BEJOM

Brazilian Electronic Journal of Mathematics. 2025, v.6: 73442

https://doi.org/10.14393/BEJOM-v6-2025-73442

ISSN: 26751313 (online edition)

Matemática Pura

A FORMA NORMAL DE HERMITE

Paola Assis Rola
Universidade Federal de Viçosa, Departamento de Matemática, Viçosa, MG, Brazil.
E-mail: paolassis123@gmail.com
https://orcid.org/0009-0006-8904-6516

Eleonesio Strey
Universidade Federal do Espírito Santo, Departamento de Matemática Pura e Aplicada, Alegre, ES, Brazil.
E-mail: eleonesio.strey@ufes.br
https://orcid.org/0000-0003-0305-9553

Mathematics Subject Classification (MSC): 15A36, 15A21, 52C07.

Resumo. A forma normal Hermite é similar à forma escalonada reduzida para matrizes com entradas inteiras. Neste artigo são apresentados alguns resultados sobre esse tema, dentre os quais destacamos o teorema da existência e unicidade, o qual afirma que toda matriz é linha equivalente sobre os inteiros a uma, e somente uma, matriz na forma normal de Hermite. Um algoritmo para calcular a forma normal Hermite de uma matriz por meio das operações elementares unimodulares também é fornecido. Por fim, são apresentados alguns conceitos e resultados preliminares de reticulados, incluindo três problemas que são respondidos utilizando a forma normal de Hermite, a saber, o problema de determinar uma base de um reticulado e os problemas da igualdade e união de reticulados.

Palavras-chave. Forma normal de Hermite, matrizes unimodulares, reticulados.

THE HERMITE NORMAL FORM

Abstract. The Hermite normal form is similar of reduced echelon form for matrices with integer entries. In this article some results on this topic are presented, among which we highlight the existence and uniqueness Theorem, which states that every matrix is row equivalent to one, and only one, matrix in the Hermite normal form. An algorithm for computing the Hermite normal form of a matrix by the elementary unimodular operations is also given. Finally, some concepts and preliminary results on lattices are presented, including three problems that are answered using the Hermite normal form, namely, the problem of finding a basis of a lattice and the problems of equality and union of lattices.

Keywords. Hermite normal form, unimodular matrices, lattices.

LA FORMA NORMAL DE HERMITE

Resumen. La forma normal de Hermite es análoga a la forma escalonada reducida para matrices con entradas enteras. En este artículo se presentan algunos resultados relacionados con este tema,

entre los cuales se destaca el teorema de existencia y unicidad, que establece que toda matriz es equivalente por filas sobre los enteros a una, y solamente una, matriz en forma normal de Hermite. Asimismo, se proporciona un algoritmo para calcular la forma normal de Hermite de una matriz mediante operaciones elementales unimodulares. Finalmente, se presentan algunos conceptos y resultados preliminares sobre reticulados, incluyendo tres problemas que se resuelven empleando la forma normal de Hermite, a saber: el problema de determinar una base de un reticulado y los problemas de igualdad y unión de reticulados.

Palabras clave. Forma normal de Hermite, matrices unimodulares, reticulados.

1 Introdução

A forma normal Hermite de uma matriz com entradas inteiras é uma matriz com caraterísticas semelhantes às matrizes na forma escalonada reduzida. Toda matriz A com entradas inteiras é linha equivalente sobre os inteiros a uma, e somente uma, matriz na forma normal de Hermite, a qual é usualmente denotada por $\mathrm{HNF}(A)$. A seguir são apresentadas uma matriz e sua forma normal de Hermite.

$$A = \begin{bmatrix} 7 & 6 & 1 & 2 \\ 3 & 1 & 2 & 4 \\ 2 & 1 & 1 & 6 \\ 5 & 4 & 1 & 6 \end{bmatrix} \qquad \mathrm{HNF}(A) = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Para determinar a forma normal de Hermite, basta aplicar convenientemente as três operações elementares unimodulares, as quais estão descritas a seguir: (i) permutação de duas linhas; (ii) substituição de uma linha pela multiplicação dela por -1; (iii) substituição de uma linha por ela mais um múltiplo inteiro de outra. A forma normal de Hermite tem sido muito útil em diversas aplicações, tais como: na abordagem de problemas básicos e não básicos da área de reticulados [1], na proposição de sistemas criptográficos baseados em reticulados [2, 3], na resolução de sistemas de equações diofantinas lineares [4], etc.

Um reticulado é qualquer subgrupo aditivo e discreto de $\mathbb{R}^n$. Equivalentemente, um reticulado também pode ser descrito como o conjunto das combinações lineares inteiras das linhas de uma matriz $m \times n$, com $m \leq n$, de posto completo. Uma matriz nas condições mencionadas é denominada uma matriz geradora e suas linhas uma base do reticulado. Para mais detalhes sobre reticulados, sugerimos as referências [5, 6].

Neste artigo é apresentado um resumo do trabalho de conclusão de curso da primeira autora, o qual foi desenvolvido sob a orientação do segundo autor. Dentre os tópicos abordados, destacamos a forma normal de Hermite, o teorema da existência e unicidade, um algoritmo para o cálculo da forma normal de Hermite e conceitos e resultados básicos da área de reticulados, incluindo três problemas que são respondidos utilizando a forma normal de Hermite (o problema

da base, o problema da igualdade e o problema da união).

2 Conceitos e resultados preliminares

Nesta seção serão apresentados os conceitos de matrizes unimodulares e matrizes linha equivalentes e, também, alguns resultados que serão necessários para desenvolvimento das seções posteriores. As principais referências utilizadas na elaboração desta seção foram [7] e [8].

Uma matriz quadrada U com entradas inteiras é dita *unimodular* se $\det(U) = \pm 1$. As matrizes listadas abaixo são unimodulares.

$$\begin{bmatrix} 1 & -1 \\ 1 & -2 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} -2 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -1 & 1 \end{bmatrix} \quad \begin{bmatrix} -2 & -1 & 2 & 2 \\ -4 & -1 & 4 & 3 \\ -1 & 0 & 1 & 1 \\ -2 & -1 & 1 & 3 \end{bmatrix}$$

Toda matriz unimodular é invertível. De fato, o determinante de uma matriz unimodular é sempre ± 1 e uma matriz é invertível se, e somente se, seu determinante é diferente de 0. A inversa de uma matriz unimodular é uma matriz unimodular. Uma demonstração deste último resultado pode ser encontrada em [9]. Se U_1 e U_2 são matrizes unimodulares de mesma ordem, então $U_1 \cdot U_2$ é uma matriz com entradas inteiras e $\det(U_1 \cdot U_2) = \det(U_1) \cdot \det(U_2) = \pm 1$. Em outras palavras, a matriz resultante do produto de duas matrizes unimodulares também é unimodular.

Definição 1. *Dada uma matriz A de ordem $m \times n$ com entradas inteiras, as seguintes operações são denominadas operações elementares unimodulares sobre as linhas:*

(i) Permutação de duas linhas da matriz;

(ii) Substituição de uma linha pela multiplicação dela por -1;

(iii) Substituição de uma linha por ela mais um múltiplo inteiro de outra.

As operações elementares unimodulares são denotadas da seguinte foma: (i) A permutação das linhas i e j é indicada por $L_i \leftrightarrow L_j$; (ii) A substituição da linha i por ela multiplicada por -1 é denotada por $L_i \to -L_i$; (iii) Por fim, se $i \neq j$ e $\alpha \in \mathbb{Z}$, a substituição da linha i por ela mais α vezes a linha j é indicada por $L_i \to L_i + \alpha L_j$.

Definição 2. *Uma matriz é chamada de matriz elementar unimodular se ela pode ser obtida da matriz identidade por meio de exatamente uma operação elementar unimodular.*

Exemplo 1. *A seguir estão três exemplos de matrizes elementares unimodulares.*

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$$

O próximo resultado mostra que as matrizes elementares unimodulares são de fato matrizes unimodulares.

Teorema 1. *Se U é uma matriz elementar unimodular, então U é unimodular.*

Demonstração. Seja U uma matriz elementar unimodular. Se U pode ser obtida a partir da identidade por meio de uma operação elementar unimodular do tipo (i), então $\det(U) = -1$. Se, porém, U pode ser obtida a partir da identidade por meio de uma operação elementar unimodular do tipo (ii), então $\det(U) = -1$. Por fim, se U pode ser obtida a partir da identidade por meio de uma operação elementar unimodular do tipo (iii), então $\det(U) = 1$. Por outro lado, U é uma matriz com entradas inteiras. Logo, a matriz U é unimodular. □

Dadas duas matrizes A e B de ordem $m \times n$ com entradas inteiras, B pode ser obtida de A por meio de um número finito de operações elementares unimodulares se, e somente se, existe uma matriz unimodular U de ordem m de modo que $B = UA$. Isto é uma consequência do fato de que cada operação elementar unimodular corresponde a uma multiplicação à esquerda por uma matriz elementar unimodular. Isto será ilustrado no próximo exemplo.

Exemplo 2. *Ao permutar a primeira e a segunda linha $(L_1 \leftrightarrow L_2)$ da matriz*

$$A = \begin{bmatrix} 0 & 1 & 4 \\ 1 & 2 & 3 \\ 1 & 3 & 7 \end{bmatrix},$$

obtemos

$$C = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 1 & 3 & 7 \end{bmatrix}.$$

A matriz C é igual ao resultado do produto U_1A, em que U_1 é a matriz elementar unimodular obtida da matriz identidade de ordem 3 permutando-se a primeira e segunda linha, isto é,

$$U_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Ao multiplicar a terceira linha da matriz C por -1 $(L_3 \to -L_3)$, obtemos

$$D = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ -1 & -3 & -7 \end{bmatrix},$$

que é igual ao produto U_2C, em que U_2 é a matriz elementar unimodular obtida da matriz identidade de ordem 3 multiplicando-se a terceira linha por -1, isto é,

$$U_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Ao somar à terceira linha da matriz D a primeira linha multiplicada por -2 ($L_3 \to L_3 - 2L_1$), obtemos

$$B = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ -3 & -7 & -13 \end{bmatrix},$$

que é igual ao produto U_3D, em que U_3 é a matriz elementar unimodular obtida da matriz identidade de ordem 3 substituindo-se a terceira linha por ela mais a primeira linha multiplicada por -2, isto é,

$$U_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}.$$

Como $C = U_1A$, $D = U_2C$ e $B = U_3D$, segue que

$$B = U_3D = U_3(U_2C) = U_3(U_2(U_1A)) = UA,$$

em que $U = U_3U_2U_1$. Por fim, observe que U é unimodular, uma vez que é um produto de matrizes unimodulares.

Definição 3. *Duas matrizes A e B são denominadas linha equivalentes sobre $\mathbb{Z}$, e escrevemos $A \sim B$, se existir uma matriz unimodular U tal que $B = UA$.*

Exemplo 3. *As matrizes A e B do Exemplo 2 são linha equivalentes sobre $\mathbb{Z}$, pois existe uma matriz unimodular U tal que $B = UA$.*

O próximo teorema mostra que a relação definida acima é reflexiva, simétrica e transitiva, ou seja, é uma relação de equivalência.

Teorema 2. *Sejam A, B e C matrizes de ordem $m \times n$ com entradas inteiras. Então,*

(i) (Reflexiva) $A \sim A$;

(ii) (Simétrica) Se $A \sim B$, então $B \sim A$;

(iii) (Transitiva) Se $A \sim B$ e $B \sim C$, então $A \sim C$.

Demonstração. Sejam A, B e C matrizes de ordem $m \times n$ com entradas inteiras. (i) Como a matriz identidade I_m é unimodular e $A = I_mA$, segue que $A \sim A$. (ii) Suponha que $A \sim B$. Assim, existe uma matriz unimodular U de ordem m tal que $B = UA$. Multiplicando à esquerda

ambos os lados desta última igualdade por U^{-1}, obtemos $U^{-1}B = A$. Como a inversa de uma matriz unimodular é uma matriz unimodular, segue que $B \sim A$. (iii) Suponha que $A \sim B$ e $B \sim C$. Assim, existem matrizes unimodulares U_1 e U_2 de ordem m tais que $B = U_1A$ e $C = U_2B$. Logo, $C = U_2B = U_2(U_1A) = (U_2U_1)A = U_3A$, em que $U_3 = U_2U_1$. Portanto, $A \sim C$, uma vez que o produto de duas matrizes unimodulares é uma matriz unimodular. □

Teorema 3. *Se $A \sim B$, então qualquer linha de A pode ser escrita como uma combinação linear inteira das linhas de B.*

Demonstração. Sejam A e B matrizes de ordem $m \times n$, com entradas inteiras, tais que $A \sim B$. Pelo item (ii) do Teorema 2, temos que $B \sim A$, isto é, existe uma matriz unimodular U tal que $A = UB$. Sejam $i \in \{1, \ldots, m\}$ e e_i a matriz de ordem $1 \times m$, cuja i-ésima entrada é igual a 1 e as demais entradas são iguais a 0. Como

$$e_iA = e_i(UB) = (e_iU)B$$

e e_iU é uma matriz linha com entradas inteiras, segue que a i-ésima linha de A pode ser escrita como uma combinação linear inteira das linhas de B. □

O Teorema 3 garante que se duas matrizes são linha equivalentes sobre $\mathbb{Z}$, então cada linha de uma delas pode ser escrita como uma combinação linear inteira das linhas da outra. A demonstração do mesmo fornece implicitamente um método de como obter essa combinação linear, o qual será ilustrado no Exemplo 4.

Exemplo 4. *Considere novamente as matrizes A, B e U do Exemplo 2. A relação entre elas é $B = UA$. Para expressar, por exemplo, a terceira linha de B como uma combinação linear inteira das linhas de A, basta efetuar os seguintes cálculos:*

$$\begin{bmatrix} -3 & -7 & -13 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ -3 & -7 & -13 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \cdot \left(\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 4 \\ 1 & 2 & 3 \\ 1 & 3 & 7 \end{bmatrix} \right) =$$

$$= \left(\begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2 & -1 \end{bmatrix} \right) \cdot \begin{bmatrix} 0 & 1 & 4 \\ 1 & 2 & 3 \\ 1 & 3 & 7 \end{bmatrix} = \begin{bmatrix} 0 & -2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 4 \\ 1 & 2 & 3 \\ 1 & 3 & 7 \end{bmatrix}$$

Isto mostra que $(-3, -7, -13) = 0 \cdot (0, 1, 4) - 2 \cdot (1, 2, 3) - 1 \cdot (1, 3, 7)$.

3 A Forma Normal de Hermite

Uma matriz na Forma Normal de Hermite é uma matriz num formato similar à Forma Escalonada Reduzida (Definição 4). Um dos destaques desta seção é o resultado que garante que qualquer matriz com entradas inteiras é linha equivalente a uma, e somente uma, matriz na Forma Normal de Hermite (Teorema 4). Este resultado nos permite definir o que chamaremos de Forma Normal de Hermite de uma matriz (Definição 5). As principais referências utilizadas na elaboração desta seção foram [8], [10] e [11].

Definição 4. *Seja $H = [h_{ij}]$ uma matriz de ordem $m \times n$ com entradas inteiras. Dizemos que H está na Forma Normal de Hermite se existir um inteiro r, $0 \leq r \leq m$, tal que:*

(i) As últimas $m - r$ linhas de H são nulas;

(ii) Existem índices $j_1, j_2, \ldots, j_r$, com $1 \leq j_1 < j_2 < \cdots < j_r \leq n$, de modo que as entradas à esquerda de h_{ij_i} são iguais a zero e $h_{ij_i} \geq 1$;

(iii) Todas as entradas acima de h_{ij_i} são não negativas e menores do que h_{ij_i}.

Exemplo 5. *As seguintes matrizes estão na Forma Normal de Hermite.*

$$\begin{bmatrix} 5 & 2 & 1 & 8 \\ 0 & 3 & 0 & 5 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 & 2 & 7 \\ 0 & 0 & 6 & 1 \\ 0 & 0 & 0 & 10 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 2 & 3 & 0 & 11 & -2 \\ 0 & 0 & 0 & 5 & 0 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 15 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Um subconjunto não vazio de $\mathbb{R}^n$ é linearmente independente se, e somente se, nenhum de seus elementos pode ser escrito como uma combinação linear, com coeficientes reais, dos demais elementos. Para mais detalhes sobre conceitos e resultados de Álgebra Linear, sugerimos a referência [7]. As linhas não nulas de uma matriz na forma normal de Hermite são linearmente independentes. Se H é uma matriz que satisfaz as condições da Definição 4, então $\text{posto}(H) = r$. Por exemplo, as matrizes listadas no Exemplo 5 têm posto igual a $4, 3, 3$ e 0, respectivamente.

Os dois lemas a seguir estabelecem relações entre matrizes que são linha equivalentes e estão na Forma Normal de Hermite. O objetivo destes resultados é simplificar a demonstração do Teorema 4.

Lema 1. *Sejam $H = [h_{ij}]$ e $H' = [h'_{ij}]$ matrizes na Forma Normal de Hermite tais que $H \sim H'$. Temos que h_{ij_i} é a primeira entrada não nula da i-ésima linha de H se, e somente se, h'_{ij_i} é a primeira entrada não nula da i-ésima linha de H'.*

Demonstração. Denote as linhas de H por $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_m$ e as de H' por $\boldsymbol{h}'_1, \boldsymbol{h}'_2, \ldots, \boldsymbol{h}'_m$. Para cada i, a linha $\boldsymbol{h}_i$ é não nula se, e somente se, a linha $\boldsymbol{h}'_i$ é não nula, uma vez que H e H'

estão na forma normal de Hermite e $\text{posto}(H) = \text{posto}(H')$. A última igualdade é garantida pelo Teorema 3, pois $H \sim H'$. Seja k o número de linhas não nulas de cada uma das matrizes. Para cada $i \in \{1, \ldots, k\}$, sejam h_{ij_i} e $h'_{i\ell_i}$ as primeiras entradas não nulas de $\boldsymbol{h}_i$ e $\boldsymbol{h}'_i$, respectivamente. O objetivo é mostrar que $j_i = l_i, \forall i \in \{1, \ldots, k\}$. Pelo Teorema 3, a linha $\boldsymbol{h}_1$ pode ser escrita como uma combinação linear inteira das linhas de H', uma vez que $H \sim H'$. Como H e H' estão na forma normal de Hermite, segue que $j_1 \geq \ell_1$. De forma análoga, observando que a linha $\boldsymbol{h}'_1$ pode ser escrita como uma combinação linear inteira das linhas de H, obtemos $j_1 \leq \ell_1$. Logo, $j_1 = \ell_1$. Agora, seja $1 < i < k$ e assuma que $j_1 = \ell_1, j_2 = \ell_2, \ldots, j_{i-1} = \ell_{i-1}$. Suponha, por absurdo, que $j_i \neq \ell_i$. Sem perda de generalidade, podemos assumir que $j_i < \ell_i$. Escreva

$$H' = \begin{bmatrix} A_{(i-1)\times\ell_{i-1}} & B_{(i-1)\times(n-\ell_{i-1})} \\ 0_{(m-i+1)\times\ell_{i-1}} & C_{(m-i+1)\times(n-\ell_{i-1})} \end{bmatrix},$$

onde $0_{(m-i+1)\times j_i}$ é a matriz nula. Por construção, as linhas de A são linearmente independentes. Como $j_i - 1 \geq \ell_{i-1}$, pois $j_i > j_{i-1} = \ell_{i-1}$, e as primeiras $j_i - 1$ entradas da matriz $\boldsymbol{h}_i$ são iguais a zero, o Teorema 3 fornece que a linha $\boldsymbol{h}_i$ pode ser escrita como uma combinação linear inteira das linhas da matriz

$$\hat{C} = \begin{bmatrix} 0_{(m-i+1)\times\ell_{i-1}} & C_{(m-i+1)\times(n-\ell_{i-1})} \end{bmatrix}.$$

Por outro lado, a matriz $\hat{C}$ está forma normal de Hermite e a primeira entrada não nula de sua primeira linha é $\hat{c}_{1\ell_i}$, uma vez que suas linhas são $\boldsymbol{h}'_i, \ldots, \boldsymbol{h}'_m$. Logo, $\hat{C}$ pode ser particionada como

$$\hat{C} = \begin{bmatrix} 0_{(m-i+1)\times(\ell_i-1)} & D_{(m-i+1)\times(n-\ell_i+1)} \end{bmatrix}$$

e, portanto, as primeiras j_i entradas de $\boldsymbol{h}_i$ são nulas, uma vez que $j_i < \ell_i$. Isto contradiz a hipótese $h_{ij_i} \neq 0$. □

Lema 2. *Sejam H e H' matrizes na Forma Normal de Hermite. Se $H \sim H'$, então $H = H'$.*

Demonstração. Sejam $H = [h_{ij}]$ e $H' = [h'_{ij}]$ matrizes de ordem $m \times n$, ambas na Forma Normal de Hermite, tais que $H \sim H'$. Suponha, por absurdo, que $H \neq H'$. Escolha $h_{i_0j_0} \neq h'_{i_0j_0}$ de modo que j_0 seja o menor possível. Podemos assumir sem perda de generalidade que $h_{i_0j_0} > h'_{i_0j_0}$. Denote as linhas de H por $\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_m$ e as de H' por $\boldsymbol{h}'_1, \boldsymbol{h}'_2, \ldots, \boldsymbol{h}'_m$. As primeiras $j_0 - 1$ entradas da matriz linha $\boldsymbol{h}_{i_0} - \boldsymbol{h}'_{i_0}$ são iguais a zero enquanto que a j_0-ésima entrada (isto é, $h_{i_0j_0} - h'_{i_0j_0}$) é diferente de zero. Como $H \sim H'$, o Teorema 3 garante que $\boldsymbol{h}'_{i_0}$ pode ser escrito como uma combinação linear inteira das linhas de H. Consequentemente, $\boldsymbol{h}_{i_0} - \boldsymbol{h}'_{i_0}$ também pode ser escrito como uma combinação linear inteira das linhas de H, uma vez que $\boldsymbol{h}_{i_0}$ é uma dessas linhas. Como H está na Forma Normal de Hermite, existe um inteiro k ($1 \leq k \leq j_0$) tal que $\boldsymbol{h}_{i_0} - \boldsymbol{h}'_{i_0}$ pode ser escrito como uma combinação linear inteira das linhas $\boldsymbol{h}_k, \boldsymbol{h}_{k+1}, \ldots, \boldsymbol{h}_m$ (essas são exatamente as linhas que possuem as primeiras $j_0 - 1$ entradas iguais a zero). A j_0-ésima entrada de cada uma das linhas $\boldsymbol{h}_{k+1}, \ldots, \boldsymbol{h}_m$ também é igual a

zero. Assim, $h_{i_0j_0} - h'_{i_0j_0} = \alpha h_{kj_0}$ para algum inteiro α. Como $h_{i_0j_0} \neq h'_{i_0j_0}$, segue que $h_{kj_0} \neq 0$. Logo, h_{kj_0} é a primeira entrada não nula de $\boldsymbol{h}_k$, o que implica que $h_{kj_0} > 0$, as demais entradas da j_0-ésima coluna de H são não negativas e $h_{kj_0} > h_{ij_0}$ se $i \neq k$, uma vez que H está na Forma Normal de Hermite. Dessa forma, tem-se $\alpha \geq 1$, uma vez que $h_{kj_0} > 0$, $0 < h_{i_0j_0} - h'_{i_0j_0} = \alpha h_{kj_0}$ e $\alpha \in \mathbb{Z}$. Consequentemente,

$$h_{i_0j_0} - h'_{i_0j_0} = \alpha h_{kj_0} \geq h_{kj_0} \geq h_{i_0j_0}. \tag{1}$$

Isto mostra que $h'_{i_0j_0} \leq 0$. Pelo Lema 1, h'_{kj_0} é a primeira entrada não nula da linha h'_k, portanto $h'_{ij_0} \geq 0$ para todo i pela forma normal de Hermite de H'. Assim $h'_{i_0j_0} \geq 0$ e consequentemente $h'_{i_0j_0} = 0$. Pela desigualdade (1) temos que $h_{i_0j_0} = h_{kj_0}$, ou seja, $i_0 = k$. Pelo Lema 1, $h'_{i_0j_0} \neq 0$. Absurdo. □

O próximo resultado será de suma importância na abordagem das aplicações que serão apresentadas neste artigo, uma vez que está diretamente relacionado ao resultado que faz a conexão entre matrizes na forma normal de Hermite e reticulados (Teorema 6).

Teorema 4. *Se A é uma matriz de ordem $m \times n$ com entradas inteiras, então existe uma única matriz H na Forma Normal de Hermite que é linha equivalente a A.*

Demonstração. (Existência) Seja $A = [a_{ij}]$ uma matriz com entradas inteiras. A demonstração da existência da matriz H será feita por indução sobre o número de colunas de A. Se A é a matriz nula de ordem $m \times 1$ não há o que demonstrar. Suponha, então, que A é uma matriz $m \times 1$ não nula, com exatamente k entradas diferentes de zero. Sem perda de generalidade, pelas operações (i) e (ii), podemos assumir que $0 < a_{11} \leq a_{21} \leq \cdots \leq a_{k1}$ e $a_{i1} = 0$, para $i \in \{k+1, \ldots, m\}$. Substituindo cada linha L_i por $L_i - q_{i1}L_1$ (sendo q_{i1} o quociente da divisão de a_{i1} por a_{11}), com exceção da primeira e das últimas $m - k$ linhas, obtemos a matriz coluna A_1 cujas primeiras entradas são $a_{11}, r_{21}, \ldots, r_{k1}$, onde r_{i1} é o resto da divisão de a_{i1} por a_{11}, e as demais são iguais a zero. Se $r_{i1} = 0$, para todo $i \in \{2, \ldots, k\}$, temos o resultado desejado. Caso contrário, aplicamos o processo descrito acima à matriz A_1, e repetimos se necessário, até obter o resultado desejado. Este processo finaliza após um número finito de etapas, pois as matrizes obtidas no decorrer do processo possuem entradas inteiras positivas, a primeira entrada é sempre maior do que as demais e menor do que a primeira entrada da matriz da etapa anterior. Agora, suponha que A é uma matriz de ordem $m \times n$, com $n \geq 2$, e que o resultado é válido para toda matriz cujo número de colunas é menor do que n. Aplicando convenientemente as operações elementares, de forma análoga ao caso $n = 1$, obtemos uma matriz da forma

$$\left[\begin{array}{c|ccc} \hat{a}_{11} & \hat{a}_{12} & \cdots & \hat{a}_{1n} \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right],$$

na qual B é uma matriz com entradas inteiras de ordem $(m-1)\times(n-1)$. Assim, a hipótese de indução garante que existe uma matriz $\hat{H}$ na Forma Normal de Hermite tal que B e $\hat{H}$ são linha equivalentes sobre $\mathbb{Z}$. Logo, a matriz A é linha equivalente sobre $\mathbb{Z}$ à matriz

$$\left[\begin{array}{c|ccc} \hat{a}_{11} & \hat{a}_{12} & \cdots & \hat{a}_{1n} \\ \hline 0 & & & \\ \vdots & & \hat{H} & \\ 0 & & & \end{array}\right].$$

Para obter a condição (iii) da Definição 4, aplicamos no máximo $n-1$ operações elementares unimodulares do tipo (iii) à primeira linha, de modo a obter H, que está na Forma Normal de Hermite.

(Unicidade) Agora, suponha que existem matrizes H e H' de ordem $m\times n$, ambas na Forma Normal de Hermite e linha equivalentes a A. Como $H\sim A$ e $H'\sim A$, o Teorema 2 garante que $H\sim H'$. Pelo Lema 2, temos que $H=H'$, uma vez que ambas estão na Forma Normal de Hermite. Portanto, existe uma única matriz H na Forma Normal de Hermite que é linha equivalente a A. □

Definição 5. *A matriz H do Teorema 4 é chamada de Forma Normal de Hermite de A e é denotada por* $\mathrm{HNF}(A)$.

No restante desta seção é apresentado um algoritmo para o cálculo da forma normal de Hermite de uma matriz. Seja A uma matriz de ordem $m\times n$ com entradas inteiras. Se A é a matriz nula, então $\mathrm{HNF}(A)=A$, ou seja, não há o que calcular. Suponha que A é não nula e sua j_1-ésima coluna seja a primeira não nula. Para obter a forma normal de Hermite, iniciamos aplicando o algoritmo descrito a seguir e o repetimos até obtermos uma matriz cuja j_1-ésima coluna tenha exatamente uma entrada não nula.

1. Escolher uma entrada da j_1-ésima coluna que tenha o menor valor absoluto diferente de zero. Digamos que a entrada escolhida seja $a_{i_1j_1}$.

2. Para cada i, $1\leq i\leq m$ e $i\neq i_1$, determinar os inteiros q_i e r_i tais que $a_{ij_1}=q_ia_{i_1j_1}+r_i$ e $0\leq r_i<|a_{i_1j_1}|$. A existência e unicidade de tais inteiros é garantida pelo Teorema da Divisão [12].

3. Substituir cada linha L_i, com $1\leq i\leq m$ e $i\neq i_1$, por $L_i-q_iL_{i_1}$.

Em seguida, se necessário, aplicar as operações elementares (i) e (ii) para que a primeira entrada da j_1-ésima coluna da matriz obtida seja positiva.

Exemplo 6. *Seja*

$$A = \begin{bmatrix} 7 & 6 & 1 & 2 \\ 3 & 1 & 2 & 4 \\ 2 & 1 & 1 & 6 \\ 5 & 4 & 1 & 6 \end{bmatrix}.$$

A primeira coluna de A é não nula e a entrada a_{31} é a que possui o menor valor absoluto diferente de zero. Substituindo as linhas L_1, L_2 e L_4, respectivamente, por $L_1 - 3L_3$, $L_2 - L_3$ e $L_4 - 2L_3$ (pois $7 = 3 \cdot 2 + 1$, $3 = 1 \cdot 2 + 1$ e $5 = 2 \cdot 2 + 1$), obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 1 & 0 & 1 & -2 \\ 2 & 1 & 1 & 6 \\ 1 & 2 & -1 & -6 \end{bmatrix}.$$

As entradas da primeira coluna da matriz obtida no passo anterior que possuem o menor valor absoluto diferente de zero são a_{11}, a_{21} e a_{41}. Para dar seguimento ao algoritmo, escolhemos a_{11} e, consequentemente, substituímos as linhas L_2, L_3 e L_4 por $L_2 - L_1$, $L_3 - 2L_1$ e $L_4 - L_1$, respectivamente (pois $1 = 1 \cdot 1 + 0$, $2 = 2 \cdot 1 + 0$ e $1 = 1 \cdot 1 + 0$). Dessa forma, obtemos a matriz

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & -3 & 3 & 14 \\ 0 & -5 & 5 & 38 \\ 0 & -1 & 1 & 10 \end{bmatrix}.$$

Com isso, a primeira etapa é finalizada, pois há apenas uma entrada diferente de zero na primeira coluna e essa encontra-se na primeira linha.

Finalizada a primeira etapa, passamos para a segunda etapa. Suponha que a j_2-ésima coluna da matriz obtida na primeira etapa seja a primeira coluna cujas entradas, a partir da segunda, sejam não todas nulas. A segunda etapa consiste em repetir o algoritmo descrito abaixo até obtermos uma matriz cuja j_2-ésima coluna tenha exatamente uma entrada não nula a partir da segunda.

1. Escolher uma entrada da j_2-ésima coluna, a partir da segunda, que tenha o menor valor absoluto diferente de zero. Digamos que a entrada escolhida seja $a_{i_2 j_2}$.

2. Para cada i, $2 \leq i \leq m$ e $i \neq i_2$, determinar os inteiros q_i e r_i de modo que $a_{ij_2} = q_i a_{i_2 j_2} + r_i$ e $0 \leq r_i < |a_{i_2 j_2}|$. A existência e unicidade de tais inteiros é garantida pelo Teorema da Divisão [12].

3. Substituir cada linha L_i, com $2 \leq i \leq m$ e $i \neq i_2$, por $L_i - q_i L_{i_2}$.

Em seguida, se necessário, aplicar as operações elementares (i) e (ii) para que a segunda entrada da j_2-ésima coluna da matriz obtida seja positiva.

Exemplo 7. *Considere a matriz obtida no Exemplo 6, isto é,*

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & -3 & 3 & 14 \\ 0 & -5 & 5 & 38 \\ 0 & -1 & 1 & 10 \end{bmatrix}.$$

A segunda coluna dessa matriz é a primeira cujas entradas, a partir da segunda, não são todas nulas e a entrada a_{42} é a que possui o menor valor absoluto diferente de zero. Substituindo as linhas L_2 e L_3 por $L_2 - 3L_4$ e $L_3 - 5L_4$, respectivamente (pois $-3 = 3 \cdot (-1) + 0$ e $-5 = 5 \cdot (-1) + 0$), obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 0 & 0 & -16 \\ 0 & 0 & 0 & -12 \\ 0 & -1 & 1 & 10 \end{bmatrix}.$$

Aplicando a operação elementar $L_2 \leftrightarrow L_4$ e, em seguida, $L_2 \to -L_2$, obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & 0 & -16 \end{bmatrix}.$$

Isto conclui a segunda etapa.

Finalizada a segunda etapa, passamos para a terceira etapa. Suponha que a j_3-ésima coluna da matriz obtida na segunda etapa seja a primeira coluna cujas entradas, a partir da terceira, sejam não todas nulas. A terceira etapa consiste em repetir o algoritmo descrito abaixo até obtermos uma matriz cuja j_3-ésima coluna tenha exatamente uma entrada não nula a partir da terceira.

1. Escolher uma entrada da j_3-ésima coluna, a partir da terceira, que tenha o menor valor absoluto diferente de zero. Digamos que a entrada escolhida seja a_{i3j3}.

2. Para cada i, $3 \leq i \leq m$ e $i \neq i_3$, determinar os inteiros q_i e r_i de modo que $a_{ij_3} = q_i a_{i_3 j_3} + r_i$ e $0 \leq r_i < |a_{i_3 j_3}|$. A existência e unicidade de tais inteiros é garantida pelo Teorema da Divisão [12].

3. Substituir cada linha L_i, com $3 \leq i \leq m$ e $i \neq i_3$, por $L_i - q_i L_{i_3}$.

Em seguida, se necessário, aplicar as operações elementares (i) e (ii) para que a terceira entrada da j_3-ésima coluna da matriz obtida seja positiva.

Exemplo 8. *Considere a matriz obtida no Exemplo 7, isto é,*

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & 0 & -16 \end{bmatrix}.$$

A quarta coluna dessa matriz é a primeira cujas entradas, a partir da terceira, não são todas nulas e a entrada a_{34} é a que possui o menor valor absoluto diferente de zero. Substituindo a linha L_4 por $L_4 - 2L_3$ (pois $-16 = 2 \cdot (-12) + 8$), obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & 0 & 8 \end{bmatrix}.$$

A entrada da quarta coluna da matriz obtida no passo anterior, a partir da terceira, que possui o menor valor absoluto diferente de zero é a_{44}. Substituindo a linha L_3 por $L_3 + 2L_4$ (pois $-12 = (-2) \cdot 8 + 4$), obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 8 \end{bmatrix}.$$

A entrada da quarta coluna da matriz obtida no passo anterior, a partir da terceira, que possui o menor valor absoluto diferente de zero é a_{34}. Substituindo a linha L_4 por $L_4 - 2L_3$ (pois $8 = 2 \cdot 4 + 0$), obtemos

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Isto conclui a terceira etapa.

Continuando este processo, após no máximo m etapas, obtemos um inteiro r, $1 \leq r \leq m$, e uma matriz cujas últimas $m - r$ linhas são nulas, as entradas à esquerda de a_{ij_i} são iguais a zero e $a_{ij_i} \geq 1$ para todo $i \in \{1, 2, \ldots, r\}$, ou seja, uma matriz que satisfaz as condições (i) e (ii) da Definição 4.

Para obter a forma normal de Hermite de A, a partir da matriz obtida no processo descrito acima, basta aplicar o seguinte algoritmo (iniciar com $k = 2$): Para cada $i < k$, se $a_{ij_k} \geq a_{kj_k}$

ou $a_{ij_k} < 0$, substituir a linha L_i por $L_i \to L_i - q_i L_k$, em que q_i é o quociente da divisão de a_{ij_k} por a_{kj_k}. Em seguida, substituir k por $k+1$. Retornar ao início se $k+1 \leq r$ e finalizar caso contrário. Este processo será ilustrado no próximo exemplo.

Exemplo 9. *Considere a matriz obtida no Exemplo 8, isto é,*

$$\begin{bmatrix} 1 & 3 & -2 & -16 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Como a_{12} é maior do que a_{22} e esta última é a entrada $a_{i_2j_2}$, substituímos a linha L_1 por $L_1 - 3L_2$, pois $3 = 3 \cdot 1 + 0$. Dessa forma, obtemos

$$\begin{bmatrix} 1 & 0 & 1 & 14 \\ 0 & 1 & -1 & -10 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Como as novas entradas a_{14} e a_{24} possuem valor absoluto maior que a_{34} e esta última é a entrada $a_{i_3j_3}$, substituímos as linhas L_1 e L_2 por $L_1 - 3L_3$ e $L_2 + 3L_3$, respectivamente (pois $14 = 3 \cdot 4 + 2$ e $-10 = (-3) \cdot 4 + 2$). Após efetuar as substituições indicadas, obtemos a forma normal de Hermite da matriz A definida no Exemplo 6, a saber,

$$\mathrm{HNF}(A) = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

4 Aplicações

Nesta seção, a forma normal de Hermite será utilizada na abordagem de três problemas básicos do contexto de reticulados, são eles: o problema de determinar uma base de um reticulado e os problemas da igualdade e união de reticulados. As principais referências desta seção são [5] e [1].

Um *reticulado* é qualquer subgrupo aditivo e discreto de $\mathbb{R}^n$. Equivalentemente, um subconjunto Λ de $\mathbb{R}^n$, $\Lambda \neq \{\mathbf{0}\}$, é um reticulado se, e somente se, existem vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{R}^n$ linearmente independentes de modo que

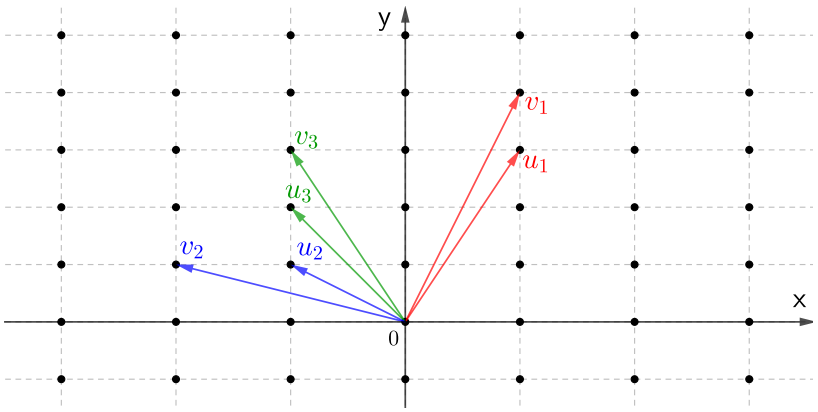
$$\Lambda = \{\alpha_1 \boldsymbol{b}_1 + \cdots + \alpha_m \boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}.$$

Na descrição acima, o conjunto $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ é denominado uma *base* de Λ. No exemplo a

seguir é apresentado um reticulado e algumas bases do mesmo.

Exemplo 10. *Seja $\Lambda \subset \mathbb{R}^2$ o reticulado gerado pela base $\{\boldsymbol{u}_1, \boldsymbol{v}_1\}$, em que $\boldsymbol{u}_1 = (2,3)$ e $\boldsymbol{v}_1 = (2,4)$. Esse reticulado tem infinitas bases. Na Figura 1 estão ilustradas três bases de Λ, a saber, $\{\boldsymbol{u}_1, \boldsymbol{v}_1\}$, $\{\boldsymbol{u}_2, \boldsymbol{v}_2\}$ e $\{\boldsymbol{u}_3, \boldsymbol{v}_3\}$, em que $\boldsymbol{u}_2 = (-2,1)$, $\boldsymbol{v}_2 = (-4,1)$, $\boldsymbol{u}_3 = (-2,2)$ e $\boldsymbol{v}_3 = (-2,3)$. Para verificar que essas são de fato bases de Λ, basta aplicar o Teorema 7 que veremos mais adiante.*

Figura 1: Bases do reticulado Λ.



Fonte: Os autores.

É importante ressaltar que nem todo conjunto constituído por dois vetores do reticulado Λ, linearmente independentes, formam uma base do mesmo. Por exemplo, os vetores $\boldsymbol{u}_2 = (-2,1)$ e $\boldsymbol{v}_3 = (-2,3)$ são linearmente independentes e pertencem a Λ, mas não formam uma base de Λ. De fato, o vetor $\boldsymbol{u}_3 = (-2,2)$ pertence a Λ e não pode ser escrito como uma combinação linear inteira deles, uma vez que $\boldsymbol{u}_3 = \frac{1}{2}\boldsymbol{u}_2 + \frac{1}{2}\boldsymbol{v}_3$.

A quantidade de elementos de uma base de um reticulado é invariante, isto é, duas bases de um mesmo reticulado possuem o mesmo número de elementos. Isso nos permite definir o *posto* de um reticulado como o número de vetores de uma base qualquer do mesmo. Dizemos que um reticulado $\Lambda \subset \mathbb{R}^n$ tem *posto completo* se possui posto igual a n. O reticulado apresentado no Exemplo 10 tem posto completo.

Dados um reticulado $\Lambda \subset \mathbb{R}^n$ e uma base $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m\}$ de Λ tal que $\boldsymbol{b}_i = (b_{i1}, \ldots, b_{in})$, para $i \in \{1, \ldots, m\}$, a matriz

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

é denominada uma *matriz geradora* de Λ. Neste caso, escrevemos $\Lambda = \Lambda(B)$. Este reticulado pode ser representado matricialmente por

$$\Lambda(B) = \{\mathbf{u}B;\ \mathbf{u} \in M_{1\times m}(\mathbb{Z})\}.$$

Em outras palavras, um elemento $\boldsymbol{b}$ pertence ao reticulado $\Lambda(B)$ se, e somente se, $\boldsymbol{b}$ pode ser escrito como uma combinação linear inteira das linhas da matriz B. Na descrição acima, o símbolo $M_{1\times m}(\mathbb{Z})$ denota o conjunto das matrizes com entradas inteiras de ordem $1\times m$. Temos que B_1 e B_2 são matrizes geradoras de Λ se, e somente se, existe uma matriz unimodular U tal que $B_2 = UB_1$ [5, 9].

Teorema 5. *Sejam B_1 e B_2 matrizes de ordem $m \times n$ ($m \leq n$) com entradas inteiras e posto completo. Temos que*

$$\Lambda(B_1) = \Lambda(B_2) \Longleftrightarrow B_1 \sim B_2.$$

Demonstração. ($\Rightarrow$) Sejam B_1 e B_2 matrizes de ordem $m \times n$, $m \leq n$, com entradas inteiras e posto completo. Suponha que $\Lambda(B_1) = \Lambda(B_2)$. Assim, existe uma matriz unimodular U tal que $B_2 = UB_1$ e, logo, $B_1 \sim B_2$. ($\Leftarrow$) Sejam B_1 e B_2 matrizes com entradas inteiras tais que $B_1 \sim B_2$. Assim, existe uma matriz unimodular U tal que $B_2 = UB_1$. Isto implica que B_1 e B_2 geram o mesmo reticulado, isto é, $\Lambda(B_1) = \Lambda(B_2)$. □

O próximo resultado estabelece uma conexão entre a forma normal de Hermite e reticulados. Este será de grande importância na abordagem das aplicações que serão apresentadas neste artigo.

Teorema 6. *Todo reticulado contido em $\mathbb{Z}^n$ possui uma, e somente uma, matriz geradora na forma normal de Hermite.*

Demonstração. Sejam Λ um reticulado e B uma matriz geradora de Λ. O Teorema 4 garante que existe uma matriz H na forma normal de Hermite tal que $H \sim B$, o que implica que H é uma matriz geradora de Λ. Logo, todo reticulado possui uma matriz geradora na Forma Normal de Hermite. A unicidade é garantida pelo Lema 2. □

No que segue serão abordados três problemas básicos do contexto de reticulados utilizando a forma normal de Hermite. Inicialmente será apresentado o *problema da base*, que consiste em determinar uma base de um reticulado a partir de um conjunto de geradores. Com efeito, dados vetores $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m \in \mathbb{Z}^n$, não necessariamente linearmente independentes, considere $\Lambda = \{\alpha_1\boldsymbol{b}_1 + \cdots + \alpha_m\boldsymbol{b}_m;\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}\}$. Pode-se verificar facilmente que Λ é um reticulado. Para determinar uma base de Λ, basta calcular $\mathrm{HNF}(A)$, em que A é a matriz de ordem $m \times n$ cujas linhas são $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$. Como $\mathrm{HNF}(A) \sim A$, cada um dos elementos de Λ pode ser escrito como uma combinação linear inteira das linhas de $\mathrm{HNF}(A)$. Portanto, as linhas não nulas de $\mathrm{HNF}(A)$ formam uma base de Λ.

Exemplo 11. *Sejam $\boldsymbol{b}_1 = (7, 6, 1, 2)$, $\boldsymbol{b}_2 = (3, 1, 2, 4)$, $\boldsymbol{b}_3 = (2, 1, 1, 6)$, $\boldsymbol{b}_4 = (5, 4, 1, 6)$ e $\Lambda = \{\alpha_1\boldsymbol{b}_1 + \alpha_2\boldsymbol{b}_2 + \alpha_3\boldsymbol{b}_3 + \alpha_4\boldsymbol{b}_4;\ \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Z}\}$. Considere a matriz A cujas linhas são*

$\boldsymbol{b}_1$, $\boldsymbol{b}_2$, $\boldsymbol{b}_3$ e $\boldsymbol{b}_4$, respectivamente. Pelo Exemplo 9, temos que

$$\mathrm{HNF}(A) = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Logo, $\{(1,0,1,2),(0,1,-1,2),(0,0,0,4)\}$ é uma base de Λ.

Agora, será abordado o *problema da igualdade*, que consiste em determinar se duas matrizes com entradas inteiras são matrizes geradoras do mesmo reticulado. O próximo resultado soluciona este problema, uma vez que ele garante que duas matrizes com entradas inteiras são matrizes geradoras de um mesmo reticulado se, e somente se, elas possuem a mesma forma normal de Hermite.

Teorema 7. *Sejam B_1 e B_2 matrizes de ordem $m \times n$, $m \leq n$, com entradas inteiras e posto completo. Temos que*

$$\Lambda(B_1) = \Lambda(B_2) \iff \mathrm{HNF}(B_1) = \mathrm{HNF}(B_2).$$

Demonstração. ($\Rightarrow$) Como $\Lambda(B_1) = \Lambda(B_2)$, o Teorema 5 garante que $B_1 \sim B_2$. Por outro lado, o Teorema 4 garante que $B_1 \sim \mathrm{HNF}(B_1)$ e $B_2 \sim \mathrm{HNF}(B_2)$. Logo, pelo Teorema 2, $\mathrm{HNF}(B_1) \sim \mathrm{HNF}(B_2)$. Aplicando o Lema 2, obtemos $\mathrm{HNF}(B_1) = \mathrm{HNF}(B_2)$. ($\Leftarrow$) Suponha que $\mathrm{HNF}(B_1) = \mathrm{HNF}(B_2)$. Logo, $\Lambda(\mathrm{HNF}(B_1)) = \Lambda(\mathrm{HNF}(B_2))$. Como $B_1 \sim \mathrm{HNF}(B_1)$ e $B_2 \sim \mathrm{HNF}(B_2)$, segue que $\Lambda(B_1) = \Lambda(\mathrm{HNF}(B_1))$ e $\Lambda(B_2) = \Lambda(\mathrm{HNF}(B_2))$, respectivamente. Portanto, $\Lambda(B_1) = \Lambda(B_2)$. □

Exemplo 12. *Sejam*

$$B_1 = \begin{bmatrix} 2 & 1 & 1 \\ 4 & 0 & 2 \end{bmatrix},\ B_2 = \begin{bmatrix} 8 & 2 & 4 \\ -6 & -1 & -3 \end{bmatrix},\ B_3 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\ \textit{e}\ B_4 = \begin{bmatrix} 1 & 1 \\ -1 & 2 \end{bmatrix}.$$

O Teorema 7 garante que $\Lambda(B_1) = \Lambda(B_2)$ e $\Lambda(B_3) \neq \Lambda(B_4)$, uma vez que

$$\mathrm{HNF}(B_1) = \mathrm{HNF}(B_2) = \begin{bmatrix} 2 & 1 & 1 \\ 0 & 2 & 0 \end{bmatrix}$$

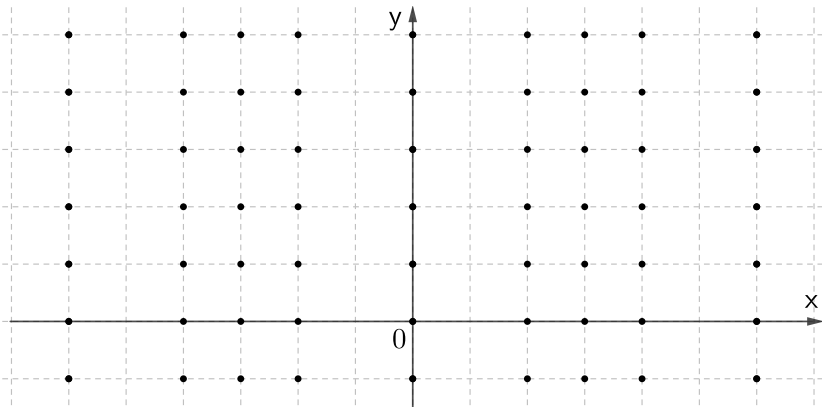
e

$$\mathrm{HNF}(B_3) = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 3 \end{bmatrix} = \mathrm{HNF}(B_4).$$

A união de dois reticulados nem sempre é um reticulado. De fato, basta observar que $\Lambda_1 = \{(2k, s);\ k, s \in \mathbb{Z}\}$ e $\Lambda_2 = \{(3k, s);\ k, s \in \mathbb{Z}\}$ são reticulados em $\mathbb{R}^2$, mas $\Lambda_1 \cup \Lambda_2$ não é

um reticulado (Figura 2). É um conjunto discreto, mas não é um subgrupo aditivo de $\mathbb{R}^2$, pois $(2,0),(3,0) \in \Lambda_1 \cup \Lambda_2$ e $(1,0) = (3,0) - (2,0) \notin \Lambda_1 \cup \Lambda_2$. Dados dois reticulados, ambos contidos em $\mathbb{Z}^n$, o *problema da união* consiste em determinar uma base para o menor reticulado que os contém. O próximo resultado juntamente com a solução do problema da base fornecem uma solução para este problema.

Figura 2: $\Lambda_1 \cup \Lambda_2$ não é um reticulado.



Fonte: Os autores.

Teorema 8. *Sejam B e $\hat{B}$ matrizes com entradas inteiras de ordem $k \times n$ e $m \times n$ ($k \leq n$ e $m \leq n$), respectivamente. Se B e $\hat{B}$ têm posto completo (isto é, possuem linhas linearmente independentes) e Λ é o menor reticulado que contém $\Lambda(B)$ e $\Lambda(\hat{B})$, então Λ é constituído por todas as combinações lineares inteiras das linhas da matriz*

$$A = \begin{bmatrix} B \\ \hat{B} \end{bmatrix}.$$

Demonstração. Seja W o subespaço vetorial de $\mathbb{R}^n$ gerado pelas linhas de A. Como $\tilde{\Lambda} := \Lambda \cap W$ é um reticulado que contém $\Lambda(B)$ e $\Lambda(\hat{B})$ e está contido em Λ, segue que $\tilde{\Lambda} = \Lambda$ e $\Lambda \subset W$, uma vez que Λ é o menor reticulado que contém $\Lambda(B)$ e $\Lambda(\hat{B})$. Assim, para cada elemento $\boldsymbol{v}$ de Λ, existem números reais $x_1, \ldots, x_k$ e $y_1, \ldots, y_m$ tais que $\boldsymbol{v} = x_1\boldsymbol{b}_1 + \cdots + x_k\boldsymbol{b}_k + y_1\hat{\boldsymbol{b}}_1 + \cdots + y_m\hat{\boldsymbol{b}}_m$, em que $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\}$ e $\{\hat{\boldsymbol{b}}_1, \ldots, \hat{\boldsymbol{b}}_m\}$ são as linhas de B e $\hat{B}$, respectivamente. Por outro lado, $x_1\boldsymbol{b}_1 + \cdots + x_k\boldsymbol{b}_k \in \Lambda(B)$ e $y_1\hat{\boldsymbol{b}}_1 + \cdots + y_m\hat{\boldsymbol{b}}_m \in \Lambda(\hat{B})$. Assim, existem inteiros $\alpha_1, \ldots, \alpha_k$ e $\beta_1, \ldots, \beta_m$ tais que $x_1\boldsymbol{b}_1 + \cdots + x_k\boldsymbol{b}_k = \alpha_1\boldsymbol{b}_1 + \cdots + \alpha_k\boldsymbol{b}_k$ e $y_1\hat{\boldsymbol{b}}_1 + \cdots + y_m\hat{\boldsymbol{b}}_m = \beta_1\hat{\boldsymbol{b}}_1 + \cdots + \beta_m\hat{\boldsymbol{b}}_m$, isto é, $(x_1 - \alpha_1)\boldsymbol{b}_1 + \cdots + (x_k - \alpha_k)\boldsymbol{b}_k = \boldsymbol{0}$ e $(y_1 - \beta_1)\hat{\boldsymbol{b}}_1 + \cdots + (y_m - \beta_m)\hat{\boldsymbol{b}}_m = \boldsymbol{0}$. Logo, $x_1, \ldots, x_k$ e $y_1, \ldots, y_m$ são inteiros, uma vez que por hipótese $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\}$ e $\{\hat{\boldsymbol{b}}_1, \ldots, \hat{\boldsymbol{b}}_m\}$ são conjuntos linearmente independentes. Isto mostra

que todo elemento de Λ pode ser escrito como uma combinação linear inteira das linhas da matriz A. Reciprocamente, se $\boldsymbol{v}$ é uma combinação linear inteira das linhas de A, então existem $\boldsymbol{u} \in \Lambda(B)$ e $\hat{\boldsymbol{u}} \in \Lambda(\hat{B})$ tais que $\boldsymbol{v} = \boldsymbol{u} + \hat{\boldsymbol{u}}$. Como $\Lambda(B)$ e $\Lambda(\hat{B})$ são subconjuntos de Λ, segue que $\boldsymbol{v}$, pois Λ é um subgrupo de $\mathbb{R}^n$. □

Exemplo 13. *Sejam*

$$B = \begin{bmatrix} 7 & 6 & 1 & 2 \\ 3 & 1 & 2 & 4 \end{bmatrix} \quad e \quad \hat{B} = \begin{bmatrix} 2 & 1 & 1 & 6 \\ 5 & 4 & 1 & 6 \end{bmatrix}.$$

Considere a matriz

$$A = \begin{bmatrix} B \\ \hat{B} \end{bmatrix} = \begin{bmatrix} 7 & 6 & 1 & 2 \\ 3 & 1 & 2 & 4 \\ 2 & 1 & 1 & 6 \\ 5 & 4 & 1 & 6 \end{bmatrix}.$$

Pelos Exemplos 6, 7, 8 e 9, a forma normal de Hermite de A é

$$\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Logo, $\{(1,0,1,2),(0,1,-1,2),(0,0,0,4)\}$ é uma base do menor reticulado que contém $\Lambda(B)$ e $\Lambda(\hat{B})$.

Além das três aplicações apresentadas, existem várias outras tanto básicas como não básicas, algumas delas estão listadas na referência [1].

Conflitos de Interesse

Os autores declaram que não têm conflitos de interesse.

Financiamento

O presente trabalho contou com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, referente à bolsa de mestrado da primeira autora.

O segundo autor agradece ao apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq Universal 405842/2023-6).

Aprovação do Comitê de Ética

Não se aplica.

Licença

Referências

[1] Micciancio, D. *Lattice Algorithms and Applications*. https://cseweb.ucsd.edu/classes/sp14/cse206A-a/. Acesso em: 22 de fevereiro de 2024.

[2] Micciancio, D. "Improving lattice based cryptosystems using the Hermite normal form". Em: *International Cryptography and Lattices Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 126–145.

[3] Peikert, C. "A decade of lattice cryptography". Em: *Foundations and Trends in Theoretical Computer Science* 10.4 (2016), pp. 283–424.

[4] Hashimoto, M. "Bases de Hilbert". Dissertação de Mestrado. São Paulo, SP: IME-USP, 2007.

[5] Costa, S. I. R. et al. *Lattices applied to coding for reliable and secure communications*. Springer International Publishing, 2017.

[6] Jorge, G. C. "Reticulados q-ários e algébricos". Tese de Doutorado. Campinas, SP: IMECC - UNICAMP, 2012.

[7] Boldrini, J. L. et al. *Álgebra linear*. 3ª ed. São Paulo: Harper & Row do Brasil, 1980.

[8] Bremner, M. R. *Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications*. Boca Raton: CRC Press, 2011.

[9] Strey, E. "Construções de reticulados a partir de códigos q-ários". Tese de Doutorado. Campinas, SP: IMECC - UNICAMP, 2017.

[10] Shmonin, G. *Hermite normal form: Computation and applications*. https://www.epfl.ch/labs/disopt/wp-content/uploads/2018/09/hnf.pdf. Acesso em: 22 de fevereiro de 2024.

[11] Shmonin, G. *Lattices and Hermite normal form*. https://www.epfl.ch/labs/disopt/wp-content/uploads/2018/09/lattices.pdf. Acesso em: 22 de fevereiro de 2024.

[12] Hefez, A. *Curso de Álgebra*. 4ª ed. Rio de Janeiro: IMPA, 2010.

Corresponding Author:
Eleonesio Strey, *eleonesio.strey@ufes.br*

Submitted: May 03, 2024
Accepted: March 26, 2025
Published: August 20, 2025
https://seer.ufu.br/index.php/BEJOM/index