Camilla Hollanti | Jyrki Lahtonen

Maximal Orders in the Design of Dense Space-Time Lattice Codes

Turku Centre *for* Computer Science

TUCS Technical Report
No 790, October 2006

Maximal Orders in the Design of Dense Space-Time Lattice Codes

Camilla Hollanti
Turku Centre for Computer Science
Joukahaisenkatu 3-5 B, 20520 Turku, Finland
cajoho@utu.fi
Jyrki Lahtonen
University of Turku, Department of Mathematics
20014 Turku, Finland
lahtonen@utu.fi

TUCS Technical Report
No 790, October 2006

Abstract

We construct explicit rate-one, full-diversity, geometrically dense matrix lattices with large, non-vanishing determinants (NVD) for four transmit antenna multiple-input single-output (MISO) space-time (ST) applications. The constructions are based on the theory of rings of algebraic integers and related subrings of the Hamiltonian quaternions and can be extended to a larger number of Tx antennas. The usage of ideals guarantees a non-vanishing determinant larger than one and an easy way to present the exact proofs for the minimum determinants. The idea of finding denser sublattices within a given division algebra is then generalized to a multiple-input multiple-output (MIMO) case with an arbitrary number of Tx antennas by using the theory of cyclic division algebras (CDA) and maximal orders. It is also shown that the explicit constructions in this paper all have a simple decoding method based on sphere decoding. Related to the decoding complexity, the notion of defect is introduced for the first time and shown to be relevant both in theory and practice. Simulations in a quasi-static Rayleigh fading channel show that our dense quaternionic constructions outperform both the earlier rectangular lattices and the rotated ABBA lattice as well as the DAST lattice.

Keywords: Cyclic division algebras, defect, dense lattices, maximal orders, multiple-input multiple-output (MIMO) channels, multiple-input single-output (MISO) channels, number fields, quaternions, space-time block codes (STBCs), sphere decoding

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Introduction and background

Multiple-antenna wireless communication promises very high data rates, in particular when we have perfect channel state information (CSI) available at the receiver. In [1] the design criteria for such systems were developed and further on the evolution of ST codes took two directions: trellis codes and block codes. Our work concentrates on the latter branch.

The very first ST block code for two transmit antennas was the *Alamouti code* [2] representing multiplication in the ring of quaternions. As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting STBC meets the rank criterion. Matrix representations of other division algebras have been proposed as STBCs at least in [3]-[14], and (though without explicitly saying so) [15]. The most recent work [6]-[15] has concentrated on adding multiplexing gain, i.e. multiple input-multiple output (MIMO) applications, and/or combining it with a good minimum determinant. In this work, we do not specifically seek any multiplexing gains, but want to improve upon e.g. the diagonal algebraic space time (DAST) lattices introduced in [5] by using non-commutative division algebras. Other efforts to improve the DAST lattices and ideas alike can be found in [16]-[18].

The main contributions of this work are:

- We give energy efficient MISO lattice codes with simple decoding that win over e.g. the rotated ABBA [19] and the DAST lattice codes in terms of the block error rate (BLER) performance.

- It is shown that by using a non-rectangular lattice one can gain major energy savings without significant increasement in decoding complexity. The usage of ideals moreover guarantees a non-vanishing determinant > 1 and an easy way to present the exact proofs for the minimum determinants.

- In addition to the explicit MISO constructions, we present a general method for finding dense sublattices within a given CDA in a MIMO setting. This is tempting as it has been shown in [14] that CDA-based square ST codes with NVD achieve the diversity-multiplexing gain (D-MG) tradeoff introduced in [20]. When a CDA is chosen the next step is to choose a corresponding lattice or, what amounts to the same thing, choose an order within the algebra. Most authors, among which e.g. [10], [14], and [15], have gone with the so-called natural order (see Section 3.2, Example 3.2). In a CDA based construction, the density of a sublattice is lumped together with the concept of maximality of an order. The idea is that one can, on some occasions, use several cosets of the natural order without sacrificing anything in terms of the minimum determinant. So the study of maximal orders is easily motivated by an analogy from the theory of error correcting codes: why one would use a particular code of a given minimum distance and length, if a larger code with the same parameters is available.

- Furthermore, related to the decoding complexity, the notion of defect is introduced for the first time, and shown to be relevant both in theory and practice.

At first, we are interested in the coherent MISO case with perfect CSI available at the receiver. The received signal $\mathbf{y} \in \mathbb{C}^n$ has the form

$$\mathbf{y} = \mathbf{h}X + \mathbf{n},$$

where $X \in \mathbb{C}^{m\times n}$ is the transmitted codeword drawn from a ST code $\mathcal{C}$, $\mathbf{h} \in \mathbb{C}^m$ is the Rayleigh fading channel response and the components of the noise vector $\mathbf{n} \in \mathbb{C}^n$ are i.i.d. complex Gaussian random variables.

A *lattice* is a discrete finitely generated free abelian subgroup of a real or complex finite dimensional vector space V, also called the ambient space. Thus, if L is a k-dimensional lattice, there exists a finite set of vectors $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\} \subset V$ such that $\mathcal{B}$ is linearly independent over the integers and that

$$L = \{\sum_{i=1}^{k} z_i\mathbf{b}_i \mid z_i \in \mathbb{Z}, \mathbf{b_i} \in V \text{ for all } i = 1, 2, \ldots, k\}.$$

In the space-time setting a natural ambient space is the space $\mathbb{C}^{n\times n}$ of complex $n \times n$ matrices. When a code is a subset of a lattice L in this ambient space, the *rank criterion* [21] states that any non-zero matrix in L must be invertible. This follows from the fact that the difference of any two matrices from L is again in L.

The receiver and the decoder, however, (recall that we work in the MISO setting) observe vector lattices instead of matrix lattices. When the channel state is $\mathbf{h}$, the receiver expects to see the lattice $\mathbf{h}L$. If $\mathbf{h} \neq 0$ and L meets the rank criterion, then $\mathbf{h}L$ is, indeed, a free abelian group of the same rank as L. However, it is well possible that $\mathbf{h}L$ is not a lattice, as its generators may be linearly dependent over the reals — the lattice is said to *collapse*, whenever this happens.

From the pairwise error probability (PEP) point of view [21], 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 $X, X' \in \mathcal{C}$, also called the *rank* of the code $\mathcal{C}$. When $\mathcal{C}$ is full-rank, the coding gain is proportional to the determinant of the matrix $(X - X')(X - X')^H$, where X^H denotes the transpose conjugate of the matrix X. The minimum of this determinant taken over all distinct code matrices is called the *minimum determinant* of the code $\mathcal{C}$ and denoted by $\delta_{\mathcal{C}}$. If $\delta_{\mathcal{C}}$ is bounded away from zero even in the limit as SNR $\to \infty$, the ST code is said to have the *non-vanishing determinant* property [8]. As mentioned above, for non-zero square matrices being full-rank coincides with being invertible.

The *data rate* R in symbols per channel use is given by

$$R = \frac{1}{n}\log_{|S|}(|\mathcal{C}|),$$

where $|S|$ and $|\mathcal{C}|$ are the sizes of the symbol set and code respectively. This is not to be confused with the *rate of a code design* defined as the ratio of the number of transmitted information symbols to the decoding delay (equivalently, block length) of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. If this ratio is equal to the delay, the code is said to have *full rate*.

This report is organized as follows: basic definitions of algebraic number theory and explicit MISO lattice constructions are provided in Section 2. As a (MIMO) generalization for the idea of finding denser lattices within a given division algebra, the theory of cyclic algebras and maximal orders is briefly introduced in Section 3. In Section 4, we consider the decoding of the nested sequence of quaternionic lattices from Section 2. A variety of results on decoding complexity is established in Section 4, where also the notion of defect is taken into account and shown to be relevant. Simulation results are discussed in Section 5 along with energy considerations. Related figures are provided at the end of the report.

This work has been partly published in a conference, see [3] and [4]. For more background we refer to [21]-[28].

2 Rings of algebraic numbers, quaternions and lattice constructions

We shall denote the sets of integers, rationals, reals, and complex numbers by $\mathbb{Z},\ \mathbb{Q},\ \mathbb{R}$, and $\mathbb{C}$ respectively.

Let us recall the set

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{R}\ \forall t\},$$

where $i^2 = j^2 = k^2 = -1,\ ij = k$, as the ring of *Hamiltonian quaternions*. Note that $\mathbb{H} \simeq \mathbb{C} \oplus \mathbb{C}j$, when the imaginary unit is identified with i. A special interest lies on the subsets

$$\mathbb{H}_{\mathcal{L}} = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{Z}\ \forall t\} \subseteq \mathbb{H}$$

and

$$\mathbb{H}_{\mathcal{H}} = \{a_1 \rho + a_2 i + a_3 j + a_4 k \mid a_t \in \mathbb{Z}\ \forall t,\ \rho = \frac{1}{2}(1 + i + j + k)\} \subseteq \mathbb{H}$$

called the *Lipschitz'* and *Hurwitz' integral quaternions* respectively.

We shall use extension rings of the Gaussian integers

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

inside a given division algebra. It would be easy to adapt the construction to use the slightly denser hexagonal ring of the Eisensteinian integers

$$\mathcal{E} = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where $\omega^3 = 1$, as a basic alphabet. However, the Gaussian integers nicely fit with the popular 16-QAM and QPSK alphabets. Natural examples of such rings are the rings of algebraic integers inside an extension field of the quotient fields of $\mathcal{G}$, as well as their counterparts inside the quaternions. To that end we need division algebras $\mathcal{A}$ that are also 4-dimensional vectors spaces over the field $\mathbb{Q}(i)$.

2.1 Base lattice constructions

Let now $\zeta = e^{\pi i/8}$ (resp. $\xi = e^{\pi i/4} = (1+i)/\sqrt{2}$) be a primitive 16^{th} (resp. 8^{th}) root of unity. Our main examples of suitable division algebras are the number field

$$\mathbf{L} = \mathbb{Q}(\zeta),$$

and the following subskewfield

$$\mathbf{H} = \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi) \subseteq \mathbb{H}$$

of the Hamiltonian quaternions. Note that as $zj = jz^*$ for all complex numbers z, and as the field $\mathbb{Q}(\xi)$ is stable under the usual complex conjugation $(^*)$, the set $\mathbf{H}$ is, indeed, a subskewfield of the quaternions.

As always, multiplication (from the left) by a non-zero element of a division algebra $\mathcal{A}$ is an invertible $\mathbb{Q}(i)$-linear mapping (with $\mathbb{Q}(i)$ acting from the right). Therefore its matrix with respect to a chosen $\mathbb{Q}(i)$-basis $\mathcal{B}$ of $\mathcal{A}$ is also invertible. Our example division algebras $\mathbf{L}$ and $\mathbf{H}$ have the sets $\mathcal{B}_L = \{1, \zeta, \zeta^2, \zeta^3\}$ and $\mathcal{B}_H = \{1, \xi, j, j\xi\}$ as natural $\mathbb{Q}(i)$-bases. Thus we immediately arrive at the following matrix representations of our division algebras.

Proposition 2.1 *Let the variables c_1, c_2, c_3, c_4 range over all the elements of $\mathbb{Q}(i)$. The division algebras $\mathbf{L}$ and $\mathbf{H}$ can be identified via an isomorphism ϕ with the following rings of matrices*

$$\mathbf{L} = \left\{ M_L = M_L(c_1, c_2, c_3, c_4) = \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix} \right\}$$

and

$$\mathbf{H} = \left\{ M = M(c_1, c_2, c_3, c_4) = \begin{pmatrix} c_1 & ic_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & ic_4^* & -c_3^* \\ c_3 & ic_4 & c_1^* & c_2^* \\ c_4 & c_3 & -ic_2^* & c_1^* \end{pmatrix} \right\}.$$

The isomorphism ϕ from $\mathbf{L}$ into the matrix ring is determined by $\mathbb{Q}(i)$-linearity and the fact that ζ corresponds to the choice $c_2 = 1, c_1 = c_3 = c_4 = 0$. The isomorphism ϕ from $\mathbf{H}$ into the matrix ring is determined by $\mathbb{Q}(i)$-linearity and the facts that ξ corresponds to the choice $c_2 = 1$, $c_1 = c_3 = c_4 = 0$, and j corresponds

to the choice $c_3 = 1$, $c_1 = c_2 = c_4 = 0$. *In particular, the determinants of these matrices are non-zero whenever at least one of the coefficients* c_1, c_2, c_3, c_4 *is non-zero.* ■

In order to get ST lattices and useful bounds for the minimum determinant, we need to identify suitable subrings S of these two algebras. Actually, we would like these rings to be free right $\mathcal{G}$-modules of rank 4. This is due to the fact that then the determinants of the matrices of Proposition 2.1 that belong to the subring $\phi(S)$ must be elements of the ring $\mathcal{G}$. We repeat the well-known reason for this for the sake of completeness: the determinant of the matrix representing the multiplication by a fixed element $x \in S$ does not depend on the choice of the basis $\mathcal{B}$ and thus we may assume that it is a $\mathcal{G}$-module basis. However, in that case $x\mathcal{B} \subseteq S$, so the matrix will have entries in $\mathcal{G}$ as all the elements of S are $\mathcal{G}$-linear combinations of $\mathcal{B}$. The claim follows.

In the case of the field $\mathbf{L}$ we are only interested in its ring of integers $\mathcal{O}_L = \mathbb{Z}[\zeta]$ that is a free $\mathcal{G}$-module with the basis $\mathcal{B}_L$. In this case the ring $\phi(\mathcal{O}_L)$ consists of those matrices of $\mathbf{L}$ that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. Similarly, the $\mathcal{G}$-module

$$\mathcal{L} = \mathcal{G} \oplus \xi\mathcal{G} \oplus j\mathcal{G} \oplus j\xi\mathcal{G}$$

spanned by our earlier basis $\mathcal{B}_H$ is a ring of the required type. We call this the ring of *Lipschitz' integers of* $\mathbf{H}$. Again $\phi(\mathcal{L})$ consists of those matrices of $\mathbf{H}$ that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. While $\mathcal{O}_L$ is known to be maximal among the rings satisfying our requirements, the same is not true about $\mathcal{L}$. The ring $\mathbb{H}_{\mathcal{H}}$ also has an extension of the prescribed type inside $\mathbf{H}$, called the ring of *Hurwitz' integers of* $\mathbf{H}$. This ring, denoted by

$$\mathcal{H} = \rho\mathcal{G} \oplus \rho\xi\mathcal{G} \oplus j\mathcal{G} \oplus j\xi\mathcal{G},$$

is the right $\mathcal{G}$-module generated by the basis $\mathcal{B}_{Hur} = \{\rho, \rho\xi, j, j\xi\}$, where again $\rho = (1 + i + j + k)/2$. The fact that $\mathcal{H}$ is a subring can easily be verified by straightforward computations, e.g. $\xi\rho = \rho\xi - j\xi$. For future use we express the ring $\mathcal{H}$ in terms of the basis $\mathcal{B}_H$ of Proposition 2.1. It is not difficult to see that the element

$$q = c_1 + \xi c_2 + jc_3 + j\xi c_4 \in \mathbf{H}$$

is an element of $\mathcal{H}$, if and only if the coefficients c_t satisfy the requirements $(1 + i)c_t \in \mathcal{G}$ for all $t = 1, 2, 3, 4$ and $c_1 + c_3, c_2 + c_4 \in \mathcal{G}$. As the ideal generated by $1 + i$ has index two in $\mathcal{G}$, we see that $\mathcal{L}$ is an additive, index four subgroup in $\mathcal{H}$. We summarize these findings in Proposition 2.2. The bound on the minimum determinant is a consequence of the fact that all the elements of $\mathcal{G}$ have a norm at least one.

Proposition 2.2 *The following rings of matrices form ST lattices with minimum determinant equal to one.*

$$L_1 = \{M_L(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \mathcal{G}\},$$

$$L_2 = \{M(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \mathcal{G}\},$$

$$L_3 = \{M(c_1, c_2, c_3, c_4) \mid c_1, c_2, c_3, c_4 \in \frac{1+i}{2}\mathcal{G},\ c_1 + c_3 \in \mathcal{G}, c_2 + c_4 \in \mathcal{G}\}.$$

■

Remark 2.1 *The lattice L_1 is quite similar to the DAST lattice in the sense that all of its matrices can be simultaneously diagonalized. See more details in Section 4.2. The lattice L_2, for its part, is a more developed case from the so-called quasi-orthogonal STBC suggested e.g. in [29]. The matrix $M(c_1, c_2, c_3, c_4)$ of Proposition 2.1 can also be found as an example in the landmark paper [6], but no optimization has been done there by using, for example, ideals as we shall do here.*

A drawback shared by the lattices L_1 and L_2 is that in the ambient space of the transmitter they are isometric to the rectangular lattice $\mathbb{Z}^8$. The rectangular shape does carry the advantage that the sets of information carrying coefficients of the basis matrices are simple and all identical which is useful in e.g. sphere decoding. But, on the other hand, this shape is very wasteful in terms of transmission power. Geometrically denser sublattices of $\mathbb{Z}^8$, e.g. the checkerboard lattice

$$D_8 = \left\{ (x_1, ..., x_8) \in \mathbb{Z}^8 \;\middle|\; \sum_{i=1}^{8} x_i \equiv 0 \pmod 2 \right\}$$

and the diamond lattice

$$E_8 = \left\{ (x_1, ..., x_8) \in \mathbb{Z}^8 \;\middle|\; x_i \equiv x_j \pmod 2,\ \sum_{i=1}^{8} x_i \equiv 0 \pmod 4 \right\},$$

are well-known (cf. e.g. [30]). However, we must be careful in picking the copies of the sublattices, as it is the minimum determinant we want to keep an eye on (see Remark 2.3).

2.2 Dense sublattices inside the base lattice L_2

As our earlier simulations [3],[4] have shown that L_2 outperforms L_1, we concentrate on finding good sublattices of L_2. The units of the ring L_2 are exactly the non-zero matrices whose determinants have the minimal absolute value of one. Thus a natural way to find a sublattice with a better minimum determinant is to take the lattice $\phi(\mathcal{I})$, where $\mathcal{I} \subset S$ is a proper ideal. This idea has appeared at least in [3], [4], and [8]. Even earlier, ideals of rings of algebraic integers were used in [26] to produce dense lattices. Let us first record the following simple fact.

Lemma 2.3 *Let A and B be diagonalizable complex square matrices of the same size. Assume that they commute and that their eigenvalues are all real and non-negative. Then*

$$\det(A+B) \geq \det A + \det B$$

with a strict inequality if both A and B are invertible.

Proof. As A and B commute, they can be simultaneously diagonalized. Hence, we can reduce the claim to the case of diagonal matrices with non-negative real entries. In that case the claim is obvious. ∎

In Proposition 2.4 we give a construction isometric to the checkerboard lattice D_8

Proposition 2.4 *Let $\mathcal{I}$ be the prime ideal of the ring $\mathcal{G}$ generated by $1+i$. Define*

$$\mathcal{I}_{\mathcal{L}} = \{(c_1+\xi c_2)+j(c_3+\xi c_4) \in \mathcal{L} \mid c_1+c_2+c_3+c_4 \in \mathcal{I}\}.$$

Then $\mathcal{I}_{\mathcal{L}}$ is an ideal of index two in $\mathcal{L}$. The corresponding lattice

$$L_4 = \{M(c_1,c_2,c_3,c_4) \in L_2 \mid c_1+c_2+c_3+c_4 \in \mathcal{I}\}$$

is an index 2 sublattice in L_2. Furthermore, the absolute value of $\det(MM^H)$, $M \in L_4 \setminus \{0\}$, is then at least 4.

Proof. It is straightforward to check that $\mathcal{I}_{\mathcal{L}}$ is stable under (left or right) multiplication with the quaternions ξ and j, so $\mathcal{I}_{\mathcal{L}}$ is an ideal in $\mathcal{L}$.

Let us consider a matrix $M \in L_4$ and write it in the block form

$$M = \begin{pmatrix} A & -B^H \\ B & A^H \end{pmatrix}.$$

We see that

$$MM^H = \begin{pmatrix} AA^H+BB^H & 0 \\ 0 & AA^H+BB^H \end{pmatrix},$$

and

$$AA^H+BB^H = \begin{pmatrix} \alpha & k^* \\ k & \alpha \end{pmatrix},$$

where $\alpha = \sum_{j=1}^4 |c_j|^2$ is a non-negative integer and $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$ is a Gaussian integer with the property $k^* = ik$. We are to prove that $\det MM^H = (\alpha^2 - |k|^2)^2 \geq 4$. Assume first that $c_3 = c_4 = 0$, i.e. the block $B = 0$. Then $\det(A)$ is the relative norm

$$\det(A) = N_{\mathbb{Q}(i)}^{\mathbb{Q}(\xi)}(c_1+\xi c_2),$$

which is a Gaussian integer. As $c_1+\xi c_2$ is a non-zero element of the ideal $\mathcal{I}$, we conclude that $\det(A)$ is a non-zero non-unit. Therefore $\det(A)\det(A^H) \geq 2$, and the claim follows.

Let us then assume that both A and B are non-zero. Then $\det(A)$ and $\det(B)$ are non-zero Gaussian integers and have a norm at least one. The matrices A, A^H, B, and B^H all commute, so by Lemma 2.3 we get

$$\det(MM^H) > \det(AA^H)^2 + \det(BB^H)^2 \geq 2.$$

As $\det(MM^H) = (\alpha^2 - |k|^2)^2$ is a square of a rational integer, it must be at least 4. ∎

Remark 2.2 *It is easy to see that in the previous proposition $a + bi \in \mathcal{I}$, if and only if $a+b$ is an even integer. Thus geometrically the matrix lattice L_4 is, indeed, isometric to D_8.*

We proceed to describe two more interesting sublattices of L_2 with even better minimum determinants. To that end we use the ring $\mathcal{H}$ (or the lattice L_3). The first sublattice is isometric to the direct sum $D_4 \perp D_4$ [30] of two 4-dimensional checkerboard lattices.

Proposition 2.5 *Let again $\mathcal{I}$ be the ideal $(1+i)\mathcal{G}$. The lattice*

$$L_5 = \{M(c_1, c_2, c_3, c_4) \in L_2 \mid c_1 + c_3, c_2 + c_4 \in \mathcal{I}\}$$

has a minimum determinant equal to 16. The index of L_4 in L_2 is 4.

Proof. The coefficients c_1 and c_3 can be chosen arbitralily within $\mathcal{G}$. The the ideal $\mathcal{I}$ has index 2 in $\mathcal{G}$, and the coefficients c_2 and c_4 now must belong to the cosets $c_1 + \mathcal{I}$ and $c_3 + \mathcal{I}$ respectively. Whence, the index of L_5 in L_2 is 4. The matrices A in the lattice L_5 are of the form $A = (1+i)M$, where M is a matrix in the lattice L_3 of Proposition 2.2. Thus $\det(AA^H) = 16\det(MM^H)$ and the claim follows from Proposition 2.2. ∎

The diamond lattice E_8 can be described in terms of the Gaussian integers as (cf. [31])

$$E_8 = \frac{1}{1+i}\{(c_1, c_2, c_3, c_4) \in \mathcal{G}^4 \mid c_1 + \mathcal{I} = c_t + \mathcal{I},\ t = 2, 3, 4,\ \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}.$$

By our identification of quadruples $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ and the elements of $\mathbf{H}$ it is straightforward to verify that $(1+i)E_8$ has $\{2, (1+i)+(1+i)\xi, (1+i)\xi+(1+i)j, 1+\xi+j+j\xi\} \subseteq \mathcal{L}$ as a $\mathcal{G}$-basis, whence the set $\{1+i, 1+\xi, \xi+j, \rho+\rho\xi\} \subseteq \mathcal{H}$ is a $\mathcal{G}$-basis for E_8. By another simple computation we see that $E_8 = \mathcal{H}(1+\xi)$, i.e. E_8 is the left ideal of the ring $\mathcal{H}$ generated by $1+\xi$.

Table 1: Lattices from a coding theoretical point of view

$L_2 \leftrightarrow$ The 8-dimensional rectangular grid $\mathbb{Z}^8$
$\leftrightarrow$ no coding
$\downarrow$
$L_4 \leftrightarrow$ The checkerboard lattice D_8
$\leftrightarrow$ overall parity check code of length 8
$\downarrow$
$L_5 \leftrightarrow$ The lattice $D_4 \perp D_4$
$\leftrightarrow$ two blocks of the overall parity check code of length 4
$\downarrow$
$L_6 \leftrightarrow$ The diamond lattice E_8
$\leftrightarrow$ extended Hamming-code of length 8

Proposition 2.6 *The lattice*

$$L_6 = \{M(c_1, c_2, c_3, c_4) \in L_2 \mid c_1 + \mathcal{I} = c_t + \mathcal{I},\ t = 2, 3, 4,\ \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}$$

is an index 16 sublattice of L_2. Furthermore, the minimum determinant of L_6 is 64.

Proof. Let $M_I = M(1, 1, 0, 0)$ be the matrix $\phi(1 + \xi)$ under the isomorphism of Proposition 2.1. We see that $\det(M_I M_I^H) = 4$. By the preceding discussion any matrix A of the lattice L_6 has the form $A = MM_I(1 + i)$, where M is a matrix in L_3. As in the proof of Proposition 2.5, we see that $\det AA^H = 16 \det(M_I M_I^H) \det(MM^H)$. The claim on the minimum determinant now follows from Proposition 2.2. We see that the coefficient c_1 can be chosen arbitrarily within $\mathcal{G}$. The coefficients c_2 and c_3 then must belong to the coset $c_1 + \mathcal{I}$, and c_4 must be chosen such that $c_1 + c_2 + c_3 + c_4 \in 2\mathcal{G} = \mathcal{I}^2$. As $\mathcal{I}$ has index two in $\mathcal{G}$, we see that the index of L_6 in L_2 is 16 as claimed. ∎

Remark 2.3 *We have now produced a nested sequence of lattices*

$$2\mathbb{Z}^8 = 2L_2 \subseteq L_6 \subseteq L_5 \subseteq L_4 \subseteq L_2 = \mathbb{Z}^8 (\subseteq L_3). \tag{1}$$

We concentrate on the lattices that are sandwiched between $2\mathbb{Z}^8$ and $\mathbb{Z}^8$. It is worthwhile to note that these lattices are in a bijective correspondence with a binary linear code of length 8 by projection modulo 2, see Table 1 above. As it happens, within this sequence of lattices the minimum Hamming distance of the binary linear code and the minimum determinant of the lattice are somewhat related.

Thereupon it is natural to ask that what if we simply concatenate the use of L_2 with a good binary code (extended over several L_2-blocks, if needed), and be done with it. While the binary linear codes appearing above are the first ones that come to one's mind, we want to caution the unwary end-user. Namely, it is possible that there are high weight units in the ring in question. If such binary words are included, then the minimum determinant of the corresponding lattice is equal to 1, i.e. no coding gain will take place. E.g. the unit $(1-\xi^3)/(1-\xi) = 1+\xi+\xi^2 = (1+i)+\xi$ of the ring $\mathcal{L}$ corresponds to the matrix $M(1+i,1,0,0)$ of determinant 1, and thus we must not allow such words of weight 3. If the lattice L_1 were used, the situation would be even worse, as then we have units like $(1-\zeta^7)/(1-\zeta)$ in the ring $\mathcal{O}_L$ that would be mapped to a word of Hamming weight 7. A construction based on ideals provides a mechanism to avoid this problem caused by high weight units.

3 Cyclic algebras and orders

In Section 2 we produced a nested sequence (1) of quaternionic lattices with the property that as the lattice gets denser after rescaling the increased minimum determinant back to one, the BLER perfomance gets better. As the sequence (1) lies within a specific division algebra, an obvious question evokes how to generalize this idea. The theory of cyclic division algebras and their maximal orders offer us an answer. When designing square ST matrix lattices for MIMO use, cyclic division algebras are of utmost interest as it has been shown in [14] that a non-vanishing determinant is a sufficient condition for full-rate CDA based STBC-designs to achieve the upper bound on the optimal D-MG tradeoff, hence proving that the upper bound itself is the optimal DM-G tradeoff for any number of transmitters and receivers. Given the number of transmitters n, we pick a suitable cyclic division algebra of index n (more on this in a forthcoming paper, see Section 6. See also [14]). The matrix representation of the algebra, with some constraints on the elements, will then correspond to the base lattice, similarly as did the lattice L_2 in Section 2. Now in order to make the lattice denser, we choose the elements in the matrices from an order. The natural first choice for an order is the one corresponding to the ring of algebraic integers of the maximal subfield inside the algebra. The densest possible sublattice is the one where the elements come from a maximal order.

All algebras considered here are finite dimensional associative algebras over a field.

3.1 Cyclic algebras

The basic theory of cyclic algebras and their representations as matrices are thoroughly considered in [[32], Chapter 8.5] and [6]. We are only going to recapitulate

the essential facts here.

In the following, we consider number field extensions E/F, where F denotes the base field. F^* (resp. E^*) denotes the set of non-zero elements of F (resp. E). Let E/F be a cyclic field extension of degree n with the Galois group $Gal(E/F) = \langle\sigma\rangle$, where σ is the generator of the cyclic group. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of *index* n, that is,

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

with $u \in \mathcal{A}$ such that $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in F^*$. An element $a = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix

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

Let us compute the third column as an example:

$$\begin{aligned} u^2 \mapsto au^2 &= x_0u^2 + ux_1u^2 + \cdots + u^{n-1}x_{n-1}u^2 \\ &= u\sigma(x_0)u + u^2\sigma(x_1)u + \cdots + \gamma\sigma(x_{n-1})u \\ &= u^2\sigma^2(x_0) + u^3\sigma^2(x_1) + \cdots + u\gamma\sigma^2(x_{n-1}), \end{aligned}$$

and hence as the third column we get the vector

$$(\gamma\sigma^2(x_{n-2}), \gamma\sigma^2(x_{n-1}), \sigma^2(x_0), \ldots, \sigma^2(x_{n-3}))^T.$$

Let us denote the ring of algebraic integers of E by $\mathcal{O}_E$. A basic, rate-n MIMO STBC $\mathcal{C}$ is usually defined as

$$\mathcal{C} = \left\{ \left(\begin{array}{cccc} x_0 & \gamma\sigma(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \cdots & \sigma^{n-1}(x_0) \end{array} \right) \middle| \, x_i \in \mathcal{O}_E \right\}. \tag{3}$$

Further optimization might be carried out by using e.g. ideals. If we denote the basis of E over $\mathcal{O}_F$ by $\{1, e_1, ..., e_{n-1}\}$, then the elements $x_i,\ i = 0, ..., n-1$ in (3) take the form $x_i = \sum_{k=0}^{n-1} f_k e_k$, where $f_k \in \mathcal{O}_F$ for all $k = 0, ..., n-1$. Hence n complex symbols are transmitted per channel use, i.e. the design has rate n. In literature this is often referred to as having a *full rate*.

Definition 3.1 *An algebra $\mathcal{A}$ is called simple if it has no nontrivial ideals. An F-algebra $\mathcal{A}$ is central if its center $Z(A) = \{a \in \mathcal{A} | aa' = a'a\ \forall a' \in \mathcal{A}\} = F$.*

Definition 3.2 *An ideal $\mathcal{I}$ is called nilpotent if $\mathcal{I}^k = 0$ for some $k \in \mathbb{Z}_+$. An algebra $\mathcal{A}$ is semisimple if it has no nontrivial nilpotent ideals. Any finite dimensional semisimple algebra over a field is a finite and unique direct sum of simple algebras.*

Definition 3.3 *The determinant (resp. trace) of the matrix A is called the reduced norm (resp. reduced trace) of an element $a \in \mathcal{A}$ and is denoted by $nr(a)$ (resp. $tr(a)$).*

Remark 3.1 *The connection with the usual norm map $N_{A/F}(a)$ (resp. trace map $T_{A/F}(a)$) and the reduced norm $nr(a)$ (resp. reduced trace $tr(a)$) of an element $a \in \mathcal{A}$ is $N_{A/F}(a) = (nr(a))^n$ (resp. $T_{A/F}(a) = ntr(a)$), where n is the degree of E/F.*

In Section 2 we have attested that the algebra **H** is a division algebra. The next old result due to A. A. Albert [[33], Chapter V.9] provides us with a condition for when an algebra is indeed a division algebra.

Proposition 3.1 *The algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of index 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 in E^*, is n.* ■

3.2 Orders

We are now ready to present some of the basic definitions and results from the theory of maximal orders. The general theory of maximal orders can be found in [34].

Let S denote a Noetherian integral domain with a quotient field F, and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 3.4 *An S-order in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over S and generates $\mathcal{A}$ as a linear space over F.*

As usual, an S-order in $\mathcal{A}$ is said to be *maximal*, if it is not properly contained in any other S-order in $\mathcal{A}$. If the integral closure $\overline{S}$ of S in $\mathcal{A}$ happens to be an S-order in $\mathcal{A}$, then $\overline{S}$ is automatically the unique maximal S-order in $\mathcal{A}$.

Let us illustrate the above definition by the following example.

Example 3.1 *(a) Orders always exist: If M is a full S-lattice in $\mathcal{A}$, i.e. $FM = \mathcal{A}$, then the left order of M defined as*

$$\mathcal{O}_l(M) = \{x \in \mathcal{A} \mid xM \subseteq M\}$$

is an S-order in $\mathcal{A}$. The right order is defined in an analogous way.

(b) If $\mathcal{A} = \mathcal{M}_n(F)$, the algebra of all $n \times n$ matrices over F, then $\Lambda = \mathcal{M}_n(S)$ is an S-order in $\mathcal{A}$.

(c) Let $a \in \mathcal{A}$ be integral over S, that is, a is a zero of a monic polynomial over S. Then the ring $S[a]$ is an S-order in the F-algebra $F[a]$.

(d) Let S be a Dedekind domain, and let E be a finite separable extension of F. Denote by $\overline{S}$ the integral closure of S in E. Then $\overline{S}$ is an S-order in E. In particular, taking $S = \mathbb{Z}$, we see that the ring of algebraic integers of E is a $\mathbb{Z}$-order in E.

Hereafter, F will be an algebraic number field and S a Dedekind ring with F as a field of fractions.

Proposition 3.2 *Let $\mathcal{A}$ be a finite dimensional semisimple algebra over F and Λ be a $\mathbb{Z}$-order in $\mathcal{A}$. Let $\mathcal{O}_F$ stand for the ring of algebraic integers of F. Then $\Gamma = \mathcal{O}_F\Lambda$ is an $\mathcal{O}_F$-order containing Λ. As a consequence, a maximal $\mathbb{Z}$-order in $\mathcal{A}$ is a maximal $\mathcal{O}_F$-order as well.* ■

The following proposition provides us with a useful tool for finding a maximal order within a given algebra.

Proposition 3.3 *Let Λ be an S-order in $\mathcal{A}$. For each $a \in \Lambda$ we have $nr(a) \in S$ and $tr(a) \in S$.* ■

Proposition 3.4 *Let Γ be a subring of $\mathcal{A}$ containing S, such that $F\Gamma = \mathcal{A}$, and suppose that each $a \in \Gamma$ is integral over S. Then Γ is an S-order in $\mathcal{A}$. Conversely, every S-order in $\mathcal{A}$ has these properties.* ■

Corollary 3.5 *Every S-order in $\mathcal{A}$ is contained in a maximal S-order in $\mathcal{A}$. There exists at least one maximal S-order in $\mathcal{A}$.* ■

Remark 3.2 *As the previous corollary indicates, a maximal order of an algebra is not necessarily unique.*

Remark 3.3 *The algebra $\mathbf{H}$ can also be viewed as a cyclic division algebra. As it is a subring of the Hamiltonian quaternions, its center consists of the intersection $\mathbf{H} \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$. Also $\mathbb{Q}(\xi)$ is an example of a splitting field of $\mathbf{H}$. In the notation above we have an obvious isomorphism*

$$\mathbf{H} \simeq (\mathbb{Q}(\xi)/\mathbb{Q}(\sqrt{2}), \sigma, -1),$$

where σ is the usual complex conjugation.

Remark 3.4 *In principle, the lattices from Section 2 could also be used as MIMO codes, but when we pack $\mathbf{H}$ in the form of (2), $\delta_{\mathcal{C}}$ becomes vanishing and the DM-G tradeoff cannot be achieved.*

One extremely well-performing CDA based code taking advantage of a maximal order is the celebrated *Golden code* [8] treated in the following example.

Example 3.2 *In any cyclic algebra where the element γ happens to be an algebraic integer, we have the following natural order*

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

where $\mathcal{O}_E$ is the ring of integers of the field E. We note that $\mathcal{O}_E$ is the unique maximal order in E. In the so-called Golden Division Algebra (GDA) [8], i.e. the cyclic algebra $(E/F, \sigma, \gamma)$ gotten from the data $E = \mathbb{Q}(i, \sqrt{5})$, $F = \mathbb{Q}(i)$, $\gamma = i$, $n = 2$, $\sigma(\sqrt{5}) = -\sqrt{5}$, the natural order Λ is already maximal [35]. The ring of algebraic integers $\mathcal{O}_E = \mathbb{Z}[i][\theta]$, when we denote the golden ratio by $\theta = \frac{1+\sqrt{5}}{2}$. The authors of [8] further optimize the code by using an ideal $(\alpha) = (1 + i - i\theta)$, and the Golden code is then defind as

$$\mathcal{GC} = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & i\sigma(\alpha)\sigma(x_1) \\ \alpha x_1 & \sigma(\alpha)\sigma(x_0) \end{pmatrix} \;\middle|\; x_0, x_1 \in \mathcal{O}_E \right\}. \tag{4}$$

The Golden code achieves the DM-G tradeoff as the element $\gamma = i$ is not in the image of the norm map. For the proof, see [8].

Remark 3.5 *We feel that in [8], the usage of a maximal order is just a coincidence, as in this case it coincides with the natural order which is generally used in ST code designs (cf. (3)). At least the authors do not mention maximal orders. As far as we know, above our construction there does not exist any designs using a maximal order other than the natural one.*

Next we prove that the lattice L_6 is optimal within the cyclic division algebra $\mathbf{H}$ in the sense that the diamond lattice $E_8 = \mathcal{H}(1 + \xi)$ corresponds to a proper ideal of a maximal order in $\mathbf{H}$.

Proposition 3.6 *The ring*

$$\mathcal{H} = \{q = c_1 + \xi c_2 + jc_3 + j\xi c_4 \in \mathbf{H} \mid c_1, \ldots, c_4 \in \mathbb{Q}(i),$$

$$(1 + i)c_t \in \mathcal{G}\ \forall t, c_1 + c_3, c_2 + c_4 \in \mathcal{G}\}$$

is a maximal $\mathbb{Z}$-order of the division algebra $\mathbf{H}$.

Proof. Clearly the $\mathbb{Q}$-span of $\mathcal{H}$ is the whole algebra $\mathbf{H}$, and we have seen that $\mathcal{H}$ is a ring, so it is an order of $\mathbf{H}$. Furthermore, if Λ is any order of $\mathbf{H}$, then so is $\Lambda[\sqrt{2}] = \Lambda \cdot \mathbb{Z}[\sqrt{2}]$, as the element $\sqrt{2}$ is in the center of $\mathbf{H}$ (cf. Proposition 3.2). Therefore it suffices to show that $\mathcal{H}$ is a maximal $\mathbb{Z}[\sqrt{2}]$-order. In what follows, we will call rational numbers in the coset $(1/2) + \mathbb{Z}$ half-integers. Assume for

contradiction that we could extend the order $\mathcal{H}$ into a larger order $\Gamma = \mathcal{H}[q]$ by adjoining the quaternion $q = a_1 + a_2 j$, where the coefficients

$$a_t = m_{t,0} + m_{t,1}\xi + m_{t,2}\xi^2 + m_{t,3}\xi^3, \quad m_{t,\ell} \in \mathbb{Q} \text{ for all } t, \ell$$

are elements of the field $\mathbb{Q}(\xi)$. As $\xi - \xi^3 = \sqrt{2}$, and $\xi^* = -\xi^3$, we see that

$$tr(q) = a_1 + a_1^* = 2m_{1,0} + \sqrt{2}(m_{1,1} - m_{1,3}).$$

By Proposition 3.3 this must be an element of $\mathbb{Z}[\sqrt{2}]$, so we may conclude that $m_{1,0}$ must be an integer or a half-integer, and that $m_{1,1} - m_{1,3}$ must be an integer. Similarly

$$tr(q\xi) = -2m_{1,3} + \sqrt{2}(m_{1,0} - m_{1,2})$$

must be an element of $\mathbb{Z}[\sqrt{2}]$. We may thus conclude that all the coefficients $m_{1,\ell},\ \ell = 0, 1, 2, 3$ are integers or half-integers, and that the pairs $m_{1,0}, m_{1,2}$ (resp. $m_{1,1}, m_{1,3}$) must be of the same type, i.e. either both are integers or both are half-integers. A similar study of $tr(qj)$ and $tr(qj\xi)$ shows that the same conclusions also hold for the coefficients $m_{2,\ell},\ \ell = 0, 1, 2, 3$. Because $\mathbb{Z}[\xi] \subseteq \mathcal{H}$, replacing q with any quaternion of the form $q - \omega$, where $\omega \in \mathbb{Z}[\xi]$ will not change the resulting order Γ. Thus we may assume that the coefficients $m_{1,\ell},\ \ell = 0, 1, 2, 3$ all belong to the set $\{0, 1/2\}$. Similarly, if needed, replacing q with $q - \omega' j$ for some $\omega' \in \mathbb{Z}[\xi]$ allows us to assume that the coefficients $m_{2,\ell},\ \ell = 0, 1, 2, 3$ also all belong to the set $\{0, 1/2\}$. Further replacements of q by $q - \rho$ or $q - \rho\xi$ then permit us to restrict ourselves to the case $m_{2,\ell} = 0$, for all $\ell = 0, 1, 2, 3$. If we are to get a proper extension of $\mathcal{H}$, we are left with the cases $q = (1 + i)/2$, $q = \xi(1 + i)/2$ and $q = (1 + \xi)(1 + i)/2$. We immediately see that none of these have reduced norms in $\mathbb{Z}[\sqrt{2}]$, so we have arrived at a contradiction. ■

4 Decoding of the nested sequence of lattices

In this section, let us consider the coherent MIMO case where the receiver perfectly knows the channel coefficients. The received signal is

$$\mathbf{y} = B\mathbf{x} + \mathbf{n},$$

where $\mathbf{x} \in \mathbb{R}^m$, $\mathbf{y},\ \mathbf{n} \in \mathbb{R}^n$ denote the channel input, output and noise signals, and $B \in \mathbb{R}^{n \times m}$ is the Rayleigh fading channel response. The components of the noise vector $\mathbf{n}$ are i.i.d. complex Gaussian random variables. In the special case of a MISO channel ($n = 1$), the channel matrix takes a form of a vector $B = \mathbf{h} \in \mathbb{R}^m$ (cf. Section 1).

The information vectors to be encoded into our code matrices are taken from the pulse amplitude modulation (PAM) signal set $\mathcal{X}$ of the size Q, i.e.,

$$\mathcal{X} = \{u = 2q - Q + 1 \ \mid \ q \in \mathbb{Z}_Q\}$$

with $\mathbb{Z}_Q = \{0, 1, ..., Q-1\}$.

Under this assumption, the optimal detector $g : \mathbf{y} \mapsto \hat{\mathbf{x}} \in \mathcal{X}^m$ that minimizes the average error probability

$$P(e) \stackrel{\Delta}{=} P(\hat{\mathbf{x}} \neq \mathbf{x})$$

is the maximum-likelihood (ML) detector given by

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x} \in \mathbb{Z}_Q^m} \mid \mathbf{y} - \mathbf{B}\mathbf{x} \mid^2, \tag{5}$$

where the components of the noise $\mathbf{n}$ have a common variance equal to one.

4.1 Code controlled sphere decoding

The search in (5) for the *closest lattice point* to a given point $\mathbf{y}$ is known to be NP-hard in the general case where the lattice does not exhibit any particular structure. In [36], however, Pohst proposed an efficient strategy of enumerating all the lattice points within a sphere $\mathcal{S}(\mathbf{y}, \sqrt{C_0})$ centered at $\mathbf{y}$ with a certain radius $\sqrt{C_0}$ that works for lattices of a moderate dimension. For background, see [37]-[40]. For finite PAM signals sphere decoders can also be visualized as a *bounded search* in a tree.

The complexity of sphere decoders critically depends on the preprocessing stage, the ordering in which the components are considered, and the initial choice of the sphere radius. We shall use the standard preprocessing and ordering that consists of the *Gram-Schmidt orthonormalization*

$$B = (Q, Q') \begin{pmatrix} R \\ 0 \end{pmatrix}$$

of the columns of the channel matrix B (equivalently, QR *decomposition* on B) and the natural back-substitution component ordering given by $x_m, ..., x_1$. The matrix R is an $m \times m$ upper triangular matrix with positive diagonal elements, Q (resp. Q') is an $n \times m$ (resp. $n \times (n-m)$) unitary matrix, and 0 is an $(n-m) \times m$ zero matrix.

The condition $B\mathbf{x} \in \mathcal{S}(\mathbf{y}, \sqrt{C_0})$ can be written as

$$\mid \mathbf{y} - B\mathbf{x} \mid^2 \leq C_0 \tag{6}$$

which after applying the QR decomposition on B takes the form

$$\mid \mathbf{y}' - R\mathbf{x} \mid^2 \leq C_0', \tag{7}$$

where $\mathbf{y}' = Q^T\mathbf{y}$ and $C_0' = C_0 - |(Q')^T\mathbf{y}|^2$. Due to the upper triangular form of R, (7) implies the set of conditions

$$\sum_{j=i}^{m} \left| y_j' - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \right|^2 \leq C_0', \quad i = 1, ..., m. \tag{8}$$

The sphere decoding algorithm outputs the point $\hat{\mathbf{x}}$ for which the distance

$$d^2(\mathbf{y}, B\mathbf{x}) = \sum_{j=1}^{m} \Big| y'_j - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \Big|^2 \tag{9}$$

is minimum. See details in [40].

The decoding of the base lattice L_2 can be performed by using the algorithm below proposed in [40].

Algorithm II, Smart Implementation (Input $C'_0,\ \mathbf{y}',\ R$. Output $\hat{\mathbf{x}}$.)

STEP 1: (Initialization) Set $i := m,\ T_m := 0,\ \xi_m := 0$, and $d_c := C'_0$ (current sphere squared radius).

STEP 2: (DFE on x_i) Set $x_i := \lfloor (y'_i - \xi_i)/r_{i,i} \rceil$ and $\Delta_i := sign(y'_i - \xi_i - r_{i,i}x_i)$.

STEP 3: (Main step) If $d_c < T_i + \mid y'_i - \xi_i - r_{i,i}x_i \mid^2$, then go to STEP 4 (i.e., we are outside the sphere).

Else if $x_i \notin \mathbb{Z}_Q$ go to STEP 6 (i.e., we are inside the sphere but outside the signal set boundaries).

Else (i.e., we are inside the sphere and signal set boundaries) if $i > 1$, then {let $\xi_{i-1} := \sum_{j=i}^{m} r_{i-1,j}x_j, \quad T_{i-1} := T_i + \mid y'_i - \xi_i - r_{i,i}x_i \mid^2, \quad i := i - 1$, and go to STEP 2}.

Else (i=1) go to STEP 5.

STEP 4: If $i = m$, terminate, else set $i := i + 1$ and go to STEP 6.

STEP 5: (A valid point is found) Let $d_c := T_1 + \mid y'_1 - \xi_1 - r_{1,1}x_1 \mid^2$, save $\hat{\mathbf{x}} := \mathbf{x}$. Then, let $i := i + 1$ and go to STEP 6.

STEP 6: (Schnorr-Euchner enumeration of level i) Let $x_i := x_i + \Delta_i,\ \Delta_i := -\Delta_i - sign(\Delta_i)$, and go to STEP 3.

Note that given the values $x_{i+1}, ..., x_m$, taking the ZF-DFE (zero-forcing decision-feedback equalization) on x_i avoids retesting other nodes at level i in case we fall outside the sphere. Setting $d_c = \infty$ would ensure that the first point found by the algorithm is the ZF-DFE point (or the Babai point) [40]. However, if the distance between the ZF-DFE point and the received signal is very large this choice may cause some inefficiency, especially for high dimensional lattices.

The decoding of the other three lattices in (1) also relies on this algorithm, but we need to run some additional parity checks. This simply means that in addition to the checks concerning the facts that we have to be both inside the sphere radius and inside the signal set boundaries, we also have to lie inside a given sublattice. This will be taken care of by a method we call *code controlled sphere decoding* (CCSD), that combines the algorithm above with certain case considerations. To this end, let us write the constraints on the elements c_i as *modulo* 2

Table 2: CCSD: Additional case considerations

CASE L_4	$\sum_{i=1}^{8} x_i \equiv 0 \pmod 2$
CASE L_5	$x_1 + x_2 \equiv x_5 + x_6$, $x_3 + x_4 \equiv x_7 + x_8 \pmod 2$
CASE L_6	$x_1 + x_2 \equiv x_3 + x_4 \equiv x_5 + x_6 \equiv x_7 + x_8$, $\sum_{2\mid i} x_i \equiv \sum_{2\nmid i} x_i \equiv 0 \pmod 2$

operations. Denote by $\mathbf{x} = (x_1, x_2, ..., x_8) = (\Re c_1, \Im c_1, ..., \Re c_4, \Im c_4) \in \mathbb{R}^8$ the real vector corresponding to the channel input. Note that when exploiting these relations in the CCSD algorithm, we have to use different orderings for the basis matrices of the lattice in different cases in order to make the parity checks as simple as possible. Let us first order the basis matrices as $B_1 = M(1,0,0,0), B_2 = M(i,0,0,0), ..., B_7 = M(0,0,0,1), B_8 = M(0,0,0,i)$. Then when decoding e.g. the L_5 lattice, we reorder the basis matrices as $B_1, B_2, B_5, B_6, B_3, B_4, B_7, B_8$ in order to get the sum c_1+c_3 as the sum of the first 4 components and the sum c_2+c_4 as the sum of the last 4 components (cf. Proposition 2.5). The conditions for the Gaussian elements of Propositions 2.4-2.6 can clearly be translated into the following modulo 2 integer conditions, see for instance Remark 2.2. The additional parity check steps will hence be as shown in Table 2 above.

As the Alamouti scheme [2] has a very efficient decoding algorithm available, and our quaternionic lattices have an Alamouti-like block structure, it is natural to ask whether any of the benefits of Alamouti decoding will survive for our lattices. We shall see that the block structure allows us to decode the two blocks independently from each other. The following simple observation is the underlying geometric reason for our ability to do this.

Lemma 4.1 *Let A and B be two $n \times n$ matrices with the property that the matrices A, B, A^H, B^H commute. Let $\mathbf{h} \in \mathbb{C}^{2n}$ be any (row) vector and write*

$$M(A,B) = \begin{pmatrix} A & B \\ -B^H & A^H \end{pmatrix}.$$

Then the vectors $\mathbf{h}M(A,0)$ and $\mathbf{h}M(0,B)$ are orthogonal to each other when we identify $\mathbb{C}^{2n}$ with $\mathbb{R}^{4n}$ and use the usual inner product of a vector space over the real numbers.

Proof. With the identification $\mathbb{C}^{2n} = \mathbb{R}^{4n}$ the real inner product is the real part of the hermitian inner product $\langle\ ,\ \rangle$ of $\mathbb{C}^{2n}$. Write the vector $\mathbf{h}$ in the block form $\mathbf{h} = (h^{(1)}, h^{(2)})$, where the blocks $h^{(j)}, j = 1, 2$, are (row) vectors in $\mathbb{C}^n$. Then we

can compute

$$\begin{aligned}\langle \mathbf{h}M(A,0), \mathbf{h}M(0,B)\rangle &= \langle \mathbf{h}M(A,0)M(0,B)^H, \mathbf{h}\rangle \\ &= \langle \mathbf{h}M(A,0)M(0,-B), \mathbf{h}\rangle \\ &= \langle \mathbf{h}M(0,-AB), \mathbf{h}\rangle \\ &= \langle h^{(2)}A^H B^H, h^{(1)}\rangle - \langle h^{(1)}AB, h^{(2)}\rangle.\end{aligned}$$

As $\langle \mathbf{u}M, \mathbf{v}\rangle = \langle \mathbf{v}M^H, \mathbf{u}\rangle^*$ for all vectors $\mathbf{u}, \mathbf{v}$ and matrices M, we see that the above hermitian inner product is pure imaginary. ■

Corollary 4.2 *Let A and B range over sets of $n \times n$-matrices. Let $\mathbf{h}$ and $\mathbf{r}$ be vectors in $\mathbb{C}^{2n}$. Then the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(A,B)$ is minimized for the $A = A_0$ and $B = B_0$, when A_0 minimizes the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(A,0)$ and B_0 minimizes the Euclidean distance between $\mathbf{r}$ and $\mathbf{h}M(0,B)$.*

Proof. Write V_A (resp. V_B) for the real vector space spanned by the vectors $\mathbf{h}M(A,0)$ (resp. $\mathbf{h}M(0,B)$). These subspaces are orthogonal to each other in the sense of Lemma 4.1. Whence we can uniquely write $\mathbf{r} = r_A + r_B + r_\perp$, where $r_A \in V_A, r_B \in V_B$ and $r_\perp$ is in the (real) orthogonal complement of the direct sum $V_A \oplus V_B$. A similar decomposition for the vector $\mathbf{h}M(A,B)$ is $\mathbf{h}M(A,B) = h_A + h_B$, where $h_A = \mathbf{h}M(A,0) \in V_A$ and $h_B = \mathbf{h}M(0,B) \in V_B$. By the Pythagorean theorem

$$|\mathbf{r} - \mathbf{h}M(A,B)|^2 = |r_A - \mathbf{h}M(A,0)|^2 + |r_B - \mathbf{h}M(0,B)|^2 + |r_\perp|^2.$$

Furthermore, here

$$|r_A - \mathbf{h}M(A,0)|^2 = |\mathbf{r} - \mathbf{h}M(A,0)|^2 - |r_B|^2 - |r_\perp|^2,$$

so the quantities $|r_A - \mathbf{h}M(A,0)|^2$ and $|\mathbf{r} - \mathbf{h}M(A,0)|^2$ are minimized for the same choice of the matrix A. A similar argument applies to the B-components, so the claim follows. ■

4.2 Complexity analysis and the notion of defect

The number of nodes in the search tree is used as a measure of complexity so that the implementation details or the physical environment do not affect it. We have analyzed many different kinds of situations concerning the change of complexity of the sphere decoder when moving in (1) from right to left.

In Fig. 1 we have plotted the average number of points visited by the algorithm in different cases at the rates approximately 4 and 8 bpcu. The SNR regions cover

the block error rates between $\approx 10\% - 0.01\%$. As can be seen, in the low SNR end, the difference in complexity between the different lattices is clear but evens out when the SNR increases. For the sublattices $L_4,\ L_5$, and L_6 the algorithm visits $1.1 - 2.1$ times as many points as for the base lattice L_2. In the larger SNR end, the performance is fairly similar for all the lattices. E.g. at 4 and 8 bpcu, when all the lattices reach the bound of maximum 20 points visited, the block error rates of $L_4,\ L_5$, and L_6 are still as big as $5\%,\ 2\%$, and 1% respectively.

Definition 4.1 *In a MISO setting we say that a matrix lattice L has defect r [4], if its rank is m, but the minimum positive real dimension of the span of $\mathbf{b}L$ is $m-r$. In other words, the lattice collapses by dimension r. What comes to the decoding complexity, a high defect means bad worst case decoding complexity.*

In Example 4.1 below we show that for certain non-zero choices of the channel vector the receiver's version of the four antenna DAST lattice (see [4],[5]) collapses into a dense set within a real vector space of dimension 2. Thus the 8-dimensional four antenna DAST lattices have defect six.

Example 4.1 *There exist 8-dimensional lattices [5] of 4×4 matrices of the form*

$$M_{DAST} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -x_2 & x_3 & -x_4 \\ x_1 & x_2 & -x_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{pmatrix}.$$

When $\mathbf{h} = (1,1,1,1)$, the receiver observes the vector lattice

$$\mathbf{h}M_{DAST} = (4x_1, 0, 0, 0),$$

so the image lattice is contained in a vector space of dimension at most 2.

We proceed to determine the defects of the lattices L_1 of Proposition 2.2 and the ones within the nested sequence (1). Let us first consider L_1. Let

$$U = \begin{pmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_4 \end{pmatrix}$$

be the 4×4 matrix with rows $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \mathbf{h}_4$ of the form $(1, \zeta^j, \zeta^{2j}, \zeta^{3j})$ for $j = 1, 5, 9, 13$. Recall that earlier we have used $\{1, \zeta, \zeta^2, \zeta^3\}$ as an integral basis, so the rows of U are the images of this ordered basis under the action of the Galois group G of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}(i)$. Now it happens that the matrix U is unitary (up to a constant factor) as $UU^* = 4I_4$. Let $z = c_1 + c_2\zeta + c_3\zeta^2 + c_4\zeta^3$ be an arbitrary algebraic integer of $\mathbb{Q}(\zeta)$, and $M(z) = M_L(c_1, c_2, c_3, c_4) \in L_1$ be the corresponding matrix of Proposition 2.2. According to the theory of algebraic

numbers (and also trivially verified by hand) the rows of U are (left) eigenvectors of $M(z)$, and

$$UM(z)U^{-1} = \begin{pmatrix} z & 0 & 0 & 0 \\ 0 & \sigma_2(z) & 0 & 0 \\ 0 & 0 & \sigma_3(z) & 0 \\ 0 & 0 & 0 & \sigma_4(z) \end{pmatrix}$$

is a diagonal matrix with entries gotten by applying the elements of the Galois group $G = \{\sigma_1 = id, \sigma_2, \sigma_3, \sigma_4\}$ to the number z.

So all the matrices $M_L(c_1, c_2, c_3, c_4)$ are diagonalized by U. Therefore we might call the lattice L_1 'DAST-like', as it shares this property with the lattices from [5].

Nevertheless, our ability to simultaneously diagonalize all the matrices in the lattice gives the following somewhat unwelcome result.

Proposition 4.3 *The lattice L_1 has defect six.*

Proof. Let $\mathbf{h} \in \mathbb{C}^4$ be any non-zero channel vector. Then obviously the vectors $\mathbf{h} = \mathbf{h}M_L(1,0,0,0)$ and $i\mathbf{h} = \mathbf{h}M_L(i,0,0,0)$ are linearly independent over the reals. Thus the real span of $\mathbf{h}L_1$ has dimension at least two, whence the defect cannot be higher than six.

On the other hand, let $\mathbf{h}$ be one of the common eigenvectors of all the matrices of the lattice, i.e. a scalar multiple of one of the rows of the matrix U above. Then $\mathbf{h}L_1$ consists of various (complex) scalar multiples of $\mathbf{h}$ and thus has real dimension exactly 2. ∎

In order to study the quaternionic lattices we first observe that the 2×2-matrices A and B appearing as blocks of a matrix $M \in L_2$ all have $(1, \pm\xi)$ as their common (left) eigenvectors. The same holds for the adjoints A^*, B^* as they also appear as blocks of M^* that also happens to belong to the lattice L_2. From the proof of Proposition 2.4 we see that the matrix MM^*, $M = M(c_1, c_2, c_3, c_4)$, has eigenvalues $\alpha \pm |k|$ with respective (left) eigenvectors $(1, \pm\xi, 0, 0)$ and $(0, 0, 1, \pm\xi)$. Here $\alpha = \sum_{j=1}^{4} |c_j|^2$ and $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$.

Proposition 4.4 *The lattices $L_t,\ t = 2, 4, 5, 6$, have defect four.*

Proof. As $2L_2 \subset L_6 \subset L_5 \subset L_4 \subset L_2$, it suffices to prove the statement for L_2. We first observe that the 4-dimensional real vector space generated by $M_1 = M(1,0,0,0), M_2 = M(i,0,0,0), M_3 = M(0,0,1,0)$, and $M_4 = M(0,0,i,0)$ consists of invertible matrices only (apart from the zero matrix). This is because these matrices really are 2×2 Alamouti matrices, where each complex entry is replaced by a 2×2 scalar block. If $\mathbf{h}$ is a non-zero channel vector, the vectors $\mathbf{h}M_j, j = 1, 2, 3, 4$ must then be linearly independent over the reals. Otherwise, $\mathbf{h}$

would belong to the eigenvalue zero for the corresponding linear combination of the matrices M_j contradicting the fact that the matrix in question is invertible. We may thus conclude that the defect of L_2 is at most four.

On the other hand, if $\mathbf{h} = (1, \xi, 0, 0)$ then by our earlier observations $\mathbf{h}M$ is a complex linear combination of $\mathbf{h}$ and $(0, 0, 1, \xi)$ for all the matrices $M \in L_2$. Thus $\mathbf{h}L_2$ spans a 4-dimensional real vector space, so the defect is also at least four. ■

We skip the proof of the following rather trivial observation.

Proposition 4.5 *Let V_+ (resp. V_-) be the complex subspace of $\mathbb{C}^4$ generated by the vectors $(1, \xi, 0, 0)$ and $(0, 0, 1, \xi)$ (resp. by $(1, -\xi, 0, 0)$ and $(0, 0, 1, -\xi)$). The subspaces V_+ and V_- are orthogonal complements of each other in $\mathbb{C}^4$, so any channel vector can be uniquely written as*

$$\mathbf{h} = \mathbf{h}_+ + \mathbf{h}_-,$$

where $\mathbf{h}_\pm \in V_\pm$ respectively. If $\mathbf{h}$ belongs to one of the subspaces V_+, V_-, the lattice $\mathbf{h}L_2$ collapses. ■

Remark 4.1 *Similarly, the lattice L_1 collapses if $\mathbf{h}$ is in the span of any three or less of the rows of the matrix U above. Also for any DAST lattice L_{DAST} of 4×4-matrices there are four 'forbidden' subspaces V_1, V_2, V_3, V_4 of $\mathbb{C}^4$ with the property that $\mathbf{h}L_{DAST}$ does not collapse if, and only if, $\mathbf{h}$ has a non-zero component in each one of the subspaces $V_j,\ j = 1, 2, 3, 4$.*

Remark 4.2 *A plausible explanation to the performance of suboptimal decoding algorithms based on iterative interference cancellation is that such algorithms cannot work well, when $\mathbf{h}$ is in one of the forbidden subspaces V leading to a collapsed lattice $\mathbf{h}L$. Thus the 'effective' diversity is cut down by $\dim_{\mathbb{C}} V$.*

Let us now yet more closely analyze the situation in which the receiver's version of the lattice L_2 collapses in the sense that the real span V of the free abelian group $\mathbf{h}L_2$ has dimension strictly less than 8. Obviously, the space V is the $\mathbb{R} \otimes_{\mathbb{Q}} \mathbf{H}$-submodule of $\mathbb{C}^4$ generated by the vector $\mathbf{h}$. It is readily seen that the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Q}} \mathbf{H}$ is a direct sum of two copies of the algebra of the Hamiltonian quaternions. Thus the space $\mathbb{C}^4$ will also be a direct sum of two 4-dimensional submodules, i.e. the defect is 4 (cf. Definition 4.1 and Proposition 4.4), and the lattice collapses exactly when the channel state vector happens to be in one of the submodules. This is in sharp contrast to the case of the commutative ring L_1 and the DAST construction due to the fact that the $\mathbb{R}$-algebra $\mathbb{R} \otimes_{\mathbb{Q}} \mathbf{L}$ is isomorphic to a direct sum of four copies of the field of complex numbers (a consequence of simultaneous diagonalizability). Thus in those cases the receiver's signal space $\mathbb{C}^4$ has four submodules of real dimension 6 (i.e., defect $= 6$, cf. Example 4.1

and Proposition 4.3) as well as smaller submodules that are intersections of the maximal ones. Therefore, we have theoretical reasons to expect that the lattice will collapse more often, if we use, e.g. the lattice L_1 or the DAST lattices as compared to the L_2 lattice. The set of these critical channel vectors (= the union of proper submodules) obviously has measure zero, but, nevertheless, it can be assumed that something vicious will happen, when we approach the critical set. Our simulations indeed show that the complexity of a sphere decoder increases sharply, when we approach the critical set. A comparison between the lattices L_1 and L_2 does not show a dramatic difference between the average complexities of a sphere decoder, but the difference becomes very apparent, when studying the high-complexity tails of the complexity distribution.

In Fig. 2 and 3 we have plotted the complexity distribution of 5000 transmissions for different data rates. On the horizontal axis the quantity $\min(\ |\mathbf{h}_i|^2\ )$ (resp. $\min(\ |\mathbf{h}_+|^2, |\mathbf{h}_-|^2\ )$) describes how close the lattice L_1 (resp. L_2) is to the situation where it would collapse. That is, how close to zero the minimum of the components $\mathbf{h}_i \in V_i,\ i = 1, 2, 3, 4$, (resp. $\mathbf{h}_\pm \in V_\pm$) gets (cf. Remark 4.1 and Proposition 4.5). For both L_1 and L_2 the figure shows that the smaller the quantity, the higher the complexity. We can also conclude that the lattice L_1 nearly collapses a lot more often than the lattice L_2. In addition, the number of points visited by the sphere decoding algorithm is much higher for L_1 than for L_2. These are phenomena caused by the defect. In Fig. 4 and 5 the scaled impact of defect is depicted.

Note that as L_{DAST} has the same structure in terms of the defect as L_1, we can equally well analyze the behavior of the DAST lattice on the basis of Fig. 2–Fig. 5.

5 Energy considerations and simulations

As a summary of Propositions 2.2–2.6 we get the following.

Proposition 5.1 *(1) The lattice L_2 is isometric to the rectangular lattice $\mathbb{Z}^8$ and has a minimum determinant equal to 1.*

(2) The lattice L_4 isometric to D_8 is an index two sublattice of L_2 and has a minimum determinant equal to 4.

(3) The lattice L_5 isometric to $D_4 \perp D_4$ is an index four sublattice of L_2 and has a minimum determinant equal to 16.

(4) The lattice L_6 isometric to E_8 is an index 16 sublattice of L_2 and has a minimum determinant equal to 64. ■

In order to compare these lattices we scale them to the same minimum determinant. When a real scaling factor ρ is used the minimum determinant is multiplied by ρ^2. As all the lattices have rank 8, the fundamental volume is then multiplied by ρ^8. Let us choose the units so that the fundamental volume of L_2 is $m(L_2) = 1$.

Then after scaling $m(L_4) = 1/2$, $m(L_5) = 1/4$, and $m(L_6) = 1/4$. As the density of a lattice is inversely proportional to the fundamental volume, we thus expect the codes constructed within e.g. the lattices L_4 and L_6 to outperform the codes of the same size within L_2.

The exact average transmission power data in Fig. 6 is computed as follows. Given the size K of the code we choose a random set of K shortest vectors from each lattice. The average energy of the code

$$E_{av} = \frac{\sum_{x \in \mathcal{C}} \|x\|^2}{K}$$

is then computed with the aid of theta functions [30]. All the lattices were normalized to have minimum determinant equal to 1. When using the matrices $M(c_1, c_2, c_3, c_4)$ of Proposition 2.1, in some cases we are better off selecting the input vectors (c_1, c_2, c_3, c_4) from the coset $\frac{1}{2}(1+i, 1+i, 1+i, 1+i) + \mathcal{G}^4$ instead of letting them range over $\mathcal{G}^4$. Obviously such a translation does not change the minimum determinant of the code, but it sometimes results in significant energy savings. E.g. to get a code of size 256 it is clearly desirable to let the coefficients c_1, c_2, c_3, c_4 range over the QPSK-alphabet.

Fig. 7 and Fig. 8 show the block error rates of the various competing lattice codes at the rates approximately 2, 4, 6, and 8 bpcu, i.e. all the codes contain roughly $2^8, 2^{16}, 2^{24}$ or 2^{32} matrices respectively. For the lattices L_1, L_2, L_{DAST}, and L_{ABBA} [19] this simply amounted to letting the coefficients c_1, c_2, c_3, c_4 take all the values in a QPSK-alphabet. Therefore, it would have been easy to obtain bit error rates as well. For the lattices L_4, L_5, L_6 the rate is not exact, see (10) below and the preceding explanation. Of course also the exact rate equal to a power of two could be achieved by just choosing a more or less random set of shortest lattice vectors. As there is no natural way to assign bit patterns to vectors of D_8, $D_4 \perp D_4$ or E_8, we chose to show the block error rates instead of the bit error rates.

The simulations were set up, here, so that the 95 per cent reliability range amounts to a relative error of about 3 per cent at the low SNR end and to about 10 per cent at the high SNR end (or to about 4000 and 400 error events respectively). One receiver was used for all the lattices.

When moving left in (1) the minimum determinant increaces while the BLER decreases at the same time. However, the other side of the coin is that improvements in the BLER performance cause a slightly more complex decoding process by increasing the number of points visited in the search tree. Still after this increasement, even the lattice L_6 admits a fairly low average complexity as compared to the lattices L_1 and L_{DAST} due to its lower defect. In part of the pictures in Fig. 7 and Fig. 8, the order of the curves seems not to respect the above mentioned order, but this only happens because the rates are not exactly the same for all the lattices. E.g. at the rate ≈ 4 bpcu, the exact rates for $L_2, L_4, L_5,$ and L_6 are $4, 3.75, 4.14,$ and 4.17 bpcu respectively. Consequently, the lattice L_4 seems

to perform better than what it actually does. Let us shortly explain how these rates follow: when picking the elements $x_1, ..., x_8$ from the set $\mathbb{Z}_Q$ (cf. Section 4 (5) and the discussion after Algorithm II), the size of the code within the lattice $L_i,\ i = 2, 4, 5, 6$, will be $\frac{Q^8}{[L_2:L_i]} = 2^{\log \frac{Q^8}{[L_2:L_i]}}$, where $[L_2 : L_i]$ is the index of the sublattice L_i inside L_2 (cf. Proposition 5.1). Hence, the data rate in bits per channel use can be computed as

$$R = \frac{\log \frac{Q^8}{[L_2:L_i]}}{4}. \tag{10}$$

Now, for instance, to get as close to the rate $R = 4$ bpcu as possible, we have to choose $Q = 4, Q = 4, Q = 5$, and $Q = 6$ for the lattices L_2, L_4, L_5, and L_6 respectively. By substituting Q and the sublattice index in question to (10) we obtain the above rates.

Simulations at the rate 6 bpcu with one receiver show that the lattice L_6 wins by approximately 1 dB over the lattice L_2 and by at least 2.5 dB over L_{DAST}. At the rate 2 bpcu, the rotated ABBA lattice L_{ABBA} is already beaten by the L_2 lattice by a fraction of a dB. The difference between L_2 and L_{DAST} is even clearer: L_2 gains $1 - 2$ dB over L_{DAST}, depending on the SNR. At all data rates the lattice L_6 outperforms all the other lattices.

6 Conclusions and suggestions for further research

In this paper, we have presented new constructions of rate-one, full-diversity, and energy efficient 4×4 space-time codes with non-vanishing determinant by using the theory of rings of algebraic integers and their counterparts within the division rings of Lipschitz' and Hurwitz' integral quaternions. A comfortable, purely number theoretic way to improve space-time lattice constellations was introduced. The use of ideals provided us with denser lattices and an easy way to present the exact proofs for the minimum determinants. The constructions can be extended also to a larger number of transmit antennas, and they nicely fit with the popular Q^2-QAM and QPSK modulation alphabets. The idea of finding denser sublattices within a given division algebra was also generalized to a MIMO case with arbitrary number of Tx antennas by using the theory of cyclic division algebras and, as a novel method, their maximal orders. This is encouraging as the CDA based square ST constructions with NVD are known to achieve the DM-G tradeoff. We have also shown that the explicit constructions in this paper all have a simple decoding method based on sphere decoding. Related to the decoding complexity, the notion of defect was introduced for the first time in this paper. Both the theory and experimental results have proven the relevance of this new notion.

Comparisons with the four antenna DAST block code have shown that our codes provide lower energy and block error rates due to their good minimum determinant, i.e. high density and low defect. At the moment, we are searching for

well-performing MIMO codes arising from the theory of crossed product algebras and maximal orders of cyclic division algebras. We have noticed that also the discriminant of a maximal order plays an important role in code design. It is desirable to choose cyclic division algebras for which the discriminant of a maximal order is as small as possible [41]. By now, we are able to construct an explicit cyclic division algebra of an arbitrary index over $\mathbb{Q}(i)$ (or $\mathbb{Q}(w)$) that has a maximal order with minimal discriminant. Despite the fact that we have not yet fully analyzed the practical performance of codes arising from these constructions, the preliminary results have been very promising. Further details on this and on the algorithmic properties of maximal orders (see also [42]-[44]) will be given in a forthcoming paper.

References

[1] J.-C. Guey, M. P. Fitz, M. R. Bell, and W. Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels", in *Proc. IEEE Vehicular Technology Conf.*, 1996, pp. 136–140. Also in *IEEE Trans. Commun.*, vol. 47, pp. 527–537, April 1999.

[2] 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.

[3] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Four Antenna Space-Time Lattice Constellations from Division Algebras", in *Proc. IEEE ISIT 2004*, p. 338., Chicago, June 27 - July 2, 2004.

[4] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Dense Full-Diversity Matrix Lattices for Four Antenna MISO Channel", in *Proc. IEEE ISIT 2005*, pp. 1290–1294, Adelaide, September 4 - 9, 2005.

[5] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal Algebraic Space-Time Block Codes", *IEEE Trans. Inf. Theory*, vol. 48, pp. 628–636, March 2002.

[6] 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.

[7] J.-C. Belfiore and G. Rekaya, "Quaternionic Lattices for Space-Time Coding", in *Proc. ITW 2003*, Paris, France, March 31 - April 4, 2003.

[8] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: A 2x2 Full-Rate Space-Time Code with Non-Vanishing Determinants", in *Proc. IEEE ISIT 2004*, p. 308, Chicago, June 27 - July 2, 2004.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Algebraic 3x3, 4x4 and 6x6 Space-Time Codes with Non-Vanishing Determinants", in *Proc. IEEE ISITA 2004*, Parma, Italy, October 10 - 13, 2004.

[10] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, "Perfect Space-Time Block Codes", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[11] 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.

[12] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman "STBCs using capacity achieving designs from crossed-product division algebras", in *Proc. IEEE ICC 2004*, pp. 827–831, Paris, France, 20-24 June 2004.

[13] 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.

[14] 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.

[15] 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.

[16] M. O. Damen, H. E. Gamal, and N. C. Beaulieu, "Linear Threaded Algebraic Space-Time Constellations", *IEEE Trans. Inf. Theory*, vol. 49, pp. 2372–2388, October 2003.

[17] M. O. Damen and H. E. Gamal, "Universal Space-Time Coding", *IEEE Trans. Inf. Theory*, vol. 49, pp. 1097–1119, May 2003.

[18] P. Dayal and K. Varanasi, "Algebraic Space-Time Codes with Full Diversity and Low Peak-To-Mean Power Ratio", in *Proc. Commun. Th. Symp., IEEE GLOBECOM*, San Francisco, CA, Dec. 2003.

[19] O. Tirkkonen, A. Boariu, and A. Hottinen, "Minimal Non-Orthogonality Rate 1 Space-Time Block Code for 3+ TX Antennas", in *Proc. IEEE ISSSTA*, vol. 2, pp. 429–432, September 2000.

[20] 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.

[21] 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.

[22] I. Stewart and D. Tall, *Algebraic Number Theory*, Chapman and Hall, London 1979.

[23] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, “Space-Time Block Codes from Orthogonal Designs”, *IEEE Transactions on Information Theory*, vol. 45, pp. 1456–1467, July 1999.

[24] O. Tirkkonen, “Optimizing Space-Time Block Codes by Constellation Rotations”, in *Proceedings Finnish Wireless Communications Workshop FWCW’01*, pp. 59–60, October 2001.

[25] A. Hottinen and O. Tirkkonen, “Square-Matrix Embeddable Space-Time Block Codes for Complex Signal Constellations”, *IEEE Trans. Inf. Theory*, vol. 48 (2), pp. 384–395, February 2002.

[26] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, “Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels”, *IEEE Trans. Inf. Theory*, vol. 42, pp. 502–518, March 1996.

[27] B. Hassibi, B. M. Hochwald, A. Shokrollahi, and W. Sweldens, “Representation Theory for High-Rate Multiple-Antenna Code Design”, *IEEE Trans. Inf. Theory*, vol. 47, pp. 2335–2364, September 2001.

[28] F. E. Oggier and E. Viterbo, “Algebraic number theory and code design for Rayleigh fading channels", *Foundations and Trends in Communications and Information Theory*, December 2004.

[29] H. Jafarkhani, “A Quasi-Orthogonal Space-Time Block Code”, *IEEE WCNC*, vol. 1, pp. 42–45, September 2000.

[30] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der Mathematischen Wissenschaften #290, Springer-Verlag, New York 1988.

[31] D. Allcock, “New Complex- and Quaternion-Hyperbolic Reflection Groups”, *Duke Mathematical Journal*, vol. 103, pp. 303–333, June 2000.

[32] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, San Francisco 1980.

[33] A. A. Albert, *Structure of Algebras*, American Mathematical Society, New York City 1939.

[34] I. Reiner, *Maximal Orders*, Academic Press, London 1975.

[35] C. Hollanti and J. Lahtonen, "A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras", in *Proc. IEEE ITW 2006*, pp. 322–326, Punta del Este, March 13-17, 2006.

[36] M. Pohst, "On the Computation of Lattice Vectors of Minimal Length, Successive Minima and Reduced Basis with Applications", *ACM SIGSAM*, vol. 15, pp. 37–44, 1981.

[37] E. Viterbo and J. Boutros, "A Universal Lattice Code Decoder for Fading Channel", *IEEE Transactions on Information Theory*, vol. 45, pp. 1639–1642, July 1999.

[38] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest Point Search in Lattices", *IEEE Transactions on Information Theory*, vol. 48, pp. 2201–2214, August 2002.

[39] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice Codes Decoder for Space-Time Codes", *IEEE Commun. Lett.*, vol. 4, pp. 161–163, May 2000.

[40] M. O. Damen, H. El Gamal, and G. Caire, "On Maximum-Likelihood Detection and the Search for the Closest Lattice Point", *IEEE Transactions on Information Theory*, vol. 49, pp. 2389–2402, October 2003.

[41] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, "Optimal Matrix Lattices for MIMO Codes from Division Algebras", in *Proc. IEEE ISIT 2006*, pp. 783–787, Seattle, July 9 - 14, 2006.

[42] L. Rónyai, "Algorithmic Properties of Maximal Orders in Simple Algebras Over Q", *Computational Complexity 2*, pp. 225–243, 1992.

[43] G. Ivanyos and L. Rónyai, "On the complexity of finding maximal orders in algebras over Q", Computational Complexity 3, pp. 245–261, 1993.

[44] Web page:
http://magma.maths.usyd.edu.au/magma/htmlhelp/text835.htm#8121.

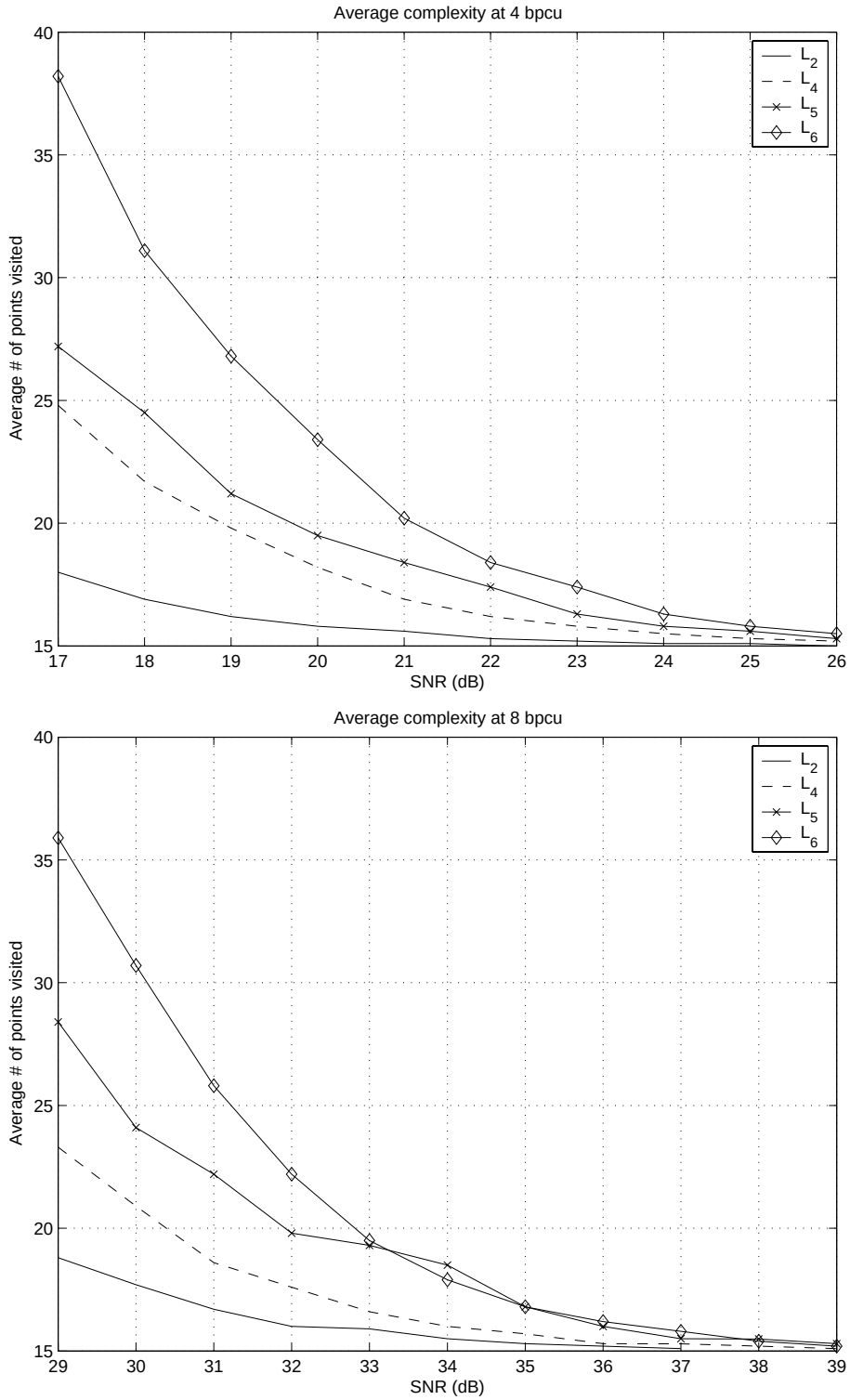

Figure 1: Average complexity of 4 tx-antenna matrix lattices at rates (approximately) $R = 4$ and $R = 8$ bpcu.

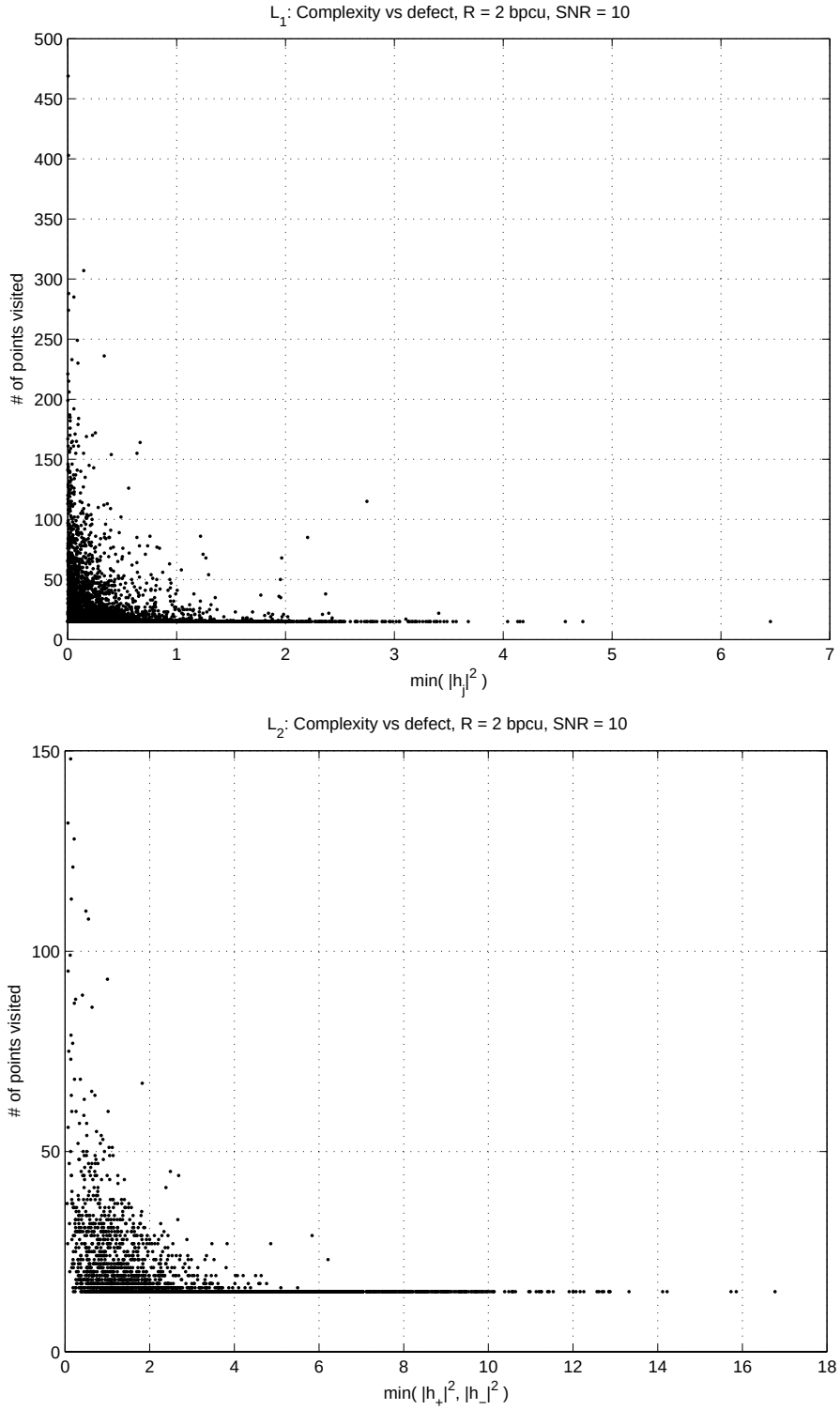

Figure 2: The impact of defect on complexity, L_1 ($\sim L_{DAST}$) vs L_2.

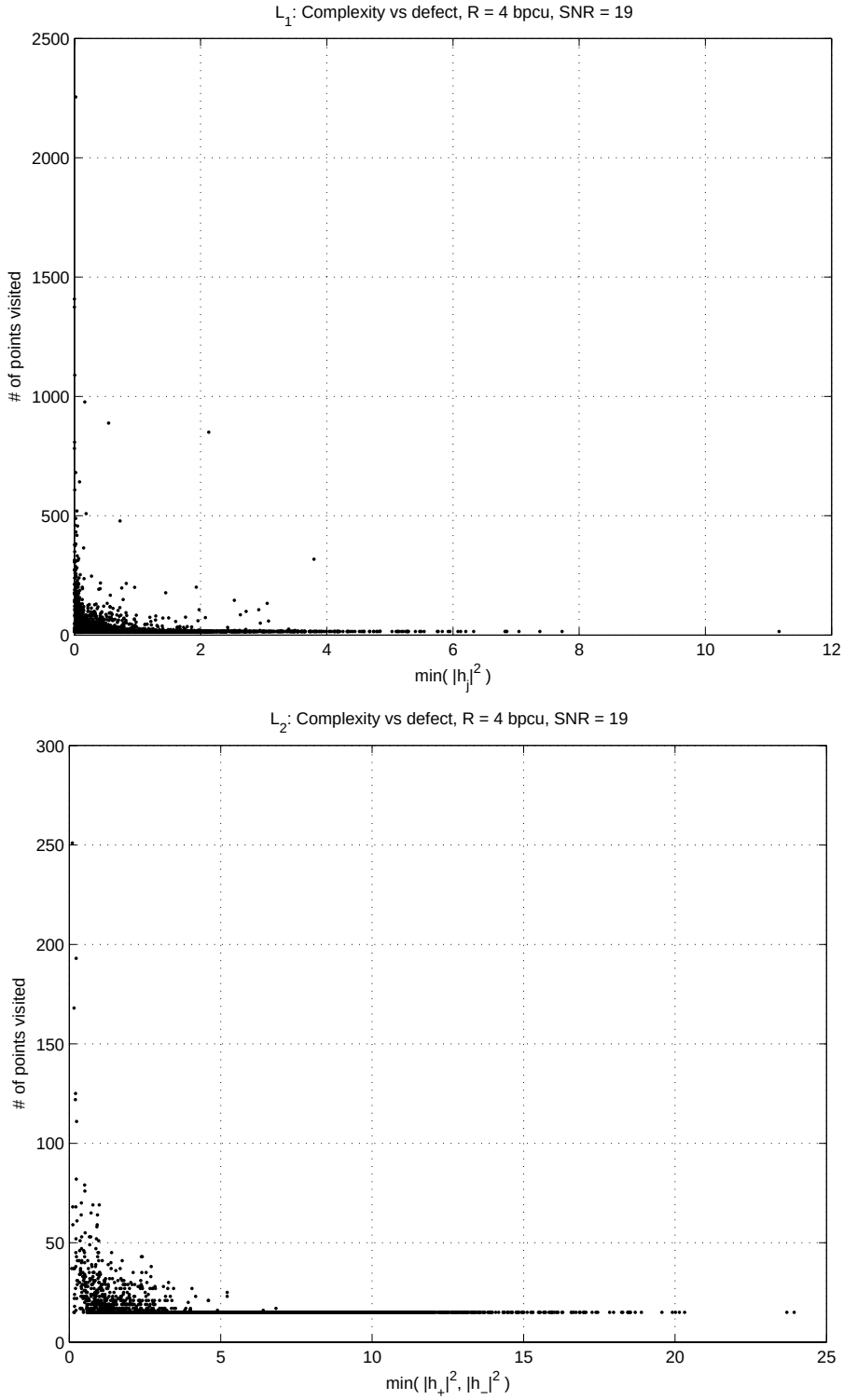

Figure 3: The impact of defect on complexity, L_1 ($\sim L_{DAST}$) vs L_2.

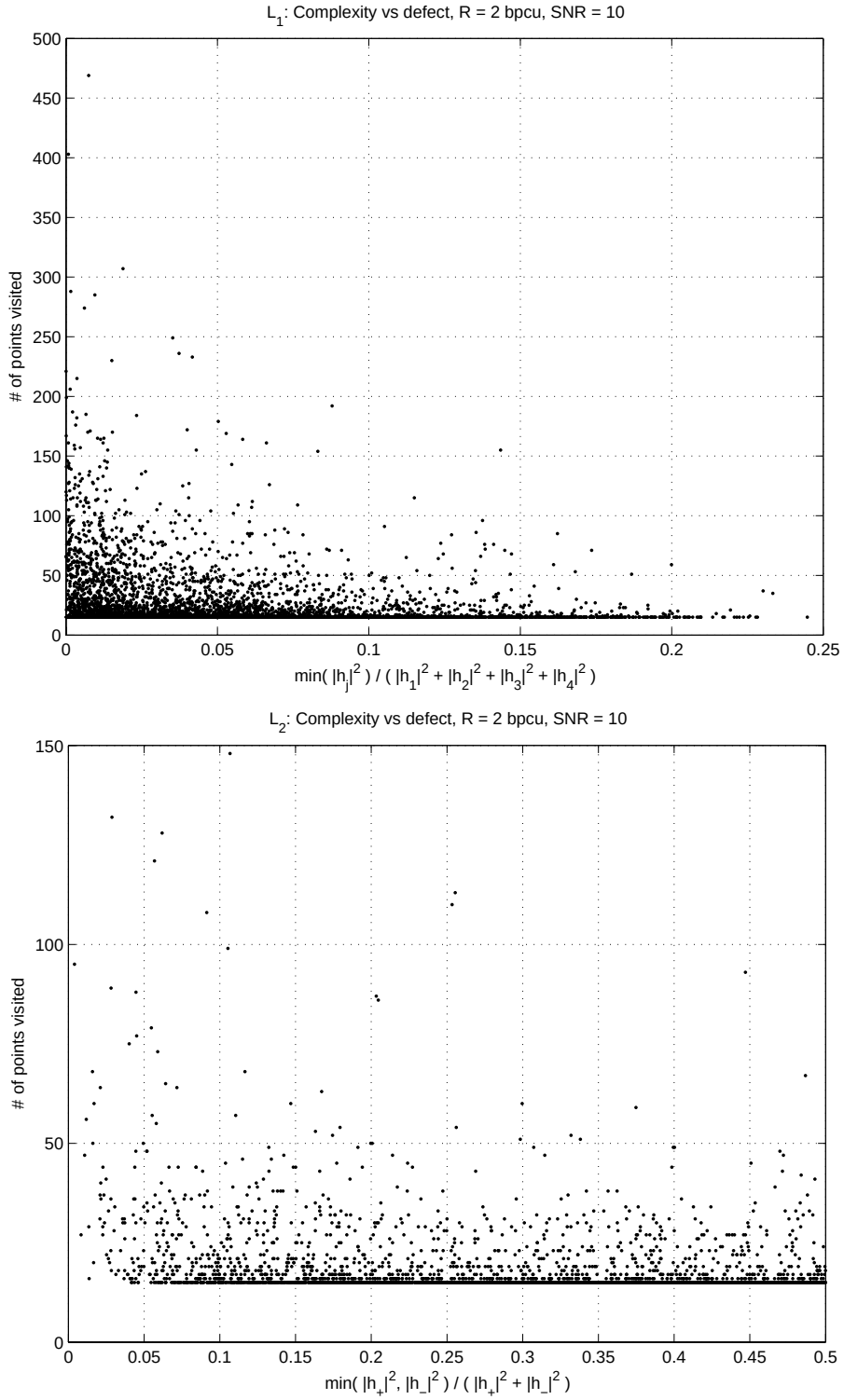

Figure 4: The scaled impact of defect on complexity, L_1 ($\sim L_{DAST}$) vs L_2.

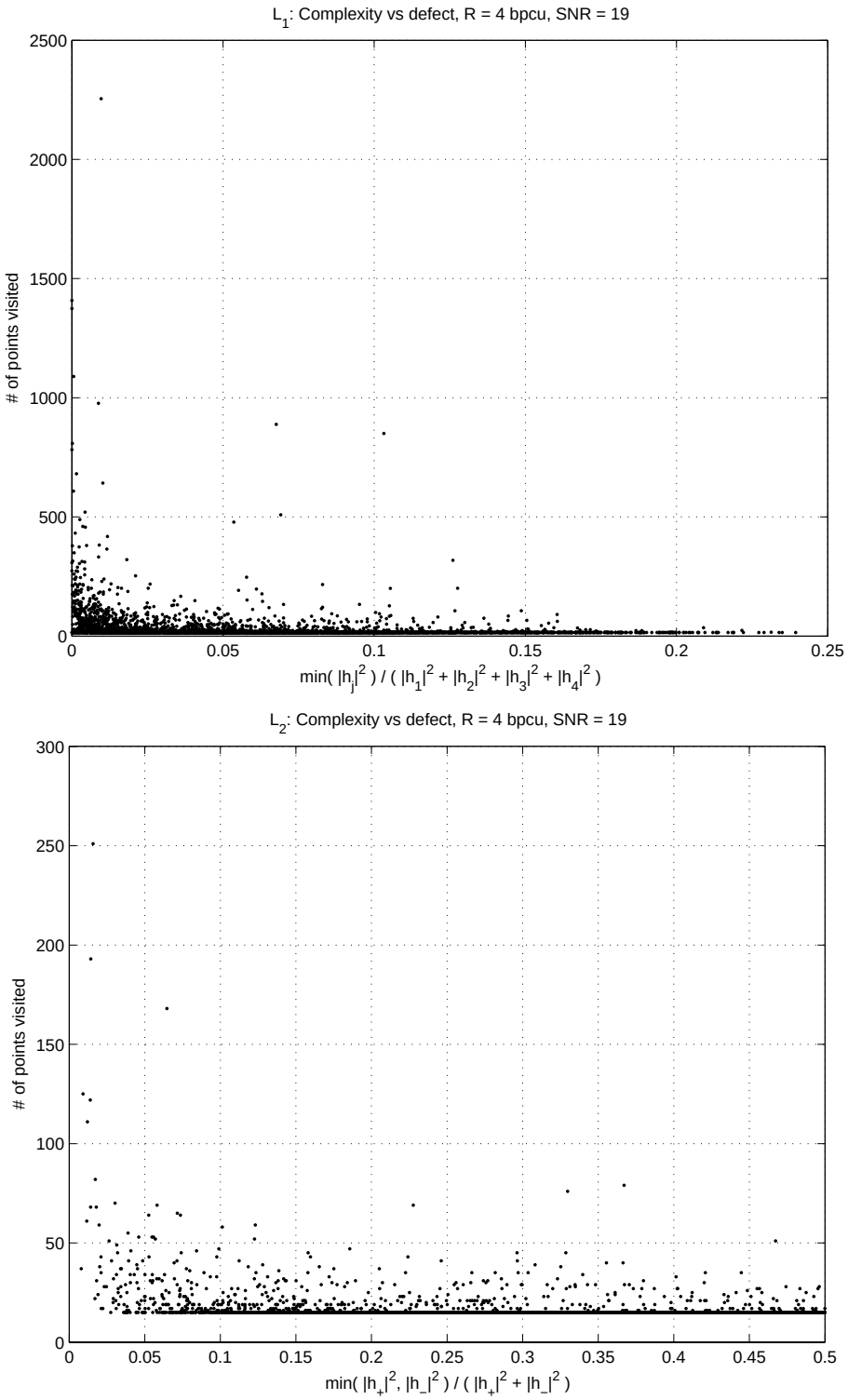

Figure 5: The scaled impact of defect on complexity, L_1 ($\sim L_{DAST}$) vs L_2.

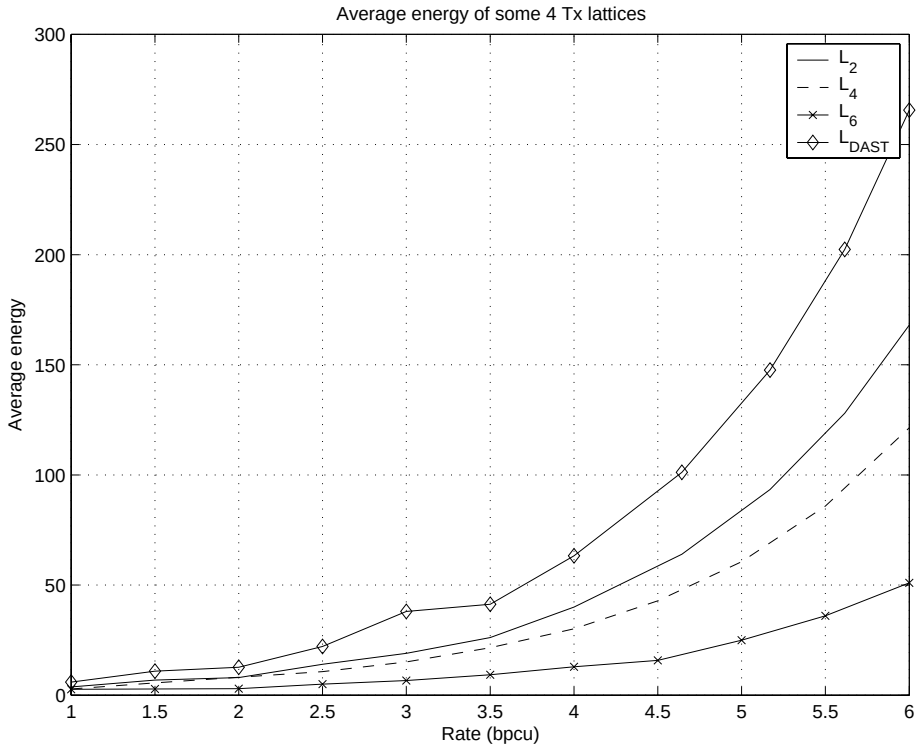

Figure 6: Average energy of 4 Tx antenna lattices.

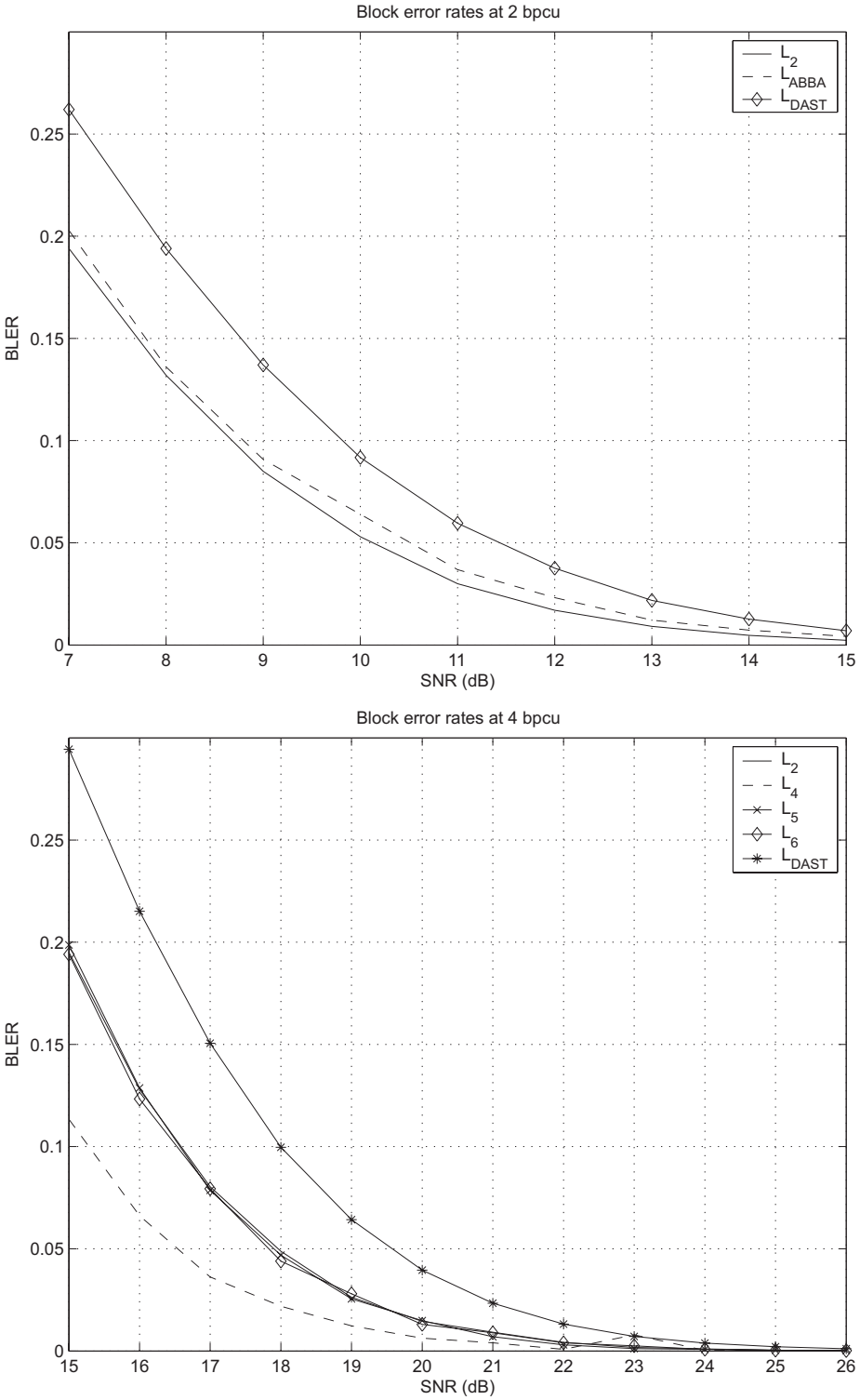

Figure 7: Block error rates of 4 tx-antenna lattices at approximately 2.0 and 4.0 bpcu.

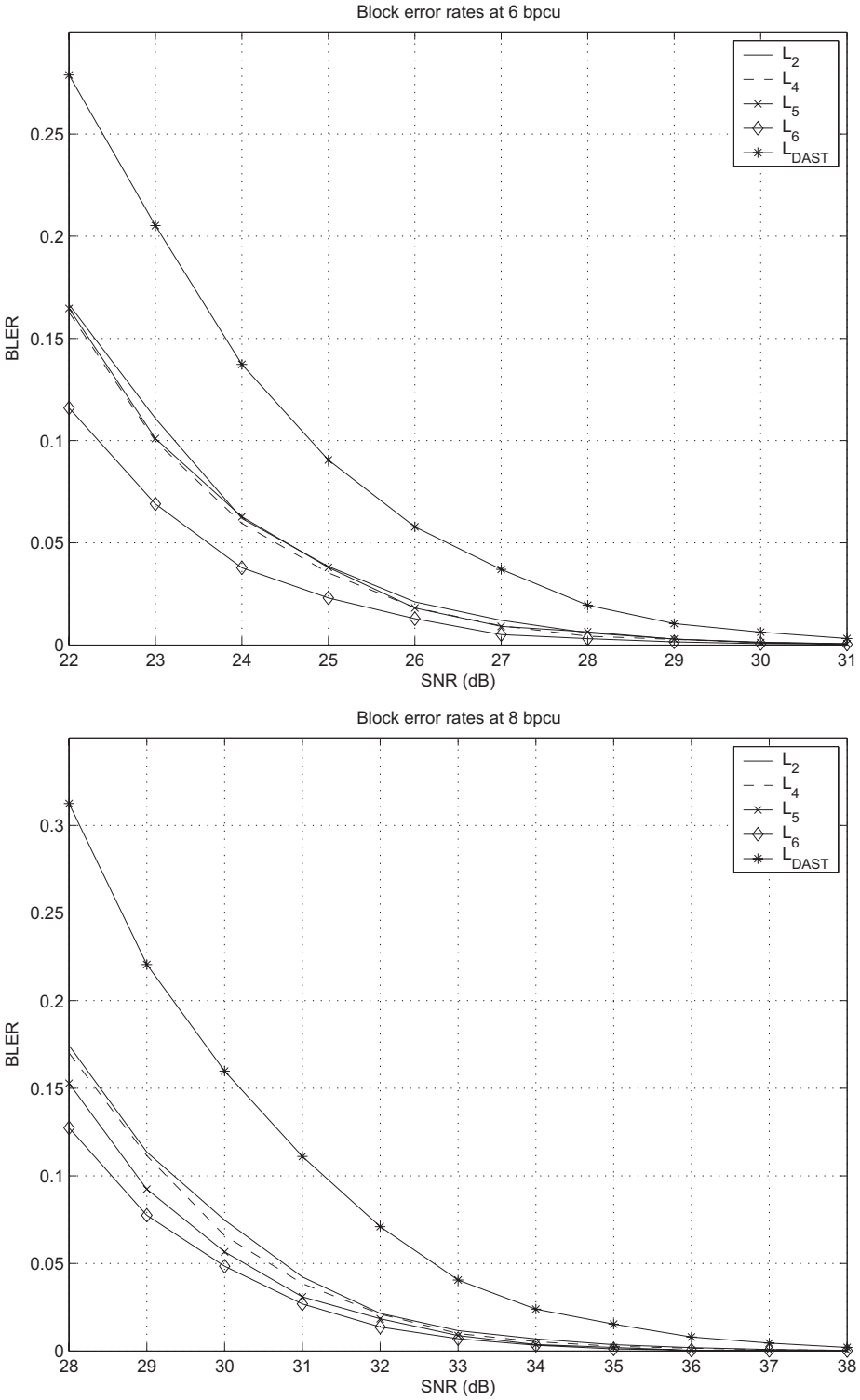

Figure 8: Block error rates of 4 tx-antenna lattices at approximately 6.0 and 8.0 bpcu.

Turku
Centre *for*
Computer
Science

Lemminkäisenkatu 14 A, 20520 Turku, Finland | 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 Sciences

ISBN 952-12-1789-8
ISSN 1239-1891