ENCONTRO DE CÓDIGOS, RETICULADOS E INFORMAÇÃO

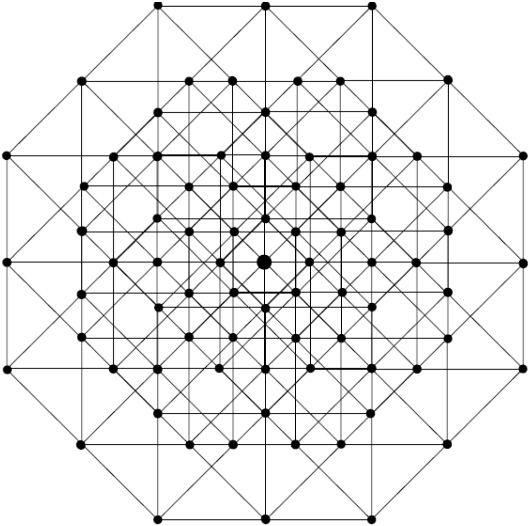
- ENCORI -

Códigos e Reticulados via Álgebra dos Quatérnios: Resultados e Perspectivas

Cintya Wink de Oliveira Benedito
cintya.benedito@unesp.br

15 de Junho de 2023

Introdução



Introdução

- Reticulados Hiperbólicos
  - Códigos Geometricamente Uniformes Hiperbólicos (Particionamento de Ungerboeck)
- Reticulados Algébricos
  - Códigos de Bloco Espaço-Tempo 2×2

Álgebra dos Quatérnios

Definição

Uma **álgebra dos quatérnios** $\mathscr{A} = (a, b)_{\mathbb{K}}$ *sobre um corpo de números* $\mathbb{K}$ *é uma álgebra simples central de dimensão 4 sobre* $\mathbb{K}$*, com uma base* $\{1, i, j, k\}$*, satisfazendo a condição de que* $i^2 = a$*,* $j^2 = b$*,* $k = ij = -ji$ *e que* $k^2 = -ab$*, em que* $a, b \in \mathbb{K} \setminus \{0\}$.

Exemplo

O exemplo padrão de álgebra dos quatérnios sobre um corpo de números totalmente real é a álgebra dos quatérnios de Hamilton $\mathscr{H} = (-1, -1)_{\mathbb{Q}}$.

Álgebra dos Quatérnios

Definição

Se

$$x = x_1 + x_2 i + x_3 j + x_4 k \in \mathscr{A},$$

em que $x_1, x_2, x_3, x_4 \in \mathbb{K}$, *então* $\bar{x} = x_1 - x_2 i - x_3 j - x_4 k \in \mathscr{A}$ *é chamado de* **conjugado** *de* x.

Definição

O **traço reduzido** *e a* **norma reduzida** *de um elemento* $x \in \mathscr{A}$ *são definidos respectivamente por*

$$Trd(x) = x + \bar{x} \text{ e } Nrd(x) = x \cdot \bar{x}.$$

- Considerando φ um homomorfismo de $\mathscr{A} = (a,b)_{\mathbb{K}}$ em $M(2,\mathbb{K}(\sqrt{a}))$, cada elemento x de $\mathscr{A}$ é identificado com

$$x \longmapsto \varphi(x) = \begin{pmatrix} x_1 + x_2\sqrt{a} & x_3 + x_4\sqrt{a} \\ b\left(x_3 - x_4\sqrt{a}\right) & x_2 - x_2\sqrt{a} \end{pmatrix}. \tag{1}$$

  - $Nrd(x) = \det(\varphi(x))$.

- Uma álgebra dos quatérnios $\mathscr{A} = (a,b)_{\mathbb{K}}$ é uma **álgebra de divisão** se, e somente se, $Nrd(x) \neq 0$ para todo $x \in \mathscr{A} \setminus \{0\}$.

- $\mathscr{A}$ é dita **definida positiva** se, e somente se, a forma quadrática $Trd(x\bar{y})$ em $\mathscr{A}$ é definida positiva, para todo $x, y \in \mathscr{A}$.

Definição

*Seja $\mathscr{A}$ uma álgebra dos quatérnios sobre $\mathbb{K}$ e R um anel de $\mathbb{K}$. Então, uma R-***ordem** *$\mathscr{O}$ em $\mathscr{A}$ é um subanel com unidade de $\mathscr{A}$ que é um R-módulo finitamente gerado tal que $\mathscr{A} = \mathbb{K}\mathscr{O}$.*

Considerando R um anel de $\mathbb{K}$ e a álgebra $\mathscr{A} = (a,b)_{\mathbb{K}}$, com $a,b \in R$, então $\mathscr{O} = \{x_1 + x_2 i + x_3 j + x_4 k : x_1, x_2, x_3, x_4 \in R\}$, é uma ordem em $\mathscr{A}$ denotada por $\mathscr{O} = (a,b)_R$.

Definição

Uma **ordem maximal** *dos quatérnios $\mathscr{M}$ de uma álgebra dos quatérnios $\mathscr{A}$ é uma R-ordem que não está propriamente contida em nenhuma outra ordem.*

- Modelos Hiperbólicos $\mathbb{H}^2$ e $\mathbb{D}^2$.

Modelos Hiperbólicos	**Semi-plano superior** $\mathbb{H}^2 = \{z \in \mathbb{C} : Im(z) > 0\}$	**Disco de Poincaré** $\mathbb{D}^2 = \{z \in \mathbb{C} : \lvert z\rvert < 1\}$
Fronteira	$\partial \mathbb{H}^2 = \mathbb{R} \cup \{\infty\}$	$\partial \mathbb{D}^2 = \{z \in \mathbb{C} : \lvert z\rvert = 1\}$
Comprimento hiperbólico	$\int_a^b \frac{\lvert\sigma'(t)\rvert}{Im(\sigma(t))} dt$	$\int_a^b \frac{2}{1-\lvert\sigma(t)\rvert^2} \lvert\sigma'(t)\rvert dt$
Área hiperbólica	$\mu_{\mathbb{H}^2}(A) = \int_A \frac{1}{(Im(z))^2} dz$	$\mu_{\mathbb{D}^2}(A) = \int_A \frac{4}{(1-\lvert z\rvert^2)^2} dz$
Isometrias	$\gamma(z) = \frac{az+b}{cz+d}$, $a,b,c,d \in \mathbb{R},\ ad-bc > 0$	$\gamma(z) = \frac{az+b}{\bar{b}z+\bar{a}}$, $a,b \in \mathbb{C},\ \lvert a\rvert^2 - \lvert b\rvert^2 > 0$
Geodésicas	semi-retas verticais e semi-círculos ortogonais a $\partial \mathbb{H}^2$	arcos de círculos e diâmetros em $\mathbb{D}^2$ que encontram $\partial \mathbb{D}^2$ ortogonalmente

Definição

Seja $PSL(2,\mathbb{R})$ o conjunto de todas as transformações de Möbius, $T : \mathbb{H}^2 \longrightarrow \mathbb{H}^2$, definidas por $T_A(z) = \frac{az+b}{cz+d}$, onde $a,b,c,d \in \mathbb{R}$ e $ad-bc = 1$. Um **grupo Fuchsiano** *Γ é um subgrupo discreto de $PSL(2,\mathbb{R})$.*

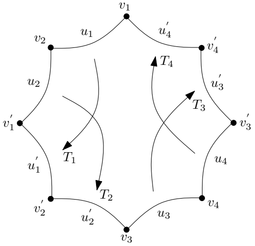
Tesselações Hiperbólicas

Definição

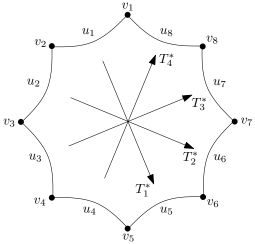
Uma **tesselação regular no plano hiperbólico** *é uma partição deste plano por polígonos regulares não sobrepostos, todos congruentes, sujeitos à restrição de se interceptarem somente em suas arestas ou vértices, de modo a termos o mesmo número de polígonos partilhando um mesmo vértice, independente do vértice.*

Se os polígonos de uma tesselação de $\mathbb{H}^2$ contém p lados, onde cada vértice é o encontro de q desses polígonos, então a tesselação será denotada por $\{p, q\}$. Em particular, se $p = q$, então a tesselação é chamada **auto-dual**.

- Tesselação auto dual $\{4g, 4g\}$ com $g \geq 2$.



(a) $\mathscr{P}_8$-emparelhamento usual



(b) $\mathscr{P}_8$-emparelhamento diametralmente oposto

Figura 1: Tesselação auto dual $\{8, 8\}$.

- Tesselação auto dual $\{4g+2, 2g+1\}$ com $g \geq 2$.
- Tesselação $\{12g-6, 3\}$ com $g \geq 2$.

Tesselações Hiperbólicas

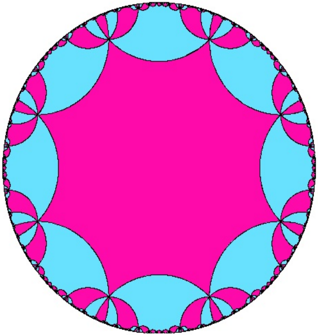


Figura 2: *Tesselação hiperbólica* $\{8,8\}$ *no disco de Poincaré* $\mathbb{D}^2$.

Grupos Fuchsianos Aritméticos

Teorema

(Katok) $\Gamma(\mathscr{A},\mathscr{O}) \simeq PSL(2,\mathbb{R})$ *é um grupo Fuchsiano.*

Definição

O grupo Fuchsiano $\Gamma(\mathscr{A},\mathscr{O})$ *é chamado grupo Fuchsiano aritmético.*

Definição

Considere $\mathscr{A} = (a,b)_{\mathbb{K}}$ *uma álgebra dos quatérnios sobre o corpo de números totalmente real* $\mathbb{K}$. *Definimos uma R-ordem* $\mathscr{O}$ *em* $\mathscr{A}$ *como um* **reticulado hiperbólico** *devido a sua identificação com um grupo Fuchsiano aritmético* Γ.

Teorema

(Condição de Fermat) *Se Γ_p é um grupo fuchsiano proveniente de uma tesselação $\{p,q\}$, então é possível encontrar os geradores de $\Gamma \simeq \Gamma_p$ e, portanto, o grupo fuchsiano aritmético, se p e q puderem ser decompostos na forma:*

$$2^k \ \ ou \ \ 2^k p_1 p_2 \dots p_s, \tag{2}$$

em que k é um inteiro não negativo e os p_i's são números distintos de Fermat.

Teorema

Dado $g \geq 2$ o gênero da superfície, como em (2), associada à tesselação $\{4g, 4g\}$, os elementos do grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$ são identificados, via isomorfismo, com elementos do grupo dos invertíveis $\mathcal{O}^1$ da ordem $\mathcal{O} = (\theta, -1)_R$, onde $R = \mathbb{O}_{\mathbb{K}}$ e θ dependendo do gênero g. Consequentemente, $\{1, \sqrt{\theta}, Im, \sqrt{\theta} Im\}$ é uma R-base para o reticulado hiperbólico $\mathcal{O}$. Além disso, o grupo Fuchsiano $\Gamma \simeq \Gamma_{4g}$, associado ao polígono hiperbólico regular $\mathscr{P}_{4g}$, é derivado de uma álgebra de divisão dos quatérnios $\mathscr{A} = (\theta, -1)_{\mathbb{K}}$ sobre o corpo de números totalmente real $\mathbb{K} = \mathbb{Q}(\theta)$.

$$\theta = \begin{cases} \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}} & \text{, contendo } n \text{ radicais, para } g = 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}} & \text{, contendo } n+1 \text{ radicais, para } g = 3\cdot 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}} & \text{, contendo } n+2 \text{ radicais, para } g = 5\cdot 2^n; \\ \sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}} & \text{, contendo } n+3 \text{ radicais, para } g = 3\cdot 5\cdot 2^n. \end{cases} \quad (3)$$

Ou

$$\mathbb{K} = \begin{cases} \mathbb{Q}(\zeta_{2^r}+\zeta_{2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}\right) & \text{, com } r > 2; \\ \mathbb{Q}(\zeta_{3.2^r}+\zeta_{3.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\sqrt{3}}}}\right) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{5.2^r}+\zeta_{5.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\sqrt{2+\frac{\sqrt{10+2\sqrt{5}}}{2}}}}\right) & \text{, com } r > 1; \\ \mathbb{Q}(\zeta_{3.5.2^r}+\zeta_{3.5.2^r}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\ldots+\frac{\sqrt{7+\sqrt{5}+\sqrt{30+6\sqrt{5}}}}{2}}}\right) & \text{, com } r > 1. \end{cases} \quad (4)$$

Ordens Maximais dos Quatérnios

Teorema

Sejam $\mathscr{A} = (\theta, -1)_{\mathbb{K}}$ *uma álgebra dos quatérnios, onde* $\theta = \sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}$ *contendo n radicais,* $n > 1$*,* $\mathbb{K} = \mathbb{Q}(\theta)$ *e* $m = [\mathbb{K} : \mathbb{Q}] = 2^n$*. Considere a base dada por*

$$B = \left\{1, i, \frac{1}{2}((\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3}) + \theta^{m-1}i + j),\right.$$
$$\left. -\frac{1}{2\theta}(2 + (\theta^{m-1} + \theta^{m-2} + \ldots + \theta^{m-\frac{m}{2}} + 1 - \theta^{m-3})i + k)\right\}.$$

Se $Nrd(x) \in \mathbb{O}_{\mathbb{K}} = \mathbb{Z}[\theta]$*, para todo* $x \in B$*, então* $\mathscr{M} \supseteq \mathscr{O} = (\theta, -1)_{\mathbb{O}_{\mathbb{K}}}$ *é uma ordem maximal dos quatérnios para a álgebra* $\mathscr{A}$ *caracterizada pela base B.*

- A ordem maximal dos quatérnios $\mathscr{M} \supseteq \mathscr{O} = (\sqrt{2}, -1)_{\mathbb{O}_{\mathbb{K}}}$, em que $\mathbb{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$, produz um reticulado hiperbólico completo quando associada ao grupo Fuchsiano aritmético Γ_8, proveniente da tesselação $\{8, 8\}$.

Sejam $\mathscr{A} = (\sqrt{2}, -1)_{\mathbb{Q}[\sqrt{2}]}$ uma álgebra dos quatérnios e $\alpha = \sqrt{2} + j \in \mathscr{O} = (\sqrt{2}, -1)_{\mathbb{Z}[\sqrt{2}]}$. Temos que $N(\alpha) = 3 \in \mathbb{Z}$ e o quociente $\frac{\mathscr{O}}{<\alpha>}$ possui $Nrd(\alpha)^4 = 3^4 = 81$ elementos, os quais serão os centros dos 81 octógonos pertencentes a tesselação $\{8, 8\}$ contidos no polígono fundamental P_{328}.

A constelação de sinais obtida pelo quociente $\frac{\mathscr{O}}{<\sqrt{2}+j>}$, pode ser visualizada através do seguinte grafo:

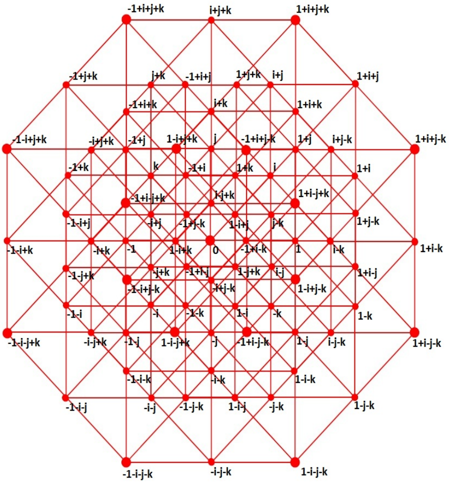
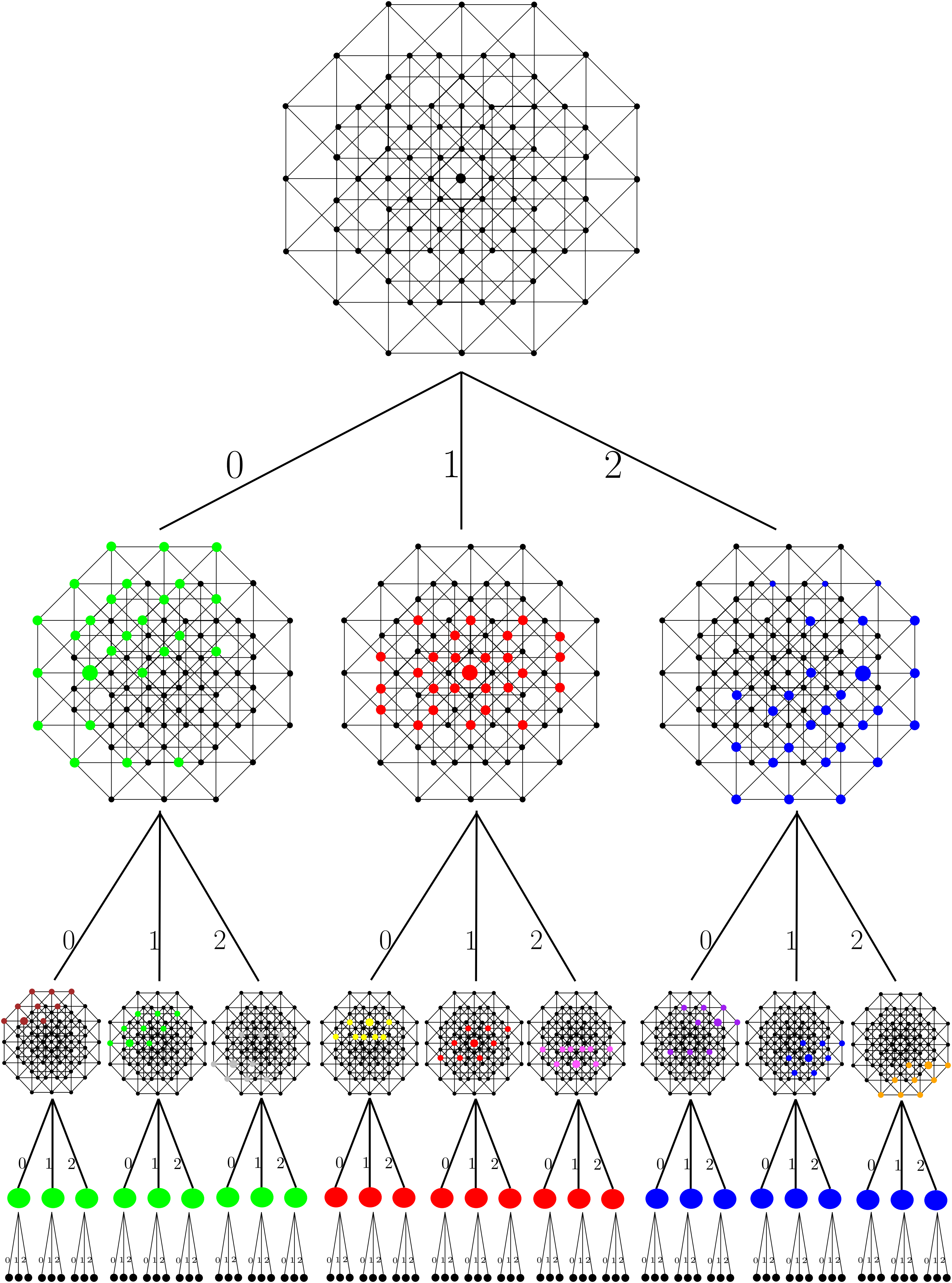


Figura 3: *81 elementos da constelação de sinais* $\frac{\mathcal{O}}{<\sqrt{2}+j>}$.



0
1
2
0
1
2
0
1
2
0
1
2

- C. W. O. Benedito, R. Palazzo and J. C. Interlando, “An algorithm to construct arithmetic Fuchsian groups derived from quaternion algebras and the corresponding hyperbolic lattices”, Journal of Pure and Applied Algebra, vol 220 (5), pp. 1902-1923, 2016, https://doi.org/10.1016/j.jpaa.2015.10.006.
- C. R. O. Q. Queiroz, C. W. O. Benedito, J. C. Interlando and R. Palazzo, “Complete hyperbolic lattices derived from tessellations of type $\{4g, 4g\}$”, Journal of Algebra and Its Applications, Volume 15, 2015, doi: 10.1142/S0219498816501577.
- C. R. O. Q. Queiroz and R. Palazzo, “Construction of Signal Sets From Quotient Rings of the Quaternion Orders Associated With Arithmetic Fuchsian Groups,” in IEEE Access, vol. 8, pp. 196050-196061, 2020, doi: 10.1109/ACCESS.2020.3034455.
- E.M.V. Gomes, E.D. Carvalho, C.A.R. Martins, W.S. Soares Jr., E.B. Silva, “Hyperbolic Geometrically Uniform Codes and Ungerboeck Partitioning on the Double Torus”, Symmetry, 14(3):449, 2022, https://doi.org/10.3390/sym14030449.

Seja $\mathscr{A}$ uma álgebra dos quatérnios definida positiva sobre um corpo de números totalmente real $\mathbb{K}$ de grau n. Se $x = x_1 + x_2 i + x_3 j + x_4 k \in \mathscr{A}$ então podemos identificar $\mathscr{A}$ com $\mathbb{K}^4$ por

$$\begin{array}{cccc} \phi_1 : & \mathscr{A} & \rightarrow & \mathbb{K}^4 \\ & x & \mapsto & (x_1, x_2, x_3, x_4) \end{array}. \tag{5}$$

Considerando $\sigma_1, \cdots, \sigma_n$ os n monomorfismos reais de $\mathbb{K}$, podemos identificar $\mathbb{K}^4$ com $\mathbb{R}^{4n}$ por

$$\begin{array}{cccc} \phi_2 : & \mathbb{K}^4 & \rightarrow & \mathbb{R}^{4n} \\ & (x_1, x_2, x_3, x_4) & \mapsto & \left(\sigma_1(x_1), \cdots, \sigma_n(x_1), \cdots, \sigma_1(x_4), \cdots, \sigma_n(x_4)\right) \end{array}. \tag{6}$$

Através da composição dos homomorfismos (5) e (6), podemos definir um homomorfismo de $\mathscr{A}$ em $\mathbb{R}^{4n}$ como

$$\sigma_{\mathscr{A}}(x) = \left(\sigma_1(x_1), \cdots, \sigma_n(x_1), \cdots, \sigma_1(x_4), \cdots, \sigma_n(x_4)\right). \tag{7}$$

Definição

Sejam $\mathbb{K}$ um corpo de números totalmente real de grau n, α um elemento totalmente positivo de $\mathbb{K}$ e $\mathscr{A}$ uma álgebra dos quatérnios definida positiva sobre $\mathbb{K}$. Se $x = x_1 + x_2 i + x_3 j + x_4 k \in \mathscr{A}$ então definimos o **homomorfismo torcido $\sigma_{\alpha\mathscr{A}}$ de $\mathscr{A}$ em $\mathbb{R}^{4n}$** *por*

$$\sigma_{\alpha\mathscr{A}}(x) = \Big(\sqrt{2\sigma_1(\alpha)}\sigma_1(x_1), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(x_1), \cdots, \sqrt{2\sigma_1(\alpha)}\sigma_1(x_4), \cdots, \sqrt{2\sigma_n(\alpha)}\sigma_n(x_4)\Big), \quad (8)$$

em que $\sigma_1, \cdots, \sigma_n$ são os n-monomorfismos de $\mathbb{K}$ em $\mathbb{R}$.

Teorema

Sejam $\mathbb{K}$ um corpo de números totalmente real de grau n, α um elemento totalmente positivo de $\mathbb{K}$ e $\mathscr{A}$ uma álgebra dos quatérnios definida positiva sobre $\mathbb{K}$. Se $\mathscr{I} \subseteq \mathscr{M}$ é um ideal à direita de uma ordem maximal dos quatérnios $\mathscr{M}$ de $\mathscr{A}$ com $\mathbb{Z}$-base $\{w_1, \cdots, w_{4n}\}$, então $\sigma_{\alpha\mathscr{A}}(\mathscr{I})$ é um reticulado com base $\{\sigma_{\alpha\mathscr{A}}(w_1), \cdots, \sigma_{\alpha\mathscr{A}}(w_{4n})\}$ e volume

$$\mathscr{V}ol(\sigma_{\alpha\mathscr{A}}(\mathscr{I})) = \left(N_{\mathbb{K}/\mathbb{Q}}(\alpha)d_{\mathbb{K}}\right)^2 \left(N_{\mathbb{K}/\mathbb{Q}}(\det(Trd(v_s\bar{v}_{s'}))_{s,s'=1}^4\right)^{1/2}, \qquad (9)$$

em que $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ é a norma de α, $d_{\mathbb{K}}$ é o discriminante de $\mathbb{K}$ e $\{v_1, v_2, v_3, v_4\}$ é a $\mathbb{O}_{\mathbb{K}}$-basis of $\mathscr{I}$.

Proposição

Seja $\mathscr{A} = (a,b)_{\mathbb{K}}$ *uma álgebra dos quatérnios definidida positiva sobre um corpo de números totalmente real* $\mathbb{K}$ *de grau n. Se* $x \in \mathscr{A}$ *então*

$$|\sigma_{\alpha\mathscr{A}}(x)|^2 = Tr_{\mathbb{K}/\mathbb{Q}}(Trd(\alpha x\bar{x})), \tag{10}$$

em que $\sigma_{\alpha\mathscr{A}}$ *é o homomorfismo definido em (8).*

Logo,

$$||v|| = min\{|\sigma_{\alpha\mathscr{A}}(x)|,\ x \in \mathscr{I},\ x \neq 0\} = min\{\sqrt{Tr_{\mathbb{K}/\mathbb{Q}}(Trd(\alpha x\bar{x}))},\ x \in \mathscr{I},\ x \neq 0\}.$$

Portanto, a densidade de centro do reticulado algébrico $\Lambda = \sigma_{\alpha\mathscr{A}}(\mathscr{I})$ é dada por

$$\delta(\sigma_{\alpha\mathscr{A}}(\mathscr{I})) = \frac{(\sqrt{t_\alpha})^n}{2^n(N_{\mathbb{K}/\mathbb{Q}}(\alpha)d_{\mathbb{K}})^2(N_{\mathbb{K}/\mathbb{Q}}(\det(Trd(v_s\bar{v_{s'}}))^4_{s,s'=1})^{1/2}}, \tag{11}$$

em que $t_\alpha = min\{Tr_{\mathbb{K}/\mathbb{Q}}(Trd(\alpha x\bar{x})),\ x \in \mathscr{I},\ x \neq 0\}$.

- $$\delta(\Lambda) = \frac{||v||^n}{2^n Vol(\Lambda)}$$

- $$\delta(\sigma_\alpha(\mathscr{I})) = \frac{1}{2^n (N(\alpha)|d_{\mathbb{K}}|)^{\frac{1}{2}}} \frac{||v||^{\frac{n}{2}}}{N(\mathscr{I})}$$

- $$\delta(\sigma_{\alpha\mathscr{A}}(\mathscr{I})) = \frac{(\sqrt{t_\alpha})^n}{2^n (N_{\mathbb{K}/\mathbb{Q}}(\alpha) d_{\mathbb{K}})^2 (N_{\mathbb{K}/\mathbb{Q}}(\det(Trd(v_s \bar{v_{s'}}))_{s,s'=1}^4)^{1/2}}$$

$$\begin{array}{c} \mathbb{K} = \mathbb{Q}(\theta) \\ \mid \; n \\ \mathbb{Q} \end{array} \qquad \begin{array}{c} \mathscr{A} = (a,b) \\ \mid \; 4 \\ \mathbb{K} = \mathbb{Q}(\theta) \\ \mid \; n \\ \mathbb{Q} \end{array}$$

Exemplo

Seja $\mathscr{A} = (-1,-1)_{\mathbb{K}=\mathbb{Q}(\sqrt{2})}$ *uma álgebra dos quatérnios definidda positiva e* $\mathscr{M} = \mathscr{I} \supseteq (-1,-1)_{\mathbb{Z}[\sqrt{2}]}$ *uma ordem maximal dos quatérnios caracterizada pela base*

$$B_3 = \left\{1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}\right\}.$$

Tomando $\alpha = 2-\sqrt{2} \in \mathbb{K}$*, podemos construir o reticulado* $\Lambda = \sigma_{\alpha,\mathscr{A}}(\mathscr{I})$ *através do homomorfismo torcido dado em (8). Como* $d_{\mathbb{K}} = 8$ *e* $N(\alpha) = 2$*, aplicando (9), segue que*

$$\mathscr{V}ol(\Lambda) = 2^8.$$

Temos ainda que

$$t_\alpha = min\{Tr_{\mathbb{K}/\mathbb{Q}}(Trd(\alpha x\bar{x})),\ x \in \mathscr{I},\ x \neq 0\} = 8.$$

Exemplos

Então, por (11), a densidade de centro do reticulado algébrico $\Lambda = \sigma_{\alpha\mathscr{A}}(\mathscr{I})$ é

$$\delta(\Lambda) = \frac{\left(\sqrt{8}\right)^8}{2^8 \cdot 2^8} = \frac{2^{12}}{2^{16}} = \frac{1}{16},$$

que é a mesma densidade de centro do reticulado E_8. Portanto, $\Lambda = \sigma_{\alpha\mathscr{A}}(\mathscr{I})$ é uma versão rotacionada do reticulado E_8.

Exemplos

Exemplo

Um reticulado com a mesma densidade de centro do reticulado $\Lambda_{16} = BW_{16}$ *pode ser construído a partir da álgebra dos quaténios definida positiva* $\mathscr{A} = (-1,-1)_{\mathbb{K}_4}$*, em que* $\mathbb{K}_4 = \mathbb{Q}\left(\eta_4\right)$*,* $\eta_4 = \sqrt{2+\sqrt{2}}$*. Uma ordem maximal* $\mathscr{M}_4$ *é caracterizada pela base*

$$\begin{aligned} B_4 &= \left\{1, \frac{\eta_4^2-2}{2}(1+i), \frac{\eta_4^2-2}{2}(1+j), \frac{1+i+j+k}{2}\right\} \\ &= \left\{1, \frac{1}{\sqrt{2}}(1+i), \frac{1}{\sqrt{2}}(1+j), \frac{1+i+j+k}{2}\right\}. \end{aligned}$$

Escolhendo $\alpha = (2-\eta_4)^3$ *e* $\mathscr{I} = \mathscr{M}_4$*, obtemos um reticulado 16-dimensional* $\Lambda = \sigma_{\alpha\mathscr{A}_4}(\mathscr{I})$ *com volume*

$$\mathscr{V}ol(\Lambda) = \left(2^3 \cdot 2^{11}\right)^2 \sqrt{1} = 2^{28}.$$

Exemplos

E,

$$t_\alpha = min\{Tr_{\mathbb{K}/\mathbb{Q}}(Trd(\alpha x\bar{x})),\ x \in \mathscr{I},\ x \neq 0\} = 32.$$

Assim, por (11) a densidade de centro de Λ é

$$\delta(\Lambda) = \frac{\left(\sqrt{32}\right)^{16}}{2^{16} \cdot 2^{28}} = \frac{2^{40}}{2^{44}} = \frac{1}{16},$$

que é a mesma densidade do reticulado BW_{16}.

Seja $\mathscr{A} = (a, b)_{\mathbb{K}}$ uma álgebra dos quatérnios definida positiva sobre um corpo de números $\mathbb{K}$. Se $\mathscr{A}$ é uma álgebra de divisão então podemos construir um Código de Bloco Espaço-Tempo 2×2 com diversidade máxima dado por

$$\mathscr{C} = \left\{ X = \begin{pmatrix} x_1 + x_2\sqrt{a} & x_3 + x_4\sqrt{a} \\ b\left(x_3 - x_4\sqrt{a}\right) & x_2 - x_2\sqrt{a} \end{pmatrix}; x_0, x_1, x_2, x_3 \in \mathscr{O}_{\mathbb{K}} \right\},$$

em que $\det(x) \neq 0$, para todo $x \neq 0$.

- Usualmente $\mathbb{K} = \mathbb{Q}(i)$ ($\mathbb{O}_{\mathbb{K}} = \mathbb{Z}[i]$).

Exemplo

- *Golden code:* $\mathscr{A} = (5, i)_{\mathbb{Q}(i)}$.
- *Silver code:* $\mathscr{A} = (7, i)_{\mathbb{Q}(i)}$.

Códigos de Bloco Espaço-Tempo 2×2

Agora, seja $\mathscr{A} = (a,b)_{\mathbb{K}}$ uma álgebra dos quatérnios definida positiva, em que $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números totalmente real de grau n.

$$\begin{array}{c} \mathscr{A} = (a,b) \\ \mid\ 2 \\ \mathbb{L} = \mathbb{Q}(\sqrt{a}, b) \\ \mid\ 2 \\ \mathbb{K} = \mathbb{Q}(\theta) \\ \mid\ n \\ \mathbb{Q} \end{array}$$

Como $\mathscr{A}$ é definida positiva, ou seja, $Trd(x\bar{y}) > 0$, $\forall x, y \in \mathscr{A}$, então $a, b < 0$ e $\mathbb{L} = \mathbb{Q}(\sqrt{a}, b) = \mathbb{Q}(i\sqrt{-a}, b)$. Portanto,

$$\begin{aligned} \mathscr{C} &= \left\{ X = \begin{pmatrix} x_1 + x_2\sqrt{a} & x_3 + x_4\sqrt{a} \\ b\left(x_3 - x_4\sqrt{a}\right) & x_2 - x_2\sqrt{a} \end{pmatrix} ; x_0, x_1, x_2, x_3 \in \mathbb{O}_{\mathbb{K}} \right\} \\ &= \left\{ X = \begin{pmatrix} y_1 + y_2\sqrt{a} & y_3 + y_4\sqrt{a} \\ b\left(y_3 - y_4\sqrt{a}\right) & y_2 - y_2\sqrt{a} \end{pmatrix} ; y_0, y_1, y_2, y_3 \in \mathbb{Z}[i] \right\} \end{aligned}$$

é um STBC 2×2 via $\mathscr{A} = (a,b)_{\mathbb{K}}$, em que $\mathbb{K}$ é um corpo de números totalmente real.

Exemplo

Sejam $\mathscr{A} = (-1,-1)_{\mathbb{K}}$ *uma álgebra dos quatérnios sobre* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ *e* $\mathscr{M} = \mathscr{I} \supseteq (-1,-1)_{\mathbb{Z}[\sqrt{2}]}$ *uma ordem maximal caracterizada pela base*

$$B = \left\{1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}\right\}.$$

As palavras-código obtidas a partir de $\mathscr{A} = (-1,-1)_{\mathbb{K}}$ *é*

$$X = \begin{pmatrix} x_1 + x_2 i & x_3 + x_4 i \\ -\left(x_3 - x_4 i\right) & x_1 - x_2 i \end{pmatrix},$$

em que $x_0, x_1, x_2, x_3 \in \mathbb{K} = \mathbb{Q}(\sqrt{2})$. *Observe que*

$$x_l = a_l + b_l\sqrt{2}, \quad l = 0,1,2,3.$$

Exemplo

Então

$$\begin{aligned} x_0 + x_1 i &= (a_0 + b_0\sqrt{2}) + (a_1 + b_1\sqrt{2})i \\ &= (a_0 + a_1 i) + (b_0 + b_1 i)\sqrt{2} \\ &= y_0 + y_1\sqrt{2}, \end{aligned}$$

em que $y_0, y_1 \in \mathbb{Q}(i)$. Da mesma forma

$$x_2 + x_3 i = y_2 + y_3\sqrt{2},$$

em que $y_2, y_2 \in \mathbb{Q}(i)$. Portanto, se tomarmos $x_l \in B$ e $y_l \in \mathbb{Z}[i]$, para todo $l = 0, 1, 2, 3$, temos um STBC 2×2 dado por

$$\mathscr{C} = \left\{ X = \begin{pmatrix} x_1 + x_2\sqrt{2} & x_3 + x_4\sqrt{2} \\ -(x_3 - x_4\sqrt{2}) & x_1 - x_2\sqrt{2} \end{pmatrix}; x_0, x_1, x_2, x_3 \in \mathbb{Z}[i] \right\},$$

com diversidade máxima pois $\det(x) \neq 0$, para todo $x \neq 0$.

- C. W. O. Benedito, C. Alves, N. G. Brasil Jr and S. I. R. Costa, "Algebraic construction of lattices via maximal quaternion orders", Journal of Pure and Applied Algebra, vol 224, Issue 5, 106221, 2020, https://doi.org/10.1016/j.jpaa.2019.106221.
- N. G. Brasil Jr, Benedito, C. W. O. Benedito and S. I. R. Costa, "Lattices Associated with Octonion Algebras", Journal of Communication and Information Systems, 33(1), 2018. https://doi.org/10.14209/jcis.2018.24.
- F. Oggier, G. Rekaya, J. . -C. Belfiore and E. Viterbo, "Perfect Space–Time Block Codes", in IEEE Transactions on Information Theory, vol. 52, no. 9, pp. 3885-3902, Sept. 2006, doi: 10.1109/TIT.2006.880010.

Agradecimentos

unesp
UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Faculdade de Engenharia - Câmpus de São João da Boa Vista

ENCONTRO DE CÓDIGOS, RETICULADOS E INFORMAÇÃO
- ENCORI -

UNICAMP

- Prof. Dr. Antonio Aparecido de Andrade
- Prof. Dr. Reginaldo Palazzo Jr.
- Profa. Dra. Sueli. I. R. Costa

Obrigada!