International Symposium on Information Theory and its Applications, ISITA2006
Seoul, Korea, October 29–November 1, 2006

Code Controlled Sphere Decoding of Four Efficient MISO Lattices

Camilla HOLLANTI†

† Department of Mathematics
FIN-20014 University of Turku, Finland
Email: cajoho@utu.fi

Abstract

Previously we have constructed some geometrically dense, full-rank, rate-one matrix lattices with large non-vanishing minimum determinants for 4 transmit antenna MISO applications. In this paper, we will consider the decoding of these lattices. The main concern is not in improving existing algorithms, but in finding a way to decode our lattices that are not as simple in structure, at least not at the first glance, as the majority of previously known ST lattices. We show that the decoding can be efficiently performed by using a modified version of a certain sphere decoding algorithm. We call this method "Code Controlled Sphere Decoding" (CCSD). Our lattice constructions are based on the theory of rings of algebraic integers and related subrings of the Hamiltonian quaternions. Simulations in a quasi-static Rayleigh fading channel have shown that our dense quaternionic constructions outperform the earlier rectangular lattices as well as the DAST-lattice.

1. BACKGROUND AND BASIC DEFINITIONS

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

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

where $\mathbf{x} \in \mathbb{R}^m$, $\mathbf{y}$, $\mathbf{n} \in \mathbb{R}^n$ denote the channel input, output and noise signals, and $\mathbf{B} \in \mathbb{R}^{n\times m}$ 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, the channel matrix takes a form of a vector $\mathbf{b} \in \mathbb{R}^m$.

A *lattice* is 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 $\mathcal{M}_n(\mathbb{C})$ of complex $n \times n$-matrices. When a code is a subset of a lattice L in this ambient space, the *rank criterion* 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. As a main design criterion we recall the *minimum determinant* of the code $\mathcal{C}$. In the case of a square matrix lattice this takes the form

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

where $\mathbf{M}^*$ is the adjoint of the matrix $\mathbf{M}$. When working in the MISO setting, the receiver observes vector lattices instead of matrix lattices. When the channel state is $\mathbf{b}$, the receiver expects to see the lattice $\mathbf{b}L$.

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

$$P(e) \triangleq P(\hat{\mathbf{x}} \neq \mathbf{x})$$

is the maximum-likelihood (ML) detector given by

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}\in\mathbb{Z}_Q^m} |\mathbf{y} - \mathbf{B}\mathbf{x}|^2 \qquad (1)$$

where the components of the noise $\mathbf{n}$ have a common variance equal to 1.

The search in (1) 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 [1], 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 [2]-[5]. 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

This work was supported by the Nokia Foundation, the Foundation for Technical Development, and the Research Foundation of the Rolf Nevanlinna Institute, Finland.

considered, and the initial choice of the sphere radius. We shall use the standard preprocessing and ordering that consist of the *Gram-Schmidt orthonormalization* $\mathbf{B} = (\mathbf{Q}, \mathbf{Q}') \begin{pmatrix} \mathbf{R} \\ \mathbf{0} \end{pmatrix}$ of the columns of the channel matrix $\mathbf{B}$ (equivalently, $\mathbf{QR}$ *decomposition* on $\mathbf{B}$) and the natural back-substitution component ordering given by $x_m, ..., x_1$. The matrix $\mathbf{R}$ is an $m \times m$ upper triangular matrix with positive diagonal elements, $\mathbf{Q}$ (resp. $\mathbf{Q}'$) is an $n \times m$ (resp. $n \times (n-m)$) unitary matrix, and $\mathbf{0}$ is an $(n-m) \times m$ zero matrix.

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

$$|\mathbf{y} - \mathbf{Bx}|^2 \leq C_0 \tag{2}$$

which after applying the $\mathbf{QR}$ decomposition on $\mathbf{B}$ takes the form

$$|\mathbf{y}' - \mathbf{Rx}|^2 \leq C_0', \tag{3}$$

where $\mathbf{y}' = \mathbf{Q}^T\mathbf{y}$ and $C_0' = C_0 - |(\mathbf{Q}')^T\mathbf{y}|^2$. Due to the upper triangular form of $\mathbf{R}$, (3) implies the set of conditions

$$\sum_{j=i}^{m} | \, y_j' - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \, |^2 \leq C_0', \quad i = 1, ..., m. \tag{4}$$

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

$$d^2(\mathbf{y}, \mathbf{Bx}) = \sum_{j=1}^{m} | \, y_j' - \sum_{\ell=j}^{m} r_{j,\ell} x_\ell \, |^2 \tag{5}$$

is minimum. See details in [5]. See also [6].

This work is a continuation of [7] and [8]. The reader interested in more background is referred to [9]-[12].

2. RINGS OF ALGEBRAIC NUMBERS AND LATTICE CONSTRUCTIONS

It is widely known how the so called *Alamouti design* 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 [8] and [13]-[16].

The set $\{a_1 + a_2 i + a_3 j + a_4 k \mid a_i \in \mathbb{R} \, \forall i\}$, where $i^2 = j^2 = k^2 = -1$, $ij = k$, is recalled as the ring of Hamiltonian quaternions. Our constructions use extension rings of the Gaussian integers $\mathcal{G} = \{a + bi \mid a, b \in \mathbb{Z}\}$ inside a given division algebra as they 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 A that are also 4-dimensional vectors spaces over the field $K = \mathbb{Q}(i)$. Let $\zeta = e^{\pi i/4} = (1+i)/\sqrt{2}$ be a primitive 8^{th} root of unity. Our constructions will all lie inside the division algebra $\mathbf{H} = \mathbb{Q}(\zeta) \oplus j\mathbb{Q}(\zeta)$. As $zj = jz^*$ for all complex numbers z, and as the field $\mathbb{Q}(\zeta)$ is stable under the usual complex conjugation $(^*)$, the set $\mathbf{H}$ is a subskewfield of the quaternions.

As always, multiplication (from the left) by a nonzero element of the division algebra 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 A is also invertible. The division algebra $\mathbf{H}$ has $\mathcal{B} = \{1, \zeta, j, j\zeta\}$ as a natural $\mathbb{Q}(i)$-basis and the following representation as a set of matrices over $\mathbb{Q}(i)$. We will refer to the lattice consisting of these matrices $\mathbf{H} =$

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

as the "base" lattice.

Let now $\mathcal{I}$ be the prime ideal of $\mathcal{G}$ generated by $1+i$. Next we will shortly bring back to mind the nested sequence of the four lattices from [8],

$$2\mathbb{Z}^8 = 2L_2 \subseteq L_6 \subseteq L_5 \subseteq L_4 \subseteq L_2 = \mathbb{Z}^8, \tag{6}$$

where

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

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

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

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

These lattices have minimum determinants equal to 1, 4, 16, and 64 respectively. The lattice L_4 is isometric to the checkerboard lattice D_8 while L_5, for its part, is isometric to the direct sum $D_4 \perp D_4$ of two 4-dimensional checkerboard lattices. The lattice L_6 is optimal in the sense that it is isometric to the densest 8-dimensional package, namely to the diamond lattice E_8. For details, see [17].

In [8] two more lattices, namely L_1 and L_3, were introduced. Although they are not of any relevance for this paper, we kept here the same indexing for the sake of consistence.

3. DECODING OF THE NESTED SEQUENCE OF LATTICES

Decoding of the base lattice L_2 can be performed by using the algorithm below proposed in [5]. More detailed information on the function of this algorithm can be found in [5] and [6]. We use the notation from Section 1.

Algorithm II, Smart Implementation (Input C_0', $\mathbf{y}'$, $\mathbf{R}$. 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 $d_c < T_i + |y_i' - \xi_i - r_{i,i}x_i|^2$, 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 $\xi_{i-1} := \sum_{j=i}^{m} r_{i-1,j}x_j$, $T_{i-1} := T_i + |y_i' - \xi_i - r_{i,i}x_i|^2$, $i := i-1$, 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 $d_c := T_1 + |y_1' - \xi_1 - r_{1,1}x_1|^2$, 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 (or the Babai point) point [5]. 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 (6) 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 *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. Section 2). The conditions for the Gaussian elements of the lattices L_2, L_4, L_5, and L_6 can clearly be translated into the following modulo 2 integer conditions. The additional parity check steps will hence be as shown below.

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: $x_1 + x_2 \equiv x_3 + x_4 \equiv x_5 + x_6 \equiv x_7 + x_8$,

$$\sum_{2|i} x_i \equiv \sum_{2\nmid i} x_i \equiv 0 \pmod 2$$

It is also worthwhile to note that these four lattices are in a bijective correspondence with *binary linear codes* 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 determinant of the lattice are somewhat related [8], see Table 1.

Table 1: Lattices from the coding theoretical point of view

The 8-dimensional rectangular grid $\mathbb{Z}^8$ $\leftrightarrow$ 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 diamond lattice E_8 $\leftrightarrow$ extended Hamming-code of length 8

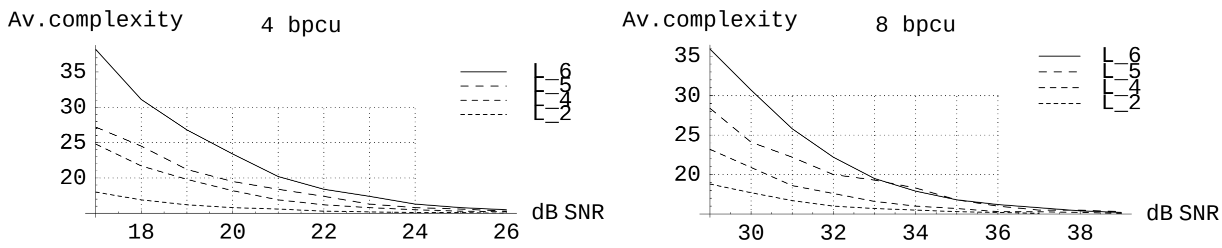

Figure 1: Average complexity of 4 tx-antenna matrix lattices at rates (approximately) 4 and 8 bpcu.

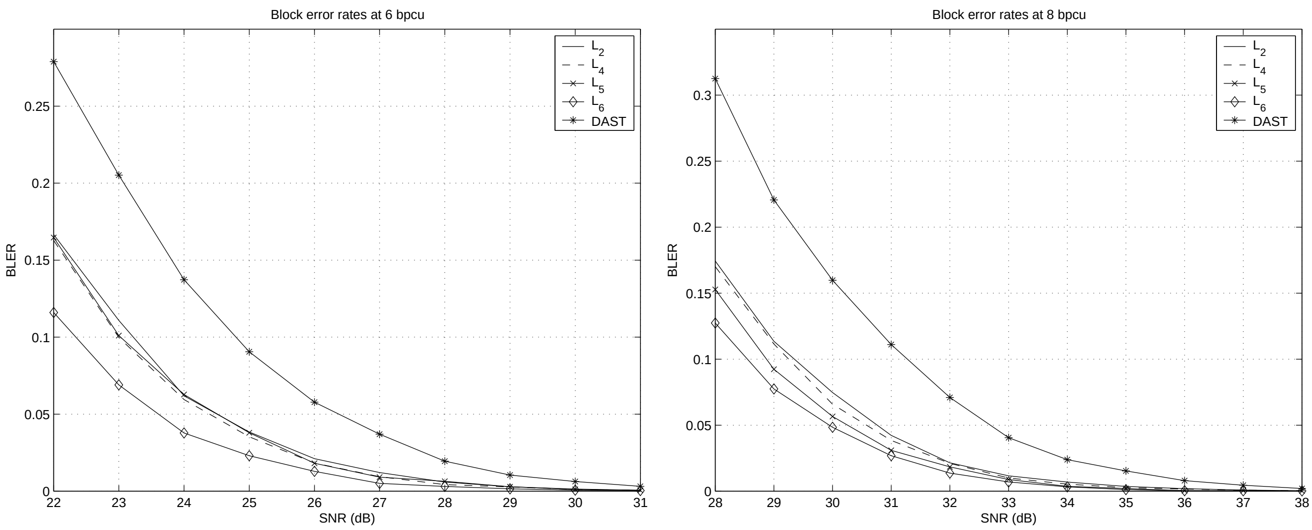

Figure 2: Block error rates of 4 tx-antenna matrix lattices at rates (approximately) 6 and 8 bpcu.

In a MISO setting we say that a matrix lattice L has *defect* r [7], if its rank is m, but the minimum positive real dimension of the span of $\mathbf{b}L$ is $m-r$. For example, for certain non-zero choices of the channel vector the receiver's version of the four antenna DAST-lattice (see [7], [13]) collapses into a dense set within a real vector space of dimension 2. Thus the 8-dimensional 4 antenna DAST lattices have defect six. The lattices $L_t,\ t=2,4,5,6$, have defect four. What comes to decoding complexity, a high defect means bad worst case decoding complexity.

4. SIMULATION RESULTS

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 simulations on the change of complexity of the sphere decoder when moving in (6) from right to left. Due to lack of space we only include here a few.

In Figure 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.

The BLER performance of our codes has been more closely analyzed in [8]. When moving left in (6) the minimum determinant increaces while the BLER decreases at the same time. E.g. simulations at the rate 2 bpcu with one receiver show that the lattice L_6 wins approximately by 1 dB over the lattice L_2, and by 2 dB over the DAST-lattice. However, the other side of the coin is that improvements in performance cause a slightly more complex decoding process and an increased number of points visited in the search tree. See Figure 2 for the BLER performance at higher data rates.

5. CONCLUSIONS

In this paper, we have considered the decoding of some previously constructed lattices. The main concern was not in improving existing algorithms, but in finding a way to decode our lattices that are not necessarily as simple in structure, at least not at the first glance, as the majority of ST lattices. The decoding was efficiently performed by using "Code Controlled Sphere Decoding" (CCSD), a modified version of a certain sphere decoding algorithm. Simulations in a quasi-static Rayleigh fading channel have shown that our dense quaternionic constructions outperform the earlier rectangular lattices as well as the DAST-lattice.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time", IEEE Transactions on Information Theory, vol. 48, no. 7, pp. 1804–1824, July 2002.

[7] J. Hiltunen, C. Hollanti, and J. Lahtonen, "Four Antenna Space-Time Lattice Constellations from Division Algebras", in *Proceedings IEEE ISIT 2004*, p. 338, July 2004.

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

[9] 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.

[10] 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.

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

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

[13] 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.

[14] 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.

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

[16] G. Wang, X.-G. Xia, "On Optimal Multi-Layer Cyclotomic Space-Time Code Designs", *IEEE Transactions on Information Theory*, vol. 51, pp. 1102–1135, March 2005.

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