Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Densidade de Centro de uma Família de Reticulados Cíclicos

William Lima da Silva Pinto[1], Carina Alves[2]
Departamento de Matemática, UNESP, Rio Claro, SP

Resumo. Um reticulado é dito ser cíclico se a rotação cíclica de todo vetor do reticulado pertence ao reticulado. Neste trabalho apresentamos uma estratégia para simplificar a norma mínima de uma família de reticulados cíclicos, estabelecemos uma expressão para o cálculo do determinante de tais reticulados e avaliamos sob quais condições é possível obter reticulados com maior densidade de centro.

Palavras-chave. Reticulados Cíclicos, Norma Mínima, Densidade de Centro, Matriz Geradora

1 Introdução

Um reticulado n-dimensional é um subgrupo aditivo discreto de $\mathbb{R}^n$, consistindo de combinações lineares de vetores linearmente independentes em $\mathbb{R}^n$ com coeficientes inteiros. Da teoria de reticulados sabe-se que a densidade de centro de um reticulado depende da norma mínima [3]. Encontrar um vetor de norma mínima de um reticulado não é uma tarefa fácil [7] e tem chamado a atenção de matemáticos e pesquisadores da computação por causa de sua relação com programação linear inteira [1, 5].

Classes de reticulados que tem o cálculo do vetor de norma mínima simplificado, seja por construção ou por algoritmos [2, 3, 6], são desejáveis. Neste trabalho, consideramos uma classe particular de reticulados cíclicos, em que o cálculo do vetor de norma mínima pode ser simplificado sob determinadas condições. Reticulados cíclicos foram introduzidos por Micciancio em [8] e suas propriedades foram estudadas nos últimos anos por vários autores devido à sua importância na criptografia [9].

A abordagem mais comum encontrada na literatura tem sido realizar deslocamentos circulares em um vetor $\mathbf{u} \in \mathbb{Z}^n$, [4]. Aqui, consideramos $\mathbf{u} \in \mathbb{R}^n$ e exibimos algumas estratégias para simplificar o cálculo do vetor de norma mínima e determinante da matriz geradora do reticulado. Neste cenário, encontramos reticulados tão densos quanto o reticulado D_n, com n ímpar.

Este trabalho é organizado como segue. Na Seção 2 apresentamos o conceito de reticulados, reticulados cíclicos e de alguns parâmetros relacionados a reticulados. Na Seção 3 fornecemos condições sob as quais a norma do vetor de um reticulado cíclico pode ser simplificada. Na Seção 4 apresentamos a matriz geradora e densidade de centro de um reticulado cíclico. Finalmente, na Seção 5, apresentamos nossa conclusão.

[1] williamlima.algebra@gmail.com
[2] carina.alves@unesp.br

2 Reticulados Cíclicos

Dizemos que $\Lambda \subset \mathbb{R}^n$ é um *reticulado* se existem vetores linearmente independentes $\mathbf{v}_1, \ldots, \mathbf{v}_m \in \mathbb{R}^n$, com $m \leq n$, tal que todo $\boldsymbol{v} \in \Lambda$ pode ser escrito como $\boldsymbol{v} = \sum_{i=1}^{m} x_i \mathbf{v}_i$, onde $x_i \in \mathbb{Z}$ para $i = 1, 2, \ldots, m$. O conjunto $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ é chamado uma *base* para Λ. Uma matriz G cujas linhas são esses vetores é dita ser uma *matriz geradora* para Λ e sua *matriz de Gram* é $H = GG^t$, onde ^{t} representa a transposição. O *determinante* de Λ é dado por $det(\Lambda) = det(H)$ e ele é um invariante sob a mudança de base [3]. O *mínimo* de um reticulado Λ é definido por

$$|\Lambda| = min\{\|\boldsymbol{v}\|^2 : \boldsymbol{v} \in \Lambda,\ \boldsymbol{v} \neq 0\}. \tag{1}$$

Neste trabalho vamos considerar reticulados de posto completo, isto é, quando $m = n$ e neste caso, sua *densidade de centro* é dada por

$$\delta(\Lambda) = \frac{(\sqrt{|\Lambda|}/2)^n}{|det(G)|}. \tag{2}$$

Seja $n \geq 2$ e defina o operador rot : $\mathbb{R}^n \to \mathbb{R}^n$ por $\text{rot}(x_1, x_2, \cdots, x_{n-1}, x_n) = (x_n, x_1, x_2, \cdots, x_{n-1})$. Um reticulado $\Lambda \subset \mathbb{R}^n$ é dito ser *cíclico* se para todo $\boldsymbol{v} \in \Lambda$, $\text{rot}(\boldsymbol{v}) \in \Lambda$. Se existe um vetor $\mathbf{u} = (\rho_1, \rho_2, \cdots, \rho_n) \in \mathbb{R}^n$ tal que $\{\mathbf{u}, \text{rot}(\mathbf{u}), \cdots, \text{rot}^{n-1}(\mathbf{u})\}$ é uma base para Λ, então Λ é cíclico. Denotamos tal reticulado por $\Lambda_{\mathbf{u}}$.

O vetor $\mathbf{u}$ determina uma matriz circulante $G_{\mathbf{u}}$ da forma

$$G_{\mathbf{u}} = \begin{pmatrix} \rho_1 & \rho_2 & \cdots & \rho_n \\ \rho_n & \rho_1 & \cdots & \rho_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_2 & \rho_3 & \cdots & \rho_1 \end{pmatrix}.$$

Algumas propriedades gerais de reticulados cíclicos foram discutidas em [4] quando $\mathbf{u} \in \mathbb{Z}^n$. Investigamos neste trabalho, no entanto, o caso em que $\mathbf{u} \in \mathbb{R}^n$ e por uma abordagem diferente da apresentada em [4, 8]. Vamos impor condições sobre o vetor $\mathbf{u}$ tais que $\det(G_{\mathbf{u}}) \neq 0$ e $\Lambda_{\mathbf{u}}$ seja o mais denso possível.

3 Norma do Reticulado Cíclico $\Lambda_{\mathbf{u}}$

Dado um vetor arbitrário $\boldsymbol{w} \in \Lambda_{\mathbf{u}}$, estamos interessados em calcular $||\boldsymbol{w}||^2$, a fim de investigar $|\Lambda_{\mathbf{u}}|$. Para isso, considere o conjunto $I_n = \{1, 2, \cdots, n\}$ e para cada $r \in \{1, 2, \cdots, n-1\}$ defina

$$P_n(r)\,\mathbf{x} = \sum_{\substack{i,j \in I_n \\ i<j \\ j-i=r}} x_i x_j \quad \text{e} \quad \mathcal{P}_n(r)\,\mathbf{x} = \sum_{\substack{i,j \in I_n \\ i<j \\ j-i \in \{r, n-r\}}} x_i x_j, \tag{3}$$

para todo $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{R}^n$. Consideramos ao longo de todo o trabalho $a, b \in \mathbb{R}$, os coeficientes que multiplicam t^{n-1} e t^{n-2} em $f(t) = \prod_{i=1}^{n}(t - \rho_i) \in \mathbb{R}[t]$, respectivamente. Segue das fórmulas de Viète [10], que $-a = \sum_{i=1}^{n} \rho_i$ e $b = \sum_{i<j} \rho_i \rho_j$, consequentemente, $\sum_{i=1}^{n} \rho_i^2 = a^2 - 2b$.

Quando consideramos um reticulado cíclico caracterizamos a norma de um vetor como no teorema a seguir.

Teorema 3.1. *Sejam* $n \geq 2$ *e* $\mathbf{u} = (\rho_1, ..., \rho_n) \in \mathbb{R}^n$ *tal que* $\det G_{\mathbf{u}} \neq 0$. *Então, para* $\boldsymbol{w} = \sum_{i=1}^{n} x_i rot^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$,

$$\|\boldsymbol{w}\|^2 = (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + 2\sum_{r=1}^{\lfloor \frac{n-1}{2} \rfloor} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x} + \tau_n\Big(4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x}\Big), \tag{4}$$

onde $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$ *e* $\tau_n = (1 + (-1)^n)/2$.

Demonstração. Seja $\boldsymbol{w} = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$. Usando a definição e propriedades do produto interno, segue que

$$\begin{aligned}
\|\boldsymbol{w}\|^2 &= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \sum_{i=1}^{n} x_i^2 \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{i-1}(\mathbf{u})\rangle + \sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \sum_{i=1}^{n} x_i^2 \|\mathrm{rot}^{i-1}(\mathbf{u})\|^2 + \sum_{r=1}^{n-1}\sum_{\substack{i,j\in I_n\\ |i-j|=r}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= \|\mathbf{u}\|^2 \sum_{i=1}^{n} x_i^2 + \tau_n 2\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=r}} x_i x_j \langle \mathrm{rot}^{i-1}(\mathbf{u}), \mathrm{rot}^{j-1}(\mathbf{u})\rangle \\
&= (\rho_1^2 + ... + \rho_n^2)\sum_{i=1}^{n} x_i^2 + \tau_n 2\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=\frac{n}{2}}} x_i x_j \Big(2\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\Big) + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\sum_{\substack{i,j\in I_n\\ i<j\\ j-i=r}} x_i x_j \mathcal{P}_n(r)\,\mathbf{u} \\
&= (a^2 - 2b)\sum_{i=1}^{n} x_i^2 + \tau_n 4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x} + 2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1} \mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x}.
\end{aligned} \tag{5}$$

Note que, se $r \neq \frac{n}{2}$, então

$$\mathcal{P}_n(r)\,\mathbf{x} = P_n(r)\,\mathbf{x} + P_n(n-r)\,\mathbf{x} = P_n(n-(n-r))\,\mathbf{x} + P_n(n-r)\,\mathbf{x} = \mathcal{P}_n(n-r)\,\mathbf{x}. \tag{6}$$

Logo, se n é par e após algumas manipulações algébricas temos que,

$$\begin{aligned}
2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1} \mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x} &= 2\Big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x} + \mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x} + ... + \mathcal{P}_n(\tfrac{n}{2}-1)\,\mathbf{u}\,P_n(\tfrac{n}{2}-1)\,\mathbf{x} + \\
&\qquad + \mathcal{P}_n(\tfrac{n}{2}+1)\,\mathbf{u}\,P_n(\tfrac{n}{2}+1)\,\mathbf{x} + ... + \mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x}\Big) \\
&= 2\sum_{r=1}^{\frac{n}{2}-1} \mathcal{P}_n(r)\,\mathbf{u}\,(P_n(r)\,\mathbf{x} + P_n(n-r)\,\mathbf{x}) \\
&= 2\sum_{r=1}^{\frac{n-2}{2}} \mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}.
\end{aligned} \tag{7}$$

DOI: 10.5540/03.2023.010.01.0039

Por outro lado, se n é ímpar,

$$\begin{aligned}
2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x} &= 2\big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x}+\mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x}+\ldots+\mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x}\big)\\
&= 2\Big(\mathcal{P}_n(1)\,\mathbf{u}\,P_n(1)\,\mathbf{x}+\mathcal{P}_n(n-1)\,\mathbf{u}\,P_n(n-1)\,\mathbf{x}+\\
&\quad+\mathcal{P}_n(2)\,\mathbf{u}\,P_n(2)\,\mathbf{x}+\mathcal{P}_n(n-2)\,\mathbf{u}\,P_n(n-2)\,\mathbf{x}+\\
&\quad+\ldots+\mathcal{P}_n(\tfrac{n-1}{2})\,\mathbf{u}\,P_n(\tfrac{n-1}{2})\,\mathbf{x}+\mathcal{P}_n(\tfrac{n-1}{2}+1)\,\mathbf{u}\,P_n(\tfrac{n-1}{2}+1)\,\mathbf{x}\Big)\\
&= 2\sum_{r=1}^{\frac{n-1}{2}}\mathcal{P}_n(r)\,\mathbf{u}\,(P_n(r)\,\mathbf{x}+P_n(n-r)\,\mathbf{x})\\
&= 2\sum_{r=1}^{\frac{n-1}{2}}\mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}. \qquad (8)
\end{aligned}$$

Como

$$\left\lfloor\frac{n-1}{2}\right\rfloor=\begin{cases}\frac{n-1}{2} & \text{se } n \text{ é ímpar}\\ \frac{n-2}{2} & \text{se } n \text{ é par,}\end{cases}$$

segue que

$$2\sum_{\substack{r=1\\ r\neq\frac{n}{2}}}^{n-1}\mathcal{P}_n(r)\,\mathbf{u}\,P_n(r)\,\mathbf{x}=2\sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor}\mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}. \qquad (9)$$

Portanto,

$$\|\boldsymbol{w}\|^2=(a^2-2b)\sum_{i=1}^{n}x_i^2+\tau_n 4\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{u}\,\mathcal{P}_n(\tfrac{n}{2})\,\mathbf{x}+2\sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor}\mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}, \qquad (10)$$

o que prova o teorema. □

Para facilitar o cálculo da norma mínima, neste trabalho vamos considerar $\mathcal{P}_n(r)\,\mathbf{u}$ igual a zero, exceto no máximo um único $r\in\{1,2,...,\lfloor n/2\rfloor\}$. Denotemos tal r por r_0. Nessas condições, usando o Teorema 3.1 e o fato que $b=2\sum_{r=1}^{\lfloor\frac{n}{2}\rfloor}\mathcal{P}_n(r)\,\mathbf{u}$ podemos provar o corolário que segue.

Corolário 3.1. *Sejam $n\geq 2$, $\mathbf{x}=(x_1,\cdots,x_n)\in\mathbb{Z}^n$ e $\mathbf{u}=(\rho_1,...,\rho_n)\in\mathbb{R}^n$ tal que $\det G_{\mathbf{u}}\neq 0$. Se $\mathcal{P}_n(r_0)\,\mathbf{u}\neq 0$ e $\mathcal{P}_n(r)\,\mathbf{u}=0$ para $r\neq r_0$, em que $r, r_0\in\{1,2,...,\lfloor n/2\rfloor\}$, então para cada $\boldsymbol{w}=\sum_{i=1}^{n}x_i rot^{i-1}(\mathbf{u})\in\Lambda_{\mathbf{u}}$,*

$$\|\boldsymbol{w}\|^2=\begin{cases}(a^2-2b)\sum_{i=1}^{n}x_i^2+4b\mathcal{P}_n(r_0)\,\mathbf{x}, & \text{se } n \text{ é par e } r_0=\frac{n}{2}\\ (a^2-2b)\sum_{i=1}^{n}x_i^2+2b\mathcal{P}_n(r_0)\,\mathbf{x}, & \text{caso contrário.}\end{cases} \qquad (11)$$

Note que se n é par e $r_0=\frac{n}{2}$ então $2\sum_{r=1}^{\lfloor\frac{n-1}{2}\rfloor}\mathcal{P}_n(r)\,\mathbf{u}\,\mathcal{P}_n(r)\,\mathbf{x}=0$. Neste trabalho focamos no caso n ímpar e $r_0\neq\frac{n}{2}$.

4 Matriz Geradora e Densidade de Centro do Reticulado Cíclico $\Lambda_{\mathbf{u}}$

Nesta seção, vamos obter uma expressão para o determinante da matriz geradora de um reticulado cíclico $\Lambda_{\mathbf{u}}$, para posteriormente estabelecer sua densidade de centro.

Teorema 4.1. *Sejam n ímpar, $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$ e $\mathbf{u} = (\rho_1, ..., \rho_n) \in \mathbb{R}^n$. Se $\mathcal{P}_n(1)\,\mathbf{u} = ... = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = ... = \mathcal{P}_n(\lfloor n/2 \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, ..., \lfloor (n-1)/2 \rfloor\}$, então*

$$\det G_{\mathbf{u}} = -a \prod_{j=1}^{\frac{n-1}{2}} \left(a^2 - 2b + b\big(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\big)\right), \tag{12}$$

onde $\zeta_n = \cos(2\pi/n) + i\, sen(2\pi/n)$ é uma raiz n-ésima primitiva da unidade.

Demonstração. Como $G_{\mathbf{u}}$ é cíclica, seus autovalores são da forma $\lambda_j = \rho_1 + \rho_2\zeta_n^j + ... + \rho_n\zeta_n^{(n-1)j}$, $j = 0, 1, ..., n-1$.

É conhecido que o determinante de uma matriz é o produto de seus autovalores, isto é,

$$\det G_{\mathbf{u}} = \prod_{j=0}^{n-1} (\rho_1 + \rho_2\zeta_n^j + ... + \rho_n\zeta_n^{(n-1)j}) = -a \prod_{j=1}^{n-1} (\rho_1 + \rho_2\zeta_n^j + ... + \rho_n\zeta_n^{(n-1)j}). \tag{13}$$

Agora,

$$\prod_{j=1}^{n-1} (\rho_1 + \rho_2\zeta_n^j + ... + \rho_n\zeta_n^{(n-1)j}) = \prod_{j=1}^{\frac{n-1}{2}} (\rho_1 + \rho_2\zeta_n^j + ... + \rho_n\zeta_n^{(n-1)j})(\rho_1 + \rho_2\zeta_n^{-j} + ...+ \\ + \rho_n\zeta_n^{(n-1)(n-j)}). \tag{14}$$

Note que cada termo do produto acima é da forma

$$(\rho_1^2 + ... + \rho_n^2) + \mathcal{P}_n(1)\,\mathbf{u}\,(\zeta_n^j + \zeta_n^{-j}) + \mathcal{P}_n(2)\,\mathbf{u}\,(\zeta_n^{2j} + \zeta_n^{-2j}) + ... + \mathcal{P}_n(\tfrac{n-1}{2})\,\mathbf{u}\left(\zeta_n^{\frac{n-1}{2}j} + \zeta_n^{-\frac{n-1}{2}j}\right).$$

Consequentemente, como $\mathcal{P}_n(1)\,\mathbf{u} = ... = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = ... = \mathcal{P}_n((n-1)/2) = 0$, temos que

$$\begin{aligned} \det G_{\mathbf{u}} &= -a \prod_{j=1}^{\frac{n-1}{2}} \left(a^2 - 2b + \mathcal{P}_n(r_0)\,\mathbf{u}\,\left(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\right)\right) \\ &= -a \prod_{j=1}^{\frac{n-1}{2}} \left(a^2 - 2b + b\big(\zeta_n^{r_0 j} + \zeta_n^{-r_0 j}\big)\right), \end{aligned} \tag{15}$$

o que prova o resultado. □

Veremos que a condição $0 \neq a^2 = 4b$ fornece reticulados interessantes.

Corolário 4.1. *Sejam n ímpar e $\mathbf{u} = (\rho_1, ..., \rho_n) \in \mathbb{R}^n$ tal que $\mathcal{P}_n(1)\,\mathbf{u} = ... = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = ... = \mathcal{P}_n(\lfloor n/2 \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, ..., \lfloor (n-1)/2 \rfloor\}$ tal que $n/(r_0, n) \notin 2\mathbb{Z}$. Se $a^2 = 4b \neq 0$, então*

$$\det G_{\boldsymbol{u}} = \pm \frac{a^n}{2^{n-(r_0,n)}}, \tag{16}$$

onde $(r_0, n) = mdc(r_0, n)$.

Demonstração. Pelo Teorema 4.1, como $a^2 = 4b$, segue que

$$\det G_{\mathbf{u}} = -\frac{a^n}{2^{n-1}} \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j} + 2). \tag{17}$$

Como n é ímpar, segue que $mdc(2, n) = 1$. Desta forma, após algumas manipulações algébricas e usando o fato que $\zeta_n^{r_0 j} = 1 \Leftrightarrow j \in \left\{ \frac{n}{(r_0,n)}, \frac{2n}{(r_0,n)}, ..., \frac{((r_0,n)-1)n}{(r_0,n)} \right\}$, obtemos

$$\begin{aligned} \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{r_0 j} + \zeta_n^{-r_0 j} + 2) &= \prod_{j=1}^{\frac{n-1}{2}} (\zeta_n^{2r_0 j} + \zeta_n^{-2r_0 j} + 2) \\ &= \prod_{j=1}^{n-1} (1 + \zeta_n^{r_0 j}) \\ &= 2^{(r_0,n)-1} \left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) \right). \end{aligned} \tag{18}$$

Além disso,

$$\left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{r_0 j}) \right) \left(\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) \right) = \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{2r_0 j}) = \prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 - \zeta_n^{r_0 j}). \tag{19}$$

Logo,

$$\prod_{\substack{1 \le j \le n-1 \\ \zeta_n^{r_0 j} \neq 1}} (1 + \zeta_n^{r_0 j}) = 1, \tag{20}$$

e portanto,

$$\det G_{\mathbf{u}} = -\frac{a^n}{2^{n-1}} 2^{(r_0,n)-1} = -\frac{a^n}{2^{n-(r_0,n)}}. \tag{21}$$

□

Teorema 4.2. *Sejam n ímpar e $\mathbf{u} = (\rho_1, ..., \rho_n) \in \mathbb{R}^n$ tal que $\mathcal{P}_n(1)\,\mathbf{u} = ... = \mathcal{P}_n(r_0 - 1)\,\mathbf{u} = \mathcal{P}_n(r_0 + 1)\,\mathbf{u} = ... = \mathcal{P}_n(\lfloor n/2 \rfloor)\,\mathbf{u} = 0$ para algum $r_0 \in \{1, 2, ..., \lfloor (n-1)/2 \rfloor\}$ tal que $n/(r_0, n) \notin 2\mathbb{Z}$. Se $0 \neq a^2 = 4b$, então*

$$\delta(\Lambda_{\mathbf{u}}) = \frac{1}{2^{(r_0,n)+\frac{n}{2}}}, \tag{22}$$

onde $(r_0, n) = mdc(r_0, n)$.

Demonstração. Pelo Corolário 3.1, para todo $\boldsymbol{w} = \sum_{i=1}^{n} x_i \mathrm{rot}^{i-1}(\mathbf{u}) \in \Lambda_{\mathbf{u}}$,

$$||\boldsymbol{w}||^2 = \frac{a^2}{2} \left(\sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x} \right), \tag{23}$$

onde $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{Z}^n$. Agora, note que se $\mathbf{x} = (1, 0, ..., 0)$ então $\sum_{i=1}^{n} x_i^2 + \mathcal{P}_n(r_0)\,\mathbf{x} = 1$. Portanto, $|\Lambda_{\mathbf{u}}| = \frac{a^2}{2}$. Aplicando o Corolário 4.1 em (2), segue o resultado. □

DOI: 10.5540/03.2023.010.01.0039

Note que, em particular, se $mdc(r_0, n) = 1$ então a densidade de centro do reticulado $\Lambda_{\mathbf{u}}$ é igual a densidade de centro do reticulado D_n. O reticulado D_n tem a melhor densidade de centro para $n = 3, 4$ e 5, [3].

5 Considerações Finais

Neste trabalho apresentamos uma expressão para a norma de um vetor arbitrário em um reticulado cíclico. Vimos que sob determinadas restrições e considerando n ímpar, obtivemos uma família de reticulados cíclicos que possui a mesma densidade de centro do reticulado D_n. Estabelecer os resultados e analisar a densidade de centro para n par é uma das perspectivas futuras deste trabalho.

Agradecimentos

Esta pesquisa é financiada pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Processos: 2023/07667-2, 2019/20800-8 e 2018/12702-3.

Referências

[1] L. Babai. "On Lovász' Lattice Reduction and the Nearest Lattice Point Problem". Em: **Combinatorica** 6 (1986), pp. 1–13. DOI: 10.1007/BF02579403.

[2] Y. -L. Chuang, C. -I. Fan e Y. -F. Tseng. "An Efficient Algorithm for the Shortest Vector Problem". Em: **IEEE Access** 6 (2018), pp. 61478–61487. DOI: 10.1109/ACCESS.2018.2876401.

[3] J. H. Conway e N. J. A. Sloane. **Sphere Packings, Lattices and Groups**. 3a. ed. New York: Springer, 1999. ISBN: 978-1-4757-6568-7.

[4] L. Fukshansky e X. Sun. "On the Geometry of Cyclic Lattices". Em: **Discrete Computational Geometry** 52 (2014), pp. 240–259. DOI: 10.1007/s00454-014-9608-3.

[5] R. Kannan. "Minkowski's Convex Body Theorem and Integer Programming". Em: **Mathematics of Operations Research** 3 (1987), pp. 415–440. DOI: 10.1287/moor.12.3.415.

[6] R. G. McKilliam, W. D. Smith e V. L. Clarkson. "Linear-Time Nearest Point Algorithms for Coxeter Lattices". Em: **IEEE Transactions on Information Theory** 56 (2010), pp. 1015–1022. DOI: 10.1109/TIT.2009.2039090.

[7] D. Micciancio. "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions". Em: **Computational Complexity** 16 (2007), pp. 365–411. DOI: 10.1007/s00037-007-0234-9.

[8] D. Micciancio. "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions from Worst-Case Complexity Assumptions". Em: **Proceedings of the 43rd Symposium on Foundations of Computer Science**. 2002, pp. 356–365. ISBN: 0769518222.

[9] C. Peikert e A. Rosen. "Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices". Em: **Theory of Cryptography, Third Theory of Cryptography Conference**. Vol. 3876. Springer, 2006, pp. 145–166. DOI: 10.1007/11681878_8.

[10] E. B. Vinberg. **A Course in Algebra**. 1a. ed. Moscow: American Mathematical Society, 2003. ISBN: 978-0821833186.

