Four Antenna Space-Time Lattice Constellations from Division Algebras

Jarkko Hiltunen, Camilla Hollanti & Jyrki Lahtonen*

March 8, 2005

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

1 Introduction and Background

It is well known [2] that full rate orthogonal designs do not exist for more than two transmit antennas. One must either use non-orthogonal codes, codes of a lower rate, settle for a lower diversity, or place some restrictions on the choice of the components of the input vector. For 4 transmit antennas the best one can do is to use the rate 3/4 orthogonal design from [1] that allows the transmission of 3 complex symbols in 4 time intervals with full diversity.

Examples of full rate and full diversity schemes can be constructed using tools from algebraic number theory. We mention the DAST-lattice (=diagonal algebraic space time code) [5] as an example. In this type of a construction the range of the input vectors must be decided in advance, e.g. the cartesian power of the Gaussian integers $\mathbf{Z}[i]^4$ is a possibility giving full rate. Our construction is similar to DAST in the sense that it achieves full rate and diversity, and that the range of input vectors is constrained to a cartesian power of a two-dimensional lattice in the complex plane. A key tool in our construction is the theory of rings of algebraic integers and their counterparts within the division ring of Hamiltonian quaternions.

1.1 Lattices

A lattice is simply a discrete finitely generated free abelian subgroup L of a real (or complex) finite dimensional vector space 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 L in this ambient space, the so called rank criterion takes the form: any non-zero matrix in L must be invertible. This is because the difference of any two matrices from L is again in L. The receiver and the decoder on the other hand work in the space $\mathbf{C}^n$. When the channel state is h, they expect to see the lattice hL. If $h \neq 0$ and L meets the rank criterion, then hL is, indeed, a free abelian group of the same rank as L. However, it is possible that hL isn't a lattice, as its generators may be linearly dependent over the reals. We call a matrix lattice L *universally proper*, if hL is a lattice for any non-zero channel vector h.

*University of Turku, Department of Mathematics, FIN-20014 Turku, Finland

We easily see that any lattice within the ambient space of an orthogonal design is automatically universally proper. Number theoretic constructions lead to lattices that are not universally proper. For example, for certain non-zero choices of the channel vector the receiver's version of the four antenna DAST-lattice (see [5]) collapses into a dense set within a real vector space of dimension 2. We shall say that a matrix lattice L has *defect* r, if its rank is k, but the minimum real dimension of the span of hL is $k - r$. Thus the lattices constructed from orthogonal designs have zero defect, and the 8-dimensional 4 antenna DAST lattices have defect six. Our goal is to construct rank 8 4×4 matrix lattices of defect four.

The defect is a crude measure of how warped can the geometry of the lattice become in the worst case. Thus it is natural that high defect will make life difficult for the decoder. Indeed, our experience on decoding the lattices of defect 4 and 6 constructed in this paper, suggests that using a suboptimal decoder based on iterative interference cancellation will lose $r/2$ of the antenna diversity.

1.2 Algebraic numbers, quaternions and lattice constructions

It is well-known, how the so called Alamouti design represents multiplication in the ring of quaternions (coordinatized by two complex numbers). As the quaternions form a division algebra, such matrices must be invertible, i.e. the resulting ST-code meets the rank criterion. We generalize this approach to the extension rings of the Gaussian integers $\mathcal{G} = \{a + bi \,|\, a, b \in \mathbf{Z}\}$. It would be easy to adapt the construction to use the ring of the Eisenstein's 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. The natural examples of such rings are the rings of algebraic integers inside an extension field of the fields of quotients of these two rings as well as their counterparts inside the quaternions. We shall concentrate in the interesting case of 4 transmit antennas, and will thus look for extension domains that are also free $\mathcal{G}$- or $\mathcal{E}$-modules of rank 4.

For example, let $\zeta = e^{\pi i/8}$ be a 16^{th} primitive root of unity. Then the ring $\mathbf{Z}[\zeta]$ is a free $\mathcal{G}$-module with a basis $\mathcal{B} = \{1, \zeta, \zeta^2, \zeta^3\}$. Multiplication by $x = c_1 + c_2\zeta + c_3\zeta^2 + c_4\zeta^3$ with respect to this basis then gives rise to the matrices of the following Proposition.

Proposition 1.1. *For a non-zero vector of Gaussian integers $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ the matrix*

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

is invertible. Furthermore, the absolute value of $\det(M_{NF})$ *is then at least 1. The collection of all the matrices $M_{NF}(c_1, c_2, c_3, c_4)$ forms a lattice L_{NF} of rank 8 in $\mathcal{M}_4(\mathbf{C})$.*

As a quaternionic example we consider the following ring. Let ξ be a square root of i, and let j be the usual quaternion satisfying $j^2 = -1, ij = -ji$. Then $\mathcal{O} = \mathbf{Z}[\xi] = R \cdot 1 \oplus R \cdot \xi$ is a free $\mathcal{G}$-module, and the right $\mathcal{G}$-span $\mathbf{H}_\mathcal{O}$ of $\mathcal{B}' = \{1, \xi, j, j\xi\}$ is a subdomain of the quaternions. Let $x = c_1 + c_2\xi + j(c_3 + c_4\xi)$, and let $\lambda : \mathbf{H}_\mathcal{O} \to \mathbf{H}_\mathcal{O}$ be the mapping $q \mapsto xq$. Let us compute the images of the elements of the basis

$$\lambda(1) \;=\; c_1 + \xi c_2 + jc_3 + j\xi c_4$$

$$\begin{aligned}\lambda(\xi) &= c_1\xi + c_2\xi^2 + jc_3\xi + jc_4\xi^2 = ic_2 + \xi c_1 + j(ic_4) + j\xi c_3 \\ \lambda(j) &= c_1 j + c_2\xi j + jc_3 j + jc_4\xi j = -c_3^* + \xi(ic_4^*) + jc_1^* + j\xi(-ic_2^*) \\ \lambda(j\xi) &= c_1 j\xi + c_2\xi j\xi + jc_3 j\xi + jc_4\xi j\xi = -c_4^* + \xi(-c_3^*) + j(c_2^*) + j\xi(c_1^*)\end{aligned}$$

Here we have used the identities $j^2 = -1, \xi^2 = i, \xi^* = -i\xi, zj = jz^*, \forall\, z \in \mathbf{C}$ many times. This time we arrive at the following result

Proposition 1.2. *For a non-zero vector of Gaussian integers $(c_1, c_2, c_3, c_4) \in \mathcal{G}^4$ the matrix*

$$M_{QNF}(c_1, c_2, c_3, c_4) = \begin{pmatrix} c_1 & ic_2 & -c_3^* & -c_4^* \\ c_2 & c_1 & ic_4^* & -c_3^* \\ c_3 & ic_4 & c_1^* & c_2^* \\ c_4 & c_3 & -ic_2^* & c_1^* \end{pmatrix}$$

is invertible. Furthermore, the absolute value of $\det(M_{QNF})$ *is then at least 1. The collection of all the matrices $M_{QNF}(c_1, c_2, c_3, c_4)$ forms a lattice L_{QNF} of rank 8 in $\mathcal{M}_4(\mathbf{C})$.*

We want to draw the reader's attention to the 2×2 block structure of the matrix in Proposition 1.2. If we call the two blocks on the two first columns A and B, we see that the complete matrix has the familiar Alamouti-like structure

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

where, e.g. A^* is the adjoint of the matrix A. Furthermore, the blocks A, A^*, B and B^* represent multiplication in the field F, so they commute, i.e. $AB = BA$.

2 Ideals, defects and product kissing numbers

The best way to use the lattices of Propositions 1.1 and 1.2 is to select the input vectors (c_1, c_2, c_3, c_4) from the coset $\frac{1}{2}(1+i, 1+i, 1+i, 1+i) + \mathbf{Z}[i]^4$. As the difference of any two such vectors will be in $\mathbf{Z}[i]^4$, the conclusions of the propositions will still be valid. So we get the matrix lattices L_{NF} and L_{QNF} consisting of matrices $M_{NF}(c_1, c_2, c_3, c_4)$ and $M_{QNF}(c_1, c_2, c_3, c_4)$ respectively, where (c_1, c_2, c_3, c_4) ranges over the coset mentioned above. Both of these lattices have minimum product distance 1.

A somewhat disappointing fact is that the lattices L_{NF} and L_{QNF} have poor density. Geometrically they look like the 8-dimensional rectangular grid $\mathbf{Z}^8$, which is far from optimal in this sense. Denser lattices can be constructed as sublattices of $\mathbf{Z}^8$, namely the checkerboard lattice D_8 and the root lattice E_8. We next describe a useful sublattice of M_{QNF} isometric to D_8 gotten by restricting the range of the input vectors (c_1, c_2, c_3, c_4) to correspond with a proper ideal of the ring $\mathbf{H}_{\mathcal{O}}$.

Proposition 2.1. *Let $\mathcal{I}$ be the (prime) ideal of the ring $\mathcal{G}$ generated by $1 + i$. Define*

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

Then $\mathbf{H}_{\mathcal{I}}$ *is an ideal of index two in* $\mathbf{H}_{\mathcal{O}}$*. The corresponding index two sublattice*

$$L_{\mathcal{I}} = \{M_{QNF}(c_1, c_2, c_3, c_4) \,|\, c_1 + c_2 + c_3 + c_4 \in \mathcal{I}\}$$

of L_{QNF} *is of minimum product distance* $\sqrt{2}$*.*

Remark 2.1. The minimum product distance of $L_{\mathcal{I}}$ is quite good in the sense that when we scale the lattice to minimum product distance 1, we have to use a scaling factor $\rho = 2^{-1/4}$. Thus the measure of the fundamental region of $\rho L_{\mathcal{I}}$ is only one half of that of L_{QNF}. In other words, the lattice $\rho L_{\mathcal{I}}$ has double density. Therefore we expect the codes constructed from $\rho L_{\mathcal{I}}$ to offer energy savings over L_{QNF}. We shall also show that the product distance distribution of $\rho L_{\mathcal{I}}$ is better.

We proceed to determine the defects of the lattices L_{NF} and L_{QNF}. Let us first consider L_{NF}. Let U be the 4×4-matrix with rows of the form $(1, \zeta^j, \zeta^{2j}, \zeta^{3j})$, for $j = 1, 5, 9, 13$. Let $z = c_1 + c_2\zeta + c_3\zeta^2 + c_4\zeta^3$ be an arbitrary algebraic integer of $\mathbf{Q}(\zeta)$ and $M(z) = M_{NF}(c_1, c_2, c_3, c_4)$ be the corresponding matrix of Proposition 1.1. It is well-known (and easily verified) that the rows of U are (left) eigenvectors of $M(z)$, and $UM(z)U^{-1} = diag\ (z, \sigma_2(z), \sigma_3(z), \sigma_4(z))$ is a diagonal matrix with entries gotten by applying the elements $\sigma_1 = id, \sigma_j, j = 2, 3, 4$ of the Galois group of the extension $\mathbf{Q}(\zeta)/\mathbf{Q}(i)$ to the number z.

So all the matrices $M_{NF}(c_1, c_2, c_3, c_4)$ are diagonalized by U. Therefore we might call the lattice L_{NF} 'DAST-like', as it shares this property with the lattices from [5]. We prefer not to call it a DAST-lattice, as no optimization has been done on this version as opposed to the heavy optimization carried out to produce the lattices of [5]. We then easily see that

Proposition 2.2. *The lattice* L_{NF} *has defect six.*

In order to study the quaternionic lattices we first observe that the 2×2-matrices A and B appearing as blocks of a matrix $M \in L_{QNF}$ 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_{QNF}. If $M = M_{QNF}(c_1, c_2, c_3, c_4)$ then from the proof of Proposition 2.1 we see that the matrix MM^* 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 $k = -ic_1c_2^* + c_2c_1^* - ic_3c_4^* + c_4c_3^*$. Using these observations it is easy to prove that

Proposition 2.3. *The lattices* L_{QNF} *and* $L_{\mathcal{I}}$ *have defect four.*

In addition to the minimum product distance of a code the product distance distribution will always play a role. In an AWGN-channel the number of 'closest' neighbors, or, in the case of a lattice code, the 'kissing number' is a secondary design criterion. In a ST-setting, the 'product kissing number' (cf. [3] for the case of a single antenna fast fading channel) is the natural substitute.

For our lattices the product kissing number unfortunately becomes infinite. For both L_{NF} and L_{QNF}, the matrices at minimum product distance 1 from the origin will be exactly the units of the corresponding ring. From the Dirichlet's theorem of units we may infer that the unit group of L_{NF} has the structure $C_{16} \times C_{\infty}^3$. It is well-known [4] that $M_{NF}(1 + \zeta + \cdots + \zeta^{j-1})$, for $j = 3, 5, 7$ are (independent) multiplicative generators for the torsion-free rank 3 part of this unit group. We shall see shortly that the unit group in the quaternionic lattice L_{QNF} has a free abelian group of rank 1 (as opposed to rank 3) as a subgroup of a finite index. Thus there is every reason to expect that a code within L_{QNF} will have a smaller number of closest neighbors than the corresponding set in L_{NF}.

Lemma 2.4. *Let K be a number field stable under the usual comlex conjugation. Let $\mathcal{O}$ be its ring of integers and let $\mathbf{H}_\mathcal{O}$ be the consisting of the quaternions $q = z_1 + jz_2$. Then q is a unit of $\mathbf{H}_\mathcal{O}$, iff one of the complex coordinates z_1 and z_2 is zero and the other is a unit in $\mathcal{O}$.*

Theorem 2.5. *Let K and $\mathcal{O}$ be as above. Then the unit group G of $\mathbf{H}_\mathcal{O}$ has the unit group $\mathcal{O}^*$ as a subgroup of a finite index. In particular in the case $K = \mathbf{Q}(\xi)$ the group G can be expressed as a direct product*

$$G = C_\infty \times G_0,$$

where C_∞ is generated by the real unit $u = \xi^{-1} + 1 + \xi$ and G_0 is a finite group of order 16 generated by ξ and j.

We feel that this theorem and its consequences for our codes are yet another manifestation of the advantage the quaternionic algebraic constructions have over the real/complex constructions in ST-coding. We also want to emphasize that it is highly unlikely for these results to be unknown to algebraists and/or number theorists. We have included them here for lack of a reference.

3 Decoding and simulation results

Assume that perfect channel state information is available for the receiver. When one of the matrix lattices L of the previous section is used, the decoding problem is more or less equivalent to that of finding the closest point of the lattice hL. Complications arise from the possibility that the lattice hL may have collapsed (or nearly collapsed) into a smaller dimensional subspace, in which case one may be forced to carry out an exhaustive search over a subset of the code. We shall next make a couple of observations that will allow one to speed up decoding no matter what the chosen lattice decoding method is.

The first observation is that knowledge of the minimum distance within hL can be used as a condition to exit from any loop carrying out even a partial search. As our simulations using exhaustive search proved that the codes in L_{QNF} perform better, we concentrate on this lattice. The following bound can be achieved, when knowledge of the channel vector h is taken into account.

Proposition 3.1. *Let C be a subset of the lattice L_{QNF}. Let $V_\pm$ be the complex subspace of $\mathbf{C}^4$ generated be the vectors $(1, \pm\xi, 0, 0)$ and $(0, 0, 1, \pm\xi)$. Assume that $h = h_+ + h_-$, where $h_\pm \in V_\pm$. Let $\gamma = \min\{|h_-|^2, |h_+|^2\}$ and $\delta = ||h_-|^2 - |h_+|^2|$. Let λ be the minimal singular value of the difference of two distinct matrices from C, and let d^2 be the minimum squared Euclidean distance between two vectors from the set hC. Then*

$$d^2 \geq 2\gamma + \delta\lambda.$$

As the Alamouti scheme has a very efficient decoding algorithm available, and our quaternionic lattices have the Alamouti-like block structure, it is natural to ask, if 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 3.2. *Let A and B be two $n \times n$ matrices with the property that the matrices A, B, A^*, B^* commute. Let $h \in \mathbf{C}^{2n}$ be any (row) vector and write*

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

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

Corollary 3.3. *Let A and B range over certain sets of $n \times n$-matrices. Let h and r be vectors in $\mathbf{C}^{2n}$. Then the Euclidean distance between r and $hM(A,B)$ is minimized for the choices $A = A_0$ and $B = B_0$, when A_0 (resp. B_0) minimizes the Euclidean distance between r and $hM(A,0)$ (resp. B_0 minimizes the Euclidean distance between r and $hM(0,B)$).*

We have done computer simulations in a quasi-static complex Rayleigh fading channel. We pitted finite subsets our lattices against rivals of the same size constructed within the 6-dimensional ambient space of the the rate 3/4 orthogonal design using the densest 6-dimensional lattice E_6. At rate 2 bits/s/Hz there were no dramatic differences between the block error rates, except that L_{NF} faired (expectedly) a little bit worse and that the idelic lattice $L_{\mathcal{I}}$ was the winner by approximately 0.5 dB.

At rate 4 bits/s/Hz the difference was more pronounced. The lattice L_{QNF} won over the use of orthogonal design by about 1 dB. This was hardly a surprise, as for codes of this size it was to expected that the elbow room given by a higher rank lattice allowed energy savings. In that simulation we used the lattice $L_{\mathcal{I}}$ only at the rate 3.75 bits/s/Hz (i.e. as an overall parity checked code). That resulted in saving another 1 dB at the cost of a slightly lower rate.

References

[1] V.Tarokh, H. Jafarkhani, and A.R.Calderbank, "Space-time Block Codes from Orthogonal designs," IEEE Transactions on Information Theory, vol. 45, July 1999

[2] 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,

[3] 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, March 1996

[4] T. Metsänkylä, personal communication,

[5] M.O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal Space-Time Block Codes", IEEE Transactions on Information Theory, vol. 48, March 2002