Roope Vehkalahti

Class Field Theoretic Methods in the Design of Lattice Signal Constellations

Turku Centre *for* Computer Science

TUCS Dissertations
No 100, March 2008

Class Field Theoretic Methods in the Design of Lattice Signal Constellations

by

Roope Vehkalahti

To be presented, with the permission of the Faculty of Mathematics and Natural Sciences of the University of Turku, for public criticism in Auditorium XXI of the University on April 16th, 2008, at 12 noon

University of Turku
Department of Mathematics
FI-20014 Turku, Finland

2008

SUPERVISOR

DOCENT JYRKI LAHTONEN
Department of Mathematics
University of Turku
FIN-20014 Turku
Finland

REVIEWERS

PROFESSOR GARY MCGUIRE
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4
Ireland
PROFESSOR BHARATH SETHURAMAN
Department of Mathematics
California State University
Cal State Northridge
18111 Nordhoff St
Northridge, CA 91330-8313
United States of America

OPPONENT

PROFESSOR GRÉGORY BERHUY
Universite Joseph Fourier
Institut Fourier
100 rue des Maths
B.P. 74
38402 St Martin d'Heres
France

ISBN 978-952-12-2065-4
ISSN 1239-1883
Turku, Finland
2008

Acknowledgements

First of all I would like to thank my supervisor Docent Jyrki Lahtonen. It was a pleasure to work with him.

Great thanks go also to my team mates Dr. Kalle Ranto and Ph.D. student Camilla Hollanti for fruitful collaboration. Particularly, I thank Camilla for producing figures 2.1 and 3.4 and Kalle for proofreading my thesis.

Special thanks are due to Professor Bharath Sethuraman and Professor Gary McGuire for the preliminary examination of the thesis.

I would like to thank the Department of Mathematics and Turku Center for Computer Science (TUCS) for financial support and for providing a great working environment.

Finally, I thank Eeva for all the great and funny moments and apologize Aaro for me being always in a hurry and not spending as much time with him as he deserves.

Turku
March 2008 Roope Vehkalahti

Contents

Introduction

Wireless transmission in the urban environment is a difficult task. Not only is the transmitted signal corrupted by the gentle thermal noise, but it can also get reflected and distorted, due to interference of infrastructure. One way to fight these harsh conditions is to increase the number of transmitting and receiving antennas and spread the signal not only in time but also in space. This approach can increase the transmission reliability, and at the same time the transmission rate. A code that is designed for such multiple-input multiple-output (MIMO) transmission is called a *space-time block code* (STBC) or a *MIMO code*. In algebraic terms a MIMO code is a finite set of matrices.

Traditional coding theory has been mostly interested in the situation where the transmitter and the receiver use a single antenna. During the relatively short history of coding theory researchers have exploited several algebraic structures in the quest for finding optimal codes and explore the limits of performance. Some of these questions have led to fascinating interplay between central algebraic questions and properties of simple codes. One of the most beautiful examples is the relation between linear codes and Riemann–Roch spaces of function fields (see [41]). This connection allows one to use strong algebraic-geometric methods in the research of linear codes. The use of these methods leads to existence results of codes with better performance than was believed to be possible.

In the MIMO case, however, the channel model is totally different. Therefore not much of the so far used algebra is useful and it is clear that new ideas are needed. One of the first answers to these problems was given by Alamouti in 1998 [1]. The *Alamouti code* represented multiplication in the quaternion algebra. This approach was soon generalized and the basics of use of division algebras in MIMO coding were presented by Sethuraman et al. in [39]. However, only a small piece of the true potential of division algebras was used. The problem was that MIMO codes from division algebras are infinite lattices from where a finite set of codewords is chosen for the actual transmission and at this point the increase in the size of a code could have an unexpected effect on the performance of the code.

In 2003 Belfiore and Rekaya [6] suggested that instead of the whole algebra one should use a certain subring for code construction. The resulting matrix lattices had the non-vanishing determinant property (NVD). This raised interest,

especially when it was proved by Elia et al. in [12] that such codes achieve the diversity-multiplexing gain trade-off of Tse and Zheng [47], revealing that in an asymptotic sense such codes responded optimally to the increase of the code size.

This resulted into intense race to produce STBC's from division algebras. One of the highlights was the introduction of the perfect codes by Rekaya et. al [35].

Yet there was one fundamental observation to be made. In [16] Hollanti and Lahtonen showed that the widely used specific ring, so-called *natural order*, was just an example of well known algebraic objects called *orders*. What was before seen as a lucky accident was now revealed to be an expression of the general theory. In [16] it was also pointed out that of all the orders the best coding gain was achieved by the use of *maximal orders*. In the following, we will show how their observation leads to the codes that break all the coding gain records of square, fully multiplexing MIMO codes.

In this thesis we create a coding theoretic context that allows us to discuss coding theoretic properties of general order codes. After that we relate the performance of order codes to structure theory of central simple algebras, which is a beautiful and central part of class field theory and non-commutative algebra.

As an example of the strength of our theory we show how the coding gain of a code from an order of a division algebra depends on the local structure of the underlying algebra. This connection then allows us to explore the bounds of performance of these codes. The most interesting result of this theory is a bound that limits the coding gain of order codes. The proof of this result also reveals that there exist division algebras attaining this bound. While the proof is not constructive, it describes the algebras well enough so that we are able to construct them for all practical numbers of antennas. The resulting codes have the largest known coding gain.

The structure of the thesis is the following. We begin with a discussion on lattice codes. While these codes are interesting on their own right our treatment is partly done to give an idea of our goals in the MIMO case. In a single antenna fast Rayleigh fading channel the coding gain depends on the minimum product distance of the corresponding lattice. In Chapter 1 we give a bound for the product distance of rotated $\mathbb{Z}^n$-lattices (see [4]). For relatively large values of n this bound is better than the previous bound in [4].

We then show how the product distance of the complex lattice, derived from an algebraic number field, depends on the $\mathbb{Z}$-discriminant of the corresponding field. This result is a generalization of [4, Theorem 5.1] and should simplify the proofs in [45] and [10]. As an example of the strength of our results we give two examples of complex lattices having the best known normalized minimum product distance.

We then consider orthogonal complex lattices. In the special case where the orthogonal lattice is a rotated $\mathbb{Z}[i]^n$-lattice (see [4]) our bound is considerably stronger than the previous one presented in [4]. As a corollary we get that the

best rotated $\mathbb{Z}[i]^n$-lattices in [13] and [4] are optimal orthogonal lattices when n is a power of two.

Then we turn into MIMO codes. Our main interest here are infinite, square, fully multiplexing MIMO codes which are full lattices in $M_n(\mathbb{C})$. We also suppose that our codes have the non-vanishing determinant property. So far these kind of codes have appeared at least in [12], [44], [21], [30], and [11].

The code constructions in [12], [21], [30], and [11] use division algebras. These codes can be divided into two groups. In the first group are the shaped codes in [11] and [30] and in the other are the codes from the natural orders in [12] and [21]. In the following we give coding gain bounds for all the previously mentioned codes.

In Section 2.1.1 we define the *normalized minimum determinant*, which in special cases has been used in [44] and in [30]. This concept then allows us to discuss the relation between the *shortest vector* (Definition 1.2.6) and the minimum determinant (Definition 2.1.8) of a MIMO lattice. With the help of a simple inequality we get a relation where the Frobenius norm of the matrix bounds the size of the determinant. This connection then allows us to limit the minimum determinant of a MIMO lattice with a help of the sphere packing bounds. While the bound achieved is generally not very tight it is very effective when the code lattice has a certain shape (Section 3.2).

We then proceed to consider MIMO codes produced from orders of division algebras. In [18] the authors proved a result that connects the *coding gain* of the lattice and an invariant of the order called *the discriminant*. It reveals that in order to maximize the coding gain one has to minimize the discriminant of an order.

The authors of [16] suggested that one should use a maximal order of an algebra as a code lattice, instead of the widely used natural order, in order to maximize the coding gain. In Section 2.4.2 we show that this view is extremely fruitful as the discriminant of the maximal orders of an algebra can be linked to the Hasse invariants of the algebra.

A fundamental exact sequence of Brauer groups then allows us to derive a tight bound for the discriminant (Theorem 2.4.26) of any order. These results then translate into coding gain bounds for MIMO lattices from orders of division algebras. In particular, these bounds restrict the coding gain of codes in [12] and [21]. Theorem 2.4.26 also describe the minimal discriminants achieving the bound. In Section 2.4.4 these results are translated into coding theoretic language and the existence of infinite families of MIMO codes with the best known coding gain is proved.

In Section 2.5 we briefly discuss code lattices in $M_n(\mathbb{R})$ and show how our theory works in that context.

We then analyze some of the existing codes and start with a discussion on natural orders. We first show that in the most interesting algebras the natural orders do not reach the coding gain of maximal orders with minimal discriminants.

Proposition 3.1.8 then give us a better view of the performance of codes from natural orders. It shows that the coding gain of the codes from natural orders is always far from the coding gain of the best maximal orders.

In Section 3.2 we show that the simple general bounds in Corollaries 2.2.5 and 2.2.4 gives us very tight bounds for shaped codes in [11]. The comparison to the best codes from maximal orders proves that the shaped codes can never achieve the coding gain of the codes from maximal orders and that when the number of receiving and transmitting antennas grow the difference grows considerably.

In the final chapter we give a general construction for division algebras achieving the bound of Theorem 2.4.26.

Chapter 1

Lattice codes

Our main interest in this thesis lies on the MIMO codes (Definition 2.1.2) but we first discuss a simpler situation where the transmitter and the receiver both have only one antenna. This setup leads us to discuss lattices in $\mathbb{C}^n$ and $\mathbb{R}^n$ (see [31]). While the lattice codes are interesting on their own right partly the motivation to present the following results is to reveal the simple analogy existing between the lattice codes and the MIMO codes. We will return to this question several times later.

For practical reasons many authors have concentrated on lattice codes that are orthogonal. In the following we study how the demand of orthogonality affects the minimum product distance.

1.1 Algebraic number fields

In this thesis we expect the reader to have a working knowledge on algebraic number theory. However, we like to recall some of the basic concepts that are central in the later parts of the thesis. Particularly we concentrate on the concept of a prime in algebraic number field and the similarities between infinite and finite primes. The valuation theoretic definition we are going to give is not a pointless generalization of a prime ideal. At first the roles of the infinite and the finite primes seem to be rather different. However, when we begin to consider central simple algebras and their local structure theory, we will see that the infinite primes share many of the characteristics of the prime ideals in the ring of algebraic integers. For the details of this section we refer the reader to [25] and [26].

In this thesis an algebraic number field is a finite algebraic extension of $\mathbb{Q}$. Let K be an algebraic number field and $\mathcal{O}_K$ the ring of algebraic integers in K. Let us consider the set of valuations on the field K. Each of these valuations induce a metric on K. We define an equivalence of valuations by setting that two valuations are equivalent if and only if the corresponding metrics are equivalent.

Definition 1.1.1. A *prime P* in K is an equivalence class of nontrivial valuations on K.

Theorem 1.1.2. *Let K be an algebraic number field. There exists exactly one prime of K*

(a) *for each prime ideal P;*

(b) *for each real embedding;*

(c) *for each conjugate pair of complex embeddings.*

In the following we refer to the additive P-adic valuation with v_P. In each equivalence class of valuations of K we can select a normalized valuation as follows:

- for a prime ideal P of $\mathcal{O}_K$, $|a|_P = (1/[\mathcal{O}_K : P])^{v_P(a)}$;
- for a real embedding $\sigma : K \hookrightarrow \mathbb{R}$, $|a|_\sigma = |\sigma(a)|$;
- for a nonreal complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, $|a|_\sigma = |\sigma(a)|$.

We simply refer to these valuations with $|\cdot|_P$. The corresponding primes are called finite, real, and complex, respectively. When we discuss finite primes we identify the prime ideals of $\mathcal{O}_K$ and the corresponding normalized valuations. An element of K is said to be positive at the real prime corresponding to an embedding $K \hookrightarrow \mathbb{R}$ if it maps to a positive element of $\mathbb{R}$.

Definition 1.1.3. Let $K/\mathbb{Q}$ be a finite extension of degree n. Suppose that r_1 and $2r_2$ are the numbers of real and complex embeddings of K to $\mathbb{C}$. We call the 2-tuple (r_1, r_2) *the signature* of the field K.

Proposition 1.1.4. *Let $[K : \mathbb{Q}] = n$. Then*

$$r_1 + 2r_2 = n.$$

Remark 1.1.5. A typical method to determine the number of real and complex embeddings of an algebraic number field is to pick a primitive element a of the extension $K/\mathbb{Q}$ and then count the number of real and complex zeros of the minimal polynomial of a.

If the signature of a field K is $(r_1, 0)$, we say that the field is *totally real* and if the signature is $(0, r_2)$, we say that the field is *totally complex*. An element a of a totally real field K is *totally positive* if it is positive respect to all the real embeddings.

Let P be a prime of K. By K_P we refer to the analytic completion of the field K respect to the metric defined by the valuation $|\ |_P$. If the prime P is infinite, K_P

is $\mathbb{R}$ or $\mathbb{C}$ depending on whether the prime is real or complex, respectively. If P is finite, then K_P is just the familiar P-adic completion of the field K.

Now we would like to discuss the ramification theory of ideals in finite extensions. Suppose that B is a prime in L and that the restriction of this valuation to K is P. We then use the phrase that B lies above P or that B extends the valuation P.

Proposition 1.1.6. *Above each prime of K there lies finitely many primes of L.*

Remark 1.1.7. For the finite primes this definition coincides with the usual ideal theoretic language. The valuations that extend a prime P corresponds to the prime ideals of $\mathcal{O}_L$ that lie above P in L.

If the prime P of K is real and one of the primes that lie above P in L is complex, we say that the prime P is ramified in the extension L/K. Otherwise we say that P is nonramified. For finite primes we use the usual ideal theoretic language.

Example 1.1.8. Let us consider the extension $K/\mathbb{Q}$, where $K = \mathbb{Q}(\sqrt{-3})$. The field $\mathbb{Q}$ has only one infinite prime ∞, that corresponds the normal absolute valuation. The element $\sqrt{-3}$ has a minimal polynomial $x^2+3 = (x-\sqrt{-3})(x+\sqrt{-3})$. We then see that there is exactly one infinite prime in K and that this prime is complex and lies above the prime ∞. Therefore we can say that ∞ is ramified in the extension $K/\mathbb{Q}$.

The following example can be seen as an illustration of *the product formula* of valuations, that bundles up all the valuations in an algebraic number field.

Example 1.1.9. Let us consider the field $K = \mathbb{Q}(\sqrt{-m})$, where m is a positive squarefree integer. Each of the elements c in K can be uniquely presented in the form $c = a + b\sqrt{-m}$, where a and b are rational numbers. We then have

$$nr_{K/\mathbb{Q}}(c) = (a+b\sqrt{-m})(a-b\sqrt{-m}) = a^2+b^2m = |c|^2.$$

If the element c is in $\mathcal{O}_K$, the algebraic norm takes c to $\mathbb{Z}$. The previous equation then gives us that

$$|c| \geq 1,$$

for every c in $\mathcal{O}_K^*$. Later in this thesis this simple result will play a crucial role.

Definition 1.1.10. Suppose that L/K is an n-dimensional extension of algebraic number fields and that $tr_{L/K}$ is the trace function. The *discriminant* $d(L/K)$ of the extension L/K is an ideal in $\mathcal{O}_K$ generated by the set

$$\{\det(tr_{L/K}(x_i x_j))_{i,j=1}^n \mid (x_1,...,x_n) \in \mathcal{O}_L^n\}.$$

If we like to emphasize that the discriminant considers the relation between $\mathcal{O}_K$ and $\mathcal{O}_L$, we can also write $d(\mathcal{O}_L/\mathcal{O}_K)$.

If $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, then

$$d(\mathcal{O}_L/\mathcal{O}_K) = \det(tr(x_i x_j))_{i,j=1}^n,$$

where $\{x_1,\ldots,x_n\}$ is any $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

The following theorem connects the ramification of finite primes and the discriminant.

Theorem 1.1.11. *Let P be a prime ideal of the ring $\mathcal{O}_K$ and $p = \mathrm{char}(\mathcal{O}_K/P)$. Suppose that*

$$P\mathcal{O}_L = B_1^{e_1}\cdots B_g^{e_g}$$

is the prime decomposition of P in the ring $\mathcal{O}_L$. Let f_i stand for the inertial degree $f(B_i|P)$. Then

$$v_P(d(L/K)) = (e_1-1)f_1 + \cdots + (e_g-1)f_g,$$

if $p \nmid e_i$, $i = 1,2,\ldots,g$, and

$$v_P(d(L/K)) > (e_1-1)f_1 + \cdots + (e_g-1)f_g,$$

if $p \mid e_i$ for some index i.

We say that a prime P is wildly ramified if and only if $p \mid e_i$, for some i, otherwise we say that it is tamely ramified. From the previous proposition we see that the ramification of a tame prime P defines totally the P power index of the discriminant. For wildly ramified ideals we only get a lower bound.

While the discriminant and infinite primes do not seem to have any connection the following result proves the opposite. In 1977 Andrew Odlyzko [29] gave a lower bound $C_{(r_1,r_2)}$ for the discriminants of fields with signature (r_1,r_2). For small values of r_1 and r_2 there exists tables for $C_{(r_1,r_2)}$. Asymptotically, when $n \to \infty$, we have

$$|d(K/\mathbb{Q})|^{1/n} \geq (60.8395...)^{r_1/n}(22.3816...)^{2r_2/n} - O(n^{-2/3}) = C_{(r_1,r_2)}. \quad (1.1)$$

When the signature is clear from the context we abbreviate $C_{(r_1,r_2)}$ to C_n. An informal and incorrect but suggestive interpretation of this result is, that the minimal amount of ramification is somewhat constant, but the part of the ramification that happens on infinite primes does not contribute to the discriminant.

We will need later the following two technical lemmas.

Lemma 1.1.12. *Let $K_2 \supseteq K_1 \supseteq F$ be a tower of finite extensions of $\mathbb{Q}$. Then*

$$d(K_2/F) = nr_{K_1/F}(d(K_2/K_1))d(K_1/F)^{[K_2:K_1]},$$

where $nr_{K_1/F}$ is the usual relative norm of algebraic number theory.

Proof. For the proof we refer the reader to [36, p.249]. □

Lemma 1.1.13. *Suppose that we have an abelian extension L/K of degree n, with a Galois group $\{\sigma_1,\ldots,\sigma_n\}$, and suppose that $\{x_1,x_2,\ldots,x_n\}$ is some $\mathscr{O}_K$ basis of the ring $\mathscr{O}_L$. Then*

$$\det(tr_{L/K}(x_ix_j))_{i,j=1}^n = \pm\det(tr_{L/K}(\sigma_k(x_i)x_j))_{i,j=1}^n.$$

Proof. We define $X_i = (\sigma_i(x_1),\ldots,\sigma_i(x_n))$ and consider the matrix X which has vectors X_i as rows. We then have that

$$\det(tr_{L/K}(x_ix_j))_{i,j=1}^n = \det(X^TX).$$

If we replace the rows X_i in the matrix X with the rows

$$\sigma_k(X_i) = (\sigma_k(\sigma_i(x_1)),\ldots,\sigma_k(\sigma_i(x_n))),$$

we get a matrix $\sigma_k(X)$. Then

$$\det(tr_{L/K}(\sigma_k(x_i)x_j))_{i,j=1}^n = \det(\sigma_k(X)^TX).$$

Clearly

$$\det(\sigma_k(X)) = \pm\det(X),$$

and the claim follows.

□

We shall now recall some facts of P-adic fields. Suppose that P is a finite prime of an algebraic number field K, K_P the P-adic completion, and $p = \mathrm{char}(\mathscr{O}_K/P)$. We may consider K_P as a finite algebraic extension of $\mathbb{Q}_p$ and then refer to the algebraic closure of the ring $\mathbb{Z}_p$ in K_P with $\mathscr{O}_{K_P}$, and simply call it the ring of integers in K_P. In the following we identify the prime P and the unique prime ideal $P\mathscr{O}_{K_P}$ of the ring $\mathscr{O}_{K_P}$, and refer to both by P.

We extend the concept of wild and tame ramification to local fields. Let L be a finite algebraic extension of K_P, and B the unique prime ideal of $\mathscr{O}_L$. We say that P is wildly ramified if p divides the ramification index $e(B|P)$; otherwise we say that P is tamely ramified.

Definition 1.1.14. Let L be a finite and totally inert Galois extension of K_P and that B is the unique prime ideal of the ring of the P-adic algebraic integers $\mathscr{O}_L$ in L. Suppose that $[\mathscr{O}_{K_P} : P] = q$. Then $\mathrm{Gal}(L/K_P)$ has an element $(P,L/K_P)$ called the (local) *Frobenius automorphism*. It is the unique element of $\mathrm{Gal}(L/K_P)$ satisfying

$$(P,L/F_P)(x) \equiv x^q \pmod{B}\,\forall x \in \mathscr{O}_L.$$

Suppose that L is an abelian extension of K_P and that U is the group of units in $\mathscr{O}_{K_P}$.

Definition 1.1.15. The smallest f such that $nr_{L/K_p}(L^*)$ contains $1+P^f$ is called the *conductor* of L/K_P, except that, when $nr_{L/K_p}(L^*) \subset U$, the conductor is said to be 0.

Remark 1.1.16. In the last definition we expected the existence of some f. This is a nontrivial result.

In some special cases the determination of the conductor is easy. For the proof we refer the reader to [25, p.12]

Lemma 1.1.17. *The extension L/K_P is unramified if and only if its conductor is 0, and it is tamely ramified if and only if its conductor is ≤ 1.*

1.2 Basic definitions

If we have a lattice L in $\mathbb{R}^n$, we say that it is *full* if it has n linearly independent basis vectors. If we have a lattice L in $\mathbb{C}^n$, we say that it is full if it has $2n$ basis vectors that are linearly independent over $\mathbb{R}$.

We shall compare such lattices exclusively in terms of their product distances. This is the figure of merit that emerges when the performance of a lattice is analyzed in a fast-fading channel, in particular when the complex channel coefficients follow the Rayleigh distribution.

Definition 1.2.1. *A lattice code* is a full lattice in a vector space F^n, where $F = \mathbb{R}$ or $F = \mathbb{C}$.

One of the main design criteria for this kind of lattice codes is the maximization of the *product distance* (Definition 1.2.2). In the following we discuss the lattice codes with this criterion in mind.

In the following we suppose that F is the field of real or complex numbers.

Definition 1.2.2. Let $v = (v_1, ..., v_n)$ be a vector in F^n. We define the *norm* of v as

$$n(v) = \prod_{i=1}^{n} |v_i|.$$

If L is a lattice in F^n, the minimum product distance $\mathrm{d}_{\mathrm{p,min}}(L)$ of L is defined to be the infimum of the norms of all non-zero vectors in the lattice.

Definition 1.2.3. Let $v = (v_1, ..., v_n)$ be a vector in F^n. The *Euclidean norm* of v is

$$||v||_E = \sqrt{\sum_{i=1}^{n} |v_i|^2}.$$

If L is a lattice in F^n, the minimum product distance $\mathrm{d}_{\mathrm{p,min}}(L)$ of L is defined to be the infimum of the norms of all non-zero vectors in the lattice.

Suppose now we have a full lattice L in $\mathbb{R}^n$. We denote the measure (or hypervolume) of the fundamental parallelotope of the lattice L by $m(L)$. By saying that a lattice $L \in \mathbb{R}^n$ is orthogonal we mean that it has an orthogonal basis.

We can spread the vectors $v = (v_1, \ldots, v_n)$ of $\mathbb{C}^n$ to $2n$-tuples $\phi(v) \in \mathbb{R}^{2n}$ by replacing a complex number v_i with a 2-tuple with entries $\Re v_i$ and $\Im v_i$. The resulting mapping ϕ is clearly $\mathbb{R}$-linear and maps full $\mathbb{C}^n$ lattices to full $\mathbb{R}^{2n}$ lattices. We also have an equality $||v||_E = ||\phi(v)||_E$ and therefore ϕ is an isometry.

Suppose we now have a full complex lattice L in $\mathbb{C}^n$. We denote the measure (or hypervolume) of the fundamental parallelotope of the lattice $\phi(L)$ by $m(L)$ and we call it *the volume of the fundamental parallelotope* of the lattice L. By saying that a complex lattice is orthogonal we mean that the lattice $\phi(L)$ is orthogonal.

Let L be a full lattice in F^n. We denote by $\mathrm{Nd}_{\mathrm{p,min}}(L)$ the *normalized minimum product distance* of the lattice L, i.e. here we first scale L to have a unit size fundamental parallelotope and then take $\mathrm{d}_{\mathrm{p,min}}(L')$ of the resulting lattice.

Example 1.2.4. Suppose that L is a full lattice in $\mathbb{C}^n$ and $\mathrm{d}_{\mathrm{p,min}}(L) = a$. Then

$$\mathrm{Nd}_{\mathrm{p,min}}(L) = \mathrm{d}_{\mathrm{p,min}}\left(\frac{1}{m(L)^{1/2n}}L\right) = \frac{1}{m(L)^{1/2}}\mathrm{d}_{\mathrm{p,min}}(L) = \frac{a}{m(L)^{1/2}}.$$

Definition 1.2.5. Let us define *the optimal product distance* by

$$\mathrm{Nd}_{\mathrm{p,min}}(n) = \sup_L \mathrm{d}_{\mathrm{p,min}}(L),$$

where the supremum is taken over the set of full lattices in F^n normalized to unit fundamental parallelotope. Any full lattice L satisfying $\mathrm{Nd}_{\mathrm{p,min}}(L) = \mathrm{Nd}_{\mathrm{p,min}}(n)$ is said to have an *optimal product distance*.

Definition 1.2.6. If we have a full lattice L in the space $\mathbb{R}^n$, we denote the length of the shortest non-zero vector of this lattice with $\mathrm{sv}(L)$ and the *normalized shortest vector*

$$\frac{1}{m(L)^{\frac{1}{n}}}\mathrm{sv}(L)$$

by $\mathrm{Nsv}(L)$. We define *the longest possible shortest vector* by

$$\mathrm{Nsv}(n) = \sup_L(\mathrm{Nsv}(L)),$$

where the supremum is taken over the set of full lattices in $\mathbb{R}^n$.

1.3 Real lattices

We briefly describe a typical way to construct full real lattices by using algebraic number fields (see [3]). Let K be a totally real algebraic number field and $a \in K$ so-called *twisting element* that should be totally positive. Suppose now that $\sigma_1, \ldots, \sigma_n$

are the natural embeddings of the field K into $\mathbb{R}$. We set $\sigma_i(a) = \alpha_i$ and consider the mapping σ_a

$$\sigma_a(w) = (\sqrt{\alpha_1}\sigma_1(w), \ldots, \sqrt{\alpha_n}\sigma_n(w)).$$

It is well known that σ_a maps ideals of $\mathscr{O}_K$ into full lattices in $\mathbb{R}^n$. The following result was proved in [4].

Proposition 1.3.1. *Let K be a totally real algebraic number field, $a \in K$ a twisting element and b an element of the ring $\mathscr{O}_K$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma_a(b\mathscr{O}_K)) = \frac{1}{\sqrt{|d(K/\mathbb{Q})|}},$$

where $d(K/\mathbb{Q})$ is the discriminant of the extension $K/\mathbb{Q}$.

Example 1.3.2. Let us consider the field $\mathbb{Q}(\sqrt{3}) = K$ with the ring of integers $\mathbb{Z} \oplus \mathbb{Z}\sqrt{3}$. Buy choosing $a = b = 1$, we get that

$$\sigma_a(\mathscr{O}_K) = \sigma_a(\mathbb{Z} \oplus \mathbb{Z}\sqrt{3}) = \mathbb{Z}(1,1) \oplus \mathbb{Z}(\sqrt{3}, -\sqrt{3}).$$

Proposition 1.3.1 now states that

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma_a(\mathscr{O}_K)) = \frac{1}{\sqrt{|d(K/\mathbb{Q})|}} = \frac{1}{\sqrt{12}}.$$

When the twisting element is chosen to be 1, as was the case in this example, the canonical embedding is just the usual one from Minkowski's geometry of numbers.

One of the carrying themes in [4] was to pick the field K, the principal ideal $b\mathscr{O}_K$ and the twisting element a so that the corresponding lattice is orthonormal. What can be said of the minimum product distance of such lattices?

The best known general bound for $\mathrm{Nd}_{\mathrm{p,min}}(n)$ is due to Rogers [14, p. 615]. For small values of n it has the following form.

Theorem 1.3.3. *Let L be a full lattice in $\mathbb{R}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) < \frac{(1/2 + \ln(2))(n+1)n!}{n^n e^{n/2}}.$$

A simple but weaker bound that precedes the previous theorem is the following result by Hermann Minkowski [22, Theorem 2.13.4].

Theorem 1.3.4. *Let L be a full lattice in $\mathbb{R}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) \leq \frac{n!}{n^n}.$$

These results naturally also bound the minimum product distance of orthogonal lattices. However, if we concentrate on orthogonal lattices that are derived from totally real algebraic number fields we can apply Odlyzko's lower bounds to Proposition 1.3.1.

Proposition 1.3.5. *Let K be a totally real algebraic number field, $a \in K$ a twisting element and b an element of the ring $\mathcal{O}_K$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma_a(b\mathcal{O}_K)) \leq \frac{1}{\sqrt{|C_n^n|}},$$

where C_n is the Odlyzko bound in the totally real case.

We refer to this bound by $B_{Odlyzko}$. It was first proved in [4] and it is considerably better than the general bound of Theorem 1.3.3 by Rogers. It is also known that $B_{Odlyzko}$ is quite tight.

Now it seems that in order to construct orthogonal lattices with large minimum product distance, it is enough to find a totally real number field with minimal discriminant and then choose a suitable twisting element and ideal. At first this strategy is effective. When $n < 9$, the totally real number fields with the smallest discriminants are known and at least the 7 first fields have orthogonal principal ideals [4]. Also when n grows slightly, the orthogonal constructions seem to follow $B_{Odlyzko}$ rather closely (see [4]). However, this is not the trend when n grows.

Lemma 1.3.6. *Let L be a full lattice in $\mathbb{R}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) \leq \frac{Nsv(L)^n}{n^{n/2}}.$$

Proof. Let $x = (x_1, \ldots, x_n)$ be the shortest vector in L. Then

$$\left(\prod_{i=1}^{n} |x_i|^2\right)^{1/n} \leq \frac{\sum_{i=1}^{n} |x_i|^2}{n}$$

by the arithmetic-geometric inequality. Raising both sides to the power $n/2$ gives us the claim. □

Proposition 1.3.7. *Let L be an orthogonal lattice in $\mathbb{R}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) \leq \frac{1}{n^{n/2}}.$$

Proof. When an orthogonal lattice has a fundamental parallelotope of a unit measure, at least one of the vectors in an orthogonal basis has length at most 1. Lemma 1.3.6 now gives us the result. □

We refer to the bound of Proposition 1.3.7 by B_{ort}.

Corollary 1.3.8. *Let K be a totally real algebraic number field and $a \in K$ a twisting element. If $\mathcal{O}_K$ has an ideal B for which $\sigma_a(B)$ is orthogonal, then*

$$|d(K/\mathbb{Q})| \geq n^n.$$

Proof. It was noted in [4] that

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma_a(B)) \geq \mathrm{Nd}_{\mathrm{p,min}}(\mathcal{O}_K) = \frac{1}{\sqrt{|d(K/\mathbb{Q})|}}.$$

The claim now follows from Proposition 1.3.7. □

Example 1.3.9. Immediately when $n = 40$ and $B_{ort} < B_{Odlyzko}$ there exists a totally real field with root discriminant 39.457... [37]. Corollary 1.3.8 now states that this field cannot have an ideal that yields an orthogonal lattice with the construction described above.

In Figure 1.1 we have drawn $B_{Odlyzko}$ and B_{ort} for values less than 100. To ease the comparison we consider functions $(1/B_{Odlyzko})^{2/n}$ and $(1/B_{ort})^{2/n}$.

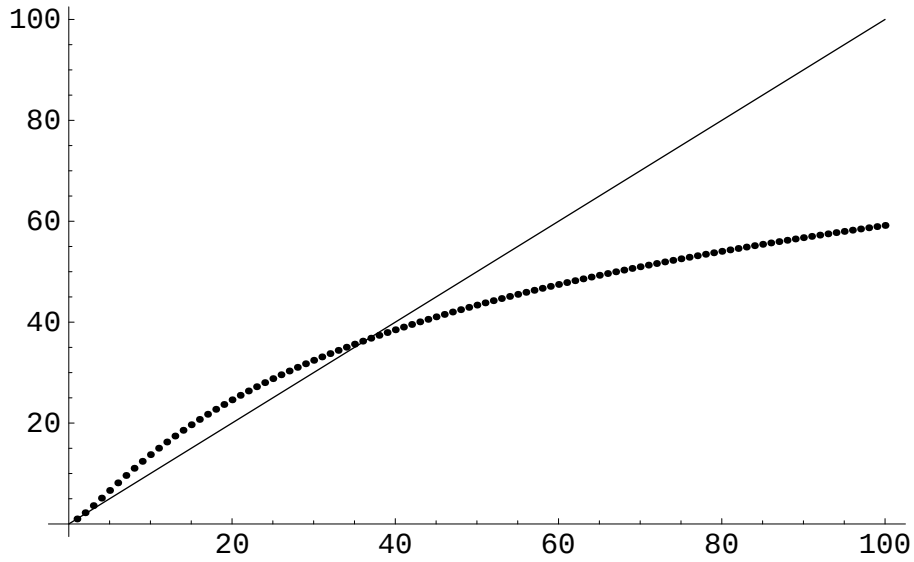


Figure 1.1: $(1/B_{Odlyzko})^{2/n}$ (dots) vs $(1/B_{ort})^{2/n}$ (solid)

The idea gotten from this figure is correct as

$$\lim_{n\to\infty}(B_{Odlyzko}(n))^{2/n} = \frac{1}{60.83...}$$

and

$$\lim_{n\to\infty}(B_{ort}(n))^{2/n} = 0.$$

We note that while the Odlyzko bound is tighter for small values of n the situation changes dramatically when n grows. The problem here is not the existence of totally real number fields with small discriminants, but that we cannot find an orthogonal ideal from these fields.

1.4 Complex lattices

In this section we are considering full lattices in $\mathbb{C}^n$. Again, we are interested in maximizing the product distance.

We briefly describe a method to construct full complex lattices with good product distance (see [4]). Let m be a square free positive integer, $K/\mathbb{Q}(\sqrt{-m})$ a Galois extension of degree n and $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-m})) = \{\sigma_1,\ldots,\sigma_n\}$. Then we can define a *relative canonical embedding* of K into $\mathbb{C}^n$ by

$$\sigma(x) = (\sigma_1(x),\ldots,\sigma_n(x)).$$

Every ideal of the ring $\mathscr{O}_K$ has a $\mathbb{Z}$-basis $W = \{w_1,\ldots,w_{2n}\}$. In Lemma 1.4.2 we show that $\sigma(W)$ is a $\mathbb{Z}$-basis for the full lattice $\sigma(\mathscr{O}_K)$.

Remark 1.4.1. We immediately see that $|nr_{K/\mathbb{Q}(\sqrt{-m})}(x)| = n(\sigma(x))$ and therefore $\mathrm{d}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = 1$.

Before we go further we note the following. Let $x_1,\ldots,x_{2n}$ be a set of vectors in $\mathbb{C}^n$. We can then form the Gram matrix G of the vectors $\phi(x_1),\ldots,\phi(x_{2n})$ by

$$G(\phi(x_1),\ldots,\phi(x_{2n})) = (\Re(x_i\overline{x}_j^T))_{(ij)}.$$

In particular, the vectors $\phi(x_1),\ldots,\phi(x_{2n})$ are linearly independent if and only if $\det(\Re(x_i\overline{x}_j^T)_{(ij)}) \neq 0$.

Lemma 1.4.2. *Let $K/\mathbb{Q}(\sqrt{-m})$ be a Galois extension of degree n and let σ be the relative canonical embedding. Then*

$$m(\sigma(\mathscr{O}_K)) = 2^{-n}\sqrt{|d(K/\mathbb{Q})|}.$$

Proof. We denote the field $\mathbb{Q}(\sqrt{-m})$ by F. Let $W = \{w_1,\ldots,w_{2n}\}$ be a $\mathbb{Z}$-basis for the ring $\mathscr{O}_K$ and let us consider the $2n\times 2n$ matrix M with $\phi(\sigma(w_i))$ as the rows. We can then write the Gram matrix G of the basis W as

$$G = MM^T = (\Re(\sigma(w_i)\overline{\sigma(w_j)^T}))_{(ij)}.$$

We also have that

$$MM_1^T = (\Re(\sigma(w_i)\sigma(w_j)^T))_{(ij)}.$$

where M_1^T has $\phi(\overline{\sigma(w_i)})$ as columns. We know that $tr_{F/\mathbb{Q}}(a) = 2\Re(a)$ and therefore

$$MM_1^T = (\Re(tr_{K/F}(w_i w_j)))_{(ij)} = (2^{-1} tr_{F/\mathbb{Q}}(tr_{K/F}(w_i w_j)))_{(ij)}.$$

This implies

$$\det(MM_1^T) = 2^{-2n} d(K/\mathbb{Q}).$$

It is also easily seen that

$$|\det(M^T)| = |\det(M_1^T)|$$

and therefore

$$|\det(G)| = |\det(MM_1^T)| = |2^{-2n} d(K/\mathbb{Q})|.$$

□

Proposition 1.4.3. *With the notation of Lemma 1.4.2*

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = \frac{2^{n/2}}{|d(K/\mathbb{Q})|^{1/4}} = \frac{2^{n/2}}{|d(F/\mathbb{Q})|^{n/4}\sqrt{|d(K/F)|}}.$$

Proof. In order to scale $\sigma(\mathscr{O}_K)$ to have a fundamental parallelotope of size one we have to scale it with the factor $1/m(\sigma(\mathscr{O}_K))^{1/2n}$. On the other hand we know that $\mathrm{d}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = 1$. Therefore

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = \mathrm{d}_{\mathrm{p,min}}\left(\left(\frac{1}{m(\sigma(\mathscr{O}_K))}\right)^{1/2n}\sigma(\mathscr{O}_K)\right) = \frac{1}{m(\sigma(\mathscr{O}_K))^{1/2}}.$$

The first equality now follows from Lemma 1.4.2. The last equality follows from Lemma 1.1.12 as

$$|d(K/\mathbb{Q})| = |d(F/\mathbb{Q})^n d(K/F)^2|.$$

□

Remark 1.4.4. The last result generalizes [4, Theorem 5.1] and proves that in order to maximize the product distance one should simply search for totally complex fields with minimal discriminants.

Example 1.4.5. Let us consider the extension K/F where $K = \mathbb{Q}(i, \sqrt{-3})$ and $F = \mathbb{Q}(i)$. It is easily calculated that $|d(\mathbb{Q}(i, \sqrt{-3})/\mathbb{Q}(i))| = 3$. Proposition 1.4.3 then gives us

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = \frac{1}{\sqrt{3}} = 0.577\ldots.$$

For a comparison in [13] the authors considered an extension $K^*/\mathbb{Q}(i)$ where $K^* = \mathbb{Q}(\zeta_8)$. In [4] it was proved that the resulting lattice $\sigma(\mathscr{O}_{K^*})$ is orthogonal and that $\mathrm{d}_{\mathrm{p,min}}(\sigma(\mathscr{O}_{K^*}) = 1/2$. The lattice $\sigma(\mathscr{O}_K)$ was also constructed in [45]. The significant point here is that the lattice $\sigma(\mathscr{O}_K^*)$ reaches the bound of Corollary 1.4.10 and that $\sigma(\mathscr{O}_K)$ clearly exceeds it.

Example 1.4.6. Let us consider the field $F = \mathbb{Q}(\omega)$, where $\omega = (-1+\sqrt{-3})/2$, and an extension $F(a)/F$ where a is a zero of the polynomial $f_a = x^2 + (-\omega - 1)x + (\omega + 1)$. This extension was found in [8] where the authors were searching for totally complex fields with minimal discriminants. They also proved that the extension $F(a)/F$ is Galois and that the extension $F(a)/\mathbb{Q}$ has discriminant $3^2 \cdot 13$. By Proposition 1.4.3

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_{F(a)})) = 0.608\ldots.$$

As far as we know, this is the best full complex lattice of degree two. By considering the relative discriminant $d(F(a)/F)$ and the discriminant of the polynomial f_a we see that $\{1,a\}$ is a $\mathbb{Z}[\omega]$-basis for the ring $\mathscr{O}_{F(a)}$. This implies that

$$W = \{1, \omega, a, \omega a\}$$

is a $\mathbb{Z}$-basis of the ring $\mathscr{O}_{F(a)}$ and the $\mathbb{Z}$-basis for $\sigma(\mathscr{O}_{F(a)})$ is

$$\sigma(W) = \{\,(1,1),\,(\omega,\omega),\,(a,\sigma_1(a)),\,(\omega a,\omega\sigma_1(a))\,\}, \tag{1.2}$$

where σ_1 is the generator of the Galois group $\mathrm{Gal}(F(a)/F)$. Solving the equation $f_a = 0$, we get that $a = -0.121744 + 1.30662i$ and $\sigma_1(a) = 0.621744 - 0.440597i$. Substituting these complex numbers to (1.2) gives us a concrete lattice basis for the lattice $\sigma(\mathscr{O}_{F(a)})$.

Example 1.4.7. The field $\mathbb{Q}(i) = F$ has an abelian extension $F(a)$, where a is a zero of the polynomial $f_a(x) = x^4 + (-i+2)x^3 + (-i+1)x^2 + (-i+1)x - i$. Again this field is from [8]. The extension $F(a)/\mathbb{Q}$ has discriminant $2^8 17^3$. We now have

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_{F(a)})) = 0.11944\ldots.$$

In [4] the authors used the method just described to produce so-called "rotated" $\mathbb{Z}[i]$-lattices that are easily seen to be full orthogonal lattices in $\mathbb{C}^n$. In order to determine the normalized product distance and achieve the orthogonal shape they had to restrict their constructions to cases where K is a CM-field. Then they compared the normalized product distance of their lattices to the Odlyzko bound for discriminant, and conclude that their constructions are far away from the bound. The following results shed light into this question. The proofs are analogous to those in the real case.

Proposition 1.4.8. *Let $K/\mathbb{Q}(\sqrt{-m})$ be a Galois extension of degree n and let σ be the relative canonical embedding. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(\sigma(\mathscr{O}_K)) = \frac{2^{n/2}}{|d(K/\mathbb{Q})|^{1/4}} \leq \left(\frac{2}{|C_{2n}|}\right)^{n/2},$$

where C_{2n} is the Odlyzko's bound in a totally complex case.

Proposition 1.4.9. *Let L be a full lattice in $\mathbb{C}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) \leq \frac{Nsv(\phi(L))^n}{n^{n/2}}.$$

Corollary 1.4.10. *Let L be a orthogonal full lattice in $\mathbb{C}^n$. Then*

$$\mathrm{Nd}_{\mathrm{p,min}}(L) \leq \frac{1}{n^{n/2}}.$$

We can now conclude that the previously described behavior was not only due to CM-fields, which tend to have big discriminants, but the fact that the rotated $\mathbb{Z}[i]$-lattices are orthonormal full lattices in $\mathbb{C}^n$ and therefore Corollary 1.4.10 bounds the product distance of such lattices. Actually, some of the existing constructions [4, 13], namely when n is a power of two, attain the bound of Corollary 1.4.10. In Figure 1.2 we present the bounds $B_{Odlyzko}$ and B_{ort} for values less than 50. In contrast to the real case the product distance of best orthogonal and non-orthogonal lattices begin to differ from the start.

Remark 1.4.11. It is an easy task to use tables of fields with minimal discriminants to create full diversity complex lattices for any n. For the first few values of n that we tried, the corresponding lattices had better product distances than the lattices in [45] and [4]. This is not a big surprise as in [45] the authors are considering only cyclotomic fields, in [4] only CM-fields and rotated $\mathbb{Z}[i]$-lattices and in [10] fields that are compositums of certain extensions of $\mathbb{Q}$. Proposition 1.4.3 is the key for our improvements as it allows us to compare discriminants of any kind of totally complex fields. It is clear that the normalized product distance of orthogonal codes can never reach that of the best non-orthogonal codes. This raises the relevant question, whether the benefits of the orthogonal shape are enough to cover the loss in the product distance.

Remark 1.4.12. Results and definitions in Sections 1.1 and 1.2 are well known, although the definition of the normalized product distance for complex lattices is slightly more general than the one usually used (see [45, 4, 10]). In Section 1.3 Lemma 1.3.6 is trivial, and similar ideas have been widely used (see [9, Chapter 8, Section 7, Theorem 8]). However the applications in Proposition 1.3.7 and Corollary 1.3.8 are first time proposed in this thesis. In Section 1.4 Proposition 1.4.10,

Lemma 1.4.2 and Proposition 1.4.3 are new results. One should note that Lemma 1.4.2 and Proposition 1.4.3 are generalizations of similar results in [45, 4] and [10]. Proposition 1.4.8 is a straightforward generalization of the corresponding result in [4].

Remark 1.4.13. During the pre-examination process of this thesis Chaoping Xing published and article in November 2007 issue of IEEE Transactions on Information Theory [46]. Xing's article includes Proposition 1.4.3, although with out a proof, and the corresponding Examples 1.4.6 and 1.4.7, that were, during the writing of this thesis, the best known. He also use the relation between geometric and product distance and give the corresponding general bounds. The effect of orthogonality to product distance or the comparison to Odlyzko's bound is not discussed in his paper.

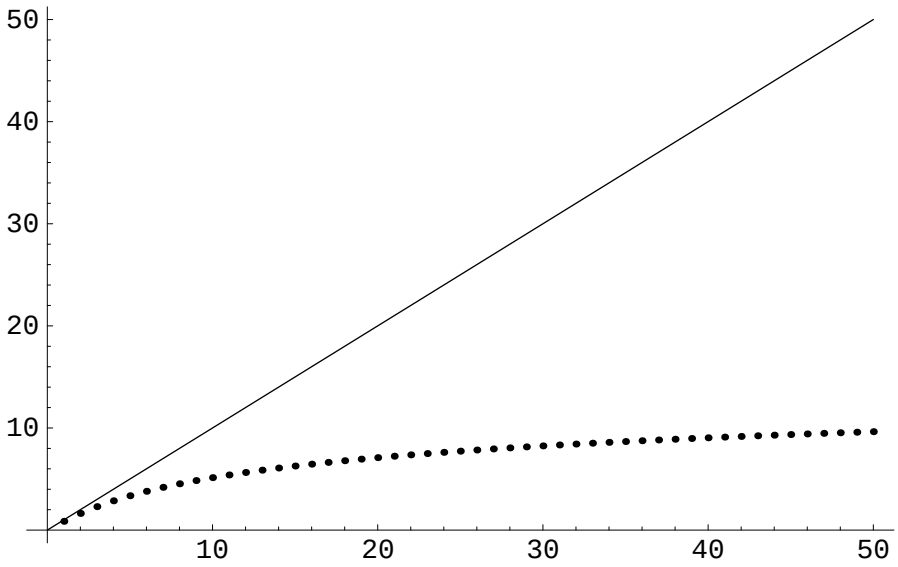


Figure 1.2: $(1/B_{Odlyzko})^{2/n}$ (dots) vs $(1/B_{ort})^{2/n}$ (solid)

Chapter 2

MIMO codes

In this chapter we discuss infinite, square, fully multiplexing MIMO codes which are full lattices in $M_n(\mathbb{C})$. For such codes, the coding gain is one of the main code design criterions. In the following we explore the question of optimal coding gain. First in the general case and later in the case where the code is derived from an order of a division algebra. This study does not only result in general bounds for coding gain, but also proves the existence of MIMO codes with the best known coding gain.

2.1 Coding theoretic preliminaries

In this section we give an informal introduction to some of the basics of space-time coding. For proper introduction and for definition of several used notions we refer the reader to [42].

We are interested in the coherent multiple input-multiple output (MIMO) case where the receiver perfectly knows the channel coefficients. We also suppose that the quasi-static interval and number of transmit and receiving antennas are all equal. The received signal is then

$$\mathbf{Y}_{n\times n} = \sqrt{\rho}\mathbf{H}_{n\times n}\mathbf{X}_{n\times n} + \mathbf{N}_{n\times n},$$

where $\mathbf{H}$ is the channel matrix whose entries are independent identically distributed (i.i.d.) zero-mean complex circular Gaussian random variables with the variance 1, and $\mathbf{N}$ is the noise matrix whose entries are i.i.d. zero-mean complex circular Gaussian random variables with the variance 1. The matrix $\mathbf{X}$ is the transmitted codeword taken from the code $C \subset \mathscr{M}_n(\mathbb{C})$ that satisfies the overall power constraint

$$\frac{1}{|C|} \cdot \sum_{X\in C} ||X||_F^2 = n, \tag{2.1}$$

where $\|X\|_F = \sqrt{tr(XX^H)}$ is the Frobenius norm. We then easily see that the parameter ρ presents the average SNR (signal-to-noise ratio) at the receiving antennas.

Assume that the receiver has to decide (based on the Euclidean metric), whether X or X' was transmitted. For large values of ρ the probability P_e that the receiver makes an error between X and X' is

$$P_e \approx \frac{1}{\det((X-X')(X-X')^H)\rho^n}.$$

This gives us a natural code design criteria. From the pairwise error probability (PEP) point of view [42], the performance of a space-time code is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of the rank of the difference matrix $X - X'$ taken over all distinct code matrices $X, X' \in C$, also called the *rank* of the code C. When C is full-rank, the coding gain is proportional to the determinant of the matrix $(X-X')(X-X')^H$. The minimum of this determinant taken over all distinct pairs of code matrices is called the *coding gain* of the code C.

Remark 2.1.1. When we are discussing the coding gain of a finite code we always suppose that the code is scaled so that overall energy constraints in (2.1) is met. This normalization allows us to reasonably compare two finite codes of same size.

In order to assist the decoding it is beneficial that C is carved from a free lattice $C_\infty \subset M_n(\mathbb{C})$ by choosing $|C|$ matrices with smallest energy. To maximize the transmission rate we only consider full rank lattices that have a basis $x_1, x_2, \ldots, x_{2n^2}$ consisting of matrices that are linearly independent over the field of real numbers. We explain this in detail in Remark 2.1.4.

Definition 2.1.2. From now on when we talk about MIMO codes we refer to the code C_∞ that is a full lattice in $M_n(\mathbb{C})$.

The next lemma proves that our definition for MIMO codes leads us to codes with *full multiplexing gain* (see [12] and [47] for definition).

Lemma 2.1.3. *Let L be a full lattice in $M_n(\mathbb{C})$ and*

$$L_r = \{a \,|\, a \in L, \, ||a||_F \leq \sqrt{nr}\},$$

then

$$\lim_{r\to\infty} \frac{\log |L_r|}{\log \sqrt{nr}} = n^2.$$

Proof. This result is easy to see by considering the real lattice $\phi(L) \in \mathbb{R}^{2n^2}$. We then have that

$$\phi(L_r) = \{\, \phi(a) \,|\, a \in L, \, ||\phi(a)||_E \leq \sqrt{nr}\,\},$$

and therefore $|\phi(L_r)| = |L_r|$ is the number of lattice points of a full lattice inside a ball of radius $\sqrt{nr}$ in $\mathbb{R}^{2n^2}$. It is then a known fact that

$$\lim_{r\to\infty} \frac{\log|L_r|}{\log\sqrt{nr}} = n^2.$$

□

Remark 2.1.4. The full multiplexing gain can be considered as a direct generalization of the concept of *full rate*. Suppose that we have a complex quadratic field F and suppose that we have a $\mathcal{O}_F$-lattice L in $M_n(\mathbb{C})$, such that L has a basis of n^2 elements $\{e_1,...,e_{n^2}\}$ that are linearly independent over F.

Then the elements x of L take the form $x = \sum_{k=1}^{n^2} e_k f_k$, where $f_k \in \mathcal{O}_F$ for all $k = 1,...,n^2$. Hence n^2 complex symbols ($\in \mathcal{O}_F$) are transmitted in one block (matrix). In literature this is often referred to as having a *full rate*. It is then clear that L is also a full lattice in $M_n(\mathbb{C})$ and by our previous considerations has full multiplexing gain.

When we are considering the performance of an infinite MIMO code we are actually discussing the performance of an infinite family of finite codes. However, the lattice structure of the infinite code allows us to predict the coding gain of these finite codes.

Let us suppose that we have a MIMO code $L \subset M_n(\mathbb{C})$ and we pick a finite code C from L by choosing $|C|$ matrices with the smallest energy. For the actual code we then have to scale the code C with constant c so that the overall energy constraints (2.1) is fulfilled. If we use relatively high SNR ρ for the transmission, we get that the error probability P_e that the receiver makes an error between X and X' is

$$P_e \approx \frac{1}{\det((cX - cX')(cX - cX')^H)\rho^n}.$$

The code C is derived from the lattice L and therefore $X - X' = X_1 \in L$. That is

$$P_e \approx \frac{1}{c^{2n}|\det(X_1)|^2\rho^n}. \tag{2.2}$$

Definition 2.1.5. The minimum determinant $\det_{min}(L)$ of the lattice L is defined to be the infimum of the absolute values of the determinants of all non-zero matrices in the lattice.

We now see that the minimum determinant of the MIMO lattice L bounds the coding gain of the finite codes derived from L. Following [12] it is therefore reasonable to insist on the non-vanishing determinant (NVD) property $\det_{min}(L) > 0$.

Theorem 3 in [12] with Lemma 2.1.3 proves that MIMO lattices with NVD achieve the optimal diversity-multiplexing trade-off from [47]. The D-MG tradeoff shows that all MIMO codes (in the sense of this thesis) with NVD property are

optimal, but only in a very coarse asymptotic sense when the SNR and the size of the code simultaneously grows to infinity (see [47] for definitions). When we consider codes that are used in practice the code size is finite and so is the SNR. Therefore we have to find other methods to decide which of these D-MG optimal codes are the best. Here the traditional PEP oriented coding gain comes to use. While it is not a perfect code design criteria, as it only considers PEP and not the actual error probability, it has predicted the performance of those codes we have tested surprisingly well. So from now on we focus on PEP and our take on MIMO codes is coding gain oriented.

2.1.1 Normalized minimum determinant and coding gain

In the definition of the coding gain for finite code we require that the overall energy constraint (2.1) is met. This normalization allows us to reasonably compare two finite codes. In the following we present a similar normalization for infinite MIMO codes.

In the following we only consider MIMO lattices L, where L is full in $M_n(\mathbb{C})$. We can flatten the matrices A of $M_n(\mathbb{C})$ to $2n^2$ vectors $\phi(A) \in \mathbb{R}^{2n^2}$ by first forming a vector of length n^2 out of the entries (e.g. row by row) and then replacing a complex number z with the pair of its real and imaginary parts $\Re z$ and $\Im z$. This mapping ϕ is clearly $\mathbb{R}$-linear and maps full $M_n(\mathbb{C})$ lattices to full $\mathbb{R}^{2n^2}$ lattices. We also have the equality $||A||_F = ||\phi(A)||_E$ and therefore ϕ is also an isometry.

Definition 2.1.6. We say that a lattice L in $M_n(\mathbb{C})$ is orthogonal or rectangular if the corresponding real lattice $\phi(L)$ is orthogonal.

We denote the measure (or hypervolume) of the fundamental parallelotope of the lattice $\phi(L)$ with $m(L)$ and we call it the *volume of the fundamental parallelotope of the lattice* L. If $x_1, \ldots, x_{2n^2}$ is a basis of L, we can form a matrix M by using vectors $\phi(x_i)$ as column blocks. Then the *Gram matrix* of the lattice L is

$$G(L) = MM^T = \left(\Re tr(x_i x_j^H)\right)_{1 \le i,j \le 2n^2},$$

where H indicates the complex conjugate transpose of a matrix. The Gram matrix then has a positive determinant equal to $m(L)^2$.

Any full lattice L can be scaled (i.e. multiplied by a real constant r) to satisfy $m(L) = 1$. As the minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a lattice. We shall denote by $\delta(L)$ the *normalized minimum determinant* of the lattice L, i.e. here we first scale L to have a unit size fundamental parallelotope. A simple computation shows that if a is the minimum determinant of the lattice L before the scaling, after the scaling it is

$$\delta(L) = \frac{a}{m(L)^{1/2n}}. \tag{2.3}$$

Definition 2.1.7. Let L be a full lattice in $M_n(\mathbb{C})$ having NVD. We then refer to $\delta(L)^2$ as the coding gain of the lattice L.

Definition 2.1.8. Let us define the optimal minimum determinant by

$$\delta(n) = \sup_L \delta(L),$$

where the supremum is taken over the set of lattices of rank $2n^2$ inside $M_n(\mathbb{C})$ normalized to unit fundamental parallelotope. Any lattice L satisfying $\delta(L) = \delta(n)$ is said to have the optimal minimum determinant.

To shorten the notation we write $\mathrm{sv}(L) = \mathrm{sv}(\phi(L))$ and $\mathrm{Nsv}(L) = \mathrm{Nsv}(\phi(L))$, when L is a full lattice in $M_n(\mathbb{C})$. The reader can recall the definition for the shortest vector from Chapter 1.

Remark 2.1.9. Section 2.1 mainly consists of well known theory. The only exception is the definition for the normalized minimum determinant which is slightly more general than the one usually used (see for example [30]). The definition was given in [23].

2.2 General bounds

Ever since it was discovered that orders of division algebras can be used to generate MIMO codes, several code constructions have been proposed. Still there does not exist any bounds for the normalized minimum determinant.

In this section we study the relation between the shortest vector and the minimum determinant of a MIMO lattice. With the help of a simple inequality we get a relation where the Frobenius norm of the matrix bounds the size of the determinant. This connection then allows us to bound the minimum determinant of a MIMO lattice with the help of sphere packing bounds. While in general case the achieved bound is not very tight, it works very well when we are considering MIMO lattices that have certain shape. These simple results give us good bounds for the coding gain of the so-called *perfect codes* (see [30] and [11]). We return to this question in Section 3.2.

Lemma 2.2.1. *Let A be an $n \times n$ complex matrix. We have the inequality*

$$|\det A| \leq \frac{\|A\|_F^n}{n^{n/2}}.$$

Proof. Let A_j, $j = 1, 2, \ldots, n$, be the rows of A. By the Hadamard inequality

$$|\det A| \leq \prod_{j=1}^{n} \|A_j\|_E.$$

Squaring this inequality and using the fact that $\|A\|_F^2 = \sum_{j=1}^{n} \|A_j\|_E^2$ together with the well-known inequality between the geometric and arithmetic means of n positive numbers give the claimed bound. □

Lemma 2.2.2. *Suppose we have a full lattice L in $M_n(\mathbb{C})$. Then*

$$\det_{\min}(L) \leq \left(\frac{\mathrm{sv}(L)^2}{n}\right)^{n/2}.$$

Proof. The result is direct consequence of Lemma 2.2.1.

□

Corollary 2.2.3. *For full lattices in $M_n(\mathbb{C})$ we have an upper bound*

$$\delta(n) \leq \left(\frac{\mathrm{Nsv}(2n^2)^2}{n}\right)^{n/2}.$$

Corollary 2.2.4. *If L is a rectangular MIMO lattice in $M_n(\mathbb{C})$. Then*

$$\delta(L) \leq \frac{1}{n^{n/2}}.$$

Proof. When a rectangular lattice has a fundamental parallelotope of unit measure, at least one of the vectors in an orthogonal basis has length at most 1. The determinant of such a matrix is at most $1/n^{n/2}$ by Lemma 2.2.1. □

Corollary 2.2.5. *Let L be a full lattice in $M_n(\mathbb{C})$ and suppose that $\phi(L)$ has shape $A_2^{n^2}$, where A_2 is the hexagonal lattice, then*

$$\delta(n) \leq \left(\frac{2}{\sqrt{3}n}\right)^{n/2}.$$

Proof. The lattice $\phi(L)$ is a direct sum of n^2 copies of A_2. If we suppose that $\phi(L)$ has a fundamental parallelotope of size 1, then all the copies of A^2 in the sum must have a fundamental parallelotope equal to one. Knowing that $\mathrm{Nsv}(A_2) = (2/\sqrt{3})^{1/2}$ the lemma 2.2.2 gives us the claim.

□

Example 2.2.6. The root lattice E_8 has the best minimum distance among 8-dimensional lattices (cf. e.g. [9]). When we scale its fundamental parallelotope to have unit measure, the shortest vectors have length $\sqrt{2}$. In other words, any lattice L of rank 8 inside $M_2(\mathbb{C})$ has a non-zero matrix A with $\|A\|_F \leq \sqrt{2}$. Lemma 2.2.1 then tells us that $|\det A| \leq 1$.

For lattices finding the value of $\mathrm{Nsv}(n)$ is equivalent for finding the density of the densest lattice packing. This is generally a very hard problem and the actual value of $\mathrm{Nsv}(n)$ is known only for some values of n. However, there exist some general bounds (see [9]). We refer to the best known bound for $\mathrm{Nsv}(n)$ by $\mathrm{Bsv}(n)$. Corollary 2.2.3 translates this bound into a bound for the minimum determinant. We refer to the resulting bound as $\mathrm{B}\delta(n)$.

Finally, Proposition 2.2.4 gives us the bound $\mathrm{B}_{\mathrm{ort}}$ for the minimum determinant of the orthogonal lattices and Corollary 2.2.5 the bound B_{hex} for $A_2^{n^2}$-lattices.

Remark 2.2.7. Albeit Lemma 2.2.2 is extremely simple it reveals one fundamental fact of MIMO codes. A MIMO code with small Euclidean distance cannot have good coding gain. One should still remember that a good Euclidean distance does not assure that a code has good coding gain.

Remark 2.2.8. The results in Section 2.2 are from [23].

2.3 Central simple algebras

The cyclic division algebras (Definition 2.3.7) are the main object of interest for us, but in order to fully understand these algebras we have to widen our view and consider a larger class of algebras. As we will see the class of *central simple algebras* (Definition 2.3.4) is a proper context for our theory.

In this section we give a short introduction into the theory of central simple algebras. The proofs for the following results can be found from a nice book by Irving Reiner [34].

Definition 2.3.1. Let F be any field and assume that E/F is a cyclic Galois extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. We can now define an associative F-algebra

$$\mathscr{A} = (E/F, \sigma, \gamma) = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathscr{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. We call this type of algebra *cyclic algebra*.

Example 2.3.2. The extension $\mathbb{C}/\mathbb{R}$ is a Galois extension of degree two. The algebra

$$\mathbf{H} = (\mathbb{C}/\mathbb{R}, \sigma, -1),$$

where σ is the complex conjugation, is a cyclic algebra called the *quaternion algebra*.

Definition 2.3.3. An algebra $\mathscr{A}$ is called *simple* if it has no non-trivial ideals. An F-algebra $\mathscr{A}$ is *central* if its center $Z(\mathscr{A}) = \{a \in \mathscr{A} \mid aa' = a'a \ \forall a' \in \mathscr{A}\} = F$.

Definition 2.3.4. A *central simple* F-algebra is a simple algebra which is finite dimensional over its center F.

Proposition 2.3.5. *Every cyclic algebra is central simple.*

Also the reverse is true if we are considering F-central simple algebras, where F is an algebraic number field.

Theorem 2.3.6. *Let F be an algebraic number field. Every F-central simple algebra is cyclic.*

Definition 2.3.7. A central simple F-algebra $\mathscr{A}$ is a division algebra if every non-zero element of $\mathscr{A}$ is invertible.

The next proposition due to A. A. Albert [2, Theorem 11.12, p. 184] tells us when a cyclic algebra is a division algebra.

Proposition 2.3.8 (Norm condition). *The cyclic algebra $\mathscr{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbb{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.*

Due to the above proposition, the element γ is often referred to as the *non-norm element*.

Example 2.3.9. Let us consider the quaternion algebra $\mathbf{H}$. The norm map in the extension $\mathbb{C}/\mathbb{R}$ is $nr_{\mathbb{C}/\mathbb{R}}(a) = a\overline{a}$, when $a \in \mathbb{C}$. It is then easily seen that $nr_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*) = \mathbb{R}^+$. This shows that -1 is not in the image of the norm map and therefore we recover the known fact that $\mathbf{H}$ is a division algebra.

The following simple result, is a slight generalization to [21, Theorem 1]. We denote the multiplicative ideal group of the field F by $(I_F)^*$.

Lemma 2.3.10. *Suppose that F is a P-adic field or an algebraic number field. Let E be a Galois extension of F and let P be a prime ideal of $\mathscr{O}_F$ that lies under the prime B of the ring $\mathscr{O}_E$. If the inertial degree of P in the extension E/F is f and γ is such an element of F that $(v_P(\gamma), f) = 1$, then $\gamma^i \notin N_{E/F}(E)$ for any $i = 1, 2, \ldots, f-1$.*

Proof. The ideal norm of B is $N_{E/F}(B) = P^f$, where f is the inertial degree of P in the extension E/F. It is clear that the group $N_{E/F}((I_F)^*)$ is generated by the norms of prime ideals and that $\{N_{E/F}(a)\mathscr{O}_F \,|\, a \in E^*\} \subseteq N_{E/F}((I_F)^*)$. Therefore $f | v_P(N_{E/F}(a)\mathscr{O}_F)$ for all $a \in E$. □

We are most interested in cyclic division algebras $\mathscr{A}$ where the center F is an algebraic number field. However, in order to understand these algebras we have

to consider the localizations of the algebra $\mathscr{A}$. These localizations force us out of the world of simple division algebras.

If F' is an extension field of F and $\mathscr{A}$ is a central simple F-algebra, then the tensor product $\mathscr{A}' = \mathscr{A} \otimes_F F'$ is a central simple F'-algebra. We refer to this algebra as the algebra obtained from $\mathscr{A}$ by *extending the scalars to* F'.

Definition 2.3.11. Let F be an algebraic number field that is finite dimensional over $\mathbb{Q}$ and let P be some prime of F. If $\mathscr{A}$ is an F-central simple algebra, then we call the algebra $\mathscr{A}_P = F_P \otimes_F \mathscr{A}$ *the localization* of $\mathscr{A}$ at P.

Proposition 2.3.12. *With the notation of the previous definition*

$$[\mathscr{A} : F] = [\mathscr{A}_P : F_P].$$

The theorem of Wedderburn reduces the classification of central simple algebras to the case of division algebras.

Theorem 2.3.13 (Wedderburn). *If $\mathscr{A}$ is an F-central simple algebra then*

$$\mathscr{A} \simeq M_n(\mathscr{D}),$$

where $\mathscr{D}$ is some F-central division algebra. The integer n and the algebra $\mathscr{D}$ are uniquely determined (up to isomorphism).

Definition 2.3.14. Let $\mathscr{A}$ be the algebra of the previous theorem. We call $\text{index}[\mathscr{A}] = \sqrt{[\mathscr{D} : F]}$ *the index* of the algebra $\mathscr{A}$. We note that the index is always an integer.

Definition 2.3.15. Let $\mathscr{A}$ be an F-central simple algebra. We then call

$$\sqrt{[\mathscr{A} : F]}$$

the degree of the algebra.

Remark 2.3.16. One should note that an F-central simple algebra $\mathscr{A}$ is a division algebra if and only if $\text{index}[\mathscr{A}] = \sqrt{[\mathscr{A} : F]}$.

Theorem 2.3.13 gives us that $F_P \otimes_F \mathscr{A} \simeq M_s(\mathscr{D}_P)$, where $\mathscr{D}_P$ is some F_P-central division algebra. This leads us to consider the division algebras where F_P is some completion of F.

The following theorem classifies the cases where P is infinite.

Theorem 2.3.17. *There is only two $\mathbb{R}$-central division algebras* **H** *and $\mathbb{R}$. The only $\mathbb{C}$-central division algebra is $\mathbb{C}$ itself.*

Let F be an algebraic number field that is finite dimensional over $\mathbb{Q}$ and let P be a finite prime of F.

Proposition 2.3.18. *The cyclic algebra*

$$\mathscr{A}(n,r) = (E/F_P, \sigma, \pi^r), \quad (r,n) = 1 \quad 0 \leq r < n,$$

where E is the unique unramified extension of F_P of degree n, σ is the Frobenius automorphism, and π is a prime element of F_P, is a division algebra. The algebras $\mathscr{A}(n,r_1)$ and $\mathscr{A}(n,r_2)$ are isomorphic if and only if $r_1 = r_2$.

Theorem 2.3.19. *Let $\mathscr{A}$ be a F_P-central division algebra of index n. Then*

$$\mathscr{A} \simeq \mathscr{A}(n,r)$$

for some r.

Definition 2.3.20. Let $\mathscr{A}$ be the F_P-central division algebra at the previous theorem. We call the rational number $\text{inv}[\mathscr{A}] = \frac{r}{n}$ the Hasse invariant of $\mathscr{A}$.

Definition 2.3.21. We define that the Hasse invariant inv[**H**] of **H** is $\frac{1}{2}$. We also define inv[$\mathbb{R}$]=0 and inv[$\mathbb{C}$]=0.

Now we are ready to define the following.

Definition 2.3.22. Suppose that F is an algebraic number field and P some prime of F. Let $\mathscr{A}$ be an F-central simple algebra and

$$F_P \otimes_F \mathscr{A} = M_{\kappa_p}(\mathscr{D}_P),$$

where $\mathscr{D}_P$ is a F_P-central division algebra. We refer to $inv[\mathscr{D}_P] = h_P = r_P/m_P$ as the Hasse invariant of $\mathscr{A}$ at P and to m_P as the *local index*. The integer κ_P is referred to as the *local capacity* (at P).

Remark 2.3.23. The fact that the local capacity and Hasse invariants are well defined follows from the uniqueness part of Theorem 2.3.13.

Note that $m_P = 1$ if and only if

$$\mathscr{A}_P \simeq M_{\kappa_P}(F_P).$$

We say that a prime P is ramified in the algebra $\mathscr{A}$ if the corresponding local index is not 1.

Theorem 2.3.24. *Let $\mathscr{A}$ be an F-central simple algebra. There exist only a finite set $\{P_1, \ldots, P_n\}$ of primes in F that have non-zero Hasse invariants and*

$$\text{index}[\mathscr{A}] = LCM\{m_{P_i}\}.$$

Corollary 2.3.25. *Suppose that $\mathscr{A}$ is an F-central simple algebra of degree n. If $\mathscr{A}$ has such a local index m_P that*

$$m_P = n,$$

then $\mathscr{A}$ is a division algebra.

2.3.1 Brauer group

In order to get a better grip of the central simple algebras it is beneficial to consider them as elements in a group. This deceivingly simple step, taken by Richard Brauer, gives us a great insight on central simple algebras.

Proposition 2.3.26. *Let $\mathscr{A}$ and $\mathscr{B}$ be F-central simple algebras. Then $\mathscr{A} \otimes_F \mathscr{B}$ is an F-central simple algebra.*

Let us now consider the family of all F-central simple algebras. Two central simple F-algebras $\mathscr{A} = M_n(\mathscr{D}_{\mathscr{A}})$ and $\mathscr{B} = M_s(\mathscr{D}_{\mathscr{B}})$ are said to be *similar*, if $\mathscr{D}_{\mathscr{A}} \simeq \mathscr{D}_{\mathscr{B}}$. We refer to a similarity class of a central simple algebra $\mathscr{A}$ with $[\mathscr{A}]$.

Similarity classes of F-central simple algebras form a group (under tensor product over F), called the *Brauer group* $\mathrm{Br}(F)$ of the field F. The identity element of $\mathrm{Br}(F)$ is the similarity class of F and the inverse of the element $[\mathscr{A}] \in \mathrm{Br}(F)$ is the similarity class of the *opposite algebra* $\mathscr{A}^{opp}$.

Theorem 2.3.27. *Let F be an algebraic number field and suppose that $\mathscr{A}$ and $\mathscr{B}$ are F-central simple algebras. Then*

$$\mathscr{A} \sim \mathscr{B} \Longleftrightarrow \mathscr{A}_P \sim \mathscr{B}_P \quad \forall P \in F.$$

This theorem now allows us to introduce the following map.

Lemma 2.3.28. *Let $\mathscr{A}$ be an$F$-central simple algebra where F is an algebraic number field and P a prime in F. Then the map defined by*

$$\mathscr{A} \longmapsto F_P \otimes_F \mathscr{A},$$

is a group homomorphism from $\mathrm{Br}(F)$ *to* $\mathrm{Br}(F_P)$.

Following theorem gives us a concrete view on the previous map.

Theorem 2.3.29. *Suppose that L/F is a cyclic Galois extension,* $\mathrm{Gal}(L/F) = \langle \sigma \rangle$ *and $a \in F^*$. Let E be any field containing F, and let EL be the compositum of E and L in some larger field containing both E and L. We may write*

$$H = \langle \sigma^k \rangle = \mathrm{Gal}(L/L \cap E) \simeq \mathrm{Gal}(EL/E),$$

where k is the least positive integer such that σ^k fixes $L \cap E$. Then

$$E \otimes_F (L/F, \sigma, a) \sim (EL/E, \sigma^k, a).$$

Example 2.3.30. Let λ be the square root of the complex number $2+i$ belonging to the first quadrant of the complex plane. Let us consider the algebra $\mathscr{GA}+ = (\mathbb{Q}(\lambda,i)/\mathbb{Q}(i), \sigma, i)$, where the automorphism σ is determined by $\sigma(\lambda) = -\lambda$. The field $\mathbb{Q}(i) = F$ has only one infinite prime (∞) and $F_{(\infty)} = \mathbb{C}$. We can now suppose that $\mathbb{Q}(\lambda,i) \subseteq \mathbb{C}$. We then have that

$$F_{(\infty)} \otimes_F \mathscr{GA}+ \sim (\mathbb{CQ}(\lambda,i)/\mathbb{CQ}(i), \sigma^2, i) = (\mathbb{C}/\mathbb{C}, id, i) \simeq \mathbb{C}.$$

2.3.2 Orders and discriminants of a division algebra

The main algebraic object in the design of code lattices from algebraic number fields is the ring of algebraic integers. In the division algebras the analogy of this concept is the *maximal order*. We begin with an example.

Example 2.3.31. Suppose that E/F is a cyclic extension of algebraic number fields. Let $\mathscr{A} = (E/F, \sigma, \gamma)$ be a cyclic division algebra and let $\gamma \in F^*$ to be an algebraic integer. We immediately see that the $\mathscr{O}_F$-module

$$\Lambda = \mathscr{O}_E \oplus u\mathscr{O}_E \oplus \cdots \oplus u^{n-1}\mathscr{O}_E,$$

where $\mathscr{O}_E$ is the ring of integers, is a subring in the cyclic algebra $(E/F, \sigma, \gamma)$. We refer to this ring as the *natural order*. Note also that if γ is not an algebraic integer, then Λ fails to be closed under multiplication.

Remark 2.3.32. What we call a natural order is actually an example of *crossed product orders*.

Let F/K be a finite extension (could be also the trivial extension F/F) of algebraic number fields and $\mathscr{A}$ an F-central division algebra of degree n.

Definition 2.3.33. An $\mathscr{O}_K$-order Λ in $\mathscr{A}$ is a subring of $\mathscr{A}$, having the same identity element as $\mathscr{A}$, and such that Λ is a finitely generated module over $\mathscr{O}_K$ and generates $\mathscr{A}$ as a linear space over K.

Example 2.3.34. If we have a trivial division algebra $\mathscr{A} = F$, then $\mathscr{O}_F$, the ring of algebraic integers in F, is an $\mathscr{O}_K$-order.

Our main interest are $\mathscr{O}_F$-orders, where F is the center, but sometimes it is beneficial to consider these as $\mathscr{O}_K$-orders.

Proposition 2.3.35. *Every $\mathscr{O}_F$-order $\Lambda \subseteq \mathscr{A}$ is also an $\mathscr{O}_K$-order.*

Definition 2.3.36. An $\mathscr{O}_K$-order Λ is called *maximal*, if it is not properly contained in any other $\mathscr{O}_K$-order.

Proposition 2.3.37. *Any F-central division algebra $\mathscr{A}$ has a maximal $\mathscr{O}_K$-order and any order inside $\mathscr{A}$ is contained in at least one maximal order.*

Remark 2.3.38. While much of the intuition, gained from the study of rings of algebraic integers, is valid when we are considering maximal orders in division algebras, there are some fundamental differences. For example, the ring of algebraic integers in an algebraic number field is the unique maximal order, but a division algebra can contain several maximal orders.

In order to research the relation between the ring $\mathscr{O}_K$ and the $\mathscr{O}_K$-order Λ it can be beneficial to consider the division algebra $\mathscr{A}$ as a subalgebra in a matrix algebra.

Theorem 2.3.39. *Let $\mathscr{A}$ be a division algebra with center F. Every maximal subfield E of $\mathscr{A}$ contains F. Further, if $[\mathscr{A}:F]=n^2$, then*

$$[E:F]=n.$$

Remark 2.3.40. It is clear that any division algebra contains at least one maximal subfield.

Let $\mathscr{A}$ be an F-central division algebra where $[\mathscr{A}:F]=n^2$ and suppose that E is a maximal subfield of $\mathscr{A}$. Then we can consider $\mathscr{A}$ as a n-dimensional right vector space and the left multiplication with an element c of $\mathscr{A}$ is a E-linear transformation of $\mathscr{A}$. Therefore c can be seen as a matrix $C\in M_n(E)$. So described representation gives us an injective F-algebra homomorphism ψ from $\mathscr{A}$ to $M_n(E)$. To shorten the notation we often identify the algebra $\mathscr{A}$ and its matrix representation. We refer to maps ψ by calling them *maximal representations*. We refer the reader to [39, Chapter 6, Section A] for details of this map.

Definition 2.3.41. The determinant (resp. trace) of the matrix C above is called the *reduced norm* (resp. *reduced trace*) of the element $c\in\mathscr{A}$ and is denoted by $nr_{\mathscr{A}/F}(c)$ (resp. $tr_{\mathscr{A}/F}(c)$).

Proposition 2.3.42. *Let $\mathscr{A}$ be an F-central division algebra and a an element of $\mathscr{A}$. Then $nr(a)$ and $tr(a)\in F$.*

Example 2.3.43. Suppose that E/F is a cyclic extension of algebraic number fields. Let $\mathscr{A}=(E/F,\sigma,\gamma)$ be a cyclic division algebra.

We can consider $\mathscr{A}$ as a right vector space over E and every element $a=x_0+ux_1+\cdots+u^{n-1}x_{n-1}\in\mathscr{A}$ has the following representation as a matrix

$$A=\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1)\\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2)\\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3)\\ \vdots & & & & \vdots\\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0)\end{pmatrix}.$$

Proposition 2.3.44. *The norm and trace maps do not depend on the maximal representation.*

Definition 2.3.45. We then define the reduced trace and norm of a to K by

$$tr_{\mathscr{A}/K}(a)=tr_{F/K}(tr_{\mathscr{A}/F}(a))$$

$$nr_{\mathscr{A}/K}(a)=nr_{F/K}(nr_{\mathscr{A}/F}(a)).$$

where $nr_{F/K}$ and $tr_{F/K}$ are the usual norm and trace maps of algebraic number theory.

Remark 2.3.46. The connection with the usual norm map $N_{\mathscr{A}/K}(a)$ (resp. trace map $T_{\mathscr{A}/K}(a)$) and the reduced norm $nr_{\mathscr{A}/K}(a)$ (resp. reduced trace $tr_{\mathscr{A}/K}(a)$) of an element $a \in \mathscr{A}$ is $N_{\mathscr{A}/K}(a) = (nr_{\mathscr{A}/K}(a))^n$ (resp. $T_{\mathscr{A}/F}(a) = ntr_{\mathscr{A}/K}(a)$), where $n = \sqrt{[\mathscr{A} : F]}$.

Proposition 2.3.47. *Let Λ be an $\mathscr{O}_K$-order in an F-central division algebra $\mathscr{A}$. Then for any element $a \in \Lambda$ its reduced norm $nr_{\mathscr{A}/K}(a)$ and reduced trace $tr_{\mathscr{A}/K}(a)$ are elements of the ring of integers $\mathscr{O}_K$ of the field K. If a is non-zero, then so is $nr_{\mathscr{A}/K}(a)$.*

Now we are ready to define one of the main algebraic objects of this thesis.

Definition 2.3.48. Let $\mathscr{A}$ be an F-central division algebra and $m = dim_K \mathscr{A}$. The *$\mathscr{O}_K$-discriminant* of the $\mathscr{O}_K$-order Λ is the ideal $d(\Lambda/\mathscr{O}_K)$ in $\mathscr{O}_K$ generated by the set

$$\{\det(tr_{\mathscr{A}/K}(x_i x_j))_{i,j=1}^m \mid (x_1, ..., x_m) \in \Lambda^m\}.$$

If Λ is free $\mathscr{O}_K$-module, then

$$d(\Lambda/\mathscr{O}_K) = \det(tr(x_i x_j))_{i,j=1}^m,$$

where $\{x_1, \ldots, x_m\}$ is any $\mathscr{O}_K$-basis of Λ.

Example 2.3.49. We consider again the case $\mathscr{A} = F$, where $\mathscr{O}_F$ is the unique maximal $\mathscr{O}_K$-order in F. The $\mathscr{O}_K$-discriminant $d(\mathscr{O}_F/\mathscr{O}_K)$ is just the usual discriminant of the extension F/K.

From now on when we are discussing orders we are referring to $\mathscr{O}_F$-orders, where F is the center of the algebra. If we consider $\mathscr{O}_K$-orders or discriminants, we always mention it.

Proposition 2.3.50. *All the maximal orders of an F-central division algebra share the same discriminant.*

Now we can define the following.

Definition 2.3.51. Let $\mathscr{A}$ be an F-central division algebra and let Λ be some maximal order in $\mathscr{A}$. Then we refer to $d(\Lambda/\mathscr{O}_F) = d_{\mathscr{A}}$ as the *discriminant of the algebra $\mathscr{A}$*.

Remark 2.3.52. Although we are not discussing the ramification theory of ideals in maximal orders in this thesis, we note that the discriminant of a maximal order plays similar role in this theory as the discriminant of a number field in algebraic number theory.

Following lemma connects the discriminants $d(\Lambda/\mathscr{O}_K)$ and $d(\Lambda/\mathscr{O}_F)$.

Lemma 2.3.53. *Let $\mathscr{A}$ be an F-central division algebra of index n. If Λ is an $\mathscr{O}_F$-order in $\mathscr{A}$, then*

$$d(\Lambda/\mathscr{O}_K) = nr_{F/K}(d(\Lambda/\mathscr{O}_F))d(\mathscr{O}_F/\mathscr{O}_K)^{n^2}.$$

Remark 2.3.54. All the results in Section 2.3 are well known and can be found from literature (see [34]).

2.4 Codes from division algebras

Let F be a complex quadratic field. We assume that E/F is a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $\mathscr{A} = (E/F, \sigma, \gamma)$ be a cyclic division algebra of index n, that is,

$$\mathscr{A} = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

as a (right) vector space over E. Here $u \in \mathscr{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$.

Let us now consider the map ψ described in Example 2.3.43 and identify the algebra $\mathscr{A}$ and its matrix representation.

In order to achieve a MIMO lattice with NVD the authors in [7] restricted coefficients of u^j to the algebraic integers. As a result we get a natural order

$$\Lambda_n = \mathscr{O}_E \oplus u\mathscr{O}_E \oplus u^2\mathscr{O}_E \oplus \cdots \oplus u^{n-1}\mathscr{O}_E.$$

Proposition 2.3.47 and Example 1.1.9 then assures that $|\det(\psi(a))| \geq 1$, for every non-zero $a \in \Lambda_n$. It is also easily proved (Lemma 2.4.6) that the lattice $\psi(\Lambda_n)$ is full in $M_n(\mathbb{C})$. These properties show that Λ_n is a promising space-time code in the sense of this thesis.

If $\mathscr{O}_E$ has an $\mathscr{O}_F$-basis $\{1, e_1, ..., e_{n-1}\}$, then the elements $x \in \mathscr{O}_E$ take the form $x = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathscr{O}_F$ for all $k = 0, ..., n-1$. Hence when we send $\psi(a) \in \psi(\Lambda_n)$, n^2 complex symbols are transmitted, i.e. the design has full rate. We note that $\mathscr{O}_E$ always has an $\mathscr{O}_F$-basis when $\mathscr{O}_F$ is PID. Especially this is true when $F = \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$.

However, these remarkable properties are not true only for natural orders. We could have chosen any $\mathscr{O}_F$-order (and any maximal representation ψ) and got all the benefits of the natural order. In the following, we discuss the coding theoretic properties of $\mathscr{O}_F$-orders supposing always that we use some maximal representation ψ. As we are considering F-central division algebras, the reader can always suppose that we are using some cyclic generation and representation ψ attached to it. At this point, the volumes of fundamental parallelotopes of the orders can depend on the chosen map ψ, and therefore we use the notation m_ψ, Nsv_ψ and δ_ψ to underline this.

For simplicity, we suppose that F is a complex quadratic field. The case where the center is $\mathbb{Q}$ will be discussed later in Section 2.5. Let $\mathscr{A}$ be an F-central division algebra of index n.

Proposition 2.4.1. *Let Λ be an $\mathscr{O}_F$-order in $\mathscr{A}$. Then*

$$\det_{min}(\Lambda) = 1$$

and

$$\mathrm{sv}(\Lambda) = \sqrt{n}.$$

Proof. The first equation is just Proposition 2.3.47 stated on different language. We claim that $\phi(1)$ is the shortest vector in $\phi(\Lambda)$. Because $\det_{min}(\Lambda) = 1$, we get by Lemma 2.2.2 that

$$\mathrm{sv}(\Lambda) \geq \sqrt{n}.$$

On the other hand $||\phi(1)||_F = \sqrt{n}$. □

Corollary 2.4.2. *Suppose we have an $\mathscr{O}_F$-order Λ in an F-central division algebra $\mathscr{A}$ of index n. Then*

$$\delta_\psi(\Lambda) = \left(\frac{1}{m_\psi(\Lambda)}\right)^{\frac{1}{2n}}$$

and

$$\mathrm{Nsv}_\psi(\Lambda) = \frac{\sqrt{n}}{m_\psi(\Lambda)^{1/(2n^2)}}.$$

This reveals that in order to measure the normalized minimum determinant and the minimum Euclidean distance of an order, we have to determine the volume of the fundamental parallelotope.

Corollary 2.4.3. *Let $\Lambda_1 \subseteq \Lambda_2$ be two $\mathscr{O}_F$-orders inside an F-central division algebra $\mathscr{A}$. Then*

$$\delta_\psi(\Lambda_1) \leq \delta_\psi(\Lambda_2)$$

$$\mathrm{Nsv}_\psi(\Lambda_1) \leq \mathrm{Nsv}_\psi(\Lambda_2)$$

and we have equality if and only if $\Lambda_1 = \Lambda_2$.

Proposition 2.4.4. *Suppose we have two maximal orders $\Lambda_1, \Lambda_2 \subseteq \mathscr{A}$. Then*

$$\delta_\psi(\Lambda_1) = \delta_\psi(\Lambda_2)$$

and

$$\mathrm{Nsv}_\psi(\Lambda_1) = \mathrm{Nsv}_\psi(\Lambda_2).$$

Proof. The proof is postponed to Section 2.4.1. □

It is now evident that in order to maximize the minimum determinant we have to use maximal orders as any other order is always contained in a maximal one with a better minimum determinant.

We now give a quick peek how the switch from the natural order to a maximal order can change the performance and the minimum determinant of the code. The simulation setting is explained in Section 4.3. In Figure 2.1 we compare the performance of the natural Λ_n and maximal Λ_{max} orders of the algebra $\mathscr{G}_2$ (Section 4.1.2). We use the same ψ for both orders. By the methods we will present later we have that $\delta(\Lambda_{nat}) = 0.44...$ and $\delta(\Lambda_{max}) = 0.620...$.

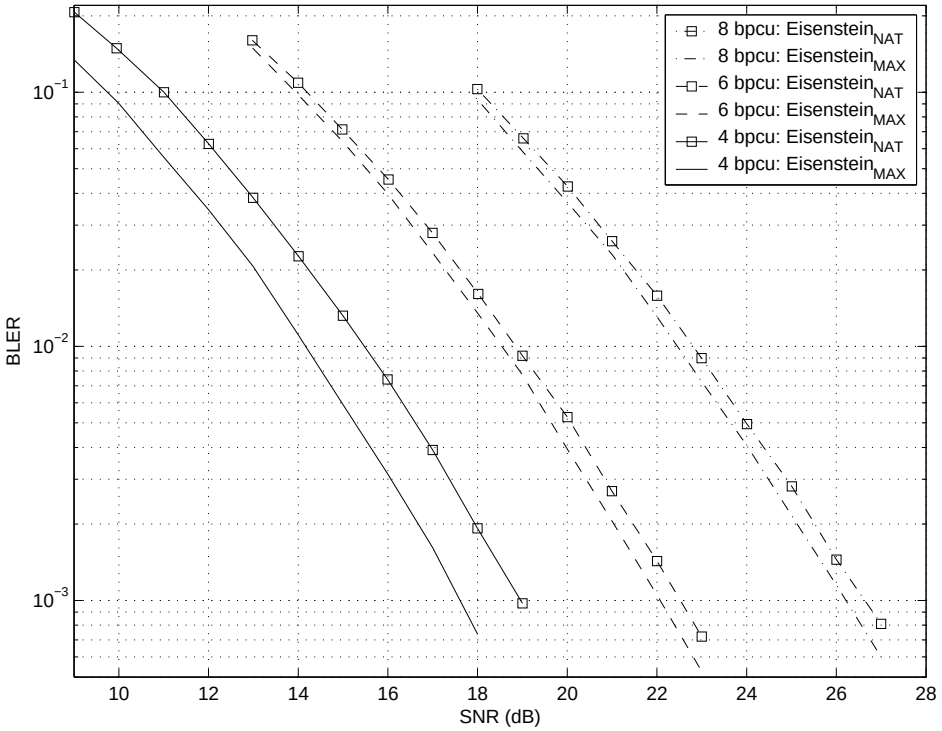


Figure 2.1: natural order of $\mathscr{G}_2$ (NAT) vs maximal order of $\mathscr{G}_2$ (MAX)

Remark 2.4.5. The first division algebra based STBC code was the Alamouti code [1]. The general principles for division algebra codes were first presented in [39]. The idea to consider natural orders to achieve the NVD property was first proposed in [6], although the concept of an order was not used. In [16] it was recognized that the algebraic construction used in [6] was an order and the use of maximal orders was suggested to increase the coding gain.

The propositions and corollaries of this section can be found, in one form or another, from [18] and [23].

2.4.1 Discriminant and the volume of the fundamental parallelotope

For coding theoretical purposes we are interested in $\mathcal{O}_F$-orders inside an F-central division algebra. However, in order to determine the volume of fundamental parallelotope of these orders it is easier to consider them as $\mathbb{Z}$-orders. This, of course, is not a problem as every $\mathcal{O}_F$-order is also a $\mathbb{Z}$-order. In the following proposition we use some chosen maximal representation ψ.

Proposition 2.4.6. *Let Λ be a $\mathbb{Z}$-order of the F-central division algebra $\mathcal{A}$ of index n, where F is an imaginary quadratic field. Then*

$$m_\psi(\Lambda) = 2^{-n^2}\sqrt{|d(\Lambda/\mathbb{Z})|}. \tag{2.4}$$

Proof. Let $A = (a_{ij})$ be an $n \times n$ complex matrix. We flatten it out into a $2n^2$-tuple $L(A)$ with the map ϕ of Subsection 1.2.

If A and B are two square matrices with n rows, we can easily verify the identities

$$L(A)L(B)^T = \Re(tr(AB^H)) \tag{2.5}$$

and

$$L(A)L(B^H)^T = \Re(tr(AB)). \tag{2.6}$$

Next let $\mathcal{B} = \{x_1, x_2, \ldots, x_{2n^2}\}$ be a $\mathbb{Z}$-basis for Λ. We form the $2n^2 \times 2n^2$ matrix $L(\mathcal{B})$ by stacking the matrices $L(x_i)$ on top of each other and $R^*(\mathcal{B})$ by using $L(x_i)^T$ as columns. The Gram matrix of the basis $\mathcal{B}$ can then be presented as

$$G = L(\mathcal{B})R^*(\mathcal{B}).$$

It is easily seen that $|\det(R^*(\mathcal{B}))| = |\det(R(\mathcal{B}))|$, where $R(\mathcal{B})$ is a matrix with columns $L(x_i^H)^T$. This assures that

$$|\det(G)| = |\det(L(\mathcal{B})R(\mathcal{B}))|.$$

By (2.6) the matrix $M = L(\mathcal{B})R(\mathcal{B})$ consists of elements

$$L(x_i)L(x_j^H)^T = \Re tr_{\mathcal{A}/F}(x_i x_j).$$

Knowing that $tr_{F/\mathbb{Q}}(a) = 2\Re(a)$ the last equation transforms into

$$L(x_i)L(x_j^H)^T = 2^{-1} tr_{F/\mathbb{Q}}(tr_{\mathcal{A}/F}(x_i x_j)).$$

It is now easily seen that

$$\sqrt{|\det(G)|} = \sqrt{|\det(M)|} = 2^{-n^2}\sqrt{|d(\Lambda/\mathbb{Z})|}.$$

□

Combined with Corollary 2.4.1, Proposition 2.4.6 reveals that the normalized minimum determinant of an order does not depend on the map ψ. So from now on we can just simply use the term $m(\Lambda)$ for the fundamental parallelotope of an order.

Now we also have the proof for Proposition 2.4.4 as we know that all the maximal orders of an algebra share the same discriminant.

Corollary 2.4.7. *With the notation of the previous proposition we have*

$$\delta(\Lambda) = \frac{2^{n/2}}{|d(\Lambda/\mathbb{Z})|^{1/4n}}.$$

Now we can make Proposition 2.4.3 more explicit.

Lemma 2.4.8. *Let $\Lambda \subseteq \Gamma$ be two orders in an F-central division algebra $\mathscr{A}$. Then*

$$[\mathbb{Z} : d(\Lambda/\mathbb{Z})] = [\Gamma : \Lambda]^2 [\mathbb{Z} : d(\Gamma/\mathbb{Z})].$$

Proof. For the proof we refer the reader to [34, p.66]. □

The following lemma leads us back to considering $\mathscr{O}_F$-orders.

Lemma 2.4.9. *With the notation of Proposition 2.4.6. Let Λ be an $\mathscr{O}_F$-order. Then*

$$m(\Lambda) = |2^{-n^2} d(\Lambda/\mathscr{O}_F)(d(\mathscr{O}_F/\mathbb{Z}))^{n^2/2}|.$$

Proof. Lemma 2.3.53 gives us that

$$d(\Lambda/\mathbb{Z}) = |d(\Lambda/\mathscr{O}_F)|^2 d(\mathscr{O}_F/\mathbb{Z})^{n^2}.$$

Substituting this into (2.4) in Proposition 2.4.6 gives us the result. □

The previous proposition shows that if we fix the center F, then the normalized minimum determinant of an order Λ essentially depends on the discriminant $d(\Lambda/\mathscr{O}_F)$.

Remark 2.4.10. Lemma 2.4.7 will be essential in our forthcoming discussion. This is because the $\mathbb{Z}$-discriminant of an order is a rather complicated object, but the $\mathscr{O}_F$-discriminant we can control with the aid of the local theory. In 2.4.2 we will return to this subject.

Corollary 2.4.11. *Assume that $\mathscr{A}$ is a $\mathbb{Q}(i)$-central division algebra of index n. Let $\Lambda \subset \mathscr{A}$ be a $\mathbb{Z}[i]$-order. Then*

$$m(\Lambda) = |d(\Lambda/\mathbb{Z}[i])|$$

and

$$\delta(\Lambda) = \frac{1}{|d(\Lambda/\mathbb{Z}[i])|^{1/2n}}.$$

Corollary 2.4.12. *Assume that $\mathscr{A}$ is a $\mathbb{Q}(\omega)$-central division algebra of index n. Let $\Lambda \subset \mathscr{A}$ be a $\mathbb{Z}[\omega]$-order. Then the measure of the fundamental parallelotope equals*

$$m(\Lambda) = (\sqrt{3}/2)^{n^2} |d(\Lambda/\mathbb{Z}[\omega])|$$

and

$$\delta(\Lambda) = (2/\sqrt{3})^{n/2} / |d(\Lambda/\mathbb{Z}[\omega])|^{1/2n}.$$

Now we have found out that with a given center F and a given index n, the algebra that has the smallest discriminant has also the maximal order with largest normalized minimum determinant. This problem is analogous to the commutative case. In order to find a lattice with a maximal product distance, we had to find a field with a minimal discriminant. This classical problem is very hard. In the totally real case the problem is solved only for the fields of degree < 9. In the general case and for larger fields the best we have is the Odlyzko bound (1.1) that gives us a lower bound. In the following, we will see that the situation is much better in the non-commutative case.

Before we proceed one should remember our coding theoretical goal. To produce MIMO codes with optimal coding gain. So far we have achieved the following correspondence.

- maximal coding gain$\longleftrightarrow$ maximal order with a minimal discriminant

Remark 2.4.13. The results of Section 2.4.1 are from [17] and [18], except that the Proposition 2.4.6 is slightly generalized and simplified version of the corresponding one in [17].

2.4.2 Brauer group, Hasse invariants and the discriminant of a division algebra

In the previous subsection we proved that the normalized minimum determinant of an order depends on the discriminant. Especially, the minimum determinant of a maximal order depends on the discriminant of the algebra. It is now evident that there are some optimal algebras that have minimal discriminants. To find or even describe these optimal algebras we have to reach a deeper understanding of the discriminant of an algebra.

In this and in the following subsection we take a little distance to our coding theoretical discussion and consider the discriminants of a division algebra more generally. In Section 2.4.4 we return to our original route and apply our general results to get bounds for normalized minimum determinants of codes from orders of division algebras.

In this section we give two results, Equation (2.7) and Theorem 2.4.15, that are crucial in Section 2.4.3. We take (2.7) as given because even a sketch of a proof

would take us far away from our original problems. However, we outline a proof for Theorem 2.4.15. In this sketch we are forced to use some terminology and results that are not presented in this thesis. These can be found from the Reiner's book [34].

Let F be an algebraic number field that is of finite degree over $\mathbb{Q}$. Then we have the *fundamental exact sequence of Brauer groups* (see e.g. [34] or [25])

$$0 \longrightarrow \mathrm{Br}(F) \longrightarrow \oplus \mathrm{Br}(F_P) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \tag{2.7}$$

Here the first nontrivial map is obtained by mapping the similarity class of a F-central simple algebra $\mathscr{A}$ to a vector consisting of the similarity classes of all the simple algebras $\mathscr{A}_P$ gotten from $\mathscr{A}$ by extending the scalars from F to F_P, where P ranges over all the primes of $\mathscr{O}_F$. Note that the injectivity of this map is stated in Theorem 2.3.27. That such a mapping is well defined is due to Lemma 2.3.28 and Theorem 2.3.24.

The second nontrivial map of the fundamental exact sequence is then simply the sum of the Hasse invariants of the division algebras $\mathscr{A}_P$ representing elements of the Brauer groups $\mathrm{Br}(F_P)$.

The sequence tells us that the sum of the nontrivial Hasse invariants of any central simple algebra must be an integer. Furthermore, this is the only constraint for the Hasse invariants, i.e. any combination of Hasse invariants (a/m_P) such that only finitely many of them are non-zero, and that they sum up to an integer, is realized as a collection of the Hasse invariants of some central simple algebra $\mathscr{A}$ over F. We warn the reader that when considering infinite primes the Hasse invariants have strict restrictions.

We give one simple result, following from Sequence (2.7), for later use.

Corollary 2.4.14. *Suppose that $\mathscr{A}$ and $\mathscr{B}$ are F-central division algebras of coprime indices $n_{\mathscr{A}}$ and $n_{\mathscr{B}}$. Let $m_P^{\mathscr{A}}$ and $m_P^{\mathscr{B}}$ be the local indices of $\mathscr{A}$ and $\mathscr{B}$ at P. Then*

$$m_P^{\mathscr{A}\otimes\mathscr{B}} = m_P^{\mathscr{A}} m_P^{\mathscr{B}}, \tag{2.8}$$

and the algebra $\mathscr{A}\otimes\mathscr{B}$ is a division algebra of index $n_{\mathscr{A}} n_{\mathscr{B}}$.

Proof. Because $m_P^{\mathscr{A}} | n_{\mathscr{A}}$ and $m_P^{\mathscr{B}} | n_{\mathscr{B}}$, $(m_P^{\mathscr{A}}, m_P^{\mathscr{B}}) = 1$. The exact sequence 2.7 reveals that the Hasse invariant $h_P^{\mathscr{A}\otimes\mathscr{B}}$ is the fractional part of $h_P^{\mathscr{B}} + h_P^{\mathscr{A}}$. This implies the first result. The elementary properties of the tensor product tell us that

$$\sqrt{[\mathscr{A}\otimes\mathscr{B} : F]} = n_{\mathscr{A}} n_{\mathscr{B}}.$$

On the other hand (2.8) and Theorem 2.3.24 imply that

$$\mathrm{index}[\mathscr{A}\otimes\mathscr{B}] = n_{\mathscr{A}} n_{\mathscr{B}}.$$

□

From now on when we talk about sums of Hasse invariants we refer to the fractional part of that sum.

We note that each similarity class includes exactly one division algebra. This means that the Hasse invariants of a division algebra define the algebra not only up to similarity but up to isomorphism. Therefore it is not a great surprise that the discriminant of a division algebra is totally determined by its Hasse invariants.

Theorem 2.4.15. *Let F be an algebraic number field and $\mathscr{A}$ an F-central division algebra of index n. Suppose that the only finite ramified primes in $\mathscr{A}$ are $P_1,\dots,P_n$ and let Λ be a maximal order in $\mathscr{A}$. Then*

$$d(\Lambda/\mathscr{O}_F)=\prod_{i=1}^{n}P_i^{(m_{P_i}-1)\frac{[\mathscr{A}:F]}{m_{P_i}}}.$$

Proof. In what follows we identify the prime ideal P and $P\mathscr{O}_{F_P}$. With this notation we have that

$$d(\Lambda/\mathscr{O}_F)=\prod_{i=1}^{n}d(\mathscr{A}_{P_i}).$$

Let us now determine the local discriminant $d(\mathscr{A}_P)$. Wedderburn's theorem together with Theorem 2.3.19 give us that

$$\mathscr{A}_P\simeq M_{\kappa_P}(\mathscr{A}(k,s)),$$

where $\mathscr{A}(k,s)=(E/F_P,\sigma,\pi^s)$ is the division algebra of Proposition 2.3.18. We note that $\pi\mathscr{O}_{F_P}=P\mathscr{O}_{F_P}$. It is then easily seen that

$$d(\mathscr{A}_P)=(d(\mathscr{A}(m_P,s)))^{\kappa_P^2}.$$

To evaluate $d(\mathscr{A}(m_P,s))$ we use a simple isomorphism

$$\mathscr{A}(m_P,s)\simeq\mathscr{A}^*=(E/F_P,\sigma^h,\pi),$$

where h is chosen so that $(\sigma^h)^s=\sigma$ and that s is the smallest integer with this property. Theorem [34, 13.3] states that the natural order,

$$\Lambda=\mathscr{O}_E\oplus u\mathscr{O}_E\oplus\cdots\oplus u^{m_P}\mathscr{O}_E,$$

of $\mathscr{A}^*$ is maximal. The extension E/F_P is unramified and therefore $d(E/F_P)=\mathscr{O}_{F_P}$. Lemma 3.1.1 is also applicable in this local situation and we get that

$$d(\Lambda/\mathscr{O}_{F_P})=P^{m_P(m_P-1)}.$$

We now have that

$$d(\mathscr{A}_P)=d(\mathscr{A}(m_P,s))^{\kappa_P^2}=d(\mathscr{A}^*)^{\kappa_P^2}=P^{m_P(m_P-1)\kappa_P^2}$$

and

$$d(\Lambda/\mathcal{O}_F) = \left(\prod_{i=1}^{n} P_i^{(m_{P_i}-1)m_{P_i}\kappa_{P_i}^2} \right). \tag{2.9}$$

Proposition 2.3.12 gives us that

$$[F_P \otimes \mathscr{A} : F_P] = [\mathscr{A} : F].$$

On the other hand we have

$$[F_P \otimes \mathscr{A} : F_P] = [M_{\kappa_P}(\mathscr{A}(m_P, s)) : F_P] = (\kappa_P)^2[\mathscr{A}(m_P, s) : F_P] = (\kappa_P)^2(m_P)^2.$$

By combining these results we get

$$\kappa_P = \frac{\sqrt{[\mathscr{A} : F]}}{m_P}.$$

By substituting this into (2.9) we get the claim. □

Remark 2.4.16. The proof we gave here still does not give a very deep insight to the discriminant of a division algebra. The proper way to discuss the discriminants would be through the local and global differents and ideal theory of maximal orders. For this theory and for an alternative proof of Theorem 2.4.15 we refer the reader to [34, Theorem 25.7]. The proof of [34, Theorem 14.9] gives a nice insight to the determination of the local discriminant.

Remark 2.4.17. The formula for the discriminant of a division algebra is unsurprising and is rather similar to the discriminant formula for tamely ramified Galois extensions of algebraic number fields L/F. The κ_P^2 can be considered as the number of splitting primes g over a prime P of $\mathcal{O}_F$ and m_P as the usual ramification index e. However, the inertial degree f is always the same as the ramification index m_P. The biggest difference here is that wild ramification does not exist in division algebras. The local discriminant is exactly determined by the local index m_P. This will be one of the key points why we are able to give very strong bounds for the discriminants of division algebras in the following section.

Remark 2.4.18. This is not the first time when the fundamental exact sequence (2.7) has been used in coding theory. In [27] Morandi and Sethuraman used the corresponding exact sequence, that appears in the theory of function fields over finite fields, to produce analogues of Goppa codes from division algebras. This paper gave us the basic idea for our application.

Remark 2.4.19. The results in Section 2.4.2 are well known. The proof of Theorem 2.4.15 is an alternative for the one usually found from the literature (see [34]).

2.4.3 Bounds for the discriminant

Let us now suppose that with a given number field F we would like to produce a division algebra $\mathscr{A}$ of a given index n, having F as its center and the smallest possible discriminant. We proceed to show that we can describe the algebra well and we can derive an explicit formula for its discriminant.

Again let F be an algebraic number field that is finite dimensional over $\mathbb{Q}$, and $\mathscr{O}_F$ its ring of integers. In what follows we discuss the size of ideals of $\mathscr{O}_F$. By this we mean that ideals are ordered by the absolute values of their norms to $\mathbb{Q}$, so e.g. in the case $\mathscr{O}_F = \mathbb{Z}[i]$ we say that the prime ideal generated by $2+i$ is smaller than the prime ideal generated by 3 as they have norms 5 and 9, respectively.

Remark 2.4.20. As we are going to consider the size of the discriminant of a division algebra, in the light of Lemma 2.3.53, our definition for the size of the ideals is well defined.

Theorem 2.4.21. *Assume that $P_1, \ldots, P_s$ are a set of finite prime ideals of $\mathscr{O}_F$ and $P_{s+1}, \ldots, P_n$ are a set of real primes.*

Assume further that a sequence of rational numbers

$$a_1/m_{P_1}, \ldots, a_s/m_{P_s}, a_{s+1}/m_{P_{s+1}}, \ldots, a_n/m_{P_n},$$

subject to restriction that when $i > s$, $a_i/m_{P_i} = 1/2$, satisfies

$$\sum_{i=1}^{n} \frac{a_i}{m_{P_i}} \equiv 0 \qquad (mod \quad 1),$$

$1 \leq a_i \leq m_{P_i}$, *and* $(a_i, m_{P_i}) = 1$.

Then there exist an F-central division algebra $\mathscr{A}$ that has local indices m_{P_i} and the least common multiple (LCM) of the numbers $\{m_{P_i}\}$ as an index.

If Λ is a maximal $\mathscr{O}_F$-order in $\mathscr{A}$, then the discriminant of Λ is

$$d(\Lambda/\mathscr{O}_F) = \prod_{i=1}^{s} P_i^{(m_{P_i}-1)\frac{[\mathscr{A}:F]}{m_{P_i}}}.$$

Proof. By the exactness of the sequence (2.7) we know that there exist an F-central simple algebra $\mathscr{A}_0$ which has local indices m_{P_i}. By Wedderburn's Theorem the similarity class of $\mathscr{A}_0$ includes also a division algebra $\mathscr{A}$ which shares the local indices of $\mathscr{A}_0$.

The rest now follows directly from Theorem 2.3.24 and Theorem 2.4.15. □

At this point, it is clear that the discriminant $d_{\mathscr{A}}$ of a division algebra depends only on its local indices m_{P_i}.

Now we have an optimization problem to solve. Given the center F and an integer n we should decide how to choose the local indices and the Hasse invariants

so that the LCM of the local indices is n, the sum of the Hasse invariants is an integer, and that the resulting discriminant is as small as possible. We immediately observe that at least two of the Hasse invariants must be non-integral.

Observe that the exponent $d(P)$ of the prime ideal P in the discriminant formula equals

$$d(P) = (m_P - 1)\frac{[\mathscr{A} : F]}{m_P} = n^2\left(1 - \frac{1}{m_P}\right),$$

where n is the index of the algebra $\mathscr{A}$.

Lemma 2.4.22. *Let $\mathscr{A}$ be an F-central division algebra of degree $p^k = n$ where p is a prime. Then $\mathscr{A}$ has at least two Hasse invariants with the local indices p^k.*

Proof. We know that there has to be at least two nontrivial Hasse invariants and at least one that has local index p^k. Knowing that the sum of the Hasse invariants is an integer reveals that there must be at least two primes with the local indices p^k. □

Lemma 2.4.23. *Let $\mathscr{A}$ be an F-central division algebra of index $n = p_1^{k_1} \cdots p_s^{k_s}$ where $p_1, \ldots, p_s$ are distinct primes. Then*

$$\mathscr{A} = \mathscr{A}_{p_1^{k_1}} \otimes \cdots \otimes \mathscr{A}_{p_s^{k_s}} \tag{2.10}$$

where $\mathscr{A}_{p_i^{k_i}}$ are F-central division algebras of index $p_i^{k_i}$. Let P be a prime of F and let m_P be the local index of $\mathscr{A}$ at P and m_P^* the local index of $\mathscr{A}_{p_i^{k_i}}$ at P. Then

$$v_{p_i}(m_P) = v_{p_i}(m_P^*). \tag{2.11}$$

The algebra $\mathscr{A}$ can have a minimal discriminant only if each of $\mathscr{A}_{p_i^{k_i}}$ has exactly two nontrivial Hasse invariants.

Proof. The proof for the existence of the prescribed decomposition of the algebra $\mathscr{A}$ can be found from [2, Theorem 15]. Equation (2.11) follows directly from the fact that the Hasse invariants of the algebra $\mathscr{A}$ are sums of the invariants of the component algebras $\mathscr{A}_{p_i^{k_i}}$.

We already know that each $\mathscr{A}_{p_i^{k_i}}$ has at least two Hasse invariants with local indices $m_{P_x} = p_i^{k_i}$ and $m_{P_y} = p_i^{k_i}$. If any algebra $\mathscr{A}_{p_i^{k_i}}$ has more than two nontrivial Hasse invariants, say, also at P_z, we can replace it in (2.10) with a division algebra $\mathscr{A}'_{p_i^{k_i}}$ having Hasse invariants

$$h_{P_x} = \frac{1}{p_i^{k_i}} \quad \text{and} \quad h_{P_y} = \frac{p_i^{k_i} - 1}{p_i^{k_i}}.$$

Corollary 2.4.14 assures that the resulting algebra $\mathscr{A}'$ is division a algebra of an index n. Because $m_{P_z}(\mathscr{A}') < m_{P_z}(\mathscr{A})$, $\mathscr{A}'$ has smaller discriminant than $\mathscr{A}$. □

Remark 2.4.24. Suppose that the algebra $\mathscr{A}$ has an index $2^k m$, $(2,m) = 1$. If $k \neq 1$, the proof of the last lemma reveals that we can always suppose that an algebra with minimal discriminant does not have ramified infinite primes. The same is of course true if the center F does not have real primes.

In the following, we naturally expand our definition of the size of ideals by setting that $A^k \leq B^h$, where A and B are ideals of $\mathscr{O}_F$ and k and h are rational numbers, if and only if $|nr_{F/\mathbb{Q}}(A)|^k \leq |nr_{F/\mathbb{Q}}(B)|^h$.

Lemma 2.4.25. *Suppose that a, b and c are positive integers. Let $P_1 \leq P_2$ be a pair of finite primes of an algebraic number field F. Then*

$$P_1^{(1-\frac{1}{abc})} P_2^{(1-\frac{1}{b})} \leq P_1^{(1-\frac{1}{ab})} P_2^{(1-\frac{1}{bc})}.$$

Proof. Because $P_1 \leq P_2$ and $(1-\frac{1}{b}) \leq (1-\frac{1}{bc})$, the inequality

$$P_1^{(1-\frac{1}{abc})} P_2^{(1-\frac{1}{b})} \leq P_1^{(1-\frac{1}{ab})} P_2^{(1-\frac{1}{bc})}$$

is true if

$$P_1^{(1-\frac{1}{abc})} P_1^{(1-\frac{1}{b})} \leq P_1^{(1-\frac{1}{ab})} P_1^{(1-\frac{1}{bc})}$$

is. The last inequality follows from the fact that

$$2 - \left(\frac{1+ac}{abc}\right) \leq 2 - \left(\frac{a+c}{abc}\right).$$

□

Theorem 2.4.26. *Assume that F is a number field, and that P_1 and P_2 are a pair of smallest prime ideals in $\mathscr{O}_F$. If we do not allow ramification on infinite primes, then the smallest possible discriminant of all central division algebras over F of index n is*

$$(P_1 P_2)^{n(n-1)}.$$

Proof. By Theorem 2.4.21 the division algebra with Hasse invariants $1/n$ and $(n-1)/n$ at the primes P_1 and P_2 has the prescribed discriminant, so we only need to show that this is the smallest possible value.

Suppose that $n = p_1^{k_1} \cdots p_s^{k_s}$ where $p_1, \ldots, p_s$ are separate primes and let $\mathscr{A}$ be a division algebra of index n, with a minimal discriminant.

Lemma 2.4.23 states that we can suppose that every $p_i^{k_i}$ is the exact divisor of exactly two local indices. This results that the product of all the local indices is n^2.

If $\mathscr{A}$ now has only two finite primes having nontrivial Hasse invariants, we are done. Let $P_x \leq P_y$ be a pair of smallest ramified primes in $\mathscr{A}$ and P_z a third ramified prime. By considering the factors $p_i^{k_i}$ in the local indices we see that we can write $m_{P_x} = ab$, $m_{P_y} = d$, $m_{P_z} = bc$, where $(ab, c) = 1$. Now we have

$$\left(P_x^{(1-\frac{1}{ab})} P_z^{(1-\frac{1}{bc})} P_y^{(1-\frac{1}{d})} C\right)^{n^2} = d_{\mathscr{A}},$$

and after applying Lemma 2.4.25

$$\left(P_x^{(1-\frac{1}{abc})} P_z^{(1-\frac{1}{b})} P_y^{(1-\frac{1}{d})} C\right)^{n^2} \leq \left(P_x^{(1-\frac{1}{ab})} P_z^{(1-\frac{1}{bc})} P_y^{(1-\frac{1}{d})} C\right)^{n^2} = d_{\mathscr{A}}.$$

We can then apply Lemma 2.4.25 to $P_y^{(1-\frac{1}{1\cdot d})}$ and $P_z^{(1-\frac{1}{1\cdot b})}$ getting that

$$\left(P_x^{(1-\frac{1}{abc})} P_y^{(1-\frac{1}{db})} C\right)^{n^2} \leq d_{\mathscr{A}}.$$

Remembering that each of the terms $p_i^{k_i}$ is a factor of exactly two local indices we see that $(b, d) = 1$.

This process can be continued until the only terms left are $P_x^{(1-\frac{1}{h})}$ and $P_y^{(1-\frac{1}{k})}$. By analyzing where the terms $p_i^{k_i}$ went and recalling that the product of all the local indices of $\mathscr{A}$ was n^2, we see that $h = k = n$. We finally get

$$\left(P_1^{(1-\frac{1}{n})} P_2^{(1-\frac{1}{n})}\right)^{n^2} \leq \left(P_x^{(1-\frac{1}{n})} P_y^{(1-\frac{1}{n})}\right)^{n^2} \leq d_{\mathscr{A}}.$$

□

Proposition 2.4.27. *Let $\mathscr{A}$ be a F-central division algebra of degree $2m = n$, where m and 2 are relatively prime and let $P_1 \leq P_2$ be a pair of smallest primes in F.*

If F has at least two real primes, then the minimal discriminant of $\mathscr{A}$ is

$$(P_1 P_2)^{m(m-1)}.$$

If F has only one real prime P_∞, then the minimal discriminant of $\mathscr{A}$ is

$$P_1^{n(n-1)} P_2^{m(m-1)}.$$

Proof. In the first case, Proposition 2.4.23 reveals that the product of all the local indices at the finite primes, of an algebra with a minimal discriminant, is at least m^2. This situation corresponds to a division algebra where we have set $1/2$ and $1/2$ a the Hasse invariants at the infinite primes. The reasoning of Theorem 2.4.26 can then be used to the Hasse invariants of finite primes giving that any F-central division algebra $\mathscr{A}$ has discriminant larger than $(P_1 P_2)^{m(m-1)}$.

In the second case, Hasse invariants $h_{P_1} = \frac{m-2}{2m}$, $h_{P_2} = \frac{1}{m}$ and $h_{P_\infty} = 1/2$ give us a division algebra with discriminant $P_1^{n(n-1)} P_2^{m(m-1)}$. To prove that no algebra has a smaller discriminant than this we again use Proposition 2.4.23 to prove that the product of local indices at finite primes has to be at least $2m^2$. We then proceed as in the first case. □

Remark 2.4.28. We note that Proposition 2.4.27 and Theorem 2.4.26 cover all the centers. This follows directly from the considerations in Remark 2.4.24.

Remark 2.4.29. By analyzing the proofs of Proposition 2.4.23 and Lemma 2.4.25 we see that essentially the minimal discriminant is unique. The only variations allowed are those where we replace prime ideals P_1 and P_2 with primes of same sizes. The direct consequence is that only the algebras that have at most two ramified finite primes can have a minimal discriminant.

Yet this is not enough to define the algebra uniquely. For example, in Theorem 2.4.26 any pair of Hasse invariants a/n and $(n-a)/n$, where $0 < a < n$ and $(a,n) = 1$, leads to a division algebra with the same discriminant.

Remark 2.4.30. If we compare these discriminant bounds to the commutative case, the results are surprisingly strong. The bounds are very simple and in all the cases they are achievable. This is in a sharp contrast to Odlyzko bound in algebraic number theory.

In Remark 2.4.17 we were considering an analogy between division algebras and Galois extensions of number fields. Could it be possible to use the strategy of the proof of Theorem 2.4.26 to give a strong discriminant bounds for Galois extensions of algebraic number fields? Unfortunately there exist some fundamental differences between the commutative and the non-commutative case. The first is that there does exist wild ramification in number fields and the inertial degree and the ramification index are usually not equal. These differences prevent us using the inequalities we used in the proof of Theorem 2.4.26. The bigger difficulty is, however, the lack of an analogy for the fundamental exact sequence. When considering algebraic number fields we cannot give a set of local extensions with described ramification and then find a global field which has these local extensions as localizations. Especially, we cannot find a field where only two small primes are tamely ramified for every n. We will encounter this difference in the proof of Proposition 3.1.4.

Remark 2.4.31. Theorem 2.4.21 is well known. Theorem 2.4.26 is from [18]. Proposition 2.4.27 is introduced for the first time in this thesis.

2.4.4 Bounds for the normalized minimum determinant

Now we can return to our main interest where the center is a complex quadratic field. In this case, F does not have any real places and therefore the only rami-

fied primes in any F-central division algebra are finite. In this situation Theorem 2.4.26 gives us a minimal discriminant. In particular we are interested in the case where the center is $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$.

The smallest primes of the ring $\mathbb{Z}[i]$ are $1+i$ and $2\pm i$. They have norms 2 and 5, respectively. The smallest primes of the ring $\mathbb{Z}[\omega]$ are $\sqrt{-3}$ and 2 with respective norms 3 and 4. Together with Corollaries 2.4.11 and 2.4.12 we get the following bounds.

Corollary 2.4.32 (Discriminant bound). *Let Λ be an order of a central division algebra of index n over the field $\mathbb{Q}(i)$. Then the measure of a fundamental parallelotope of the corresponding lattice satisfies*

$$m(\Lambda) \geq 10^{n(n-1)/2}$$

and their normalized minimum determinants and shortest vectors satisfy the inequalities

$$\delta(\Lambda) \leq 1/10^{(n-1)/4}$$

and

$$\mathrm{Nsv}(\Lambda) \leq \sqrt{n} \cdot 10^{((1-n)/4n)}.$$

Furthermore, for every n there exist cyclic division algebras with center $\mathbb{Q}(i)$, whose maximal orders achieve equality in all of these bounds.

Proof. By Theorem 2.4.26 the absolute value of the minimal discriminant is $|(2+i)(1+i)|^{n(n-1)} = 10^{n(n-1)/2}$. The rest then follows directly from Corollary 2.4.11 and Corollary 2.4.2. □

Corollary 2.4.33 (Discriminant bound). *Let Λ be an order of a central division algebra of index n over the field $\mathbb{Q}(\omega)$, $\omega = (-1+\sqrt{-3})/2$. Then the measure of the fundamental parallelotope of the corresponding lattice satisfies*

$$m(\Lambda) \geq (\sqrt{3}/2)^{n^2} 12^{n(n-1)/2}$$

and their normalized minimum determinants and shortest vectors satisfy the inequalities

$$\delta(\Lambda) \leq (2/\sqrt{3})^{n/2}/12^{(n-1)/4}$$
$$\mathrm{Nsv}(\phi(\Lambda)) \leq \sqrt{n} \cdot (2/\sqrt{3})^{1/2} \cdot 12^{((1-n)/4n)}.$$

Furthermore, for every n there exist cyclic division algebras with center $\mathbb{Q}(\omega)$, whose maximal orders achieve equality in all of these bounds.

In what follows we sometimes refer to these bounds as $B_{\mathbb{Q}(i)}$ and $B_{\mathbb{Q}(\omega)}$. We note that while our results did not give us explicit constructions of the division algebras with minimal discriminants, at the local level we described them well. The following lemma benefits from this knowledge and gives us an effective method for detecting division algebras with minimal discriminants.

Lemma 2.4.34. *Let F be a complex quadratic field, and let P_1 and P_2 be a pair of smallest prime ideals of its ring of integers $\mathcal{O}_F$. Let $\mathcal{D}$ be a central division algebra over F, and let Λ be any $\mathcal{O}_F$-order in $\mathcal{D}$. If the discriminant $d(\Lambda)$ is divisible only by the primes P_1 and P_2, then any maximal order Γ of $\mathcal{D}$ achieves the discriminant bound of Theorem 2.4.26.*

Proof. We know that there exists a maximal order, say Γ_0, containing Λ. The discriminant of Γ_0 is then a factor of $d(\Lambda)$, so P_1 and P_2 are the only prime divisors of $d(\Gamma_0)$. From Theorem 2.4.21 we infer that the only nontrivial Hasse invariants of $\mathcal{D}$ occur at P_1 and P_2. As the sum of the two Hasse invariants is an integer, they have the same denominator. This must then be equal to the index of $\mathcal{D}$. The discriminant formula of Theorem 2.4.21 shows that $d(\Gamma_0)$ equals the discriminant bound. Any other maximal order in $\mathcal{D}$ shares its discriminant with Γ_0. □

In Table 2.1 we have collected relevant data of the codes which Corollaries 2.4.32 and 2.4.33 promise to exist. We refer to maximal orders that reach the bound in Corollary 2.4.32 with Λ_n^i and to orders reaching the bound in Corollary 2.4.33 with Λ_n^ω. For a comparison we have also added values of the bounds of Section 2.2 for the shortest vectors and minimum determinants.

As an example we count the few first values of the first row of Table 2.1. In this case we know the exact value of $\mathrm{sv}(2) = \sqrt{2}$ and therefore $\mathrm{Bsv}(2) = \sqrt{2}$. According to Lemma 2.2.3 then $B\delta(2) = 1$. The other relevant information can be directly read from Corollary 2.4.32 which gives us that $m(\Lambda_n) = 10$, $\mathrm{Nsv}(\phi(\Lambda_2)) = 1.065$, and $\delta(\Lambda_2) = 0.56$.

Table 2.1:

n	$B\delta(n)$	$\mathrm{Bsv}(n)$	$\mathrm{Nsv}(\Lambda_n^i)$	$\delta(\Lambda_n^i)$	$\delta(\Lambda_n^\omega)$	$\mathrm{Nsv}(\Lambda_n^\omega)$
2	1.00	1.41	1.07	0.56	0.62	1.11
3	1.16	1.82	1.18	0.32	0.36	1.23
4	1.61	2.25	1.30	0.18	0.20	1.35
5	2.57	2.70	1.41	0.10	0.12	1.46
6	4.59	3.16	1.52	0.06	0.07	1.57

Remark 2.4.35. By considering different complex quadratic fields and their discriminants and smallest prime ideals we easily see that the MIMO codes with maximal coding gain come from maximal orders with minimal discriminants in division algebras over the centers $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\sqrt{-7})$.

The orders Λ_n^ω have the best coding gain when $n < 5$. After that the best choice for the center is $\mathbb{Q}(\sqrt{-7})$ with minimal ideals $((1-\sqrt{-7})/2)$ and $((1+\sqrt{-7})/2)$. The resulting maximal orders with minimal discriminants have a considerably

better coding gain than any previously known MIMO code. We return to this question in Chapter 3.

Remark 2.4.36. Notable here is that if we consider maximal orders Λ_n^ω achieving the bound 2.4.33 the shortest vector of real lattice $\phi(\psi(\Lambda_n^\omega))$ in $\mathbb{R}^{2n^2}$ has length

$$\sqrt{n}(2/\sqrt{3})^{1/2} \cdot 12^{((1-n)/4n)}.$$

This implies that, asymptotically, the shortest vector approaches the value $\sqrt{n/3}$. This reveals that these real lattices have a center density comparable to that of the Barnes-Wall lattices. The relatively good Euclidean distance of our codes suggests that they are suitable also for low values of SNR.

Remark 2.4.37. The results in Section 2.4.4 are from [18] except Table 2.1 which is from [23].

2.5 Real matrix lattices

In some applications (see [5]) it is beneficial to have the code lattice consisting of matrices with real coefficients. In the following we quickly describe how our theory works in this setting.

A full lattice L in $M_n(\mathbb{R})$ has n^2 linearly independent basis vectors. Again we get an isometry $\phi_{\mathbb{R}}$ that maps a matrix M into a vector in $\mathbb{R}^{n^2}$. Now we can define the normalized minimum determinant and the shortest vector of a full matrix lattice $L \subseteq M_n(\mathbb{R})$ just like in Section 2.2.

One must note that in the case of real matrix lattices the scaling affects the minimum determinant differently as in the complex case. A simple computation shows that if a is the minimum determinant of the lattice L before the scaling, after the scaling it is

$$\frac{a}{m(L)^{1/n}}. \tag{2.12}$$

We list here the analogues of the results in Section 2.2.

Lemma 2.5.1. *Suppose we have a full lattice L in $M_n(\mathbb{R})$. Then*

$$\det_{\min}(L) \leq \left(\frac{\mathrm{sv}(L)^2}{n}\right)^{n/2}.$$

Corollary 2.5.2. *For a full lattices in $M_n(\mathbb{R})$ we have an upper bound*

$$\delta(n) \leq \left(\frac{\mathrm{Nsv}(n^2)^2}{n}\right)^{n/2}.$$

Proposition 2.5.3. *If L is a full rectangular lattice in $M_n(\mathbb{R})$, then*

$$\delta(L) \leq \frac{1}{n^{n/2}}.$$

2.5.1 Real division algebras

In order to construct full matrix lattices in $M_n(\mathbb{R})$ we consider a $\mathbb{Q}$-central division algebra $(L/\mathbb{Q},\sigma,\gamma)$ and use the maximal subfield representation of Section 2.4. To ensure that our matrices truly belong to the space $M_n(\mathbb{R})$ we have to use a special class of algebras and choose also the cyclic generation carefully. This method has been considered at least in [5].

Definition 2.5.4. We call a division algebra $\mathscr{A}$ *real* if it has cyclic generation $(L/\mathbb{Q},\sigma,\gamma)$ where L is a totally real extension of $\mathbb{Q}$.

The following lemma reveals that our somewhat unsatisfying definition is justified.

Lemma 2.5.5. *Let $\mathscr{A}$ be a real $\mathbb{Q}$-central division algebra of index n. Then $\mathscr{A}$ is not ramified at ∞.*

Proof. Let $\mathscr{A} = (L/\mathbb{Q},\sigma,\gamma)$, where L is totally real. If we now consider the algebra $\mathbb{R}\otimes_{\mathbb{Q}}\mathscr{A}$, Theorem 2.3.29 gives us that

$$\mathbb{R}\otimes_{\mathbb{Q}}\mathscr{A} \sim (\mathbb{R}L/\mathbb{R},\sigma',\gamma) \simeq (\mathbb{R}/\mathbb{R},\sigma',\gamma).$$

This assures that $m_\infty = 1$. □

From now on when we discuss the geometric properties of orders of real division algebras we suppose that the algebra is embedded into $M_n(\mathbb{R})$ with the help of some real cyclic generation and some maximal representation attached to it. From the following proof we see that the choice of the cyclic generation does not affect the measure of fundamental parallelotope of the corresponding lattice.

Lemma 2.5.6. *Suppose that we have a division algebra $\mathscr{A}$ that has real cyclic generation $(L/\mathbb{Q},\sigma,\gamma)$. Let Λ be a $\mathbb{Z}$-order inside $\mathscr{A}$. Then*

$$m(\Lambda) = |\sqrt{d(\Lambda/\mathbb{Z})}|.$$

Proof. We consider $\mathscr{A}$ as a matrix algebra through the maximal subfield representation ψ. Let $x_1,\ldots,x_{n^2}$ be a $\mathbb{Z}$-basis for Λ. We can flatten the x_i matrices to vectors $L(x_i)\in\mathbb{R}^{n^2}$ by using the map $\phi_{\mathbb{R}}$. It is then easily seen that

$$L(x_i)L(x_j)^T = tr(x_i x_j^T) \tag{2.13}$$

and

$$L(x_i)L(x_j^T)^T = tr(x_i x_j). \tag{2.14}$$

We form the $n^2\times n^2$ matrix $L(\mathscr{B})$ by stacking the matrices $L(x_i)$ on top of each other. Similarly we get $R(\mathscr{B})$ by using the matrices $L(x_i^T)^T$ as 'column blocks'. Then the matrix $M = L(\mathscr{B})R(\mathscr{B})$ consists of elements of

$$L(x_i)L(x_j^T)^T = tr(x_i x_j) = tr_{\mathscr{A}/\mathbb{Q}}(x_i x_j).$$

Clearly $\det R(\mathscr{B}) = \pm \det L(\mathscr{B})$, and $\det M = |d(\Lambda/R)|$. Therefore

$$|d(\Lambda/R)| = |\det L(\mathscr{B})|^2.$$

On the other hand the Gram matrix of the lattice $\psi(\Lambda)$ is

$$L(\mathscr{B})L(\mathscr{B}).$$

□

Corollary 2.5.7 (Discriminant bound). *Let Λ be an order of a real division algebra $\mathscr{A}$ of index n over the field $\mathbb{Q}$. Then*

$$|d_{\mathscr{A}}| \geq (2 \cdot 3)^{n(n-1)}, \tag{2.15}$$

$$m(\Lambda) \geq 6^{\frac{n(n-1)}{2}},$$

and

$$\delta(\Lambda) \leq 6^{\frac{(1-n)}{2}}.$$

For every n there always exists a real division algebra achieving these bounds.

Proof. Lemma 2.5.5 states that we cannot admit ramification on infinite primes and therefore we can apply Theorem 2.4.26 here. The smallest finite primes in $\mathbb{Z}$ are 2 and 3. The first results then follow from Theorem 2.4.26.

It is, however, not clear whether we can reach the bound with a real division algebra. Let $\mathscr{A}'$ be a division algebra that reaches the bound 2.15. The nontrivial local indices of $\mathscr{A}$ are $m_{(2)} = m_{(3)} = n$. We then follow the proof of Theorem 32.20 in [34]. The Grunwald-Wang Theorem [34, Theorem 32.18] implies that there exists a cyclic extension L of $\mathbb{Q}$ such that

$$[L : \mathbb{Q}] = [L_{P_2} : \mathbb{Q}_2] = [L_{P_3} : \mathbb{Q}_3] = n \quad \text{and} \quad [L_{P_\infty} : \mathbb{Q}_\infty] = 1,$$

where P_2, P_3 and P_∞ are some extensions of (2), (3) and ∞ to L. The equation concerning the ramification of the infinite prime assures that the field L is totally real. Like in [34, Theorem 32.20] we conclude that L splits $\mathscr{A}$. This, combined with the fact that $[\mathscr{A} : L] = [L : \mathbb{Q}]^2$, implies that $\mathscr{A}$ is isomorphic to some cyclic algebra $(L/\mathbb{Q}, \sigma, \gamma)$, where $\gamma \in \mathbb{Q}^*$ and $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$. □

Remark 2.5.8. The matrix lattices that Corollary 2.5.7 promises to exist have the best known normalized minimum determinant.

Remark 2.5.9. The idea to construct real matrix lattices from real division algebras was first proposed in [5]. Lemma 2.5.5 is a trivial consequence of well known theory. Other results are proposed for the first time in this thesis.

Chapter 3

Analysis of some known codes

3.1 Codes from natural orders

In [21] and [12] the authors considered codes that were derived from the natural orders of division algebras with centers $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$. However, they did not determine the coding gain of their codes. In the following we give a simple method for the determination of the normalized minimum determinant for these codes. This method allows us to create a bound for the minimum determinants of codes from natural orders.

One should note that in order to prove the following lemma one should use the maximal representation ψ attached to the maximal cyclic subfield E. While the result does not depend on this, it is easier to use the simple form this particular ψ gives for the reduced trace (see Example 2.3.43).

Lemma 3.1.1. *Let F be such an algebraic number field that $\mathcal{O}_F$ is PID. Suppose that we have a cyclic division algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ and assume that γ is an algebraic integer of F. Let Λ be the natural order of Example 2.3.31. If $d(E/F)$ is the $\mathcal{O}_F$-discriminant of $\mathcal{O}_E$ (often referred to as the relative discriminant of the extension E/F), then*

$$d(\Lambda/\mathcal{O}_F) = d(E/F)^n \gamma^{n(n-1)}.$$

Proof. The natural order has an expansion as

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E \oplus \cdots \oplus u^{n-1}\mathcal{O}_E.$$

We immediately see that $u^i\mathcal{O}_E$ and $u^j\mathcal{O}_E$ are orthogonal to each other with respect to the bilinear form given by the reduced trace except in the cases where $i + j \equiv 0 \pmod{n}$. Assume that $\{x_1, \ldots, x_n\} = X$ is an $\mathcal{O}_F$-basis of $\mathcal{O}_E$. Then $\{1X, uX, \ldots, u^{n-1}X\}$ is a $\mathcal{O}_F$-basis for the order Λ.

We then see that the discriminant matrix of the order Λ consists of $n \times n$ blocks,

$$\begin{aligned}(tr_{\mathscr{A}/F}(u^i x_k u^j x_\ell))_{k,\ell=1}^n &= (u^{i+j} tr_{\mathscr{A}/F}(\sigma(x_k)^{-j} x_\ell))_{k,\ell=1}^n \\ &= (\gamma^\varepsilon (tr_{E/F}(\sigma(x_k)^{-j} x_\ell)))_{k,\ell=1}^n,\end{aligned}$$

on the diagonal. In these blocks the exponent ε is equal to zero or n according to whether $i+j$ equals zero or n. The former case occurs only once and the latter case occurs exactly $n-1$ times. Lemma 1.1.13 now implies the claim. □

The following corollary gives us a simple formula for the determination of the normalized minimum determinant of a natural order.

Corollary 3.1.2. *Let F be a complex quadratic field, such that $\mathscr{O}_F$ is PID, and $\mathscr{A}$ an F-central division algebra of index n. If Λ is a natural order in $\mathscr{A}$, then*

$$|d(\Lambda/\mathbb{Z})| = |d(E/\mathbb{Q})^n \gamma^{2n(n-1)}|$$

and

$$\delta(\Lambda) = \frac{2^{n/2}}{|d(\Lambda/\mathbb{Z})|^{1/4n}} = \frac{2^{n/2}}{|\gamma|^{(n-1)/2} |d(E/\mathbb{Q})|^{1/4}}.$$

Proof. Lemmas 2.3.53 and 3.1.1 give us that

$$|d(\Lambda/\mathbb{Z})| = |nr_{F/\mathbb{Q}}(d(\Lambda/\mathscr{O}_F)) d(F/\mathbb{Q})^{n^2}| = |\left(d(E/F)^n \gamma^{n(n-1)}\right)^2 d(F/\mathbb{Q})^{n^2}|.$$

According to Lemma 1.1.12 we then have

$$\begin{aligned}|(d(E/F)^n \gamma^{n(n-1)})^2 d(F/\mathbb{Q})^{n^2}| &= |(d(E/F)^2 d(F/\mathbb{Q})^n)^n (\gamma)^{2n(n-1)}| \\ &= |d(E/\mathbb{Q})^n \gamma^{2n(n-1)}|.\end{aligned}$$

□

In the following we prove that for the centers $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$ the natural orders cannot reach the bounds of Corollaries 2.4.32 and 2.4.33. Later on we will see that these considerations would have been necessary only for the division algebras of index 2. However, the proof of Proposition 3.1.4 gives us a better insight into this question than Proposition 3.1.8.

In the next lemma we use some basic results from the theory of discriminants and differents. For these results and the notion of the different we refer the reader to [22, Chapter 3.12].

Lemma 3.1.3. *Suppose we have a Galois extension E/F of degree n and that there are g prime ideals B_i of E lying over a prime P of F. If the prime P is wildly ramified in the extension E/F, then*

$$v_P(d(E/F)) \geq n.$$

Proof. Suppose that $D_{E/F}$ is the different of the extension E/F. The definition of the different reveals that

$$\sigma(D_{E/F}) = D_{E/F}$$

for every $\sigma \in \mathrm{Gal}(E/F)$. Therefore $v_{B_i}(D_{E/F}) = v_{B_j}(D_{E/F})$ for every i and j. Because P was supposed to be wildly ramified

$$s = v_{B_i}(D_{E/F}) \geq e, \tag{3.1}$$

where e is the ramification index of B_i/P.

The theory of normal extensions states that $efg = n$, where f is the inertial degree of B_i/P. Taking into account this and (3.1) we can conclude that

$$v_P(d(E/F)) = v_P(N_{E/F}(D_{E/F})) = sgf \geq egf = n.$$

□

Proposition 3.1.4. *Suppose we have a division algebra $\mathscr{D} = (E/\mathbb{Q}(i), \sigma, \gamma)$, where $[E : \mathbb{Q}(i)] = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathscr{D}$, then*

$$|d(\Lambda/\mathscr{O}_{\mathbb{Q}(i)})| > |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|.$$

Proof. The natural order Λ is a subset of some maximal order Λ_{max} and therefore $|d(\Lambda/\mathscr{O}_{\mathbb{Q}(i)})| \geq |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|$. Let us then assume that $|d(\Lambda/\mathscr{O}_{\mathbb{Q}(i)})| = |(2+i)^{n(n-1)}(1+i)^{n(n-1)}|$.

According to Lemma 3.1.1 the only primes that could be ramified in the extension $E/\mathbb{Q}(i)$ are $(1+i)$, $(2+i)$, and $(2-i)$. Lemma 3.1.3 assures that none of these primes can be wildly ramified.

One of the main results of the global class field theory [25, p. 123] states that there exists a ray class field $C_{(1+i)(2+i)(2-i)}$ that contains all the cyclic extensions of $\mathbb{Q}(i)$ where only $(1+i)$, $(2+i)$, or $(2-i)$ is tamely ramified.

We can now calculate the degree of the extension $C_{(2+i)(1+i)(2-i)}/\mathbb{Q}(i)$. By [25, Theorem 1.5] we have $[C_{(2+i)(1+i)(2-i)} : \mathbb{Q}(i)] = 2$, which implies that $E = C_{(2+i)(1+i)(2-i)}$ and $n = 2$.

The ray class fields $C_{(2+i)(1+i)}$ and $C_{(2-i)(1+i)}$ that admit tame ramification at $(2+i)$ and $(1+i)$ or, at $(2-i)$ and $(1+i)$ respectively, are both trivial extensions of $\mathbb{Q}(i)$. Hence, both $(2+i)$ and $(2-i)$ are ramified in E and divide the discriminant of the extension $E/\mathbb{Q}(i)$. The discriminant of the natural order Λ now has to be divisible by at least $(2+i)^2(2-i)^2$. This gives us a contradiction. □

Proposition 3.1.5. *Suppose we have a division algebra $\mathscr{D} = (E/\mathbb{Q}(\omega), \sigma, \gamma)$, where $E/\mathbb{Q}(\omega) = n$ and γ is an algebraic integer. If Λ is the natural order of the division algebra $\mathscr{D}$, then*

$$|d(\Lambda/\mathscr{O}_{\mathbb{Q}(\sqrt{-3})})| > |(\sqrt{-3})^{n(n-1)}2^{n(n-1)}|.$$

Proof. The proof is similar to that of the previous proposition. □

Remark 3.1.6. In the proof of Proposition 3.1.4 we encountered the ray class field $C_{(2+i)(2-i)}$ that is a degree two extension over the field $\mathbb{Q}(i)$ and has the minimal polynomial x^2-5. This field is the maximal subfield for which the cyclic generation of the golden algebra $\mathscr{GA}$ (see Subsection 3.2.1) is build.

Remark 3.1.7. The proof of Proposition 3.1.4 is also a good example of the problems we encounter if we try to imitate the proof of Theorem 2.4.26 in the commutative case. All the abelian extensions with tame ramification on only limited number of primes can have only limited degree. If we like to consider larger extensions we have to allow either wild ramification or ramification in a larger set of prime ideals.

The following proposition reveals that the normalized minimum determinants of natural orders are quite far from the bounds of Corollaries 2.4.32 and 2.4.33.

Proposition 3.1.8. *Let F be a complex quadratic field, such that $\mathscr{O}_F$ is PID. If Λ is a natural order in an F-central division algebra $(E/F,\sigma,\gamma)$ of index n, then*

$$|d(\Lambda/\mathbb{Z})| \geq |C_{2n}^{2n^2}|$$

and

$$\delta(\Lambda) \leq \frac{2^{n/2}}{C_{2n}^{n/2}}.$$

Proof. We note that the maximal cyclic subfield E is always totally complex and has degree $2n$ over $\mathbb{Q}$. The claims now follow directly from the Odlyzko's bound 1.1 and Lemma 3.1.1.

□

Remark 3.1.9. We note that the bound in Proposition 3.1.8 is not very tight, because it does not take into account the effect of the non-norm element. For example, when the center is $\mathbb{Q}(i)$, the non-norm element has to be at least $1+i$ when $n>4$.

We denote the previous bound by B_{nat}. In the following figure we present $(B_{nat})^{-2/n}$ and $(B_{\mathbb{Q}(i)})^{-2/n}$ for values less than 50.

The following example suggests that actually the values of discriminants of the natural orders are considerably larger than the bound B_{nat}.

Example 3.1.10. Let $\zeta_\ell = \exp(2\pi i/2^\ell)$ be a complex 2^lth root of unity, where $\ell \geq 2$ is an integer. Then $n = [\mathbb{Q}(\zeta_\ell):\mathbb{Q}(i)] = 2^{\ell-2}$. In [21] Kiran and Rajan proved that the family of cyclic algebras

$$\mathscr{A}_\ell = (\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(i), \sigma(\zeta_\ell) = \zeta_\ell^5, 2+i),$$

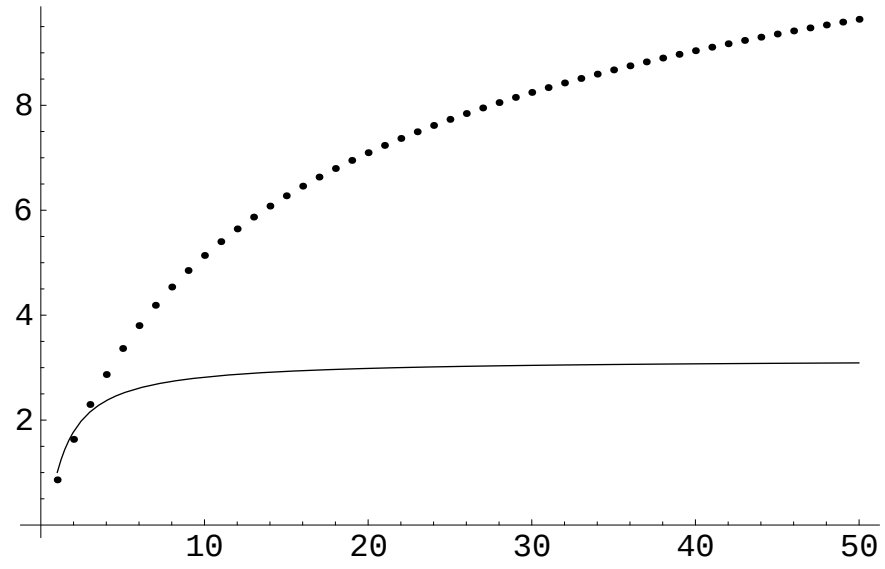


Figure 3.1: $(B_{nat})^{-2/n}$ (dots) vs $(B_{\mathbb{Q}(i)})^{-2/n}$ (solid)

with $\ell \geq 3$, consists entirely of division algebras. Let $\Lambda_{nat,\ell}$ be the natural order of the algebra $\mathscr{A}_\ell$. It is then easily calculated that

$$d(\mathbb{Z}[\zeta_\ell]/\mathbb{Z}[i]) = (1+i)^{2n(l-2)} = (1+i)^{2n\log_2(n)}.$$

Lemma 3.1.1 then gives us that the discriminant of the natural order $\Lambda_{\ell,nat}$ of $\mathscr{A}_\ell$ is

$$|d(\Lambda_\ell/\mathbb{Z}[i])| = |(1+i)^{2n^2\log_2(n)}(2+i)^{n(n-1)}| = n^{n^2}5^{n(n-1)/2}.$$

Remark 3.1.11. Lemma 3.1.1 is true also in the case where the ring $\mathscr{O}_F$ is not a PID, but for simplicity we proved it only in the PID case. The general result is easy to see by localization. This implies that we can forget the PID condition also in Proposition 3.1.8 and in Corollary 3.1.2.

Remark 3.1.12. The results in Section 3.1 are from [18] except Proposition 3.1.8 and Corollary 3.1.2 which are presented for the first time here.

3.2 Codes with shaping

Recently, in [30] the authors considered a family of MIMO codes, the so-called *perfect codes*. One of the characteristics of their codes was that when vectorized the codes had a certain shape. For HEX-information symbols the shape is $A_2^{n^2}$ and for *QAM*-symbols it is $\mathbb{Z}^{2n^2}$.

One of the drawbacks of perfect codes was that they exist only for restricted number of antennas. In [11] the authors considered a generalization of the perfect codes and achieved two infinite families of codes. Again their codes were constructed so that all the codes had shape $A_2^{n^2}$ or $\mathbb{Z}^{2n^2}$.

In next section we are going to analyze the perfect codes of [30] thoroughly. However, our order theoretic methods are not sufficient for determining the normalized minimum determinants of the codes in [11].

Still the geometric shape of codes in [30] and [11] allows us to apply the simple results of Section 2.2 and give strong bounds for the minimum determinants for all the shaped codes in [30] and [11]. The bound B_{ort} is applicable for the codes with shape $\mathbb{Z}^{2n^2}$ and the bound B_{hex} is suitable for the codes that have the shape $A_2^{n^2}$. In the following pictures we compare B_{ort} to the bound $B_{\mathbb{Q}(i)}$ and B_{hex} to the bound $B_{\mathbb{Q}(\omega)}$.

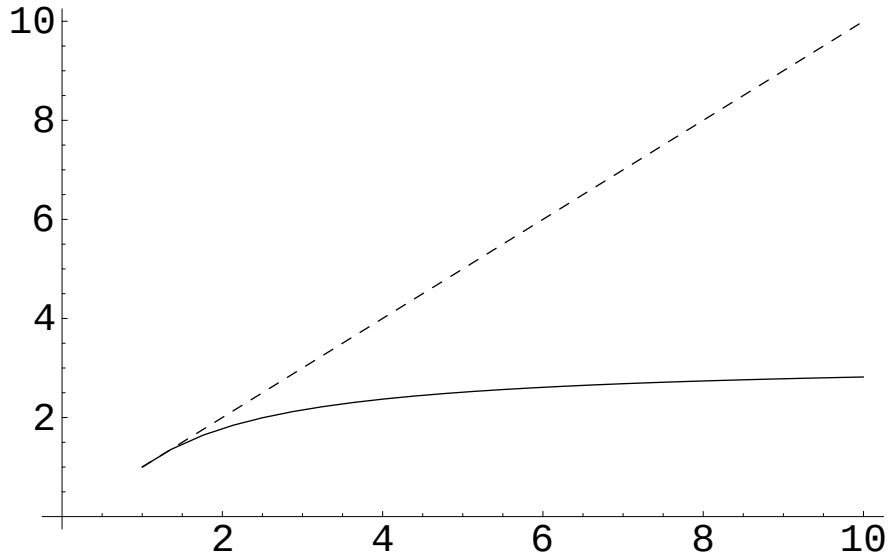


Figure 3.2: $(B_{ort})^{-2/n}$ (dots) vs $(B_{\mathbb{Q}(i)})^{-2/n}$ (solid)

When we look at the formulas for the minimum determinants of maximal orders and the formula for the orthogonal bound it is evident that no orthogonal code can have the minimum determinants of the codes Λ_n^i and Λ_n^ω and that the difference increases when n grows. The problem here is that rectangular lattices always have too short minimum vector.

The same can be said about the bound B_{hex} and the maximal orders Λ_n^i and Λ_n^ω with one exception when $n = 2$, $B_{hex} = 0.577...$, and $\delta(\Lambda_2^i) = 0.562...$.

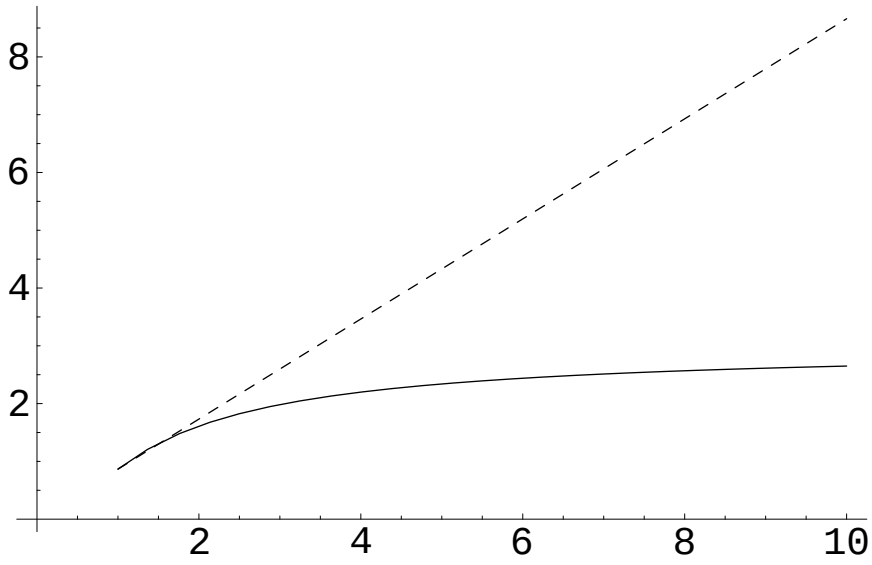


Figure 3.3: $(B_{hex})^{-2/n}$ (dots) vs $(B_{\mathbb{Q}(\omega)})^{-2/n}$ (solid)

3.2.1 Perfect codes

In the following we will analyze the perfect codes of [30]. Specifically, we are going to discuss the structure of the underlying algebras. In order to do so, we have to prove some results that allow us to use our previous machinery also in this situation.

Lemma 3.2.1. *Let Λ be an order in a cyclic division algebra of index n over an imaginary quadratic number field. Let $x \in \Lambda$ be any non-zero element, then*

$$\delta(\Lambda x) = \delta(\Lambda).$$

Proof. By the multiplicativity of the norm the minimum determinant of Λx is equal to the absolute value of $nr_{\mathscr{A}/F}(x)$. Let us now determine how the fundamental parallelotope of Λx is related to the fundamental parallelotope of Λ.

We have that $[\Lambda : \Lambda x] = |N_{\mathscr{A}/\mathbb{Q}}(x)|$ (see [34, Exercise 7, p. 131]). On the other hand , Remark 2.3.46 tells us that

$$\begin{aligned} |N_{\mathscr{A}/\mathbb{Q}}(x)| &= |(nr_{\mathscr{A}/\mathbb{Q}}(x))^n| \\ &\overset{\text{Definition 2.3.45}}{=} |(nr_{F/\mathbb{Q}}(nr_{\mathscr{A}/F}(x)))^n| \\ &\overset{[F:\mathbb{Q}]=2}{=} |nr_{\mathscr{A}/F}(x)^n|^2 \\ &= |nr_{\mathscr{A}/F}(x)|^{2n}. \end{aligned}$$

Hence, $[\Lambda : \Lambda x] = |nr_{\mathscr{A}/F}(x)|^{2n}$. This implies

$$m(\Lambda)|nr_{\mathscr{A}/F}(x)|^{2n} = m(x\Lambda),$$

and therefore

$$\delta(\Lambda x) = \frac{|nr_{\mathscr{A}/F}(x)|}{(m(\Lambda x))^{1/2n}} = \frac{1}{(m(\Lambda))^{1/2n}} = \delta(\Lambda).$$

□

We note that while the minimum determinant is invariant on multiplying with an element the same is not true when we consider the length of the minimum vector. Still we are not totally helpless.

Proposition 3.2.2. *Suppose that $\mathscr{A}$ is a division algebra of index n with a center $F = \mathbb{Q}(i)$ or $F = \mathbb{Q}(\omega)$. If Λ is an $\mathscr{O}_F$-order of $\mathscr{A}$ and x is an element of Λ then*

$$\mathrm{Nsv}(\Lambda) \leq \mathrm{Nsv}(\Lambda x).$$

Proof. Lemma 2.2.2 and the proof of Proposition 2.4.1 shows that $(\delta(\Lambda))^{1/n} \cdot \sqrt{n} = \mathrm{Nsv}(\Lambda)$. Similarly Lemma 2.2.2 gives that $(\delta(\Lambda x))^{1/n} \cdot \sqrt{n} \leq \mathrm{Nsv}(\Lambda x)$. According to Lemma 3.2.1 we have $\delta(\Lambda) = \delta(\Lambda x)$. □

Proposition 3.2.3. *Let $\mathscr{D}_1 = (E_1/F, \sigma_1, \gamma_1)$ and $\mathscr{D}_2 = (E_2/F, \sigma_2, \gamma_2)$ be division algebras that have coprime indices m_1 and m_2. Then $\mathscr{D}_1 \otimes \mathscr{D}_2$ is a division algebra with an index $m_1 m_2$. Furthermore,*

$$\mathscr{D}_1 \otimes \mathscr{D}_2 \simeq (E_1E_2/F, \sigma_1\sigma_2, \gamma_1^{m_2}\gamma_2^{m_1}),$$

where $\sigma_1\sigma_2$ is an element of $\mathrm{Gal}(E_1E_2/F) \simeq \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

Let P_1 and P_2 be some pair of minimal prime ideals of the field F. If $\mathscr{D}_1$ and $\mathscr{D}_2$ have minimal discriminants that are only divisible by P_1 and P_2, then $\mathscr{D}_1 \otimes \mathscr{D}_2$ has a minimal discriminant that is only divisible by P_1 and P_2.

Proof. For the proof of the first two claims we refer the reader to [2, Theorem 20, p. 99]. The only nontrivial Hasse invariants of the division algebras $\mathscr{D}_1$ and $\mathscr{D}_2$ are those associated with the primes P_1 and P_2. The mappings in the fundamental exact sequence (2.7) are homomorphisms of groups. Together with the fact that extending scalars to a P-adic completion commutes with the formation of a tensor product shows that the Hasse invariants of $\mathscr{D}_1 \otimes \mathscr{D}_2$ are sums of those of $\mathscr{D}_1$ and $\mathscr{D}_2$. Hence, the discriminant of $\mathscr{D}_1 \otimes \mathscr{D}_2$ is only divisible by the prime ideals P_1 and P_2. By the proof of Theorem 2.4.26 it is then minimal. □

Suppose we have a finite cyclic extension E/F of algebraic number fields. Let P be a prime of F and B some prime of E that lies over P. We denote the completion E_B by E_P or $E \cdot F_P$. This notation is valid in Galois extensions, because the fields E_B are isomorphic for all primes B that lie over P.

In the following we give an algebraic analysis of perfect codes. The resulting numerical data is collected into Table 3.1.

2×2 perfect code

The first perfect algebra is the same as the Golden algebra $\mathscr{GA} = (E/F, \sigma, \gamma)$, where the extension $E/F = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$ has discriminant $(2+i)(2-i)$. The discriminant of the natural order is therefore $(2+i)^2(2-i)^2$. Because the discriminant of the algebra $\mathscr{GA}$ divides $(2+i)^2(2-i)^2$ it can have at maximum two prime divisors $(2+i)$ and $(2-i)$. As a consequence the only Hasse invariants that can be nontrivial are $h_{(2+i)}$ and $h_{(2-i)}$.

The algebra $\mathscr{GA}$ must have at least two nontrivial Hasse invariants and therefore $h_{(2+i)}$ and $h_{(2-i)}$ are both nontrivial. Combining the equations

$$LCM[m_{(2+i)}, m_{(2-i)}] = 2$$

and $h_{(2+i)} + h_{(2-i)} = 1$ we get that $h_{(2+i)} = h_{(2-i)} = 1/2$. Theorem 2.4.21 states that the discriminant of $\mathscr{GA}$ is $(2+i)^2(2-i)^2$. Comparing this to the discriminant of the natural order we see that the natural order Λ_2 is maximal. The actual code is then

$$B_2 = \frac{1}{c}\Lambda_2 a$$

where $a \subseteq \mathscr{O}_E$ and $c \in \mathbb{R}$ is normalizing factor. The element a is chosen so that the vectorized code has shape $\mathbb{Z}^{2n^2}$.

3×3 perfect code

The underlying algebra of the 3×3 perfect code is $\mathscr{P}_3 = (E/F, \sigma, \omega)$, where again $\omega = (-1+\sqrt{-3})/2$, $F = \mathbb{Q}(\omega)$, $E = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \omega)$ and $\sigma : \zeta_7 + \zeta_7^{-1} \longmapsto \zeta_7^2 + \zeta_7^{-2}$. The algebra $\mathscr{P}_3$ has a representation as

$$L \oplus u \cdot L \oplus u^2 \cdot L$$

where $u^3 = \omega$.

The discriminant of the extension E/F is $(2+\sqrt{-3})^2(2-\sqrt{-3})^2 = P_1^2 P_2^2$ and the discriminant of the natural order has therefore only two prime factors. By Lemma 2.4.34 the only nontrivial Hasse invariants of $\mathscr{P}_3$ are h_{P_1} and h_{P_2}. Because LCM $[m_{P_1}, m_{P_2}] = 3$. We get that $m_{P_1} = m_{P_2} = 3$.

To calculate the Hasse invariant h_{P_1} we pass to the completion $\mathscr{P}_{P_1} = F_{P_1} \otimes \mathscr{P}_3$. From Theorem 2.3.29 we get a cyclic generation

$$\mathscr{P}_{P_1} = (E_{P_1}/F_{P_1}, \sigma_{P_1}, \omega),$$

where E_{P_1}/F_{P_1} is a totally ramified extension and σ_{P_1} is the natural extension of the automorphism σ. Because the local index $m_{P_1} = 3$, we know that $\mathscr{P}_{P_1}$ is a division algebra.

Next we try to find another cyclic generation for this algebra so that we can use the definition of Hasse invariant to calculate the value of h_{P_1}.

It is readily verified that the field $F_{P_1}(u) = T_{P_1} \subseteq \mathscr{P}_{P_1}$ is a cyclic and totally inert extension of F_{P_1}. The Frobenius automorphism of the extension T_{P_1}/F_{P_1} is defined by the $(T_{P_1}/F_{P_1}, P_1)(u) = u^7$. The Noether-Skolem Theorem ([34, Theorem 7.21]) states that there is an element $x \in \mathscr{P}_{P_1}$ such that

$$(T_{P_1}/F_{P_1}, P_1)(a) = x^{-1}ax \quad \forall a \in T_{P_1}. \tag{3.2}$$

For an element x to fulfill (3.2) it is enough to satisfy the equation

$$(T_{P_1}/F_{P_1}, P_1)(u) = u^7 = xux^{-1}.$$

By considering the equation $ux = xu^7 = x\omega^2 u$ we see that $x = \zeta_7 + \zeta_7^{-1} + \omega^2(\zeta_7^2 + \zeta_7^{-2}) + \omega(\zeta_7^4 + \zeta_7^{-4}) \in L$ is a suitable element.

We now prove that x^3 is an element of F_{P_1}, and that $v_{P_1}(x^3) = 1$. The first statement follows from $u\sigma(x^3) = x^3u = x^2u\omega^2x = ux^3$. The second statement is obtained from the equation $v_{P_1}(x^3) = v_{P_1}(nr_{E/F}(x)) = v_{P_1}(7(2 + (\sqrt{-3}))\omega) = 2$.

Proposition 2.3.10 now states that $\mathscr{B}_1 = (T_{P_1}/F_{P_1}, (T_{P_1}/F_{P_1}, P_1), x^3)$ is a division algebra of index 3. By (3.2) we can consider $\mathscr{B}_1$ as a subset of the algebra $\mathscr{P}_3$. But $\mathscr{B}_1$ is a F_{P_1}-central division algebra and hence a 9 dimensional over F_{P_1}. From this we can conclude that $(T_{P_1}/F_{P_1}, (T_{P_1}/F_{P_1}, P_1), x^3) = \mathscr{P}_{P_1}$.

Proposition 4.2.6 now implies that $h_{P_1} = 2/3$. Because the sum of the Hasse invariants has to be an integer, the invariant h_{P_2} equals $1/3$.

By considering the local indices we see that the discriminant of the maximal order is $P_1^6P_2^6$, that is, equal to the discriminant of the natural order Λ_6. Thus, the natural order has to be maximal.

The actual code B_3 is produced similarly to the 2×2 case with exception that the vectorized code lattice has now shape $A_2^{n^2}$.

4×4 **perfect code**

The underlying division algebra under the 4×4 perfect code is $\mathscr{P}_4 = (E/F, \sigma, i)$, where $\mathbb{Q}(i) = F$, $\mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1}) = E$ and $\sigma : \zeta_{15} + \zeta_{15}^{-1} \longmapsto \zeta_{15}^2 + \zeta_{15}^{-2}$.

The extension $E/\mathbb{Q}(i)$ has discriminant $d(E/\mathbb{Q}(i)) = (2+i)^3(2-i)^3(3)^2$, and the only Hasse invariants that can be nontrivial are $h_{(3)}, h_{(2+i)}$ and $h_{(2-i)}$. We use similar methods to those in the case of $\mathscr{P}_3$ to get that $h_{(2+i)} = 3/4$ and $h_{(2-i)} = 1/4$. The sum $h_{(2-i)} + h_{(2+i)} = 1$ and therefore $h_{(3)}$ must be trivial. Further, the local indices reveal that the discriminant of the algebra is $(2+i)^{12}(2-i)^{12}$. The discriminant of the natural order on the other hand is $(2+i)^{12}(2-i)^{12}(3)^8$.

The code B_4 is again constructed by using a principal ideal of the natural order.

6×6 perfect code

In the 6×6 perfect code construction the center is $F = \mathbb{Q}(\omega)$ and the maximal subfield $E = K(\theta)$, where $\theta = \zeta_{28} + \zeta_{28}^{-1}$.

In [30] where the perfect codes were introduced, the authors gave the mapping σ_1 by the equation $\sigma_1 : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^2 + \zeta_{28}^{-2}$. Unfortunately, this mapping is not an F-automorphism of the field E. We replace σ_1 with the automorphism σ defined by the equation $\sigma : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^5 + \zeta_{28}^{-5}$. The relative discriminant of the extension E/F is $(2)^6(2+\sqrt{-3})^5(2-\sqrt{3})^5 = (2)^6(7)^5$. We denote the resulting algebra by $\mathscr{P}_6$.

Thus the Hasse invariants of $\mathscr{P}_6$ that can be nontrivial are $h_{(2+\sqrt{-3})}$, $h_{(2-\sqrt{-3})}$, and $h_{(2)}$.

Now we are going to present $\mathscr{P}_6$ as a product of two smaller division algebras. We first calculate the Hasse invariants of these smaller algebras and then from these derive the Hasse invariants of $\mathscr{P}_6$.

Let us first consider the algebra $\mathscr{B}_2 = (\mathbb{Q}(\sqrt{7},\omega)/\mathbb{Q}(\omega), \sigma_2, -\omega)$. The algebra $\mathscr{B}_2$ is a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = h_{(2+\sqrt{-3})} = 1/2$. The proof is postponed until the end of Section 4.1.

The algebra $\mathscr{P}_3 = (E/F, \sigma_3, \omega)$ was previously shown to be a division algebra with Hasse invariants $h_{(2-\sqrt{-3})} = 2/3$ and $h_{(2+\sqrt{-3})} = 1/3$. We now consider the algebra $\mathscr{B}_3 = (E/F, \sigma_3, \omega^2)$. By [34, Theorem 30.4] we have $\mathscr{P}_3 \otimes \mathscr{B}_3 \sim (E/F, \sigma_3, 1) \simeq M_3(F)$. This shows that $\mathscr{P}_3 \otimes \mathscr{B}_3$ has trivial Hasse invariants and therefore the Hasse invariants of $\mathscr{B}_3$ are $h_{(2-\sqrt{-3})} = 1/3$ and $h_{(2+\sqrt{-3})} = 2/3$.

If we now consider the algebra $\mathscr{B}_2 \otimes \mathscr{B}_3 \simeq$

$$\simeq (\mathbb{Q}(\sqrt{7},\omega) \cdot \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \omega)/\mathbb{Q}(\omega), \sigma_2\sigma_3, (-\omega)^3 \cdot (\omega^2)^2)$$

it is seen that the corresponding Hasse invariants are $h_{(2-\sqrt{-3})} = 1/3 + 1/2 = 5/6$ and $h_{(2+\sqrt{-3})} = 1/2 + 2/3 \equiv 1/6 \pmod 1$.

By considering the equation $\sigma_3(\zeta_7 + \zeta_7^{-1}) = \zeta_7^2 + \zeta_7^{-2} = \zeta_7^5 + \zeta_7^{-5}$ we notice that $\sigma_2\sigma_3 = \sigma_6$. Combining this and the equation $(-\omega)^3 \cdot \omega^4 = -\omega$ we get that $\mathscr{B}_3 \otimes \mathscr{B}_2 \simeq \mathscr{P}_6$.

The algebra $\mathscr{P}_6$ has only two nontrivial Hasse invariants that are $h_{(2+\sqrt{-3})} = 5/6$ and $h_{(2-\sqrt{-3})} = 1/6$. Whence, the discriminant of the maximal order is $(2-\sqrt{-3})^{30}(2+\sqrt{-3})^{30} = (7)^{30}$. On the other hand the discriminant of the natural order is $(2)^{36}(7)^{30}$.

The actual code B_6 now has form

$$\frac{1}{c}\Lambda_n I$$

where I is a non-principal ideal of $\mathscr{O}_E$ and $c \in \mathbb{R}$ is a normalizing element. Again I is chosen so that the shape of the lattice is $A_2^{6^2}$. Here our methods fail to deter-

mine the exact value of the normalized minimum determinant. In [30] the authors represent an upper and lower bounds for the minimum determinant.

Into Table 3.1 we have collected the information of the normalized minimum determinants and shortest vectors of the perfect codes and of the underlying natural orders. For a comparison we have added the bound B_{ort} or B_{hex} depending on the index under consideration. We refer to these values with $B_{ort/hex}$.

As an example we show how the values for the first row of the table 3.1 has been calculated. The discriminant of the natural order Λ_2 of the golden algebra $\mathscr{GA}$ is $(2+i)^2(2-i)^2$. This implies that the volume of the fundamental parallelotope is 25. Corollary 2.4.2 then gives that $\mathrm{Nsv}(\Lambda_2) = 0.95$ and that $\delta(\Lambda_2) = 0.45$.

The actual code B_2 is then $a\Lambda_2$ where a is a suitable element of the natural order. Lemma 3.2.1 states that $\delta(\Lambda_2 a) = \delta(\Lambda_2) = 0.45$. But as the code is orthonormal we have that $\mathrm{Nsv}(a\Lambda) = 1$. This is a good example of the phenomenon, where $\mathrm{Nsv}(\Lambda) < \mathrm{Nsv}(\Lambda a)$.

Table 3.1:

n	$B_{ort/hex}\delta(n)$	$\delta(\Lambda_n)$	$\delta(B_n)$	$\mathrm{Nsv}(\Lambda_n)$	$\mathrm{Nsv}(B_n)$
2	0.50	0.45	0.45	0.95	1
3	0.24	0.14	0.14	0.97	1.07
4	0.06	0.03	0.03	0.83	1
6	0.007	0.0001	?	0.77	1.07

If we compare the perfect codes to the orthogonal $B_{ort}(n)$ and the hexagonal $B_{hex}(n)$ bounds, the minimum determinants of the codes are quite close to these bounds. Still there is quite a much room for possible improvements.

Into the Table 3.2 we have collected values comparing the normalized minimum determinants of perfect codes and maximal order codes. For a comparison we have also added the bounds $B_{hex}(n)$ and $B_{ort}(n)$.

Table 3.2:

n	$\delta(\Lambda_n^i)$	$\delta(\Lambda_n^\omega)$	$B_{hex}(n)$	$\delta(B_n)$	$B_{ort}(n)$
2	0.562	0.620	0.577	0.447	0.500
3	0.316	0.358	0.239	0.14	0.192
4	0.177	0.207	0.083	0.030	0.063
5	0.100	0.119	0.026		0.018
6	0.056	0.069	0.007	?	0.005

In the following figure we present the performance of Golden code and the code from maximal order of the algebra $\mathscr{G}_2$ (Section 4.1.2), that reaches the bound $B_{\mathbb{Q}(\omega)}$. In Section 4.3 we briefly describe how the simulations were done.

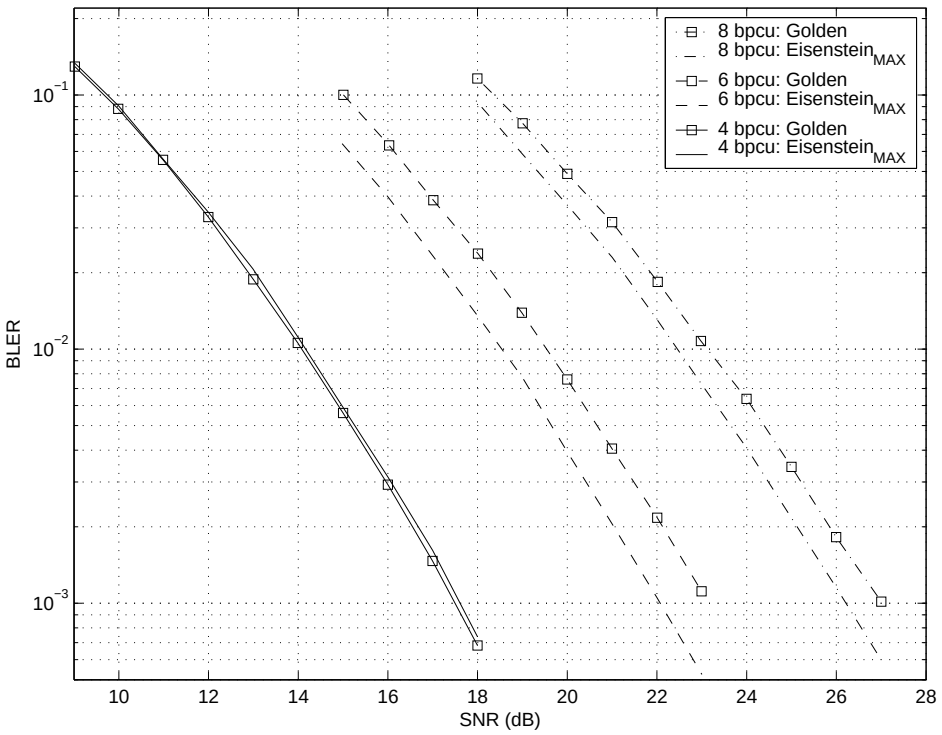


Figure 3.4: The Golden code vs maximal order of $\mathscr{G}_2$

Remark 3.2.4. While the raw block error rate performance of the maximal order code $\mathscr{G}_2$, for most data rates, is better than the performance of the golden code one should note that the comparison is not totally fair. This is due the fact that the orthogonal shape allows a simple bit labeling strategy. For maximal orders one must use a look up table. This is not a bad problem as the use of look up tables is rather common in applications. However, at the moment it is not totally clear how the bit labeling should be done so that the good block error rates will get realized as good bit error rates.

Remark 3.2.5. The results in Section 3.2 are from [18], except the determination of the shortest vectors and comparison to orthogonal and hexagonal bounds which was done in [23]. One should note that the coding gain of the perfect codes was already determined by the inventors in [30].

Chapter 4

Constructing division algebras with a minimal discriminant

In Section 2.4.4 we proved the existence of extremely attractive MIMO codes with largest known coding gain. We even described them well. Still these promising codes seem to exist only as an abstract objects in the depths of class field theory, far from being usable in the actual transmission.

In this chapter we take first steps to find the actual codes by giving an explicit construction of division algebras with minimal discriminants. After the correct algebra is found we can use existing algorithms to find the maximal order (see [38, 16]). We return to this subject in the end of this thesis.

Two of the codes we will construct has also been tested on computer simulations (see [18] and Figure 3.4) and performed excellently.

In the following we give an explicit construction for $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$-central division algebras with minimal discriminants. When one is using natural orders for code construction, large non-norm element may result in a power imbalance between transmitting antennas. While this is not so clear, when we are using maximal orders, the test data we have collected [18] suggests that the big non-norm element may negatively affect the performance of the code. Therefore it is beneficial to aim at small non-norm elements. However, as noted in [30], we can choose an unit non-norm element only when $n < 7$.

We have divided this section into two parts. In the first part we are concentrating on algebras that have a cyclic generation with a unit non-norm element γ.

In the second part we relax the restriction on the size of γ and we give a general construction for $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$-central division algebras with a minimal discriminant.

4.1 Algebras with a unit γ

4.1.1 Center $\mathbb{Q}(i)$

Table 4.1: $\mathbb{Q}(i)$-central division algebras with a unit γ

n	γ	f_n
2	i	$x^2+(2+i)$
4	i	$x^4+(2+i)$

In Table 4.1 we give a cyclic generation for algebras of degree 2 and 4 with minimal discriminants. Proposition 2.3.8 implies that 4 is the largest degree that we can hope to have a cyclic division algebra with a unit γ. There does not exist such an algebra of degree 3. The reason for this is that in every cyclic extension $E/\mathbb{Q}(i)$ of degree 3, all the units of $\mathbb{Q}(i)$ are third powers and therefore are in the image of the norm $N_{E/\mathbb{Q}(i)}$.

In the following we use the generic notation $\mathbb{Q}(i)=F$ and $E=F(a_n)$, where a_n is a zero of the polynomial f_n, and prove that the algebras in Table 4.1 are division algebras with minimal discriminants.

Algebra $\mathscr{D}_2$: For the proof we refer the reader to [18]. Alternate proof can be made by following the strategy of the next case.

Algebra $\mathscr{D}_4$: When considering $\mathscr{D}_4$ we first have to check whether it really is a division algebra. We note that $(2+i)$ is a totally ramified prime in E/F. Consequently the local extension $E_{(2+i)}/F_{(2+i)}$ is totally and tamely ramified cyclic extension of degree 4. We note that $\#(\mathscr{O}_{F_{(2+i)}}/(2+i)\mathscr{O}_{F_{(2+i)}})=\#(\mathscr{O}_F/(2+i))=5$.

Proposition 2.3.8 states that $\mathscr{D}_4$ is a division algebra if i satisfies the norm condition, i.e. none of the elements $\{i,-1,-i\}$ is a norm.

Hasse Norm Theorem [34, Theorem 32.8] states that it is enough to show that the elements $\{i,-1\}$ are not norms in the extension $E_{(2+i)}/F_{(2+i)}$. Elementary local theory [26, Proposition 7.19] states that if we have any complete residue system $\{0,1,a,b,c\}$ of the group $\mathscr{O}_{F_{(2+i)}}/(2+i)\mathscr{O}_{F_{(2+i)}}$ and an arbitrary unit $e\in F_{(2+i)}$ then

$$F^*_{(2+i)}=\{1,a,b,c\}\times(1+(2+i)\mathscr{O}_{F_{(2+i)}})\times\langle e(2+i)\rangle. \tag{4.1}$$

The prime $(2+i)$ is tamely ramified in $E_{(2+i)}/F_{(2+i)}$ and therefore the local conductor is $(2+i)$ (see Lemma 1.1.17). The definition of the conductor now implies that $(1+(2+i)\mathscr{O}_{F_{2+i}})\subseteq N_{E_{(2+i)}/F_{(2+i)}}(E_{(2+i)})$. Because the prime $(2+i)$

is totally ramified, we have $e_1(2+i) \subseteq N_{E_{(2+i)}/F_{(2+i)}}(E_{(2+i)})$ for some unit $e_1 \in F_{(2+i)}$. The previous results now imply that $(1+(2+i)\mathscr{O}_{E_{(2+i)}}) \times \langle e_1(2+i)\rangle \subseteq N_{E_{(2+i)}/F_{(2+i)}}(E_{(2+i)})$.

On the other hand one of the main theorems of local class field theory [25, Theorem 1.1] states that $F^*_{(2+i)}/(N_{E_{(2+i)}/F_{(2+i)}}(E^*_{2+i})) = \mathrm{Gal}(E_{(2+i)}/F_{(2+i)})$. By considering (4.1) we see that the elements $\{a,b,c\}$ are not norms. Because the elements $\{0,i,-1,-i,1\}$ form a complete residue system of the group $\mathscr{O}_{E_{(2+i)}}/(2+i)\mathscr{O}_{E_{(2+i)}}$ we find that none of the elements $\{i,-1,-i\}$ is a norm.

The discriminant of the extension E/F has only two prime divisors $(2+i)$ and $(1+i)$ and therefore also the discriminant of the natural order of $\mathscr{D}_4$ has only two prime divisors. This implies that the discriminant of the algebra is minimal.

4.1.2 Center $\mathbb{Q}(\sqrt{-3})$

Table 4.2: $\mathbb{Q}(\sqrt{-3})$-central division algebras with a unit γ

n	γ	f_n
2	$-\omega$	$x^2+\sqrt{-3}$
3	ω	x^3-2
6	$-\omega^2$	$x^6-3\sqrt{-3}x^4+4x^3-9x^2+12\sqrt{-3}x+3\sqrt{-3}+4$

In Table 4.2 we give cyclic generations for algebras of degrees $2,3$, and 6. The theorem of Albert 2.3.8 shows that 6 is the biggest degree we could hope to have a division algebra with a unit γ. We cannot have a division algebras of degrees 4 and 5 as tensoring these with a division algebra $\mathscr{G}_3$ (below) would give us division algebras of degrees 12 and 15 respectively with a unit γ.

We use the same generic notation as in the case of $\mathbb{Q}(i)$-central algebras.

Algebra $\mathscr{G}_2$: We use here the same methods that were used with the algebra $\mathscr{D}_4$. We remark that $P=(\sqrt{-3})$ is tamely ramified in the extension E/F. If we pass to the completion E_P/F_P we get that the local conductor is P and that $\{-\omega,1,0\}$ is a complete set of representatives of the group $\mathscr{O}_{F_P}/P$. As a result it is seen that $-\omega$ is not a norm in the extension E_P/F_P and therefore it is not a norm in the extension E/F either. From this it follows that $\mathscr{G}_2$ is a division algebra.

By now it is obvious that the discriminant of the natural order of the algebra $\mathscr{G}_2$ has only two divisors $(\sqrt{-3})$ and (2), and hence the maximal order admits a minimal discriminant.

Algebra $\mathscr{G}_3$: The proof of this case is similar to that of $\mathscr{G}_2$ except that the tamely ramified prime P is 2, and that the suitable set of representatives is $\{1,\omega,\omega^2\}$.

Algebra $\mathscr{G}_6$: The algebra $\mathscr{G}_6$ we get as a tensor product from the algebras $\mathscr{G}_2$ and $\mathscr{G}_3$.

Determination of Hasse invariants of $\mathscr{B}_2$: When we were discussing the 6×6 perfect code we postponed the analysis of the algebra $\mathscr{B}_2 = (E/F, \sigma_2, -\omega)$, where $E/F = \mathbb{Q}(\sqrt{7}, \omega)/\mathbb{Q}(\omega)$. Now we have enough methods to attack this problem. We use similar strategy as in the case of the algebra $\mathscr{D}_4$.

The prime $(2+\sqrt{-3}) = P_1$ is tamely ramified in the extension E/F. By passing to the P_1-adic completion E_{P_1}/F_{P_1} we find that the local conductor is P_1. The image of the norm $N_{E_{P_1}/F_{P_1}}$ includes $\langle(1+P_1)\rangle \times \langle e(2+\sqrt{-3})\rangle$, where e is a unit of F_{P_1}.

The set $\{0, 1, \omega, -\omega, \omega^2, -\omega^2\}$ is a complete residue system of the group $\mathscr{O}_{F_{P_1}}/P_1\mathscr{O}_{F_{P_1}}$ and whence

$$F_{P_1}^* = \langle -\omega\rangle \times (1+P_1) \times \langle e(2+\sqrt{-3})\rangle.$$

On the other hand, $\#((F_{P_1})^*/N_{E_{P_1}/F_{P_1}}(E_{P_1}^*)) = 2$ and therefore $-\omega$ cannot be a norm. From this it follows that the local algebra $(\mathscr{B}_2)_{P_1}$ is a division algebra of index two.

There is no other choice for the Hasse invariant h_{P_1} than $1/2$.

Replacing the prime P_1 with $P_2 = (2-\sqrt{-3})$ in the above considerations we see that $h_{P_2} = 1/2$.

The extension E/F has only three ramified primes $(2-\sqrt{-3}), (2+\sqrt{-3})$, and (2). Thus, the discriminant of the algebra $\mathscr{B}_2$ can have three prime divisors at maximum. The potential nontrivial Hasse invariants of $\mathscr{B}_2$ are now h_{P_1}, h_{P_2}, and $h_{(2)}$. The sum of h_{P_1} and h_{P_2} is 1, and therefore $h_{(2)}$ must be trivial.

4.2 General construction

In their recent paper [12] Elia et al. gave an explicit construction for division algebras of an arbitrary degree with centers $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. In their general constructions they used non-unit, but relatively small, non-norm elements. As they were not interested in maximal orders nor the discriminants of the corresponding division algebras their algebras (with few exceptions) did not happen to have minimal discriminants.

We are now going to give a general construction for division algebras of arbitrary degree and with minimal discriminants. According to Proposition 3.2.3 it suffices to study the case, where the index is a prime power. As a drawback our constructions will be dependent on the existence of certain prime numbers. We discuss this existence problem in Section 4.2.1 which is purely number theoretic. We note that the fields we use in our construction are just simple modifications of the fields in [33].

We first consider two easy prime powers and then move forward to more complicated ones.

For ease of notation in this subsection we will denote by $\mathbb{Z}_m$ the residue class ring modulo m, i.e. $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Thus e.g. $\mathbb{Z}_m^*$ is logically the group of units of that ring.

Lemma 4.2.1. *Suppose that E is a cyclic extension of F and that $a\mathcal{O}_F = P_1$ and P_2 are a pair of smallest primes in F. Assume that P_1 is totally inert and P_2 is the only ramified prime in the extension E/F. Then*

$$\mathcal{A} = (E/F, \sigma, a),$$

where $\langle\sigma\rangle = \mathrm{Gal}(E/F)$, is a division algebra that has a minimal discriminant.

Proof. Lemma 2.3.10 combined with Proposition 2.3.8 gives that A is a division algebra. The minimality of the discriminant follows from Lemma 2.4.34. □

Example 4.2.2. Let $\ell > 2$ be an integer. The maximal orders of the cyclic division algebra $\mathcal{A}_\ell = (\mathbb{Q}(\zeta_\ell)/\mathbb{Q}(i), \sigma, 2+i)$ from Example 3.1.10 achieve the discriminant bound.

Example 4.2.3. The field $\mathbb{Q}(\zeta_{3^{k+1}})$ has a unique subfield Z where $[Z:\mathbb{Q}] = 3^k$. The extension $\mathbb{Q}(\sqrt{-3})Z/\mathbb{Q}(\sqrt{-3})$ has degree 3^k and the prime (2) is totally inert in this extension. The extension also has a very limited ramification, the prime $(\sqrt{-3})$ is the only ramified one.

Primes $(\sqrt{-3})$ and (2) are a pair of minimal primes in the field $\mathbb{Q}(\sqrt{-3})$. Lemma 4.2.1 states now that the cyclic algebra $\mathcal{A} = (\mathbb{Q}(\sqrt{-3})Z/\mathbb{Q}(\sqrt{-3}), \sigma, 2)$ is a division algebra with a minimal discriminant.

In Example 4.2.3 we found a suitable extension $E/\mathbb{Q}(\sqrt{-3})$ that only had one ramified prime $(\sqrt{-3})$. However we can prove that for an arbitrary degree there usually does not exist a cyclic extension that has ramification over $(\sqrt{-3})$ or (2) only. This assures that in general we cannot use such simple methods. Next we will provide a construction method that takes care of most of the prime power degrees. First we need some preliminary results.

Recall the concept of the global Frobenius automorphism. Suppose we have a finite Galois extension E/F and that B is such a prime ideal of $\mathcal{O}_E$ that $B \cap \mathcal{O}_F = P$ is unramified in the extension E/F. There exists a unique element σ of the group $\mathrm{Gal}(E/F)$ that is associated to the prime B and satisfies

$$\sigma(B) = B \tag{4.2}$$
$$\sigma(a) \equiv (a)^{[\mathcal{O}_F:P]} \pmod{B}. \tag{4.3}$$

We call this element the Frobenius automorphism of B and denote it with $(B, E/F)$.

If the extension E/F is abelian, all the primes B_i that lie over P share the same Frobenius automorphism and we can denote $(B,E/F)$ by $(P,E/F)$.

For the properties of the Frobenius automorphism we refer the reader to [28, p. 379].

Example 4.2.4. Let $p_1 \neq p$. Then the Frobenius automorphism $(p_1,\mathbb{Q}(\zeta_p)/\mathbb{Q})$ can be defined by

$$(p_1,\mathbb{Q}(\zeta_p)/\mathbb{Q})(\zeta_p) = \zeta_p^{p_1}.$$

We consider a tower of fields $F_1 \subseteq F_2 \subseteq L$ of finite extensions.

Proposition 4.2.5. *If $F_1 \subseteq F_2 \subseteq E$, E/F_1 and F_2/F_1 are normal and B is such a prime ideal of E that $B \cap F_1 = P$ is unramified in E/F_1, then*

$$(B,E/F_1)|_{F_2} = (B \cap F_2, F_2/F_1).$$

The prime P is totally inert in the extension E/F_1 if and only if $(B,E/F_1)$ generates the group $\mathrm{Gal}(E/F_1)$.

Proof. See [28, Theorem 7.10]. □

The next lemma is a rather direct consequence of the definition of Hasse invariant.

Lemma 4.2.6. *Let*

$$\mathscr{A} = (E/F,\sigma,\gamma)$$

be a division algebra where $\langle\sigma\rangle = \mathrm{Gal}(E/F)$, $\gamma \in K^*$, $[L:K] = n$ and suppose that P is a prime ideal of K that is totally inert in the extension E/F. If k is the smallest possible positive integer so that σ^k is the Frobenius automorphism of P then the Hasse invariant of P

$$h_P = \frac{kv_P(\gamma)}{n}.$$

Proof. [34, p. 281]. □

Let us next consider a tower of fields $F_1 \subseteq F_2 \subseteq E$ of finite extensions. The proofs of the next two well known lemmas will be omitted.

Lemma 4.2.7. *Let B be a prime ideal of E, $P_2 = \mathscr{O}_{F_2} \cap B$ and $P_1 = \mathscr{O}_{F_1} \cap B$.*

1. Let $f(B/P_1)$, $f(B/P_2)$, and $f(P_2/P_1)$ be the respective inertia degrees of B over P_1, B over P_2, and P_2 over P_1. Then

$$f(B/P_1) = f(B/P_2)\,f(P_2/P_1).$$

2. Let $e(B/P_1)$, $e(B/P_2)$, and $e(P_2/P_1)$ be the respective ramification indices of B over P_1, B over P_2, and P_2 over P_1. Then

$$e(B/P_1) = e(B/P_2)e(P_2/P_1).$$

Lemma 4.2.8. *Let E/F be a Galois extension, B a prime ideal of E and $P = F \cap B$. Then*

$$e(B/P) \mid [E:F]$$

and

$$f(B/P) \mid [E:F].$$

Lemma 4.2.9. *Let p be a prime and n such an integer that $n|(p-1)$. The field $\mathbb{Q}(\zeta_p)$ has a unique subfield Z with $[Z:\mathbb{Q}] = n$.*

There exists a group isomorphism ϕ from $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbb{Q})$ that takes any prime $p_1 \neq p$ to the corresponding Frobenius automorphism $(p_1, Z/\mathbb{Q})$ in $\mathrm{Gal}(Z/\mathbb{Q})$.

The prime $p_1 \neq p$ is totally inert in the extension $Z/\mathbb{Q}$ if and only if p_1^t is not an nth power $(\mathrm{mod}\, p)$ for $t = 1, \ldots, n-1$.

Proof. It is well known that there exists a unique isomorphism ψ from $\mathbb{Z}_p^*$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ which takes prime $p_1 \neq p$ to $(p_1, \mathbb{Q}(\zeta_p)/\mathbb{Q})$. We denote the fixed field of the group $\psi(\mathbb{Z}_p^*)^n$ by Z. It is now clear that Z is unique and $[Z:\mathbb{Q}] = n$. If we first map the elements of $\mathbb{Z}_p^*$ with ψ to $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and then restrict the resulting automorphisms to the field Z, we obtain an isomorphism ϕ from $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^n$ to $\mathrm{Gal}(Z/\mathbb{Q})$. Proposition 4.2.5 states that ϕ has the claimed properties.

The last claim follows from the properties of ϕ combined with the last statement of Proposition 4.2.5. □

Proposition 4.2.10. *Suppose that $F = \mathbb{Q}(\sqrt{c})$ is a quadratic field, $q \neq 2$ is a given prime and n a given integer. We suppose that P_1 and P_2 are the smallest primes ideals in F and p_1 and p_2 are the prime numbers that lie under P_1 and P_2.*

Let p be such a prime that $q^n|(p-1)$, $(p,c) = 1$, and that p_1 and p_2 are totally inert in the extension $Z/\mathbb{Q}$, where Z is the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree q^n. We also suppose that p is inert in the extension $F/\mathbb{Q}$.

The extension FZ/F is a cyclic Galois extension of degree q^n where the prime ideals P_1 and P_2 are totally inert and $P = p\mathcal{O}_F$ is the only ramified prime ideal in the extension FZ/F.

Proof. Let B be a prime ideal of FZ, $P_Z = \mathcal{O}_Z \cap B$, $P_F = \mathcal{O}_F \cap B$ and $b = \mathbb{Q} \cap B$. We denote the corresponding ramification indices by $e(B/P_Z)$, $e(P_Z/P_F)$ and $e(P_F/b)$. According to Lemma 4.2.7

$$e(B/b) = e(B/P_Z)e(P_Z/b) = e(B/P_F)e(P_F/b).$$

Lemma 4.2.8 for its part states that $e(B/P_Z), e(P_F/b) \mid 2$ and $e(P_Z/b), e(B/P_F) \mid q^n$. This together with the previous equation shows that the prime $P_F \subset \mathcal{O}_F$ is ramified in the extension FZ/F if and only if the prime b is ramified in the extension $Z/\mathbb{Q}$.

The prime p is the only ramified prime in $Z/\mathbb{Q}$ and because p is inert in the extension $F/\mathbb{Q}$ we see that P is the only ramified ideal in the extension ZF/F.

If we choose B so that $P_F = P_1$ or $P_F = P_2$, then

$$f(B/b) = f(B/P_Z)f(P_Z/b) = f(B/P_F)f(P_F/b) = q^n \cdot g,$$

where $g = 1$ or $g = 2$. This combined with Lemma 4.2.8 implies that $f(B/P_F) = q^n$. □

In the following propositions we use the notation from Proposition 4.2.10. We set that $f_1 = f(P_1|p_1)$ and $f_2 = f(P_2|p_2)$.

Lemma 4.2.11. *There exists a group isomorphism ρ between* $\mathrm{Gal}(FZ/F)$ *and* $\mathrm{Gal}(Z/\mathbb{Q})$ *such that*

$$\rho((P_i, FZ/F)) = (p_i, Z/\mathbb{Q})^{f_i}.$$

Proof. It is a well-known fact that there exists a well defined surjective homomorphism from $\mathrm{Gal}(FZ/\mathbb{Q})$ to $\mathrm{Gal}(Z/\mathbb{Q})$ for which $\sigma \longmapsto \sigma_{|Z}$. The kernel of this map consists of those elements of $\mathrm{Gal}(FZ/\mathbb{Q})$ that act trivially on the field Z. On the other hand, if we restrict the domain of the map to those elements that act trivially on F this map is an injection because the only element of $\mathrm{Gal}(FZ/\mathbb{Q})$ that acts trivially on both fields F and Z is the identity map. As we know that $|\mathrm{Gal}(FZ/F)| = |\mathrm{Gal}(Z/\mathbb{Q})|$ the described map must be an isomorphism. Now the statement about Frobenius maps follows from the basic properties of the Frobenius automorphism. □

Proposition 4.2.12. *Let*

$$p_1^{f_1} p_2^{f_2} = 1 \tag{4.4}$$

in the group $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^{q^n}$, $P_1 = a_1\mathscr{O}_F$, and $P_2 = a_2\mathscr{O}_F$. Then

$$\mathscr{A} = (FZ/F, \sigma, a_1a_2)$$

with $\langle\sigma\rangle = \mathrm{Gal}(FZ/F)$ is a division algebra that has a minimal discriminant.

Proof. The prime P_1 is totally inert in the extension FZ/F. Thus, Lemma 2.3.10 states that $\mathscr{A}$ is a division algebra.

From the cyclic representation of the algebra $\mathscr{A}$ we instantly see that $\mathscr{A}$ has only three Hasse invariants that can be nontrivial: h_{P_1}, h_{P_2}, and h_P. In what follows we show that the invariant h_P must be trivial.

We first choose σ to be the Frobenius automorphism of P_1. Lemma 4.2.6 now shows that the Hasse invariant of P_1 is

$$\frac{1}{q^n} = h_{P_1}.$$

Because the group $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^{q^n}$ is cyclic we get from (4.4) that $p_2^{f_2} = (p_1^{f_1})^{(q^n-1)}$ in $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^{q^n}$. This implies that $(p_2, Z/\mathbb{Q})^{f_2} = ((p_1, Z/\mathbb{Q})^{f_1})^{(q^n-1)}$. According to Lemma 4.2.11 then $(P_2, FZ/F) = ((P_1, FZ/F)^{q^n-1}$. Lemma 4.2.6 now states that

$$\frac{q^n-1}{q^n} = h_{P_2}.$$

The sum of the Hasse invariants of $\mathscr{A}$ must be zero (mod 1), whence

$$h_{P_1} + h_{P_2} + h_P \in \mathbb{Z}.$$

But, we already saw that $h_{P_1} + h_{P_2} \in \mathbb{Z}$, which implies that $h_P \in \mathbb{Z}$. The discriminant of the algebra $\mathscr{A}$ has now only two divisors P_1 and P_2.

In the beginning of our proof we make the assumption that σ is the Frobenius of the prime P_1. However, the choice of the generator of the group $\mathrm{Gal}(FZ/F)$ in a cyclic generation does not change the discriminant of the corresponding algebra. □

Example 4.2.13. Suppose that the center $F = \mathbb{Q}(i)$. The primes $(1+i)$ and $(2+i)$ are a pair of smallest prime ideals in this field. We want to produce a division algebra of index 10 that has a minimal discriminant. It is not difficult to check that 2^t and 5^t are not 5th powers (mod 11) for $t = 1, \ldots, 4$, and that 11 is inert in the extension $F/\mathbb{Q}$. Lemma 4.2.10 states that $\mathbb{Q}(\zeta_{11})$ has a subfield Z, $[Z : \mathbb{Q}] = 5$, and that 2 and 5 are totally inert in the extension $Z/\mathbb{Q}$.

Proposition 4.2.10 states that the primes $(1+i)$ and $(2+i)$ are totally inert in the extension FZ/F and the prime ideal $11\mathscr{O}_F$ is the only ramified ideal in the extension FZ/F.

We easily see that $2 \cdot 5 = 1$ in $\mathbb{Z}_{11}^*/(\mathbb{Z}_{11}^*)^5$. Therefore,

$$(FZ/F, \sigma_1, (1+i)(2+i))$$

is a division algebra with a minimal discriminant.

We previously saw that $\mathscr{A} = (\mathbb{Q}(\zeta_{2^4})/F, \sigma_2, 2+i)$ is a division algebra of index 2 and has a minimal discriminant. Finally, from Proposition 3.2.3

$$(\mathbb{Q}(\zeta_{2^4})Z/F, \sigma_1\sigma_2, (1+i)^2(2+i)^7)$$

is seen to be a division algebra of degree 10 with a minimal discriminant.

4.2.1 The existence of suitable primes

Propositions 4.2.10 and 4.2.12 have turned our construction project into a hunt of suitable prime numbers. The problem is that we do not know if there are "enough" suitable prime numbers. The answer is that in most cases there are. This will be proved in Theorem 4.2.17, but first we need some preliminary results.

For the definition and the basic properties of Kummer extensions we refer the reader to [22, p. 197].

Proposition 4.2.14. *Let E/F be a Kummer extension with $E = F(\alpha)$, $\alpha^n = a \in \mathcal{O}_F$, and let P be a prime ideal of F that is not a divisor of $a \cdot n$. Furthermore, let t be the largest divisor of n such that the congruence*

$$x^t \equiv a \pmod{P}$$

has a solution in $\mathcal{O}_F$. Then P decomposes in E into a product of t prime ideals of degree n/t over P.

Lemma 4.2.15. *Suppose that q and p are prime numbers and that $q^t|(p-1)$ for some integer t. If c is an integer and the equation*

$$c \equiv x^q \pmod{p} \tag{4.5}$$

is not solvable, then neither is any of the equations

$$c^k \equiv x^{q^t} \pmod{p}, \tag{4.6}$$

where $k = 1, \ldots, q^t - 1$.

Proof. Let a be a generator of the cyclic group $\mathbb{Z}_p^*$. Then we can write that $c \equiv a^n \pmod{p}$ for some integer n.

Let us assume that (4.5) has no solution. This implies that q is not a factor of n. Assume then that for some k there is a solution d for (4.6). If we write $d \equiv a^s$, then (4.6) gives that $kn - sq^t = v(p-1)$, where v is some integer. As $q^t|(p-1)$ this would mean that $q^t|kn$. That gives us a contradiction. □

In the following we use the phrase "the prime P has inertia in the extension E/F". By that we mean that at least one prime ideal B of E that lies over the P has inertial degree $f(P|B) > 1$.

Lemma 4.2.16. *Suppose that F_1 and F_2 are Galois extensions of a field F and $F_1 \cap F_2 = F$. The prime P of $\mathcal{O}_F$ has inertia in the extension F_1F_2 if and only if it has inertia in the extension F_1 or F_2. The prime P is ramified in the extension F_1F_2 if and only if it is ramified in F_1 or in F_2.*

Proof. For the proof the reader is referred to [36, p. 263]. □

The proof of the following theorem is a slightly modified version of the proof of [33, Theorem 1]. We do not suppose here that the center is totally complex nor that the ring $\mathcal{O}_F$ is a PID. However, we suppose that $p_1 \neq p_2$. For the simplicity we also suppose that $f_2 \neq 2$.

Theorem 4.2.17. *Assume that $F = \mathbb{Q}(\sqrt{c})$ is a quadratic field, P_1 and P_2 are the smallest primes in F, $q \nmid 2p_1$ is a given prime, and n a given integer.*

If $q \nmid c$, then there exists infinitely many prime numbers p so that p is inert in F, $\mathbb{Q}(\zeta_p)$ has a unique subfield Z, $[Z : \mathbb{Q}] = q^n$, where p_1 and p_2 are totally inert, and $p_1^{f_1} p_2^{f_2} = 1$ in $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^{q^n}$.

Proof. Let us denote $q^n = s$, $K = \mathbb{Q}(\zeta_s)((p_1^{f_1} p_2^{f_2})^{1/s})$, $K_1 = K((p_1)^{1/q})$ and suppose that $q \neq p_1$. By considering the prime ideal factorization of $p_1 p_2$ in $\mathbb{Q}(\zeta_s)$ we may conclude that $(p_1^{f_1} p_2^{f_2})^d$ cannot be an sth power for any $d = 1, \ldots, s-1$. Therefore $[K : \mathbb{Q}(\zeta_s)] = s$.

As we have supposed that $q \nmid c$ there has to be at least one prime p_3 that has a ramification index 2 in the extension $F/\mathbb{Q}$, but which is not ramified in the extension $\mathbb{Q}(\zeta_s)/\mathbb{Q}$. Earlier, we saw that $[K : \mathbb{Q}(\zeta_s)] = s$. Because p_3 is not ramified in $\mathbb{Q}(\zeta_s)/\mathbb{Q}$ and 2 does not divide $[K : \mathbb{Q}(\zeta_s)]$, none of the prime ideals P_3 in $\mathcal{O}_K$ that lie over p_3 has 2 as a divisor of the ramification index $e(P_3|p_3)$. This implies that $F \not\subseteq K$.

By [33, Lemma 2] we know that $[K_1 : K] = q$. Because $q \neq 2$ and $F \not\subseteq K$, the extension $K_1 F/K$ is cyclic and $[K_1 F : K] = 2q$.

Chebotarev's density theorem [28, Lemma 7.14] states that K has infinitely many prime ideals that have absolute degree one and are totally inert in the extension $K_1 F/K$. We choose one, P, that not only has an absolute degree one but that is also unramified in the extension $K/\mathbb{Q}$.

We denote the prime of $\mathbb{Q}$ that lies under P by p. The field $\mathbb{Q}(\zeta_{q^n})$ is a subfield of K and therefore p splits completely in the extension $\mathbb{Q}(\zeta_{q^n})/\mathbb{Q}$. The theory of cyclotomic fields [22, p. 195] now gives that

$$p \equiv 1 \pmod{q^n}.$$

Next we are going to show that p_1^t is not an sth power (mod p) for $t = 1, \ldots, s-1$. Lemma 4.2.15 suggests that we should consider the equation $p_1 \equiv x^q \pmod{p}$. Suppose that $p_1 \equiv a^q \pmod{p}$ for some integer a. Now $p_1 \equiv a^q \pmod{P}$. This last equation however cannot be true because P is totally inert in the Kummer extension K_1/K. Lemma 4.2.15 now states that equation $p_1^t \equiv x^{q^n} \pmod{p}$ does not have a solution for any $t = 1, \ldots, q^n - 1$.

Lemma 4.2.9 states that $\mathbb{Q}(\zeta_p)$ has a unique subfield Z with $[Z : \mathbb{Q}] = q^n$, and that p_1 is totally inert in the extension $Z/\mathbb{Q}$.

The prime P has absolute degree one in K and therefore $(p_1^{f_1} p_2^{f_2})^{1/q^n} \equiv c \pmod{P}$, where c is some integer. This implies that

$$p_1^{f_1} p_2^{f_2} \equiv c^{q^n} \pmod{p}.$$

If we use the notation of Lemma 4.2.9, the map ϕ takes p_1 to the generator g of the group $\mathrm{Gal}(Z/\mathbb{Q})$ and $p_1^{f_1} \cdot p_2^{f_2}$ to identity. Because $2 \nmid |\mathrm{Gal}(Z/\mathbb{Q})|$ we have that $\phi(p_1)^{f_1}$ is also a generator of $\mathrm{Gal}(Z/\mathbb{Q})$. The map ϕ is a homomorphism and therefore $\phi(p_2)^{f_2}$ and $\phi(p_2)$ are again generators of the group $\mathrm{Gal}(Z/\mathbb{Q})$. Lemma 4.2.9 now shows that p_2 is totally inert in the extension $Z/\mathbb{Q}$.

To complete the proof we have to show that the prime p is inert in the extension $F/\mathbb{Q}$. The prime P must be inert in the extension FK/K and therefore the prime p has at least some inertia in the extension $FK/\mathbb{Q}$. Because p is totally split in the

extension $K/\mathbb{Q}$ it does not have any inertia in this extension and therefore Lemma 4.2.16 states that p must be inert in the extension $F/\mathbb{Q}$. □

Theorem 4.2.17 states that for the center $\mathbb{Q}(i)$ the only problematic prime power indices are of the form 2^k. Luckily, the construction of example 4.2.2 covers these cases. As a consequence, we can construct a division algebra with a minimal discriminant for an arbitrary index. In Table 4.3 we give explicit representations for division algebras with a prime power index less than 20 and a minimal discriminant.

For each index q^n we have searched the prime p of the Theorem 4.2.17 along the lines of example 4.2.13. After the prime p is found the actual minimal polynomial of the extension FZ/F can be easily found by considering the subfields of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Both tasks were done by the help of computer algebra system PARI [32].

If the center is $\mathbb{Q}(\sqrt{-3})$, the problematic prime powers are 2^n and 3^n. Algebras of degree 3^n we get from Example 4.2.3, but degrees 2^n are more difficult. For index 2 we can use the division algebra of Section 4.1. As a conclusion we can construct a division algebra with a minimal discriminant if the index is not divisible by 4.

In Table 4.4 we give explicit representations for our algebras.

Example 4.2.18. From Table 4.3 we get that

$$\mathscr{A}_3 = (\mathbb{Q}(i)(a_3)/\mathbb{Q}(i), \sigma_3, (1+i)(2+i))$$

and

$$\mathscr{A}_2 = (\mathbb{Q}(i)(a_2)/\mathbb{Q}(i), \sigma_2, (2+i))$$

are division algebras with minimal discriminants. According to Proposition 3.2.3 algebra $\mathscr{A}_2 \otimes \mathscr{A}_3 = (\mathbb{Q}(i)(a_6)/\mathbb{Q}(i), \sigma_2\sigma_3, (2+i)^5(1+i)^2)$, where a_6 is a zero of the polynomial $x^6 - 2x^5 + (-3i-51)x^4 + (4i-30)x^3 + (-2i+755)x^2 + (-298i+2134)x + -593i + 1628$, is a division algebra of degree 6 and has a minimal discriminant.

One of the unfortunate properties of our construction is that when we produce division algebras of a composite index the resulting algebras tend to have relatively large non-norm elements γ. In the following example we solve this problem in one specific case and show that we can always use $\gamma = (2+i)(1+i)$. The method has a straightforward generalization to more general situations.

Example 4.2.19. In what follows we produce the algebra $\mathscr{A}_6$ as a tensor product of two smaller algebras.

Let a_2 be a zero of the polynomial x^2+i. The algebra $\mathscr{B}_2 = (F(a_2)/F, \sigma_2, (1+i)(2+i))$ is a slightly modified version of the algebra $\mathscr{A}_2$ of Table 4.3. It is a division algebra with a minimal discriminant.

The algebra $\mathscr{B}_3 = (F(a_3)/F, \sigma_3, (2+i)^{-1}(1+i)^{-1})$ is a modified version of the algebra $\mathscr{A}_3$. Proposition 2.3.10 gives us that $\mathscr{B}_3$ is still a division algebra. By considering the equation $\mathscr{B}_3 \otimes \mathscr{A}_3 \sim M_n(F)$ we see that $\mathscr{B}_3$ has the same discriminant as the algebra $\mathscr{A}_3$.

Because $\mathscr{B}_2$ and $\mathscr{B}_3$ are division algebras with minimal discriminants it follows from Proposition 3.2.3 that the tensor product

$$\mathscr{A}_6 = \mathscr{B}_3 \otimes \mathscr{B}_2 = (F(a_2, a_3)/F, \sigma_2\sigma_3, (2+i)(1+i))$$

is a division algebra with a minimal discriminant. The polynomial f_6 is just simply the minimal polynomial of the generator a_6 of the field $F(a_2, a_3)$.

Remark 4.2.20. The results in Chapter 4 are from [18] and [43], although the general construction method of Proposition 4.2.12 is just slightly modified version of that presented in [33].

4.3 Simulation setting

We have given two figures 2.1 and 3.4 where we illustrated the performance of different codes from orders of division algebras. We briefly describe how these figures were produced.

The maximal order of the algebra $\mathscr{G}_2$, that is used in the simulations 2.1 and 3.4, is determined with the computer algebra system MAGMA ([24]). The code from the natural order of the algebra $\mathscr{G}_2$ that is used in Figure 2.1 is gotten through the natural representation (Example 2.3.43). The actual Golden code we used in 3.4 is from [30].

The *data rate R* in symbols per channel use is given by

$$R = \frac{1}{2}\log_2(|\mathscr{C}|),$$

where $|C|$ is the size of the code C. Our code constructions are based on selecting the prescribed number of lowest energy matrices from the infinite code. In order to reach a target bandwidth utilization of 4, 6 or 8 bpcu we thus selected 256, 4096 or 65536 matrices respectively.

The error rates in Figures 2.1 and 3.4 are block error rates (BLER).

Table 4.3: The conductor p of the cyclotomic field $\mathbb{Q}(\zeta_p)$, the non-norm element γ, and the minimal polynomial f_n of the extension $\mathbb{Q}(i)(a_n)/\mathbb{Q}(i)$

n	p	γ	f_n
2		$2+i$	x^2+i
3	79	$(1+i)(2+i)$	$x^3+x^2-26x+41$
4		$2+i$	x^4+i
5	11	$(1+i)(2+i)$	$x^5+x^4-4x^3-3x^2+3x+1$
7	211	$(1+i)(2+i)$	$x^7+x^6-90x^5+69x^4+1306x^3+124x^2-5249x-4663$
8		$(1+i)(2+i)$	x^8+i
9	271	$(1+i)(2+i)$	$x^9+x^8-120x^7-543x^6+858x^5+6780x^4+7217x^3-2818x^2-4068x-261$
11	859	$(1+i)(2+i)$	$x^{11}+x^{10}-390x^9-653x^8+52046x^7+146438x^6-2723930x^5-11558015x^4+36326009x^3+250960565x^2+385923388x+145865807$
13	6163	$(1+i)(2+i)$	$x^{13}+x^{12}-2844x^{11}-6017x^{10}+2908490x^9+10238862x^8-1340405033x^7-6785664624x^6+281925130086x^5+1909036915713x^4-21097272693753x^3-192054635052100x^2-235667966495418x+213548387827457$
16		$2+i$	$x^{16}+i$
17	239	$(1+i)(2+i)$	$x^{17}+x^{16}-112x^{15}-47x^{14}+3976x^{13}+4314x^{12}-64388x^{11}-136247x^{10}+422013x^9+1631073x^8+411840x^7-5840196x^6-11894369x^5-10635750x^4-4739804x^3-938485x^2-54850x-619$
19	8779	$(1+i)(2+i)$	$x^{19}+x^{18}-4158x^{17}+8463x^{16}+6281539x^{15}-34466097x^{14}-4291513699x^{13}+39454551948x^{12}+1357034568541x^{11}-17014625218525x^{10}-184614267432185x^9+3035523756071878x^8+10088401800577582x^7-253111326110358151x^6-143208448461319868x^5+1061243979137656047 1x^4-3774559232798357892x^3-220041647923912963182x^2+8608393212050159813 9x+179422120229746149964 1$

Table 4.4: The conductor p of the cyclotomic field $\mathbb{Q}(\zeta_p)$, the non-norm element γ, and the minimal polynomial f_n of the extension $\mathbb{Q}(\sqrt{-3})(a_n)/\mathbb{Q}(\sqrt{-3})$

n	p	γ	f_n
2			
3		2	x^3-3x+1
4			
5	131	$\sqrt{-3}\cdot 2$	$x^5+x^4-52x^3-89x^2+109x+193$
7	449	$\sqrt{-3}\cdot 2$	$x^7+x^6-192x^5+275x^4+3952x^3+4136x^2-81x-863$
8			
9		2	$x^9-9x^7+27x^5-30x^3+9x+1$
11	23	$\sqrt{-3}\cdot 2$	$x^{11}+x^{10}-10x^9-9x^8+36x^7+28x^6-56x^5-35x^4+35x^3+15x^2-6x-1$
13	1613	$\sqrt{-3}\cdot 2$	$x^{13}+x^{12}-744x^{11}-2071x^{10}+172627x^9+432959x^8-17309406x^7-33601543x^6+751073656x^5+1289004819x^4-10171466974x^3-28375196178x^2-23821205823x-6355270027$
16			
17	239	$\sqrt{-3}\cdot 2$	$x^{17}+x^{16}-112x^{15}-47x^{14}+3976x^{13}+4314x^{12}-64388x^{11}-136247x^{10}+422013x^9+1631073x^8+411840x^7-5840196x^6-11894369x^5-10635750x^4-4739804x^3-938485x^2-54850x-619$
19	14897	$\sqrt{-3}\cdot 2$	$x^{19}+x^{18}-7056x^{17}-40523x^{16}+17080680x^{15}+72065222x^{14}-20162799933x^{13}-16167485303x^{12}+12640227359901x^{11}-36746089501267x^{10}-4111622563682675x^9+26076550916951212x^8+59051701290483139 4x^7-5563085347769988171x^6-1858701946459493040 4x^5+24907729711797663886 8x^4+89570134984571927459x^3-24264433001385631990 68x^2-25140759214549268090 76x+12376644127186204447 87$

Suggestions for further work

The most interesting, and probably quite difficult, open question is whether the determinant bounds we made for codes from orders of division algebras can be broken with other code constructing methods. While nothing suggest that our matrix lattices should be optimal, some computer simulations and results (see [23]) suggests that we might be close to optimal at least in the case of 2×2 matrices. The first obvious direction is to consider sublattices, that are not orders, of division algebras.

Another question which has only slight coding theoretic interest, but might be interesting from the algebraic point of view, is to consider how small discriminants we can achieve from natural orders (ore more generally from crossed product orders). This problem is so tightly linked to the classical question of size of discriminants in algebraic number fields, that any progress might be valuable.

It would also be interesting to study the lattice theoretic properties of the real lattices we get by vectorizing the matrix lattices derived from maximal orders (see Remark 2.4.36). After all these lattices have a relatively large center density. Considering the typical questions of lattice theory has it own interest, but could also lead into better code design criterions for codes from orders.

One of the problems in the use of our codes from maximal orders is that after we have found the correct division algebra we do not have an easy method to explicitly construct the actual order. There exists an algorithm [20], that is implemented in the computer algebra system MAGMA [24]. However, at least in a way that it is implemented in MAGMA it uses considerable amounts of memory. Even for relatively small values of n running the program on a typical PC was impossible.

Therefore it would be nice to have an explicit construction method for maximal orders from division algebras we constructed in Section 4.2. Preliminary research, we have done, suggests that we can use the methods of [33] with minor modifications.

The same question can be also considered in the case where the matrices have real coefficients (see Section 2.5).

Bibliography

[1] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communication", *IEEE J. on Select. Areas in Commun.*, vol. 16, pp. 1451–1458, October 1998.

[2] A. A. Albert, *Structure of Algebras*, American Mathematical Society, New York City 1939.

[3] E. Bayer-Fluckiger, "Lattices and number Fields", *Contemporary Mathematics*, vol. 241, pp. 69–84, 1999.

[4] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "Algebraic Lattice Constellations: Bounds on Performance", *IEEE Trans. Inf. Theory*, vol. 52, pp. 319–327, January 2006.

[5] C. Abou-Rjeily, N. Daniele, and J.C. Belfiore, "Space-Time Coding for Multiuser Ultra-Wideband Communications", *IEEE Trans. Commun.*, vol.54, no.11, pp. 1960–1972, Nowember 2006.

[6] J.-C. Belfiore and G. Rekaya, "Quaternionic Lattices for Space-Time Coding", *Proc. ITW 2003*, Paris, France, March 31 - April 4, 2003.

[7] J.-C. Belfiore, G. Rekaya, and E. Viterbo: "The Golden Code: A 2x2 Full-Rate Space-Time Code With Non-vanishing Determinant", *IEEE Trans. Inf Theory*, vol. 51, pp. 1432–1436, April 2005.

[8] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, "A Table of Totally Complex Number Fields of Small Discriminants", Algorithmic number theory (Portland, OR, 1998), *Lecture Notes in Comput. Sci.*, 1423, pp.381–391, Springer, Berlin, 1998.

[9] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988.

[10] P. Dayal, and M. Varanasi, "An Algebraic Family of Complex Lattices for Fading Channels With Application to Space-Time Codes", *IEEE Trans. Inf. Theory* , vol. 51, pp. 4184–4202, December 2005.

[11] P. Elia, B. A. Sethuraman and P. Vijay Kumar, "Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas", preprint, available from ArXiv.org.

[12] P. Elia, K. R. Kumar, P. V. Kumar, H.-F. Lu, and S. A. Pawar, "Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3869–3884, September 2006.

[13] X. Giraud, E. Boutillon, and J. C. Belfiore, "Algebraic tools to build modulation schemes for fading channels", *IEEE Trans. Inf. Theory*, vol.43, pp. 938–952, May 1997.

[14] Helmut Hasse, *Number Theory*, Springer, Berlin, 1980.

[15] C. Hollanti and J. Lahtonen, "Maximal Orders in the Design of Dense Space-Time Lattice Codes", submitted to *IEEE Trans. Inf. Theory*, September 2006.

[16] C. Hollanti and J. Lahtonen, "A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras", *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, March 13-17, 2006.

[17] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal Matrix Lattices for MIMO Codes from Division Algebras", *Proc. IEEE ISIT 2006*, pp. 783–787, Seattle, July 9 - 14, 2006.

[18] C. Hollanti, J. Lahtonen, K. Ranto and R. Vehkalahti, "On the Densest MIMO Lattices from Cyclic Division Algebras" (submitted in December 2006, preprint available from ArXiv).

[19] R. Hull, "Maximal Orders in Rational Cyclic Algebras of Odd Prime Degree", *Transactions of the American Mathematical Society*, vol. 38, no. 3, pp. 515–530, 1935.

[20] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in algebras over $\mathbb{Q}$", Computational Complexity 3, pp. 245–261, 1993.

[21] Kiran. T. and B. S. Rajan, "STBC-Schemes with Non-Vanishing Determinant For Certain Number of Transmit Antennas", *IEEE Trans. Inf. Theory*, vol. 51, pp. 2984–2992, August 2005.

[22] H. Koch, *Number Theory, Algebraic Numbers and Functions*, American Mathematical Society, New York, 2000.

[23] J.Lahtonen and R. Vehkalahti, "Dense MIMO matrix lattices - a meeting point for class field theory and invariant theory", *Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)*, Indian Institute of Science, Bangalore, December 16-20, 2007.

[24] Web page:
http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.

[25] J.S. Milne, *Class Field Theory*, Lecture notes for a course given at the University of Michigan, Ann Arbor, http://www.jmilne.org/math/coursenotes/.

[26] J.S. Milne, *Algebraic Number Theory*, Lecture notes for a course given at the University of Michigan, Ann Arbor, http://www.jmilne.org/math/coursenotes/.

[27] Patrick J. Morandi, B.A. Sethuraman, "Divisors on division algebras and error correcting codes", *Communications in Algebra*, vol. 26, issue 19, pp.3211–3221, 1998.

[28] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, Berlin, 1980.

[29] A. M. Odlyzko, "Lower bounds for discriminants of number fields II", *Tohoku Math. J.*, no. 29, pp. 209–216, 1977.

[30] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[31] F. Oggier, E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels", Foundations and Trends in Communications and Information Theory, December 2004.

[32] PARI/GP, version `2.2.12`, Bordeaux, 2005, http://pari.math.u-bordeaux.fr.

[33] S. Perlis, "Maximal Orders in Rational Cyclic algebras of composite degree", *Transactions of the American Mathematical Society*,vol.46, n.1, pp. 82–96, July 1939.

[34] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.

[35] G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Algebraic 3x3, 4x4 and 6x6 Space-Time Codes with Non-Vanishing Determinants", *Proc. IEEE ISITA 2004*, Parma, Italy, October 10 - 13, 2004.

[36] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, New York, 2001.

[37] Web page of Roblot Xavier-François:
http://math.univ-lyon1.fr/$\sim$ roblot/tables.html

[38] L. Rónyai, "Algorithmic Properties of Maximal Orders in Simple Algebras Over $\mathbb{Q}$", *Computational Complexity 2*, pp. 225–243, 1992.

[39] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2596–2616, October 2003.

[40] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "Information-Lossless STBCs from Crossed-Product Algebras", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3913–3935, September 2006.

[41] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.

[42] V. Tarokh, N. Seshadri, and A.R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction", *IEEE Transactions on Information Theory*, vol. 44, pp. 744–765, March 1998.

[43] R. Vehkalahti, "Constructing optimal division algebras for space-time coding", *Proc. IEEE ITW 2007*, pp. 105–110, Bergen, Norway, July 1 - 6, 2007.

[44] G. Wang and X.-G. Xia, "On Optimal Multi-Layer Cyclotomic Space-Time Code Designs", *IEEE Trans. Inf. Theory*, vol. 51, pp. 1102–1135, March 2005.

[45] Genyuan Wang, Huiyong Liao, Haiquan Wang, and Xiang-Gen Xia, "Systematic and Optimal Cyclotomic Lattices and Diagonal Space-Time Block Code Designs", *IEEE Trans. Inf. Theory*, vol. 50,pp. 3348–3360, December 2004.

[46] Chaoping Xing, "Diagonal Lattice Space-Time Codes From Number Fields and Asymptotic Bounds", *IEEE Trans. Inf. Theory*, vol.53, pp. 3921–3926, Nowember 2007.

[47] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

Turku Centre for Computer Science
TUCS Dissertations

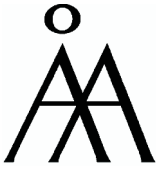
67. **Adrian Costea**, Computational Intelligence Methods for Quantitative Data Mining
68. **Cristina Seceleanu**, A Methodology for Constructing Correct Reactive Systems
69. **Luigia Petre**, Modeling with Action Systems
70. **Lu Yan**, Systematic Design of Ubiquitous Systems
71. **Mehran Gomari**, On the Generalization Ability of Bayesian Neural Networks
72. **Ville Harkke**, Knowledge Freedom for Medical Professionals – An Evaluation Study of a Mobile Information System for Physicians in Finland
73. **Marius Cosmin Codrea**, Pattern Analysis of Chlorophyll Fluorescence Signals
74. **Aiying Rong**, Cogeneration Planning Under the Deregulated Power Market and Emissions Trading Scheme
75. **Chihab BenMoussa**, Supporting the Sales Force through Mobile Information and Communication Technologies: Focusing on the Pharmaceutical Sales Force
76. **Jussi Salmi**, Improving Data Analysis in Proteomics
77. **Orieta Celiku**, Mechanized Reasoning for Dually-Nondeterministic and Probabilistic Programs
78. **Kaj-Mikael Björk**, Supply Chain Efficiency with Some Forest Industry Improvements
79. **Viorel Preoteasa**, Program Variables – The Core of Mechanical Reasoning about Imperative Programs
80. **Jonne Poikonen**, Absolute Value Extraction and Order Statistic Filtering for a Mixed-Mode Array Image Processor
81. **Luka Milovanov**, Agile Software Development in an Academic Environment
82. **Francisco Augusto Alcaraz Garcia**, Real Options, Default Risk and Soft Applications
83. **Kai K. Kimppa**, Problems with the Justification of Intellectual Property Rights in Relation to Software and Other Digitally Distributable Media
84. **Dragoş Truşcan**, Model Driven Development of Programmable Architectures
85. **Eugen Czeizler**, The Inverse Neighborhood Problem and Applications of Welch Sets in Automata Theory
86. **Sanna Ranto**, Identifying and Locating-Dominating Codes in Binary Hamming Spaces
87. **Tuomas Hakkarainen**, On the Computation of the Class Numbers of Real Abelian Fields
88. **Elena Czeizler**, Intricacies of Word Equations
89. **Marcus Alanen**, A Metamodeling Framework for Software Engineering
90. **Filip Ginter**, Towards Information Extraction in the Biomedical Domain: Methods and Resources
91. **Jarkko Paavola**, Signature Ensembles and Receiver Structures for Oversaturated Synchronous DS-CDMA Systems
92. **Arho Virkki**, The Human Respiratory System: Modelling, Analysis and Control
93. **Olli Luoma**, Efficient Methods for Storing and Querying XML Data with Relational Databases
94. **Dubravka Ilić**, Formal Reasoning about Dependability in Model-Driven Development
95. **Kim Solin**, Abstract Algebra of Program Refinement
96. **Tomi Westerlund**, Time Aware Modelling and Analysis of Systems-on-Chip
97. **Kalle Saari**, On the Frequency and Periodicity of Infinite Words
98. **Tomi Kärki**, Similarity Relations on Words: Relational Codes and Periods
99. **Markus M. Mäkelä**, Essays on Software Product Development: A Strategic Management Viewpoint
99. **Roope Vehkalahti**, Class Field Theoretic Methods in the Design of Lattice Signal Constellations

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku

- Department of Information Technology
- Department of Mathematics



Åbo Akademi University

- Department of Information Technologies

Turku School of Economics

- Institute of Information Systems Sciences

ISBN 978-952-12-2065-4
ISSN 1239-1883

Roope Vehkalahti

Class Field Theoretic Methods in the Design of Lattice Signal Constellations

Roope Vehkalahti

Class Field Theoretic Methods in the Design of Lattice Signal Constellations