setminus \{0\}$ such that E/F is a cyclic extension, $(E/L, \sigma, \gamma)$ is a cyclic division algebra, and the absolute value $|\text{Nm}_{\mathcal{O}_F}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_F))|$ is the minimum possible among all cyclic division algebras satisfying the fixed conditions. Our constructions rely on some key properties of cyclic division algebras and their orders that we will next present as lemmata.

Lemma 1 [8, Lem. 5.4] and [9, Prop. 5.3] *Let $(E/L, \sigma, \gamma)$ be a cyclic division algebra of index n_r and $\gamma \in \mathcal{O}_L \setminus \{0\}$ a non-norm element. We have*

$$\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_L) = \text{disc}(E/L)^{n_r} \cdot \gamma^{n_r(n_r-1)},$$

with $\text{disc}(E/L)$ the \mathcal{O}_L -discriminant of \mathcal{O}_E . Hence, if $F \subset L$, then by the discriminant tower formula

$$\begin{aligned} \text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_F) &= \text{Nm}_{L/F}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_L)) \cdot \text{disc}(L/F)^{n_r^2} \\ &= \text{disc}(E/F)^{n_r} \cdot \text{Nm}_{L/F}^{n_r(n_r-1)}(\gamma). \end{aligned} \tag{6}$$

Lemma 2 [11, Thm. 2.4.26] *Let L be a number field and $(\mathfrak{p}_1, \mathfrak{p}_2)$ a pair of norm-wise smallest prime ideals in \mathcal{O}_L . If we do not allow ramification on infinite primes, then the smallest possible discriminant of all central division algebras over L of index n_r is*

$$(\mathfrak{p}_1 \mathfrak{p}_2)^{n_r(n_r-1)}. \tag{7}$$

We have arrived at the following *optimization problem*: in order to minimize the discriminant $\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_F)$ of a natural order of an index- n_r L -central division algebra over a fixed base field $F \subset L$, we must jointly minimize the relative discriminant of the extension E/F and the relative norm of the non-norm element γ .

Our findings are summarized in the following table and will be proved, row by row, in the subsequent five theorems. Here, α is a root of the polynomial $X^2 + X - i$ and β denotes a root of the polynomial $X^3 - (1+i)X^2 + 5iX - (1+4i)$.

F	n	n_r	n_t	rate	$\text{Nm}_{\mathcal{O}_F}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_F))$	L	E	γ
\mathbb{Q}	1	2	2	1	$2^2 \cdot 3^2$	\mathbb{Q}	$\mathbb{Q}(i\sqrt{3})$	2
\mathbb{Q}	2	2	4	1	$2^4 \cdot 5^6$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\zeta_5)$	-4
$\mathbb{Q}(i)$	2	2	4	2	$2^4 \cdot 17^3$	$\mathbb{Q}(i, \alpha)$	$\mathbb{Q}(i, \sqrt{\alpha})$	$1 + i$
$\mathbb{Q}(i)$	2	3	6	3	$3^{18} \cdot 13^{12}$	$\mathbb{Q}(i, i\sqrt{3})$	$\mathbb{Q}(i, i\sqrt{3}, \beta)$	$\frac{1+i\sqrt{3}}{2}$
$\mathbb{Q}(i)$	3	2	6	2	$2^6 \cdot 3^{12} \cdot 13^8$	$\mathbb{Q}(i, \beta)$	$\mathbb{Q}(i, i\sqrt{3}, \beta)$	$1 + i$

Table 1 Main results summarized.

Remark 4 It is often preferred that $|\gamma| = 1$ for balanced transmission power. However, there are good ‘remedy’ techniques for the case when $|\gamma| > 1$, see e.g., [6, 12].

3.1 General Strategy

We briefly elaborate on the three-step strategy that we will follow to prove each of the theorems. Let F , n and n_r be fixed.

Step 1. We start by finding an explicit cyclic extension E/L of degree n_r , $F \subset L$, such that $[L : F] = n$ and E/F is cyclic with $|\text{Nm}_{\mathcal{O}_F}(\text{disc}(E/F))|$ smallest possible. In the cases where $F = \mathbb{Q}$, our extension E/F will either be quadratic or quartic cyclic, and we simply use well-known formulas for computing $\text{disc}(E/\mathbb{Q})$. For $F = \mathbb{Q}(i)$ we resort to the following results from Class Field Theory (all the details can be found in [13]).

Let $F \subset E$ be an abelian extension of number fields. For each prime \mathfrak{p} of F that is unramified in E there is a unique element $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(E/F)$ that induces the Frobenius automorphism $x \mapsto x^{\#k_{\mathfrak{p}}}$ on the residue field extensions $k_{\mathfrak{p}} \subset k_{\mathfrak{q}}$ for the primes \mathfrak{q} in E extending \mathfrak{p} . The order of $\text{Frob}_{\mathfrak{p}}$ in $\text{Gal}(E/F)$ equals the residue class degree $[k_{\mathfrak{q}} : k_{\mathfrak{p}}]$, and the subgroup $\langle \text{Frob}_{\mathfrak{p}} \rangle$ of $\text{Gal}(E/F)$ is the decomposition group of \mathfrak{p} . The *Artin map* for E/F is the homomorphism

$$\begin{aligned} \psi_{E/F} : I_F(\text{disc}(E/F)) &\longrightarrow \text{Gal}(E/F) \\ \mathfrak{p} &\longmapsto \text{Frob}_{\mathfrak{p}} \end{aligned}$$

on the group $I_F(\text{disc}(E/F))$ of fractional \mathcal{O}_F -ideals generated by the prime ideals \mathfrak{p} of F that do not divide the discriminant $\text{disc}(E/F)$. These are unramified in E . For an ideal \mathfrak{a} in $I_F(\text{disc}(E/F))$ we call $\psi_{E/F}(\mathfrak{a})$ the *Artin symbol* of \mathfrak{a} in $\text{Gal}(E/F)$.

The *Artin Reciprocity Law* states that if $F \subset E$ is an abelian extension, then there exists a nonzero ideal $\mathfrak{m}_0 \mathcal{O}_L$ such that the kernel of the Artin map $\psi_{E/L}$ contains all principal \mathcal{O}_L -ideals $x \mathcal{O}_L$ with x totally positive and $x \equiv 1 \pmod{\mathfrak{m}_0}$. We define a *modulus* of L to be a formal product $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$, where \mathfrak{m}_0 is a nonzero \mathcal{O}_E -ideal and \mathfrak{m}_∞ is a subset of the real primes of L . We write $x \equiv 1 \pmod{\times \mathfrak{m}}$ if $\text{ord}_{\mathfrak{p}}(x-1) \geq \text{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$ at the primes \mathfrak{p} dividing the finite part \mathfrak{m}_0 and x is positive at the real primes in the infinite part \mathfrak{m}_∞ . In the language of moduli, Artin's Reciprocity Law asserts that there exists a modulus \mathfrak{m} such that the kernel of the Artin map contains the *ray group* $R_{\mathfrak{m}}$ of principal \mathcal{O}_L -ideals $x \mathcal{O}_L$ generated by elements $x \equiv 1 \pmod{\times \mathfrak{m}}$. The set of these *admissible* moduli for L/E consists of the multiples of some minimal modulus $\mathfrak{f}_{E/L}$, the *conductor* of L/E . The primes occurring in $\mathfrak{f}_{E/L}$ are the primes of L , both finite and infinite, that ramify in E .

If $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ is an admissible modulus for L/E , and $I_{\mathfrak{m}}$ denotes the group of fractional \mathcal{O}_L -ideals generated by the primes \mathfrak{p} coprime to \mathfrak{m}_0 , then the Artin map induces a surjective homomorphism

$$\begin{aligned} \psi_{E/L} : \text{Cl}_{\mathfrak{m}} = I_{\mathfrak{m}}/R_{\mathfrak{m}} &\longrightarrow \text{Gal}(E/L), \\ [\mathfrak{p}] &\longmapsto \text{Frob}_{\mathfrak{p}}, \end{aligned} \quad (8)$$

where $\text{Cl}_{\mathfrak{m}}$ is the *ray class group*, and $\ker(\psi_{E/F}) = A_{\mathfrak{m}}/R_{\mathfrak{m}}$ with

$$A_{\mathfrak{m}} = \text{Nm}_{E/F}(I_{\mathfrak{m}} \mathcal{O}_F) \cdot R_{\mathfrak{m}}. \quad (9)$$

The *existence theorem* from Class Field Theory states that for every modulus \mathfrak{m} of F , there exists an extension $F \subset H_{\mathfrak{m}}$ for which the map in (8) is an isomorphism. Inside some fixed algebraic closure of F , the *ray class field* $H_{\mathfrak{m}}$ is uniquely determined as the maximal abelian extension of F in which all the primes in the ray group $R_{\mathfrak{m}}$ split completely. Conversely, if $F \subset E$ is abelian then $E \subset H_{\mathfrak{m}}$ whenever \mathfrak{m} is an admissible modulus for $F \subset E$. For $E = H_{\mathfrak{m}}$, we have $A_{\mathfrak{m}} = R_{\mathfrak{m}}$ in (9) and an *Artin isomorphism*

$$\text{Cl}_{\mathfrak{m}} \simeq \text{Gal}(H_{\mathfrak{m}}/F). \quad (10)$$

For all \mathfrak{m} , the ray group $R_{\mathfrak{m}}$ is contained in the subgroup $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ of principal ideals in $I_{\mathfrak{m}}$, with $I_{\mathfrak{m}}/P_{\mathfrak{m}} = \text{Cl}_F$, the class group of F . There is a natural exact sequence

$$\mathcal{O}_F^{\times} \longrightarrow (\mathcal{O}_F/\mathfrak{m})^{\times} \longrightarrow \text{Cl}_{\mathfrak{m}} \longrightarrow \text{Cl}_F \longrightarrow 0, \quad (11)$$

and the residue class in $\text{Cl}_{\mathfrak{m}}$ of $x \in \mathcal{O}_L$ coprime to \mathfrak{m}_0 in the finite group $(\mathcal{O}_F/\mathfrak{m})^{\times} = (\mathcal{O}_F/\mathfrak{m})^{\times} \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \langle -1 \rangle$ consists of its ordinary residue class modulo \mathfrak{m}_0 and the signs of its images under the real primes $\mathfrak{p} | \mathfrak{m}_\infty$.

Finally, we compute the discriminant $\text{disc}(E/F)$ using Hasse's conductor-discriminant formula

$$\text{disc}(E/F) = \prod_{\chi: I_{\mathfrak{m}}/A_{\mathfrak{m}} \rightarrow \mathbb{C}^{\times}} \mathfrak{f}(\chi)_0, \quad (12)$$

where χ ranges over the characters of the finite group $I_{\mathfrak{m}}/A_{\mathfrak{m}} \simeq \text{Gal}(E/F)$ and $\mathfrak{f}(\chi)_0$ denotes the finite part of the conductor $\mathfrak{f}(\chi)$ of the ideal group A_{χ} modulo \mathfrak{m} satisfying $A_{\chi}/A_{\mathfrak{m}} = \ker \chi$.

Step 2. Unfortunately, having $|\mathrm{Nm}_{\mathcal{O}_F}(\mathrm{disc}(E/F))|$ smallest possible is not sufficient for $|\mathrm{Nm}_{\mathcal{O}_F}(\mathrm{disc}(\mathcal{O}_{\mathrm{nat}}/\mathcal{O}_F))|$ to be smallest possible as well. Using (6) and (7) we can derive a positive lower bound on the size of a non-norm element $\gamma \in \mathcal{O}_L$ as

$$|\mathrm{Nm}_{\mathcal{O}_L}(\gamma^{n_r-1})| \geq \frac{|\mathrm{Nm}_{\mathcal{O}_L}(\mathfrak{p}_1\mathfrak{p}_2)^{n_r-1}|}{|\mathrm{Nm}_{\mathcal{O}_L}(\mathrm{disc}(E/L))|} =: \lambda_{E,L} \in \mathbb{N}, \quad (13)$$

where $(\mathfrak{p}_1, \mathfrak{p}_2)$ is a pair of norm-wise smallest prime ideals in \mathcal{O}_L . If $\mathrm{disc}(E/L)$ is minimal and $\lambda_{E,L} > 1$, as will be the case in Theorems 1 and 2 below, we need to balance the size of $\mathrm{disc}(E/F)$ and γ in order to achieve minimality of $|\mathrm{Nm}_{\mathcal{O}_F}(\mathrm{disc}(\mathcal{O}_{\mathrm{nat}}/\mathcal{O}_F))|$.

In the last three theorems, we will then proceed as follows. Given two cyclic algebras $(E/L, \sigma, \gamma)$ and $(E'/L', \sigma', \gamma')$ of index n_r , where $\langle \sigma \rangle = \mathrm{Gal}(E/L)$, $\langle \sigma' \rangle = \mathrm{Gal}(E'/L')$ and such that $\mathbb{Q}(i) \subset L, L'$, we have by (6), since norms in $\mathbb{Q}(i)$ are positive,

$$\begin{aligned} \mathrm{Nm}_{\mathbb{Z}[i]}(\mathrm{disc}(\mathcal{O}_{\mathrm{nat}}/\mathbb{Z}[i])) &\leq \mathrm{Nm}_{\mathbb{Z}[i]}(\mathrm{disc}(\mathcal{O}'_{\mathrm{nat}}/\mathbb{Z}[i])) \\ &\Leftrightarrow \\ D_{E/L}(\gamma) &\leq D_{E'/L'}(\gamma'), \end{aligned} \quad (14)$$

with

$$D_{E/L}(\gamma) := \mathrm{Nm}_{\mathbb{Z}[i]}(\mathrm{disc}(E/\mathbb{Q}(i))) \cdot \mathrm{Nm}_{\mathcal{O}_L}(\gamma)^{n_r-1}. \quad (15)$$

Our strategy will be to fix a non-norm element $\gamma \in \mathcal{O}_L$ of smallest possible norm, compute $D_{E/L}(\gamma)$ and, along the lines of Step 1, compare $D_{E/L}(\gamma)$ with $D_{E'/L'}(\gamma')$, where E'/L' runs over all degree- n_r cyclic field extensions such that $\mathbb{Q}(i) \subset L'$ and $\gamma' \in \mathcal{O}_L$ is a non-norm element for E'/L' of smallest possible norm.

Step 3. If $\mathrm{disc}(E/L)$ is smallest possible and $\lambda_{E,L} < 1$, as will be the case in Theorems 3, 4 and 5, the optimal situation would be to be able to choose a non-norm element γ which is a unit, $\gamma \in \mathcal{O}_L^\times$. Hasse's Norm Theorem will help us decide whether such an element exists and, if it does, how to find it. We use the following strategy from the theory of local fields to compute $\mathrm{Nm}_{K/k}(K^\times)$ when K/k is an extension of non-Archimedean local fields (all the details can be found in [14, Chp. 7]).

Let k be a field, complete under a discrete valuation v_k . Let A_k be its valuation ring with maximal ideal \mathfrak{m}_k , generated by a local uniformizing parameter π_k with $v_k(\pi_k) = 1$, and $\bar{k} = A_k/\mathfrak{m}_k$ the residue field, where $|\bar{k}| = q_k$ is a power of a rational prime p . Denote by $U_k = A_k - \mathfrak{m}_k$ the multiplicative group of invertible elements A_k^\times of A_k , and set $U_k^i = 1 + \mathfrak{m}_k^i$, $i \geq 1$. Then, $U_k = S_k \times U_k^1$, where S_k is a complete set of representatives of \bar{k} , and

$$k^\times = \langle \pi_k \rangle U_k = S_k \times \langle \pi_k \rangle \times U_k^1.$$

As \bar{k}^\times is cyclic of order $q_k - 1$, we may take $S_k = \{0\} \cup \{\zeta_{q_k-1}^i \mid 1 \leq i \leq q_k - 1\}$, where ζ_n denotes a primitive n -th root of unity in \bar{k} .

Let K be finite separable extension of k , A_K the integral closure of A_k in K , and let v_K , \mathfrak{m}_K , π_K , \bar{K} , q_K and U_K^i be defined as above. As usual, we denote the ramification index and residue degree of \mathfrak{m}_K in K/k by $e_{K/k}$ and $f_{K/k}$, respectively. We have $e_{K/k} \cdot f_{K/k} = [K : k]$ and $\pi_K = \pi_K^{e_{K/k}} \times u$ with u a unit, so that $\text{Nm}_{K/k}(\pi_K) = \pi_k^{f_{K/k}}$.

The group $\text{Nm}_{K/k}(U_K)$ is a subgroup of U_k with $[U_k : \text{Nm}_{K/k}(U_K)] = e_{K/k}$, and $\text{Nm}_{K/k}(U_K^1) \subset U_k^1$ with $[U_k^1 : \text{Nm}_{K/k}(U_K^1)]$ a power of p . Consequently, if the extension is unramified, i.e. $e_{K/k} = 1$, then $\text{Nm}_{K/k}(U_K) = U_k$ and every unit is a norm.

Suppose hereinafter that K/k is a totally tamely ramified extension, thus $f_{K/k} = 1$, $(p, e_{K/k}) = 1$, $\bar{K} = \bar{k}$, $q_K = q_k$ and the *local conductor*, i.e., the smallest integer f such that $U_k^f \subset \text{Nm}_{K/k}(K^\times)$, is 1 ([15, Aside 1.9]). Then $\text{Nm}_{K/k}(\zeta_{q_K-1}) = \zeta_{q_k-1}^{[K:k]}$ and $\text{Nm}_{K/k}(U_K^1) = U_k^1$. Consequently,

$$\text{Nm}_{K/k}(K^\times) = \langle \text{Nm}_{K/k}(\pi_K), \zeta_{q_k-1}^{[K:k]} \rangle U_k^1.$$

Since π_K is not a unit, we conclude that in the totally tamely ramified case,

$$U_k \cap \text{Nm}_{K/k}(K^\times) = \langle \zeta_{q_k-1}^{[K:k]} \rangle U_k^1. \quad (16)$$

With the above information at hand, we go back to the extension E/L found in Step 1 with $\lambda_{E,L} < 1$. In order to produce a suitable unit $\gamma \in \mathcal{O}_L^\times$ which is not a local norm at some prime ramifying in the extension, we compute the ramified primes as well as $\langle \zeta_{q_k-1}^{[K:k]} \rangle U_k^1$ in the corresponding local extension K/k . Considering \mathcal{O}_L as a subset of A_k and using Hensel's lemma, we look for a unit in \mathcal{O}_L^\times such that its image in \bar{k} lies outside $\langle \zeta_{q_k-1}^{[K:k]} \rangle$. Unfortunately, if $\mathcal{O}_L^\times \subset \langle \zeta_{q_k-1}^{[K:k]} \rangle U_k^1$, as will be the case in Theorems 3 and 5, a non-norm unit for E/L will not exist. In those cases the sizes of $\text{disc}(E/F)$ and γ in (6) must be balanced using (15) in order to achieve minimality of $|\text{Nm}_{\mathcal{O}_F}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathcal{O}_F))|$.

3.2 Main Results

We are now ready to state and prove the main results of this article.

Theorem 1 *Let $\mathbb{Q} \subset E = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ square-free, and $\text{Gal}(E/L) = \langle \sigma \rangle$. Any cyclic division algebra $(E/\mathbb{Q}, \sigma, \gamma)$ of index 2 satisfies $|\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})| \geq 36$, and equality is achieved for $E = \mathbb{Q}(i\sqrt{3})$, $\gamma = 2$.*

Proof : The proof follows the strategy described above.

Step 1. The smallest possible quadratic discriminant over \mathbb{Q} is $\text{disc}(E/\mathbb{Q}) = 3$, corresponding to the field $E = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\omega)$, ω a primitive cubic root of unity. Let $\text{Gal}(E/\mathbb{Q}) = \langle \sigma \rangle$.

Step 2. A pair of smallest primes in \mathbb{Z} is $(2, 3)$, so that $\lambda_{E,\mathbb{Q}} = \frac{6}{3} > 1$ (cf. (13)). Thus, any non-norm element $\gamma \in \mathbb{Z}$ satisfies $|\gamma| \geq 2$.

To ensure that we can choose $\gamma = 2$, we first show that the equation $x^2 + 3y^2 = 2$ has no solution in \mathbb{Q} . Consequently, $2 \notin \text{Nm}_{E/\mathbb{Q}}(E^\times)$ and $(\mathbb{Q}(i\sqrt{3})/\mathbb{Q}, \sigma, 2)$ is a division algebra with $\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}) = 36$.

Suppose that $(\frac{a}{b})^2 + 3(\frac{c}{d})^2 = 2$, with $a, b, c, d \in \mathbb{Z}$ and such that $(a, b) = (c, d) = 1$. Then,

$$(ad)^2 + 3(bc)^2 = 2(bd)^2. \quad (17)$$

It is easy to deduce from (17) that 3^s , $s \geq 0$, is the largest power of 3 dividing b if and only if it is the largest power of 3 dividing d . If $(3, bd) = 1$, then equation (17) has no solution in \mathbb{Z} , as 2 is not a square mod 3. Set $b = 3^s b'$ and $d = 3^s d'$, with $(3, b'd') = 1$, $s \geq 1$. Substituting into (17) yields

$$(ad')^2 + 3(b'c)^2 = 2 \cdot 3^s (b'd')^2,$$

which is absurd, since $(3, ad') = 1$.

Next, we use (6) to see that for $E' = \mathbb{Q}(\sqrt{d})$ with $d \neq 1, -3$ a square-free integer and $\text{Gal}(E'/\mathbb{Q}) = \langle \sigma' \rangle$, the cyclic division algebra $(E'/\mathbb{Q}, \sigma', \gamma')$ satisfies $|\text{disc}(\mathcal{O}'_{\text{nat}}/\mathbb{Z})| > 36$ for any choice of non-norm element $\gamma' \in \mathbb{Z}$.

- i) If $d \equiv 2, 3 \pmod{4}$, then $|\text{disc}(E'/\mathbb{Q})| = 4|d| \geq 8$, and (6) guarantees that for any $\gamma' \in \mathbb{Z}$, $|\text{disc}(\mathcal{O}'_{\text{nat}}/\mathbb{Z})| \geq 8^2 \gamma'^2 \geq 64$.
- ii) If $d \equiv 1 \pmod{4}$ and $|d| \geq 7$, then $|\text{disc}(E'/\mathbb{Q})| = |d|$ and (6) implies $|\text{disc}(\mathcal{O}'_{\text{nat}}/\mathbb{Z})| \geq 7^2 \gamma'^2 \geq 49$.
- iii) For $d = 5$, we have $\text{disc}(E'/\mathbb{Q}) = 5$ and $\lambda_{E', \mathbb{Q}} = \frac{6}{5} = 2$ (cf. (13)). Using (6) we conclude that for any non-norm element $\gamma' \in \mathbb{Z}$, $\text{disc}(\mathcal{O}'_{\text{nat}}/\mathbb{Z}) \geq 5^2 \cdot 2^2 > 36$.

□

Theorem 2 *Let $\mathbb{Q} \subset L \subset E$ with $[E : \mathbb{Q}] = 4$, $[E : L] = 2$ and $\text{Gal}(E/L) = \langle \sigma \rangle$. If $(E/L, \sigma, \gamma)$ is a cyclic division algebra, then $\text{Nm}_{\mathbb{Z}}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})) \geq 2^4 \cdot 5^6$. Equality is achieved for $L = \mathbb{Q}(\sqrt{5})$, $E = \mathbb{Q}(\zeta_5)$ and $\gamma = -4$, with ζ_5 a primitive 5th root of unity.*

Proof : The fields L and E can be uniquely expressed as $L = \mathbb{Q}(\sqrt{D})$ and $E = \mathbb{Q}\left(\sqrt{A(D + B\sqrt{D})}\right)$, with $A, B, C, D \in \mathbb{Z}$ such that A is square-free and odd, $D = B^2 + C^2$ is square-free, $B, C > 0$ and $(A, D) = 1$ ([16], [17]).

Step 1.

- i) If $D \equiv 0 \pmod{2}$, then $\text{disc}(E/\mathbb{Q}) = 2^8 \cdot A^2 \cdot D^3 \geq 2^{11}$. The lower bound is attained for $D = 2$, $B = C = 1$, and $|A| = 1$. Using (6) we deduce that $|\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})| \geq 2^{22} > 2^4 \cdot 5^6$ for any choice of $\gamma \in \mathcal{O}_L$.
- ii) If $D \equiv B \equiv 1 \pmod{2}$, then $\text{disc}(E/\mathbb{Q}) = 2^6 \cdot A^2 \cdot D^3 \geq 2^6 \cdot 5^3$. This expression attains its minimum value for $D = 5$ and $|A| = B = 1$. Hence, $|\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})| \geq 2^{12} \cdot 5^6 > 2^4 \cdot 5^6$ for any choice of $\gamma \in \mathcal{O}_L$.
- iii) If $D \equiv 1 \pmod{2}$, $B \equiv 0 \pmod{2}$ and $A + B \equiv 3 \pmod{4}$, we have $\text{disc}(E/\mathbb{Q}) = 2^4 \cdot A^2 \cdot D^3 \geq 2^4 \cdot 5^3$. The minimum value is attained for $D = 5$, $B = 2$, and $A = 1$, so that $|\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})| \geq 2^8 \cdot 5^6 > 2^4 \cdot 5^6$ for any choice of $\gamma \in \mathcal{O}_L$.

iv) Finally, if $D \equiv 1 \pmod{2}$, $B \equiv 0 \pmod{2}$, $A + B \equiv 1 \pmod{4}$ and $A \equiv \pm C \pmod{4}$, we have $\text{disc}(E/\mathbb{Q}) = A^2 \cdot D^3 \geq 5^3$. The minimum of this expression is attained for $D = 5$, $B = 2$ and $A = -1$, corresponding to the fields $E = \mathbb{Q}(\zeta_5)$ and $L = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$.

The last case provides us with a field extension $E/L = \mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$ with $\text{disc}(E/L) = 5$ and $\text{disc}(E/\mathbb{Q}) = 5^3$. If we show $|\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z})| = 2^4 \cdot 5^6$ for $\gamma = -4$ a non-norm element, the theorem will be proved.

Step 2. The two smallest prime ideals in \mathcal{O}_L are $\mathfrak{p}_2 = 2\mathcal{O}_L$ and \mathfrak{p}_5 , a factor of $5\mathcal{O}_L = \mathfrak{p}_5\mathfrak{p}'_5$, of respective norms 4 and 5. Hence, $\lambda_{E,L} = 4$, and any suitable non-norm element for E/L will satisfy $|\text{Nm}_{\mathcal{O}_L}(\gamma)| \geq 4$ (cf. (13)). We show that $-4 \notin \text{Nm}_{E/L}(E^\times)$. Since the norm is multiplicative and $4 = \text{Nm}_{E/L}(2)$, it suffices to show that $-1 \notin \text{Nm}_{E/L}(E^\times)$. Suppose that $x \in L$ with $\text{Nm}_{E/L}(x) = -1$. Then $\text{Nm}_{E/\mathbb{Q}}(x) = 1$, and we can write $x = \zeta v$ with ζ a root of unity and $v \in L^\times$ [14, Prop. 6.7]. Consequently, $-1 = \text{Nm}_{E/L}(\zeta) \cdot \text{Nm}_{E/L}(v) = v^2$. But -1 is not a square in L . \square

In the remaining cases, our base field will be $F = \mathbb{Q}(i)$. For each rational prime p , we write $p\mathbb{Z}[i] = \mathfrak{p}_p^2$, $\mathfrak{p}_p\mathfrak{p}'_p$ or $\mathfrak{p}_p = (p)$ for the cases where p is ramified, split or inert in $\mathbb{Z}[i]$, respectively.

Theorem 3 *Let $\mathbb{Q}(i) \subset L \subset E$, with $[E : \mathbb{Q}(i)] = 4$ and $[E : L] = 2$. Let $\text{Gal}(E/L) = \langle \sigma \rangle$. Any cyclic division algebra $(E/L, \sigma, \gamma)$ under these assumptions satisfies $\text{Nm}_{\mathbb{Z}[i]}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i])) \geq 2^4 \cdot 17^6$, with quality attained for $L = \mathbb{Q}(i, \alpha)$, $E = \mathbb{Q}(i, \sqrt{\alpha})$ and $\gamma = 1 + i$, with α a root of $f(X) = X^2 + X - i$.*

Proof :

Step 1. We start by finding the smallest possible discriminant over $\mathbb{Q}(i)$ for cyclic extensions of degree 4. Let E any be any such extension. By the existence theorem of Class Field Theory, we know that E is contained in the ray class field $H_{\mathfrak{m}}$, where \mathfrak{m} is an admissible modulus for the extension $E/\mathbb{Q}(i)$. The smallest ray class field will have conductor $\mathfrak{f} = \mathfrak{f}_{E/\mathbb{Q}(i)}$, which, since $\mathbb{Q}(i)$ is a complex field, will be an ideal of $\mathbb{Z}[i]$.

The restriction of the Artin map (8) to $I_{\mathfrak{f}}$ gives us a canonical isomorphism $\text{Gal}(H_{\mathfrak{f}}/\mathbb{Q}(i)) \simeq I_{\mathfrak{f}}/P_{\mathfrak{f}} = C_{\mathfrak{f}}$ (cf. (10)), which implies $[H_{\mathfrak{f}} : \mathbb{Q}(i)] = |C_{\mathfrak{f}}|$. Furthermore, since the class group $C_{\mathbb{Q}(i)}$ is trivial and $\mathbb{Z}[i]^\times = \langle i \rangle$, by (11) we have the exact sequence

$$0 \rightarrow \langle i \rangle \rightarrow (\mathbb{Z}[i]/\mathfrak{f})^\times \rightarrow C_{\mathfrak{f}} \rightarrow 0.$$

Thus, $C_{\mathfrak{f}} \simeq (\mathbb{Z}[i]/\mathfrak{f})^\times / \text{Im}\langle i \rangle$. The ray class field of conductor 2 is trivial, which is not our case, so \mathfrak{f} does not divide 2. The map $\langle i \rangle \rightarrow (\mathbb{Z}[i]/\mathfrak{f})^\times$ is injective, so that $[H_{\mathfrak{f}} : \mathbb{Q}(i)] = \frac{1}{4} |(\mathbb{Z}[i]/\mathfrak{f})^\times|$. Consequently,

$$4 = [E : \mathbb{Q}(i)] | [H_{\mathfrak{f}} : \mathbb{Q}(i)] \Rightarrow 16 | |(\mathbb{Z}[i]/\mathfrak{f})^\times| = \text{Nm}(\mathfrak{f}) \text{ and } \text{Nm}(\mathfrak{f}) \geq 17.$$

Fortunately we can find ideals of norm 17 with the required properties. We fix $\mathfrak{f} = 1 + 4i$ (or $\mathfrak{f} = 1 - 4i$), so that the ray class field of conductor \mathfrak{f} is precisely $H_{\mathfrak{f}} = \mathbb{Q}(i, \sqrt[4]{1 + 4i})$. Since \mathfrak{f} is a prime ideal, all non-trivial characters of

$\text{Gal}(H_{\mathfrak{f}}/\mathbb{Q}(i))$ have conductor \mathfrak{f} , so that by the conductor-discriminant formula (12), $\text{disc}(H_{\mathfrak{f}}/\mathbb{Q}(i)) = \mathfrak{f}^3$. The absolute discriminant is $\text{disc}(H_{\mathfrak{f}}/\mathbb{Q}) = 17^3 \cdot 4^4$.

We choose $L = \mathbb{Q}(i, \sqrt{1+4i})$ and $E = H_{\mathfrak{f}}$, and prove that this choice yields the smallest possible discriminant of a cyclic extension of degree 4 over $\mathbb{Q}(i)$. To that end, let \mathfrak{m} be any ideal of $\mathbb{Z}[i]$ of norm different from 17 for which $16 \mid |(\mathbb{Z}[i]/\mathfrak{m})^\times|$, and let $E' \subset H_{\mathfrak{m}}$ be a subfield with $E'/\mathbb{Q}(i)$ cyclic of degree 4. Assume that $\text{disc}(E'/\mathbb{Q}) \leq 17^3 \cdot 4^4$. Since E' has conductor \mathfrak{m} , by the minimality of \mathfrak{m} the quartic characters of $\text{Gal}(E'/\mathbb{Q}(i))$ have conductor \mathfrak{m} . The quadratic character could have smaller conductor, but it cannot be smaller than 3, since $\mathbb{Q}(i)$ admits no ray class field of conductor \mathfrak{m} with $\text{Nm}(\mathfrak{m}) < 9$. Using the conductor-discriminant formula and as norms in $\mathbb{Q}(i)$ are positive, we have

$$\begin{aligned} 9 \cdot \text{Nm}(\mathfrak{m}^2) &\leq \text{Nm}(\text{disc}(E'/\mathbb{Q}(i))), \\ \Rightarrow 9 \cdot \text{Nm}(\mathfrak{m})^2 \cdot 4^4 &\leq \text{disc}(E'/\mathbb{Q}) < 17^3 \cdot 4^4, \\ \Rightarrow \text{Nm}(\mathfrak{m}) &< 23, 36 \dots, \end{aligned} \quad (18)$$

and so $|(\mathbb{Z}[i]/\mathfrak{m})^\times| < 23$. Since $16 \mid |(\mathbb{Z}[i]/\mathfrak{m})^\times|$, we have $|(\mathbb{Z}[i]/\mathfrak{m})^\times| = 16$. But then necessarily $\text{Nm}(\mathfrak{m}) = 17$, a contradiction to our assumption.

Step 2. Let $\mathcal{O}_L = \mathbb{Z}[i, \alpha]$, with α a root of $f(X) = X^2 + X - i$. A pair of norm-wise smallest primes in \mathcal{O}_L is $(\mathfrak{p}_2, \mathfrak{p}_5)$, of respective norms 2 and 5. Consequently, $\lambda_{E,L} = \frac{20^2}{17^6} < 1$ (cf. (13)), so that $\text{Nm}_{\mathbb{Z}[i]}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i]))$ will achieve the smallest possible value among all central division algebras satisfying the given conditions for a unit non-norm element $\gamma \in \mathcal{O}_L^\times$. Unfortunately, as we will show next, there is no suitable unit in this case, forcing us to consider other non-norm elements.

Step 3. By the Hasse Norm Theorem, to show that an element in L^\times is not a norm, it suffices to show that it is not a local norm at some prime of E . We need to produce a unit $\gamma \in \mathcal{O}_L^\times$ with $\gamma \notin \text{Nm}_{E/L}(E^\times)$, and since in an unramified local extension all units are norms, we consider the local extension corresponding to the ramifying prime $\mathfrak{f} = (1+4i)\mathbb{Z}[i]$. It is not difficult to verify that $\mathfrak{f}\mathcal{O}_L = \mathfrak{p}_L^2$, $\mathfrak{p}_L\mathcal{O}_E = \mathfrak{p}_E^2$ and $\text{Nm}_L(\mathfrak{p}_L) = \text{Nm}_E(\mathfrak{p}_E) = 17$.

Let $k = L_{\mathfrak{p}_L}$ and $K = E_{\mathfrak{p}_E}$ be the completions of E and L with respect to the discrete valuations associated to the primes \mathfrak{p}_L of L and \mathfrak{p}_E of E . Then K/k is a totally and tamely ramified cyclic local extension of degree 2, with $\overline{K} = \overline{k} = \mathbb{F}_{17}$. Using (16), $U_k \cap \text{Nm}_{K/k}(K^\times) = \langle \zeta_{16}^2 \rangle U_L^{(1)}$ and, by Hensel's lemma, an element in \mathcal{O}_L^\times will be a non-norm element for E/L if and only if its image in \mathbb{F}_{17} is not a square in \mathbb{F}_{17}^\times .

Since $\text{Nm}_{L/\mathbb{Q}}(x) = \text{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\text{Nm}_{L/\mathbb{Q}(i)}(x))$ and the norm of every unit in $\mathbb{Z}[i]$ is 1, we have $\text{Nm}_{L/\mathbb{Q}}(\mathcal{O}_L^\times) = \{1^2\}$. Consequently, the norm of the image in \mathbb{F}_{17} of every element in \mathcal{O}_L^\times is a square. Over finite fields, this is the case if and only if such an image is itself a square, which for its part implies that every element in \mathcal{O}_L^\times maps to $\langle \zeta_{16}^2 \rangle$ and, hence, is in the image of the map $\text{Nm}_{E/L}$. We conclude that there exists no unit which is a non-norm element

for E/L , forcing us to use (15) to balance the sizes of $\text{disc}(E/\mathbb{Q}(i))$ and γ in (6) in order to achieve minimality of $\text{Nm}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i]))$.

Since the norm of an element $x \in \mathcal{O}_L$ is the product of the norms of the prime ideals dividing x , it is easy to verify that the smallest possible norm in \mathcal{O}_L is 4. We set $\gamma = 1 + i \in \mathcal{O}_L$ with $\text{Nm}_L(1 + i) = 4$, which yields $D_{E/L}(\gamma) = 17^3 \times 2^2$. In order to study the possible values of $D_{E'/L'}(\gamma')$, let \mathfrak{m} be any ideal of $\mathbb{Z}[i]$ of norm different from 17, for which $16 \mid |(\mathbb{Z}[i]/\mathfrak{m})^\times|$, and let E' be a subfield of the ray class field $H_{\mathfrak{m}}$, with $E'/\mathbb{Q}(i)$ cyclic of degree 4.

The smallest possible norms for \mathfrak{m} are given by

$$\begin{aligned} 4 &= \text{Nm}(\mathfrak{p}_{17}\mathfrak{p}_2), & 49 &= \text{Nm}(\mathfrak{p}_7), & 64 &= \text{Nm}(\mathfrak{p})^6, \\ 68 &= \text{Nm}(\mathfrak{p}_{17}\mathfrak{p}_2^2), & 128 &= \text{Nm}(1 + i)^7, & \dots & \end{aligned}$$

Using (18), we see that $9 \cdot \text{Nm}(\mathfrak{m})^2 \leq \text{Nm}(\text{disc}(E'/\mathbb{Q}(i)))$, so that we only need to consider the cases for which $9 \cdot \text{Nm}(\mathfrak{m})^2 \leq 17^3 \times 2^2 \Rightarrow \text{Nm}(\mathfrak{m}) \leq 46, 728, \dots$, *i.e.*, only the case $\mathfrak{m} = (1 + 4i)(1 + i)$.

We compute $\text{Nm}(\text{disc}(E'/F))$. The smallest quadratic discriminant for an extension in which both $(1 + i)$ and a prime of norm 17 ramify is $(4 + i)(1 + i)^2$, corresponding to the extension $L' = \mathbb{Q}(\sqrt{4 + i})$. Thus, $E' = \mathbb{Q}(\sqrt[4]{4 + i})$, with $\text{disc}(E'/\mathbb{Q}(i)) = (4 + i)^3(1 + i)^4$ and $\text{Nm}(\text{disc}(E'/\mathbb{Q}(i))) = 17^3 \cdot 2^4$. Consequently, for all $\gamma' \in \mathcal{O}_{L'}$, $D_{E'/L'}(\gamma') \geq 17^3 \times 2^4 > 17^3 \times 2^2 = D_{E/L}(\gamma)$. By (14), we are done. \square

Theorem 4 *Let $\mathbb{Q}(i) \subset L \subset E$ with $[E : \mathbb{Q}(i)] = 6$ and $[E : L] = 3$. Any cyclic division algebra $(E/L, \sigma, \gamma)$ satisfies $\text{Nm}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i])) \geq 3^{18} \cdot 13^{12}$. The lower bound is achieved for $L = \mathbb{Q}(\zeta_{12})$, $E = L(\beta)$ and $\gamma = \frac{1+i\sqrt{3}}{2} \in \mathcal{O}_L^\times$, where ζ_{12} is a primitive 12th root of unity and β a root of $f(X) = X^3 - (1 + i)X^2 + 5iX - (1 + 4i)$.*

Proof :

Step 1. We start by finding the smallest possible discriminant over $\mathbb{Z}[i]$ for cyclic extensions of degree 6. We denote by L_2 , L_3 and $E = L_2L_3$ cyclic extensions of degree 2 and 3 over $F = \mathbb{Q}(i)$ and their compositum, respectively. Using (11), (12) and arguments similar to those used in Theorem 3, we deduce that the smallest possible cubic discriminant is $\mathfrak{p}_{13}^2 = (2 - 3i)^2$, corresponding to the extension $\mathbb{Q}(i, \beta)/\mathbb{Q}(i)$ [18, Table p. 883, row 32], where β is a root of the polynomial $f(X) = X^3 - (1 + i)X^2 + 5iX - (1 - 4i)$.

Since we want to minimize $\text{disc}(L_2L_3/\mathbb{Q}(i))$, the use of (11), (12) requires that we consider separately the cases where \mathfrak{m} is and is not relatively prime to \mathfrak{p}_{13} , and check which case yields a smaller value for this discriminant.

- i) $(\mathfrak{m}, \mathfrak{p}_{13}) = 1$. The smallest possible discriminant corresponds to the extension $L_2 = \mathbb{Q}(i)(\sqrt{-3}) = \mathbb{Q}(\zeta_{12})$ of $\mathbb{Q}(i)$, with $\text{disc}(L_2L_3/\mathbb{Q}(i)) = 3^3\mathfrak{p}_{13}^4$, of norm $\text{Nm}(\text{disc}(L_2L_3/\mathbb{Q}(i))) = 13^4 \cdot 3^6$.

ii) $(\mathfrak{m}, \mathfrak{p}_{13}) \neq 1$. If $\text{disc}(L'_2/\mathbb{Q}(i)) = \mathfrak{p}_{13} \times \mathfrak{a}$ for some ideal $\mathfrak{a} \neq (1)$, the best possibility is $\mathfrak{p}_{13}\mathfrak{p}_2^2$, corresponding to the extension $L'_2 = \mathbb{Q}(i)(\sqrt{3-2i})$ of $\mathbb{Q}(i)$ with discriminant ideal $\mathfrak{p}_{13} \times \mathfrak{p}_2^2$. This choice yields⁶ $\text{disc}(L'_2L_3/\mathbb{Q}(i)) = \mathfrak{p}_{13}^5 \times \mathfrak{p}_2^6$, with $\text{Nm}(\text{disc}(L'_2L_3/\mathbb{Q}(i))) = 13^5 \cdot 2^6 > 13^4 \cdot 3^6$.

We conclude that the smallest possible discriminant over $\mathbb{Z}[i]$ for cyclic extensions of degree 6 is $3^6 \cdot 13^4$, achieved in the extension $E = L_2L_3$. The involved rings of integers are $\mathcal{O}_2 = \mathbb{Z}\left[i, \frac{i+\sqrt{3}}{2}\right]$ and $\mathcal{O}_3 = \mathbb{Z}[i, \beta]$. The discriminants of the extensions involved are summarized in Table 2 below.

	$\text{disc}(\cdot/\mathbb{Q}(i))$	$\text{Nm}_{\mathbb{Z}[i]}$	$\text{disc}(\cdot/L_2)$	$\text{Nm}_{\mathcal{O}_2}$	$\text{disc}(\cdot/L_3)$	$\text{Nm}_{\mathcal{O}_3}$
E	$\mathfrak{p}_3^3\mathfrak{p}_{13}^4$	$3^6 \cdot 13^4$	$\mathfrak{q}_{13}^2\mathfrak{q}_{13}^2$	13^4	\mathfrak{s}_3	3^6
L_3	\mathfrak{p}_{13}^3	13^2				
L_2	\mathfrak{p}_3	3^2				

Table 2 Relative discriminants of the field extensions involved.

Step 2. A pair of smallest primes in \mathcal{O}_2 is $(\mathfrak{q}_2, \mathfrak{q}_3)$ of norms 4 and 9, respectively, where \mathfrak{q}_2 is any prime above 2, and \mathfrak{q}_3 is any prime above 3. Consequently, $\lambda_{E,L} = \frac{4^2 9^2}{13^4} < 1$ (cf. (13)), and $\text{Nm}_{\mathbb{Z}[i]}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i]))$ will achieve its smallest possible value for a unit non-norm element $\gamma \in \mathcal{O}_2^\times$, $\gamma \notin \text{Nm}_{E/L_2}(E^\times)$.

Step 3. To simplify notation, we set, $L_2 = L$, and $\mathcal{O}_2 = \mathcal{O}_L$. We prove that the unit $\gamma = \frac{1+i\sqrt{3}}{2} \in \mathcal{O}_L^\times$ satisfies $\gamma \notin \text{Nm}_{E/L}(E^\times)$.

The prime \mathfrak{q}_{13} ramifies in the extension E/L . Let \mathfrak{t}_{13} be a prime of E extending \mathfrak{q}_{13} , and $k = L_{\mathfrak{q}_{13}}$, $K = E_{\mathfrak{t}_{13}}$ be the completions of L and E with respect to the corresponding valuations, with $|\bar{k}| = |\bar{K}| = 13$.

The local extension K/k is a totally and tamely ramified extension of degree 3. Since the image of the unit $\gamma = \frac{1+i\sqrt{3}}{2}$ in the residue field \mathbb{F}_{13} is 4, which has multiplicative order 6, we deduce that $\gamma \notin \langle \bar{\zeta}_{12}^3 \rangle U_L^{(1)}$. By (16) and Hasse's Norm Theorem, the theorem follows. \square

Theorem 5 *Let $\mathbb{Q}(i) \subset L \subset E$ with $[E : \mathbb{Q}(i)] = 6$ and $[E : L] = 2$, and let $(E/L, \sigma, \gamma)$ be a cyclic division algebra. Then, $\text{Nm}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i])) \geq 2^6 \cdot 3^{12} \cdot 13^8$ with equality for $\gamma = 1 + i$ and $E = LL_2$, where $L_2 = \mathbb{Q}(i, i\sqrt{3}) = \mathbb{Q}(\zeta_{12})$ and $L = \mathbb{Q}(i, \beta)$ with β a root of the polynomial $f(X) = X^3 - (1+i)X^2 + 5iX - (1+4i)$.*

Proof :

Step 1, 2. Let E and L be as in the statement of the theorem. By Theorem 4, the same choice of field E ensures the minimality of the discriminant $\text{disc}(E/\mathbb{Q}(i)) = 3^6 \cdot 13^4$ among all possible discriminants of cyclic sextic extensions over $\mathbb{Q}(i)$.

⁶ The factor \mathfrak{p}_{13}^5 comes from the fact that E/L_3 is tamely ramified and, thus, has as discriminant the prime \mathfrak{q}_{13} lying above 13 in L_3 .

Let $L = \mathbb{Q}(i, \beta)$. A pair of smallest primes in \mathcal{O}_L is $(\mathfrak{s}_2, \mathfrak{s}_{13})$, of norms 2^3 and 13 , respectively. Consequently, $\lambda_{E,L} = \frac{2^3 13}{3^3} < 1$ (cf. (13)), and the norm $\text{Nm}_{\mathbb{Z}[i]}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i]))$ will attain its smallest possible value for a unit non-norm element $\gamma \in \mathcal{O}_L^\times$.

Step 3. We encounter here the same situation as in Theorem 3. On the one hand, since $\text{Nm}_{L/\mathbb{Q}}(x) = \text{Nm}_{\mathbb{Q}(i)/\mathbb{Q}}(\text{Nm}_{L/\mathbb{Q}(i)}(x))$ and the norm of every unit in $\mathbb{Z}[i]$ is 1, every element in \mathcal{O}_L^\times maps to a square in the residue field. On the other hand, $[E : L] = 2$, and (16) tells us that $\mathcal{O}_L^\times \cap \text{Nm}_{E/L}(E^\times)$ consists of those elements in \mathcal{O}_L^\times which map to squares in the residue field of any ramifying prime. Consequently, every element in \mathcal{O}_L^\times is in the image of the map $\text{Nm}_{E/L}$, and there exists no non-norm unit element for E/L . We thus need to balance the sizes of $\text{disc}(E/\mathbb{Q}(i))$ and γ in (6) to achieve minimality of $\text{Nm}(\text{disc}(\mathcal{O}_{\text{nat}}/\mathbb{Z}[i]))$. We observe that this argument holds for any choice of E and L , as long as $\mathbb{Q}(i) \subset L$ and $[E : L] = 2$.

We fix $\gamma = 1 + i$ of norm 2^3 , corresponding to the smallest possible norm in \mathcal{O}_L . Substituting into (15), we get $D_{E/L}(\gamma) = 3^6 \cdot 13^4 \cdot 2^3$. We conclude the proof by showing that $D_{E/L}(\gamma) \leq D_{E'/L'}(\gamma')$ for any other choice of E', L' and γ' under the given assumptions.

Any possible $E' \neq E$ is of the form $E' = L'_2 L$ with $L'_2 \neq L_2$ or $E' = L'_2 L'$ with $L' \neq L$ (L'_2 could be equal to L_2) and $[L' : \mathbb{Q}(i)] = 3$. In the first case, by the minimality arguments in the choice of L_2 and γ , for all choices of L'_2 and $\gamma' \in \mathcal{O}_L \setminus \mathcal{O}_L^\times$,

$$3^6 \cdot 13^4 \cdot 2^3 \leq \text{Nm}(\text{disc}(L'_2 L/\mathbb{Q}(i))) \cdot \text{Nm}(\gamma),$$

and so $D_{E/L}(\gamma) \leq D_{L'_2 L/L}(\gamma')$.

Suppose next that $E' = L'_2 L'$ with $L' \neq L$ and $[L' : \mathbb{Q}(i)] = 3$. As we saw in Step 1 of the proof of Theorem 4, the conductor of a cubic extension $L' \neq L$ of $\mathbb{Q}(i)$ is ideal $\mathfrak{m} \in \mathbb{Z}[i]$ of norm greater than 13 and such that $|(\mathbb{Z}[i]/\mathfrak{m})^\times|$ is a multiple of 12. By the conductor-discriminant formula, the corresponding extension L' will have discriminant \mathfrak{m}^2 , and by the minimality in the choice of L_2 , $\text{Nm}(\text{disc}(L_2 L'/\mathbb{Q}(i))) = 3^6 \text{Nm}(\mathfrak{m})^4 \leq \text{disc}(L_2 L'_3/\mathbb{Q}(i))$ for any quadratic extension L'_3 of $\mathbb{Q}(i)$. Consequently,

$$3^6 \text{Nm}(\mathfrak{m})^4 \cdot 2 \leq \text{disc}(L'_3 L_2/\mathbb{Q}(i)) \cdot \text{Nm}(\gamma') = D_{E'/L'}(\gamma')$$

for all choices of $\gamma' \in \mathcal{O}_L \setminus \mathcal{O}_L^\times$. Now,

$$3^6 \text{Nm}(\mathfrak{m})^4 \cdot 2 \geq 3^6 \cdot 13^4 \cdot 2^3 \Leftrightarrow \text{Nm}(\mathfrak{m}) \geq 13\sqrt{2} > 13.$$

We conclude that $D_{E/L}(\gamma) \leq D_{E'/L'}(\gamma')$ for all possible choices of E', L' and γ' , and the theorem follows. \square

4 Conclusions

In this article we have introduced the reader to a technique used in multiple-input multiple-output wireless communications known as space–time coding. Within this framework, we have recalled several design criteria which have been derived in order to ensure a good performance of codes constructed from representations of orders in central simple algebras. In particular, we have explained why it is crucial to choose orders with small discriminants as the underlying algebraic structure in order to maximize the coding gain. While maximal orders achieve the minimal discriminant and hence the maximal coding gain among algebraic space–time codes, we have motivated why in practice it may sometimes be favorable to use the so-called natural orders instead. However, one should bear in mind that orthogonal lattices have yet additional benefits such as simple bit labeling and somewhat simpler encoding and decoding, so there is a natural tradeoff between simplicity and coding gain.

For the base fields $F = \mathbb{Q}$ or F imaginary quadratic (corresponding to the most typical signaling alphabets), and pairs of extension degrees (n_t, n_r) in an asymmetric channel setup, we have computed an explicit number field extension (E/L) and a non-norm element $\gamma \in \mathcal{O}_L \setminus \{0\}$ giving rise to a cyclic division algebra whose natural order \mathcal{O}_{nat} achieves the minimum discriminant among all cyclic division algebras with the same degree and base field assumptions. This way we have produced explicit space–time codes attaining the optimal coding gain among codes arising from natural orders.

Acknowledgements A. Barreal and C. Hollanti are financially supported by the Academy of Finland grants #276031, #282938, and #303819, as well as a grant from the Foundation for Aalto University Science and Technology.

The authors thank Jean Martinet, René Schoof, and Bharath Sethuraman for their useful suggestions, and the anonymous reviewers for their valuable comments to improve the quality of the manuscript.

References

1. V. Tarokh, N. Seshadri, and A. R. Calderbank, Space–Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction, *IEEE Transactions on Information Theory* 44(2), pp. 744–765, 1998.
2. J.-C. Belfiore and G. Rekaya, Quaternionic Lattices for Space–Time Coding, *Proceedings of the IEEE Information Theory Workshop*, 2003.
3. B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, Full-Diversity, High-Rate Space–Time Block Codes from Division Algebras, *IEEE Transactions on Information Theory* 49(10), pp. 2596–2616, 2003.
4. J.-C. Belfiore, G. Rekaya, and E. Viterbo, The Golden Code: a 2×2 Full-Rate Space–Time Code with Non-vanishing Determinants, *IEEE Transactions on Information Theory* 51(4), pp. 1432–1436, 2005.
5. F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, Perfect Space–Time Block Codes, *IEEE Transactions on Information Theory* 52(9), pp. 3885–3902, 2006.
6. P. Elia, B. A. Sethuraman, and P. V. Kumar, Perfect Space–Time Codes for Any Number of Antennas, *IEEE Transactions on Information Theory* 53(11), pp. 3853–3868, 2007.

7. C. Hollanti, J. Lahtonen, and H.-f. Lu, Maximal Orders in the Design of Dense Space–Time Lattice Codes, *IEEE Transactions on Information Theory* 54(10), pp. 4493–4510, 2008.
8. R. Vehkalahti, C. Hollanti, J. Lahtonen, and K. Ranto, On the Densest MIMO Lattices From Cyclic Division Algebras, *IEEE Transactions on Information Theory* 55(8), pp. 3751–3780, 2009.
9. C. Hollanti and H.-f. Lu, Construction Methods for Asymmetric and Multiblock Space–Time Codes, *IEEE Transactions on Information Theory* 55(3), pp. 1086–1103, 2009.
10. I. Reiner, Maximal Orders, *London Mathematical Society Monographs New Series* 28, 2003.
11. R. Vehkalahti, Class Field Theoretic Methods in the Design of Lattice Signal Constellations, *TUCS Dissertations* 100, 2008.
12. R. Vehkalahti, C. Hollanti, and F. Oggier, Fast-Decodable Asymmetric Space-Time Codes From Division Algebras, *IEEE Transactions on Information Theory* 58(4), pp. 2362–2385, 2012.
13. H. Cohen and P. Stevenhagen, Computational Class Field theory, *Algorithmic Number Theory, MSRI Publications* 44, pp. 497–534, 2008.
14. J. S. Milne, Algebraic Number Theory (v3.07), *Graduate course notes*, 2017, available at www.jmilne.org/math/CourseNotes/.
15. J. S. Milne, Class Field Theory (v4.02), *Graduate course notes*, 2013, available at www.jmilne.org/math/CourseNotes/.
16. R. H. Hudson and K. S. Williams, The Integers of a Cyclic Quartic Field, *Rocky Mountains Journal of Mathematics* 20(1), pp. 145–150, 1990.
17. J.G. Huard, B.K. Spearman, and K. S. Williams, Integral Bases for Quartic Fields with Quadratic Subfields, *Carleton-Ottawa Mathematical Lecture Notes Series* 7, pp. 87–102, 1986.
18. A.-M. Bergé, J. Martinet, and M. Olivier, The Computation of Sextic Fields with a Quadratic Subfield, *Mathematics of Computation* 54(190), pp. 869–884, 1990.