Constructions A of lattices from number fields and division algebras

Vehkalahti, Roope; Kositwattanarerk, Wittawat; Oggier, Frédérique

2014

Vehkalahti, R., Kositwattanarerk, W., & Oggier, F. Constructions a of lattices from number fields and division algebras. 2014 IEEE International Symposium on Information Theory (ISIT), 2326-2330.

https://hdl.handle.net/10356/79610

https://doi.org/10.1109/ISIT.2014.6875249

Constructions A of Lattices from Number Fields and Division Algebras

Roope Vehkalahti
Department of Mathematics and Statistics
University of Turku
Finland
Email: roiive@utu.fi

Wittawat Kositwattanarerk
Department of Mathematics
Mahidol University
Bangkok, Thailand
Email: wittawat.kos@mahidol.edu

Frédérique Oggier
Division of Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

***Abstract*—There is a rich theory of relations between lattices and linear codes over finite fields. However, this theory has been developed mostly with lattice codes for the Gaussian channel in mind. In particular, different versions of what is called Construction A have connected the Hamming distance of the linear code to the Euclidean structure of the lattice.**

This paper concentrates on developing a similar theory, but for fading channel coding instead. First, two versions of Construction A from number fields are given. These are then extended to division algebra lattices. Instead of the Euclidean distance, the Hamming distance of the finite codes is connected to the product distance of the resulting lattices, that is the minimum product distance and the minimum determinant respectively.

I. Introduction

Constructions of lattices from linear codes have been classically studied [1]. There are several ways to obtain lattices from linear codes, which are usually referred to as Construction A,B,C,.... For example, Construction D and its variations involve sequences of nested binary linear codes of length N that are embedded in $\mathbb{Z}^N$ in the natural way (see e.g. [2] for some recent results), while the term Construction A has been used for a family of constructions obtained by quotient: the classical Construction A takes a vector in $\mathbb{Z}^N$ and uses a map $\rho_2 : \mathbb{Z}^N \to \mathbb{F}_2^N = \{0,1\}^N$ that reduces componentwise $\pmod 2$. Then $\rho_2^{-1}(C)$ is a lattice of rank N, for $C \subset \mathbb{F}_2^N$ a linear code. This construction may be seen as a particular case of the following more general construction [3]. Let $\mathbb{Q}(\zeta_p)$ be a cyclotomic field and $\mathbb{Z}[\zeta_p]$ be its ring of integers, with p a prime, and ζ_p a primitive pth root of unity. Let $\mathbb{F}_p$ denotes the finite field with p elements. Consider $\rho_{(1-\zeta_p)} : \mathbb{Z}[\zeta_p]^N \to \mathbb{F}_p^N$ the reduction modulo the ideal $\mathfrak{p} = (1-\zeta_p)$ componentwise. Then $\rho_{(1-\zeta_p)}^{-1}(C)$ is a lattice for $C \subset \mathbb{F}_p^N$ a linear code. The first construction is obtained by choosing $p = 2$. In fact, one may replace $\mathbb{Q}(\zeta_p)$ by another number field K of degree n (that is a field extension of $\mathbb{Q}$ of degree n), which is either totally real or CM, and the prime $(1-\zeta_p)$ by a prime $\mathfrak{p}$ totally ramified [4]. Let $\rho_{\mathfrak{p}} : \mathcal{O}_K^N \to \mathbb{F}_p^N$ be the reduction $\pmod{\mathfrak{p}}$ componentwise, where $\mathcal{O}_K$ is the ring of integers of K. Then $\rho^{-1}(C)$ is a lattice of rank nN for $C \subset \mathbb{F}_p^N$ a linear code. This construction is motivated by its applications to wiretap encoding. Another incentive to revisit these classical constructions is found in the context of physical layer network coding. In [5], the lattice obtained from the ideal $\mathfrak{p}\mathcal{O}_K/p\mathcal{O}_K$ has been studied for $\mathfrak{p}$ a prime above p with a large ramification index. In the cases explored, the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is a polynomial ring, and the ideal $\mathfrak{p}\mathcal{O}_K/p\mathcal{O}_K$ corresponds to one of its ideals, which in turn defines a code over the given polynomial ring.

In this paper, we are interested in two lattice constructions from number fields, and an extension to division algebras. While classically the Euclidean properties of the lattices are of interest, here we consider instead the minimum product distance (or the minimum determinant) of the constructed lattices, having in mind coding applications to fading channels. Indeed, after the diversity (that we will guarantee), the minimum product distance [6] and determinant are respectively the main code design parameter for fading (MIMO) channels.

We will use several results and notions from algebraic number theory. We refer the reader to [7] for a basic introduction to this theory, including some standard facts and definitions that we will use without explicit reference.

a) Construction 1: Consider a degree n totally real cyclic extension $K/\mathbb{Q}$, with cyclic Galois group $\langle\sigma\rangle$, and suppose that some $p \in \mathbb{Z}$ is completely split in this extension, namely: $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n$, where $\mathfrak{p}_i$ are separate prime ideals.

The Minkowski embedding maps $x \in K$ to

$$\psi(x) = (x, \sigma(x), \sigma^2(x), \dots, \sigma^{n-1}(x)).$$

Then $\psi(\mathcal{O}_K) = L$ is a lattice in $\mathbb{R}^n$. Define a reduction map

$$red_1 : \psi(\mathcal{O}_K) \longmapsto \mathbb{F}_p^n,$$

where $(x, \sigma(x), \dots \sigma^{n-1}(x))$ gets mapped to

$$(x \pmod{\mathfrak{p}_1}, \sigma(x) \pmod{\mathfrak{p}_1}, \dots, \sigma^{n-1}(x) \pmod{\mathfrak{p}_1}).$$

Let $C \subset \mathbb{F}_p^n$ be a linear code. Then $L_C = red_1^{-1}(C)$ is the first lattice that we are interested in studying. The proof that this is indeed a lattice, together with a product distance lower bound, are given in Section II. This construction is generalized to the division algebra case, as shown in Section IV, where the determinant of the difference of lattice points is lower bounded.

b) Construction 2: Consider again a degree n totally real cyclic extension $K/\mathbb{Q}$, with cyclic Galois group, and a prime p which totally splits. We define this time the reduction map

$$red_3 : \mathcal{O}_K \longmapsto \mathbb{F}_p^n$$

where $x \mapsto (x \pmod{\mathfrak{p}_1}, x \pmod{\mathfrak{p}_2}, \ldots, x \pmod{\mathfrak{p}_n})$. We show that on average, the coset representatives are far apart in product distance in the lattice $\psi(red_3^{-1}(\mathbb{F}_p^n))$. In particular, this allows us to choose low energy codewords, as proven in Section III.

In this paper, by a lattice L, we will mean a $\mathbb{Z}$-module of rank n in $\mathbb{R}^n$, that is $L = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n \subset \mathbb{R}^n$, for some basis $\{x_i, i = 1, \ldots, n\}$. The volume of a lattice L is $|\det(x_1, \ldots, x_n)|$ and is denoted by $vol(L)$.

II. Lattice Construction 1 and Minimum Distance

Let $K/\mathbb{Q}$ be a number field of degree n, with cyclic Galois group $\langle\sigma\rangle$. We further assume that K is totally real, that is, all the n embeddings of K are real, and that a prime p is completely split in this extension, meaning that

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n,$$

where $\mathfrak{p}_i$ are separate prime ideals.

For $x \in K$, the so-called Minkowski embedding gives

$$\psi(x) = (x, \sigma(x), \sigma^2(x), \ldots, \sigma^{n-1}(x)). \qquad (1)$$

Then $\psi(\mathcal{O}_K) = L$ is an n-dimensional lattice in $\mathbb{R}^n$. Let us now define a reduction map

$$red_1 : \psi(\mathcal{O}_K) \longmapsto \mathbb{F}_p^n,$$

where $(x, \sigma(x), \ldots \sigma^{n-1}(x))$ gets mapped to

$$(x \pmod{\mathfrak{p}_1}, \sigma(x) \pmod{\mathfrak{p}_1}, \ldots, \sigma^{n-1}(x) \pmod{\mathfrak{p}_1}).$$

Indeed, $\mathcal{O}_K/\mathfrak{p}_1 \simeq \mathbb{F}_p$, since K is a Galois extension, and there are n distinct primes above p.

Since K is Galois, it is known that the automorphisms σ^k, $k = 1, \ldots, n$ permute the prime ideals $\mathfrak{p}_i$ and we have that

$$p\mathcal{O}_K = \sigma(\mathfrak{p}_1)\sigma^2(\mathfrak{p}_1)\cdots\sigma^n(\mathfrak{p}_1),$$

with $\sigma^n = 1$. Let us now fix $\mathfrak{p} = \mathfrak{p}_1$ and use the notation

$$\mathfrak{p}_i =: \sigma^i(\mathfrak{p}),\ i = 1, \ldots, n.$$

Since σ is an automorphism of K, we have a useful lemma.

Lemma 2.1: Take x and y in $\mathcal{O}_K$. The equations

$$x = y \pmod{\mathfrak{p}_i} \text{ and } \sigma^k(x) = \sigma^k(y) \pmod{\sigma^k(\mathfrak{p}_i)}$$

are equivalent for any $k \in \{1, \ldots, n\}$.

Recall the number field version of the famous Chinese Remainder Theorem.

Proposition 2.2 (Chinese Remainder Theorem): Let $M_1, \ldots, M_k$ be pairwise prime ideals in $\mathcal{O}_K$, and take arbitrary elements $a_1, \ldots, a_k$ in $\mathcal{O}_K$. Then there exists $x \in \mathcal{O}_K$ such that

$$x \equiv a_i \pmod{M_i} \forall i.$$

Furthermore

$$\mathcal{O}_K/(M_1\cdots M_k) \cong \mathcal{O}_K/M_1 \otimes \cdots \otimes \mathcal{O}_K/M_k.$$

We next prove that the proposed construction gives a lattice.

Proposition 2.3: The mapping red_1 is a surjective ring homomorphism. If C is a linear subspace in $\mathbb{F}_p^n$, then $L_C = red_1^{-1}(C)$ is a lattice of rank n in $\mathbb{R}^n$.

Proof: That red_1 is a surjective ring homomorphism follows from the Chinese Remainder Theorem, and

$$\begin{aligned} & red_1(\psi(\mathcal{O}_K))/red_1(\psi(p\mathcal{O}_K)) \\ = \; & red_1(\psi(\mathcal{O}_K))/red_1(\psi(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n)) \\ \simeq \; & \mathcal{O}_K/\mathfrak{p}_1 \otimes \cdots \otimes \mathcal{O}_K/\mathfrak{p}_n \simeq \mathbb{F}_p^n. \end{aligned}$$

Then C is a subgroup of $\mathbb{F}_p^n$, and $red_1^{-1}(C)$ is a subgroup of the lattice $\psi(\mathcal{O}_K) = L$. Since $|\mathcal{O}_K/p\mathcal{O}_K| < \infty$, $\psi(\mathcal{O}_K)$ and $red_1^{-1}(C)$ have same rank as $\mathbb{Z}$-module, and $L_C = red_1^{-1}(C)$ is a lattice of rank n in $\mathbb{R}^n$. ■

Let us now suppose that $C \in \mathbb{F}_p^n$ is a k-dimensional error correcting code with minimum Hamming distance $d_H(C) = d$. We refer to such a code as an (n, k, d) code. By abuse of notation, we write $d_H(c)$ for $d_H(c, 0)$ to denote the Hamming weight of a codeword c of C.

The following propositions give a lower bound on the minimum product distance [6] of the lattice $red_1^{-1}(C)$. The product distance of a lattice point $x = (x_1, \ldots, x_n)$ is by definition (assuming all x_i are nonzero, that is full diversity)

$$d_p(x) = \prod_{i=1}^{n} |x_i|.$$

Since a lattice point is of the form $(x, \sigma_1(x), \ldots, \sigma_{n-1}(x))$ for $x \in \mathcal{O}_K$, we may rewrite the product distance in terms of an algebraic norm:

$$\prod_{i=1}^{n} |x_i| = \prod_{i=1}^{n} |\sigma_i(x)| = |N_{K/\mathbb{Q}}(x)|.$$

Note that since K is totally real, we immediately guarantee that indeed all x_i are nonzero, and thus the diversity criterion is fulfilled. For a lattice, its minimum product distance $d_{p,min}$ is

$$\min_{x \neq 0} d_p(x)$$

over all lattice points x.

Proposition 2.4: Let $x_1 \neq x_2 \in \mathcal{O}_K$ satisfy $d_H(red_1(x_1 - x_2)) \leq t$, we then have that

$$d_p(x_1 - x_2) \geq p^{n-t}.$$

Proof: Let us set $x = x_1 - x_2$. As $red_1(x) \in \mathbb{F}_p^n$ has nonzero coefficients in at most t positions, it follows that $\sigma^i(x) \in \mathfrak{p}$ for at least $n - t$ powers i. This together with Lemma 2.1 reveals that $x \in \sigma^{n-i}(\mathfrak{p}) = \mathfrak{p}_{n-i}$ for at least $n - t$ ideals above p in K. Therefore $p^{n-t} | N_{K/\mathbb{Q}}(x)$. ■

Proposition 2.5: Let C be an (n, k, d) linear code over $\mathbb{F}_p$. The volume of $L_C = red_1^{-1}(C)$ is

$$vol(L_C) = p^{n-k}\sqrt{d(\mathcal{O}_K/\mathbb{Z})},$$

where $d(\mathcal{O}_K/\mathbb{Z})$ denotes the discriminant of $\mathcal{O}_K$.

If furthermore the highest weight codeword in C has Hamming weight t, then

$$d_{p,min}(L_C) \geq p^{n-t}.$$

Proof: The mapping red_1 is surjective, and $red_1^{-1}(C)$ is of index p^{n-k}, therefore the volume of L_C is

$$vol(L_C) = p^{n-k}\sqrt{d(\mathcal{O}_K/\mathbb{Z})}.$$

The second claim follows from Proposition 2.4, since for any $x \in \mathcal{O}_K$, $d_H(red_1(x)) \leq t$ and

$$d_p(x) \geq p^{n-t}.$$

■

Example 2.1: Let K be given by the minimal polynomial $X^3 + X^2 - 10X - 8$. It is totally real of degree $n = 3$, and has a cyclic Galois group. Furthermore

$$2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

Take $C = \{(000), (101), (011), (110)\}$, the binary parity check code with parameters $(3, 2, 2)$. Then

$$d_{p,min}(L_C) \geq p.$$

III. Lattice Construction 2 and its Properties

In this section we will describe another lattice construction method by considering a well known general form of Construction A, but by concentrating on number field lattices.

A. A First Reduction $\pmod p$

Let us consider a real lattice

$$L = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n \subset \mathbb{R}^n, \qquad (2)$$

of rank n for some basis $\{x_i,\ i = 1, \ldots, n\}$.

Let p be a prime, and $y = \sum_{i=1}^n a_i x_i \in L$ a lattice point, where $a_i \in \mathbb{Z}$. Define the mapping $red_2 : L \mapsto \mathbb{F}_p^n$ as

$$red_2(y) = (a_1 \pmod p, a_2 \pmod p, \ldots, a_n \pmod p).$$

This gives a surjective mapping from L to $\mathbb{F}_p^n$. It is well known that $red_2^{-1}(C)$, where C is a linear code in $\mathbb{F}_p^n$, is a sublattice of L.

Let us now suppose that the product distance $d_{p,min}(L) = c \neq 0$ and that we have a k-dimensional linear code $C \subseteq \mathbb{F}_p^n$.

Proposition 3.1: We have that

$$vol(red_2^{-1}(C)) = p^{n-k}vol(L),$$

$$d_{p,min}(red_2^{-1}(C)) \geq c.$$

Proof: The first equality follows just as in the previous section. The minimum product result follows as we know that $red_2^{-1}(C)$ is a sublattice in L. ■

Let us now suppose that we have a totally real field K with cyclic Galois group, and the Minkowski embedding ψ as defined in (1). As previously $L = \psi(\mathcal{O}_K) \subset \mathbb{R}^n$ is a lattice of rank n. Let $\{y_1, \ldots, y_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Let us set $x_i = \psi(y_i)$ and $X = \{x_1, x_2, \ldots, x_n\}$. We then have

$$L = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n,$$

a particular case of (2), where the basis is coming from a number field. We clearly have that

$$red_2^{-1}(0, \cdots, 0) = \psi(p\mathcal{O}_K) \text{ and } red_2^{-1}(\mathbb{F}_p^n) = \psi(\mathcal{O}_K).$$

Let us now consider the set

$$X(p) = \{\sum_{i=1}^n h_i x_i | h_i \in \mathbb{N}, 0 \leq h_i \leq p-1\}.$$

It contains p^n elements and $red_2(X(p)) \simeq \mathbb{F}_p^n$. In other words the set $X(p)$ presents a collection of coset leaders for the group $\psi(\mathcal{O}_K)/\psi(p\mathcal{O}_K)$.

The first construction of Section II gave an explicit relation between the product distance of a lattice point x and the weight of the codeword $red_1(x)$. This allowed to lower bound the product distance of the lattice $red_1^{-1}(C)$ if we knew the weight of the codewords in C. This second construction does not offer such a luxury. However, we will show next that if the ideal structure of the field K is suitable, we will find out that the elements in $X(p)$ are on average well separated in product distance. This is a desirable property to use the elements in $X(p)$ for bit labeling or for coset coding for fading channels.

B. A Second Reduction $\pmod{\mathfrak{p}}$

The general construction based on the mapping red_2 obviously works for any prime p and basis $\{x_1, \ldots, x_n\}$. However, if we again suppose that

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_n,$$

the average product distances of the elements in $X(p)$ is better understood.

For $x \in \mathcal{O}_K$, consider the reduction mapping $red_3 : \mathcal{O}_K \longmapsto \mathbb{F}_p^n$, given by

$$red_3(x) = (x \pmod{\mathfrak{p}_1}, x \pmod{\mathfrak{p}_2}, \ldots, x \pmod{\mathfrak{p}_n}).$$

Lemma 3.2: Using the previous notation we have that

$$red_3(X(p)) \simeq \mathbb{F}_p^n$$

Proof: The reduction mapping $red_3 : \mathcal{O}_K \mapsto {\mathbb{F}_p}^n$, is a surjection. This follows from Proposition 2.2. As an Abelian group $\mathcal{O}_K$ is freely generated by $y_1, y_2, \ldots, y_n$. Therefore $\langle red_3(y_1), \ldots, red_3(y_n)\rangle_{\mathbb{F}_p} = \mathbb{F}_p^n$. As there are p^n elements in $X(p)$ this mapping must be a bijection. ■

We next study the product distance of the lattice $\psi(red_3^{-1}(\mathbb{F}_p^n))$.

Lemma 3.3: Take x in $\mathcal{O}_K$ such that the vector $red_3(x)$ has Hamming weight k. Then its product distance d_p satisfies

$$d_p(\psi(x)) \geq p^{n-k}.$$

Proof: By definition $red_3(x)$ is

$$(x \pmod{\mathfrak{p}_1}, x \pmod{\mathfrak{p}_2}, \ldots, x \pmod{\mathfrak{p}_n}) \in {\mathbb{F}_p}^n.$$

Therefore if the ith coordinate of $red_3(x)$ is zero then we must have that $x \in \mathfrak{p}_i$. Therefore $N(\mathfrak{p}_i)|N_{K/\mathbb{Q}}(x)$, and $d_p(x) = |N_{K/\mathbb{Q}}(x)|$. ■

This finally gives the distribution result of the product distances between the elements in $X(p)$.

Proposition 3.4: Let us fix $t_i \in X(p)$. We then have that

$$d_p(\psi(t_i) - \psi(t_j)) \geq p,$$

for all but $(p-1)^n$ elements $t_j \in X(p), i \neq j$.

Proof: We saw in Lemma 3.2 that red_3 gives a bijection between $X(p)$ and $\mathbb{F}_p^n$. Therefore for a fixed vector t_i there are exactly $(p-1)^n$ vectors t_j, $i \neq j$ for which $red_3(t_i) - red_3(t_j) = red_3(t_i - t_j)$ has weight n. The rest then follows from Lemma 3.3. ■

In particular we have the following bound for $p = 2$.

Corollary 3.5: Pick $p = 2$ and fix $t_i \in X(2)$. Then

$$d_p(\psi(t_i) - \psi(t_j)) \geq 2,$$

for all but one $t_j \in X(2)$, $j \neq i$.

In other words, if $p = 2$, any $\mathbb{Z}$-basis of $\mathcal{O}_K$ does already give a very good separation (in product distance) for points in $X(2)$. This is meaningful for the design of codes for fading channels. If we are using classical lattice constructions for bit mapping or coset coding, it is desirable that we can choose coset representatives such that their (normalized) Euclidean distance is big. For fading channels, the coset representatives should have a good (normalized) product distance instead. The above construction cannot guarantee that the product distance between every representative is "large". However, Proposition 3.4 does show that on average the representatives are far apart in product distance. In particular this construction also allows to choose low energy codewords for the coset representatives, therefore giving a coset code promising shaping properties.

Remark 3.1: One should note that we could have also defined a third lattice construction by considering mapping

$$red_3 \circ \psi^{-1} : \psi(\mathcal{O}_K) \mapsto \mathbb{F}_p^n.$$

IV. Two Constructions for Division Algebras

In this section we will give two lattice constructions for division algebras. The first construction is a generalization of the construction of Section II for number fields. We first need a general definition of a lattice in the space $M_{n \times T}(\mathbb{C})$.

Definition 4.1: A lattice $L \subseteq M_{n \times T}(\mathbb{C})$ has the form

$$\mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_k,$$

where the matrices $B_1, \ldots, B_k$ are linearly independent over $\mathbb{R}$, *i.e.*, form a lattice basis, and k is called the *rank* or the *dimension* of the lattice.

This definition covers also the case where $L \subset \mathbb{C}^n$ (and obviously $L \subset \mathbb{R}^n$). For any lattice in $M_{n \times T}(\mathbb{C})$ we always have the general Construction A, where we simply take a reduction with respect to a given prime p on coefficients of the basis matrices (see the reduction red_2 in Section III for number fields). This method provides a reduction map from L to $(\mathbb{F}_p)^k$, where k is the dimension of the lattice L.

However, we will present two versions of Construction A that are specific to division algebras. Before we can work with division algebras, we have to generalize the number field construction to totally complex fields. We warn the reader that the algebraic prerequisites for this section are higher than for the previous sections. For applications of orders in division algebras to coding theory, we refer the reader to [8]. For the algebraic theory of orders, we suggest [9].

A. First Construction for Complex Number Fields

Suppose that $K/\mathbb{Q}(i)$ is a degree n cyclic extension of algebraic number fields with Galois group $\langle \sigma \rangle$. The relative Minkowski embedding maps $x \in K$ to

$$\psi(x) = (x, \sigma(x), \sigma^2(x), \ldots, \sigma^{n-1}(x)),$$

similarly as (1). Then $\psi(\mathcal{O}_K) = L$ is a $2n$-dimensional lattice in $\mathbb{C}^n$. Let us now suppose that $\mathfrak{p}$ is a prime in $\mathbb{Z}[i]$ such that $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}) = p$, for some prime $p \in \mathbb{Z}$, and $\mathfrak{p}$ is completely split in K, namely:

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_n,$$

for $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ distinct prime ideals of K. We then define a mapping

$$red_4 : \psi(\mathcal{O}_K) \longmapsto \mathbb{F}_p^n,$$

where $(x, \sigma(x), \ldots \sigma^{n-1}(x))$ gets mapped to

$$(x \pmod{\mathfrak{P}_1}, \sigma(x) \pmod{\mathfrak{P}_1}, \ldots, \sigma^{n-1}(x) \pmod{\mathfrak{P}_1}).$$

We then have an analogue for the real case (defined with red_1 in Section II) with the same proof.

Proposition 4.1: The mapping red_4 is a surjective ring homomorphism. If C is a linear subspace in $\mathbb{F}_p^n$, then $red_4^{-1}(C)$ is a lattice in $\mathbb{C}^n$.

B. First Construction for Division Algebras

Suppose that $K/\mathbb{Q}(i)$ is a degree n cyclic extension of algebraic number fields. Let $\mathcal{D} = (K/\mathbb{Q}(i), \sigma, \gamma)$ be a cyclic division algebra, with $\gamma \in \mathbb{Z}[i]$.

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

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

Note that from now on, ψ will refer to the map that sends an algebra element to its matrix representation given above. A $\mathbb{Z}$-order Λ in the division algebra $\mathcal{D}$ is a finitely generated subring of D such that $\mathbb{Q}(\Lambda) = \mathcal{D}$ [9]. We then have that $\psi(\Lambda)$ is a $2n^2$-dimensional lattice in $M_n(\mathbb{C})$.

Let us now consider a specific order $\Lambda = \mathcal{O}_K \oplus \mathcal{O}_K u \cdots \oplus \mathcal{O}_K u^{n-1}$ and fix a prime $\mathfrak{p}$ such that $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ for which $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}) = p$, for some prime p.

We can now define a reduction map $red_5 : \Lambda \mapsto M_n(\mathbb{F}_p)$, by simply setting for $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{D}$, that $red_5(a)$

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

Here the overline refers to reduction modulo $\mathfrak{P}_1$.

We get the following analogue to the commutative case.

Proposition 4.2: Suppose that $\mathfrak{p}$ and (γ) are pairwise prime. We then have that the mapping red_5 is a group homomorphic surjection from $\psi(\Lambda)$ to $M_n(\mathbb{F}_p)$. If C is an additive group in $M_n(\mathbb{F}_p)$, then $red_5^{-1}(C)$ is a lattice in $M_n(\mathbb{C})$.

Proof: The group homomorphism part is obvious. Surjectivity can be proved analogously to Proposition 2.3 as we can use the same proof for every layer $\psi(u^i x_i)$ independently. Note that the additional terms γ do not pose a problem as we chose γ such that it is invertible in all the groups $\mathcal{O}_K/\mathfrak{P}_i$. The fact that $red_5^{-1}(C)$ is a lattice follows again similarly to Proposition 2.3. ■

Remark 4.1: Obviously $M_n(\mathbb{F}_p)$ can be realized as a vector space $\mathbb{F}_p^{n^2}$ and any subspace $C \subseteq M_n(\mathbb{F}_p)$ can be realized as a subspace in $\mathbb{F}_p^{n^2}$.

Let us suppose that we have a set of elements $X = \{x_1, \dots, x_{p^{n^2}}\} \subset \psi(\Lambda) \subset M_n(\mathbb{C})$ such that red_5 gives us a bijection between X and $M_n(\mathbb{F}_p)$. In an analogous way to the second construction in Section III, we are now interested on average values of $det(x_i - x_j)$ between elements in X. We need a well known lemma first first.

Lemma 4.3: Let $GL_n(\mathbb{F}_p)$ be the set of matrices in $M_n(\mathbb{F}_p)$ that have non zero determinant. Then $|M_n(\mathbb{F}_p)| = p^{n^2}$ and

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

Proposition 4.4: Let us suppose that $X = \{x_1, \dots, x_{p^{n^2}}\}$ is a set of elements in $\psi(\Lambda) \subseteq M_n(\mathbb{C})$ such that $red_5(X) = \mathbb{F}_p^{n^2}$. Then

$$|det(x_i - x_j)| \geq 1, \; x_i \neq x_j.$$

If x_i is fixed, then

$$|det(x_i - x_j)| \geq \sqrt{p},$$

at least for $|M_n(\mathbb{F}_p)| - |GL_n(\mathbb{F}_p)| - 1$ elements x_j.

Proof: When x_j goes through all the elements in X we have that $red_5(x_i - x_j)$ goes through all the elements in $M_n(\mathbb{F}_p)$. Clearly the determinant and reduction mapping red_5 commute: $\overline{(det(x_i - x_j))} = det(red_5(x_i - x_j))$, where overline refers to reduction modulo $\mathfrak{P}_1$. Therefore if $red_5(x_i - x_j)$ is not invertible it means that $\mathfrak{P}_1 \mid det(x_i - x_j)$. The theory of central simple algebras tells us that $det(x_i - x_j) \in \mathbb{Z}[i]$ and therefore if $\mathfrak{P}_1 \mid det(x_i - x_j)$ we have that $\mathfrak{p} \mid det(x_i - x_j)$. The rest then follows from Lemma 4.3. ■

C. A Second Division Algebra Construction

Our previous construction was strictly restricted to the case where the ring Λ has a particularly simple structure and the prime $\mathfrak{p}$ is completely split in the maximal subfield K. In this section we present a version of Construction A, that is an analogue to the commutative version of the construction presented in Remark 3.1. The crucial point of this construction is that the prime $\mathfrak{p}$ is completely split in K. The division algebra analogue for this result is the following.

Definition 4.2: We say that the division algebra $\mathcal{D}$ splits at the prime $\mathfrak{p} \subset \mathbb{Z}[i]$ if

$$\mathcal{D} \otimes_{\mathbb{Q}(i)} \mathbb{Q}(i)_{\mathfrak{p}} \simeq M_n(\mathbb{Q}(i)_{\mathfrak{p}}),$$

where $\mathbb{Q}(i)_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of $\mathcal{D}$ at the prime $\mathfrak{p}$.

Let us now suppose that we have a $\mathbb{Q}(i)$-central index n division algebra $\mathcal{D}$ and a *maximal order* Λ. The following proposition is a collection of results from [9], stated without proof.

Proposition 4.5 ([9]): Let us suppose that we have a maximal two-sided ideal $M \subset \Lambda$ such that $M \cap \mathbb{Z}[i] = \mathfrak{p}$. If $\mathcal{D}$ is split at the prime $\mathfrak{p}$ then

$$\Lambda/M \simeq M_n(\mathbb{F}_p).$$

Let us now denote by f the reduction mapping that gives the isomorphism of the previous proposition. We next define a reduction mapping red_6 that will give us the desired lattice construction. Consider the cyclic division algebra $\mathcal{D} = (K/\mathbb{Q}(i), \sigma, \gamma)$ and let ψ be the previously defined embedding to $M_n(\mathbb{C})$.

Proposition 4.6: The mapping $red_6 : \psi(\Lambda) \mapsto M_n(\mathbb{F}_p)$ where for an $x \in \psi(\Lambda)$ we have

$$red_6(x) = f \circ \psi^{-1}(x)$$

is a group homomorphism and if C is a linear subspace in $M_n(\mathbb{F}_p)$, then $f^{-1}(C)$ is a lattice in $M_n(\mathbb{C})$.

Acknowledgement

The research of R. Vehkalahti is supported by the Academy of Finland grant #252457. The research of W. Kositwattanarerk, while still in the Division of Mathematical at Nanyang Technological University, and of F. Oggier for this work was supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07. Part of this work was discussed while W. Kositwattanarerk visited the Department of Mathematics and Statistics of the University of Turku, whose hospitality is warmly acknowledged.

References

[1] J. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", *Springer*.

[2] W. Kositwattanarerk and F. Oggier, On Construction D and Related Constructions of Lattices from Linear Codes, Proc. of the Int. Workshop on Coding and Cryptography, Bergen, Norway, pp. 428-437, April 15-19, 2013.

[3] W. Ebeling, "Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch", originally published by *Vieweg*, reedited by *Springer*.

[4] W. Kositwattanarerk, S.S. Ong, F. Oggier, "Wiretap Encoding of Lattices from Number Fields Using Codes over $\mathbb{F}_p$, ISIT 2013.

[5] F. Oggier, J.-C. Belfiore, "Enabling Multiplication in Lattice Codes via Construction A", in the proceedings of the international information theory workshop (ITW) 2013.

[6] X. Giraud, E. Boutillon, and J. C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inf. Theory*, vol.43, no. 3, pp. 938-952, May 1997.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Springer, Berlin, 1980.

[8] R. Vehkalahti, C. Hollanti, J. Lahtonen and K. Ranto,"On the densest MIMO lattices from cyclic division algebras", *IEEE Trans. Inf. Theory*, vol 55, no 8, pp. 3751–3780, August 2009.

[9] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.