Códigos de Bloco Espaço-Tempo Diagonais 2×2 com Boas Densidades Normalizadas

Carina Alves, Cintya Wink de Oliveira Benedito e João Gabriel Oliveira de Jesus

***Resumo*— Neste trabalho provamos que o código de bloco espaço-tempo diagonal 2×2, com determinante mínimo 1, baseado no polinômio quadrático $x^2 + \zeta_3 - 1$, irredutível sobre $\mathbb{Q}(\zeta_3)$ é ótimo em termos da densidade normalizada. Vimos que maximizar a densidade normalizada de um reticulado complexo Λ é equivalente a minimizar o determinante da matriz geradora do reticulado real obtido a partir de Λ. Também apresentamos códigos de bloco espaço-tempo diagonais 2×2 baseados em polinômios irredutíveis sobre $\mathbb{Q}(\sqrt{-d})$, $d = 2, 7$, que possuem boas densidades normalizadas.**

***Palavras-Chave*— Densidade normalizada, Códigos diagonais , Matriz geradora.**

***Abstract*— In this work we prove that the diagonal space-time block code 2×2 with minimum determinant 1 based on an irreducible quadratic polynomial $x^2 + \zeta_3 - 1$ over $\mathbb{Q}(\zeta_3)$ is optimal in terms of normalized density. We saw that maximizing the normalized density of a complex lattice Λ is equivalent to minimizing the determinant of the generator matrix of the real lattice obtained from Λ. We also present diagonal space-time block codes 2×2 with minimum determinant 1 based on irreducible quadratic polynomials over $\mathbb{Q}(\sqrt{-d})$, $d = 2, 7$ that have good normalized densities.**

***Keywords*— Normalized density, Diagonal codes, Generator matrix.**

I. Introdução

Do ponto de vista da probabilidade de erro par a par (PEP) [1] o desempenho de um código espaço-tempo depende de dois parâmetros: *diversidade máxima* e *determinante mínimo*.

A diversidade máxima é obtida quando a diferença de quaisquer duas matrizes distintas do código tem posto máximo. Já o determinante mínimo é o mínimo dos valores absolutos dos determinantes de todas as matrizes não nulas no código. Para aumentar a confiabilidade constrói-se códigos com diversidade máxima e maior determinante mínimo [2], [3].

Ao comparar os determinantes mínimos de diferentes códigos, deve-se sempre usar o determinante mínimo normalizado. Equivalentemente, ao invés do determinante mínimo normalizado, a *densidade normalizada* (ou *diversidade produto*) também pode ser usada para comparar o desempenho dos códigos.

Quando um código de bloco espaço-tempo é um código linear infinito, podemos identificá-lo com um reticulado em $M_n(\mathbb{C})$ [2]. Desse modo, se Λ é um reticulado em $M_n(\mathbb{C})$ então de [4] a *densidade normalizada* de Λ é definida por

$$\rho(\Lambda) = \frac{det_{min}(\Lambda)^{2n}}{m(\Lambda)}, \tag{1}$$

onde $m(\Lambda)$ denota a medida (ou hipervolume) do paralelotopo fundamental do reticulado real obtido a partir de Λ e $det_{min}(\Lambda)$ é o mínimo dos valores absolutos dos determinantes de todas as matrizes não nulas de Λ.

Quando o determinante mínimo é fixado, maximizar o determinante mínimo normalizado, isto é, maximizar a densidade normalizada de Λ é equivalente a minimizar $m(\Lambda)$.

Existem vários tipos de códigos de bloco espaço-tempo, por exemplo, códigos de bloco espaço-tempo ortogonais [5], [6], códigos de bloco espaço-tempo unitários [7], [8] e códigos de bloco espaço-tempo diagonais [9], [10]. Dentre esses códigos, alguns deles são lineares tais como os códigos de bloco espaço-tempo ortogonais e os códigos de bloco espaço-tempo diagonais, onde a linearidade é em termos dos símbolos de informação, e com isso é possível aplicar alguns algoritmos de decodificação rápida, tais como o decodificador esférico [11], [12].

Códigos de bloco espaço-tempo diagonais podem ser aplicados em sistemas com múltiplas antenas e em sistemas com antenas simples sobre canais com desvanecimento do tipo Rayleigh. Em [13] é apresentado o desempenho de tais códigos com relação a decodificação em canais com múltiplas entradas e múltiplas saídas quase estáticos. Estes códigos também tem sido usamos recentemente em sistemas de modulação espacial [14], [15].

Na literatura há várias abordagens algébricas quanto a construção de códigos espaço-tempo. Em particular, em [16] são apresentados códigos de bloco espaço-tempo diagonais via corpos de números e em [3], [17], [18] e [19] são apresentados códigos de bloco espaço-tempo diagonais, onde os símbolos de informação estão em $\mathbb{Z}[i]$ ou $\mathbb{Z}[\zeta_3]$. Estas abordagens motivou-nos a considerar *códigos de bloco espaço-tempo diagonais* 2×2 onde os símbolos de informação estão sobre o anel dos inteiros de outros corpos quadráticos imaginários.

Nossa principal contribuição neste artigo é provar que o código de bloco espaço-tempo diagonal 2×2 baseado em um polinômio quadrático irredutível sobre $\mathbb{Q}(\sqrt{-3})$ é ótimo quando comparado com qualquer outro código de bloco espaço-tempo diagonal 2×2 baseado em polinômios quadráticos irredutíveis sobre $\mathbb{F}$, onde $\mathbb{F}$ é um corpo quadrático imaginário qualquer. A otimalidade é no sentido que a densidade normalizada é máxima quando a potência média de transmissão do sinal é fixa. Para a prova, vimos que é suficiente encontrar os

Carina Alves, Departamento de Matemática, Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro-SP, e-mail: carina.alves@unesp.br; Cintya W. O Benedito, Universidade Estadual Paulista "Júlio de Mesquita Filho", São João da Boa Vista-SP, e-mail: cintya.benedito@unesp.br; João Gabriel Oliveira de Jesus, Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro-SP, e-mail: jg.jesus@unesp.br. Este trabalho foi financiado por FAPESP (2019/20800-8).

melhores códigos de bloco espaço-tempo diagonais 2×2 baseados em polinômios irredutíveis sobre $\mathbb{Q}(\sqrt{-d})$, com $d = 2$ e 7. Além disso, verificamos que os códigos obtidos quando $d = 1, 3$, e 7 possuem melhor densidade normalizada do que a do código de Ouro [20].

A razão para considerarmos símbolos de informação em outros corpos quadráticos imaginários ao invés de $\mathbb{Z}[i]$ e $\mathbb{Z}[\zeta_3]$, que são considerados na maioria dos problemas de comunicação, é que existem algumas pesquisas recentes que consideram como corpo base um anel de inteiros algébricos qualquer, por exemplo, [21]. Além disso, a redução de reticulados, isto é, o método para encontrar os vetores mais curtos de um reticulado, tem sido generalizada para o anel dos inteiros de corpos quadráticos imaginários [22]. Neste trabalho, vamos considerar códigos com diversidade máxima.

Este artigo está organizado como segue. Na Seção II, definimos reticulados reais e complexos e introduzimos a densidade normalizada de reticulados. Na Seção III, definimos os códigos de bloco espaço-tempo 2×2 e apresentamos algumas propriedades. Na Seção IV damos um critério para comparar dois códigos de bloco espaço-tempo diagonais 2×2 e alguns resultados que serão usados nas demonstrações da próxima seção. A Seção V é dedicada a encontrar os melhores códigos de bloco espaço-tempo 2×2 baseados em polinômios quadráticos irredutíveis sobre corpos quadráticos imaginários.

II. Reticulados Reais e Complexos

Nesta seção, primeiro definimos reticulados reais e complexos. Em seguida, descrevemos como um reticulado complexo pode ser representado por um reticulado real.

Definição 2.1: Um reticulado real n-dimensional $\Omega_n(M)$ é um subconjunto de $\mathbb{R}^n$:

$$\begin{aligned}\Omega_n(M) &= \{(x_1 \cdots x_n)^t = M(z_1 \cdots z_n)^t \mid \\ &\quad z_k \in \mathbb{Z} \text{ para } 1 \leq k \leq n\}, \end{aligned} \tag{2}$$

onde ^{t} denota a transposição e M é uma matriz real $n \times n$ de posto máximo, chamada de matriz geradora do reticulado real $\Omega_n(M))$ e $det(\Omega_n(M)) = (det(M))^2$.

Definição 2.2: Um reticulado complexo n-dimensional $\Lambda_n(G)$ sobre um reticulado real 2-dimensional $\Omega_2(M)$ é um subconjunto de $\mathbb{C}^n$:

$$\begin{aligned}\Lambda_n(G) &= \{(y_1 \cdots y_n)^t = G(x_1 \cdots x_n)^t \mid \\ &\quad x_k \in \Omega_2(M) \text{ para } 1 \leq k \leq n\}, \end{aligned} \tag{3}$$

onde ^{t} denota a transposição e G é uma matriz complexa $n \times n$ de posto total e é chamada de matriz geradora do reticulado complexo $\Lambda_n(G)$ e M é a matriz geradora do reticulado $\Omega_2(M)$.

Seja G uma matriz complexa $n \times n$

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{pmatrix}, \tag{4}$$

com $|det(G)| > 0$ e $\mathcal{B}$ é uma matriz real $2n \times 2n$, que é formada pelas partes reais e imaginárias de G como segue:

$$\mathcal{B} = \begin{pmatrix} Re(g_{11}) & -Im(g_{11}) & \ldots & Re(g_{1n}) & -Im(g_{1n}) \\ Im(g_{11}) & Re(g_{11}) & \ldots & Im(g_{1n}) & Re(g_{1n}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re(g_{n1}) & -Im(g_{n1}) & \ldots & Re(g_{nn}) & -Im(g_{nn}) \\ Im(g_{n1}) & Re(g_{n1}) & \ldots & Im(g_{nn}) & Re(g_{nn}) \end{pmatrix} \tag{5}$$

onde $Re(g_{ij})$ e $Im(g_{ij})$ denotam a parte real e a parte imaginária de g_{ij}, $i, j = 1, \cdots, n$, respectivamente.

Se $(y_1 \cdots y_n)^t \in \Lambda_n(G)$, então de (3) segue que $(y_1 \cdots y_n)^t = G(x_1 \cdots x_n)^t$.

Reescrevendo y_k com sua parte real e imaginária, segue que $y_k = Re(y_k) + iIm(y_k)$, para $1 \leq k \leq n$. Com isso, $(y_1 \cdots y_n)^t$ pode ser reescrito como

$$\begin{pmatrix} Re(y_1) \\ Im(y_1) \\ \vdots \\ Re(y_n) \\ Im(y_n) \end{pmatrix} = \mathcal{B} \cdot \begin{pmatrix} Re(x_1) \\ Im(x_1) \\ \vdots \\ Re(x_n) \\ Im(x_n) \end{pmatrix} \tag{6}$$

$$= \mathcal{B} \cdot \text{ diag}(M, \ldots, M)_{2n \times 2n} \cdot \begin{pmatrix} z_{11} \\ z_{12} \\ \vdots \\ z_{n1} \\ z_{n2} \end{pmatrix} \tag{7}$$

onde $z_{k1}, z_{k2} \in \mathbb{Z}$ com

$$\begin{pmatrix} x_{k1} \\ x_{k2} \end{pmatrix} = M \cdot \begin{pmatrix} z_{k1} \\ z_{k2} \end{pmatrix}. \tag{8}$$

Seja $\mathcal{G} = \mathcal{B} \cdot \text{diag}(M, \ldots, M)_{2n \times 2n}$. Se mostrarmos que $\mathcal{G}$ é uma matriz geradora de um reticulado real $2n$-dimensional, então da Definição 2.1 temos que $(Re(y_1)\ Im(y_1) \cdots Re(y_n)\ Im(y_n))^t \in \Omega_{2n}(\mathcal{G})$. Para isso, basta mostrar que $\mathcal{G}$ é uma matriz de posto máximo, isto é, $|det(\mathcal{G})| > 0$.

Como M é a matriz geradora real de um reticulado real $\Omega_2(M)$, segue que $|det(M)| > 0$. Assim, concluímos que $|det(\mathcal{G})| > 0$ pela proposição que segue.

Proposição 1: [17] Seja G uma matriz complexa $n \times n$ como definida em (4) e seja $\mathcal{B}$ a matriz real $2n \times 2n$ definida em (5). Então $|det(G)|^2 = |det(\mathcal{B})|$.

A Proposição 1 nos diz que um reticulado complexo n-dimensional $\Lambda_n(G)$ sobre $\Omega_2(M)$ pode ser equivalentemente representado como um reticulado real $2n$-dimensional $\Omega_{2n}(\mathcal{G})$. Além disso, o determinante de sua matriz geradora tem a seguinte relação:

$$\begin{aligned}|det(\mathcal{G})| &= |det(\mathcal{B})| \cdot |det(M)|^n \\ &= |det(G)|^2 \cdot |det(M)|^n. \end{aligned} \tag{9}$$

Por definição $m(\Lambda) = |det(\mathcal{G})|$ e sendo $\mathcal{G}$ uma matriz geradora de $\Omega_{2n}(\mathcal{G})$, de acordo com (9) a densidade normalizada (1) pode ser reescrita como segue:

$$\rho(\Lambda_n(G)) = \frac{det_{min}\left(\Lambda_n(G)\right)^{2n}}{|det(G)|^2 \cdot |det(M)|^n}. \tag{10}$$

Note que minimizar $m(\Lambda)$ equivale a minimizar o denominador de (10). Neste trabalho focamos no caso $n = 2$.

III. CÓDIGO DE BLOCO ESPAÇO-TEMPO DIAGONAL 2×2

Seja $\mathbb{F}$ um corpo, $x^2 + px + q$ um polinômio irredutível sobre $\mathbb{F}$, com $p, q \in \mathcal{O}_{\mathbb{F}}$, o anel dos inteiros algébricos de $\mathbb{F}$. O polinômio $x^2 + px + q$ tem duas raízes:

$$\alpha_1 = \frac{-p + \sqrt{p^2 - 4q}}{2} \notin \mathbb{F},\ \alpha_2 = \frac{-p - \sqrt{p^2 - 4q}}{2} \notin \mathbb{F}.$$

Seja $\mathbb{K} = \mathbb{F}(\alpha_1)$, assim $[\mathbb{K} : \mathbb{F}] = 2$ e $\{1, \alpha_1\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$. Sejam σ_1 e σ_2 dois monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ tais que $\sigma_i(y) = y$, para todo $y \in \mathbb{F}$, $i = 1, 2$ e $\sigma_1(\alpha_1) = \alpha_1,\ \sigma_2(\alpha_1) = \alpha_2$.

Definição 3.1: Um código de bloco espaço-tempo diagonal 2×2, $\mathcal{C} := \mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0)$, baseado em um polinômio quadrático irredutível $x^2 + px + q \in \mathcal{O}_{\mathbb{F}}[x]$ sobre $\mathbb{F}$, com raízes $\alpha_1,\ \alpha_2$ é definido por

$$\mathcal{C} = \left\{ X = \begin{pmatrix} a + b\alpha_1 & 0 \\ 0 & a + b\alpha_2 \end{pmatrix} \mid a, b \in \mathcal{O}_{\mathbb{F}} \right\}. \quad (11)$$

Definição 3.2: Seja $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0)$ um código de bloco espaço-tempo diagonal, definimos o seu determinante mínimo por

$$det_{min}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0)) = \min_{X \in \mathcal{C}, X \neq 0} |det(X)|. \quad (12)$$

O próximo lema nos diz que quando consideramos corpos quadráticos imaginários, o determinante mínimo de um código de bloco espaço-tempo diagonal 2×2 é igual a 1.

Lema 1: [19] Se $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$, com d um inteiro positivo livre de quadrados, então todo código $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0)$ tem $det_{min}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0)) = 1$.

Para encontrar um código de bloco espaço-tempo diagonal 2×2 com densidade normalizada a maior possível, consideramos $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$, com d um inteiro positivo livre de quadrados.

Se $-d \equiv 1 (mod\, 4)$ então $\mathcal{O}_{\mathbb{F}} = \{1, \frac{1+\sqrt{-d}}{2}\}$ com base integral $B_{\mathbb{F}} = \{1, \frac{1+\sqrt{-d}}{2}\}$. Caso contrário, se $-d \equiv 2, 3 (mod\, 4)$ então $\mathcal{O}_{\mathbb{F}} = \{1, \sqrt{-d}\}$ com base integral $B_{\mathbb{F}} = \{1, \sqrt{-d}\}$. Assim, a matriz geradora correspondente do reticulado 2-dimensional $\Omega_2(M)$ é

$$M = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{d}}{2} \end{pmatrix} \text{ ou } M = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{pmatrix}, \quad (13)$$

respectivamente.

A Definição 3.1 nos diz que um código de bloco espaço-tempo diagonal 2×2 é um reticulado complexo sobre $\Omega_2(M)$ dado por

$$\Lambda_{-d} = \left\{ \begin{pmatrix} a + b\alpha_1 \\ a + b\alpha_2 \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \mid a,\ b \in \Omega_2(M) \right\}, \quad (14)$$

onde

$$G = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{pmatrix} \quad (15)$$

é a matriz geradora de Λ_{-d}.

Se $\mathcal{G}$ é uma matriz geradora do reticulado real 4-dimensional obtido a partir de um reticulado Λ_{-d} em $M_2(\mathbb{C})$, então de (10) segue que

$$\begin{aligned} \rho(\Lambda_{-d}) &= \frac{1}{|\alpha_1 - \alpha_2|^2 |det(M)|^2} \\ &= \frac{1}{|\sqrt{p^2 - 4q}|^2 |det(M)|^2}, \end{aligned} \quad (16)$$

onde $p^2 - 4q$ é o discriminante do polinômio $x^2 + px + q$.

Observação 1: Denotamos o denominador de (16) por $\gamma(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0))$. Note que quanto menor é o valor de $\gamma(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, 0))$ maior é a densidade normalizada de Λ_{-d}.

IV. CRITÉRIO PARA COMPARAR CÓDIGOS DIAGONAIS

Nesta seção apresentação um critério [19] para comparar dois códigos de bloco espaço-tempo diagonais 2×2.

Sejam $\mathcal{C}(\mathbb{F}_1, \alpha_1, \alpha_2, 0)$ e $\mathcal{C}(\mathbb{F}_2, \beta_1, \beta_2, 0)$ dois códigos de bloco espaço-tempo diagonais 2×2 com

$$det_{min}(\mathcal{C}(\mathbb{F}_1, \alpha_1, \alpha_2, 0)) = det_{min}(\mathcal{C}(\mathbb{F}_2, \beta_1, \beta_2, 0)). \quad (17)$$

Dizemos que $\mathcal{C}(\mathbb{F}_1, \alpha_1, \alpha_2, 0)$ é melhor do que $\mathcal{C}(\mathbb{F}_2, \beta_1, \beta_2, 0)$ se $\gamma(\mathcal{C}(\mathbb{F}_1, \alpha_1, \alpha_2, 0)) < \gamma(\mathcal{C}(\mathbb{F}_2, \beta_1, \beta_2, 0))$, isto é,

$$|\alpha_1 - \alpha_2|^2 |det(M_1)|^2 < |\beta_1 - \beta_2|^2 |det(M_2)|^2, \quad (18)$$

onde M_1 é uma matriz geradora de $\Omega_2(M_1)$ e M_2 é uma matriz geradora de $\Omega_2(M_2)$.

Definição 4.1: Seja S um conjunto de códigos de bloco espaço-tempo diagonais 2×2, onde $det_{min}\mathcal{C} = det_{min}\overline{\mathcal{C}}$ para todo $\mathcal{C}, \overline{\mathcal{C}} \in S$. Dizemos que $\mathcal{C}$ é um código de bloco espaço-tempo diagonal 2×2 ótimo em S se

$$\gamma(\mathcal{C}) \leq \gamma(\overline{\mathcal{C}}), \quad (19)$$

para todo $\overline{\mathcal{C}} \in S$.

V. OS MELHORES CÓDIGOS DE BLOCO ESPAÇO-TEMPO DIAGONAIS 2×2

Em [18] e [19], foi provado que os códigos $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}} = \mathcal{C}(\mathbb{Q}(\sqrt{-3}), \frac{-\zeta_3 + \sqrt{\zeta_3^2 + 4}}{2}, \frac{-\zeta_3 - \sqrt{\zeta_3^2 + 4}}{2}, 0)$ e $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}} = \mathcal{C}(\mathbb{Q}(\sqrt{-1}), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, 0)$ são os melhores códigos de bloco espaço-tempo diagonais 2×2 dentre todos os códigos de bloco espaço-tempo diagonais 2×2 baseados em polinômios quadráticos irredutíveis sobre $\mathbb{Q}(\sqrt{-3})$ e $\mathbb{Q}(\sqrt{-1})$, isto é, códigos com a maior densidade normalizada, dadas por $\rho(\Lambda_{-3}) \approx 0,36980$ e $\rho(\Lambda_{-1}) \approx 0,33333$, respectivamente.

Assim, em termos da densidade normalizada, o código $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}$ é melhor do que o código $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}}$.

Os resultados apresentados nesta seção tem como objetivo responder a seguinte questão: O código $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}$ é ótimo, isto é, possui maior densidade normalizada, quando comparado com qualquer código de bloco espaço-tempo diagonal 2×2, $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}}$, em que d um inteiro positivo livre de quadrados? Para respondê-la, veremos que é suficiente encontrar os melhores códigos de blocos espaço-tempo diagonais 2×2 baseados em polinômios quadráticos irredutíveis sobre $\mathbb{Q}(\sqrt{-d})$, com $d = 2, 7$.

Suponha que exista um código de bloco espaço-tempo diagonal 2×2, $\mathcal{C}(\mathbb{Q}(\sqrt{-d}),\beta_1,\beta_2,0)$, melhor do que $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}$, em que d um inteiro positivo livre de quadrados. De acordo com (18),

$$|det(M)|^2|\beta_1-\beta_2|^2<\gamma(\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}})\approx 2,70416, \tag{20}$$

onde M é a matriz geradora do reticulado $\Omega_2(M)$, o qual é obtido via $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$.

Vamos analisar quando $|det(M)|^2<2,70416$. Na Seção III vimos que:

i) se $-d\equiv 1(mod\,4)$, então $|det(M)|^2=\frac{|d|}{4}$. Logo $d\in\{3,7\}$ são os únicos d satisfazendo $|det(M)|^2<2,70415$.

ii) se $-d\equiv 2,3(mod\,4)$ então $|det(M)|^2=|d|$. Logo, $d\in\{1,2\}$ são os únicos d satisfazendo $|det(M)|^2<2,70415$.

Como os casos $d=1$ e $d=3$ já foram analisados em [18], [19], segue que precisamos analisar somente quando $d\in\{2,7\}$.

A partir de agora vamos encontrar os melhores códigos de bloco espaço-tempo diagonais 2×2 considerando $d=2,7$ e comparar suas densidades normalizadas com a densidade normalizada de $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}}$.

A. O melhor Código de Bloco Espaço-Tempo Diagonal 2×2 $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}$

Estamos interessados em encontrar o melhor código de bloco espaço-tempo diagonal 2×2, $\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\alpha_1,\alpha_2,0)$, em termos da densidade normalizada.

Um polinômio quadrático irredutível sobre $\mathbb{Q}(\sqrt{-2})$ com menor discriminante é x^2-x+1, assim $\alpha_1=\frac{1+\sqrt{-3}}{2}$ e $\alpha_2=\frac{1-\sqrt{-3}}{2}$. A partir disso podemos estabelecer o seguinte teorema.

Teorema 1: O código $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}=\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},0)$ é o melhor código de bloco espaço-tempo diagonal 2×2, em termos da densidade normalizada, dentre todos os códigos de bloco espaço-tempo diagonais 2×2 baseados em polinômios quadráticos irredutíveis sobre $\mathbb{Q}(\sqrt{-2})$ com determinante mínimo 1.

Demonstração: Pelo Lema 1, $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}$ é um código de bloco espaço-tempo diagonal 2×2 com determinante mínimo 1. De acordo com a Seção III, como $-2\equiv 2(mod\,4)$, segue que $|det(M)|=\sqrt{2}$. Logo, por (16),

$$\rho(\Lambda_{-2})=\frac{1}{|\sqrt{-3}|^2(\sqrt{2})^2}=\frac{1}{6}\approx 0,16667. \tag{21}$$

O valor $|det(M)|^2$ é invariante, pois $\mathbb{F}=\mathbb{Q}(\sqrt{-2})$ é o corpo base, portanto podemos removê-lo em nossa análise.

Suponha por contradição que exista um código de bloco espaço-tempo diagonal 2×2, $\tilde{\mathcal{C}}=\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\beta_1,\beta_2,0)$ com determinante mínimo 1 baseado no polinômio irredutível x^2+px+q, com $p,q\in\mathbb{Z}[\sqrt{-2}]$ cujas raízes são β_1 e β_2 tal que

$$|\beta_1-\beta_2|^2=|p^2-4q|<3. \tag{22}$$

Como $p\in\mathbb{Z}[\sqrt{-2}]$, de [19] podemos assumir, sem perda de generalidade, que $|p|<|1+\sqrt{-2}|=\sqrt{3}$. Como $p=a+b\sqrt{-2}$, $a,b\in\mathbb{Z}$ então $|p|=|a+b\sqrt{-2}|<\sqrt{3}$ se

$$(a,b)\in\{(0,0),\,(0,\pm1),(\pm1,0)\}. \tag{23}$$

Novamente, como $q\in\mathbb{Z}[\sqrt{-2}]$ temos que $q=c+d\sqrt{-2}$, $c,d\in\mathbb{Z}$ e então para cada par (a,b) de (23) nós analisamos quando $|p^2-4q|=|(a+b\sqrt{-2})^2-4(c+d\sqrt{-2})|<3$. Assim, de acordo com (23) precisamos considerar os seguintes casos:

(i) $p^2=0$. Neste caso, $|p^2-4q|<3\Leftrightarrow c=d=0$, isto é, $q=0$. Quando $q=0$ temos que $x^2+px+q=x^2$, que é redutível sobre $\mathbb{Q}(\sqrt{-2})$.

(ii) $p^2=-2$. Neste caso, $|p^2-4q|<3\Leftrightarrow c=d=0$ ou $c=-1,d=0$, isto é, $q=0$ ou $q=-1$. Quando $q=0$ temos $x^2+px+q=x^2\pm\sqrt{-2}x$, que são redutíveis sobre $\mathbb{Q}(\sqrt{-2})$. Quando $q=-1$ temos que $x^2+px+q=x^2\pm\sqrt{-2}x-1$, que são redutíveis sobre $\mathbb{Q}(\sqrt{-2})$.

(iii) $p^2=1$. Neste caso, $|p^2-4q|<3\Leftrightarrow c=d=0$, isto é, $q=0$. Quando $q=0$ temos que $x^2+px+q=x^2\pm x$, que são redutíveis sobre $\mathbb{Q}(\sqrt{-2})$.

Desse modo, não existe polinômio irredutível sobre $\mathbb{Q}(\sqrt{-2})$ que satisfaça (22).

Portanto, $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}$ é o melhor código de bloco espaço-tempo diagonal 2×2 nas condições do teorema. ■

B. O melhor Código de Bloco Espaço-Tempo Diagonal 2×2 $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}}$

Um polinômio irredutível com menor discriminante sobre $\mathbb{Q}(\sqrt{-7})$ é $x^2+\left(\frac{1+\sqrt{-7}}{2}\right)x-1$. A partir disso podemos estabelecer o seguinte teorema.

Teorema 2: O código $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}}=\mathcal{C}(\mathbb{Q}(\sqrt{-7}),\alpha_1,\alpha_2,0)$, onde $\alpha_1=\frac{-1}{4}-\frac{\sqrt{-7}}{4}-\frac{1}{4}\sqrt{10+2\sqrt{-7}}$ e $\alpha_2=\frac{-1}{4}-\frac{\sqrt{-7}}{4}+\frac{1}{4}\sqrt{10+2\sqrt{-7}}$ é o melhor código de bloco espaço-tempo diagonal 2×2, em termos da densidade normalizada, dentre todos os códigos de bloco espaço-tempo diagonais 2×2 baseados em polinômios quadráticos irredutíveis sobre $\mathbb{Q}(\sqrt{-7})$ com determinante mínimo 1.

Demonstração: A demonstração é análoga a do Teorema 1. De acordo com as considerações da Seção III, como $-7\equiv 1(mod\,4)$ segue que $|det(M)|=\frac{\sqrt{7}}{2}$.

Assim, de (16),

$$\rho(\Lambda_{-7})=\frac{1}{2\sqrt{2}\left(\frac{\sqrt{7}}{2}\right)^2}=\frac{1}{\frac{7}{\sqrt{2}}}\approx 0,20203. \tag{24}$$

O valor de $|det(M)|^2$ é invariante, pois $\mathbb{F}=\mathbb{Q}(\sqrt{-7})$ é o corpo base, portanto podemos removê-lo em nossa análise.

Suponha que exista um código de bloco espaço-tempo diagonal 2×2, $\tilde{\mathcal{C}}=\mathcal{C}(\mathbb{Q}(\sqrt{-7}),\beta_1,\beta_2,\gamma)$, com determinante mínimo 1 baseado em um polinômio irredutível x^2+px+q, com $p,q\in\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, cujas raízes são β_1 e β_2, tal que

$$|\beta_1-\beta_2|^2=|p^2-4q|<2\sqrt{2}. \tag{25}$$

De [19] podemos assumir, sem perda de generalidade, que $|p|<|\frac{1+\sqrt{-7}}{2}|=\sqrt{2}$.

Como $p\in\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ temos que $p=a+b\left(\frac{1+\sqrt{-7}}{2}\right)$, $a,b\in\mathbb{Z}$, e então $|p|=|a+b\left(\frac{1+\sqrt{-7}}{2}\right)|<\sqrt{2}$ se

$$(a,b) \in \{(0,0),\ (\pm 1,0)\}. \tag{26}$$

Novamente, como $q \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, temos que $q = c + d\left(\frac{1+\sqrt{-7}}{2}\right)$, $c,d \in \mathbb{Z}$, e então para cada par (a,b) de (26), analisamos quando $|p^2-4q| = |\left(a+b\left(\frac{1+\sqrt{-7}}{2}\right)\right)^2 - 4\left(c+d\left(\frac{1+\sqrt{-7}}{2}\right)\right)| < 2\sqrt{2}$. De acordo com (26) precisamos considerar os seguintes casos:

(i) $p^2 = 0$. Neste caso, $|p^2-4q| < 2\sqrt{2} \Leftrightarrow q = 0$. Quando $q = 0$ temos que $x^2+px+q = x^2$, que é redutível sobre $\mathbb{Q}(\sqrt{-7})$.

(ii) $p^2 = 1$. Neste caso, $|p^2-4q| < 2\sqrt{2} \Leftrightarrow q = 0$. Quando $q = 0$ temos que $x^2+px+q = x^2 \pm x$, que são redutíveis sobre $\mathbb{Q}(\sqrt{-7})$.

Desse modo, não existe polinômio irredutível sobre $\mathbb{Q}(\sqrt{-7})$ que satisfaça (25). Portanto, $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}}$ é o melhor código de bloco espaço-tempo diagonal 2×2 nas condições do teorema. ■

De acordo com o que foi provado nesta seção, podemos formular o seguinte teorema.

Teorema 3: O código de bloco espaço-tempo diagonal 2×2 $\mathcal{C}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}} = \mathcal{C}(\mathbb{Q}(\sqrt{-3}), \frac{-\zeta_3+\sqrt{\zeta_3^2+4}}{2}, \frac{-\zeta_3-\sqrt{\zeta_3^2+4}}{2}, 0)$ é ótimo em termos da densidade normalizada, dentre todos os códigos de bloco espaço-tempo diagonais 2×2, com determinante mínimo 1, baseados em polinômios quadráticos irredutíveis sobre $\mathbb{F}$, onde $\mathbb{F} = \mathbb{Q}(\sqrt{-d})$, com d um inteiro positivo livre de quadrados.

Observação 2: Note que os reticulados Λ_{-d}, $d = 1,3,7$ possuem melhor densidade normalizada que o código de Ouro, que é dada por $\frac{1}{5}$ [20].

VI. Conclusões

Neste trabalho apresentamos os melhores códigos de bloco espaço-tempo diagonais 2×2, em termos da densidade normalizada, baseados em polinômios quadráticos irredutíveis sobre $\mathbb{Q}(\sqrt{-d})$, com $d \in \{2,7\}$. Isto expande o que foi proposto em [18], [19], onde os autores consideram somente símbolos de informação em $\mathbb{Z}[i]$ e $\mathbb{Z}[\zeta_3]$. Também provamos que o código de bloco espaço-tempo diagonal 2×2, com determinante mínimo 1, baseado no polinômio quadrático $x^2+\zeta_3-1$, irredutível sobre $\mathbb{Q}(\zeta_3)$ é ótimo, segundo a Definição 4.1.

Agradecimentos

Os autores agradecem ao SBrT pela oportunidade e o apoio financeiro da FAPESP Processo 2019/20800-8.

Referências

[1] V. Tarokh, N. Seshadri and A.R. Calderbank, "Space-time codes for high data rate wireless communications: performance criterion and code construction,"*IEEE Trans. Inf. Theory*, v. 44, pp. 744–765, Mar. 1998.

[2] F. Oggier, J.-C. Belfiore and E. Viterbo, *Cyclic Division Algebras: a Tool for Space-Time Coding*, Now Foundations and Trends, 2007.

[3] G. Wang and X.-G. Xia, "On optimal multilayer cyclotomic space-time code designs,"*IEEE Trans. Inf. Theory*, v.51 , pp. 1102–1135, Mar. 2005.

[4] C. Hollanti, J. Lahtonen, K. Ranto and R. Vehkalahti, "On the densest MIMO lattices from cyclic division algebras", *IEEE Trans. Inf. Theory*, v. 55, pp. 3751–3780, Aug. 2009.

[5] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs,"*IEEE Trans. Inf. Theory*, v. 45, pp. 1456–1467, Jul. 1999.

[6] W. Su, X.-G. Xia, and K. J. R. Liu, "A systematic design of high-rate complex orthogonal space-time block codes,"*IEEE Commun. Letters*, v. 8, no. 6, pp. 380–382, Jun. 2004.

[7] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes,"*IEEE Trans. Inf. Theory*, v. 48, pp. 1485–1503, Jun. 2002.

[8] X.-B. Liang and X.-G. Xia, "Unitary signal constellations for space-time modulation with two transmit antennas: Parametric codes, optimal designs, and bounds,"*IEEE Trans. Inf. Theory*, v. 48, pp. 2291–2322, Aug. 2002.

[9] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels,"*IEEE Trans. Inf. Theory*, v. 43, pp. 938–952, May 1997.

[10] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes,"*IEEE Trans. Inf. Theory*, v. 48, pp. 628–636, Mar. 2002.

[11] M. O. Damen, K. A.-Meraim, and J.-C. Belfiore, "Generalized sphere decoder for asymmetrical space-time communication architecture," *IEE Electron. Lett.*, v. 36, pp. 166-–166, Jan. 2000.

[12] H. Vikalo and B. Hassibi, "Maximum-likelihood sequence detection of multiple antenna systems over dispersive channels via sphere decoding," *EURASIPJ . Appl. Signal Processing*, no. 5, pp. 525-–531, 2002.

[13] W. Abediseid and M.-S. Alouini, "On the Performance of Diagonal Lattice Space-Time Codes", *IEEE Trans. Inf. Theory*, v. 58, no. 6, p. 4005–4013, Jun. 2012.

[14] N. T. Dong, T. X. Nam and L. M. Tuan, "Diagonal Space Time Block Coded Spatial Modulation", *Research and Development on Information and Communication Technology*, v.2019, no. 1.832, p. 1-7, Feb. 2019.

[15] L. Wang and Z. Chen, "Spatially Modulated Diagonal Space Time Codes", *IEEE Communications Letters*, 2015.

[16] C. P. Xing. Diagonal Lattice space-time codes from number fields and asymptotic bounds, IEEE Trans. Inform. Theory, v.53, no. 11, pp.3921–3926, Oct. 2007.

[17] G. Wang et al., "Systematic and optimal cyclotomic lattices and diagonal spasce-time block code designs", *IEEE Trans. Inf. Theory*, v. 50, pp. 3348–3360, Dec. 2004.

[18] H. Liao, H. Wang and X.-G. Xia, "Some Designs and Normalized Diversity Product Upper Bounds for Lattice-Based Diagonal and Full-Rate Space–Time Block Codes", *IEEE Trans. Inf. Theory*, v. 55, no.2, pp. 569–583, Feb. 2009.

[19] G. Wang, J.K. Zhan and M. Amin, "Space-time block code designs based on quadratic field extension for two-transmitter antennas", *IEEE Trans. Inf. Theory*, v. 58, no. 6, p. 4005–4013, Jun. 2012.

[20] J.-C. Belfiore, G. Rekaya and E. Viterbo, "The golden code: a 2×2 full rate space-time code with non vanishing determinants", *IEEE Trans. Inf. Theory*, v. 51, no. 4, pp.1432–1436, Apr. 2005.

[21] Y.-C. Huang, "Lattice index codes from algebraic number fields,"*IEEE Trans. Inf. Theory*, vol. 63, pp. 2098–2112, Apr. 2017.

[22] S. Lyu, C. Porter and C. Ling, "Lattice Reduction over Imaginary Quadratic Fields,"*arXiv:1806.03113v4 [cs.IT]*, Nov. 2018.