Jarkko Hiltunen | Camilla Hollanti | Jyrki Lahtonen

Dense Full-Diversity Matrix Lattices for Four Transmit Antenna MISO Channel

Turku Centre for Computer Science

TUCS Technical Report
No 664, February 2005

Dense Full-Diversity Matrix Lattices for Four Transmit Antenna MISO Channel

Jarkko Hiltunen
Turku Centre for Computer Science
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
jakahi@utu.fi
Camilla Hollanti
Turku Centre for Computer Science
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
cajoho@utu.fi
Jyrki Lahtonen
Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
lahtonen@utu.fi

TUCS Technical Report
No 664, February 2005

Abstract

We construct some geometrically dense matrix lattices with good minimum product distances for 4 transmit antenna MISO applications. The construction is based on the theory of rings of algebraic integers and related subrings of the Hamiltonian quaternions. Simulations in a quasi-static Rayleigh fading channel show that our dense quaternionic constructions outperform the earlier rectangular lattices as well as the DAST-lattice.

Keywords: space-time codes, lattices, number fields, quaternions

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Background and basic definitions

We are interested in the coherent multiple input-single output (MISO) case where the receiver perfectly knows the channel coefficients. The received signal is

$$\mathbf{y_{1\times n}} = \mathbf{h_{1\times k}X_{k\times n}} + \mathbf{n_{1\times n}},$$

where $\mathbf{X}$ is the transmitted codeword taken from Space-Time Block Code (STBC), $\mathbf{h}$ is the Rayleigh fading channel response and the components of the noise vector $\mathbf{n}$ are i.i.d. complex Gaussian random variables.

A *lattice* is simply a discrete finitely generated free abelian subgroup $\mathbf{L}$ of a real (or complex) finite dimensional vector space $\mathbf{V}$, called the ambient space. In the space-time setting a natural ambient space is the space $\mathcal{M}_n(\mathbf{C})$ of complex $n \times n$-matrices. When a code is a subset of a lattice $\mathbf{L}$ in this ambient space, the rank criterion states that any non-zero matrix in $\mathbf{L}$ must be invertible. This follows from the fact that the difference of any two matrices from $\mathbf{L}$ is again in $\mathbf{L}$. As a main design criterion we recall the *minimum product distance* of the code $\mathcal{C}$. In the case of square matrix lattice this takes the form

$$\delta_{\mathcal{C}} = \min_{\mathbf{M}\in\mathcal{C},\mathbf{M}\neq 0}\{\det(\mathbf{M}\mathbf{M}^*)^{\frac{1}{k}}\},$$

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

This work is a continuation of the reports [1] and [2]. The reader interested in more background is referred to [3]-[9].

2 Rings of algebraic numbers, quaternions and lattice constructions

It is widely known how the so called *Alamouti design* (cf. e.g. [26]) represents 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 STBC codes at least in [2], [11]-[19], and (though without explicitly saying so) [20]. The most recent work ([12]-[20]) has concentrated on adding multiplexing gain (i.e. MIMO applications) and/or combining it with good minimum product distance. We do not seek any multiplexing gains, but want to improve upon e.g. the DAST-lattices introduced in [11] by using non-commutative division algebras.

Other efforts to improve the DAST-lattices and ideas alike can be found in [21], [22], and [23].

We shall use extension rings of the Gaussian integers $\mathcal{G} = \{a + bi | a, b \in \mathbf{Z}\}$ inside a given division algebra. It would be easy to adapt the construction to use the ring of the Eisensteinian integers $\mathcal{E} = \{a + b\omega | a, b \in \mathbf{Z}\}$, where $\omega^3 = 1$, as a basic alphabet. However, the Gaussian integers fit nicely 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 A that are also 4-dimensional vectors spaces over the field $K = \mathbf{Q}(i)$. Let $\zeta = e^{\pi i/8}$ (resp. $\xi = e^{\pi i/4} = (1+i)/\sqrt{2}$) be primitive 16^{th} (resp. 8^{th}) root of unity. Our main examples of such division algebras are the number field $L = \mathbf{Q}(\zeta)$ and the following subskewfield of the Hamiltonian quaternions $\mathbf{H} = \mathbf{Q}(\xi) \oplus \mathbf{Q}(\xi) j$. Note that as $zj = j\overline{z}$ for all complex numbers z, and as the field $\mathbf{Q}(\xi)$ 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 the division algebra A is an invertible $\mathbf{Q}(i)$-linear mapping (with $\mathbf{Q}(i)$ acting from the right). Therefore its matrix with respect to a chosen $\mathbf{Q}(i)$-basis $\mathcal{B}$ of A is also invertible. Our example division algebras L and $\mathbf{H}$ have as natural $\mathbf{Q}(i)$-bases the sets $\mathcal{B}_L = \{1, \zeta, \zeta^2, \zeta^3\}$ and $\mathcal{B}_H = \{1, \xi, j, j\xi\}$ respectively. 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 $\mathbf{Q}(i)$. The division algebras L and $\mathbf{H}$ can be identified via an isomorphism ϕ with the following rings of matrices*

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

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 L into the matrix ring is determined by $\mathbf{Q}(i)$-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 $\mathbf{Q}(i)$-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.

Remark 2.1. The algebra $\mathbf{H}$ could also be viewed as cyclic division algebra in the sense of [12]. As it is a subring of the Hamiltonian quaternions, its center consists of the intersection $\mathbf{H} \cap \mathbf{R} = \mathbf{Q}(\sqrt{2})$. Also $\mathbf{Q}(\xi)$ is an example of a splitting field of $\mathbf{H}$. In the notation of section 7 of [12] we have an obvious isomorphism

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

where σ is the usual complex conjugation.

In order to get STBC-lattices and useful bounds for the minimum product distance we need to identify suitable subrings $\mathbf{R}$ of these two algebras. Actually we want these rings to be free (right) $\mathcal{G}$-modules of rank 4. This is because then the determinants of those matrices of Proposition 2.1 that belong to the subring $\phi(\mathbf{R})$ 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 multiplication by a fixed element $x \in \mathbf{R}$ does not depend on the choice of the basis $\mathcal{B}$, so we may assume that it is actually a $\mathcal{G}$-module basis. However, in that case $x\mathcal{B} \subset \mathbf{R}$, so the matrix will have entries in $\mathcal{G}$, as all the elements of $\mathbf{R}$ are $\mathcal{G}$-linear combinations of $\mathcal{B}$. The claim follows.

In the case of the field L we are only interested in its ring of integers $\mathcal{O}_L = \mathbf{Z}[\zeta]$ that is a free $\mathcal{G}$-module with basis $\mathcal{B}_L$. In this case the ring $\phi(\mathcal{O}_L)$ consists of those matrices of L that have all the coefficients $c_1, c_2, c_3, c_4 \in \mathcal{G}$. Similarly the $\mathcal{G}$-module spanned by our earlier basis $\mathcal{B}_H$ is a ring $\mathcal{L}$ of the required type. This ring should probably be called 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 of Hurwitz' integral quaternions also has an extension of the prescribed type inside $\mathbf{H}$. This ring, denoted by $\mathcal{H}$, is the (right) $\mathcal{G}$-module generated by the basis $\mathcal{B}_{Hur} = \{\rho, \rho\xi, j, j\xi\}$, where $\rho = (1 + i + j + k)/2$. 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. We easily see that the quaternion

$$q = c_1 + \xi c_2 + j c_3 + j\xi c_4$$

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

Proposition 2.2. *The following rings of matrices form STBC-lattices of minimum product distance 1.*

$$L_1 = \left\{ \begin{pmatrix} c_1 & ic_4 & ic_3 & ic_2 \\ c_2 & c_1 & ic_4 & ic_3 \\ c_3 & c_2 & c_1 & ic_4 \\ c_4 & c_3 & c_2 & c_1 \end{pmatrix} | c_1, c_2, c_3, c_4 \in \mathcal{G} \right\},$$

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

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

$$c_1 + c_3 \in \mathcal{G}, c_2 + c_4 \in \mathcal{G} \}.$$

Remark 2.2. The lattice L_1 is quite similar to the DAST-lattice in the sense that all of its matrices can be diagonalized simultaneously. The lattice L_2, for its part, is a more developed case from the so-called *quasi-orthogonal* STBC suggested e.g. in [24]. The matrix of L_2 can be found as an example also in [12], but no optimization has been done there by using, for example, ideals as we 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 $\mathbf{Z}^8$. The rectangular shape does carry the advantage that the sets of information carrying coefficients of the basic matrices are simple and all identical (this is useful in e.g. sphere decoding), but this shape is very wasteful in terms of transmission power. Geometrically denser sublattices of $\mathbf{Z}^8$, e.g. the checkerboard lattice D_8 and the root lattice E_8 are well known (cf. e.g. [25]). However, we must be careful in picking the copies of the sublattices, as it is the minimum product distance we want to keep an eye on.

As our earlier simulations ([1],[2]) showed 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 product distance is to take the lattice $\phi(\mathcal{I})$, where $\mathcal{I} \subset \mathbf{R}$ is a proper ideal. This idea has appeared in [2] and [14]. Even earlier, ideals of rings of algebraic integers were used in [8] 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*

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

and we have a strict inequality, if both A and B are invertible.

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

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

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

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

$$L_4 = \{M \in L_2 | c_1 + c_2 + c_3 + c_4 \in \mathcal{I}\}$$

is a rank 2 sublattice in L_2. Furthermore, the absolute value of $\det(MM^*)$, $M \in L_4 \setminus \{0\}$, 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

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

We see that

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

and

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

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 $\det MM^* = (\alpha^2 - |k|^2)^2 \geq 4$. Assume first that $c_3 = c_4 = 0$, i.e. the block $B = 0$. Then $\det(A)$ is the relative norm $\det(A) = N^{\mathbf{Q}(\xi)}_{\mathbf{Q}(i)}(c_1 + \xi c_2)$, 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 $\det(A)\det(A^*) \geq 2$, 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 of at least one. The matrices A, A^*, B, B^* all commute, so by Lemma 2.3 we get

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

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

Remark 2.3. It is easy to see that in the previous proposition $a + bi \in \mathcal{I}$, iff $a + b$ 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 product distances. To that end we use the ring $\mathcal{H}$ (or the lattice L_3). The first sublattice is isometric to the direct sum $D_4 \perp D_4$ of two 4-dimensional checkerboard lattices.

Proposition 2.5. *Let again $\mathcal{I}$ be the ideal $(1 + i)\mathcal{G}$ and $M(c_1, c_2, c_3, c_4)$ be the matrices of Proposition 2.1. The lattice*

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

has minimum prodcut distance equal to 2.

Proof. 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 $\det(AA^*) = 16 \det(MM^*)$, so the claim follows from Proposition 2.2. $\square$

The root lattice E_8 can be described in terms of Gaussian integers as follows (cf. [26])

$$E_8 = \frac{1}{1+i}\{(c_1, c_2, c_3, c_4) \in \mathcal{G}^4 | c_1 + \mathcal{I} = c_t + \mathcal{I},$$

$$t = 2, 3, 4, \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}.$$

By our identification of quadruples $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ and elements of $\mathbf{H}$ it is easily verified that $\Lambda = (1 + i)E_8$ 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 $1 + \xi$.

Proposition 2.6. *The lattice*

$$L_6 = \{M(c_1, c_2, c_3, c_4) \in L_2 | \ c_1 + \mathcal{I} = c_t + \mathcal{I},$$

$$t = 2, 3, 4, \sum_{t=1}^{4} c_t \in 2\mathcal{G}\}.$$

is an index 16 sublattice of L_2. Furthermore, the minimum product distance of L_6 is $2\sqrt{2}$.

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 $\det(M_I M_I^*) = 4$. By the preceeding discussion any matrix A of the lattice L_6 is of the form $A = MM_I(1+i)$, where M is a matrix from $\mathcal{H}$. As in the proof of Proposition 2.5, we see that $\det AA^* = 16\det(M_I M_I^*)\det(MM^*)$. Therefore the claim on the minimum distance 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 $\mathcal{I}$ is of index two in $\mathcal{G}$, we see that the index of L_6 in L_2 is 16 as claimed. □

Remark 2.4. We have been able to prove that the lattice L_6 is optimal within the cyclic division algebra $\mathbf{H}$ in the sense that the root lattice E_8 is a maximal order in $\mathbf{H}$. For the general theory of maximal orders required for this, see [27].

Remark 2.5. We have now produced a nested sequence of lattices

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

We concentrate on the lattices that are sandwiched between $2\mathbf{Z}^8$ and $\mathbf{Z}^8$. Such lattices are in a bijective correspondence with binary linear code of length 8 by "projection modulo 2". As it happens, within this sequence of lattices the minimum Hamming distance of the binary linear code and the minimum product distance of the lattice are somewhat related.

The 8-dimensional rectangular grid $\mathbf{Z}^8$ (no coding)
$\downarrow$
The checkerboard lattice D_8 ($\leftrightarrow$ overall parity check code of length 8)
$\downarrow$
The lattice $D_4 \perp D_4$ ($\leftrightarrow$ two blocks of the overall parity check code of length 4)
$\downarrow$
The root lattice E_8 ($\leftrightarrow$ extended Hamming-code of length 8).

Thus it is natural to ask that what if we simply concatenate the use L_2 with a good binary code (extended over several L_2-blocks, if need be), and be done with it. While the binary linear codes appearing above are the first ones that come to 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 product distance 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 the problems caused by high weight units.

3 Energy considerations and simulations

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

Proposition 3.1. *(1) The lattice L_2 is isometric to the rectangular lattice $\mathbf{Z}^8$ and has minimum product distance 1.*

(2) The lattice L_4 is an index two sublattice of L_2 and has minimum product distance $\sqrt{2}$.

(3) The lattice L_5 is an index four sublattice of L_2 and has minimum product distance 2.

(4) The lattice L_6 is an index 16 sublattice of L_2 and has minimum product distance $2\sqrt{2}$.

In order to compare these lattices we scale them to the same minimum product distance. When a real scaling factor ρ is used the minimum product distance 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.

We have collected the exact average transmission power data into Table 1. The data is computed as follows. Given the size M of the code we choose M shortest vectors from each lattice. The average energy of the code is then computed with the aid of theta functions [25]. All the lattices were normalized to have minimum product distance equal to 1. When using the matrices $M(c_1, c_2, c_3, c_4)$ of Proposition 2.1 we sometimes selected 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 product distance 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.

Figure 1 shows the block error rates of the various competing lattice codes at the rate 2 bits/s/Hz, i.e. all the codes contain 256 matrices. For the lattices L_1, L_2, L_{DAST} and L_{ABBA} [28] this simply amounted to letting the coefficients c_1, c_2, c_3, c_4 take all the values in the QPSK-alphabet. Therefore, it would have been easy to obtain bit error rates as well. For the lattices L_4, L_5 and L_6 a more or less random set of 256 shortest vectors was chosen. 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. Figure 1 shows that the lattice L_6 wins over all the other lattices.

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.

Figure 2 shows the block error rates of the code within L_6 and the Golden code [14] at the rate 4 bits/s/Hz with two receivers. At the rate 4 bits/s/Hz one block of our code consists of 16 bits, whereas one block of the Golden code carries 8 bits only. For that reason we decided to show the error rate of two consecutive blocks of the Golden code; i.e. if the usual error rate of the block of length two is p, the rate we show is $2p - p^2$.

We can conclude that the lattice L_6 outperforms the Golden code when SNR reaches about 13 dB. However, this is an unfair comparison because our code uses four transmit antennas while the Golden code uses only two — this is just a manifestation of the diversity gain, but we were interested in finding the approximate crossing point. The fact that the Golden code triumphs over our lattice at the low SNR end is not such a severe drawback either, since our codes are designed mainly for MISO channels when the Golden code is intended wholly for MIMO channels.

Table 1: Average energy of four antenna full-diversity matrix lattices

Rate	Lattice			
bit/s/Hz	L_2	L_4	L_6	L_{DAST}
1.0	3.75	2.83	2.66	5.93
1.5	6.88	5.57	2.79	10.88
2.0	8.00	8.13	2.98	12.65
2.5	14.00	10.68	4.99	22.14
3.0	19.00	15.09	6.66	30.04
3.5	26.12	21.57	9.28	41.30
4.0	40.00	30.13	12.86	63.25

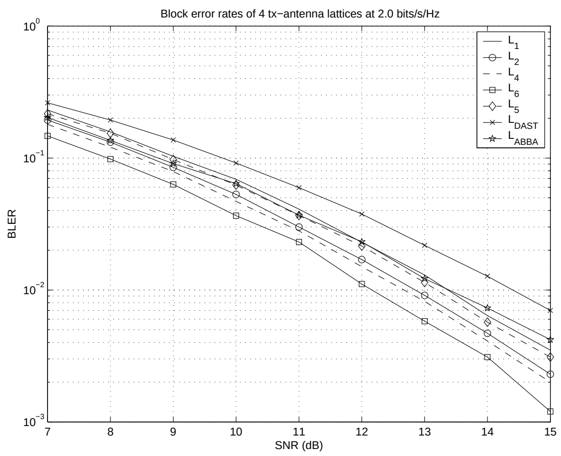

Figure 1: Block error rates of 4 tx-antenna lattices at 2.0 bits/s/Hz

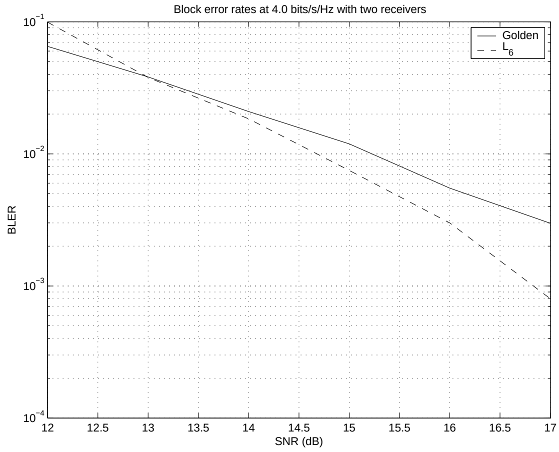

Figure 2: Block error rates at 4.0 bits/s/Hz with two receivers

4 Conclusions and suggestions for further research

In this paper, we present new constructions of rate one, full diversity, and energy efficient 4×4 space-time codes 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 is introduced. The use of ideals provides us denser lattices and an easy way to present the exact proofs for the minimum product distances. The constructions can be naturally extended also to a larger number of transmit antennas and they fit nicely with the popular Q^2-QAM and QPSK modulation alphabets.

Comparisons with DAST-code show that our codes provide lower energy and block error rates due to their good minimum product distance and high density. Despite the fact that our codes are mainly designed to use only one receiver antenna, comparisons with the Golden code give hope that the ideas of this paper will work with slight changes also with multiple receivers. For that reason, our next goal is to improve these ideas and codes so that they would perform well also in MIMO channels. We are also searching for well-performing MIMO codes arising from the theory of crossed product algebras and maximal orders of cyclic division algebras.

We have also started analyzing more closely the situation, where the receiver's version of the lattice collapses in the sense that the real span V of the free abelian group $\mathbf{hL}$ is of dimension strictly less than 8. The space V is obviously the $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{H}$-submodule of $\mathbf{C}^4$ generated by the vector $\mathbf{h}$. It is easy to see that the $\mathbf{R}$-algebra $\mathbf{R} \otimes_{\mathbf{Q}} \mathbf{H}$ is a direct sum of two copies of the algebra of Hamiltonian quaternions. Thus the space $\mathbf{C}^4$ will also be a direct sum of two 4-dimensional submodules, 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. This is because the $\mathbf{R}$-algebra $\mathbf{R} \otimes_{\mathbf{Q}} L$ 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 $\mathbf{C}^4$ has four submodules of real dimension 6 as well as smaller submodules that are intersections of the maximal ones. Therefore we have every reason to expect that the lattice will collapse more often, if we use, e.g. L_1. The set of these critical channel vectors (= the union of proper submodules) obviously has measure zero, but, nevertheless, it is natural to assume that something bad will happen, when we are close to the critical set. Preliminary simulations (we are indebted to M.Sc. Miia Mäki for carrying out this work) show that the complexity of the 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 the sphere decoder, but the difference is very clear, when studying the high-complexity tails of the complexity distribution. This phenomenon may merit further study.

References and bibliography

[1] J. Hiltunen and J. Lahtonen, ”Four Transmit Antenna Space-Time Lattice Constellations from Domains in Division Algebras”, part of the final report of the project “Telecommunications Applications of Discrete Mathematics”, Technology Development Center of Finland, January 2002.

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

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

[4] 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.

[5] 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.

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

[7] A. Hottinen and O. Tirkkonen, ”Square-Matrix Embeddable Space-Time Block Codes for Complex Signal Constellations”, IEEE Transactions on Information Theory, vol. 48 (2), pp. 384–395, February 2002.

[8] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, ”Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels”, IEEE Transactions on Information Theory, vol. 42, pp. 502–518, March 1996.

[9] B. Hassibi, B. M. Hochwald, A. Shokrollahi, and W. Sweldens, ”Representation Theory for High-Rate Multiple-Antenna Code Design”, IEEE Transactions on Information Theory, vol. 47, pp. 2335–2364, September 2001.

[10] 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.

[11] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, ”Diagonal Algebraic Space-Time Block Codes”, IEEE Transactions on Information Theory, vol. 48, pp. 628–636, March 2002.

[12] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, ”Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras”, IEEE Transactions on Information Theory, vol. 49, pp. 2596–2616, October 2003.

[13] J.-C. Belfiore and G. Rekaya, ”Quaternionic Lattices for Space-Time Coding”, ITW2003, Paris, France, March 31 - April 4, 2003.

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

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

[16] J.-C. Belfiore, F. Oggier, G. Rekaya, and E. Viterbo, ”Perfect Space-Time Block Codes”, August 2004. Submitted to IEEE Transactions on Information Theory.

[17] Kiran. T and B. S. Rajan, ”STBC-Schemes with Non-Vanishing Determinant For Certain Number of Transmit Antennas”, August 2004.

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

[19] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, ”Information-Lossless STBCs from Crossed-Product Algebras”, Proc. IEEE ISIT, p. 126, Chicago, June 27- July 2, 2004.

[20] G. Wang, X.-G. Xia, ”On Optimal Multi-Layer Cyclotomis Space-Time Code Designs”, IEEE Transactions on Information Theory (to appear in 2005).

[21] M. O. Damen, H. E. Gamal, and N. C. Beaulieu, ”Linear Threaded Algebraic Space-Time Constellations”, IEEE Transactions on Information Theory, vol. 49, pp. 2372–2388, October 2003.

[22] M. O. Damen and H. E. Gamal, ”Universal Space-Time Coding”, IEEE Transactions on Information Theory, vol. 49, pp. 1097–1119, May 2003.

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

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

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

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

[27] I. Reiner, *Maximal orders*, Academic Press, New York, 1975.

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

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 952-12-1504-6
ISSN 1239-1891