Ideal Structure of the Silver Code

Avik Ray K. Vinodh
Dept. of ECE
Indian Institute of Science
Bangalore, India.
Email: {avik, kvinodh}@ece.iisc.ernet.in

G. Rekaya-Ben Othman
Ecole Nationale Superieure
des Telecommunications
Paris, France.
Email: rekaya@telecom-paristech.fr

P. V. Kumar
Dept. of ECE
Indian Institute of Science
Bangalore, India.
Email: vijay@ece.iisc.ernet.in

***Abstract*—The Silver code has captured a lot of attention in the recent past, because of its nice structure and fast decodability. In their recent paper, Hollanti et al. show that the Silver code forms a subset of the natural order of a particular cyclic division algebra (CDA). In this paper, the algebraic structure of this subset is characterized. It is shown that the Silver code is not an ideal in the natural order but a right ideal generated by two elements in a particular order of this CDA. The exact minimum determinant of the normalized Silver code is computed using the ideal structure of the code. The construction of Silver code is then extended to CDAs over other number fields.**

I. Introduction

A 2×2 perfect space-time code has been proposed in [2], [3], [4], [5] that offers full rate and full diversity, which was also rediscovered in [6] and [7]. Recently, this code has been named as *Silver code* in [1] as it's minimum determinant is slightly less than that of the Golden code [10]. It has been shown that the Silver code has a reduced decoding complexity compared to other full rate and full diversity 2×2 space-time codes (see [8], [9]). In [8], the authors show the non vanishing determinant (NVD) property of the code for M^2-QAM and M-PAM constellations. In [1] Hollanti et al. show that the Silver code is a subset of a particular cyclic division algebra (CDA) and use this fact to prove that the code has NVD property. We shall refer to this CDA as *Silver algebra* in this paper. Hollanti et al. also give a lower bound on the minimum determinant of the normalized Silver code. Our work is motivated by the question in [1], concerning which is the ideal in the Silver algebra that generates the Silver code.

The results in this paper are as follows:

1) The algebraic structure of the Silver code (which is a perfect code) inside the Silver algebra is clarified. It is shown that Silver code is not a principal ideal in the natural order. It is then shown that the Silver code is a right ideal generated by two elements in a particular order of the Silver algebra.
2) The exact minimum determinant of the normalized Silver code is computed using the ideal structure of the code. This also coincides with the results in [8].
3) The Silver code construction is extended to CDAs over other number fields.

Notation: The symbol $|.|$ denotes the absolute value of a complex number. $\Re(.)$and $\Im(.)$ denote the real and imaginary parts of a complex number respectively and complex conjugation is denoted by $(.)^*$. The symbol i denotes $\sqrt{-1}$. The determinant of a matrix is denoted by $\det(.)$. $\mathbb{Q}$ is the set of all rational numbers and $\mathbb{Z}$ is the set of all integers. $\oplus$ denotes the direct sum of modules. $(.)^t$ denotes the transpose of a vector or a matrix.

We first provide a small introduction to cyclic division algebras.

II. Cyclic Division Algebras

Division algebras are rings with identity element in which every nonzero element has a multiplicative inverse. The center $\mathbb{F}$ of any division algebra D, i.e., the subset comprising of all elements in D that commute with every element of D, is a field. A cyclic division algebra (CDA) is a division algebra in which the center $\mathbb{F}$ and a maximum subfield $\mathbb{L}$ are such that $\mathbb{L}/\mathbb{F}$ is a finite cyclic Galois extension. In this paper, $\mathbb{F}$, $\mathbb{L}$ are number fields, with the degree of extension of $\mathbb{L}$ over $\mathbb{F}$ being n (also known as the index of the CDA). Let $\mathcal{O}_{\mathbb{F}}$ and $\mathcal{O}_{\mathbb{L}}$ denote the ring of algebraic integers of $\mathbb{F}$ and $\mathbb{L}$ respectively. Let σ denote the generator of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Let u be an indeterminate satisfying

$$\ell u \;=\; u\sigma(\ell) \quad \forall \;\; \ell \in \mathbb{L} \qquad \text{and} \qquad u^n = \gamma, \tag{1}$$

for some $\gamma \in \mathbb{F}^*$ such that $\gamma, \gamma^2, \ldots, \gamma^{n-1}$ are non-norm elements of $\mathbb{F}^*$. Then, a CDA $D(\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ with index n, center $\mathbb{F}$ and maximal subfield $\mathbb{L}$ is the set of all elements of the form

$$\sum_{i=0}^{n-1} u^i \ell_i, \quad \ell_i \in \mathbb{L}. \tag{2}$$

Every element in the CDA D has the matrix representation of the form,

$$\begin{bmatrix} \ell_0 & \gamma\sigma(\ell_{n-1}) & \gamma\sigma^2(\ell_{n-2}) & \ldots & \gamma\sigma^{n-1}(\ell_1) \\ \ell_1 & \sigma(\ell_0) & \gamma\sigma^2(\ell_{n-1}) & \ldots & \gamma\sigma^{n-1}(\ell_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \ell_{n-1} & \sigma(\ell_{n-2}) & \sigma^2(\ell_{n-3}) & \ldots & \sigma^{n-1}(\ell_0) \end{bmatrix}, \tag{3}$$

which is known as its left regular representation. A space-time (ST) code $\mathcal{X}$ can be associated to D by selecting the set of matrices corresponding to the matrix representation of elements of a finite subset of D. In this paper, we use the term space-time code for both the matrix and its representation in

the division algebra interchangeably, which will be clear from the context.

We now give the definition of an order in a division algebra. Let R denote a Noetherian integral domain with a quotient field F, and let $\mathcal{A}$ be a finite dimensional F-algebra.

Definition 1 *An R-order in the F-algebra $\mathcal{A}$ is a subring Λ of $\mathcal{A}$, having the same identity element as $\mathcal{A}$, and such that Λ is a finitely generated module over R and generates $\mathcal{A}$ as a linear space over F. An order Λ is called maximal, if it is not properly contained in any other R-order.*

Example Natural Order: The set of elements of the CDA D of the form,

$$\sum_{i=0}^{n-1} u^i \ell_i, \quad \ell_i \in \mathcal{O}_{\mathbb{L}} \ . \tag{4}$$

is an $\mathcal{O}_{\mathbb{F}}$-order of D known as its natural order.

III. Silver Code

A. Definition of Silver Code

The Silver code is given by the set of all matrices of the form,

$$X = \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{bmatrix} , \tag{5}$$

where,

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

and U is a unitary matrix given by,

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

Here $\{x_i\}_{i=1}^4$ are the information symbols drawn from a subset of the Gaussian integers $\mathbb{Z}[i]$.

B. Silver Algebra

The Silver algebra [1] is given by, $\mathbb{D} = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ where $\mathbb{F} = \mathbb{Q}(\sqrt{-7})$ is the center, $\mathbb{L} = \mathbb{F}(i)$ is the maximal subfield, $\gamma = -1$ is the non-norm element and σ is the generator of the Galois group of $\mathbb{L}/\mathbb{F}$ given by,

$$\sigma : \begin{cases} i & \rightarrow & -i \\ \sqrt{7} & \rightarrow & -\sqrt{7} \end{cases} . \tag{6}$$

(See Figure below). The ring of integers of $\mathbb{L}$ is $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[i, \theta]$, where $\theta = \frac{1+\sqrt{-7}}{2}$. The minimal polynomial of θ is $x^2 - x + 2$.

$$\begin{array}{ccc} \mathbb{D} & & \mathcal{O}_{\mathbb{L}} + u\mathcal{O}_{\mathbb{L}} \\ | & & | \\ \mathbb{L} = \mathbb{Q}(i, \sqrt{-7}) & & \mathbb{Z}[i, \theta] \quad = \mathcal{O}_{\mathbb{L}} \\ | & & | \\ \mathbb{F} = \mathbb{Q}(\sqrt{-7}) & & \mathbb{Z}[\theta] \\ | & & | \\ \mathbb{Q} & & \mathbb{Z} \end{array} \tag{7}$$

A typical element ℓ in the Silver algebra is of the form, $\ell = \ell_0 + u\ell_1$ where, $\ell_0, \ell_1 \in \mathbb{L}$ and $u^2 = -1$. The matrix representation of ℓ is given by,

$$X_\ell = \begin{bmatrix} \ell_0 & -\sigma(\ell_1) \\ \ell_1 & \sigma(\ell_0) \end{bmatrix}. \tag{8}$$

IV. Algebraic structure of the Silver code

A. Representation of Silver code as an element of the Silver algebra

In this subsection, we obtain a representation of the Silver code within the Silver algebra. Consider the Silver code described in section III. The codewords are given by,

$$X = \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{bmatrix} . \tag{9}$$

We can observe that,

$$\begin{bmatrix} z_1 & -z_2^* \\ z_2 & z_1^* \end{bmatrix} = \frac{1}{\sqrt{7}} \begin{bmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{bmatrix} \begin{bmatrix} x_3 & -x_4^* \\ x_4 & x_3^* \end{bmatrix} \tag{10}$$

Substituting the above relation in (9) and multiplying both sides of the equation by $\sqrt{-7}$ we get,

$$\begin{aligned} &\sqrt{-7}X \\ &= \begin{bmatrix} \sqrt{-7} & 0 \\ 0 & \sqrt{-7} \end{bmatrix} \begin{bmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{bmatrix} \\ &\quad + \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 1+i & -1+2i \\ 1+2i & 1-i \end{bmatrix} \begin{bmatrix} x_3 & -x_4^* \\ x_4 & x_3^* \end{bmatrix} \end{aligned} \tag{11}$$

Replacing all the matrices in the above equation by their representation in the division algebra $\mathbb{D}$ we get,

$$\sqrt{-7}x = \sqrt{-7}(x_1 + ux_2) + i\left[(1+i) + u(1+2i)\right](x_3 + ux_4) , \tag{12}$$

where $\{x_i\}_{i=1}^4 \in \mathbb{Z}[i]$ and x is the representation of X in $\mathbb{D}$. Let $\mathcal{S}$ be the set of all elements in $\mathbb{D}$ of the form defined by the above equation. Henceforth, we refer to the set $\mathcal{S}$ as the Silver code, which is just a scaled version of the Silver code as defined by (5).

Through equation (12) we can see that the Silver code $\mathcal{S}$ is a subset of the Silver algebra. We will now define the exact structure of this subset. Also, one of the open questions in [1] was "what is the ideal that generates the Silver code". We will prove that unlike other known perfect codes (see [11], [12]), the Silver code is not an ideal in the natural order whereas it is a right ideal generated by two elements in a particular order of the Silver algebra.

B. Silver code as a module

The Silver code S (see (12)) is given by,

$$\begin{aligned} \mathcal{S} \quad = \quad & \big\{\sqrt{-7}(x_1 + ux_2) \\ & + i\left[(1+i) + u(1+2i)\right](x_3 + ux_4) \mid \{x_i\}_{i=1}^4 \in \mathbb{Z}[i]\big\} \end{aligned} \tag{13}$$

We define

$$a \ := \ \sqrt{-7} \tag{14}$$

$$b \ := \ i[(1+i) + u(1+2i)] . \tag{15}$$

Then we see that $\mathcal{S}$ is a right module over $\mathbb{Z}[i]$, generated by the elements of the set $\mathcal{B}_s = \{a, au, b, bu\}$. Moreover, $\mathcal{S}$ is a direct sum of the right modules $a\mathbb{Z}[i], au\mathbb{Z}[i], b\mathbb{Z}[i], bu\mathbb{Z}[i]$

as the elements a, au, b, bu are linearly independent over $\mathbb{Z}[i]$ i.e.,

$$\mathcal{S} = a\mathbb{Z}[i] \oplus au\mathbb{Z}[i] \oplus b\mathbb{Z}[i] \oplus bu\mathbb{Z}[i]. \quad (16)$$

C. Silver code as an Ideal

Before proving that the Silver code is an ideal we first prove the following lemma.

Lemma 1 *The Silver code is not an ideal in the natural order of the Silver algebra.*

Proof: The proof is by contradiction. The natural order of the Silver algebra is given by

$$\begin{aligned} \Lambda &= \mathcal{O}_{\mathbb{L}} + u\mathcal{O}_{\mathbb{L}} & (17)\\ &= \mathbb{Z}[i,\theta] + u\mathbb{Z}[i,\theta] & (18)\end{aligned}$$

Let us suppose that Silver code $\mathcal{S}$ is an ideal in the order Λ. Consider the element $\theta \in \Lambda$ and $a \in \mathcal{S}$. We can write $a = \sqrt{-7} = 2\theta - 1$. Since $\mathcal{S}$ is an ideal in Λ, $\theta a \in \mathcal{S}$. Now,

$$\begin{aligned} \theta a &= 2\theta^2 - \theta & (19)\\ &= 2(\theta - 2) - \theta & (20)\\ &= \theta - 4 & (21)\end{aligned}$$

Since $\theta a \in \mathcal{S}$ we can represent it in the basis $\mathcal{B}_s$ over $\mathbb{Z}[i]$ (see (16)). Thus,

$$\theta a = ac_1 + auc_2 + bc_3 + buc_2 \quad (22)$$

for some $\{c_i\}_{i=1}^4 \in \mathbb{Z}[i]$. Substituting (21) in the above equation we get,

$$\theta - 4 = ac_1 + auc_2 + bc_3 + buc_4 \quad (23)$$

$$\frac{-7}{2} + \frac{\sqrt{-7}}{2} = \sqrt{-7}c_1 + \sqrt{-7}uc_2 + bc_3 + buc_4 \quad (24)$$

Note that the division algebra D is a right vector space over $\mathbb{Q}(i)$ with the basis $\{1, u, \sqrt{-7}, \sqrt{-7}u\}$. Now, comparing the coefficients of $\sqrt{-7}$ on both sides of the above equation, we get $c_1 = \frac{1}{2}$ which contradicts the fact that $c_1 \in \mathbb{Z}[i]$. Hence the Silver code cannot occur as an ideal in the natural order of the Silver algebra. □

In fact, any code which occurs as a principal ideal in the natural order of the Silver algebra cannot be a perfect code (Please see Appendix for the proof).

Now consider the $\mathbb{Z}$-order $\mathcal{R} = \mathbb{Z}[i,a] + u\mathbb{Z}[i,a]$ of the Silver algebra which is strictly contained in the natural order $\mathcal{O}_{\mathbb{L}} + u\mathcal{O}_{\mathbb{L}}$. Then we have the following theorem.

Theorem 1 *The Silver code $\mathcal{S}$ is a right ideal generated by the elements a and b in the order $\mathcal{R}$ of the Silver algebra i.e.,*

$$\mathcal{S} = a\mathcal{R} + b\mathcal{R} \ . \quad (25)$$

Proof: Let $T = \mathbb{Z}[i] + u\mathbb{Z}[i]$. Then from (16) the Silver code can be written as $\mathcal{S} = aT + bT$. Since the order $\mathcal{R} = \mathbb{Z}[i,a] + u\mathbb{Z}[i,a]$ we can write $\mathcal{R} = T + aT$. Now consider the right ideal generated by a and b in the order $\mathcal{R}$ i.e., $a\mathcal{R} + b\mathcal{R}$. We have,

$$\begin{aligned} a\mathcal{R} + b\mathcal{R} &= a(T + aT) + b(T + aT) & (26)\\ &= aT + -7T + bT + baT & (27)\end{aligned}$$

where we substituted $a^2 = -7$. The elements -7 and ba can be written as

$$\begin{aligned} -7 &= b(1+i) + bu(2-i) & (28)\\ ba &= a[(-1+i) + u(2-i)]. & (29)\end{aligned}$$

Since $T = \mathbb{Z}[i] + u\mathbb{Z}[i]$ we have,

$$\begin{aligned} -7T &= b(1+i)(\mathbb{Z}[i] + u\mathbb{Z}[i]) + bu(2-i)(\mathbb{Z}[i] + u\mathbb{Z}[i])\\ &\subseteq b(\mathbb{Z}[i] + u\mathbb{Z}[i]) + b(\mathbb{Z}[i] + u\mathbb{Z}[i])\\ &= bT & (30)\\ \text{and } baT &= abT \ \text{ (a commutes with all elements)}\\ &= a[(-1+i) + u(2-i)](\mathbb{Z}[i] + u\mathbb{Z}[i])\\ &\subseteq aT & (31)\end{aligned}$$

Thus from (30) and (31) we have $-7T \subseteq bT$ and $baT \subseteq aT$. Substituting these expressions in (27) we get,

$$\begin{aligned} a\mathcal{R} + b\mathcal{R} &= aT + bT & (32)\\ &= \mathcal{S} & (33)\end{aligned}$$

where we have used the fact that if $(R, +, .)$ is a ring, X and Y are two subrings of R and $Y \subseteq X$, then $X + Y = X$.

Thus the Silver code $\mathcal{S}$ is a right ideal generated by a and b in $\mathcal{R}$. In order to prove that $\mathcal{S}$ is not a two sided ideal, it can be shown that $ub \notin \mathcal{S}$ wherein $u \in \mathcal{R}$ and $b \in \mathcal{S}$.

V. Silver code is not a principal ideal

We first compute the reduced norm of various elements of the Silver algebra which will be used to prove that Silver code is not a principal ideal in the order $\mathcal{R}$.

A. Reduced Norm of elements of the Silver algebra

Definition 2 *Let x be an element of a cyclic division algebra D and X be its matrix representation as described in* (3)*. Then the reduced norm of x, denoted by $nr(x)$ is,*

$$nr(x) = \det(X) \ . \quad (34)$$

Consider an element $\ell = \ell_0 + u\ell_1$ in the Silver algebra $\mathbb{D}$. Then using the matrix representation of ℓ given by (8), we calculate the reduced norm of ℓ to be,

$$\begin{aligned} nr(\ell) &= \det(X_\ell) & (35)\\ &= \ell_0\sigma(\ell_0) + \ell_1\sigma(\ell_1) & (36)\\ &= N_{\mathbb{L}/\mathbb{F}}(\ell_0) + N_{\mathbb{L}/\mathbb{F}}(\ell_1) & (37)\end{aligned}$$

where $N_{\mathbb{L}/\mathbb{F}}(.)$ is the relative norm of an element in $\mathbb{L}$.

Reduced norm of an element in $\mathcal{R}$: Let $r \in \mathcal{R}$. Recall $\mathcal{R} = \mathbb{Z}[i,a] + u\mathbb{Z}[i,a]$. Let $r = r_1 + ur_2$ where $r_1, r_2 \in \mathbb{Z}[i,a]$. Then $N_{\mathbb{L}/\mathbb{F}}(r_1), N_{\mathbb{L}/\mathbb{F}}(r_2) \in \mathbb{F} \cap \mathbb{Z}[i,a] = \mathbb{Z}[a]$. Thus, from (37) the reduced norm of r is,

$$\begin{aligned} nr(r) &= N_{\mathbb{L}/\mathbb{F}}(r_1) + N_{\mathbb{L}/\mathbb{F}}(r_2) & (38)\\ &= c_1 + ac_2 & (39)\end{aligned}$$

where $c_1, c_2 \in \mathbb{Z}$.

Proposition 1 *Let $\mathbb{K}$ be a degree-2 extension of the field $\mathbb{F}$. Let $a, b \in \mathbb{K}$. Then,*

$$N_{\mathbb{K}/\mathbb{F}}(a+b) = N_{\mathbb{K}/\mathbb{F}}(a) + N_{\mathbb{K}/\mathbb{F}}(b) + Tr_{\mathbb{K}/\mathbb{F}}(a\sigma(b)) \quad (40)$$

where $N_{\mathbb{K}/\mathbb{F}}(.)$ and $Tr_{\mathbb{K}/\mathbb{F}}(.)$ denotes the norm and trace respectively.
We shall now prove a useful lemma.

Lemma 2 *The reduced norm of an element in the ideal $\mathcal{S}$ is of the form $7k_1 + 2ak_2$ where $k_1, k_2 \in \mathbb{Z}$.*
Proof: Let x be an element of the ideal $\mathcal{S}$. Then using (16), x can be written as,

$$x = ax_1 + aux_2 + bx_3 + bux_4 \quad (41)$$

where $\{x_i\}_{i=1}^4 \in \mathbb{Z}[i]$. Since $b = (-1+i) + u(2-i)$ we can rewrite the above equation as,

$$\begin{aligned} x &= ax_1 + aux_2 + [-1+i+u(2-i)]x_3 \\ &\quad +[-2-i+u(-1-i)]x_4 \\ &= [ax_1 + (-1+i)x_3 - (2+i)x_4] + \\ &\quad u[ax_2 + (2-i)x_3 - (1+i)x_4] \end{aligned} \quad (42)$$

Then the reduced norm of x is given by,

$$\begin{aligned} nr(x) &= N_{\mathbb{L}/\mathbb{F}}(ax_1 + (-1+i)x_3 - (2+i)x_4) \\ &\quad + N_{\mathbb{L}/\mathbb{F}}(ax_2 + (2-i)x_3 - (1+i)x_4) \end{aligned} \quad (43)$$

Applying Proposition 1 to the above equation we get,

$$\begin{aligned} nr(x) &= 7(|x_3|^2 + |x_4|^2 - |x_1|^2 - |x_2|^2) + 2a\Re(c) \\ &= 7k_1 + 2ak_2 \end{aligned} \quad (44)$$

where $c = ((-1+i)x_3 - (2+i)x_4)x_1^* + ((2-i)x_3 - (1+i)x_4)x_2^*,\ c \in \mathbb{Z}[i], k_1 = (|x_3|^2 + |x_4|^2 - |x_1|^2 - |x_2|^2), k_2 = \Re(c),\ k_1, k_2 \in \mathbb{Z}$. □

Now coming back to the ideal structure of the Silver code we prove the following lemma:

Lemma 3 *The Silver code $\mathcal{S}$ is not a principal ideal in $\mathcal{R}$.*
Proof: Again the proof is by contradiction. Assume that $\mathcal{S}$ is a principal ideal in $\mathcal{R}$ generated by an element $c \in \mathcal{S}$. Let $nr(c) = c_1 + ac_2$, where $nr(c)$ is the reduced norm of c and $c_1, c_2 \in \mathbb{Z}$. Since c is the generator of $\mathcal{S}$ which is a right ideal we must have,

$$a = cf \quad (45)$$

$$b = cg \quad (46)$$

for some $f, g \in \mathcal{R}$. Taking the reduced norms of equation (45) we get,

$$nr(a) = nr(c)nr(f) \quad (47)$$

$$-7 = (c_1 + ac_2)(f_1 + af_2) \quad (48)$$

where $nr(f) = (f_1 + af_2),\ f_1, f_2 \in \mathbb{Z}$ since $f \in \mathcal{R}$. Also $c \in \mathcal{S}$, therefore its reduced norm must be of the form $7k_1 + 2ak_2,\ k_1, k_2 \in \mathbb{Z}$. Now, taking magnitude square of the above equation we have,

$$49 = (49k_1^2 + 28k_2^2)(f_1^2 + 7f_2^2) \quad (49)$$

where $c_1 = 7k_1, c_2 = 2k_2,\ k_1, k_2, f_1, f_2 \in \mathbb{Z}$. The only solution to the above equation is $k_1 = \pm 1, k_2 = 0, f_1 = \pm 1, f_2 = 0$. This implies $nr(c) = \pm 7$ and $nr(f) = \pm 1$, i.e., f is a unit in $\mathcal{R}$. Similarly from equation (46) we obtain $nr(g) = \pm 1$ i.e., g is also an unit in $\mathcal{R}$. Now, for an unit $x \in \mathcal{R}$ such that $nr(x) = \pm 1$, if $x = x_1 + ux_2$, then $x^{-1} = \pm(\sigma(x_1) - ux_2)$ and thus $x^{-1} \in \mathcal{R}$. Therefore $f^{-1}, g^{-1} \in \mathcal{R}$. Now we have from equations (45) and (46), $c = f^{-1}a$ and $c = g^{-1}b$. Therefore,

$$bg^{-1} = af^{-1} \quad (50)$$

$$b = af^{-1}g \quad (51)$$

$$b = ae \quad (52)$$

where $e = f^{-1}g$ is an unit in $\mathcal{R}$. Let $e = e_1 + ue_2,\ e_1, e_2 \in \mathbb{Z}[i, a]$. Then we get,

$$b = a(e_1 + ue_2) \quad (53)$$

$$(-1+i) + u(2-i) = ae_1 + uae_2 \quad (54)$$

implying,

$$-1 + i = e_1 a \quad (55)$$

Taking magnitude of the reduced norm of $-1+i$ and $e_1 a$ we get,

$$2 = 7|nr(e_1)| \quad (56)$$

a contradiction because $|nr(e_1)| \geq 1$ (using (39)). Hence $\mathcal{S}$ is not a principal ideal of the ring $\mathcal{R}$. □

VI. Minimum determinant of the Silver code

In [1], Hollanti et al., obtained a lower bound on the minimum determinant of the normalized Silver code $\mathcal{S}$ to be $\frac{1}{14}$, using the fact that the Silver code is a subset of the natural order of the Silver algebra $\mathbb{D}$. But the actual minimum determinant verified both by numerical computation and analytical derivation for M^2-QAM constellation was only $\frac{1}{\sqrt{7}}$ (see [8]). We will now argue using the algebraic structure of the Silver code that the minimum determinant for the normalized Silver code is in fact $\frac{1}{\sqrt{7}}$ for any constellation over $\mathbb{Z}[i]$.

Lemma 4 *The minimum determinant of the normalized code matrix of the Silver code $\mathcal{S}$ is $\frac{1}{\sqrt{7}}$ for any constellation over $\mathbb{Z}[i]$.*
Proof: We have seen that the Silver code $\mathcal{S}$ is a right ideal in the order $\mathcal{R}$. The determinant of the Silver code matrix is nothing but the reduced norm of the corresponding element in the ideal $\mathcal{S}$. From lemma 2 we know that the reduced norm of any element $x \in \mathcal{S}$ is of the form $7k_1 + 2ak_2,\ k_1, k_2 \in \mathbb{Z}$. Hence the absolute value of the determinant of the corresponding code matrix X of x is of the form,

$$|\det(X)| = |nr(x)| = \sqrt{49k_1^2 + 28k_2^2} \geq \sqrt{28} = 2\sqrt{7} \quad (57)$$

since both k_1, k_2 cannot be equal to 0. After energy normalization of the code matrix X we get,

$$|\det(\frac{1}{\sqrt{14}}X)| \geq \frac{2\sqrt{7}}{14} = \frac{1}{\sqrt{7}}. \quad (58)$$

This bound is also tight, and is attained by the element $x = a(-1-u) + b(-1+ui) \in \mathcal{S}$. □

VII. Generalized Silver code constructions

Codes from CDAs over other number fields:

Let d be a positive integer such that $d \equiv 7$ modulo 8. Then the Silver code construction can be generalized to other CDAs of the form $\mathbb{D}_d = (\mathbb{L}/\mathbb{F}, \sigma, \gamma)$ where $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$ is the center, $\mathbb{L} = \mathbb{F}(i)$ is the maximal subfield, $\gamma = -1$ is the non-norm element (see [1]) and the generator of the Galois group of $\mathbb{L}/\mathbb{F}$ is σ given by,

$$\sigma : \left\{ \begin{array}{ccc} i & \rightarrow & -i \\ \sqrt{d} & \rightarrow & -\sqrt{d} \end{array} \right. . \tag{59}$$

Consider a 2×2 space-time code from this CDA of the form,

$$\begin{aligned} \mathcal{X}_d &= \Big\{ \sqrt{-d}(x_1 + ux_2) \\ &\quad + [p + uq]\,(x_3 + ux_4) \mid \{x_i\}_{i=1}^4 \in \mathbb{Z}[i] \Big\} \end{aligned}$$

where $p, q \in \mathbb{Z}[i]$ such that,

$$|p|^2 + |q|^2 = d \tag{60}$$

From Lagrange's four square theorem it is clear that we can always find $p, q \in \mathbb{Z}[i]$ such that the above equation is satisfied for any $d > 0$. It can be verified that the code $\mathcal{X}_d$ is a perfect code. The code $\mathcal{X}_d$ has a normalized minimum determinant of $\frac{1}{\sqrt{d}}$. The code having best minimum determinant in this family is the Silver code $\mathcal{S}$.

Example: Let $d = -23$. Then,

$$\begin{aligned} \mathcal{X}_{23} &= \big\{ \sqrt{-23}(x_1 + ux_2) \\ &\quad + [(3+3i) + u(1+2i)]\,(x_3 + ux_4) \mid \{x_i\}_{i=1}^4 \in \mathbb{Z}[i] \big\} \end{aligned}$$

is a 2×2 perfect space time code with normalized minimum determinant of $\frac{1}{\sqrt{23}}$.

VIII. Appendix

Perfect Codes from principal ideals in the natural order of the Silver algebra is not possible:

We show that if we choose a space time code from a principal ideal in the natural order of the Silver algebra then it cannot have cubic shaping and hence cannot be a prefect code.

Definition 3 *Cubic Shaping: Consider a linear $n \times n$ space-time code with $2K$ real information symbols of the form $X = \sum_{i=1}^{2K} A_i x_i$. Here A_i are constant $n \times n$ matrices. The real vectorized version of the code can then be written as,*

$$\widehat{vec(X)} = G\mathbf{x} \tag{61}$$

where $\mathbf{x} = [x_1 x_2, \ldots, x_{2K}]^t$ and G is the real generator matrix. The space time code is said to have cubic shaping if $GG^t = \kappa I$ for some real κ.

First we prove the following lemma.

Lemma 5 *Any space-time code from a principal ideal in the natural order of the Silver algebra cannot have cubic shaping.*

Proof: We prove the lemma only for principal right ideals and the proof for principal left ideals is along the similar lines. The proof is by contradiction. The natural order of the Silver algebra is $\Lambda = \mathcal{O}_{\mathbb{L}} + u\mathcal{O}_{\mathbb{L}}$. Consider a principal right ideal $\alpha\Lambda$ where $\alpha \in \Lambda$. Let $\alpha = \alpha_1 + u\alpha_2$, $\alpha_1, \alpha_2 \in \mathbb{Z}[i, \theta]$. Then the matrix representation of any element in this ideal is given by,

$$X = \left[\begin{array}{cc} \alpha_1\ell_0 - \sigma(\alpha_2)\ell_1 & -\alpha_1\sigma(\ell_1) - \sigma(\alpha_2)\sigma(\ell_0) \\ \sigma(\alpha_1)\ell_1 + \alpha_2\ell_0 & \sigma(\alpha_1)\sigma(\ell_0) - \alpha_2\sigma(\ell_1) \end{array} \right] \tag{62}$$

where $\ell_0, \ell_1 \in \mathbb{Z}[i, \theta]$. Let $\ell_0 = x_1 + \theta x_2, \ell_1 = x_3 + \theta x_4, \{x_i\}_{i=1}^4 \in \mathbb{Z}[i]$. Let $\mathbf{x} = [\Re(x_1), \Im(x_1), \Re(x_2), \ldots, \Im(x_4)]^t$. The inner product between the first and third columns of the real generator matrix of X is given by,

$$\begin{aligned} G(1)^t G(2) &= \Re[\theta(|\alpha_1|^2 + |\alpha_2|^2 + |\sigma(\alpha_1)|^2 + |\sigma(\alpha_2)|^2)] \\ &> 0 \end{aligned} \tag{63}$$

since both α_1, α_2 are not zero. Hence a code from the principal ideal of the natural order cannot have cubic shaping. □

Acknowledgment

This research is supported by the DRDO-IISc Program on Advanced Research in Mathematical Engineering.

References

[1] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, and E. Viterbo, "On the Algebraic Structure of the Silver Code," *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[2] O. Tirkkonen and A. Hottinen, " Square-matrix Embeddable Space-Time Block Codes for Complex Signal Constellations" *IEEE Trans. Inform. Theory*, vol. 48, no. 2, Feb. 2002.

[3] O. Tirkkonen and R. Kashaev, "Combined Information and Performance Optimization of Linear MIMO Modulations", *Proc IEEE Int. Symp. Inform. Theory* (ISIT 2002), Lausanne, Switzerland, June 2002.

[4] A. Hottinen and O. Tirkkonen,"Precoder Designs for High Rate Space-Time Block Codes" in *Proc Conf.on Information Sciences and Systems*, Princeton, NJ, March 2004.

[5] A. Hottinen, O. Tirkkonen and R. Wichmann, " Multi Antenna Transciever Techniques for 3G and Beyond", John Wiley and Sons Ltd., 2003.

[6] J. M. 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 of IEEE Intl. Conf. on Acoustics, Speech and Signal Processing* (ICASSP 2007), Honolulu, Hawaii, USA, April 2007.

[7] M. Samuel and M. P. Fitz, "Reducing the Detection Complexity by using 2×2 Multi-Srata Space-Time Codes", *Proc IEEE Int. Symp. Inform. Theory* (ISIT 2007), Nice, France, June 2007.

[8] J. M. Paredes, A. B. Gershman, and M. Gharavi-Alkhansari, "A New Full-Rate Full-Diversity Space-Time Block Code With Nonvanishing Determinants and Simplified Maximum-Likelihood Decoding" *IEEE Trans. Sig. Proc*, vol. 56, no. 6, Jun. 2008.

[9] E. Biglieri, Y. Hong and E. Viterbo, " On Fast Decodable Space-Time Block Codes" *IEEE Trans. Inform. Theory*, vol. 55, no. 2, Feb. 2009.

[10] J.-C. Belfiore, G. Rekaya and E. Viterbo " The Golden Code: A 2×2 Full Rate Space-Time Code with Non-vanishing Determinant property",*IEEE Trans. Inform. Theory*, vol. 51, no. 4, Apr. 2005.

[11] F. Oggier, G. Rekaya, J.-C. Belfiore and E. Viterbo. "Perfect Space-Time Block Codes"*IEEE Trans. Inform. Theory*, vol. 52, no. 9, Sept. 2006.

[12] P. Elia, B. A. Sethuraman, P. V. Kumar "Perfect SpaceTime Codes for Any Number of Antennas" *IEEE Trans. Inform. Theory*, vol. 53, no. 11, Nov. 2007.