On the Algebraic Structure of the Silver Code: a 2×2 Perfect Space-Time Block Code

C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, E. Viterbo

***Abstract*— Recently, a family of full-rate, full-diversity space-time block codes (STBCs) for 2×2 multiple-input multiple-output (MIMO) channels was proposed in [1], [2], [3], [4] using a combination of *Clifford algebra* and Alamouti structures, namely *twisted space-time transmit diversity* code. This family was recently rediscovered by Paredes *et al.*, and they pointed out that such STBCs enable reduced-complexity maximum-likelihood (ML) decoding. Independently, the same STBCs were found in [8], and named *multi-strata* space-time codes.**

In this paper we show how this code can be constructed algebraically from a particular cyclic division algebra (CDA). This formulation enables to prove that the code has the non-vanishing determinant (NVD) property and hence achieves the diversity-multiplexing tradeoff (DMT) optimality. The fact that the normalized minimum determinant is $1/\sqrt{7}$ places this code in the second position with respect to the Golden code, which exhibits a minimum determinant of $1/\sqrt{5}$, and motivates the name *Silver code*.

I. Introduction

A family of full-rate, full-diversity STBCs for 2×2 MIMO was recently proposed in [1], [2], [3], [4] using a combination of *Clifford algebra* and Alamouti structures [5], namely *twisted space-time transmit diversity* code. This family was recently rediscovered in [6], where it was also pointed out that such STBCs enable reduced-complexity ML decoding (see also [7] for details). Independently, the same STBCs were found in [8], and named *multi-strata* space-time codes.

In this paper we show how this code can be constructed algebraically from a particular cyclic division algebra. This formulation enables to prove that the code has the non-vanishing determinant (NVD) property [9] and hence achieves the diversity-multiplexing tradeoff (DMT) optimality [10]. The fact that the normalized minimum determinant [11] is $1/\sqrt{7}$ places this code in the second position with respect to the Golden code [9], which exhibits a minimum determinant of $1/\sqrt{5}$, and motivates the name *Silver code*.

By exploiting the algebraic structure of the Silver code we are not, however, able to derive the exact minimum determinant. Instead, we show that the minimum determinant is at least $1/7$, and verify by computer (up to 64–QAM) that the actual normalized minimum determinant is indeed $1/\sqrt{7}$. As in [6] a numerical proof for the minimum determinant (in the QAM case) based on the lattice structure of the Silver code is given, we know that this is indeed the case. The contribution of our paper is to prove that the Silver code has the NVD property, without the need of any technical and lengthy calculations as in [6]. In fact, it is enough to notice that we have a cyclic algebra with a suitable non-norm element [12].

The Silver code was originally designed to have the cubic shaping property of perfect space-time codes [13], but not the non-vanishing determinant property, which was only conjectured after it was verified up to 64–QAM.

C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti are with University of Turku and Turku Centre for Computer Science, Finland. E-mails:{cajoho, lahtonen, kara, roiive}@utu.fi. E. Viterbo is with DEIS - Università della Calabria, Via P. Bucci, 42/C, 87036 Rende (CS), Italy. E-mail: {viterbo}@deis.unical.it. J. Lahtonen and E. Viterbo are also Visiting Fellows at NRC, Helsinki, Finland.

II. System model and notation

We are interested in the coherent $n \times n$ MIMO-case where the receiver perfectly knows the channel coefficients. The $n \times n$ received signal matrix is

$$Y = HX + N,$$

where H is the Rayleigh fading channel response matrix, the elements of the noise matrix N are i.i.d. complex Gaussian random variables and X is the $n \times n$ transmitted codeword taken from the MIMO-lattice $\Lambda \subset \mathcal{M}_n(\mathbf{C})$, the set of $n \times n$ matrices over the complex field $\mathbf{C}$.

A lattice, i.e., a discrete free abelian group, is determined by its basis $X_1, X_2, \ldots, X_k$ consisting of $n \times n$ matrices that are linearly independent over the field of real numbers. The rank k is thus bounded from above by $2n^2$. A lattice is said to have *full rank*, if $k = 2n^2$. We are interested in full-rank lattices since they yield full-rate space-time codes with the maximum multiplexing gain.

The *Gram matrix* of Λ is defined by

$$G = \left(\Re[\mathrm{Tr}(X_i X_j^\dagger)]\right)_{1 \le i,j \le k}$$

where $\Re$ denotes the real part, Tr denotes the trace of the matrix and $\dagger$ denotes Hermitian transposition. The *determinant* of Λ is defined as $\det(\Lambda) = \det(G)$. The measure, or hypervolume, $m(\Lambda)$ of the *fundamental parallelotope* of the lattice is related to the lattice determinant by $\det(\Lambda) = m(\Lambda)^2$.

Given that any $n \times n$ codeword X from a space-time codebook $\mathcal{C} \subseteq \Lambda$ corresponds to a lattice point of Λ, we define the *minimum determinant* of the code as

$$\min_{X \neq X' \in \mathcal{C}} \det(X - X').$$

For the infinite code $\mathcal{C} = \Lambda$ this can be rewritten as

$$\min_{X \in \mathcal{C} \setminus \{0\}} \det(X),$$

since the difference of any two lattice points is again a lattice point.

978-1-4244-2270-8/08/$25.00 ©2008 IEEE

As the minimum determinant determines the asymptotic pairwise error probability (PEP), this gives rise to natural numerical measures for the quality of a code.

If all the codebooks of any size contained in Λ have a minimum determinant bounded from below by a non-zero constant, we say that Λ has the *non-vanishing determinant property* and we define

$$\Delta(\Lambda) = \min_{X \in \Lambda \setminus \{0\}} \det(X)$$

If we consider a scaled lattice $r\Lambda$ for some real constant $r > 0$, we have

$$m(r\Lambda) = r^k m(\Lambda)$$

and

$$\Delta(r\Lambda) = r^n \Delta(\Lambda).$$

We can choose r to normalize either $\Delta(\Lambda) = 1$ or $m(\Lambda) = 1$. In order to define a signal-to-noise ratio we can also choose r so that the entries of the codeword matrices have unit average energy, i.e., $\mathbb{E}(x_{ij}) = 1$.

Following [11], we first scale Λ to have a unit size fundamental parallelotope, and denote by $\delta(\Lambda)$ the *normalized minimum determinant* of the lattice Λ. We omit Λ from the paranthesis, whenever the lattice is clear from the context. To make fair comparisons between the minimum determinants of various codes, one should always use the normalized minimum determinant.

For example, the Golden code has $\delta = 1/\sqrt{5}$, when considering unit hypervolume and $\delta = 4/\sqrt{5}$, when assuming $\pm 1, \pm 3, \ldots$ as integer components for the QAM symbols.

III. The Silver code as a cyclic division algebra

The Silver code S is defined in [1], [2], [3], [4] as

$$S = \{X = X_A + TX_B \mid x_1, x_2, x_3, x_4 \in \mathbf{Z}[i]\},$$

where

$$X_A = X_A(x_1, x_2) = \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix},$$

$$X_B = X_B(z_1, z_2) = \begin{pmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{pmatrix},$$

the twisting matrix

$$T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = U \begin{pmatrix} x_3 \\ x_4 \end{pmatrix}$$

with a unitary matrix

$$U = \frac{1}{\sqrt{7}} \begin{pmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{pmatrix}.$$

We can also think of the code S as a (full) rank 8 lattice $\subseteq \mathcal{M}_2(\mathbf{C})$.

Let us first introduce the basic definitions that are used throughout the paper. In the following, we consider number field extensions E/F, where F denotes the base field and F^* (resp. E^*) denotes the set of the non-zero elements of F (resp. E). Usually, F is an imaginary quadratic field, either $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-3})$ in order to match the QAM and HEX modulation schemes [13]. We assume that E/F is a cyclic field extension of degree n with Galois group $\mathrm{Gal}(E/F) = \langle \sigma \rangle$. Let $\mathcal{A} = (E/F, \sigma, \gamma)$ be the corresponding cyclic algebra of degree n (n is also called the *index* of $\mathcal{A}$), that is

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

as a (right) vector space over E. Here $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ 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

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

We refer to this as the *standard matrix representation* of $\mathcal{A}$ and identify an element of a cyclic division algebra (CDA) with its standard matrix representation.

Definition 3.1: The determinant of the matrix A above is called the *reduced norm* of the element $a \in \mathcal{A}$ and is denoted by $nr(a)$.

The next proposition due to A. A. Albert [14, Theorem 11.12, p. 184] tells us when a cyclic algebra is a division algebra.

Proposition 3.1 (Norm condition): The cyclic algebra $\mathcal{A} = (E/F, \sigma, \gamma)$ of degree n is a division algebra if and only if the smallest factor $t \in \mathbf{Z}_+$ of n such that γ^t is the norm of some element of E^* is n.

Lemma 3.2: The Silver code S is contained as a subset in the cyclic division algebra $\mathcal{A}$ defined as

$$\mathcal{A} = (E/F, \sigma, \gamma),$$

where the center is $F = \mathbf{Q}(\sqrt{-7})$, $E = F(i)$, $\gamma = -1$, and

$$\sigma : \begin{cases} i \mapsto -i \\ \sqrt{7} \mapsto -\sqrt{7}. \end{cases}$$

Proof. As $\sigma(i) = -i = i^*$, the matrix

$$X_A = \begin{pmatrix} x_1 & \gamma\sigma(x_2) \\ x_2 & \sigma(x_1) \end{pmatrix} \in \mathcal{A}.$$

Let us calculate the basis matrices coming from the part TX_B of the code matrix, i.e. we compute $TX_B(z_1, z_2)$, where (x_3, x_4) ranges over the set $\{(1,0), (0,1), (i,0), (0,i)\}$. We end up with the following four basis matrices:

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} -1+i & -2-i \\ 2-i & -1-i \end{pmatrix},$$

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} -2-i & 1-i \\ -1-i & -2+i \end{pmatrix},$$

$$\frac{1}{\sqrt{-7}} \begin{pmatrix} -1-i & -1+2i \\ 1+2i & -1+i \end{pmatrix},$$

$$\frac{1}{\sqrt{-7}}\begin{pmatrix} 1-2i & -1-i \\ 1-i & 1+2i \end{pmatrix}.$$

Here we have written

$$\frac{1}{\sqrt{7}} = \frac{1}{-i\sqrt{-7}} = \frac{i}{\sqrt{-7}}$$

and multiplied i into the matrices. We see that all these basis matrices are of the form

$$\frac{1}{\sqrt{-7}}\begin{pmatrix} a & \gamma\sigma(b) \\ b & \sigma(a) \end{pmatrix},$$

where $a, b \in \mathbf{Z}[i]$. Thus, both summands in $X \in S$ are elements of $\mathcal{A}$ and $X \in \mathcal{A}$.

Now it remains to prove that $\mathcal{A}$ is a division algebra, i.e. (according to A. A. Albert) there does not exist an element $x \in E$ for which $N_{E/F}(x) = -1$.

We shall work in the extension fields of the 2-adic field $\mathbf{Q}_2$. By Hensel's lifting any integer m congruent to 1 modulo 8 has a square root in $\mathbf{Q}_2$. In particular $\sqrt{-7} \in \mathbf{Q}_2$. Thus we can view the field F as a subfield of $\mathbf{Q}_2$. For the sake of being definite we may choose $\sqrt{-7} \equiv 1 \pmod 4$. Similarly, the field E can be viewed as a subfield of $\mathbf{Q}_2(i)$. Furthermore, the norm map $N_{E/F} : E \to F$ is then a restriction of the norm map $N : \mathbf{Q}_2(i) \to \mathbf{Q}_2$, which, obviously, can be defined via the formula $N(a + bi) = a^2 + b^2$ for all $a, b \in \mathbf{Q}_2$.

Thus, in order to prove our claim, it is sufficient to show that -1 is not in the image of the map N. Assume, on the contrary, that there are 2-adic numbers a and b such that $a^2 + b^2 = -1$. We shall first show that then both a and b must be 2-adic integers. So we assume that at least one of them has a negative exponential 2-adic valuation. The non-archimedean triangle inequality then implies that $v_2(a) = v_2(b)$. In other words, there must exist an integer $t < 0$ such that $a = 2^t a'$, $b = 2^t b'$ with a', b' 2-adic units. But then $a'^2 \equiv b'^2 \equiv 1 \pmod 4$, so $v_2(a^2+b^2) = 2t+1$ is an odd integer, and hence $a^2 + b^2$ cannot be a 2-adic unit unless both a and b are 2-adic integers. In this case our claim now easily follows from a modulo 8 consideration: the square of an integer is always congruent to either 0, 1 or 4 modulo 8. Thus the sum of two such squares cannot be congruent to 7 modulo 8. In particular, it cannot be equal to -1. ■

In what follows, we denote the natural order of $\mathcal{A}$ by

$$\Lambda = \mathcal{O}_E \oplus u\mathcal{O}_E,$$

where the ring of integers of E is

$$\mathcal{O}_E = \mathbf{Z}[i] \oplus \frac{1+\sqrt{-7}}{2}\mathbf{Z}[i].$$

For the purposes of constructing MIMO lattices the reason for concentrating on orders is summarized in the following proposition (e.g. [15, Theorem 10.1, p. 125]). We simply rephrase it here in the language of MIMO-lattices.

Proposition 3.3: Let Λ be an order in a cyclic division algebra $(E/F, \sigma, \gamma)$. Then for any non-zero element $a \in \Lambda$ its reduced norm $nr(a)$ is a non-zero element of the ring of integers $\mathcal{O}_F$ of the center F. In particular, if F is an imaginary quadratic number field, then the minimum determinant of the lattice Λ is equal to one.

Theorem 3.4: The Silver code S has a nonvanishing determinant and $\min\det(S) \geq 1/7$.

Proof. When looking at the codeword matrices

$$X = X_A + TX_B \in \Lambda \oplus \frac{1}{\sqrt{-7}}\Lambda,$$

it is obvious that $\sqrt{-7}S \subseteq \Lambda$ and thus $S \subseteq \frac{1}{\sqrt{-7}}\Lambda$. Now

$$\min\det(S) \geq \left|\min\det\left(\frac{1}{\sqrt{-7}}\Lambda\right)\right| = \frac{1}{7}\min\det(\Lambda) = \frac{1}{7}.$$

■

The actual minimum determinant is better than $1/7$, it is equal to $2/\sqrt{7}$ (based on numerical calculations up to 64-QAM) which corresponds to a normalized minimum determinant $1/\sqrt{7}$.

Remark 3.1: In the draft [16] the non-vanishing determinant property is proved numerically in the special cases of PAM and QAM constellations by exploiting just the lattice structure. They derive the normalized minimum determinant $4/\sqrt{7}$ (vs $4/\sqrt{5}$ for the Golden code) for QAM signal constellations.

Our proof extends the NVD property to any signal constellation $\mathcal{X} \subseteq \mathbf{Z}^8$ of an arbitrary size though we do not, at least not yet, get the exact minimum determinant from our algebraic proof. The code generates an ideal in the lattice, and determining this ideal might by the key for solving the problem. At this point, we know that the code is not a principal ideal of the natural (nor any maximal) order.

Here we have shown (at least up to 64-QAM) that $\min\det(S) = 2/\sqrt{7}$, corresponding to a normalized minimum determinant $\delta(S) = 1/\sqrt{7}$, which is only slightly worse than $\delta(G) = 1/\sqrt{5}$ for the Golden code G and well worth the loss due to much simpler decoding it enables.

Remark 3.2: The Silver code is actually a Perfect code [13], as its Gram matrix is orthogonal and the non-norm element is a unit.

IV. Conclusions

We have presented the interesting algebraic structure of the Silver code, a 2×2 perfect space-time code with a non-vanishing minimum determinant $\geq 1/7$. By computer we have verified that the actual normalized minimum determinant is equal to $1/\sqrt{7}$.

This code is very attractive for applications since its error rate performance is only slightly (0.3dB) worse than the one of the Golden code but offers the advantage of reduced complexity decoding.

V. Acknowledgements

This work was supported by the STREP project No. IST-026905 (MASCOT) within the Sixth Framework Programme of the European Commission, by the Academy of Finland through a grant no. 108238 to K. Ranto, by the Finnish Cultural Foundation and the Väisälä Foundation, Finland through grants to C. Hollanti.

REFERENCES

[1] O. Tirkkonen and A. Hottinen, “Square-matrix embeddable space-time block codes for complex signal constellations,” in *IEEE Trans. Inform. Theory*, vol. 48, no. 2, , pp. 384–395, February 2002.

[2] O. Tirkkonen and R. Kashaev, “Combined information and performance optimization of linear MIMO modulations,” in Proc *IEEE Int. Symp. Inform. Theory (ISIT 2002)*, Lausanne, Switzerland, p. 76, June 2002.

[3] A. Hottinen and O. Tirkkonen, “Precoder designs for high rate space-time block codes,” in Proc. *Conference on Information Sciences and Systems*, Princeton, NJ, March 17–19, 2004.

[4] A. Hottinen, O. Tirkkonen and R. Wichman, “Multi-antenna Transceiver Techniques for 3G and Beyound,” WILEY publisher, 2003.

[5] 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.

[6] J. Paredes, A.B. Gershman, and M. Gharavi-Alkhansari, “A 2×2 space-time code with non-vanishing determinants and fast maximum likelihood decoding,” in Proc *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2007)*, Honolulu, Hawaii, USA, pp. 877–880, April 2007.

[7] E. Biglieri, Y. Hong, and E. Viterbo, “On fast-decodable space-time block codes,” submitted to *IEEE Trans. Inform. Theory*, available at http://arxiv.org/abs/0708.2804v1

[8] M. Samuel and M. P. Fitz, “Reducing the detection complexity by using 2×2 Multi-Strata space-time codes,” in Proc *IEEE Int. Symp. Inform. Theory (ISIT 2007)*, pp. 1946–1950, Nice, France, June 2007.

[9] J.-C. Belfiore, G. Rekaya, and E. Viterbo: “The Golden code: A 2x2 full-rate space-time code with non-vanishing determinant”, *IEEE Transactions on Information Theory*, vol. 51, n. 4, pp. 1432–1436, April 2005.

[10] 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.

[11] J. Lahtonen, “Dense MIMO matrix lattices and class field theoretic themes in their construction”, in *Proc. IEEE ITW 2007*, pp. 96–100, Bergen, Norway, July 2007.

[12] Frédérique Oggier, Jean-Claude Belfiore and Emanuele Viterbo (2007) "Cyclic Division Algebras: A Tool for Space-Time Coding", Foundations and Trends in Communications and Information Theory: Vol. 4: No 1, pp 1-95.

[13] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, “Perfect space-time block codes”, *IEEE Trans. Inf. Theory*, vol. 52, pp. 3885–3902, September 2006.

[14] A. A. Albert, *Structure of algebras*, American Mathematical Society, 1939.

[15] I. Reiner, *Maximal orders*, Academic Press, 1975.

[16] J. M. Paredes, A. B. Gersham, and M. Gharavi-Alkhansari, “A new full-rate full-diversity space-time block code with non-vanishing determinants and simplified maximum likelihood decoding”, submitted.