Space-Time Lattice Codes From Algebraic Number Fields

Jarkko Hiltunen

Turku Centre for Computer Science TUCS,
Lemminkäisenkatu 14 A, 5th floor,
FIN-20520 Turku, Finland
e-mail: jakahi@utu.fi

Jyrki Lahtonen

Department of Mathematics,
University of Turku,
FIN-20014 Turku, Finland
e-mail: lahtonen@utu.fi

Turku Centre for Computer Science
TUCS Technical Report No 489
November 2002

ISBN 952-12-1084-2
ISSN 1239-1891

Abstract

The basic principle of diversity in the wireless communication is to provide multiple copies of information for a receiver, which can select or combine the received informations to obtain the best quality for reception. Diversity is commonly introduced in either the space, time, or frequency domain.

Space-time coding is a method in which the diversity is introduced in both the time and space domains by utilizing multiple transmit antennas. The data transmitted from multiple antennas is also spread in time supplying the receiver with a sum of the transmitted signals passed over independent fading channels.

In this report we consider the design of space-time block codes for 4 transmit antennas which are based on the algebraic methods. Especially we study the design methods in which lattices and algebraic number theory have a remarkable role.

This report based on the report on the subproject "Algebraic constructions of ST codes" within the project "Telecommunications applications of discrete mathematics" funded by TEKES and Nokia Research Center.

Keywords: space-time coding, product distance, quaternions, algebraic number field

TUCS Laboratory
Discrete Mathematics for Information Technology Laboratory
Coding Theory Group

Contents

1 Introduction

1.1 Channel Model

We use complex baseband notation: at time t we transmit signal s_t and we receive the signal r_t at the receiver antenna. We assume a Rayleigh fading channel (RFC) given by:

$$r_t = h_t s_t + n_t, \quad t = 0, 1, ... \tag{1}$$

The additive noise n_t is independent, identically complex Gaussian distributed $\mathcal{CN}(0, \sqrt{N_0})$. The complex-valued fading coefficient h_t is $\mathcal{CN}(0, 1)$. The signals are normalized to have average energy one: $\mathbf{E}(|s_t|^2) = 1$; then $\frac{1}{N_0}$ represents the expected signal-to-noise ratio at the receiver. We also assume that the RFC is quasi-static in the sense that, during the transmission of L codeword symbols (L is the number of symbols in the code block) across any one of the links, the complex path gains do not change with time t, but are independent (perfect block interleaving) from one codeword transmission to the next.

1.2 The System Model

In this section we will describe a basic model for a communication system that employs ST coding with N_t transmit antennas and N_r receive antennas. In this system, the message $\mathbf{m} \in \mathcal{M}$ are encoded by function σ to the code matrix $\sigma(\mathbf{m}) \in M_{N_\times L}(\mathcal{A}) \subseteq M_{N_\times L}(\mathbb{C})$, where $\mathcal{A}$ is the constellation alphabet.

We will assume that the encoding function σ maps message $\mathbf{m}$ to the matrix

$$\sigma(\mathbf{m}) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1L} \\ c_{21} & c_{22} & \cdots & c_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N_t 1} & c_{N_t 2} & \cdots & c_{N_t L} \end{pmatrix}.$$

At each time slot t, signals $c_{it},\ i = 1, 2, ..., N_t$ are transmitted simultaneously from the N_t transmit antennas. The fading coefficient h_{ij} is the path gain from transmit antenna i to receive antenna j (we have $N_t N_r$ independent fading channels (see section 1.1)). The wireless channel is assumed to be quasi-static, i.e., the path gains are constant over a frame of length L, and vary from frame to frame. At time slot t the received signal r_{tj} at antenna j is given by

$$r_{tj} = \sum_{i=1}^{N_t} h_{ij} c_{it} \sqrt{E_s} + n_{tj},$$

where n_{tj} is AWGN noise sample for receive antenna j at time slot t (see section 1.1) and the scale factor $\sqrt{E_s}$ has chosen so that the average energy of the constellation elements is 1. The noise samples are independent samples of a zero-mean complex Gaussian random variable with variance $\frac{N_0}{2}$ per dimension.

In matrix notation, we have

$$\overline{R} = \sqrt{E_s}\overline{H}^T \sigma(\mathbf{m}) + \overline{N}$$

where

$$\begin{aligned}
\overline{R} &= \begin{pmatrix} r_{11} & r_{21} & \dots & r_{L1} \\ r_{12} & r_{22} & \dots & r_{L2} \\ \vdots & \vdots & \ddots & \vdots \\ r_{1N_r} & r_{2N_r} & \dots & r_{LN_r} \end{pmatrix}, \\
\overline{H} &= \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1N_r} \\ h_{21} & h_{22} & \dots & h_{2N_r} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_t1} & h_{N_t2} & \dots & h_{N_tN_r} \end{pmatrix}, \\
\overline{N} &= \begin{pmatrix} n_{11} & n_{21} & \dots & n_{L1} \\ n_{12} & n_{22} & \dots & n_{L2} \\ \vdots & \vdots & \ddots & \vdots \\ n_{1N_r} & n_{2N_r} & \dots & n_{LN_r} \end{pmatrix}.
\end{aligned}$$

The receiver knows $\overline{H}$ and computes the maximum likelihood estimate of the transmitted data as

$$\hat{\mathbf{m}} = \arg\min_{\mathbf{e}\in\mathcal{M}} \parallel \overline{R} - \sqrt{E_s}\overline{H}^T \sigma(\mathbf{e}) \parallel,$$

where the matrix norm is the Frobenius norm.

Definition 1.1. An $N_t \times L$ space-time code $\mathcal{C}$ of size K is the subset of $M_{N_t\times L}(\mathbb{C})$ of size K.

1.3 Performance Criteria

Let k denote the rank of matrix $A(C,E) = (C-E)(C-E)^*,\ C, E \in \mathcal{C}$ and for large SNR values (see [2])

$$E(P(C \to E)) \leq [E_s/4N_0]^{-kN_r} \left(\prod_{i=1}^{k} \lambda_i\right)^{-N_r}. \tag{2}$$

Thus a diversity advantage of $N_r k$ and a coding advantage of $(\lambda_1\lambda_2\cdots\lambda_k)^{1/k}$ is achieved. Note that $\lambda_1\lambda_2\cdots\lambda_k$ is the absolute value of the sum of determinant of all principal $k \times k$ cofactors of $A(C,E)$. Moreover it is easy to see that the ranks of the matrices $A(C,E)$ and $C-E$ are equal.

Remark. 1.1. We note that the diversity advantage is the power of SNR in the denominator of the expression for the pairwise error probability derived above. The coding advantage is an approximate measure of the gain over an uncoded system operating with the same diversity advantage.

To get $E(P(\mathbf{c} \to \mathbf{e}))$ as low as possible we try to minimize the right-hand side of (2) and thus we arrive at the following design criterion.

The Rank Criterion: To minimize $[E_s/4N_0]^{-kN_r}$ we have to achieve the maximum diversity N_tN_r, the matrix $C-E$ has to be full rank for any distinct codewords C and E. Otherwise a diversity of kN_r is achieved.

The Product Distance Criterion: To minimize $\left(\prod_{i=1}^{k} \lambda_i\right)^{-N_r}$ we have to maximize the coding advantage $(\lambda_1, \lambda_2, ..., \lambda)^{\frac{1}{k}}$ over all pairs of distinct codewords C and E. For a diversity of N_tN_r, the minimum of the determinant of $A(C,E)$ taken over all pairs of distinct code words C and E must be maximized.

The rank criterion is the more important of the two as it determines the asymptotic slope of the performance curve as a function of E_s/N_0. The product distance criterion is of secondary importance and, ideally should be optimized after the diversity advantage is maximized. The product distance criterion will motivate us to the next definition.

Definition 1.2. The minimum product distance of the space-time code $\mathcal{C}$ is the parameter

$$pd_{\min}(\mathcal{C}) = \min_{C,C' \in \mathcal{C}, C \neq C'} \det((C-C')(C-C')^*)^{\frac{1}{N_t}} \tag{3}$$

Remark. 1.2. If the space-time code $\mathcal{C}$ has not full diversity then $pd_{\min}(\mathcal{C}) = 0$.

Example 1.1. The space-time block code proposed by Alamouti [1] uses the complex orthogonal design

$$O_2^{\mathbb{C}}(z_1, z_2) = \begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix}.$$

We assume that we have a complex signal constellation $\mathcal{A}$ with 2^b elements. At the first time slot, $2b$ bits arrive et the encoder and select two complex symbols c_1 and c_2. These symbols are transmitted simultaneously from antennas one and two, respectively. At the second time slot, signals c_2^* and c_1^* are transmitted simultaneously from antennas one and two, respectively.

It is easy to see that the Alamouti scheme has full diversity.

The receiver computes the maximum likelihood estimate of the transmitted data as

$$\arg \min_{c_1, c_2 \in \mathcal{A}} \sum_{j=1}^{N_r} \left(|r_{1j} - (h_{1j}c_1 + h_{2j}c_2)|^2 + |r_{2j} - (-h_{1j}c_2^* + h_{2j}c_1^*)|^2 \right). \tag{4}$$

The block $\mathbf{r_j} = (r_{1j}, r_{2j})$ received at antenna j is given by

$$\mathbf{r_j} = (h_{1j}, h_{2j}) \begin{pmatrix} c_1 & -c_2^* \\ c_2 & c_1^* \end{pmatrix} + (n_{1j}, n_{2j}). \tag{5}$$

It is easy to see that

$$(r_{1j}, r_{2j}^*) = (c_1, c_2) \begin{pmatrix} h_{1j} & h_{2j}^* \\ h_{2j} & -h_{1j}^* \end{pmatrix} + (n_{1j}, n_{2j}^*), \tag{6}$$

where

$$H = \begin{pmatrix} h_{1j} & h_{2j}^* \\ h_{2j} & -h_{1j}^* \end{pmatrix}$$

is an orthogonal matrix.

When we multiply the equation (6) on right by matrix H^* we get

$$(\tilde{r}_{1j}, \tilde{r}_{2j}) = ((|h_{1j}|^2 + |h_{2j}|^2)c_1, (|h_{1j}|^2 + |h_{2j}|^2)c_2) + (\tilde{n}_{1j}, \tilde{n}_{2j}^*), \tag{7}$$

where $\tilde{n}_{tj}$ still are independent samples of a zero-mean complex Gaussian random variable. Thus the maximum likelihood estimates for c_1 and c_2 are

$$\hat{c}_1 = \arg \min_{c \in \mathcal{A}} \sum_{j=1}^{N_r} |\tilde{r}_{1j} - (|h_{1j}|^2 + |h_{2j}|^2)c|^2$$

and

$$\hat{c}_2 = \arg\min_{c\in\mathcal{A}} \sum_{j=1}^{N_r} |\tilde{r}_{2j} - (|h_{1j}|^2 + |h_{2j}|^2)c|^2.$$

1.4 Algebra Representation

Definition 1.3. A vector space A ($\dim(A) < \infty$), over a field K is an K-algebra with a multiplication which turns it into a ring defined such that, if $\alpha \in K$ and $x, y \in A$, then

$$\alpha(xy) = (\alpha x)y = x(\alpha y).$$

An algebra A which does not satisfy $(ab)c = a(bc)$ for all $a, b, c \in A$ is called a nonassociative algebra.

Definition 1.4. If A and B are K-algebras, then an algebra homomorphism (or K-homomorphism) of A into B is a function $\phi : A \to B$ which preserves the algebra operations, i.e., for all $c, d \in K$, $x, y \in A$

$$\begin{aligned} \phi(cx + dy) &= c\phi(x) + d\phi(y), \\ \phi(xy) &= \phi(x)\phi(y), \\ \phi(1_A) &= 1_B. \end{aligned}$$

Definition 1.5. A representation of K-algebra A is an algebra action of A on a vector space V over K by linear maps, i.e. a representation of the K-algebra A is a K-homomorphism

$$\rho : A \to \mathrm{End}(V).$$

Here we identify $\rho(a)$, $a \in A$ with its matrix form i.e., $\rho(a) \in K[\dim(V)]$, where we use $S[n]$ to stand for $n \times n$ matrices with entries in the set S.

Remark. 1.3. A representation of a group G is a group action of G on a vector space V by invertible linear maps i.e., a representation of the group G is a group homomorphism

$$\rho : G \to \mathrm{GL}(V).$$

Example 1.2. The elements of the quaternion algebra with $\mathbb{R}$-basis $\{1, i, j, k\}$ can be represented in a very simple form as follows. A quaternion is an object of the form

$$q = a + bi + cj + dk,$$

where the coordinates $a,\ b,\ c$ and d are real numbers. The addition of two quaternions is done componentwise, and the multiplication is defined by the relations

$$i^2 = j^2 = k^2 = -1, \text{ and } ij = k,\ jk = i,\ ki = j.$$

The conjugate quaternion of the above entity is $q^* = a - bi - cj - dk$. From the relation $qq^* = a^2 + b^2 + c^2 + d^2$ we see that a non-zero quaternion has an inverse, hence the quaternions form a division algebra. Let $\mathbb{H}$ denote the set of quaternions. Let q be any quaternion. The map

$$\rho(q) : \mathbb{H} \to \mathbb{H},\ x \mapsto qx$$

is a $\mathbb{R}$-linear map and

$$\rho(qq') = \rho(q) \circ \rho(q') \text{ for all } q, q' \in \mathbb{H},$$

so $q \mapsto \rho(q)$ is a representation of the $\mathbb{R}$-algebra $\mathbb{H}$. Let us study $\rho(x_1 + x_2 i + x_3 j + x_4 k) :\ \mathbb{H} \to \mathbb{H} :$

$$\begin{array}{lll} 1 & \mapsto (x_1 + x_2 i + x_3 j + x_4 k)1 & = x_1 + x_2 i + x_3 j + x_4 k \\ i & \mapsto (x_1 + x_2 i + x_3 j + x_4 k)i & = -x_2 + x_1 i - x_4 j + x_3 k \\ j & \mapsto (x_1 + x_2 i + x_3 j + x_4 k)j & = -x_3 + x_4 i + x_1 j - x_2 k \\ k & \mapsto (x_1 + x_2 i + x_3 j + x_4 k)k & = -x_4 - x_3 i + x_2 j + x_1 k, \end{array}$$

so the matrix of $\rho(x_1 + x_2 i + x_3 j + x_4 k)$ with respect to the natural basis is

$$\rho(x_1 + x_2 i + x_3 j + x_4 k) = \begin{pmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & x_4 & -x_3 \\ x_3 & -x_4 & x_1 & x_2 \\ x_4 & x_3 & -x_2 & x_1 \end{pmatrix}. \tag{8}$$

It is easy to see that $\mathbb{H}$ is an algebra with no zero divisors and thus all the matrices $\rho(q),\ q \in \mathbb{H}\backslash\{0\}$ have full rank. Moreover the matrix representation for q^* is

$$\rho(q^*) = \rho(q)^* = \rho(q)^T.$$

Remark. 1.4. The example 1.2 can be generalized for all finite dimensional associative algebras.

2 Algebraic Number Fields and Lattices

The objective in this chapter is to generalize the very attractive 2-antenna Alamouti scheme to the case of four transmit antennas by using lattices.

Unfortunately, when we consider the full rate space-time codes for more than 2-transmit antennas we must relax on the orthogonality property.

By a lattice we mean a free abelian group L_{lat} of a finite rank (i.e. as a set and a group something that looks like a direct product of a finite number of copies of the additive group of integers) together with its embedding into an ambient vector space V (real or complex) that we assume to have an suitable inner product and hence all the metric concepts (distance, inner products, orthogonality) as the lattice then inherits these structures from the ambient space.

Definition 2.1. A set $L_{lat} \subseteq V$ is a lattice, if there exists linear independent elements $b_1, ..., b_m \in V$ such that

$$L_{lat} = \{\sum_{i=1}^{m} r_i b_i \mid r_i \in \mathbb{Z}\}.$$

The set $b_1, ..., b_m$ is called a basis for L_{lat} of rank m. If $m = \dim(V)$ then we say that the lattice L_{lat} is full.

Example 2.1. If we consider $\mathbb{C}$ as a vector space over $\mathbb{R}$ with basis $\{1, i\}$ we get that the set of Gaussian integers

$$\{a + bi \mid a, b \in \mathbb{Z}\}$$

form a lattice in the complex plane $\mathbb{C}$.

In space-time coding the natural ambient space for the lattices is the vector space of complex $N_t \times L$ matrices. Here L is still the length of the code and N_t is still the number of transmit antennas. Now we only consider square matrices, i.e. the case $N_t = L$, but the more general case $L > N_t$ is surely worth studying. Thus the points in our lattice L_{lat} will actually be matrices. Now we give away the point of lattices in the space-time coding: As the difference between two lattice points is another lattice point, the so called rank criterion is now equivalent to simply demanding that all the non-zero matrices in the lattice be of full rank, or in the case $N_t = L$ that all the non-zero matrices in the lattice should be invertible. The point is that these codes have the property of geometric uniformity i.e. the code looks exactly the same from each code block. We designed our codes with this rank criterion in mind using product distance distribution, i.e. the distribution of the absolute values of the determinants of the non-zero lattice matrices, as an auxiliary design criterion.

For the purposes of fast decoding it would be very desirable that the lattice should satisfy a more strict version of the rank criterion. Namely we really would like to have our lattice L_{lat} to lie in a vector space V with the property that any non-zero matrix in the whole space V (rather than in the discrete subset L_{lat}) be of full rank/invertible. In this case we could have a degree of control of the errors introduced by a linear decoder (= matched filter) and probably at least achieve full diversity gain of N_t with a very efficient decoding algorithm. Like in the Alamouti decoding (see the example 1.1) it is very useful that we will get full rank/invertible matrix when we replace the entries of the non-zero matrix belongs to the lattice by channel coefficients.

What will be done in this paper is as follows. Let us first choose a modulation alphabet, e.g. 16-QAM or QPSK. We assume that the alphabet is a subset of a nice lattice in the complex plane. By 'nice' we mean that it is contained in the ring of integers $\mathcal{O}$ of a quadratic imaginary algebraic number field K. We will then show by examples, how the extension fields of K can be used in constructing lattices of invertible matrices. The entries of these matrices are linear functions of several variables c_i. The method of construction will guarantee that the rank criterion is met, when we restrict values of the symbols by requiring $c_i \in \mathcal{O}$. So we are tailoring the code matrices according to the choice of the modulation alphabet, and in this sense the usefulness of our matrices is limited in comparison to that of the orthogonal designs. However, it is obvious that our construction can be carried out for any number of transmit antennas, which will more than offset we hope.

The excellent starting point is the relation between the real quaternion algebra $\mathbb{H}$ and the Alamouti matrices as we seen in the example below.

Example 2.2. The elements of the quaternion algebra with $\mathbb{R}$-basis $\{1, i, j, k\}$ can be represent very simple form as follows. A quaternion is an object of the form

$$q = a + bi + cj + dk,$$

where the coordinates a, b, c and d are real numbers. The addition of two quaternions is done componentwise, and the multiplication is defined by the relations

$$i^2 = j^2 = k^2 = -1, \text{ and } ij = k, \ jk = i, \ ki = j.$$

As we have seen above the the set of quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ is a 4-dimensional vector space over $\mathbb{R}$. We can view $\mathbb{H}$ as a vector space $\mathbb{H}_{\mathbb{C}}$ over $\mathbb{C}$ be the following action:

$$z * q = qz \text{ for all } z \in \mathbb{C}, q \in \mathbb{H}.$$

Now for any $z = z_1 + z_2 i \in \mathbb{C}$ we have $zj = jz^*$ and we easily see that $\mathbb{H}_{\mathbb{C}}$ has a $\mathbb{C}$-basis $\{1, j\}$.

Let x be any quaternion. The map

$$\rho(x): \mathbb{H} \rightarrow \mathbb{H}, \ q \mapsto xq$$

is then a $\mathbb{C}$-linear map ($\mathbb{C}$ acts from the right) and we have the relation

$$\rho(x) \circ \rho(y) = \rho(xy) \text{ for all } x, y \in \mathbb{C},$$

so $x \mapsto \rho(x)$ is a representation of $\mathbb{H}$ by complex linear maps $\mathbb{H}_{\mathbb{C}} \rightarrow \mathbb{H}_{\mathbb{C}}$.

Let z_1 and z_2 be arbitrary complex numbers. Let us study $\rho(z_1 + z_2 j)$: $\mathbb{H}_{\mathbb{C}} \rightarrow \mathbb{H}_{\mathbb{C}}$:

$$\begin{aligned} 1 \mapsto z_1 + z_2 j &= z_1 * 1 + z_2^* * j \\ j \mapsto z_1 j - z_2 &= -z_2 * 1 + z_1^* * j, \end{aligned}$$

so the matrix of $\rho(z_1 + z_2^* j)$ with respect to the basis $\{1, j\}$ is

$$\begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix}$$

i.e the Alamouti matrix.

Especially the quaternions $1, i, j, k$ can be identified with 2×2 matrices

$$\begin{aligned} \rho(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \rho(i) &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ \rho(j) &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ \rho(k) &= \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}. \end{aligned} \tag{9}$$

Now it is easy to that all the matrices $\rho(q),\ q \in \mathbb{H}_{\mathbb{C}} \setminus \{0\}$ have full rank.

Some similar constructions for 4 transmit antennas have been known. The rate $\frac{3}{4}$ orthogonal design from [3] consists of matrices of the following type

$$\begin{pmatrix} z_1 & z_2 & z_3 & 0 \\ -z_2^* & z_1^* & 0 & z_3 \\ z_3^* & 0 & -z_1^* & z_2 \\ 0 & z_3^* & -z_2^* & -z_1 \end{pmatrix}.$$

The resulting code shares some of the good properties of the Alamouti scheme, e.g. it is easy to separate the individual symbols within a block at the receiving end by applying a linear process to the received complex vector (see the example 1.1). However, it is not of full rate. It is known that no full rate orthogonal designs for 4 antennas exist (see [3]). When we look for full rate codes, we must relax on the orthogonality property. This will necessarily make decoding more complex, and we must keep an eye on the decoding complexity as well. Some non-orthogonal codes have been suggested. One such is the so called ABBA-scheme (discovered at NRC by Ari Hottinen and Olav Tirkkonen, [7])

$$\begin{pmatrix} z_1 & -z_2^* & z_3 & -z_4^* \\ z_2 & z_1^* & z_4 & z_3^* \\ z_3 & -z_4^* & z_1 & -z_2^* \\ z_4 & z_3^* & z_2 & z_1^* \end{pmatrix}$$

that really has 2 distinct Alamouti matrices A and B grouped into rows of blocks AB and BA, hence the name. Unfortunately if we restrict the code symbols $z_1, ..., z_4$ to e.g. QPSK or 16-QAM constellation, it is easy to find pairs of code matrices violating the rank criterion. Nevertheless, ABBA gains some diversity over the Alamouti scheme and will serve as a reference point for our codes.

Before the next example we have to present a couple definitions.

Definition 2.2. Let the coordinates of the basis vectors for the lattice $L_{lat} \subseteq \mathbb{R}^n$ be

$$\begin{aligned} \mathbf{b}_1 &= (b_{11}, b_{12}, ..., b_{1n}), \\ \mathbf{b}_2 &= (b_{21}, b_{22}, ..., b_{2n}), \\ &\cdots \\ \mathbf{b}_m &= (b_{m1}, b_{m2}, ..., b_{mn}), \end{aligned}$$

where $n \geq m$. The matrix

$$M = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \cdots & \cdots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

is called a generator matrix for the lattice L_{lat} and the determinant of L_{lat} is the determinant of the matrix MM^*,

$$\det L_{lat} = \det(MM^*).$$

$\sqrt{\det L_{lat}}$ is the volume of fundamental region (see [8]).

Definition 2.3. The density of the lattice $L_{lat} \subseteq \mathbb{R}^n$ is given by

$$\Delta(L_{lat}) = \begin{cases} \frac{\rho^n \pi^{\frac{n}{2}}}{\left(\frac{n}{2}\right)! \sqrt{\det L_{lat}}} & \text{if } n \text{ is even,} \\ \frac{\rho^n \pi^{\lfloor \frac{n}{2} \rfloor} 2^{\lceil \frac{n}{2} \rceil}}{1 \cdot 3 \cdot 5 \cdots n \sqrt{\det L_{lat}}} & \text{if } n \text{ is odd,} \end{cases},$$

where ρ is half the minimal distance between lattice points; ρ is called the packing radius of L_{lat} (see details [8]).

Remark. 2.1. The density of the lattice $L_{lat} \subseteq \mathbb{R}^n$ is

$$\begin{aligned} \Delta(L_{lat}) &= \text{proportion of the space that is occupied by the spheres} \\ &= \frac{\text{volume of one sphere}}{\text{volume of fundamental region}}. \end{aligned}$$

Example 2.3. It is well known (see [8]) that the densest six-dimensional lattice is $E_6 = \{k_1 v_1 + k_2 v_2 + k_3 v_3 \mid k_i \in \mathcal{E}\}$, where

$$\begin{aligned} v_1 &= (\sqrt{-3}, 0, 0) \\ v_2 &= (0, \sqrt{-3}, 0) \\ v_3 &= (1, 1, 1) \end{aligned} \tag{10}$$

and $\mathcal{E} = \{a + \omega b \mid a, b \in \mathbb{Z},\ \omega = \frac{-1+\sqrt{-3}}{2}\}$ is the set of Eisenstein integers.

The mapping

$$\varphi : \mathbb{C}^3 \to \langle X(1,0,0), X(i,0,0), ..., X(0,0,i) \rangle_{\mathbb{R}}$$

$$\varphi(a_1+b_1 i, ..., a_3+b_3 i) = \frac{1}{2}(a_1 X(1,0,0)+b_1 X(i,0,0)+\cdots+a_3 X(0,0,1)+b_3 X(0,0,i))$$

is square Euclidean distance preserving and E_6 is the densest six-dimensional lattice, thus this guarantee that the finite subset of $\varphi(E_6)$ has quite good minimum product distance (= the squared minimum distance of E_6).

The decoding is quite nice because the first we can separate the symbols by using the property of orthogonality and then we can use a quite efficient decoding algorithm for E_6 (see [8]) to find the closest point belongs to E_6.

In the end of this section we will consider the code $\mathcal{C}(E_{6,256}) = \varphi(E_{6,256})$, where $E_{6,256} = \arg\min_{A \subseteq E_6, |A|=256} \sum_{a \in A} \parallel a \parallel$.

Obviously any orthogonal design will similarly work for us but we know that there are very few orthogonal designs out there (see [3]). A natural question is then the existence of other examples of vectors spaces meeting the strict rank criterion. However, in this section we concentrate on such lattices that themselves do meet the rank criterion, but won't meet the strict rank criterion, i.e. there will be singular matrices in the real vector space spanned by the lattice points. This is because such lattices do exist for all sizes. To be precise, we study some examples of lattices of 4×4 complex matrices that span an 8-dimensional vector space. We introduce a few techniques that allow us to construct lattices that avoid the singular matrices that exist in the space they span. These are really minor modifications of the well-known relation of the quaternion algebra to the complex orthogonal design.

Given a field K and an N_t-dimensional division algebra F over K, we can represent the multiplication rule in F by $N_t \times N_t$ matrices with entries in K. Simply pick a suitable K-basis $\{\beta_1, ..., \beta_{N_t}\}$ for F and represent an element $a \in F$ by the matrix of K-linear mapping $\rho(a)$ given by the multiplication rule $x \mapsto ax$ with respect to the chosen basis (see [5]). Later we suppose that the reader knows the basic facts from algebraic number theory (see [5] or [9]).

Example 2.4. If $K = \mathbb{Q}(i)$ then it is well-known that $\mathbb{Q}(i, \sqrt{i})$ is 2-dimensional division algebra over $\mathbb{Q}(i)$ with K-basis $\{1, \sqrt{i}\}$. If $x \in \mathbb{Q}(i, \sqrt{i})$ then x can be represents in the form $x = a + b\sqrt{i},\ a, b \in \mathbb{Q}(i)$ and thus

$$\rho(x) = \begin{pmatrix} a & ib \\ b & a \end{pmatrix}.$$

Now it is easy to see that $\det(\rho(x)) = a^2 - ib^2 = 0$ $(a, b \in \mathbb{Q}(i))$ if and only if $a = b = 0$.

Now the main point is that the difference of two distinct such matrices corresponds to multiplication by a non-zero element of F. Hence this difference matrix is invertible, i.e. of full rank. Thus any code that is a subset of the image of such a representation of a division algebra necessarily has full diversity.

It is a well-known fact about division algebras over the reals and the complex numbers that there are no bigger division algebras than the quaternions (and quaternions really are not an algebra over the complex numbers, but for our purposes they will more or less serve as such as the Alamouti scheme already shows). Therefore we want to see, what can be done with division algebras over a smaller field. After all, for the above construction to work, it is only necessary that the ground field K contains the modulation alphabet. The most common modulation alphabets, QPSK and 16/64-QAM, may be viewed (after scaling and possibly an additive translation) as elements of the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of Gaussian integers. Thus it is natural to consider the case $K = \mathbb{Q}(i)$ like in the example 2.4.

Remark. 2.2. If the modulation alphabet is M-PSK, then it is natural to consider the case $K = Q(e^{\frac{2\pi i}{M}})$.

2.1 Number Field Extensions

The division algebras over the field $K = \mathbb{Q}(i)$ that come to mind are its algebraic extension fields. Let F be one such a finite extension of rank n. As we want a free abelian group of matrices, it is natural to consider

$$\mathcal{O} = \{\alpha \in F \mid \mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]\},$$

the ring of algebraic integers in F. It is a basic fact from algebraic number theory that as an abelian group the ring $\mathcal{O}$ is always free and of rank $2n$ i.e. $\mathcal{O}$ is isomorphic with a free $\mathbb{Z}$-module $\mathbb{Z}^{2n}$. Because $\mathbb{Z}[i]$ is a Euclidean domain and $\mathcal{O}$ is a torsion-free finitely generated $\mathbb{Z}[i]$-module, $\mathcal{O}$ is also a free $\mathbb{Z}[i]$-module of rank k i.e. $\mathcal{O}$ is isomorphic with a free $\mathbb{Z}[i]$-module $\mathbb{Z}[i]^k$. Now it is easy to see that $k = n$. This means that we can find such a basis $\{\beta_1, ..., \beta_n\}$ for $\mathcal{O}$ that the ring $\mathcal{O}$ consists of all the element of the form

$$a = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n,$$

where the coefficients c_i are Gaussian integers.

Remark. 2.3. It is easy to see that $\{\beta_1, ..., \beta_n\}$ is also $\mathbb{Q}(i)$-basis for F.

As we want to construct a code of 4×4-matrices, we are mostly interested (in the case of an extension field L/K) in the case $n = N_t = 4$. Thus we may assume that $\mathcal{O}$ has a $\mathbb{Z}[i]$-basis $\{\beta_1, ..., \beta_4\}$, and that our code matrices are the 4×4-matrices representing multiplication in the ring $\mathcal{O}$ by the elements of the form

$$a = c_1\beta_1 + c_2\beta_2 + c_3\beta_3 + c_4\beta_4,$$

where the symbols c_i belong to our chosen alphabet, i.e. QPSK or 16-QAM.

Example 2.5. Let $\omega = e^{\frac{\pi i}{8}}$ be a 16th primitive root of unity, and let $F = \mathbb{Q}(\omega)$ be the corresponding cyclotomic field. It is easy to see that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 8$ and a basis of the extension is $\{1, \omega, \omega^2, ..., \omega^7\}$. Furthermore it can be proven that $\{1, \omega, \omega^2, ..., \omega^7\}$ is an integral basis (see [5]). Hence the ring of algebraic integers in F is equal to

$$\mathcal{O} = \mathbb{Z}[\omega] = \{a_1 + a_2\omega + \cdots + a_8\omega^7 \mid a_i \in \mathbb{Z}\}.$$

Now it is easy to see that $\omega^{4+j} = i\omega^j$ $j = 0, 1, 2, 3$ and we may choose as our $\mathbb{Z}[i]$-basis the set

$$\{1 = \beta_1, \omega = \beta_2, \omega^2 = \beta_3, \omega^3 = \beta_4\}.$$

We shall see that with respect to this basis, multiplication by $a = c_1\beta_1 + c_2\beta_2 + c_3\beta_3 + c_4\beta_4$ corresponds to the matrix

$$\rho(a) = \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix}.$$

This matrix is constructed as follows. We multiply a basis vector β_i with a and we get

$$a\beta_i = \sum_{j=1}^{4} a_{ij}\beta_j,\ i = 1, ..., 4$$

and $\rho(a) = (a_{ij})$. For example to get the second column we compute

$$\begin{aligned} a\beta_2 = (c_1 + c_2\omega + c_3\omega^2 + c_4\omega^3)\omega &= c_1\omega + c_2\omega^2 + c_3\omega^3 + c_4\omega^4 \\ &= ic_4 + c_1\omega + c_2\omega^2 + c_3\omega^3 \end{aligned}$$

and from the last form we then read the coefficients forming the second column. The first, the third and fourth columns are gotten similarly from the coordinates of the products $a\beta_1$, $a\beta_3$ and $a\beta_4$. We immediately see that here the antenna alphabets (the sets of possible entries on various rows) are all equal, as our constellation (QPSK or 16/64-QAM) is invariant under multiplication with the imaginary unit i.

Remark. 2.4. We immediately see that we get $2^k \times 2^k$-space time code if we replace $\omega = e^{\frac{2\pi i}{16}}$ by $e^{\frac{2\pi i}{2^{k+2}}}$.

To summarize: our lattice consists of the matrices $\rho(a)$, where a ranges over the ring $\mathcal{O}$ of algebraic integers in the field F, or equivalently when the coordinates c_i range over the ring $\mathbb{Z}[i]$ of Gaussian integers. As any non-zero element a has an inverse in F (but most likely not in $\mathcal{O}$), the matrix $\rho(a)$ is invertible, hence of full rank, whenever at least one of the coordinates c_i is non-zero.

2.2 Some Observations on the Product Distance of Number Field Lattices and on Their Decoding

Let us study the product distances between points of the example lattice constructed in example 2.5. As the lattice is closed under subtraction, we may simply study the determinants of the matrices within our lattice. Now the minimum product distance can be calculate as follows

$$pd_{min} = \min_{a \in \mathcal{O}\setminus\{0\}} \det\left(\rho(a)\rho(a)^*\right)^{\frac{1}{4}}.$$

Consider the algebraic integer $a = c_1 + c_2\omega + c_3\omega^2 + c_4\omega^3$ in our ring $\mathcal{O}$ where the coefficients $c_i \in \mathbb{Z}[i]$ are Gaussian integers. This number a corresponds to the following matrix in our constellation

$$\rho(a) = \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix},$$

and we would like to compute the determinant of this matrix. It is well-known (see [5]) that the determinant of this matrix is equal to the relative norm $N_{\mathbb{Q}(i)}^{\mathbb{Q}(\omega)}(a)$ of the element a. As the field extension $\mathbb{Q}(\omega)/\mathbb{Q}(i)$ is a Galois extension, we can compute the norm as the product of the images of the element a under the various mappings in the corresponding Galois group. This Galois group consists of four automorphisms $f_1,\ f_2,\ f_3$ and f_4. Each automorphism is completely determined, once we know, how it will map the generating element ω, so we may simply set $f_1(\omega) = \omega,\ f_2(\omega) = i\omega,\ f_3(\omega) = -\omega$ and $f_4(\omega) = -i\omega$. We can then compute the norm as follows

$$\begin{aligned} N_{\mathbb{Q}(i)}^{\mathbb{Q}(\omega)}(a) &= f_1(a)f_2(a)f_3(a)f_4(a) \\ &= (c_1 + c_2\omega + c_3\omega^2 + c_4\omega^3)(c_1 + ic_2\omega - c_3\omega^2 - ic_4\omega^3) \\ &* (c_1 - c_2\omega + c_3\omega^2 - c_4\omega^3)(c_1 - ic_2\omega - c_3\omega^2 + ic_4\omega^3) \end{aligned} \tag{11}$$

and we know (see [5]) that the result is a Gaussian integer and

$$\begin{aligned} pd_{min} &= \min_{a \in \mathcal{O}\setminus\{0\}} \det\left(\rho(a)\rho(a)^*\right)^{\frac{1}{4}} \\ &= \min_{a \in \mathcal{O}\setminus\{0\}} \left(\det(\rho(a))\det(\rho(a))^*\right)^{\frac{1}{4}} \\ &= \min_{a \in \mathcal{O}\setminus\{0\}} \sqrt{|N_{\mathbb{Q}(i)}^{\mathbb{Q}(\omega)}(a)|}. \end{aligned}$$

Thus the minimum product distance is equal to one.

Number theoretic tools can also be applied in designing a quick decoding algorithm. Assume that the above matrix $\rho(a)$ is transmitted and that the channel coefficients from the four antennas are some known random complex numbers $h = (h_1, h_2, h_3, h_4)(\leftrightarrow h_1 + h_2\omega + h_3\omega^2 + h_4\omega^3)$. The receiver sees

$$\begin{aligned}
\mathbf{r} &= (h_1, h_2, h_3, h_4)\begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix} + (n_1, n_2, n_3, n_4) \\
&= (c_1, c_2, c_3, c_4)\begin{pmatrix} h_1 & ih_4 & ih_3 & ih_2 \\ h_2 & h_1 & ih_4 & ih_3 \\ h_3 & h_2 & h_1 & ih_4 \\ h_4 & h_3 & h_2 & h_1 \end{pmatrix} + (n_1, n_2, n_3, n_4) \\
&= (c_1, c_2, c_3, c_4)\rho(h) + (n_1, n_2, n_3, n_4),
\end{aligned}$$

where we used the notation $\rho(h)$ to emphasize that the relation between the components and the matrix is identical, even though the components of the vector h are not in Gaussian integers in general. Now we denote

$$\begin{aligned}
f_1(h) &= h_1 + h_2\omega + h_3\omega^2 + h_4\omega^3, \\
f_2(h) &= h_1 + ih_2\omega - h_3\omega^2 - ih_4\omega^3, \\
f_3(h) &= h_1 - h_2\omega + h_3\omega^2 - h_4\omega^3, \\
f_4(h) &= h_1 - ih_2\omega - h_3\omega^2 + ih_4\omega^3,
\end{aligned}$$

i.e. we use the components of the vector h as if they were the coordinates of an element in $\mathcal{O}$.

The product of the conjugates is

$$\begin{aligned}
\rho(f_1(h))\rho(f_2(h))\rho(f_3(h))\rho(f_4(h)) &= h_1^4 - ih_2^4 - h_3^4 + 4h_2h_3^2h_4 - 2h_2^2h_4^2 + ih_4^4 \\
&- 2ih_1^2(h_3^2 + 2h_2h_4) + 4ih_1h_3(h_2^2 + ih_4^2) \\
&= N(h)I_4.
\end{aligned}$$

We can thus solve the estimates for the components c_i by applying a sequence of linear operations as follows

$$\begin{aligned}
\widetilde{\mathbf{r}} &= (\widetilde{r_1}, \widetilde{r_2}, \widetilde{r_3}, \widetilde{r_4}) \\
&= \mathbf{r}\rho(f_2(h))\rho(f_3(h))\rho(f_4(h)) \\
&= N(h)(c_1, c_2, c_3, c_4) + (n_1, n_2, n_3, n_4)\rho(f_2(h))\rho(f_3(h))\rho(f_4(h)). \quad (12)
\end{aligned}$$

Now the decoder will make the decision as follows

$$\widehat{c_i} = \arg\min_{c\in\mathcal{A}} |\widetilde{r_i} - N(h)c|, \ i = 1, 2, 3, 4.$$

Remark. 2.5. The decoding algorithm above looks very nice, but unfortunately it kills the diversity advantage. The main problem is that matrices $\rho(f_i(h)),\ i = 1, ..., 4$ are not unitary matrices, and that they may even be singular. This means that the components of the transformed noise vector are no longer independent Gaussian random variables.

3 Number Field Quaternions

3.1 Quaternions as Vector Space over $\mathbb{C}$

Let $\mathcal{R} \subseteq \mathcal{O}$ ($\subseteq \mathbb{C}$) be rings of algebraic integers within their quotient fields such that

$$[\mathbb{Q}(\mathcal{O}) : \mathbb{Q}(\mathcal{R})] < \infty$$

and that $\mathcal{O}$ is stable under the usual complex conjugation (i.e. $z \in \mathcal{O} \Rightarrow z^* \in \mathcal{O}$).

The basic results from algebraic number theory (see [5]) tell us that $\mathcal{O}$ is a finite dimensional free module over $\mathcal{R}$. Thus also the module

$$\mathbb{H}_{\mathcal{O}} \underset{\text{def}}{=} \mathcal{O} * 1 + \mathcal{O} * j = \{\alpha_1 + j\alpha_2 \in \mathbb{H} \mid \alpha_1, \alpha_2 \in \mathcal{O}\}$$

is a free module over $\mathcal{R}$. If $\{\beta_1, ..., \beta_n\}$ is an $\mathcal{R}$-basis of $\mathcal{O}$, then

$$B = \{\beta_1 * 1, ..., \beta_n * 1, \beta_1 * j, ..., \beta_n * j\}$$

is an $\mathcal{R}$-basis of $\mathbb{H}_{\mathcal{O}}$.

In the example 2.2 we studied the map

$$\rho(x) :\ \mathbb{H} \to \mathbb{H},\ q \mapsto xq,\ \text{for all } x \in \mathbb{H}.$$

$\rho(x)$ was a $\mathbb{C}$-linear map ($\mathbb{C}$ acts from the right) and we had the relation

$$\rho(x) \circ \rho(y) = \rho(xy) \text{ for all } x, y \in \mathbb{C},$$

and so $x \mapsto \rho(x)$ was a representation of $\mathbb{H}$.

It is easy to check that $\mathbb{H}_{\mathcal{O}}$ is a subring of $\mathbb{H}$ and thus the restriction map $\rho_{|\mathbb{H}_{\mathcal{O}}}$ give us the map

$$\lambda(x) :\ \mathbb{H}_{\mathcal{O}} \to \mathbb{H}_{\mathcal{O}},\ q \mapsto xq,\ \text{for all } x \in \mathbb{H}_{\mathcal{O}}.$$

Moreover the $2n \times 2n$-matrices of the $\mathbb{Q}(\mathcal{R})$-linear mapping

$$\lambda(r_1\beta_1 * 1 + \cdots + r_n\beta_n * 1 + r'_1\beta_1 * j + \cdots + r'_n\beta_n * j) : \mathbb{H}_{\mathcal{O}} \to \mathbb{H}_{\mathcal{O}}$$

with respect to the basis B is invertible for all

$$(r_1, ..., r_n, r'_1, ..., r'_n) \in \mathcal{R}^{2n} \setminus \{(0, ..., 0)\}.$$

Example 3.1. If $\mathcal{R} = \mathbb{Z}[i]$ and $\mathcal{O} = \mathbb{Z}[\omega] = \mathbb{Z}[i] + \mathbb{Z}[i]\omega$, where $\omega = \frac{1+i}{\sqrt{2}}$ then $\mathbb{H}_{\mathcal{O}}$ has an $\mathcal{R}$-basis

$$B = \{1 * 1(= 1), \omega * 1(= \omega), 1 * j(= j), \omega * j(= j\omega)\}.$$

Next we study the matrix which corresponds the $\mathbb{Q}(\mathcal{R})$-linear mapping $\lambda(z_1 * (1 * 1) + z_2 * (\omega * 1) + z_3 * (1 * j) + z_4 * (\omega * j))$.

$$\begin{array}{ll}
\lambda(z_1 * (1 * 1)) & = \lambda(z_1) : \\
1 * 1 & \mapsto z_1(1 * 1) = z_1 * (1 * 1) \\
\omega * 1 = \omega & \mapsto z_1\omega = z_1 * (\omega * 1) \\
1 * j = j & \mapsto z_1 j = j z_1^* = z_1^* * (1 * j) \\
\omega * j = j\omega & \mapsto z_1 j\omega = j z_1^* \omega = z_1^* * (\omega * j)
\end{array}$$

$$\lambda(z_1 * (1 * 1)) = \begin{pmatrix} z_1 & 0 & 0 & 0 \\ 0 & z_1 & 0 & 0 \\ 0 & 0 & z_1^* & 0 \\ 0 & 0 & 0 & z_1^* \end{pmatrix}. \tag{13}$$

$$\begin{array}{ll}
\lambda(z_2 * (\omega * 1)) & = \lambda(z_2\omega) : \\
1 * 1 & \mapsto z_2 * (\omega * 1) \\
\omega * 1 = \omega & \mapsto z_2\omega^2 = z_2 i = i z_2 * (1 * 1) \\
1 * j = j & \mapsto z_2\omega j = j(z_2^*\omega^*) = -j(z_2^* i\omega) = (-iz_2^*) * (\omega * j) \\
\omega * j = j\omega & \mapsto z_2\omega j\omega = j z_2^* \omega^* \omega = z_2^* * (1 * j)
\end{array}$$

$$\lambda(z_2 * (\omega * 1)) = \begin{pmatrix} 0 & iz_2 & 0 & 0 \\ z_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & z_2^* \\ 0 & 0 & -iz_2^* & 0 \end{pmatrix}. \tag{14}$$

$$\begin{array}{ll}
\lambda(z_3 * (1 * j)) & = \lambda(j z_3) : \\
1 * 1 & \mapsto j z_3 = z_3 * (1 * j) \\
\omega * 1 = \omega & \mapsto j z_3 \omega = z_3 * (\omega * j) \\
1 * j = j & \mapsto j z_3 j = -z_3^* = -z_3^* * (1 * 1) \\
\omega * j = j\omega & \mapsto j z_3 j\omega = -z_3^*\omega = -z_3^* * (\omega * 1)
\end{array}$$

$$\lambda(z_3 * (1 * j)) = \begin{pmatrix} 0 & 0 & -z_3^* & 0 \\ 0 & 0 & 0 & -z_3^* \\ z_3 & 0 & 0 & 0 \\ 0 & z_3 & 0 & 0 \end{pmatrix}. \tag{15}$$

$$
\begin{array}{ll}
\lambda(z_4 * (\omega * j)) & = \lambda(j z_4 \omega) : \\
1 * 1 & \mapsto j z_4 * \omega = z_4 * (\omega * j) \\
\omega * 1 = \omega & \mapsto j z_4 \omega^2 = j z_4 i = i z_4 * (1 * j) \\
1 * j = j & \mapsto j z_4 \omega j = -z_4^* \omega^* = i z_4^* (\omega * 1) \\
\omega * j = j\omega & \mapsto j z_4 \omega j \omega = -z_4^* \omega^* \omega = -z_4^* * (1 * 1)
\end{array}
$$

$$
\lambda(z_4 * (\omega * j)) = \begin{pmatrix} 0 & 0 & 0 & -z_4^* \\ 0 & 0 & i z_4^* & 0 \\ 0 & i z_4 & 0 & 0 \\ z_4 & 0 & 0 & 0 \end{pmatrix}. \tag{16}
$$

By 13,14,15 and 16 we get that

$$
\lambda(c_1 * (1 * 1) + c_2 * (\omega * 1) + c_3 * (1 * j) + c_4 * (\omega * j)) = \lambda(c_1, c_2, c_3, c_4)
$$

$$
= \begin{pmatrix} c_1 & i c_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & i c_4^* & -c_3^* \\ c_3 & i c_4 & c_1^* & c_2^* \\ c_4 & c_3 & -i c_2^* & c_1^* \end{pmatrix}. \tag{17}
$$

If

$$
C_1 = \begin{pmatrix} c_1 & i c_2 \\ c_2 & c_1 \end{pmatrix} \quad \text{and} \quad C_2 = \begin{pmatrix} c_3 & i c_4 \\ c_4 & c_3 \end{pmatrix}
$$

then

$$
\lambda(c_1, c_2, c_3, c_4) = \begin{pmatrix} C_1 & -C_2^* \\ C_2 & C_1^* \end{pmatrix}
$$

i.e. we get Alamouti matrix.

3.2 The Decoding of the Number Field Quaternion Lattice

A relatively simple decoding algorithm comes out from the following observation. If we multiply the code matrix of example 3.1

$$
\lambda(c_1, c_2, c_3, c_4) = \begin{pmatrix} c_1 & i c_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & i c_4^* & -c_3^* \\ c_3 & i c_4 & c_1^* & c_2^* \\ c_4 & c_3 & -i c_2^* & c_1^* \end{pmatrix}
$$

by its Hermitian conjugate $\lambda(c_1, c_2, c_3, c_4)^*$ (that also equals the matrix representing the conjugate quaternion), we obtain the matrix $\lambda(c_1, c_2, c_3, c_4)\lambda(c_1, c_2, c_3, c_4)^*$ of the very special form

$$\begin{pmatrix} \alpha & k^* & 0 & 0 \\ k & \alpha & 0 & 0 \\ 0 & 0 & \alpha & k^* \\ 0 & 0 & k & \alpha \end{pmatrix},$$

where $\alpha = |c_1|^2 + |c_2|^2 + |c_3|^2 + |c_4|^2$ and $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$. This simple structure should enable the use of a iterative decoding algorithm similar in spirit to the ABBA decoder (due to A.Hottinen, NRC patent). Next we consider careful how this "ABBA" decoder works in the case of number field quaternion (here we assume a single receiver antenna).

Decoding can be done as follows.

$$\begin{aligned}
\mathbf{r} &= (h_1, h_2, h_3, h_4)\lambda(c_1, c_2, c_3, c_4) + \mathbf{n} \\
&\Rightarrow \\
\mathbf{r}'^{\perp} &= \begin{pmatrix} r_1 \\ r_2 \\ r_3^* \\ r_4^* \end{pmatrix} = \begin{pmatrix} h_1 & h_2 & h_3^* & h_4^* \\ h_2 & ih_1 & ih_4^* & h_3^* \\ h_3 & h_4 & -h_1^* & -h_2^* \\ h_4 & ih_3 & -ih_2^* & -h_1^* \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} + \mathbf{n}'^{\perp} = H\mathbf{c}^{\perp} + \mathbf{n}'^{\perp} \\
&\Rightarrow \\
H^*\mathbf{r}'^{\perp} &= \begin{pmatrix} r_1'' \\ r_2'' \\ r_3'' \\ r_4'' \end{pmatrix} = H^*H\mathbf{c}^{\perp} + H^*\mathbf{n}'^{\perp} \\
&= D\mathbf{c}^{\perp} + H^*\mathbf{n}'^{\perp} \\
&= \begin{pmatrix} \alpha & k & 0 & 0 \\ k^* & \alpha & 0 & 0 \\ 0 & 0 & \alpha & k^* \\ 0 & 0 & k & \alpha \end{pmatrix} \mathbf{c}^{\perp} + H^*\mathbf{n}'
\end{aligned}$$

where

$$\alpha = \|\mathbf{h}\|^2$$

and

$$k = h_2h_1^* + ih_1h_2^* + h_4h_3^* + ih_3h_4^*. \tag{18}$$

If $\alpha^2 - |k|^2 = 0$, then we have to make the decisions $\hat{c}_1$ $\hat{c}_2$ $\hat{c}_3$ and $\hat{c}_4$ by using "brute force" decoding.

If $\alpha^2 - |k|^2 \neq 0$, then data estimates can be calculated by multiplicating

(18) by

$$D^{-1} = \frac{1}{\alpha^2 - |k|^2} \begin{pmatrix} \alpha & -k & 0 & 0 \\ -k^* & \alpha & 0 & 0 \\ 0 & 0 & \alpha & -k^* \\ 0 & 0 & -k & \alpha \end{pmatrix}.$$

Thus

$$\begin{aligned} \mathbf{r}^{(\mathbf{0})\perp} &= \begin{pmatrix} r_1^{(0)} \\ r_2^{(0)} \\ r_3^{(0)} \\ r_4^{(0)} \end{pmatrix} = D^{-1}D\mathbf{c}^\perp + D^{-1}H^*\mathbf{n}' \\ &= \mathbf{c}^\perp + D^{-1}H^*\mathbf{n}'. \end{aligned}$$

The below we consider the iterative part of "ABBA" decoder.
The decisions of $\hat{c}_1$ and $\hat{c}_2$:

step 1

$$\hat{c}_1^{(0)} = \arg\min_{c\in\mathcal{A}} |r_1^{(0)} - c|$$

and

$$\hat{c}_2^{(0)} = \arg\min_{c\in\mathcal{A}} |r_2^{(0)} - c|.$$

step 2

$$\begin{aligned} r_1^{(1)} &= r''_1 - k\hat{c}_2^{(0)}, \\ r_2^{(1)} &= r''_2 - k^*\hat{c}_1^{(0)}, \\ \hat{c}_1^{(1)} &= \arg\min_{c\in\mathcal{A}} |r_1^{(1)} - \alpha c| \\ &\text{and} \\ \hat{c}_2^{(1)} &= \arg\min_{c\in\mathcal{A}} |r_2^{(1)} - \alpha c|. \end{aligned}$$

If $\hat{c}_1^{(1)} = \hat{c}_1^{(0)}$ and $\hat{c}_2^{(1)} = \hat{c}_2^{(0)}$ then $\hat{c}_1 = \hat{c}_1^{(0)}$ and $\hat{c}_2 = \hat{c}_2^{(0)}$, else go to **step** 3.

step j $(j = 3, 4, ...)$

$$\begin{aligned} r_1^{(j-1)} &= r''_1 - k\hat{c}_2^{(j-2)}, \\ r_2^{(j-1)} &= r''_1 - k^*\hat{c}_1^{(j-2)}, \\ \hat{c}_1^{(j-1)} &= \arg\min_{c\in\mathcal{A}} |r_1^{(j-1)} - \alpha c| \\ &\text{and} \\ \hat{c}_2^{(j-1)} &= \arg\min_{c\in\mathcal{A}} |r_2^{(j-1)} - \alpha c|. \end{aligned}$$

If $\hat{c}_1^{(j-1)} = \hat{c}_1^{(j-2)}$ and $\hat{c}_2^{(j-1)} = \hat{c}_2^{(j-2)}$, then $\hat{c}_1 = \hat{c}_1^{(j-2)}$ and $\hat{c}_2 = \hat{c}_2^{(j-2)}$, else go to **step** $j+1$.

The decisions of $\hat{c}_3$ and $\hat{c}_4$:

step 1

$$\begin{aligned} \hat{c}_3^{(0)} &= \arg\min_{c\in\mathcal{A}} |r_3^{(0)} - c| \\ &\text{and} \\ \hat{c}_4^{(0)} &= \arg\min_{c\in\mathcal{A}} |r_4^{(0)} - c|. \end{aligned}$$

step 2

$$\begin{aligned} r_3^{(1)} &= r''_3 - k^*\hat{c}_4^{(0)}, \\ r_4^{(1)} &= r''_4 - k\hat{c}_3^{(0)}, \\ \hat{c}_3^{(1)} &= \arg\min_{c\in\mathcal{A}} |r_3^{(1)} - \alpha c| \\ &\text{and} \\ \hat{c}_4^{(1)} &= \arg\min_{c\in\mathcal{A}} |r_4^{(1)} - \alpha c|. \end{aligned}$$

If $\hat{c}_3^{(1)} = \hat{c}_3^{(0)}$ and $\hat{c}_4^{(1)} = \hat{c}_4^{(0)}$, then $\hat{c}_3 = \hat{c}_3^{(0)}$ and $\hat{c}_4 = \hat{c}_4^{(0)}$, else go to **step** 3.

step j $(j = 3, 4, ...)$

$$\begin{aligned} r_3^{(j-1)} &= r''_3 - k^*\hat{c}_4^{(j-2)}, \\ r_4^{(j-1)} &= r''_4 - k\hat{c}_3^{(j-2)}, \\ \hat{c}_3^{(j-1)} &= \arg\min_{c\in\mathcal{A}} |r_3^{(j-1)} - \alpha c| \\ &\text{and} \\ \hat{c}_4^{(j-1)} &= \arg\min_{c\in\mathcal{A}} |r_4^{(j-1)} - \alpha c|. \end{aligned}$$

If $\hat{c}_3^{(j-1)} = \hat{c}_3^{(j-2)}$ and $\hat{c}_4^{(j-1)} = \hat{c}_4^{(j-2)}$, then $\hat{c}_3 = \hat{c}_3^{(j-2)}$ and $\hat{c}_4 = \hat{c}_4^{(j-2)}$, else go to **step** $j+1$.

4 Parameters of the Competing Lattices with QPSK Alphabet and Simulation Results

In the table below we see the most important parameters of the codes we have presented in this section. The normalization is such that $\frac{1}{|\mathcal{C}|}\sum_{M\in\mathcal{C}}\|M\|^2 = 4$ for all table's code $\mathcal{C}$.

code	size	modulation alphabet	$pd_{\min}$
ABBA	256	QPSK	0
Number field lattice	256	QPSK	1/2
Number field quaternion	256	QPSK	1/2
$\mathcal{C}(E_{6,256})$	256		32/55

The simulation results below were obtained using brute force decoding at the receiver. This was done in order to compare the maximum possible theoretical performance of the competing codes. The results may be summarized by saying that our suggestions win over the ABBA-code because of the maximum diversity attained by the number field, the number field quaternion and $\mathcal{C}(E_{6,256})$ constructions. The distance distribution of the ABBA-code is clearly superior to that of our number field lattice. This explains, why ABBA does better at low SNRs. However, based on these simulations it is easy to declare the number field quaternion lattice the winner.

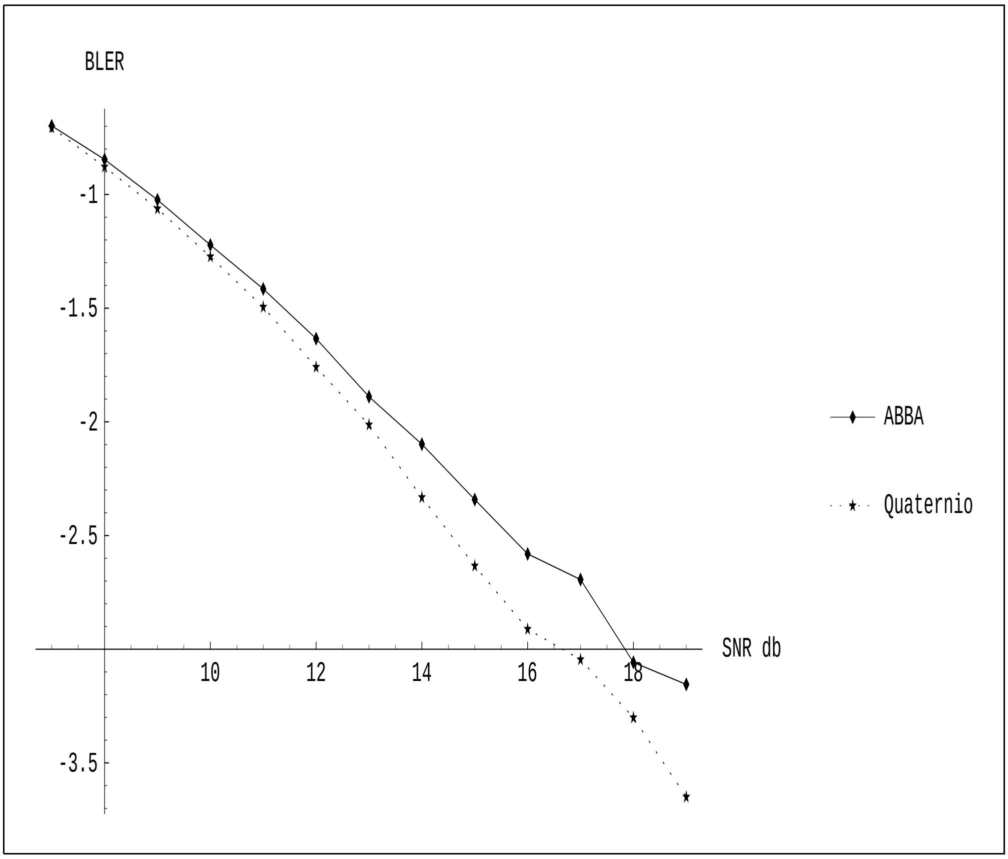

Figure 1: The BLER performance comparison between ABBA-code and the number field quaternion lattice in the Rayleigh fading channel

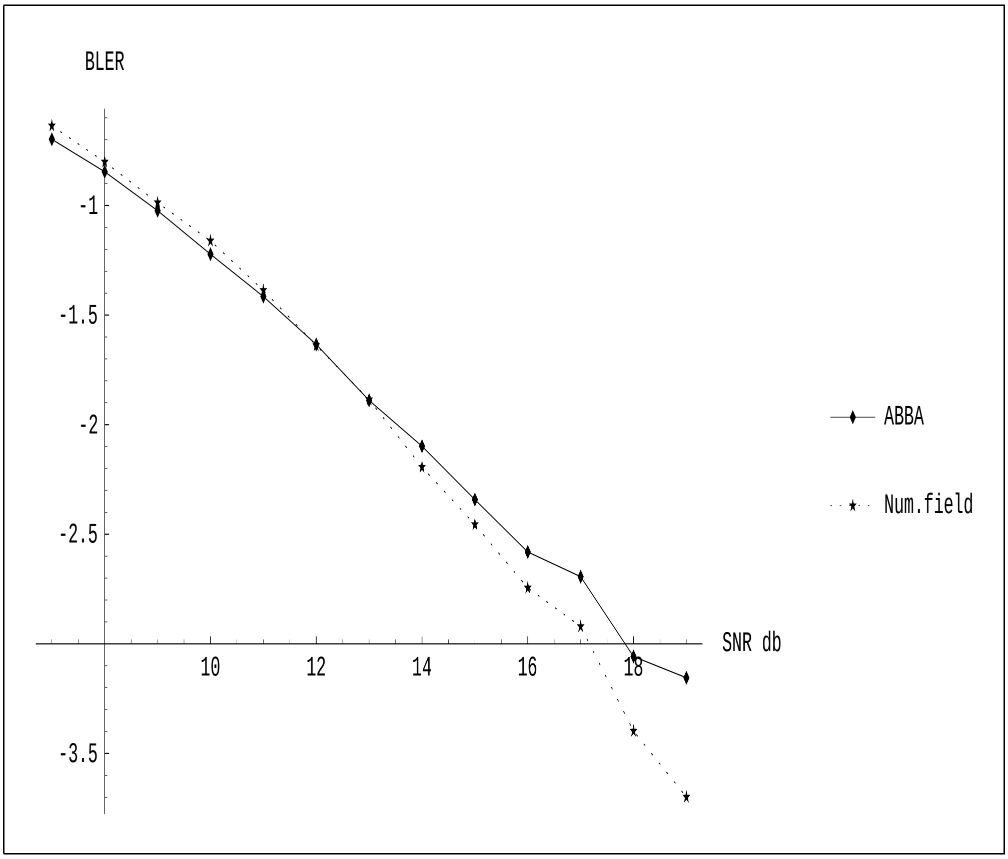

Figure 2: The BLER performance comparison between ABBA-code and the number field lattice in the Rayleigh fading channel

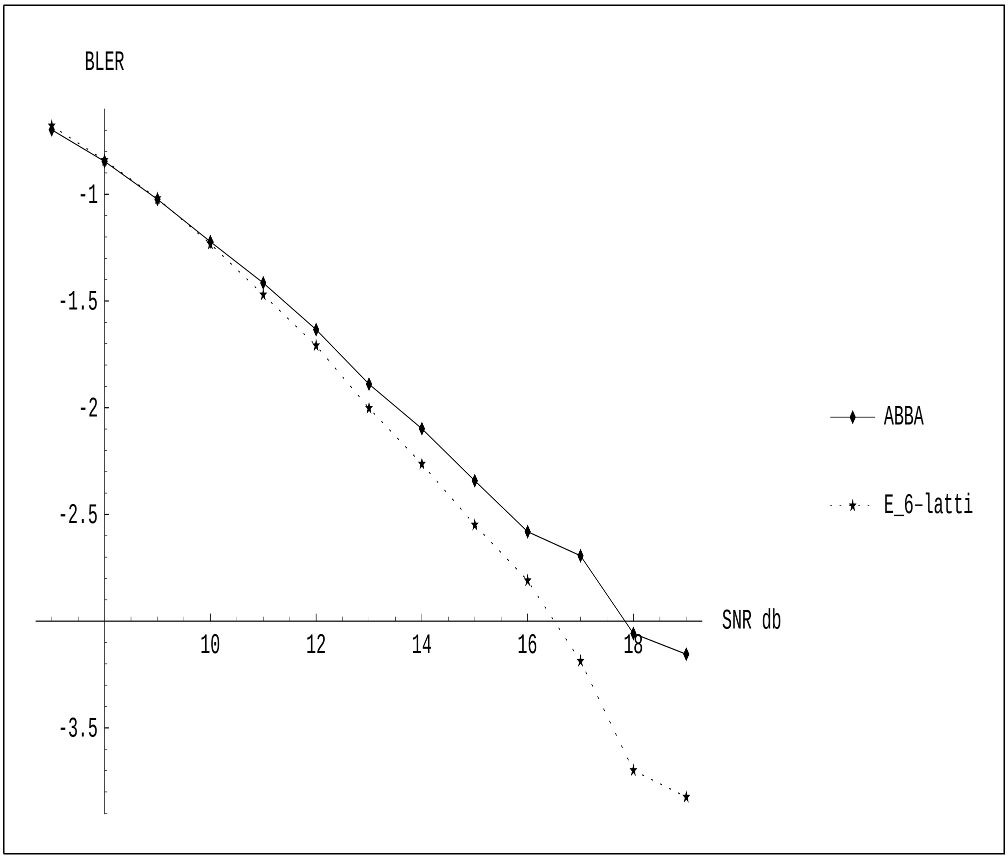

Figure 3: The BLER performance comparison between ABBA-code and $\mathcal{C}(E_{6,256})$ in the Rayleigh fading channel

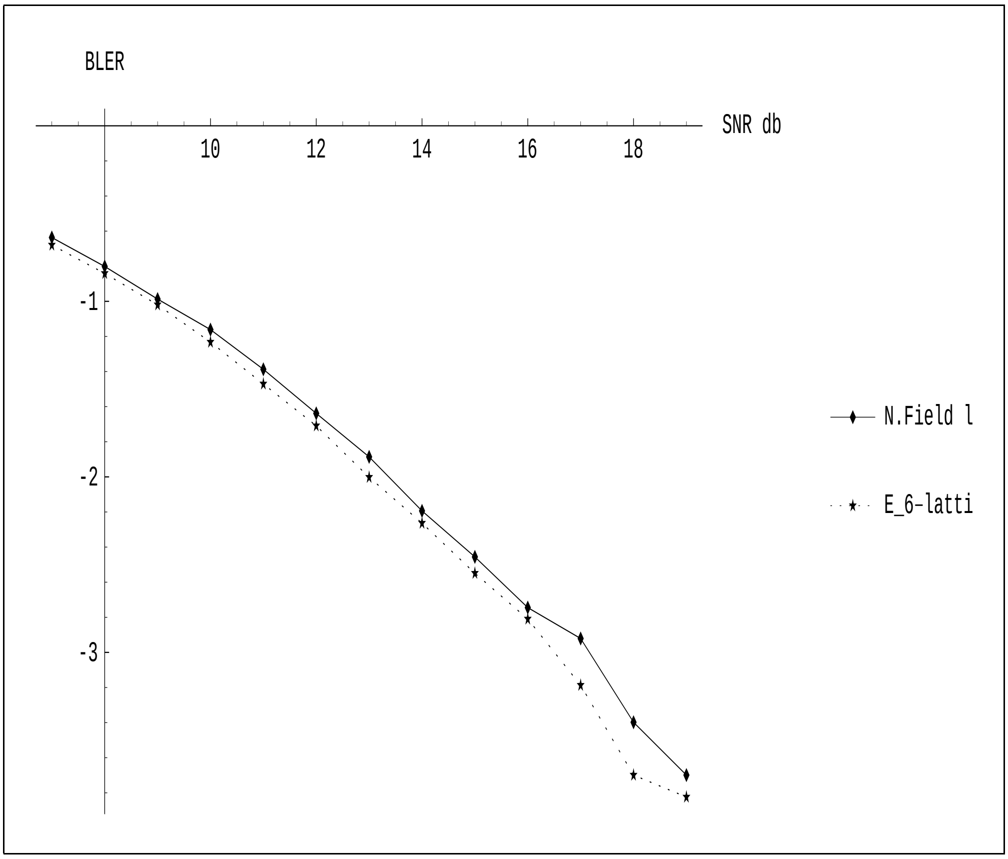

Figure 4: The BLER performance comparison between the number field lattice and $\mathcal{C}(E_{6,256})$ in the Rayleigh fading channel

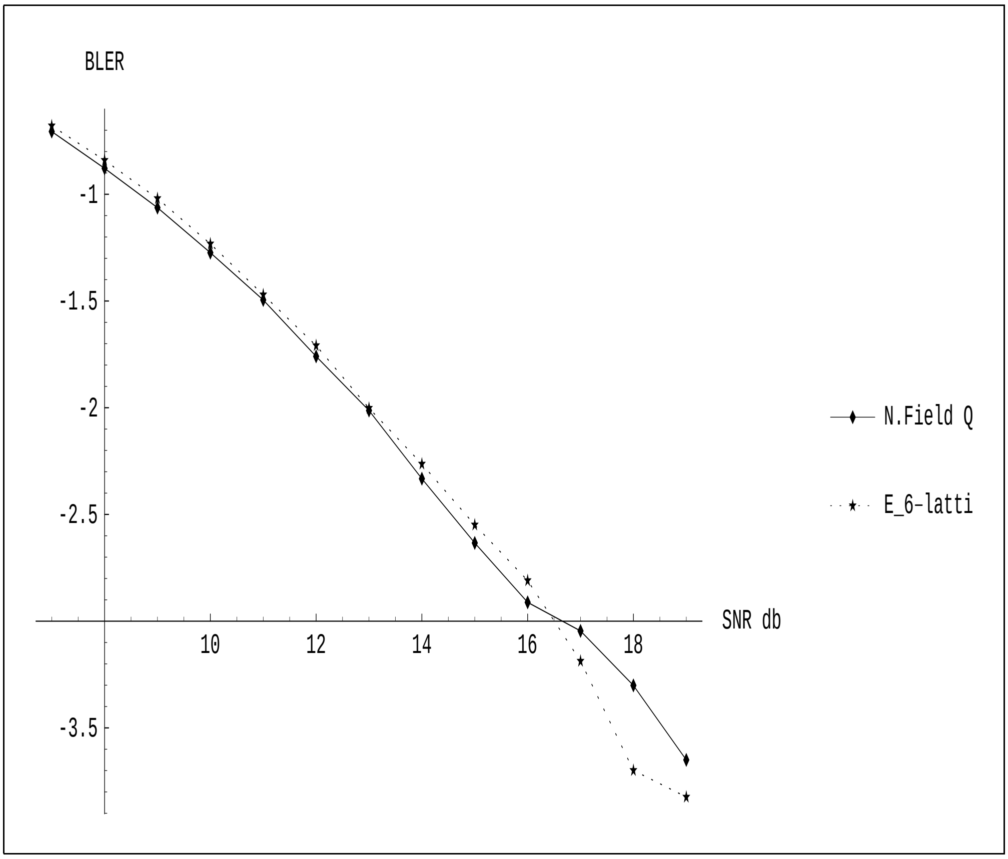

Figure 5: The BLER performance comparison between the number field quaternion lattice and $\mathcal{C}(E_{6,256})$ in the Rayleigh fading channel

References

[1] Alamouti, S. (1998). *A Simple Transmit Diversity Technique for Wireless Communications.* IEEE Journal on Selected Areas in Communications, Vol. 16, pp. 1451-1458.

[2] Tarokh, V., Seshadri, N., and Calderbank, A. R. (1998). *Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction.* IEEE Transactions on Information Theory, Vol. 44, No. 2, March 1998, pp. 744-765.

[3] Tarokh, V., Seshadri, N., and Calderbank, A. R. (1999). *Space-Time Block Codes from Orthogonal Designs.* IEEE Transactions on Information Theory, Vol. 45, No. 5, July 1999, pp. 1456-1467.

[4] Metsänkylä, T., (1996). *Ryhmäteoria*, Lecture Note, Turun Yliopisto.

[5] Metsänkylä, T., (2000). *Algebralliset Luvut*, Lecture Note, Turun Yliopisto.

[6] A. Hottinen, O. Tirkkonen. *Square-Matrix Embeddable Space-Time Block Codes for Complex Signal Constellations.* IEEE Transactions on Information Theory, Vol. 48, No. 2, February 2002.

[7] O. Tirkkonen, Adrian Boariu, and A. Hottinen. *Minimal Non-Orthogonality Rate 1 Space-Time Block Code for 3+ TX Antennas.* ISSSTA 2000.

[8] J.H. Conway, and N. J. A. Sloane. *Sphere Packings, Lattices and Group.* Springer-Verlag, 1988.

[9] T. Ono. *An introduction to algebraic number theory.* Plenum, New York 1990.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.fi

University of Turku
- **Department of Information Technology**
- **Department of Mathematics**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**