MT803D - Tópicos em Matemática Aplicada

Matrizes Inteiras

# 1 Introdução

O estudo de matrizes com coeficientes inteiros e suas propriedades possui diversas aplicações na Geometria dos Números. O objetivo é resolver o sistema linear $A\boldsymbol{x} = \boldsymbol{b}$, com $A \in \mathbb{Z}^{n\times m}$, $\boldsymbol{b} \in \mathbb{Z}^{n\times 1}$, ou determinar quando este sistema tem ou não solução. Do ponto de vista de geometria dos números, seja o espaço afim (conjunto convexo)

$$\mathcal{S} = \{A\boldsymbol{x} - \boldsymbol{b} = 0 : \boldsymbol{x} \in \mathbb{R}^m\}.$$

Gostaríamos de determinar $S \cap \mathbb{Z}^m$. As ferramentas utilizadas para encontrar a solução deste sistema serão úteis também no estudo de pontos inteiros em reticulados.

Nesta seção utilizaremos algumas notações básicas de teoria dos números. A notação $a|b$ significa que existe $k \in \mathbb{N}$ tal que $b = ka$. Dados $a, b \in \mathbb{Z}$ o máximo divisor comum $g$ entre $a$ e $b$ é um inteiro positivo tal que $g|a$, $g|b$ e se algum $g' \in \mathbb{N}$ divide $a$ e $b$, então $g'|g$. Denotamos o máximo divisor comum por $\gcd(a, b)$. Essa definição se estende naturalmente para $n$ números $a_1, \ldots a_n$. Neste caso, o máximo divisor comum satisfaz uma regra de parênteses encaixados:

$$\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n) = \ldots$$

# 2 Propriedades Iniciais

Suponha que $n = 1$ e $m = 2$. Consideremos o sistema

$$a_1x_1 + a_2x_2 = b_1, \text{ com } x_1, x_2 \in \mathbb{Z}. \tag{1}$$

Um resultado básico da Teoria dos Números é:

**Teorema 1** (Identidade de Bézout)**.** *A equação* (1) *tem solução se, e somente se* $\gcd(a_1, a_2)|b_1$*. Neste caso, se* $(x_1, x_2)$ *é uma solução, todas as outras soluções são dadas por*

$$(x, y) = (x_1, x_2) + k\left(\frac{-a_2}{\gcd(a_1, a_2)}, \frac{a_1}{\gcd(a_1, a_2)}\right), k \in \mathbb{Z}$$

.

*Demonstração.* ($\Rightarrow$) Suponha que a equação tem solução e seja $g = \gcd(a_1, a_2)$. Como $g|a_1$ e $g|a_2$, $g|d$.
($\Leftarrow$) Seja $g_0$ o mínimo valor positivo para $a_1x_1' + a_2x_2', x_1', x_2' \in \mathbb{Z}$. Dividindo $a_1$ por $g_0$, temos $a_1 = kg_0 + r$, com $r$ da forma $a_1y_1 + a_2y_2 < a_1x_1' + a_2x_2'$ e portanto da minimalidade de $g_0$, necessariamente $r = 0$, ou ainda $g_0|a_1$. Pelos mesmos argumentos, $g_0|a_2$, e da condição de minimalidade $g_0 = \gcd(a_1, a_2)$. Como $b_1 = k\gcd(a_1, a_2)$, então $x_1 = kx_1'$ e $x_2 = kx_2'$ formam uma solução para a equação. Para determinar todas as outras, seja $\overline{x}_1, \overline{x}_2$ outra solução. Temos

$$a_1(\overline{x}_1 - x_1) + a_2(\overline{x}_2 - x_2) = 0 \Rightarrow \frac{a_1}{\gcd(a_1, a_2)}(\overline{x}_1 - x_1) = -\frac{a_2}{\gcd\left(a_1, a_2\right)}(\overline{y_1} - y_1).$$

Como $a_1/\gcd\left(a_1, a_2\right)$ e $a_2/\gcd\left(a_1, a_2\right)$ são co-primos, isso implica necessariamente que $a_1/\gcd\left(a_1, a_2\right) = -k(\overline{y}_1 - y_1)$, e $a_2/\gcd\left(a_1, a_2\right) = k(\overline{x}_1 - x_1)$. $\square$

# 3 Forma Normal de Hermite

Seja $A \in \mathbb{Z}^{n\times n}$ uma matriz com determinante não-nulo. Gostaríamos de determinar as soluções para o sistema $A\boldsymbol{x} = \boldsymbol{b}$ *sem* realizar qualquer operação fracional (ou seja, apenas multiplicações por inteiros são permitidas). Neste contexto, dizemos que duas matrizes $A$ e $B$ com entradas inteiras são *equivalentes* à esquerda se existe uma matriz inteira $U$, invertível, tal que $A = UB$. É claro que uma matriz $U \in \mathbb{Z}^{n\times n}$ é invertível se, e somente se, $\det U = \pm 1$. Tais matrizes são chamadas de *unimodulares*. Como o produto de matrizes unimodulares é, novamente, uma matriz unimodular, essas matrizes formam um grupo, denotado por $\mathrm{Gl}_n(\mathbb{Z})$. Em particular, as matrizes de permutação e mudança de sinal pertencem a $\mathrm{Gl}_n(\mathbb{Z})$. Utilizaremos extensivamente o fato de que as seguintes operações elementares podem ser traduzidas por meio de multiplicação por matrizes unimodulares:

(i) Troca de linhas/colunas

(ii) Troca de sinal de uma linha/coluna

(iii) Somar à linha/coluna $i$ um múltiplo inteiro da linha/coluna $j$.

Dizemos que $A$ está na *forma normal de Hermite* (HNF daqui para frente) se $A$ é triangular superior, com $0 \leq A_{ij} < A_{jj}, j = i+1, \ldots, n$. Para realizar a forma de Hermite, operaremos apenas por linhas, mas para a forma de Smith, necessitaremos de operações por colunas.

**Teorema 2.** *Toda matriz inteira não-singular é equivalente à esquerda a uma matriz na forma normal de Hermite.*

Vamos começar por provar o seguinte lema, que será também útil na construção de Forma Normal de Smith, na próxima seção.

**Lema 1.** *Seja $A \in \mathbb{Z}^{n\times m}$. Existe uma matriz unimodular $U$ tal que*

$$UA = \begin{pmatrix} g & * & * & \ldots & * \\ 0 & * & * & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \ldots & * \end{pmatrix},$$

*em que $g = \gcd(a_{11}, a_{21}, \ldots, a_{n1})$.*

*Demonstração.* Suponhamos que $a_{11} \neq 0$, caso contrário multiplicamos $A$ à esquerda por uma matriz de permutação tal que $a_{11}$ satisfaça isso (caso todos os elementos da primeira linha sejam não-nulos, o Lema torna-se trivial). Seja $g_1 = \gcd(a_{11}, a_{21})$ e $x_{11}$, $x_{21}$ inteiros tais que $a_{11}x_{11} + a_{21}x_{21} = g_1$. Construímos a matriz unimodular $\hat{U}_1$

$$\hat{U}_1 = \begin{pmatrix} x_{11} & x_{21} \\ -a_{21}/g_1 & a_{11}/g_1 \end{pmatrix},$$

e a estendemos para uma matriz $U_1$ de ordem $n \times n$ , tal que:

$$U_1 = \begin{pmatrix} \hat{U}_1 & \mathbf{0} \\ \mathbf{0} & I_{n-1} \end{pmatrix}.$$

Temos que $U_1$ é uma matriz unimodular. Além disso, $U_1A$ é da forma

$$U_1A = \begin{pmatrix} g_1 & * & * & \ldots & * \\ 0 & * & * & \ldots & * \\ a_{31} & * & * & \ldots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & * & * & \ldots & * \end{pmatrix}.$$

Podemos agora multiplicar $U_1 A$ à esquerda por uma matriz permutação $\tilde{U}_1$ tal que

$$\tilde{U}_1 U_1 A = \begin{pmatrix} g_1 & * & * & \dots & * \\ a_{31} & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & * & * & \dots & * \end{pmatrix}.$$

Repetindo os mesmos argumentos anteriores sucessivamente, podemos encontrar, ao fim, uma matriz unimodular $U$ tal que

$$UA = \begin{pmatrix} \bar{g} & * & * & \dots & * \\ 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{pmatrix},$$

em que $\bar{g} = \gcd \dots (\gcd(\gcd(a_{11}, a_{21}), a_{31}, \dots)$. Pela regra dos parênteses encaixados, $\bar{g} = g$, o que completa a prova. $\square$

*Demonstração do Teorema 2:* Por indução na dimensão da matriz. Para $n = 1$, o teorema é trivial. Suponha que o teorema seja válido para matrizes de ordem $(n-1) \times (n-1)$. Pelo lema acima existe $U_1$ tal que

$$U_1 A = \begin{pmatrix} g & \mathbf{0} \\ \mathbf{0} & \hat{A} \end{pmatrix},$$

em que $\hat{A}$ tem dimensões $(n-1) \times (n-1)$ e os vetores nulos tem as dimensões apropriadas. Pela hipótese de indução, existe $\hat{U}_2$ tal que $\hat{U}_2 \hat{A}$ está na forma normal de Hermite. Considere a matriz unimodular

$$U_2 = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \hat{U}_2 \end{pmatrix}.$$

Claramente a matriz $B = U_2 U_1 A$ é triangular superior e satisfaz a condição da forma de Hermite, exceto pela primeira linha. Para finalizar a demonstração, basta somar à primeira linha, múltiplos convenientes das outras linhas (o que pode ser realizado através de multiplicação por matrizes unimodulares). Mais formalmente, efetuando a divisão de $B_{1j}$ por $B_{jj}$, $j \geq 2$, tomamos $k_j$ tal que

$B_{1j} = \hat{B}_{1j} + k_j B_{jj}$, $0 \leq \hat{B}_{1j} < B_{jj}$ e fazemos

$$U_3 = \begin{pmatrix} 1 & -k_2 & -k_3 & \dots & -k_n \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ 0 & 0 & \dots & \dots & 1 \end{pmatrix}.$$

O produto $U_3U_2U_1A$ está na forma de Hermite, com $U_3$, $U_2$ e $U_1$ unimodulares, finalizando a demonstração. $\square$

A generalização da forma normal de Hermite para matrizes não quadradas é natural. Por exemplo, para matrizes com $(n+t) \times n$ colunas, a matriz reduzida é da forma

$$B = \begin{pmatrix} \hat{B} \\ \mathbf{0} \end{pmatrix},$$

em que $\hat{B}$ é quadrada e satisfaz as condições de Hermite e $\mathbf{0}$ é uma matriz nula de dimensões apropriadas. Além disso, caso a matriz seja singular, podemos relaxar a condição de dominância diagonal para $A_{ii} \neq 0 \to A_{ii} > A_{ij} \geq 0, j = i+1, \dots, n$. Assim, teríamos uma decomposição de Hermite possibilitando zeros na diagonal.

Em [New72, Teo. II.3] é demonstrado que dada uma matriz $B$ de posto completo, a sua forma normal de Hermite é única. Portanto, daqui para frente falaremos *da* forma norma de Hermite de uma matriz.

Incidentalmente, na demonstração da forma normal de Hermite exibimos um algoritmo com número polinomial de operações aritméticas para calculá-la. Entretanto, pode ser que os números envolvidos nos cálculos cresçam demais, o que tornaria o algoritmo não-polinomial. Em [Coh00, Sec. 2.4] é exibido um algoritmo que evita o crescimento desses números, provando que a forma normal de Hermite pode ser realizada em um número polinomial de operações em $n, m$ e $\max|a_{ij}|$.

Um corolário da forma normal de Hermite são algoritmos *exatos* (sem problemas de arredondamento), para resolver o sistema linear $A\boldsymbol{x} = \boldsymbol{b}$ e para inverter a matriz $A$, inteira (ou racional).

# 4 Forma Normal de Smith

Seja agora uma matriz $A \in \mathbb{Z}^{m \times n}$. Gostaríamos de saber sob quais condições o sistema $A\boldsymbol{x} = \boldsymbol{b}$ possui uma solução inteira. A *Forma Normal de Smith*, reminiscente da Forma Normal de Hermite, resolve este problema. Para definir a forma de Hermite, utilizamos equivalências à esquerda. Para a forma normal de Smith, precisamos de equivalências à esquerda e à direita. Assim, diremos que duas matrizes $A, B \in \mathbb{Z}^{m\times n}$ são *equivalentes* (no sentido de Smith), se existem matrizes unimodulares $U \in \mathrm{Gl}_m(\mathbb{Z})$ e $V \in \mathrm{Gl}_n(\mathbb{Z})$ tais que $A = UBV$.

**Teorema 3.** *Toda matriz $A$ é equivalente a*

$$D = \begin{pmatrix} \hat{D} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix},$$

*em que*

$$\hat{D} = \begin{pmatrix} s_1 & 0 & \dots & 0 \\ 0 & s_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & s_k \end{pmatrix}$$

*é uma matriz satisfazendo $s_i | s_{i+1}, i = 1, \dots k$ e $k \leq \min(m, n)$.*

*Demonstração.* Faremos a prova para o caso $m = (n + t) \geq n$, $t > 0$. Se $n = 0$ o teorema é trivial, e segue do Lema 1. Para $n > 1$, suponhamos, sem perda de generalidade que $a_{11} > 0$.

(i) Redução da primeira linha e primeira coluna: Queremos encontrar matrizes $U$ e $V$ tais que

$$UAV = \begin{pmatrix} g & 0 \\ 0 & \hat{A} \end{pmatrix}. \tag{2}$$

Pelo Lema 1, existe $U_1 \in \mathrm{Gl}_m(\mathbb{Z})$ tal que

$$U_1 A = \begin{pmatrix} g_1^{(1)} & * & * & \dots & * \\ 0 & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \dots & * \end{pmatrix}, \tag{3}$$

em que $g_1^{(1)} = \gcd(a_{11}, \dots, a_{n1})$. Se todos os elementos da primeira linha de $U_1 A$ são múltiplos de $g_1^1$, podemos subtrair cada coluna de um múltiplo da primeira, de modo a obter a forma desejada (é claro que esta operação pode ser feita por meio da multiplicação à direita por uma matriz $V_1 \in Gl_n(\mathbb{Z})$). Caso contrário, aplicando uma versão "à direita" do lema, existe uma matriz

$V_1 \in \mathrm{Gl}_n(\mathbb{Z})$ tal que

$$U_1 A V_1 = \begin{pmatrix} g_1^{(2)} & 0 & 0 & \dots & 0 \\ a_{21}^{(2)} & * & * & \dots & * \\ a_{31}^{(2)} & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1}^{(2)} & * & * & \dots & * \end{pmatrix},$$

com $g_1^{(2)} = \gcd(g_1^{(1)}, a_{12}, a_{13}, \dots, a_{1m}) < g_1^{(1)}$. Novamente, se todos os elementos da primeira coluna de $U_1AV_1$ são múltiplos de $g_1^{(2)}$, podemos encontrar uma matriz $U_2$ tal que $U_2(U_1AV_1)$ possui apenas a primeira linha e primeira coluna nulas. Caso contrário, repetimos o processo para obter uma matriz como da equação 3, com $g_1^{(3)} < g_1^{(2)}$. Repetindo estas operações, como estamos decrescendo o valor de $g_1^{(i)}$ a cada passo, eventualmente teremos $g_1^{(i)} = 1$, ou todos os elementos da primeira linha/coluna da matriz correspondente múltiplos de $g_1^{(i)}$. A partir daí, realizamos mais uma redução e transformamos a matriz no formato desejado (2).

(ii) Divisão por $g$: Até este momento, obtemos apenas uma matriz $\tilde{A}$ com primeira linha/coluna nula, exceto pelo primeiro elemento, que denotaremos por $g$. Para aplicar a hipótese de indução efetivamente, precisamos garantir que $g$ divide todos os outros elementos de $\tilde{A}$. Isto pode ser garantido por operações elementares da seguinte forma.

Suponha que algum elemento $\tilde{a}_{ij}$ não é divisível por $g$. Por meio de operações elementares, substituímos a coluna 1 pela soma entre a coluna 1 e a coluna $j$ e, a partir daí, repetimos o processo do item $(i)$ para deixar a nova matriz no formato 2. A resultante será uma matriz tal que o novo elemento $(1, 1)$ é um divisor próprio de $g$. Como este processo sempre reduz $g$, eventualmente chegamos em um estágio em que o elemento $(1, 1)$ da nova matriz ($\hat{A}$, digamos) divide todos os outros elementos.

(iii) *Passo de Indução*: Realizando as operações em (i) e (ii), temos:

$$UAV = \begin{pmatrix} g & \mathbf{0} \\ 0 & \hat{A} \end{pmatrix}.$$

Pela hipótese de indução, existem $\hat{U}, \hat{V}$ tais que $\hat{U}A\hat{V}$ está na forma de Smith, o que finaliza a prova. □

## 4.1 Significado da Forma de Smith

Os elementos $s_i$ da diagonal na forma normal de Smith tem um significado muito claro em termos da matriz original. Eles são estão relacionados com o que chamamos de *divisores determinantais* de ordem $i$. Seja $\mathcal{I}_n = \{1, \dots, n\}$. Denotamos por $A_{\omega,\tau}$ a submatriz de $A$ obtida considerando as linhas de $\omega, \tau \subset \mathcal{I}_n$. O $i$-ésimo divisor determinantal de $A$ é dado por

$$d_i(A) = \gcd_{\substack{\omega,\tau \subset \mathcal{I}_n \\ \#\omega, \#\tau = k}} (\det A_{\omega,\tau}).$$

Um resultado auxiliar utilizado é a *fórmula de Cauchy-Binet*, que é válida de maneira bastante geral.

**Lema 2.** *Sejam $A \in \mathbb{R}^{n\times k}$, $B \in \mathbb{R}^{k\times n}$.*

$$\det AB = \sum_{\substack{\omega \in \mathcal{I}_n \\ \#\omega = n}} \det A_{\mathcal{I}_n,\omega} \det B_{\omega,\mathcal{I}_n}.$$

**Proposição 4.1.** *Duas matrizes equivalentes possuem os mesmos divisores determinantais.*

*Demonstração.* Seja $A = UBV$, com $U \in \mathrm{Gl}_m(\mathbb{Z})$ e $V \in \mathrm{Gl}_n(\mathbb{Z})$. Utilizando uma versão do Lema acima,

$$\det B_{\omega,\tau} = \sum_{\beta,\gamma} \det U_{\omega,\beta} \det A_{\beta,\gamma} \det V_{\gamma,\tau},$$

em que a soma é sobre todos os $\beta, \gamma \in \mathcal{I}_n$ com cardinalidade $k$. Portanto, como $d_k(A)$ divide $A_{\beta,\gamma}$, temos que $d_k(A) | \det B_{\omega,\tau}$, para qualquer $\omega, \tau$, e portanto $d_k(A)|d_k(B)$. Analogamente, temos que $d_k(B)|d_k(A)$, de onde deduzimos que $d_k(B) = d_k(A)$. $\square$

Da proposição acima, segue que $A$ e sua forma normal de Smith possuem os mesmos divisores determinantais. Mas os divisores de $D$ são claramente

$$\begin{aligned} d_1(A) &= s_1 \\ d_2(A) &= s_2 s_1 \\ &\vdots \\ d_k(A) &= s_k s_{k-1} \dots s_1. \end{aligned} \tag{4}$$

Assim $s_i = d_i(A)/d_{i-1}(A)$. Incidentalmente, isso demonstra que $d_{i-1}(A)|d_i(A)$. Definimos $k = \max_{d_i(A) \neq 0} i$ como o *posto* da matriz $A$.

**Teorema 4.** *Duas matrizes $A$ e $B$ são equivalentes se, e somente se, possuem os mesmos divisores determinantais.*

Assim, os divisores $d_i(A)$, bem como os elementos da forma de Smith $s_i(A)$ são invariantes por equivalência.

# 5 Aplicações

## 5.1 Sistemas Lineares Inteiros

Seja $A$ uma matriz $m \times n$ e $\boldsymbol{b}$. Queremos encontrar as soluções inteiras de $A\boldsymbol{x} = \boldsymbol{b}$. Aplicando a forma normal de Smith, temos $UAV = D$, considere $\boldsymbol{y} = V^{-1}\boldsymbol{x}$ e $c = U\boldsymbol{b}$

$$A\boldsymbol{x} = \boldsymbol{b} \iff D\boldsymbol{y} = \boldsymbol{c}.$$

O sistema acima tem solução se, e somente se, $s_i | c_i$. Neste caso, qualquer solução é dada por $y_i = s_i/c_i, i = 1, \ldots k$ e $y_i \in \mathbb{Z}$, $i = k+1, \ldots, n$. Assim, a forma paramétrica das soluções é dada por

$$\mathcal{S} \cap \mathbb{Z}^n = \left\{ V \begin{pmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \end{pmatrix} : \boldsymbol{y}_1 = D^{-1}\boldsymbol{c}, \text{ e } \boldsymbol{y}_2 \in \mathbb{Z}^{n-k} \right\}. \tag{5}$$

Uma outra consequência é a identidade de Bézout generalizada.

**Proposição 5.1.** *A equação $a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = d$ tem solução se, e somente se, $d = k \gcd(a_{11}, \ldots, a_{1n})$. Neste caso, dada uma solução $x_1^0, \ldots, x_n^{(0)}$, todas as outras podem ser descritas como em (5).*

Como segundo exemplo, considere o sistema linear

$$\begin{pmatrix} -1 & n_1 & 0 \\ -1 & 0 & n_2 \end{pmatrix} \cdot \begin{pmatrix} x \\ k_1 \\ k_2 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix},$$

com as variáveis $x, k_1, k_2$. Suponhamos que $\gcd(n_1, n_2) = 1$. Aplicando a redução de Smith, vemos que a matriz do lado direito é equivalente a uma matriz cujos fatores de Smith são todos iguais a 1. A partir daí, é fácil ver que o sistema sempre tem solução. Este sistema é um caso especial do Teorema do Resto Chinês [Coh00]:

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2. \end{cases}$$

## 5.2 Pontos Inteiros em Domínios Fundamentais

Seja $[0,1)^n$ o cubo $\{\boldsymbol{x} \in \mathbb{R}^n : 0 \le x_i < 1\}$. O paralelotopo fundamental associado a uma matriz $A \in \mathbb{Z}^{n \times n}$ é definido como $\mathcal{P}(A) = \{A\boldsymbol{x} : \boldsymbol{x} \in [0,1)^n\}$. Por exemplo, em $\mathbb{R}^2$, para

$$A = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}$$

temos o paralelogramo (nem aberto nem fechado)

$$\mathcal{P}(A) = \{(2x_1 + x_2, 3x_1 + 5x_2), 0 \leq x_1, x_2, < 1\},$$

que possui 7 pontos inteiros. É uma aplicação interessante da forma de Hermite (ou Smith) mostrar que $\#(\mathcal{P}(A) \cap \mathbb{Z}^n) = |\det A|$. Seja $A = UDV$, em que $D$ está na forma normal de Smith. Gostaríamos de encontrar os possíveis $\boldsymbol{y} \in \mathbb{Z}^n$ tais que

$$\boldsymbol{y} = A\boldsymbol{x}, \boldsymbol{x} \in [0,1)^n \boldsymbol{x}.$$

Esse sistema é equivalente a

$$D\boldsymbol{w} = \boldsymbol{u},$$

em que $\boldsymbol{w} = V\boldsymbol{x}$ e $\boldsymbol{u} = U^{-1}\boldsymbol{y}$. É claro que $\boldsymbol{u} \in \mathbb{Z}^n \iff \boldsymbol{y} \in \mathbb{Z}$ (resp. $\boldsymbol{w} \in \mathbb{Z}^n \iff \boldsymbol{x} \in \mathbb{Z}^n$). Da forma de Smith, temos $s_i w_i = u_i$. Como $\boldsymbol{x} \in [0,1)$ não é inteiro, excetuando a origem, as únicas opções para $u_i$ são do tipo $u_i = k_i s_i + r_i$, em que $0 \leq r_i < s_i$ (ou seja, há $s_i$ escolhas para o resto). Mostramos que fixados $r_i$, existe um único $k_i$ (e portanto um único $w$) tal que $\boldsymbol{x} = V^{-1}\boldsymbol{w} \in [0,1)^n$. Com efeito, caso contrário, $\boldsymbol{w}$ e $\boldsymbol{w}'$ tais que $V^{-1}\boldsymbol{w}, V^{-1}\boldsymbol{w}' \in [0,1)^n$. Isso implica que $V^{-1}(\boldsymbol{w} - \boldsymbol{w}') \in (-1,1)^n$, e como $\boldsymbol{w} - \boldsymbol{w}'$ é inteiro (por quê?) $V^{-1}(\boldsymbol{w} - \boldsymbol{w}')$ também é inteiro, ou seja, $\boldsymbol{w} = \boldsymbol{w}'$. Assim, cada escolha para $r_i$ está associada com um único ponto inteiro em $\mathcal{P}(A)$. Como temos $s_i$ escolhas para cada $r_i$, no total temos $s_1 s_2 \ldots s_n = |\det A|$ pontos inteiros em $\mathcal{P}(A)$.

**Exercício 1.** Seja

$$\begin{pmatrix} -868 & -980 & -231 \\ 2254 & 2695 & 630 \\ 2541 & 2569 & 616 \end{pmatrix}$$

Mostre que $A$ é equivalente a uma matriz diagonal com elementos $7, 7$ e $91$.

**Exercício 2.** (Completamento Unimodular) Seja $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ com $\gcd(x_1, \dots, x_n) = 1$. Prove que existe uma matriz $U \in \mathrm{Gl}_n(\mathbb{Z})$ cuja primeira linha é igual a $\boldsymbol{x}$. Estenda este resultado para o caso $\gcd(x_1, \dots, x_n) = g > 1$.

**Exercício 3.** (Defeito de Ortogonalidade) Seja $B \in \mathbb{Z}^{n \times n}$ uma matriz não-singular e $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n$ as suas linhas. O *defeito de ortogonalidade* dos vetores-linha de $B$ é definido como

$$\frac{\|\boldsymbol{b}_1\| \, \|\boldsymbol{b}_2\| \dots \|\boldsymbol{b}_n\|}{|\det B|},$$

em que $\|\cdot\|$ é a norma euclidiana. Mostre:

(a) Mostre que $\gamma(B) \geq 1$, para qualquer $B$

(b) Se $M = \max_{i,j} |B_{ij}|$,
$$\det B \leq (\sqrt{n}M)^n.$$

(c) Mostre que qualquer matriz não-singular $B \in \mathbb{Z}^{n \times n}$ é equivalente à esquerda a uma outra matriz cujo defeito de ortogonalidade é menor ou igual que $\sqrt{n!}$.

**Exercício 4** (Newman [New72])**.** Seja $A \in \mathbb{Z}^{n \times n}$ com $\det A \neq 0$. Mostre que o menor inteiro positivo tal que $tA^{-1} \in \mathbb{Z}^{n \times n}$ é $t = s_n(A)$ (o $n$-ésimo elemento da diagonal na sua decomposição de Smith).

# Referências


[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 2000.

[New72] M. Newmman. *Integral Matrices.* Academic Press, 1972.