Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Reticulados algébricos construídos a partir de corpos de números cíclicos

Antonio A. Andrade[1], Giliard S. dos Anjos[2]
IBILCE/UNESP, São José do Rio Preto, SP

Resumo. Um problema clássico é o de se obter um empacotamento de esferas de mesmo raio em $\mathbb{R}^n$ de tal modo que a densidade deste empacotamento no espaço seja máxima. Dentre os empacotamentos esféricos, o empacotamento reticulado é um dos mais estudados, sendo que neste os centros das esferas formam um conjunto discreto do $\mathbb{R}^n$, chamado de reticulado. Reticulados algébricos são reticulados construídos a partir da aplicação do homomorfismo canônico em $\mathbb{Z}$-módulos de corpos de números. Neste trabalho, propomos uma construção de reticulados algébricos via corpos de números cíclicos e, a partir dela, apresentamos reticulados algébricos com densidade de centro ótima.

Palavras-chave. Corpo de números cíclico, reticulado algébrico, densidade de centro.

1 Introdução

Um problema clássico na matemática é o de obter um empacotamento de esferas de mesmo raio em $\mathbb{R}^n$ de tal modo que as esferas ocupem o maior espaço possível ou, equivalentemente, que a densidade deste empacotamento seja máxima. Isto pode ser visto como uma versão do 18º problema de Hilbert, proposto em 1900 no Congresso Internacional de Matemática em Paris. O empacotamento reticulado é um tipo de empacotamento esférico onde o conjunto formado pelos centros das esferas formam um conjunto discreto no $\mathbb{R}^n$, chamado de **reticulado**. Um dos parâmetros matemáticos que medem a densidade do empacotamento é a **densidade de centro**, definida como a razão entre o raio e o volume das esferas. Para os espaços $\mathbb{R}^n$ de dimensões 2 a 8 e 24 são conhecidos empacotamentos reticulados com densidade de centro máxima (ver [7, 8, 14]). Reticulados com alta densidade de centro possuem aplicações na teoria da informação (ver [1, 3, 6, 8]).

Seja $\mathbb{K}$ um corpo de números de grau n. Assim, existem n $\mathbb{Q}$-monomorfismos $\sigma_1, \sigma_2, \ldots, \sigma_n$ de $\mathbb{K}$ em $\mathbb{C}$. Podemos reordenar tais monomorfismos de tal forma que $\sigma_1, \ldots, \sigma_{r_1}$ sejam reais e que os monomorfismos não reais satisfaçam $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \ldots, r_2$, onde $n = r_1 + 2r_2$. Defina a função $\sigma_{\mathbb{K}} : \mathbb{K} \to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} = \mathbb{R}^n$ por:

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), Re\{\sigma_{r_1+1}(x)\}, Im\{\sigma_{r_1+1}(x)\}, \ldots, Re\{\sigma_{r_1+r_2}(x)\}, Im\{\sigma_{r_1+r_2}(x)\}). \quad (1)$$

A função $\sigma_{\mathbb{K}}$ é um homomorfismo injetivo de $\mathbb{K}$ em $\mathbb{R}^n$, chamado de **homomorfismo canônico** (ou **homomorfismo de Minkowski**). Se M é um $\mathbb{Z}$-módulo de $\mathbb{K}$ de posto n, então $\sigma_{\mathbb{K}}(M)$ é um reticulado em $\mathbb{R}^n$. Tais reticulados são chamados de **reticulados algébricos** e possuem o diferencial de poderem usar resultados da Teoria Algébrica dos Números para analisar as suas

[1] antonio.andrade@unesp.br
[2] giliard.anjos@ufabc.edu.br

propriedades (ver [1, 12]). Além disso, diversos trabalhos mostram a existência de reticulados algébricos com densidade de centro ótima [4, 5, 9].

Neste trabalho, propomos uma construção de reticulados algébricos via corpos de números cíclicos. Nesta construção, a matriz geradora do reticulado é uma matriz circulante formada pelas raízes do polinômio minimal de um elemento do corpo de números. Construções semelhantes foram usadas em [2, 10, 13], onde foram construídos reticulados com altas densidades de centro para baixas dimensões. Através dessa construção, apresentamos reticulados algébricos construídos via corpos de números cíclicos de grau 3 e 5 com densidades de centro ótimas.

2 Preliminares

Nesta seção, apresentamos definições e resultados básicos utilizados neste trabalho. Mais detalhes podem ser encontrados em [1, 11, 12].

Um reticulado Λ com base $\beta = \{v_1, \ldots, v_m\}$ de $\mathbb{R}^n$ é um conjunto da forma:

$$\Lambda = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{m} a_i v_i, \text{ com } a_i \in \mathbb{Z}\}.$$

Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \ldots, m$, definimos a **matriz geradora** de Λ como sendo

$$B = \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{bmatrix}$$

e a **matriz de Gram** de Λ é a matriz $G = BB^T$. O determinante de Λ é definido como $det(\Lambda) = det(G)$. Se $v = (\alpha_1, \alpha_2, \ldots, \alpha_m)_\beta \in \Lambda$, a sua norma pode ser obtida por:

$$||v||^2 = [\alpha_1, \alpha_2, \ldots, \alpha_m] G [\alpha_1, \alpha_2, \ldots, \alpha_m]^T.$$

O valor $\Lambda_{min} = min\{||v|| \mid v \in \Lambda, v \neq 0\}$ está bem definido e Λ_{min}^2 é chamado de **norma mínima** de Λ. O maior raio ρ para o qual podemos distribuir esferas com este raio centradas nos elementos de Λ e obter um empacotamento reticulado é chamado de **raio de empacotamento** e o seu valor é $\rho = \frac{\Lambda_{min}}{2}$. A densidade de centro do reticulado Λ é definida por:

$$\delta(\Lambda) = \frac{\Lambda_{min}^n}{2^n \cdot \sqrt{det(\Lambda)}}.$$

Seja $\mathbb{K}$ um corpo de números de grau n. Dizemos que $\mathbb{K}$ é um corpo **galoisiano** se $\mathbb{K}$ é uma extensão normal de $\mathbb{Q}$. Se $\mathbb{K}$ é galoisiano e o grupo de Galois $Gal(\mathbb{K} : Q)$ é abeliano (cíclico), então $\mathbb{K}$ é dito ser um corpo de números **abeliano** (**cíclico**).

Sejam $\sigma_1, \sigma_2, \ldots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Dizemos que σ_i é **real** se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$. O corpo $\mathbb{K}$ é dito ser **totalmente real** se todos os σ_i são reais.

O traço $Tr_{\mathbb{K}}(x)$ de um elemento x de $\mathbb{K}$ pode ser obtido por:

$$Tr_{\mathbb{K}}(x) = \sigma_1(x) + \sigma_2(x) + \ldots + \sigma_n(x). \tag{2}$$

Seja $(x_1, x_2, \ldots, x_n)$ uma n-upla de elementos de $\mathbb{K}$ e considere a seguinte matriz

$$[Tr_{\mathbb{K}}(x_i x_j)] = \begin{bmatrix} Tr_{\mathbb{K}}(x_1^2) & Tr_{\mathbb{K}}(x_1x_2) & Tr_{\mathbb{K}}(x_1x_3) & \dots & Tr_{\mathbb{K}}(x_1x_n) \\ Tr_{\mathbb{K}}(x_2x_1) & Tr_{\mathbb{K}}(x_2^2) & Tr_{\mathbb{K}}(x_2x_3) & \dots & Tr_{\mathbb{K}}(x_2x_n) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{K}}(x_nx_1) & Tr_{\mathbb{K}}(x_nx_2) & Tr_{\mathbb{K}}(x_nx_3) & \dots & Tr_{\mathbb{K}}(x_n^2) \end{bmatrix}. \quad (3)$$

O discriminante da n-upla $(x_1, x_2, \dots, x_n)$ é definido por

$$D(x_1, x_2, \dots, x_n) = det([Tr_{\mathbb{K}}(x_i x_j)]).$$

Proposição 2.1. *([11, Teorema 7]) Sejam $x_1, x_2, \dots, x_n$ elementos de $\mathbb{K}$. Os vetores $x_1, x_2, \dots, x_n$ são linearmente dependentes sobre $\mathbb{Q}$ se, e somente se, $D(x_1, x_2, \dots, x_n) = 0$.*

3 Construção de reticulados algébricos via corpos de números cíclicos

Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números cíclico totalmente real de grau n. Então o grupo de Galois $Gal(\mathbb{K} : \mathbb{Q})$ de $\mathbb{K}$ é isomorfo a C_n (grupo cíclico) e, desta forma, $Gal(\mathbb{K} : \mathbb{Q}) = \{I_d, \tau, \tau^2, \dots, \tau^{n-1}\}$, para algum automorfismo τ de $\mathbb{K}$. Para $w \in \mathbb{K}$, suponha que o conjunto $\beta = \{w, \tau(w), \tau^2(w), \dots, \tau^{n-1}(w)\}$ seja base de um $\mathbb{Z}$-módulo M de posto n de $\mathbb{K}$. Assim, $\sigma_{\mathbb{K}}(M)$ é um reticulado algébrico que possui a seguinte matriz geradora:

$$B = \begin{bmatrix} w & \tau(w) & \tau^2(w) & \tau^3(w) & \dots & \tau^{n-2}(w) & \tau^{n-1}(w) \\ \tau(w) & \tau^2(w) & \tau^3(w) & \tau^4(w) & \dots & \tau^{n-1}(w) & w \\ \tau^2(w) & \tau^3(w) & \tau^4(w) & \tau^5(w) & \dots & w & \tau(w) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \tau^{n-2}(w) & \tau^{n-1}(w) & w & \tau(w) & \dots & \tau^{n-4}(w) & \tau^{n-3}(w) \\ \tau^{n-1}(w) & w & \tau(w) & \tau^2(w) & \dots & \tau^{n-3}(w) & \tau^{n-2}(w) \end{bmatrix}. \quad (4)$$

Note que tanto β quanto B são formados pelas raízes do polinômio minimal de w em $\mathbb{K}$. Além disso, B é uma matriz simétrica circulante.

A matriz de Gram de $\sigma_{\mathbb{K}}(M)$ é dada por

$$G = [Tr_{\mathbb{K}}(\tau^i(w)\tau^j(w))],$$

a qual coincide com a matriz (3) quando consideramos a n-upla $(w, \tau(w), \tau^2(w), \dots, \tau^{n-1}(w))$.

A seguir, apresentamos reticulados algébricos de dimensões 3 e 5 construídos de acordo com a construção descrita acima. Tais reticulados possuem a densidade de centro ótima para suas respectivas dimensões.

Exemplo 3.1. *Seja θ uma raiz do polinômio irredutível $p(x) = x^3 + x^2 - 2x - 1$ e seja $\mathbb{K} = \mathbb{Q}(\theta)$. Assim, $\mathbb{K}$ é um corpo de números de grau 3. Note que:*

$$\theta^3 = -\theta^2 + 2\theta + 1. \quad (5)$$

Usando (5), podemos verificar que $-\theta^2 - \theta + 1$ e $\theta^2 - 2$ também são raízes de $p(x)$ em $\mathbb{K}$. Assim, $\mathbb{K}$ é corpo de números cíclico e, desta forma, $\mathbb{K}$ é totalmente real. Além disso, os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são as funções I_d, τ, τ^2, onde τ é o $\mathbb{Q}$-monomorfismo definido por:

$$\tau(\theta) = -\theta^2 - \theta + 1. \quad (6)$$

A partir de (5) *e* (6)*, obtemos:*

$$\tau(\theta^2) = \theta + 2. \tag{7}$$

Seja o elemento $w = \frac{1}{7}(\theta^2 + 3\theta + 4) \in \mathbb{K}$*. Pelas equações* (6) *e* (7)*, temos:*

$$\tau(w) = \tfrac{1}{7}(-3\theta^2 - 2\theta + 9) \text{ e } \tau^2(w) = \tfrac{1}{7}(2\theta^2 - \theta + 1).$$

Vamos mostrar que $w, \tau(w), \tau^2(w)$ *são linearmente independentes. Temos que*

$$Tr_{\mathbb{K}}(w^2) = Tr_{\mathbb{K}}(\tau(w^2)) = Tr_{\mathbb{K}}(\tau^2(w^2)) = w^2 + \tau(w^2) + \tau^2(w^2) \text{ e}$$
$$Tr_{\mathbb{K}}(w\tau(w)) = Tr_{\mathbb{K}}(w\tau^2(w)) = Tr_{\mathbb{K}}(\tau(w)\tau^2(w)) = w\tau(w) + w\tau^2(w) + \tau(w)\tau^2(w).$$

Usando (2)*,* (6) *e* (7)*, obtemos* $Tr_{\mathbb{K}}(w^2) = 2$ *e* $Tr_{\mathbb{K}}(w\tau(w)) = 1$*. Então a matriz* (3) *relativa a tripla* $(w, \tau(w), \tau^2(w))$ *é dada por:*

$$G = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

Como $D(w, \tau(w), \tau^2(w)) = det(G) = 4$*, temos que o conjunto* $\beta = \{w, \tau(w), \tau^2(w)\}$ *é linearmente independente. Seja* M *o* $\mathbb{Z}$*-módulo gerado por* β*. Assim, a matriz de Gram do reticulado algébrico* $\sigma_{\mathbb{K}}(M)$ *será igual a* G *e a sua matriz geradora será:*

$$B = \begin{bmatrix} w & \tau(w) & \tau^2(w) \\ \tau(w) & \tau^2(w) & w \\ \tau^2(w) & w & \tau(w) \end{bmatrix}.$$

Já vimos que $det(\sigma_{\mathbb{K}}(M)) = det(G) = 4$*. Agora, vamos calcular a norma mínima de* $\sigma_{\mathbb{K}}(M)$*. Seja* $v = [\alpha_1, \alpha_2, \alpha_3]B$ *um vetor não nulo de* $\sigma_{\mathbb{K}}(M)$*. Assim:*

$$||v||^2 = [\alpha_1, \alpha_2, \alpha_3]G[\alpha_1, \alpha_2, \alpha_3]^T = 2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3).$$

Desta forma, $||v||^2$ *é um número par maior do que* 0*. Se* $\alpha_1 = 1$ *e* $\alpha_2 = \alpha_3 = 0$*, então* $||v||^2 = 2$*. Logo, a norma mínima de* $\sigma_{\mathbb{K}}(M)$ *é igual a* 2*. Com isso, a densidade de centro de* $\sigma_{\mathbb{K}}(M)$ *será*

$$\delta(\sigma_{\mathbb{K}}(M)) = \frac{(\sqrt{2})^3}{2^3 \cdot 2} = \frac{1}{4\sqrt{2}} \approx 0.176777,$$

sendo esta a densidade de centro ótima para a dimensão 3 *(ver [8, Tabela I.1, pg. xix]).*

Exemplo 3.2. *Seja* θ *uma raiz do polinômio irredutível* $p(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ *e seja* $\mathbb{K} = \mathbb{Q}(\theta)$*. Temos que* $\theta^5 = -\theta^4 + 4\theta^3 + 3\theta^2 - 3\theta - 1$ *e, a partir disso, podemos verificar que* $\theta^2 - 2$*,* $\theta^4 - 4\theta^2 + 2$*,* $\theta^3 - 3\theta$ *e* $-\theta^4 - \theta^3 + 3\theta^2 + 2\theta - 1$ *também são raízes de* $p(x)$ *em* $\mathbb{K}$*. Com isso,* $\mathbb{K}$ *é galoisiano e, portanto,* $\mathbb{K}$ *é um corpo de números cíclico totalmente real de grau* 5*. Desta forma, os* $\mathbb{Q}$*-monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são as funções* $I_d, \tau, \tau^2, \tau^3, \tau^4$*, onde* τ *é o* $\mathbb{Q}$*-monomorfismo definido por:*

$$\tau(\theta) = \theta^2 - 2. \tag{8}$$

A partir desta equação, obtemos:

$$\begin{aligned} \tau(\theta^2) &= \theta^4 - 4\theta^2 + 4, \\ \tau(\theta^3) &= -\theta^4 - \theta^3 + 6\theta^2 + 2\theta - 7, \\ \tau(\theta^4) &= 4\theta^4 + \theta^3 - 16\theta^2 - 3\theta + 14. \end{aligned} \tag{9}$$

Seja o elemento $w = \frac{1}{11}(-2\theta^4 + \theta^3 + 9\theta^2 - 6\theta - 11) \in \mathbb{K}$*. Pelas equações* (8) *e* (9)*, temos:*

$$\tau(w) = \frac{1}{11}(-3\theta^3 - 4\theta^2 + 8\theta + 2),\ \tau^2(w) = \frac{1}{11}(-\theta^4 + 3\theta^3 + 6\theta^2 - 6\theta - 9),$$
$$\tau^3(w) = \frac{1}{11}(-\theta^4 - 4\theta^3 + 4\theta^2 + 9\theta - 8),\ \tau^4(w) = \frac{1}{11}(4\theta^4 + 3\theta^3 - 15\theta^2 - 5\theta + 4).$$

Vamos mostrar que $\beta = \{w, \tau(w), \tau^2(w), \tau^3(w), \tau^4(w)\}$ *é linearmente independente. Usando* (2), (8) *e* (9), *obtemos que a matriz* (3) *relativa a* 5*-upla* $(w, \tau(w), \tau^2(w), \tau^3(w), \tau^4(w))$ *é*

$$G = \begin{bmatrix} 2 & 0 & 1 & 1 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 1 & 0 & 2 & 0 & 1 \\ 1 & 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 2 \end{bmatrix}.$$

Assim, $D(w, \tau(w), \tau^2(w), \tau^3(w), \tau^4(w)) = det(G) = 4$ *e temos que o conjunto* β *é linearmente independente. Seja* M *o* $\mathbb{Z}$*-módulo gerado por* β*. Então a matriz geradora do reticulado algébrico* $\sigma_{\mathbb{K}}(M)$ *será da forma* (4) *e sua matriz de Gram será igual a* G*. Com isso, já temos que* $det(\sigma_{\mathbb{K}}(M)) = 4$.

Agora, vamos calcular a norma mínima de $\sigma_{\mathbb{K}}(M)$*. Sendo* $v = [\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5]B$ *um vetor não nulo de* $\sigma_{\mathbb{K}}(M)$, *temos*

$$||v||^2 = 2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_5^2) + 2(\alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_2\alpha_5 + \alpha_3\alpha_5).$$

Com isso, analogamente ao exemplo anterior, obtemos que a norma mínima de $\sigma_{\mathbb{K}}(M)$ *é igual a* 2. *Logo, a densidade de centro de* $\sigma_{\mathbb{K}}(M)$ *será*

$$\delta(\sigma_{\mathbb{K}}(M)) = \frac{(\sqrt{2})^5}{2^5 \cdot 2} = \frac{1}{8\sqrt{2}} \approx 0.088388,$$

sendo esta a densidade de centro ótima para a dimensão 5 *(ver [8, Tabela I.1, pg. xix]).*

4 Considerações Finais

Neste trabalho, apresentamos uma construção de reticulados algébricos via corpos de números cíclicos totalmente reais. Nesta construção, a matriz geradora do reticulado é uma matriz simétrica circulante e a matriz de Gram pode ser determinada a partir da análise da função traço em elementos do corpo. Nos exemplos apresentados aqui, observamos que pode ser obtido um elemento do corpo de números de tal forma que a matriz de Gram do reticulado construído a partir dele tenha uma forma simples, facilitando-se assim a análise das propriedades do reticulado.

Referências

[1] C. Alves e A. A. Andrade. **Reticulados via corpos ciclotômicos**. Editora UNESP, 2014. ISBN: 978-85-68334-39-3.

[2] A. A. Andrade e L. S. Facini. **Discriminante de polinômios e aplicações**. Online. Acessado em 29/03/2022, `https://www.ibilce.unesp.br/Home/Departamentos/Matematica/xxxsemat/mm1-andrade-a.a_-facinel.s.pdf`.

[3] A. A. Andrade e R. Palazzo Jr. "Linear codes over finite rings". Em: **TEMA. Tendências em Matemática Aplicada e Computacional** 6(2) (2005), pp. 207–217. DOI: `10.5540/tema.2005.06.02.0207`.

[4] A. A. Andrade et al. "Constructions of algebraic lattices". Em: **Computational and Applied Mathematics** 29(3) (2010), pp. 493–505. ISSN: 0101-8205.

[5] A. A. Andrade et al. "Constructions of Dense Lattices over Number Fields". Em: **TEMA. Tendências em Matemática Aplicada e Computacional** 21(1) (2020), pp. 57–63. DOI: 10.5540/tema.2020.021.01.0057.

[6] J. Boutros et al. "Good lattice constellations for both the Rayleigh fading and Gaussian channels". Em: **IEEE Trans. Inform. Theory** 42(2) (1996), pp. 502–518. DOI: 10.1109/18.485720.

[7] H. Cohn et al. "The sphere packing problem in dimension 24". Em: **Ann. of Math.** 185(3) (2017), pp. 1017–1033. DOI: 10.4007/annals.2017.185.3.8.

[8] J. H. Conway e N. J. A. Sloane. **Sphere Packings, Lattices and Groups**. New York: Springer-Verlag, 1999. ISBN: 978-1-4757-6568-7.

[9] A. J. Ferrari. "Reticulados Algébricos via Corpos Abelianos". Dissertação de mestrado. IBILCE/UNESP, 2015.

[10] J. C. Interlando et al. "Four-dimensional lattices from $Q(\sqrt{3}, \sqrt{5})$". Em: **International Journal of Applied Mathematics** 30 (2017), pp. 401–408. DOI: 10.12732/ijam.v30i5.4.

[11] D. A. Marcus. **Number Fields**. 1a. ed. New York: Springer-Verlag, 1977. ISBN: 978-0-387-90279-1.

[12] P. Samuel. **Algebraic Theory of Numbers**. Paris: Hermann, 1970.

[13] T. M. Souza. "Reticulados algébricos em corpos de números abelianos". Dissertação de mestrado. IBILCE/UNESP, 2004.

[14] M. S. Viazovska. "The sphere packing problem in dimension 8". Em: **Ann. of Math.** 185(3) (2017), pp. 991–1015. DOI: 10.4007/annals.2017.185.3.7.

