Universidade Federal de Uberlândia
Faculdade de Matemática

Anais da XII Mostra IC

17 a 19 de Maio de 2023

Uberlândia
2023

Sumário

Ends de Grupos: a dimensão de um espaço vetorial quociente sobre $\mathbb{Z}_2$

Mateus Fernando Araújo Silva
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
mateus.fernando@ufu.br

Francielle Rodrigues de Castro Coelho
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
francielle@ufu.br

Palavras-chave

Espaços Vetoriais sobre $\mathbb{Z}_2$.
Espaços Quocientes.
Ends de Grupos.

Resumo

A Teoria de Ends de Grupos é bastante relevante em Álgebra Homológica. Nesta área, o número de ends de um grupo, definido por Specker, é a dimensão $\mathbb{Z}_2$ de um quociente de espaços vetoriais. Neste trabalho, apresentamos conceitos e resultados sobre ends de grupos.

1 Introdução

A Topologia Algébrica é uma área importante da Matemática na qual se resolvem problemas de Topologia com auxílio da Álgebra. Nesta área a Álgebra Homológica (na qual se estudam módulos e ends de grupos) se faz presente e tem bastante relevância.

A teoria de ends foi introduzida por Freudenthal (em 1931) e Hopf (em 1943) para grupos finitamente gerados e foi totalmente amparada na definição de ends de espaços. Em 1950, Specker, definiu de forma algébrica o número de ends de um grupo G qualquer. O conceito de ends de um grupo está intimamente relacionado com decomposição de grupos e é definido como a dimensão $\mathbb{Z}_2$ de um quociente de espaços vetoriais.

Neste trabalho, o principal objetivo é apresentar conceitos e resultados sobre ends de um grupo G, $e(G)$. Mais especificamente, calculamos $e(G)$, quando G é um grupo finito e no caso de G infinito, analisaremos algumas situações específicas (Proposição 3.2).

As principais referências para o desenvolvimento deste trabalho foram [1], [2] e [3].

2 Espaços Vetoriais sobre $\mathbb{Z}_2$

Definição 2.1. *Um conjunto não vazio V é um **espaço vetorial sobre um corpo K** ou um $K-$**espaço vetorial** (cujos elementos são denominados vetores), se estiverem definidas as seguintes duas operações:*

(A) *A cada par (u, v) de vetores de $V \times V$ se associa um vetor $u + v \in V$, chamado de soma de u e v, de modo que:*

(A_1) $(u + v) + w = u + (v + w), \forall u, v, w \in V$.

(A_2) $u + v = v + u, \forall u, v \in V$.

(A_3) *Exista um vetor em V, denominado vetor nulo e denotado por 0, tal que $0 + v = v$.*

(A_4) *Para cada vetor $v \in V$ exista um vetor em V, denotado por $-v$, tal que $v + (-v) = 0$.*

(M) *A cada par (α, v) de vetores de $K \times V$ se associa um vetor $\alpha \cdot v \in V$, denominado multiplicação por escalar de α por v, de modo que:*

(M_1) $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v), \forall \alpha, \beta \in K$ *e* $\forall v \in V$.

(M_2) $1 \cdot v = v, \forall v \in V$ *(onde 1 é o escalar unidade de K).*

(M_3) $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v, \forall \alpha \in K$ *e* $\forall u, v \in V$.

(M_4) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v, \forall \alpha, \beta \in K$ *e* $v \in V$.

Note que as condições A_1 a A_4 nos dizem que $(V, +)$ é um grupo abeliano.

Exemplo 2.2. *Seja $A \neq \emptyset$ e consideremos $V = P(A) = \{X | X \subset A\}$. Podemos verificar que $(P(A), +)$ é um grupo abeliano (em que todo elemento não nulo tem ordem 2) com a operação diferença simétrica, isto é,*

$$X \triangle Y = (X \cup Y) - (X \cap Y) = (X \cap Y^c) \cup (X^c \cap Y),$$

que iremos indicar sempre aditivamente, ou seja, $X + Y = X \triangle Y$.

Considere a multiplicação por escalar $\mathbb{Z}_2 \times P(A) \to P(A)$ *dada por* $\overline{0} \cdot X = \emptyset$ *e* $\overline{1} \cdot X = X$. *Esta multiplicação está bem definida e verifica os demais axiomas da definição de espaço vetorial sobre o corpo* $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$. *Assim,* $P(A)$ *é um espaço vetorial sobre* $\mathbb{Z}_2$ *para todo* $A \neq \emptyset$. *Em particular, se* G *é um grupo,* $P(G)$ *é um espaço vetorial sobre* $\mathbb{Z}_2$.

Este $\mathbb{Z}_2-$*espaço vetorial será de fundamental importância na definição de ends de* G.

Definição 2.3. *Seja* V *um espaço vetorial sobre um corpo* K. *Um subconjunto* W *de* V *é um* ***subespaço vetorial de*** V *se a restrição das operações de* V *a* W *torna esse conjunto um* $K-$*espaço vetorial.*

Exemplo 2.4. *Seja* $A \neq \emptyset$ *e* $F(A) = \{X \in P(A) | X$ *é finito* $\}$, $F(A)$ *é um subespaço do* $\mathbb{Z}_2-$*espaço vetorial* $P(A)$ *dado no exemplo* 2.2.

(i) *O conjunto vazio é finito (com zero elemento) e assim pertence a* $F(A)$.

(ii) $X, Y \in F(A)$, *implica* $a \cdot X + b \cdot Y \in F(A)$ *para todo* $a, b \in \mathbb{Z}_2$, *pois*

$a = \overline{0}, b = \overline{0} \Longrightarrow a \cdot X + b \cdot Y = \emptyset \in F(A)$.

$a = \overline{1}, b = \overline{0} \Longrightarrow a \cdot X + b \cdot Y = X \in F(A)$.

$a = \overline{0}, b = \overline{1} \Longrightarrow a \cdot X + b \cdot Y = Y \in F(A)$.

$a = \overline{1}, b = \overline{1} \Longrightarrow a \cdot X + b \cdot Y = X + Y = (X \cap Y^c) \cup (X^c \cap Y) \subset X \cup Y$.

Como $\emptyset$, X, Y *e* $X \cup Y$ *são finitos, segue que* $a \cdot X + b \cdot Y \in F(A)$.

Observação 2.5. *Para* $F(A)$ *definido no exemplo anterior, temos:*

• *Se* A *é finito então* $F(A) = P(A)$.

• *Se* A *é infinito então necessariamente* $F(A) \neq P(A)$, *pois* $A \in P(A)$ *e* $A \notin F(A)$.

Por exemplo, $\mathbb{Z} \in P(\mathbb{Z})$, *mas* $\mathbb{Z} \notin F(\mathbb{Z})$. *Logo,* $F(\mathbb{Z}) \neq P(\mathbb{Z})$.

Exemplo 2.6. *Seja* $(G, \cdot)$ *um grupo. Considere o* $\mathbb{Z}_2-$*espaço vetorial* $P(G)$. *Seja*

$$Q(G) = \{X \subset G | X + gX \in F(G), \forall g \in G\}.$$

Aqui, dado $g \in G, gX := \{g \cdot x | x \in X\}$, *onde "*$\cdot$*" indica a operação do grupo.*

Observemos que:

• $g(X \cup Y) = gX \cup gY$ *(claro).*

• $g(X \cap Y) = gX \cap gY$, *pois* $g \cdot x = g \cdot y \Longleftrightarrow g^{-1} \cdot g \cdot x = g^{-1} \cdot g \cdot y \Longleftrightarrow x = y$.

• $gX^c = (gX)^c$, *pois* $G = gG = g(X \cup X^c) = gX \cup gX^c$ *e* $\emptyset = g(X \cap X^c) = gX \cap gX^c$.

• $g(X+Y) = g[(X \cap Y^c) \cup (X^c \cap Y)] = g(X \cap Y^c) \cup g(X^c \cap Y) = [gX \cap (gY)^c] \cup [(gX)^c \cap gY] = gX + gY$.

Agora, mostremos que $Q(G)$ *é um subespaço vetorial de* $P(G)$. *De fato,*

• $Q(G) \neq \emptyset$, *pois* $\emptyset \in Q(G)$.

• $\forall X, Y \in Q(G), (X+Y) + g(X+Y) = X+Y+gX+gY = (X+gX)+(Y+gY) \in F(G)$. *Logo,* $X + Y \in Q(G)$.

• $\forall k \in \mathbb{Z}_2$ *e* $\forall X \in Q(G), kX \in Q(G)$ *pois* $\overline{0}X + g(\overline{0}X) = \emptyset \in F(G)$ *e* $\overline{1}X + g(\overline{1}X) = X + gX \in F(G)$.

Observação 2.7. *Se $X \in F(G)$ então $X + gX$ será finito para todo $g \in G$. Daí, $X \in Q(G)$, isto é, $F(G) \subset Q(G)$ e portanto, $F(G)$ é um subespaço vetorial de $Q(G)$.*

Observação 2.8. *No caso em que G é finito temos que $P(G) = F(G) = Q(G)$.*

Definição 2.9. *Sejam V um espaço vetorial sobre K e W um subespaço de V. Para um vetor $v \in V$, escrevemos $v + W$ para representar o conjunto de somas $v + w$ com $w \in W$, ou seja,*

$$v + W = \{v + w | w \in W\}.$$

*Esses conjuntos são chamados **classes laterais** de W em V e são denotados por $\overline{v}$.*

3 Ends de Grupos

Definição 3.1. *Dado um grupo G, o número de ends de G, denotado por $e(G)$, é definido por $e(G) := dim_{\mathbb{Z}_2}(Q(G)/F(G))$, que denotamos apenas por $dim(Q(G)/F(G))$.*

Proposição 3.2. *Seja G um grupo.*

(i) Se G é infinito, então $\overline{\emptyset}$ e $\overline{G}$ são elementos distintos em $Q(G)/F(G)$ e portanto, $e(G) \geq 1$.

(ii) G é finito se, e somente se, $e(G) = 0$.

(iii) $e(G) \geq 2$ se, e somente se, existe $\overline{A} \in Q(G)/F(G)$ tal que $\overline{A} \neq \overline{\emptyset}$ e $\overline{A} \neq \overline{G}$. Neste caso, $\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}$ são elementos distintos em $Q(G)/F(G)$.

(iv) $e(G) = 2$ se, e somente se, existe $\overline{A}$ como em (iii) tal que para qualquer $\overline{B} \in Q(G)/F(G)$, $\overline{B} \neq \overline{\emptyset}$ e $\overline{B} \neq \overline{G}$ tem-se $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Demonstração. (i) Dado um grupo G, temos que $G \in Q(G)$, pois para qualquer $g \in G, G + gG = G + G = \emptyset \in F(G)$. Assim, $\overline{G} \in Q(G)/F(G)$.

Agora, como G é infinito segue que $G \notin F(G)$. Logo, $G + F(G) \neq \emptyset + F(G)$ e então $\overline{G} \neq \overline{\emptyset}$. Portanto, $e(G) = dim(Q(G)/F(G)) \geq 1$.

(ii) Como G é finito, temos que $P(G) = F(G) = Q(G)$. Logo, $e(G) = dim(Q(G)/F(G)) = 0$.

Reciprocamente, suponhamos por absurdo que G seja infinito. Então, por (i), temos que $e(G) \geq 1$, o que contradiz a hipótese. Portanto, G é finito.

(iii) Claramente, $e(G) \geq 2$ se, e somente se, existe $\overline{A} \in Q(G)/F(G)$ tal que $\overline{A} \neq \emptyset$ e $\overline{A} \neq \overline{G}$. Neste caso, considerando um tal A temos:

• $\forall g \in G, A^c + gA^c = (A^c \cap (gA^c)^c) \cup (A \cap (gA^c)) = (A^c \cap gA) \cup (A \cap (gA)^c) = A + gA \in F(G)$ pois $A \in Q(G)$. Daí, $\overline{A^c} \in Q(G)/F(G)$.

• $\overline{A^c} \neq \overline{A}$. De fato, se $\overline{A^c} = \overline{A}$ então $A^c + A = G \in F(G)$, o que é uma contradição, pois G é infinito.

• $\overline{A^c} \neq \overline{\emptyset}$, pois como $\overline{A} \neq \overline{G}$ segue que $\overline{A} + \overline{G} \neq \overline{\emptyset}$, isto é, $A^C = A + G \notin F(G)$.

• $\overline{A^c} \neq \overline{G}$ pois se $\overline{A^c} = \overline{G}$ então $A^c + G = A \in F(G)$, o que é um absurdo, já que A é infinito.

Logo, $\{\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}\} \subset Q(G)/F(G)$ e como $\{\overline{\emptyset}, \overline{A}, \overline{A^c}, \overline{G}\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ segue que $e(G) \geq 2$.

(iv) Consequência imediata de (iii). ■

4 Considerações finais

A teoria de ends de grupos, de certo modo, nos fornece uma maneira de medir a "infinitude"de um grupo, em termos da sua estrutura de subgrupos. Esta teoria tem sua relevância em algumas áreas da Matemática, por exemplo, na Álgebra e na Topologia Algébrica. Na Álgebra, a teoria de ends está relacionada com decomposição de grupos e classificação de grupos e na Topologia Algébrica, está relacionada com a teoria de cohomologia de grupos. Além disso, esta teoria também é importante ao se estudar a classificação de variedades.

Agradecimentos

Na condição de bolsista do PET Matemática da Universidade Federal de Uberlândia, agradeço ao Programa de Eduação Tutorial da SESu/MEC pelo fomento.

Referências

[1] CIOCA, D. M. **Cohmologia e Ends de Grupos**. Dissertação (Mestrado em Matemática) - IBILCE - UNESP, 1997.

[2] LIMA, E. L. **Álgebra Linear**. Coleção Matemática Universitária. 3ª Edição. Rio de Janeiro: SBM, 2014.

[3] SCOTT, G. P.; WALL, C. T. C. **Topological Methods in Group Theory**. London Math. Soc. Lect. Notes Series 36, Homological Group Theory, 167-174, 1972.

O quão irracional são os números

Jackson Johnson Cunha Silva

Universidade Federal de Uberlândia, Departamento de Matemática - FAMAT, Uberlândia, Minas Gerias, Brasil
jackson.silva@ufu.br

Josimar Joao Ramirez Aguirre

Universidade Federal de Uberlândia, Departamento de Matemática - FAMAT, Uberlândia, Minas Gerias, Brasil
josimar.mat@ufu.br

Palavras-chave

Números Racionais.
Números Irracionais.
Medida de Irracionalidade.

Resumo

"Deus fez os inteiros, todo o resto é obra do homem". Esta frase de L. Kronecker captura exatamente a história da aparição dos conjuntos numéricos. Os números naturais aparecem do fato da necessidade do homem de ter uma contagem, logo os outros conjuntos numéricos vem dos problemas de resolver equações algébricas, por exemplo: a equação do tipo $5x - 3 = 0$ fornece a ideia de **números racionais**, mas nem todos os números reais são racionais. Esses outros números são chamados de **números irracionais**. Neste trabalho vamos apresentar um breve resumo sobre estes conjuntos e a relação de aproximar os números irracionais por números racionais, chamado de **medida de irracionalidade**.

1 Introdução

Desde o ensino fundamental, estudamos os números racionais, aprendemos fazer as operações elementares de soma, subtração, produto e divisão com eles (frações). Sabemos também que existem alguns números que não podem ser escritos como fração de dois inteiros, esses números são chamados de **números irracionais**. Iremos apresentar um breve estudos desses conjuntos numéricos, dar exemplos e demonstrações de números irracionais e a relação entre eles.

Finalmente veremos uma generalização do conceito de números racionais chamados de **números algébricos**.

2 Números racionais e irracionais

Definição 2.1. *Um número é chamado racional se é da forma* $\frac{p}{q}$ *onde* $p \in \mathbb{Z}$ *e* $q \in \mathbb{Z}^*$. *O conjunto dos números racionais é denotado por* $\mathbb{Q}$.

Exemplo 2.2. $0, 1, 7, \frac{2}{3}, -3, \frac{8}{5} \in \mathbb{Q}$.

Claramente $\mathbb{Z} \subset \mathbb{Q}$, mas existem alguns números reais que não podem ser escritos da forma de fração de dois inteiros. Esses números são definidos a seguir:

Definição 2.3. *Um número é chamado irracional quando ele não pertence ao conjunto dos números racionais. Esse conjunto será denotado por* $\mathbb{I}$.

Note que $\mathbb{R} = \mathbb{Q} \sqcup \mathbb{I}$. Veremos agora alguns exemplos de números irracionais.

Exemplo 2.4. $\sqrt{2}$ *é irracional.*

Demonstração. Suponha que $\sqrt{2} \in \mathbb{Q}$. Portanto o conjunto $S = \{n \in \mathbb{N} \mid n\sqrt{2} \in \mathbb{Z}\}$ é não vazio e logo tem elemento mínimo b, pelo Princípio da Boa Ordenação (PBO). Assim, existe $a \in \mathbb{Z}$, tal que $b\sqrt{2} = a$. Daí

$$\sqrt{2} = \frac{2-\sqrt{2}}{\sqrt{2}-1} = \frac{2-\frac{a}{b}}{\frac{a}{b}-1} = \frac{2b-a}{a-b}$$

Como $1 < \sqrt{2} < 2$, então $0 < a - b < b$. Logo $a - b \in S$ e é menor que b, contrariando a minimalidade de b. Portanto $\sqrt{2}$ não pode ser racional. ■

Exemplo 2.5. *O número de Euler* $e = 2.71828182845904\ldots$ *é irracional.*

Demonstração. Vamos construir uma sequência de intervalos onde a interseção será e. Seja o intervalo $I_1 = [2, 3]$, o seguinte intervalo é construído dividindo o I_1 em dois subintervalos de mesmo comprimento. Assim, escolhemos o segundo intervalo, da esquerda para direita, para ser o I_2. Então temos

que $I_2 = [2.5, 3]$. Agora, suponha que os $I_1, ..., I_{n-1}$ intervalos estejam construídos. Divida, I_{n-1} em n subintervalos de mesmo comprimento e defina I_n como o segundo subintervalo. Por construção, I_n tem comprimento $\frac{1}{n!}$ e assim,

$$I_1 = \left[1 + \frac{1}{1!}, 1 + \frac{2}{1!}\right] = \left[\frac{a_1}{1!}, \frac{a_1 + 1}{1!}\right]$$

$$I_2 = \left[1 + \frac{1}{1!} + \frac{1}{2!}, 1 + \frac{1}{1!} + \frac{2}{2!}\right] = \left[\frac{a_2}{2!}, \frac{a_2 + 1}{2!}\right]$$

$$\vdots$$

$$I_n = \left[1 + \frac{1}{1!} + \ldots + \frac{1}{n!}, 1 + \frac{1}{1!} + \ldots + \frac{2}{n!}\right] = \left[\frac{a_n}{n!}, \frac{a_n + 1}{n!}\right].$$

Como $I_1 \supset I_2 \supset I_3 \supset \ldots$ e o comprimento de I_n tende a zero quando n tende ao infinito, então, pelo Teorema de Cantor, ou Teorema dos Intervalos Encaixados, a interseção $\cap I_n$ é formada exatamente por um único ponto, digamos θ. Provaremos que $\theta = e$. Olhando para a forma explícita de I_n, não é difícil se convencer desse fato, visto que $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

Afirmação: $e \in \text{int } I_n$, para todo $n \geq 1$.

Claramente $e > \frac{a_n}{n!}$, para todo $n \geq 1$. Portanto, falta mostra que $e < \frac{a_n+1}{n!}$. Note que, para $n > 2$,

$$e - \sum_{j=1}^{n-1} \frac{1}{j!} = \frac{1}{n!}\left(1 + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \ldots\right) < \frac{1}{n!}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right) = \frac{2}{n!}.$$

Assim,

$$e < \sum_{j=1}^{n-1} \frac{1}{j!} + \frac{2}{n!} = \frac{a_n + 1}{n!}$$

mostrando a afirmação feita.

Como consequência, temos que $\bigcap_{n=1}^{\infty} I_n = \{e\}$. Finalmente, suponha que $e = \frac{p}{q}$, com $q > 0$. Pela afirmação anterior, temos $e \in \text{int } I_q$ e assim $\frac{a_q}{q!} < e < \frac{a_q+1}{q!}$ então $\frac{a_q}{q!} < \frac{p}{q} < \frac{a_q+1}{q!}$. Escrevendo $\frac{p}{q} = \frac{p(q-1)!}{q!}$, obtemos $a_q < p(q-1)! < a_q + 1$ que é um absurdo, pois a_q e $p(q-1)!$ são inteiros.

■

Observação 2.6. *$\mathbb{Q}$ é enumerável. Isto é, existe uma uma bijeção entre $\mathbb{Q}$ e o conjunto dos números naturais.*

3 Uma breve Introdução a Teoria da Medida

O fato de medir comprimentos, áreas, volumes é indispensável em nosso cotidiano. Agora quando trabalhamos com os conjuntos numéricos surge a necessidade de construir uma ferramenta de medição

para esses conjuntos. Existe uma teoria matemática para isso chamada de **Teoria da Medida**, mas não iremos aprofundar nela e sim dar uma pincelada desses conceitos necessários para “medir"os números racionais.

Comecemos com a ideia básica de medir intervalos: Dado um intervalo (a, b), sua medida é dada por $m(a, b) := b - a$. Avançando um pouco, podemos trabalhar com a união finita de intervalos disjuntos. Assim, a medida é dada como a soma da medidas de cada intervalo. Ou seja, se $a_1 < b_1 < a_2 < b_2 < \ldots < a_n < b_n$, temos

$$m\left(\bigcup_{i=1}^{n}(a_i, b_i)\right) = \sum_{i=1}^{n} m\left((a_i, b_i)\right) = \sum_{i=1}^{n}(b_i - a_i).$$

Seguindo esse raciocínio, podemos considerar a propriedade anterior para uma união infinita de intervalos disjuntos e ter o seguinte:

$$m\left(\bigcup_{i=1}^{\infty}(a_i, b_i)\right) = \sum_{i=1}^{\infty} m((a_i, b_i)) = \sum_{i=1}^{\infty}(b_i - a_i).$$

Um conjunto é dito **mensurável** se a sua medida está “bem"definida.
Considere as seguintes propriedades:

1. Para qualquer conjunto mensurável X, $m(X) \geq 0$
2. Para qualquer sequência disjunta de muitos conjuntos mensuráveis contáveis $X_1, X_2, \ldots,$

$$m\left(\bigcup_{i=1}^{\infty} X_i\right) = \sum_{i=1}^{\infty} m(X_i)$$

Iremos usar essas propriedades para encontrar a medida dos números racionais. Segue do fato que, se $X \subseteq Y$ são ambos conjuntos mensuráveis, então $m(X) \leq m(Y)$. Agora buscamos mostrar que a medida de qualquer conjunto unitário {x} é zero, $x \in \mathbb{R}$. Considere $\epsilon > 0$, temos que $x \subset (x - \frac{\epsilon}{2}, x + \frac{\epsilon}{2})$. Portanto

$$0 \leq m(\{x\}) \leq m\left(\left(x - \frac{\epsilon}{2}, x + \frac{\epsilon}{2}\right)\right) = x + \frac{\epsilon}{2} - \left(x - \frac{\epsilon}{2}\right) = \epsilon,$$

então $0 \leq m(\{x\}) \leq \epsilon$. Desde que $\epsilon > 0$ foi arbitrário, podemos fazer ϵ tender a zero, o que demonstra que $m(\{x\}) = 0$. Assim, finalmente podemos calcular a medida dos números racionais. Como os números racionais é enumerável, podemos enumerá-los como $\mathbb{Q} = \bigcup_{i=1}^{\infty}\{q_i\}$, então

$$m(\mathbb{Q}) = \sum_{i=1}^{\infty} m(\{q_i\}) = \sum_{i=1}^{\infty} 0 = 0.$$

Com isso chegamos que a medida dos números racionais é zero. Então, podemos dizer que quase todos os números reais são irracionais. Com a teoria da probabilidade, dado um número qualquer da reta

numérica, temos a garantia que quase todos os números são irracionais.

Agora que sabemos que ao escolher um número na reta real, com probabilidade 1, ele é irracional, podemos nos perguntar: Quão irracional ele é? Para encontrarmos essa resposta, iremos utilizar o conceito de medida de irracionalidade.

3.1 Uma medida de irracionalidade.

Vimos duas demonstrações de números irracionais, mas isso é apenas a "ponta do iceberg"de vários outros problemas relacionados. Um deles é saber quão esse número é irracional. Mais precisamente, a medida de irracionalidade para um número irracional α é uma função positiva e estritamente decrescente $f(x)$, para $x \geq 1$, e tal que

$$\left|\alpha - \frac{p}{q}\right| > f(q),$$

para todo número racional $\frac{p}{q}$, com $q \geq 1$. Ou seja, essa função mede o comportamento da distância entre α e qualquer racional.

Exemplo 3.1. *Vamos encontrar uma medida de irracionalidade para* $\sqrt{2}$.

Definimos $g(x) = x^2 - 2$ e $I = [\sqrt{2} - 1, \sqrt{2} + 1]$. Seja $\frac{p}{q} \in \mathbb{Q}$, com $q \geq 1$. Se $\frac{p}{q}$ não pertence a I, então $\left|\sqrt{2} - \frac{p}{q}\right| > 1 \geq \frac{1}{q^2}$. Para o caso $\frac{p}{q} \in I$, usamos o Teorema do Valor Médio para o intervalo fechado com extremos $\sqrt{2}$ e $\frac{p}{q}$. Assim existe ζ no interior desse intervalo, tal que

$$g(\sqrt{2}) - g\left(\frac{p}{q}\right) = g'(\zeta)\left(\sqrt{2} - \frac{p}{q}\right),$$

onde, como usual, g' denota a derivada da função g. Portanto, $\left|\sqrt{2} - \frac{p}{q}\right| = \left|\frac{g\left(\frac{p}{q}\right)}{2\zeta}\right|$. Agora é suficiente notar que $|g(\frac{p}{q})| \geq \frac{1}{q^2}$ e que $\zeta < \sqrt{2} + 1$, para obtermos $\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{2(\sqrt{2}+1)q^2}$. Daí, a desigualdade acima é válida para todo $\frac{p}{q} \in \mathbb{Q}$, e, desse modo, a função $f(x) = \frac{1}{2(\sqrt{2}+1)q^2}$ é uma medida de irracionalidade para $\sqrt{2}$.

Exemplo 3.2. *Vamos encontrar uma medida de irracionalidade para* e.

Agora, usaremos a construção geométrica feita no exemplo 2.5 para exibir uma medida de irracionalidade para e.

Definição 3.3. *A função de Smarandache* $S : \mathbb{N} \to \mathbb{N}$ *é definida por* $S(k) = min\{s \in \mathbb{N} : k|s!\}$. *Isto é,* $S(k)$ *é o menor número natural tal que* $S(k)!$ *é múltiplo de k.*

Exemplo 3.4. $S(1) = 1, S(2) = 2, S(6) = 3$ *e* $S(8) = 4$. *Além disso,* $S(p) = p, \forall p \in \mathbb{P}$.

Proposição 3.5. *Dados $p, q \in \mathbb{Z}$, com $q > 1$, então*

$$\left| e - \frac{p}{q} \right| > \frac{1}{(S(q)+1)!}.$$

Demonstração. Dados p e q como no enunciado anterior, defina $m = \frac{pS(q)!}{q}$ e $n = S(q)$. Claramente m e n são inteiros, com $n > 1$ e $\frac{p}{q} = \frac{m}{n!}$. Precisamos ainda de dois fatores:

- Pela construção de I_n, para $n > 1$, o número $\frac{a_n}{n!}$ é a fração mais próxima de e, cujo numerador é inteiro e o denominador $n!$ (caso contrário teríamos um inteiro entre a_n e $a_n + 1$).
- Para construir I_{n+1}, particionamos I_n em n subintervalos de comprimento $\frac{1}{(n+1)!}$. Como e pertence ao segundo desses subintervalos, então a distância entre e e o extremo esquerdo de I_n (isto é, $\frac{a_n}{n!}$) é maior que $\frac{1}{(n+1)!}$. Por esses motivos, temos

$$\left| e - \frac{p}{q} \right| = \left| e - \frac{m}{n!} \right| \geq \left| e - \frac{a_n}{n!} \right| > \frac{1}{(n+1)!} = \frac{1}{(S(q)+1)!},$$

como desejado.

■

4 Conclusão

Dessa forma, passando pelos elementos dos conjuntos racionais e irracionais para um estudo mais aprofundado, conseguimos encontrar uma ferramenta de operação que envolve esses elementos, assim, a medida de irracionalidade nos proporciona saber o quanto um número é irracional, através dos números racionais.

Referências

[1] MARQUES, D. **Teoria dos Números Transcendentes**. Rio de Janeiro: SBM, 2013.

[2] ROCHFORD, A. There are Almost No Rational Numbers. **Post do site Austin Rochford**. 2013. Disponível em: <https://austinrochford.com/posts/2013-12-31-almost-no-rationals.html>. Acesso em: 6 abril 2023.

Modelo fracionário do resfriamento de Newton

Fernanda de Andrade Flor

UFU, FAMAT, Uberlândia, Minas Gerais, Brasil
fernandaflor@ufu.br

Rafael Antônio Rossato

UFU, FAMAT, Uberlândia, Minas Gerais, Brasil
rafaelrossato@ufu.br

Palavras-chave

Cálculo Fracionário.
Funções de Mittag-Lefler.
Lei do resfriamento de Newton.

Resumo

Neste trabalho iremos discutir a influência da derivada de ordem fracionária segundo Caputo no modelo matemático de resfriamento de um corpo desenvolvido por Isaac Newton. Ao considerarmos uma redução na ordem da derivada para um número não inteiro entre 0 e 1, obtemos soluções que decrescem mais lentamente que no caso de ordem inteira, o que nos sugere um decrescimento na taxa de variação do modelo. Tal verificação contribui para o estudo de possíveis interpretações físicas e geométricas da derivada fracionária.

1 Introdução

Este trabalho apresenta um estudo da abordagem fracionária do clássico modelo de resfriamento de Newton, que consiste na substituição da ordem da derivada da equação diferencial deste modelo por uma ordem não inteira $\alpha \in (0, 1)$. Para isto apresentamos inicialmente alguns conceitos do Cálculo de ordem não inteira, usualmente chamado de Cálculo Fracionário.

Na Seção 2 apresentamos alguns conceitos da Transformada de Laplace e funções especiais essenciais para o estudo do Cálculo Fracionário, na Seção 3 introduzimos a Derivada Fracionária segundo Caputo, e por fim, nas Seções 4 e 5 discutimos a solução do modelo fracionário de resfriamento de Newton.

2 Conceitos preliminares

Apresentamos a seguir alguns conceitos necessários para o desenvolvimento deste trabalho. Mais detalhes sobre tais conceitos, bem como as demonstrações dos resultados, podem ser encontradas em [1] e [2]. Iniciamos apresentando o produto de convolução e a transformada de Laplace, bem como propriedades envolvendo tais conceitos.

Definição 2.1. *Sejam $f(t)$ e $g(t)$ duas funções de ordem exponencial. Definimos o produto de convolução de $f(t)$ e $g(t)$ como $(f * g)(t) = \int_0^t f(t-\tau)g(\tau)d\tau = \int_0^t f(\tau)g(t-\tau)d\tau$.*

Na definição acima usamos o conceito de uma função $f(t)$ ser de ordem exponencial, que consiste em dizer que existem constantes k, a e M tais que $|f(t)| \leq ke^a t$, para todo $t \geq M$.

Definição 2.2. *Seja $f(t)$ uma função definida no intervalo $0 \leq t < \infty$. Definimos a transformada de Laplace de $f(t)$, denotada por $\mathscr{L}[f(t)]$ ou $F(s)$, como a integral $F(s) := \mathscr{L}[f(t)] = \int_0^\infty e^{-st} f(t)dt$, onde s, o parâmetro da transformada, é tal que $s > 0$.*

A transformada de Laplace será utilizada na resolução do problema de valor inicial proposto neste trabalho. Para isto, precisaremos utilizar da propriedade de que $\mathscr{L}[f(t)]$ admite inversa, denotada por $\mathscr{L}^{-1}[F(s)]$, cuja a fórmula geral nós omitimos uma vez que envolve uma integral de função de variável complexa, o qual não se aplica neste trabalho. No entanto, pode ser provado que dada $f(t)$ uma função contínua com a transformada de Laplace $F(s)$, não existe outra função contínua possuindo a mesma transformada $F(s)$.

Abaixo listamos algumas propriedades envolvendo a Transformada de Laplace e o produto de convolução.

- Dadas funções $f(t)$, $g(t)$ cujas $\mathscr{L}\{f(t)\}$ e $\mathscr{L}\{g(t)\}$ existem, então

$$\mathscr{L}\{\alpha f(t) + \beta g(t)\} = \alpha\mathscr{L}\{f(t)\} + \beta\mathscr{L}\{g(t)\}, \quad \forall \alpha,\ \beta \in \mathbb{R}.$$

- Seja f uma função tal que f e f' são contínuas e de ordem exponencial. Então, $\mathscr{L}[f'(t)]$ existe para $s > a$ e é dada por

$$\mathscr{L}[f'(t)] = s\mathscr{L}[f(t)] - f(0). \tag{1}$$

- Sejam $f(t)$ e $g(t)$ duas funções de ordem exponencial, então

$$\mathscr{L}[(f * g)(t)] = \mathscr{L}[f(t)] \cdot \mathscr{L}[g(t)]. \tag{2}$$

2.1 Funções especiais

Nesta seção definimos algumas funções de extrema importância para o estudo do Cálculo Fracionário. Iniciamos com a Função Gama e algumas de suas propriedades.

Definição 2.3. *A função Gama é definida pela integral* $\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}dt, \quad \forall x > 0.$

A Função Gama é dita como uma generalização do conceito de fatorial para números reais em virtude da propriedade $\Gamma(n) = \int_0^\infty e^{-t}t^{n-1}dt = (n-1)!$, que pode ser provada por indução sobre n. Outra importante propriedade envolvendo a Função Gama, que nos permite estender seu domínio para todos os reais não nulos, com excessão dos inteiros negativos, é dada pela equação

$$\Gamma(x+1) = x\Gamma(x). \tag{3}$$

Abaixo introduzimos a Função de Gel'fand-Shilov e calculamos a sua Transformada de Laplace, que utilizaremos nas seções seguintes.

Definição 2.4. *Sejam $n \in \mathbb{N}$ e α um número não inteiro. Definimos a função de Gel'fand-Shilov de ordem n e α, respectivamente, por*

$$\phi_n(t) = \begin{cases} \frac{t^{n-1}}{(n-1)!}, & \textit{se } t \geq 0 \\ 0, & \textit{se } t < 0 \end{cases} \quad e \quad \phi_\alpha(t) = \begin{cases} \frac{t^{\alpha-1}}{\Gamma(\alpha)}, & \textit{se } t \geq 0 \\ 0, & \textit{se } t < 0 \end{cases}.$$

Aplicando a transformada de Laplace na função Gel'fand-Shilov, introduzindo a mudança de variável $a = st$ e utilizando, na última igualdade, a definição da Função Gama, temos

$$\mathscr{L}[\phi_\alpha] = \int_0^\infty e^{-st}\frac{t^{\alpha-1}}{\Gamma(\alpha)}dt = \frac{1}{\Gamma(\alpha)}\frac{1}{s}\int_0^\infty e^{-a}\left(\frac{a}{s}\right)^{\alpha-1}da = \frac{s^{-\alpha}}{\Gamma(\alpha)}\int_0^\infty e^{-a}a^{\alpha-1}da = s^{-\alpha}. \tag{4}$$

Para a resolução da equação diferencial ordinária presente no modelo da Lei de Resfriamento de Newton, utilizaremos a Transformada de Laplace da função $E_\alpha(kt^\alpha)$, onde onde k é uma constante e $E_\alpha(t)$ é a Função de Mittag-Leffler de um parâmetro que definimos a seguir.

Definição 2.5. *Denotada por $E_\alpha(t)$, com $\alpha > 0$ e $t > 0$, definimos a Função de Mittag-Leffler de um*

parâmetro pela seguinte série

$$E_\alpha(t) = \sum_{k=0}^{\infty} \frac{t^k}{\Gamma(\alpha k + 1)}.$$

A função de Mittag-Leffler é considerada uma generalização fracionária da função exponencial, uma vez que $E_1(t) = e^t$.

Calculemos agora a Transformada de Laplace da função $E_\alpha(kt^\alpha)$.

Suponhamos $s > |k|$. Assim, pela definição de Transformada de Laplace e da Função de Mittag-Leffler, segue que

$$\mathscr{L}[E_\alpha(kt^\alpha)] = \int_0^\infty e^{-st} E_\alpha(kt^\alpha)dt = \sum_{i=0}^{\infty} \frac{(k)^i}{\Gamma(\alpha i + 1)} \int_0^\infty e^{-st} t^{\alpha i} dt. \tag{5}$$

Fazendo a mudança de variável $u = st$, e pela definição de Função Gama, temos

$$\int_0^\infty e^{-st} t^{\alpha i} dt = \int_0^\infty e^{-u} \left(\frac{u}{s}\right)^{\alpha i} \frac{du}{s} = \frac{1}{s^{\alpha i+1}} \int_0^\infty e^{-u} u^{\alpha i} du = \frac{1}{s^{\alpha i+1}} \Gamma(\alpha i + 1).$$

Substituindo em (5), obtemos

$$\mathscr{L}[E_\alpha(kt^\alpha)] = \frac{1}{s} \sum_{i=0}^{\infty} \left[\frac{k}{s^\alpha}\right]^i = \frac{1}{s} \frac{1}{1 - \frac{k}{s^\alpha}} = \frac{s^{\alpha-1}}{s^\alpha - k}. \tag{6}$$

3 Cálculo Fracionário

Nesta seção apresentamos a definição da integral fracionária e a derivada fracionária segundo Caputo. Destacamos que neste trabalho consideramos o caso real destas definições, porém tais conceitos podem ser estendidos a ordem complexas (ver [1]).

Denotando por I o operador integral, é possível demonstrar que $I^n f(t) = \int_0^t \frac{(t-\tau)^{n-1}}{(n-1)!} f(\tau)d\tau$, utilizando indução sobre n. Esta propriedade sugere uma forma de definir a integral de ordem não inteira, valendo-se da generalização do fatorial pela função Gama.

Definição 3.1. *Seja $f(t)$ uma função integrável. A integral fracionária de Riemann-Liouville de ordem $\nu > 0$ de $f(t)$ denotada por $I^\nu f(t)$ é definida como sendo:*

$$I^\nu f(t) = \phi_\nu(t) * f(t) = \int_0^t \frac{(t-\tau)^{\nu-1}}{\Gamma(\nu)} f(\tau)d\tau.$$

Definimos também que $I^0 f(t) = f(t)$.

Definição 3.2. *Sejam $\beta > 0$ e $n \in \mathbb{N}$, tal que, $n - 1 < \beta \leq n$. A derivada de Caputo de ordem β de $f(x)$, com $x > 0$, denotada por $D^\beta f(x)$, é definida como*

$$D^\beta f(x) = I^{n-\beta}[D^n f(x)] = \frac{1}{\Gamma(n-\beta)} \int_0^x \frac{f^{(n)}(\tau)}{(x-\tau)^{\beta+1-n}} d\tau.$$

Observemos que se $\beta = n$, então $D^{\beta}[f(x)] = I^{n-\beta}[D^n f(x)] = I^0[D^n f(x)] = D^n f(x)$. Isto é, a derivada usual é um caso particular da derivada fracionária segundo Caputo.

Teorema 3.3. *Sejam $\beta > 0$ e $n \in \mathbb{N}$, tal que, $n-1 < \beta \leq n$. Então $\mathscr{L}[D^{\beta} f(t)] = s^{\beta-n}\mathscr{L}[D^n f(t)]$.*

Demonstração. Pelas Definições 3.1 e 3.2, equações (2) e (4), temos

$$\mathscr{L}[D^{\beta} f(t)] = \mathscr{L}[I^{n-\beta} D^n f(t)] = \mathscr{L}[\phi_{n-\beta}(t) * D^n f(t)] = \mathscr{L}[\phi_{n-\beta}(t)] \cdot \mathscr{L}[D^n f(t)] = s^{\beta-n}\mathscr{L}[D^n f(t)].$$

■

4 Lei de resfriamento de Newton

De acordo com Isaac Newton a variação da temperatura de um corpo no decorrer do tempo é proporcional a diferença de temperatura entre o corpo e o meio no qual ele se encontra. Matematicamente, podemos escrever a Lei do resfriamento de Newton pela seguinte equação diferencial ordinária, $C'(t) = k(C(t) - a)$, sendo $k \in \mathbb{R}$ a constante de proporcionalidade, $C(t)$ a temperatura do objeto no instante $t > 0$ e $a \in \mathbb{R}$ a temperatura do meio. Consideremos a versão fracionária deste modelo dada pela equação

$$D^{\alpha} C(t) = k(C(t) - a), \tag{7}$$

com $0 < \alpha \leq 1$ e condição incial $C(0) = C_0$. Aplicando a Transformada de Laplace, usando a sua linearidade, o Teorema 3.3 e a equação (1), temos

$$\mathscr{L}[D^{\alpha} C(t)] - k\mathscr{L}[C(t)] + ak\mathscr{L}[1] = 0 \Rightarrow s^{\alpha-1}[s\mathscr{L}[C(t)] - C(0)] - k\mathscr{L}[C(t)] + \frac{ak}{s} = 0.$$

Denotando $F(s) = \mathscr{L}[C(t)]$, obtemos $F(s) = \frac{s^{\alpha-1}}{s^{\alpha}-k} C_0 - a\frac{k}{s(s^{\alpha}-k)}$. Observemos que

$$F(s) = \frac{s^{\alpha-1}}{s^{\alpha}-k} C_0 + a\left(\frac{1}{s} - \frac{s^{\alpha-1}}{s^{\alpha}-k}\right) = (C_0 - a)\frac{s^{\alpha-1}}{s^{\alpha}-k} + \frac{a}{s}.$$

Portanto, segue pela equação (6) que a solução da equação diferencial fracionária (7), é

$$C(t) = (C_0 - a)E_{\alpha}(kt^{\alpha}) + a.$$

Na Figura 1, esboçamos alguns gráficos de $C(t)$ para diferentes valores da ordem α.

5 Conclusão

Utiliza-se da modelagem fracionária com o objetivo de aumentar a precisão dos modelos matemáticos e chegar o mais próximo possível da realidade. Ao modelar um problema, no geral adotam-se simplificações da realidade e isso no geral acaba por implicar uma diminuição da taxa de variação

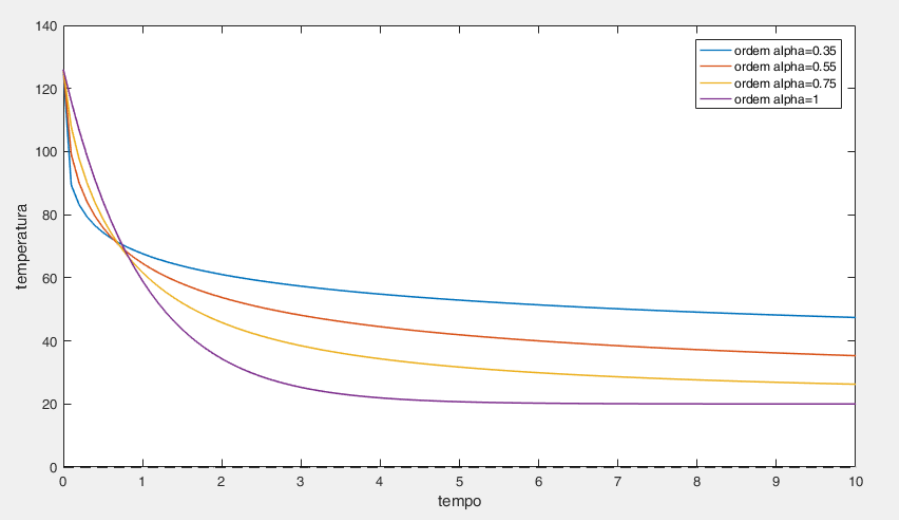


Figura 1: Gráficos da solução da equação 7 para diferentes valores da ordem α.
Fonte: Elaboração própria.

envolvida. Logo, em alguns casos, ao invés de considerar diversos fatores na equação diferencial ordinária, a influência destes pode ser estimada através de alterações na ordem da derivada.

No caso do modelo de resfriamento de Newton, ao substituirmos a ordem 1 da derivada do modelo original pela ordem não inteira $0 < \alpha \leq 1$, obtemos soluções que decrescem mais lentamente que no caso clássico, o que nos sugere um decrescimento na taxa de variação do modelo. O resultado obtido contribui para o estudo do cálculo fracionário, uma vez que não há na literatura significados físicos ou geométricos acerca da derivada fracionária.

Referências

[1] VARALTA, N. **Das transformadas integrais ao cálculo fracionário aplicado à equação logística.** 2014. Dissertação (Mestrado em Biometria) - Instituto de Biociências, Universidade Estadual Paulista Júlio de Mesquita Filho, Botucatu, 2014.

[2] BOYCE, W. E., DIPRIMA, R. C., IORIO, V. M. **Equações Diferenciais Elementares e Problemas de Valores de Contorno**. 10 ed., Rio de Janeiro: LTC, 2015.

Funções Analíticas e as Equações de Cauchy-Riemann

Lorena Bezerra de Almeida
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
lore.lo2310@gmail.com

Elisa Regina dos Santos
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
elisars@ufu.br

Palavras-chave

Funções Complexas.
Funções Contínuas.
Funções Analíticas.
Equações de Cauchy-Riemann.

Resumo

O objetivo principal deste trabalho é apresentar as equações de Cauchy-Riemann e demonstrar um teorema muito importante no estudo das funções analíticas, o qual diz que se as derivadas parciais das partes real e imaginária de uma função f são contínuas numa região R, então a função f é analítica em R se, e somente se, as equações de Cauchy-Riemann são satisfeitas.

1 Introdução

A teoria das funções de uma variável complexa é uma extensão natural das funções de uma variável real. Desde seu surgimento, no final do século XVIII, essa teoria tem se mostrado uma das áreas mais frutíferas da Matemática e de importância fundamental, tanto na matemática pura como nas áreas aplicadas. Em particular, na Análise Complexa, as equações de Cauchy-Riemann, em conjunto com alguns critérios de continuidade, formam uma condição necessária e suficiente para uma função complexa ser analítica.

Tais equações foram vistas pela primeira vez na obra de Jean le Rond d'Alembert, publicada em 1752. Entretanto, foi Leonhard Euler quem percebeu sua relação com as funções analíticas, em 1797. Posteriormente, essas equações foram utilizadas por Cauchy no desenvolvimento de sua teoria das funções, realizado em 1814, que serviu como base para a dissertação de doutorado de Riemann, publicada em 1851.

As referências utilizadas no desenvolvimento deste trabalho foram [1] e [2]

2 Definições e Resultados Preliminares

Apresentaremos, primeiramente, algumas definições preliminares sobre as funções complexas.

Definição 2.1. *Sejam $z_0 \in \mathbb{C}$ e $r > 0$. Chamamos de **disco aberto** de centro z_0 e raio r o conjunto $D_r(z_0)$ que contém todos os números complexos que estão a uma distância menor que r do ponto z_0, ou seja,*

$$D_r(z_0) = \{z : |z - z_0| < r\}.$$

Definição 2.2. *Dizemos que um conjunto C é **aberto** se para cada ponto z_0 de C existe um disco $D_r(z_0)$ contido em C.*

Definição 2.3. *Um **arco** é um conjunto C de pontos dado parametricamente por*

$$C = \{z(t) = x(t) + iy(t) : a \leq t \leq b\},$$

onde $x(t)$ e $y(t)$ são funções reais contínuas de t.

Definição 2.4. *Dizemos que um conjunto é **conexo** se podemos ligar quaisquer dois de seus pontos por um arco todo contido no conjunto.*

Definição 2.5. *Uma **região** é um conjunto aberto e conexo.*

Definição 2.6. *Sejam $z_0 \in \mathbb{C}$ e $C \subset \mathbb{C}$. Dizemos que z_0 é um **ponto de acumulação** de C se*

$$\forall \epsilon > 0, (D_\epsilon(z_0) - \{z_0\}) \cap C \neq \emptyset.$$

Definição 2.7. *Seja z_0 um ponto de acumulação do domínio D de uma função f. Diz-se que f* ***tem limite*** *L com z tendendo a z_0 se dado qualquer $\epsilon > 0$ existe $\delta > 0$ tal que*

$$z \in D,\ 0 < |z - z_0| < \delta \implies |f(z) - L| < \epsilon.$$

Denotamos: $\lim_{z \to z_0} f(x) = L$.

Teorema 2.8. *Seja $f = u + iv$ uma função com domínio D, e seja $L = U + iV$. Então,*

$$\lim_{z \to z_0} f(z) = L$$

se, e somente se

$$\lim_{z \to z_0} u(x, y) = U \ \textbf{\textit{e}} \ \lim_{z \to z_0} v(x, y) = V.$$

Demonstração. Veja [1], Teorema 2.12. ■

Antes de seguirmos, é importante destacar o fato de que as noções de continuidade e derivabilidade no caso complexo são análogas ao caso real.

Definição 2.9. *Diz-se que uma função f é* ***analítica*** *em uma região R se ela é derivável em cada ponto de R; e f é* ***analítica em um ponto*** *z_0 se f é analítica numa região contendo z_0.*

Para finalizar esta seção, vamos recordar um teorema do Cálculo que será útil na próxima seção.

Teorema 2.10 (Teorema do Valor Médio)**.** *Seja $f : [a, b] \to \mathbb{R}$ uma função contínua em $[a, b]$ e derivável em (a, b). Então, existe $c \in (a, b)$ tal que $f'(c) = \dfrac{f(b) - f(a)}{b - a}$.*

Demonstração. Veja [2], p. 291. ■

3 Equações de Cauchy-Riemann

Seja $f = u + iv$ uma função derivável em um ponto $z = x + iy$. Então,

$$f'(z) = \lim_{\Delta z \to 0} \frac{f(z + \Delta z) - f(z)}{\Delta z}$$

independentemente da forma como $\Delta z \to 0$. Em particular, podemos fazer Δz tender a zero por valores reais, $\Delta z = k$ e, separadamente, por valores imaginários, $\Delta z = it$. Assim,

$$\begin{aligned} f'(z) &= \lim_{k \to 0} \frac{[u(x + k, y) - u(x, y)] + i[v(x + k, y) - v(x, y)]}{k}, \\ f'(z) &= \lim_{t \to 0} \frac{[u(x, y + t) - u(x, y)] + i[v(x, y + t) - v(x, y)]}{it}. \end{aligned}$$

De acordo com o Teorema 2.8, a existência desses limites implica a existência, separadamente, dos limites das partes real e imaginária, isto é,

$$\begin{aligned} f'(z) &= \lim_{k\to 0}\frac{u(x+k,y)-u(x,y)}{k} + i\cdot\lim_{k\to 0}\frac{v(x+k,y)-v(x,y)}{k}, \\ f'(z) &= \lim_{t\to 0}\frac{v(x,y+t)-v(x,y)}{t} - i\cdot\lim_{t\to 0}\frac{u(x,y+t)-u(x,y)}{t}. \end{aligned}$$

Consequentemente, as funções u e v possuem derivadas parciais no ponto (x,y) e valem as igualdades:

$$f'(z) = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x} = \frac{\partial v}{\partial y} - i\frac{\partial u}{\partial y}.$$

Disso, obtemos as **equações de Cauchy-Riemann**:

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \text{ e } \frac{\partial v}{\partial x} = -\frac{\partial u}{\partial y}.$$

Tudo isso mostra que as equações de Cauchy-Riemann são condições necessárias para a existência da derivada de uma função f. No entanto, a validade dessas equações não é suficiente para garantir a existência da derivada. Um exemplo disso é dado pela função

$$f(z) = \sqrt{|xy|}, \text{ onde } z = x + iy.$$

Observe que $v = 0$, pois f não tem parte imaginária. Então, $v_x = v_y = 0$. Por outro lado, $u(x,y) = \sqrt{|xy|}$. Logo,

$$u_x(0,0) = \lim_{k\to 0}\frac{u(k,0)-u(0,0)}{k} = 0$$

pois $u(k,0) = u(0,0) = 0$. De forma análoga, $u_y(0,0) = 0$. Assim, as equações de Cauchy-Riemann são satisfeitas no ponto $z = 0$. Entretanto, f não é derivável em $z = 0$. De fato, tomando $\Delta z = r\cdot e^{i\theta} = r\cdot\cos\theta + i\cdot r\cdot \operatorname{sen}\theta$, obtemos

$$\frac{f(\Delta z)-f(0)}{\Delta z} = \frac{\sqrt{|r^2\cdot\cos\theta\cdot\operatorname{sen}\theta|}}{r\cdot e^{i\theta}} = \frac{\sqrt{|\cos\theta\cdot\operatorname{sen}\theta|}}{e^{i\theta}}, \text{ para } r > 0.$$

Logo, como tal expressão depende de θ, o qual varia livremente, temos que $f'(0)$ não existe.

Embora o fato das equações de Cauchy-Riemann serem satisfeitas não garantir que uma função $f = u + iv$ tenha derivada, se a elas adicionarmos a condição de que as derivadas parciais de u e v sejam contínuas numa região, obtemos um teorema muito importante no estudo das funções analíticas.

Teorema 3.1. *Sejam $u(x,y)$ e $v(x,y)$ funções reais com derivadas parciais contínuas numa região R. Então a função $f(z) = u(x,y) + iv(x,y)$ é analítica em R se, e somente se, as equações de Cauchy-Riemann são satisfeitas em R.*

Demonstração. O fato de que as Equações de Cauchy-Riemann são uma condição necessária já foi provado anteriormente, então basta demonstrar que essa é uma condição suficiente. Considere um ponto $z = x + iy \in R$ e um número $\delta > 0$ tal que o disco $D_\delta(z) = \{(x+k)+i(y+t) : k^2+t^2 < \delta^2\}$ esteja todo contido em R, como ilustra a Figura 1. Em particular, os segmentos zz_1 e z_1z_2, onde

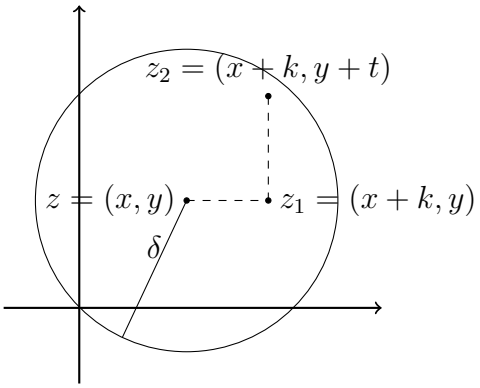


Figura 1: Disco $D_\delta(z)$

$z_1 = (x + k, y)$ e $z_2 = (x + k, y + t)$, estão contidos em R. Logo, pelo Teorema 2.10, existem $\theta_1, \theta_2 \in (0, 1)$ tais que

$$u(x+k,y) - u(x,y) = k \cdot u_x(x + \theta_1 k, y), \tag{1}$$

$$u(x+k,y+t) - u(x+k,y) = t \cdot u_y(x + k, y + \theta_2 t). \tag{2}$$

Somando as equações (1) e (2), temos

$$\Delta u = u(x+k,y+t) - u(x,y) = k \cdot u_x(x + \theta_1 k, y) + t \cdot u_y(x + k, y + \theta_2 t). \tag{3}$$

Como u_x e u_y são contínuas, podemos escrever

$$u_x(x + \theta_1 k, y) = u_x(x, y) + \delta_1, \tag{4}$$

$$u_y(x + k, y + \theta_2 t) = u_y(x, y) + \delta_2, \tag{5}$$

onde δ_1 e δ_2 tendem a zero com $k^2 + t^2 \to 0$. Substiuindo (4) e (5) em (3), obtemos

$$\Delta u = u(x+k,y+t) - u(x,y) = k \cdot u_x(x,y) + t \cdot u_y(x,y) + k\delta_1 + t\delta_2.$$

De modo análogo, deduzimos

$$\Delta v = v(x+k,y+t) - v(x,y) = k \cdot v_x(x,y) + t \cdot v_y(x,y) + k\delta_3 + t\delta_4,$$

onde δ_3 e δ_4 tendem a zero com $k^2 + t^2 \to 0$. Fazendo $\Delta z = h = k + it$ e usando as equações de

Cauchy-Riemann, segue que

$$\begin{aligned} f'(z) &= \lim_{\Delta z \to 0} \frac{f(z+\Delta z) - f(z)}{\Delta z} = \lim_{h \to 0} \frac{\Delta u + i\Delta v}{h} \\ &= \lim_{h \to 0} \frac{(ku_x(x,y) + itv_y(x,y)) + i(kv_x(x,y) - itu_y(x,y))}{h} + \frac{k}{h}(\delta_1 + i\delta_3) + \frac{t}{h}(\delta_2 + i\delta_4) \\ &= \lim_{h \to 0} u_x(x,y) + iv_x(x,y) + \frac{k}{h}(\delta_1 + i\delta_3) + \frac{t}{h}(\delta_2 + i\delta_4) \\ &= u_x(x,y) + iv_x(x,y) \end{aligned}$$

pois $|\frac{k}{h}| \leq 1$, $|\frac{t}{h}| \leq 1$ e δ_1, δ_2, δ_3 e δ_4 tendem a 0 quando $\Delta z \to 0$. Portanto, $f'(z)$ existe e é dada por $u_x + iv_x = v_y - iu_y$. ■

4 Considerações finais

Neste trabalho, vimos que as equações de Cauchy-Riemann e o Teorema 3.1 são muito importantes na Análise Complexa, visto que facilitam a identificação de funções analíticas.

Agradecimentos

Na condição de bolsista do PET Matemática da Universidade Federal de Uberlândia, agradeço ao Programa de Eduação Tutorial da SESu/MEC pelo fomento.

Referências

[1] ÁVILA, G. **Variáveis complexas e aplicações**. 3ª Edição. Rio de Janeiro: LTC, 2008.

[2] STEWART, J. **Cálculo**. Volume I. 5ª Edição. São Paulo: Pioneira Thomson Learning, 2006.

As constantes $D(n)$ e $E(n)$

Edinilson Ferreira Vilela
UFU, FAMAT, Uberlândia, MG, Brasil
edinilsonfvilela@uf.br

Alonso Sepúlveda Castellanos
UFU, FAMAT, Uberlândia, MG, Brasil
alonso.castellanos@ufu.br

Palavras-chave

Teoria Aditiva dos Números.
Constante $D(n)$.
Constante $E(n)$.

Resumo

Neste trabalho apresentamos uma introdução sobre a Teoria Aditiva dos Números, em particular, falamos sobre as constantes $D(n)$ e $E(n)$, que descrevem o comprimento mínimo de uma sequência de inteiros para que exista uma subsequência cuja soma de seus termos seja congruente à zero.

1 Introdução

A Teoria Aditiva dos Números é uma área da Matemática que estuda o comportamento dos números inteiros junto com a operação de adição. Aqui veremos algumas propriedades relacionadas à soma zero de uma sequência de números inteiros. Uma sequência $(a_1, a_2, \ldots, a_k)$ é dita possuir soma zero quando $a_1 + a_2 + \cdots + a_k \equiv 0 \pmod{n}$ para algum n natural.

2 Constantes D(n) e E(n)

Definição 2.1. *Seja G um grupo abeliano finito de ordem n, definimos $D(n)$ como sendo o menor natural t, tal que, qualquer sequência com t elementos contidos em G possui uma subsequência não vazia cuja soma é zero.*

Definição 2.2. *Seja G um grupo abeliano finito de ordem n, definimos $E(n)$ como sendo o menor natural t, tal que, toda sequência com t elementos contidos em G possui uma subsequência de comprimento n cuja soma é zero.*

Exemplo 2.3. *Dado $G = \mathbb{Z}_3$, temos então que $D(3) = 3$. É fácil ver que toda sequência de 3 elementos possui uma subsequência cuja soma é zero, seja (x_1, x_2, x_3) uma sequência de 3 elementos, se pelo menos um de seus elementos for 0 então a subsequência (0) tem soma zero, se por outro lado a sequência não possuir nenhum elemento 0 então ela é formada por apenas 1 ou 2, se ela for da forma $(1, 1, 1)$ então a subsequência $(1, 1, 1)$ tem soma zero, analogamente, se $(2, 2, 2)$, então $(2, 2, 2)$ tem soma zero, se a sequência for formada por 1 e 2, então a subsequência $(1, 2)$ forma soma zero, logo qualquer sequência de 3 elementos possui uma subsequência cuja soma é zero. Além disso, nem toda sequência de 2 elementos possui soma zero, em particular $(1, 1)$ não possui nenhuma subsequência cuja soma é zero. Portanto 3 é o menor comprimento possível para que toda sequência possua uma subsequência de soma zero, ou seja, $D(3) = 3$.*

Exemplo 2.4. *Dado $G = \mathbb{Z}_3$, temos então que $E(3) = 5$. Dada uma sequência de 5 elementos, se 0, 1 e 2 são elementos dessa sequência, então a subsequência $(0, 1, 2)$ tem soma zero, do contrário, se a sequência não possui 0 ou 1 ou 2, então ela terá um de seus elementos repetidos pelo menos 3 vezes, logo ela possui uma subsequência de 3 elementos cuja soma é zero, assim qualquer sequência de 5 elementos possui uma subsequência de 3 elementos cuja soma é zero. Por outro lado, a sequência $(0, 0, 1, 1)$ de 4 elementos não possui nenhuma subsequência de 3 elementos cuja soma é zero. Assim, 5 é o menor comprimento possível tal que toda subsequência de 3 elementos possua soma zero.*

A diferença entre $D(n)$ e $E(n)$ é simplesmente que, quando falamos de $D(n)$ as subsequências podem ter qualquer comprimento, já quando falamos de $E(n)$, as subsequências devem ter comprimento fixo n.

Teorema 2.5. *Dada uma sequência de inteiros com comprimento n, existe uma subsequência que é soma zero. Isto é $D(n) = n$*

Demonstração. Dada uma sequência de números inteiros $(a_1, \ldots, a_n)$ de comprimento n, se $a_j = 0$ para alguma $j = 1, \ldots, n$, então a subsequência (0) é soma zero. Suponhamos que $a_j \neq 0$ para todo $j = 1, \ldots, n$. Seja $s_j = \sum_{i=1}^{j} a_j$, se todos os s_j são distintos, obtemos n elementos distintos, logo existe algum $j = 1, \ldots, n$ tal que $s_j = 0$. Se $s_i = s_j$ para algum i, j, com $i < j$, então a subsequência $(a_{i+1}, \ldots, a_j)$ é soma zero. Logo $D(n) \leq n$, mostremos agora que $D(n) \geq n$. Dado uma sequência de inteiros de comprimento $n - 1$ da forma $(1, 1, \ldots, 1)$, essa sequência não possui subsequência soma zero. Logo $D(n) \geq n$. ■

Exemplo 2.6. *Tomemos a sequência* $(1, 3, 5, 7, 9, 11, 13)$ *de comprimento* 7*, o teorema garante que existe uma subsequência cuja soma seja congruente à zero módulo* 7*. De fato, tomemos a subsequência* $(1, 5, 9, 13)$*, temos que* $1 + 5 + 9 + 13 \equiv 0 \pmod 7$

Teorema 2.7 (Chevalley-Warning)**.** *Seja* p *um número primo e* $\mathbb{F}_q$ *um corpo finito com* $q = p^t$ *elementos, onde* $t \in \mathbb{N}$*. Para* $i = 1, 2, \ldots, m$ *seja* $f_i(x_1, x_2, \ldots, x_n)$ *um polinômio de grau* d_i *em* n *variáveis com coeficientes em* $\mathbb{F}_q$*. Denotamos por* N *o número de n-uplas* $(x_1, x_2, \ldots, x_n)$ *de elementos de* $\mathbb{F}_q^n$ *tais que* $f_i(x_1, x_2, \ldots, x_n) = 0$*, para todo* $i = 1, 2, \ldots, m$*. Se* $\sum_{i=1}^{m} d_i = d_1 + d_2 + \cdots + d_m < n$*, então,* $N \equiv 0 \pmod p$

A demonstração do teorema pode ser encontrada em [2, Teorema 1.2].

Exemplo 2.8. *Sejam* $f_1(x, y, z) = 2x + y + z$ *e* $f_2(x, y, z) = x + 3y + z$ *definidos em* $\mathbb{F}_5$*, o grau de ambos os polinômios é* 1*, portanto a soma é* $1 + 1 = 2 < 3$*, logo, pelo Teorema de Chevalley-Warning, o número de soluções é um múltiplo de* 5*. De fato as soluções simultâneas para os dois polinômios são cinco:* $(0, 0, 0), (1, 3, 0), (2, 1, 0), (3, 4, 0)$ *e* $(4, 2, 0)$.

Teorema 2.9 (Erdös-Ginzburg-Ziv)**.** *Dada uma sequência de números inteiros com* $2n - 1$ *elementos, onde* n *é um número natural, então existe uma subsequência de comprimento* n *cuja soma de seus elementos é um múltiplo de* n*. Isto é,* $E(n) = 2n - 1$

Demonstração. Para provarmos o teorema, devemos mostrar primeiro que o teorema é válido para o caso onde o n é um número primo. E depois mostramos que se o teorema vale para dois naturais m e n, então ele vale para mn. Mostremos primeiro para o caso em que n é um primo p.

Dada uma sequência $(a_1, a_2, \ldots, a_{2p-1})$ de números inteiros, tomemos a sequência $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{2p-1}})$ em $\mathbb{F}_p$ como sendo a redução módulo p da primeira sequência, ou seja, $\overline{a_i} \equiv a_i \pmod p$ para todo $i = 1, 2, \ldots, 2p - 1$. Consideremos os polinômios $f_1, f_2 \in \mathbb{F}_q[x_1, x_2, \ldots, x_{2p-1}]$ definidos por

$$f_1(x_1, \ldots, x_{2p-1}) = x_1^{p-1} + x_2^{p-1} + \cdots + x_{2p-1}^{p-1} = \sum_{j=1}^{2p-1} x_j^{p-1}$$

$$f_2(x_1, \ldots, x_{2p-1}) = \overline{a_1} x_1^{p-1} + \overline{a_2} x_2^{p-1} + \cdots + \overline{a_{2p-1}} x_{2p-1}^{p-1} = \sum_{j-1}^{2p-1} \overline{a_j} x_j^{p-1}$$

Ambos os polinômios possuem grau $p-1$. Denotemos por N o número de soluções simultâneas desses polinômios. Como a soma dos graus dos polinômios f_1 e f_2 é $(p-1)+(p-1) = 2p-2 < 2p-1$, então pelo Teorema de Chevalley-Warning temos que o número de soluções $N \equiv 0 \pmod{p}$.

Portanto o número de soluções simultâneas de f_1 e f_2 é um múltiplo de p, e como (0, 0, ..., 0) é um solução, temos que o $N > 1$ e assim $N \geq p \geq 2$. Portanto, os polinômios f_1 e f_2 têm uma solução não trivial, ou seja, existem $t_1, t_2, \ldots, t_{2p-1} \in \mathbb{Z}_p$ não todos nulos tais que $(t_1, t_2, \ldots, t_{2p-1})$ seja solução simultânea de f_1 e f_2, ou seja,

$$f_1(t_1, \ldots, t_{2p-1}) = t_1^{p-1} + t_2^{p-1} + \cdots + t_{2p-1}^{p-1} = \sum_{j=1}^{2p-1} t_j^{p-1} = \overline{0} \tag{1}$$

$$f_2(t_1, \ldots, t_{2p-1}) = \overline{a_1} t_1^{p-1} + \overline{a_2} t_2^{p-1} + \cdots + \overline{a_{2p-1}} t_{2p-1}^{p-1} = \sum_{j-1}^{2p-1} \overline{a_j} t_j^{p-1} = \overline{0} \tag{2}$$

Como $t^{p-1} = \overline{1}$ para todo $t \neq \overline{0}$, segue pela Equação 1 que existem exatamente p elementos $t_{j_1}, t_{j_2}, \ldots, t_{j_p}$ distintos de zero. Logo, pela Equação 2 temos que $\overline{a_{j_1}} + \overline{a_{j_2}} + \cdots + \overline{a_{j_p}} = \overline{0}$, ou seja $a_{j_1} + a_{j_2} + \cdots + a_{j_p} \equiv 0 \pmod{p}$.

Portanto, dada uma sequência $(a_1, a_2, \ldots, a_{2p-1})$ de números inteiros, existe uma subsequência $(a_{j_1}, a_{j_2}, \ldots, a_{j_p})$ de comprimento p tal que a soma dos elementos dessa subsequência é um múltiplo de p.

Agora vamos generalizar o caso para uma sequência de comprimento n não necessariamente prima. Devemos mostrar agora que se o teorema vale para duas sequências de comprimento m e n, onde m e n são números naturais, então ela vale para mn.

Por hipótese temos que, para cada subconjunto A de $\{x_1, x_2, \ldots, x_{2mn-1}\}$ com $2mn-1$ elementos, onde $x_1, x_2, \ldots, x_{2mn-1} \in \mathbb{Z}$, existe um subconjunto $B \subset A$ com n elementos tal que a soma de seus elementos seja um múltiplo de n.

Construiremos um conjunto B_j para todo $1 \leq j \leq 2m-1$ da seguinte forma: Escolhemos um subconjunto $A_j \subset \{x_1, x_2, \ldots, x_{2mn-1}\} \setminus \bigcup_{1 \leq k < j} B_k$ com $2n-1$ elementos, e um subconjunto $B_j \subset A_j$ com n elementos tal que a soma de seus elementos sejam um múltiplo de n. Ou seja,

$$\begin{aligned}
&A_1 \subset \{x_1, x_2, \ldots, x_{2mn-1}\}, && B_1 \subset A_1 \text{ e } \sum_{x \in B_1} x \equiv 0 \pmod{n} \\
&A_2 \subset \{x_1, x_2, \ldots, x_{2mn-1}\} \setminus B_1, && B_2 \subset A_1 \text{ e } \sum_{x \in B_2} x \equiv 0 \pmod{n} \\
&A_3 \subset \{x_1, x_2, \ldots, x_{2mn-1}\} \setminus B_1 \cup B_2, && B_3 \subset A_1 \text{ e } \sum_{x \in B_3} x \equiv 0 \pmod{n} \\
&\vdots && \vdots \\
&A_{2m-1} \subset \{x_1, x_2, \ldots, x_{2mn-1}\} \setminus \bigcup_{k=1}^{2m-2} B_k, && B_{2m-1} \subset A_{2m-1} \text{ e } \sum_{x \in B_{2m-1}} x \equiv 0 \pmod{n}
\end{aligned}$$

Observe que para $j \leq 2m-1$, temos que o número de elementos é

$$\left|\{x_1, x_2, \ldots, x_{2mn-1}\} \setminus \bigcup_{1\leq k<j} B_k\right| = 2mn - 1 - (j-1)n$$
$$\geq 2mn - 1 - (2m-2)n$$
$$= 2n - 1$$

O que garante a construção do B_j até $j = 2m-1$. Definamos agora os inteiros $y_j = \frac{1}{n}\sum_{x\in B_j} x$ para $1 \leq j \leq 2m-1$. Novamente, por hipótese, existe um subconjunto $C \subset \{x_1, x_2, \ldots, x_{2m-1}\}$ com m elementos tal que $\sum_{y_j\in C} y_j \equiv 0 \pmod{m}$ e assim,

$$\sum_{y_j\in C} y_j = \sum_{y_j\in C}\left(\frac{1}{n}\sum_{x\in B_j} x\right) = \frac{1}{n}\sum_{y_j\in C}\sum_{x\in B_j} x \Rightarrow \sum_{y_j\in C}\sum_{x\in B_j} x = n\sum_{y\in C} y_j$$

é uma soma de $|C||B_j| = mn$ inteiros, que é múltiplo de mn.

Logo o teorema vale para qualquer comprimento n natural. ■

Exemplo 2.10. *Tomemos a sequência* $(1, 1, 2, 3, 5, 8, 13, 21, 34)$*, esta é uma sequência de comprimento* 9*, o teorema garante a existência de uma subsequência de comprimento* 5*, tal que a soma dos seus elementos sejam um múltiplo de 5. De fato tomando a subsequência* $(1, 2, 5, 13, 34)$*, como* $1 + 2 + 5 + 13 + 34 = 55$*, então* $1 + 2 + 5 + 13 + 34 \equiv 0 \pmod{5}$.

Vale observar que o Teorema de Erdös-Ginzburg-Ziv garante o caso de menor comprimento possível, isso é, para sequências de comprimento menor do que $2n-1$ nem sempre existe uma subsequência de comprimento n cuja soma resulta em um múltiplo de n. Tomemos como Exemplo o seguinte caso:

Uma sequência $(\overbrace{0, \ldots, 0}^{n-1}, \overbrace{1, \ldots, 1}^{n-1})$ de comprimento $2n-2$, essa sequência não possui nenhuma subsequência de comprimento n cuja soma dos seus termos é um múltiplo de n.

3 Considerações finais

Apresentamos aqui a definição das constantes $D(n)$ e $E(n)$ e também vimos quais são seus valores para sequências de inteiros. Essas constantes podem ser generalizadas para casos mais gerais onde se atribui pesos às somas, isto é, cada termo da soma pode possuir um peso pelo qual é multiplicado.

Agradecimentos

Agradecimento ao CNPq pelo fomento da Bolsa de Iniciação Científica do PICME.

Referências

[1] M. B. NATHANSON. **Additive Number Theory: Inverse Problems and the Geometry of Sumsets.** 1ª Edição. New York: Springer.

[2] F. A. D. OLIVEIRA. **Teorema de Erdös-Ginzuburg-Ziv**. Dissertação de mestrado. Universidade Federal de Viçosa, 2014.

[3] W. Adriana. **Representação Aditivas em Grupos Abelianos Finitos**. Dissertação de mestrado. Universidade Estadual de Maringá, 2008.

Equação de Pell

Rodrigo Carneiro

UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
r-carneiro@ufu.br

Victor Gonzalo Lopez Neumann

UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
victor.neumann@ufu.br

Palavras-chave

Equação de Pell.
Solução fundamental.
Fração contínua.

Resumo

O objetivo deste trabalho é estudar as equações de Pell e as propriedades das suas soluções. Além disso, utilizamos frações contínuas para determinar o conjunto de soluções da equação de Pell.

1 Introdução

Equações diofantinas são equações polinomiais de duas ou mais variáveis para as quais procuram-se soluções inteiras ou racionais. Neste trabalho, estudaremos especificamente alguns resultados das equações $x^2 - dy^2 = 1$, as quais recebem o nome de equação de Pell em homenagem ao matemático inglês John Pell. Dado um inteiro positivo d, procuraremos as soluções inteiras (x, y) dessa equação.

Observação 1.1. *Note que se d é um quadrado perfeito, ou seja, $d = k^2$, temos que $x^2 - dy^2 = (x - ky)(x + ky) = 1$. Nesse caso, $(x - ky) = (x + ky) = \pm 1$ e, portanto, as únicas soluções são $x = \pm 1$ e $y = 0$.*

2 Equação de Pell

Definição 2.1. *Sejam d um número inteiro positivo e x, y números inteiros. Define-se a norma de $u = x + y\sqrt{d}$ da seguinte forma:*

$$N(u) = u\overline{u},$$

onde $\overline{u} = x - y\sqrt{d}$. Assim, $N(u) = x^2 - dy^2$.

Teorema 2.2. *Seja $d \in \mathbb{Q}$ tal que $\sqrt{d}$ é irracional. Então, existem infinitos inteiros p,q com $q > 0$, tais que p/q é irredutível e $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$.*

Demonstração. Ver [2, Theorem 13.6]. ■

Teorema 2.3. *A equação $x^2 - dy^2 = 1$, com d um inteiro positivo não quadrado, possui solução não trivial em inteiros positivos, isto é, com $x + y\sqrt{d} > 1$.*

Demonstração. Pelo Teorema 2.2, a desigualdade $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$ tem infinitas soluções racionais p/q. Note que, se $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$, então

$$\left|p^2 - dq^2\right| = q^2 \left|\sqrt{d} - \frac{p}{q}\right| \left|\sqrt{d} + \frac{p}{q}\right| < \left|\sqrt{d} + \frac{p}{q}\right| \leq 2\sqrt{d} + \left|\sqrt{d} - \frac{p}{q}\right| \leq 2\sqrt{d} + 1.$$

Considerando infinitos pares de inteiros positivos (p_n, q_n) com $\left|\sqrt{d} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$, teremos sempre $|p_n^2 - dq_n^2| < 2\sqrt{d} + 1$, portanto temos um número finito de possibilidades para $p_n^2 - dq_n^2$. Consequentemente, existe um inteiro $k \neq 0$ tal que $p_n^2 - dq_n^2 = k$ para infinitos valores de n. Ordenando esses pares, construímos duas sequências crescentes de pares de inteiros positivos (u_r, v_r) tais que $u_r^2 - dv_r^2 = k$, para todo $r \in \mathbb{N}$. Como há apenas k^2 possibilidades para esses pares módulo k, existem infinitos pares (u_r, v_r) tais que $u_r \equiv a \pmod{k}$ e $v_r \equiv b \pmod{k}$. Sejam $r < s$ índices satisfazendo

as propriedades supracitadas. Então,

$$\frac{u_s+v_s\sqrt{d}}{u_r+v_r\sqrt{d}}=\frac{(u_s+v_s\sqrt{d})(u_r-v_r\sqrt{d})}{u_r^2-dv_r^2}=\frac{u_su_r-dv_sv_r}{k}+\left(\frac{u_rv_s-u_sv_r}{k}\right)\sqrt{d}.$$

Temos, $u_su_r-dv_sv_r\equiv u_r^2-dv_r^2=k\equiv 0 \pmod{k}$ e $u_rv_s-u_sv_r\equiv ab-ab=0 \pmod{k}$ e, portanto, $x=\dfrac{u_su_r-dv_sv_r}{k}$ e $y=\dfrac{u_rv_s-u_sv_r}{k}$ são inteiros. Por outro lado, como $(x+y\sqrt{d})(u_r+v_r\sqrt{d})=u_s+v_s\sqrt{d}$, temos $N(x+y\sqrt{d})N(u_r+v_r\sqrt{d})=N(u_s+v_s\sqrt{d})$. De $N(u_r+v_r\sqrt{d})=N(u_s+v_s\sqrt{d})=k$, segue que $N(x+y\sqrt{d})=x^2-dy^2=1$. Além disso, como $r<s$, temos $u_r+v_r\sqrt{d}<u_s+v_s\sqrt{d}$ e $x+y\sqrt{d}=\dfrac{u_s+v_s\sqrt{d}}{u_r+v_r\sqrt{d}}>1$. ■

3 Soluções da equação de Pell

Demonstramos, anteriormente, que a equação de Pell $x^2-dy^2=1$, com d um inteiro não quadrado, possui pelo menos uma solução (x,y) satisfazendo $x+y\sqrt{d}>1$. Na proposição subsequente provaremos que, a partir de uma solução dada, podemos encontrar infinitas soluções.

Proposição 3.1. *Seja $x^2-dy^2=1$ uma equação de Pell e (x_1,y_1) uma solução em inteiros tal que $x_1+y_1\sqrt{d}>1$. Então, para todo inteiro positivo n, existem inteiros x_n,y_n tais que $u^n=x_n+y_n\sqrt{d}$ e o par (x_n,y_n) é, igualmente, uma solução da equação de Pell.*

Demonstração. Seja $u=x_1+y_1\sqrt{d}$, onde (x_1,y_1) é uma solução da equação de Pell. Veja que para todo $n\geq 1$, existem inteiros (x_n,y_n) tais que $u^n=x_n+y_n\sqrt{d}$, pois

$$(x_1+y_1\sqrt{d})^n=\sum_{j=0}^{n}\binom{n}{j}x_1^{n-j}(y_1\sqrt{d})^j=\sum_{j\text{ par}}\binom{n}{j}x_1^{n-j}y_1^jd^{j/2}+\sqrt{d}\sum_{j\text{ ímpar}}\binom{n}{j}x_1^{n-j}y_1^jd^{(j-1)/2}.$$

Perceba, também, que $N(u^n)=u^n\cdot\overline{u^n}=(u\cdot\overline{u})^n=N(u)^n=1$. Dessa forma, o par (x_n,y_n) é uma solução da equação de Pell. Além disso, como $u>1$, temos $u<u^2<u^3<\cdots$. Isso implica que obtemos uma solução diferente para cada potência de u. ■

Veja que se $u=x_1+y_1\sqrt{d}$ e $N(u)=1$, então (x_1,y_1) é uma solução da equação de Pell $x^2-dy^2=1$. Por abuso de notação, diremos que u é uma solução da equação de Pell.

Definição 3.2. *Sendo $u=x_1+y_1\sqrt{d}>1$ uma solução da equação de Pell, essa solução será chamada de solução mínima ou fundamental se $x_1>1$, $y_1>0$ e não existe solução positiva $1<x_2+y_2\sqrt{d}<x_1+y_1\sqrt{d}$.*

Teorema 3.3. *Se $x_1+y_1\sqrt{d}>1$ é a solução fundamental da equação de Pell $x^2-dy^2=1$, então toda solução em inteiros positivos é da forma $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$, para algum inteiro positivo n.*

Demonstração. Ver [1, Capítulo 4, páginas 169-170]. ■

4 Frações contínuas e solução fundamental

Definição 4.1. *Uma fração contínua é uma expressão da forma:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

onde $a_0, a_1, a_2, \dots$ são todos valores inteiros. Essa expressão é representada por $[a_0, a_1, a_2, a_3, \dots]$.

Uma fração contínua $[a_0, a_1, a_2, a_3, \dots]$ é chamada de fração contínua periódica se existem inteiros $k \geq -1$ e $m \geq 1$ tais que, para todo inteiro positivo n, tem-se $a_{k+n} = a_{k+n+m}$. Assim, uma fração contínua periódica é da forma $[a_0, a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_{k+m}, a_{k+1} \dots, a_{k+m}, \dots]$, a qual é representada por $[a_0, a_1, a_2, \dots, a_k, \overline{a_{k+1}, a_{k+2}, \dots, a_{k+m}}]$.

Dizemos, também, que a fração contínua é puramente periódica se $k = -1$, ou seja, se sua fração contínua é da forma $[\overline{a_0, a_1, a_2, \dots, a_{m-1}}]$.

Definição 4.2. *Dado $x = \dfrac{a + b\sqrt{d}}{c}$, onde a, b, c são inteiros e $\sqrt{d}$ é um irracional (x é um número irracional quadrático), dizemos que x é reduzido se*

$$x > 1 \quad \textit{e} \quad -1 < \overline{x} < 0.$$

Proposição 4.3. *Seja $x \in \mathbb{R}$. Existe um inteiro a_0 e inteiros positivos $a_1, a_2, \dots$ tais que*

$$x = [a_0, a_1, a_2, \dots].$$

Demonstração. Ver [1, Capítulo 3, páginas 108-111]. ■

Observe que quando escrevemos $x = [a_0, a_1, a_2, \dots]$ estamos, na realidade, querendo dizer que

$$x = \lim_{n \to \infty} [a_0, a_1, \dots, a_n].$$

Teorema 4.4. *A fração contínua de um número real x é puramente periódica se, e somente se, x é um número irracional quadrático reduzido.*

Demonstração. Ver [2, Theorem 13.11]. ■

Proposição 4.5. *Sejam $a_0, a_1, \dots$ números reais positivos. Para todo $k \geq 0$, definem-se*

$$p_k = a_k p_{k-1} + p_{k-2} \qquad \textit{e} \qquad q_k = a_k q_{k-1} + q_{k-2},$$

com $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$ e $q_{-1} = 0$. Então, $\dfrac{p_n}{q_n} = [a_0, a_1, a_2, \dots, a_n]$.

Demonstração. Ver [2, Proposition 13.1] ■

Usamos a proposição anterior para aproximar $\sqrt{d}$ de modo prático e rápido usando frações contínuas. Veremos como utilizar esse resultado para obter a solução fundamental da equação de Pell.

Lema 4.6. *Seja x um irracional quadrático e $x = [a_0, a_1, a_2, \dots]$ sua fração contínua. Para todo número não negativo, define-se x_n como o número real que satisfaz $x = [a_0, a_1, \dots, a_{n-1}, x_n]$. Dado $n \geq 0$, se x_n é reduzido, então x_{n+1} é reduzido.*

Demonstração. Ver [2, Lemma 13.12] ■

Lema 4.7. *Sejam d um inteiro positivo não quadrado e $x_k = \dfrac{A_k + \sqrt{d}}{B_k}$, onde A_k e B_k são inteiros tais que $B_k \mid d - A_k^2$. Dado um inteiro a_k definem-se $A_{k+1} = a_k B_k - A_k$ e $B_{k+1} = \dfrac{d - A_{k+1}^2}{B_k}$. Então A_{k+1} e B_{k+1} são inteiros, $B_{k+1} \mid d - A_{k+1}^2$ e $\dfrac{1}{x_k - a_k} = \dfrac{A_{k+1} + \sqrt{d}}{B_{k+1}}$.*

Demonstração. Ver [2, Lemma 13.14]. ■

Lema 4.8. *Sejam d um inteiro positivo não quadrado e $x = \dfrac{A + \sqrt{d}}{B}$ onde A, B são inteiros. Se x é reduzido, então $B > 0$ e $A^2 < d$.*

Demonstração. Ver [2, Lemma 13.15]. ■

Lema 4.9. *Sejam $\sqrt{d} = [a_0, a_1, \dots, a_k, x_{k+1}]$ e $x_{k+1} = \dfrac{A_{k+1} + \sqrt{d}}{B_{k+1}}$. Então, $p_k^2 - dq_k^2 = (-1)^{k-1} B_{k+1}$.*

Demonstração. Ver [2, Lemma 13.17]. ■

Teorema 4.10. *Seja d um inteiro positivo não quadado. A fração contínua de $\sqrt{d}$ é da forma*

$$[a_0, \overline{a_1, a_2, \dots, a_{n_1}, a_n}],$$

onde $a_n = 2a_0$ e $a_k \leq a_0$, para $1 \leq k < n$. Se $m \geq 1, x = p_{mn-1}$ e $y = q_{mn-1}$, então $x^2 - dy^2 = \pm 1$.

Demonstração. O cálculo da fração contínua se inicia com

$$\sqrt{d} = a_0 + (\sqrt{d} - a_0) = a_0 + \frac{1}{x_1} = [a_0, x_1].$$

Desde que $0 < \sqrt{d} - a_0 < 1$, $x_1 = 1/(\sqrt{d} - a_0) > 1$. Como $-\sqrt{d} - a_0 < -1$, então

$$-1 < \overline{x_1} = 1/(-\sqrt{d} - a_0) < 0.$$

Isso significa que x_1 é reduzido e a expansão de sua fração contínua é puramente periódica. Portanto, $\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_n}]$, para alguns inteiros positivos $a_0, a_1, \dots, a_n$. Tomando $z = a_0 + \sqrt{d}$, obtemos

$$z = 2a_0 + (\sqrt{d} - a_0) = 2a_0 + \frac{1}{x_1} = [2a_0, \overline{a_1, a_2, \dots, a_n}].$$

Mas, como $z > 1$ e $-1 < \overline{z} = -\sqrt{d} + a_0 < 0$, z é reduzido e a expansão de sua fração contínua também é puramente periódica, então $a_n = 2a_0$ e $x_n = a_0 + \sqrt{d}$. Como $x = (0 + \sqrt{d})/1$ satisfaz as condições do Lema 4.7, com $A_0 = 0$ e $B_0 = 1$, concluimos que, A_j e B_j são inteiros para todo $j \geq 1$. Desde que x_1 é reduzido, pelo Lema 4.6, x_j é reduzido para todo $j \geq 1$. Por conseguinte, pelo Lema 4.8, $A_{k+1}^2 < d$ para todo $k \geq 0$. Como $|A_{k+1}|$ é um inteiro menor que $\sqrt{d}$ então $|A_{k+1}| \leq a_0 = \lfloor \sqrt{d} \rfloor$. Logo,

$$B_{k+1}a_{k+1} < B_{k+1}x_{k+1} = A_{k+1} + \sqrt{d} \leq a_0 + \sqrt{d}.$$

Como $B_{k+1}a_{k+1}$ é um inteiro, $B_{k+1}a_{k+1} \leq a_0 + a_0 = 2a_0$, então $a_{k+1} \leq 2a_0/B_{k+1}$. Se $B_{k+1} \geq 2$, temos que $a_{k+1} \leq a_0$. Quando $B_{k+1} = 1$ (por exemplo, $k + 1 = n$), então, pelo Lema 4.9, $p_k^2 - dq_k^2 = (-1)^{k-1}B_{k+1} = \pm 1$ e $x_{k+1} = A_{k+1} + \sqrt{d}$. Como x_{k+1} é reduzido, $-1 < A_{k+1} - \sqrt{d} < 0$, ou seja, $\sqrt{d} - 1 < A_{k+1} < \sqrt{d}$, então $A_{k+1} = \lfloor \sqrt{d} \rfloor = a_0$. Dessa forma, temos que $x_{k+1} = a_0 + \sqrt{d}$ e

$$a_{k+1} = \lfloor x \rfloor = \lfloor a_0 + \sqrt{d} \rfloor = 2a_0.$$

Finalmente, temos que a fração contínua para $\sqrt{d}$ se repete em x_{k+2}. Prova-se, portanto, que $a_{k+1} \leq a_0$ quando $B_{k+1} > 1$, $a_{k+1} = 2a_0$ e a fração contínua começa a se repetir quando $B_{k+1} = 1$. Além disso, quando $B_{k+1} = 1$, temos que $p_k^2 - dq_k^2 = \pm 1$. ■

5 Conclusões Finais

Vimos que, dada uma equação de Pell, suas soluções serão boas aproximações racionais de um irracional $\sqrt{d}$. Além disso, utilizando o método das frações contínuas, encontraremos a solução fundamental da equação e, consequentemente, obteremos todas as demais soluções.

Agradecimentos

Os autores agradecem o apoio financeiro da FAPEMIG, edital 07/2022 PIBIC (primeiro autor) e bolsa APQ-00470-22 (segundo autor).

Referências

[1] MARTINEZ, F. B. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. Rio de Janeiro: IMPA, 2010

[2] KRAFT, J. S.; WASHINGTON, L. C. **An Introduction to Number Theory with Cryptography**. 1ª Edição. Nova Iorque: Chapman and Hall/CRC, 2013.

O Teorema dos Zeros de Hilbert

Victor Cruz Borges
UFU, FAMAT, Uberlândia, Minas Gerais, Brasil
victor.cruz@ufu.br

Victor Gonzalo Lopez Neumann
UFU, FAMAT, Uberlândia, Minas Gerais, Brasil
victor.neumann@ufu.br

Palavras-chave

Ideais.
Variedades.
Zeros de Hilbert.

Resumo

O objetivo deste trabalho é trazer uma relação entre alguns tipos de variedades afins de um ideal sobre um anel de polinômios em n variáveis sobre um corpo $\mathbb{K}$. Para isso, serão trazidos alguns conteúdos iniciais referentes a propriedades básicas das variedades de ideais e de ideais de variedades. Além disso, o critério para dizer se um sistema de equações polinomiais (cujos polinômios têm n variáveis e coeficientes em $\mathbb{K}$) é solúvel ou não será explicitado a partir do Teorema Fraco dos Zeros de Hilbert, presente nesse trabalho junto com o Teorema dos Zeros de Hilbert, que nos permitirá inferir algumas sentenças sobre ideais diferentes representarem a mesma variedade quando seus coeficientes estão num corpo algebricamente fechado.

1 Introdução

Ao se estudar álgebra, aparece o conceito de ideal de anéis de polinômios em n variáveis sobre um corpo $\mathbb{K}$. Nesse sentido, dado um ideal, pode-se questionar se os polinômios desse ideal têm raíz(es) em comum. O conjunto formado por esse(s) ponto(s) será chamado de variedade afim do ideal. Existe uma correspondência entre variedades afins e ideais, mas o foco deste trabalho será outro.

2 Conceitos Iniciais

Ao longo deste trabalho $\mathbb{K}$ denotará um corpo e n um inteiro positivo.

Definição 2.1. *Define-se o espaço afim de dimensão n sobre $\mathbb{K}$ o conjunto*

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathbb{K}\}.$$

Definição 2.2. *Sejam $f_1, \ldots, f_s$ polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Define-se o conjunto*

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f_i(a_1, \ldots, a_n)\}$$

como a variedade afim definida por $f_1, \ldots, f_s$.

Como exemplo, no plano $\mathbb{R}^2$ a variedade $V(x^2 + y^2 - 1)$ é a circunferência de raio 1 centrada na origem.

Lema 2.3. *Se $V, W \subset \mathbb{K}^n$ são variedades afins, então $V \cup W$ e $V \cap W$ também são.*

Demonstração. Ver [2, Proposition 1.2.2]. ■

Definição 2.4. *Seja $V \subset \mathbb{K}^n$ uma variedade afim. Define-se*

$$I(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0,\ \forall\ (a_1, \ldots, a_n) \in V\}.$$

A observação crucial é que $I(V)$ é um ideal.

Lema 2.5. *Se $V \subset \mathbb{K}^n$ é uma variedade afim, então $I(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ é um ideal. Chamaremos $I(V)$ por ideal de V.*

Demonstração. Ver [2, Proposition 1.4.6]. ■

Lema 2.6. *Se $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, então $\langle f_1, \ldots, f_s \rangle \subset I(V(f_1, \ldots, f_s))$.*

Demonstração. Ver [2, Proposition 1.4.7]. ■

Mas, ainda vale questionar: Dados $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, qual a relação entre $\langle f_1, \ldots, f_s \rangle$ e $I(V(f_1, \ldots, f_s))$?

3 O Teorema dos Zeros de Hilbert

Anteriormente, vimos que uma variedade $V \subset \mathbb{K}^n$ pode ser estudada ao passar para o ideal $I(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0,\ \forall\ (a_1, \ldots, a_n) \in V\}$ de todos os polinômios que se anulam em V.

Por outro lado, dado um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, podemos definir o conjunto $V(I) = \{x \in \mathbb{K}^n : f(x) = 0, \text{ para todo } f \in I\}$. O Teorema da Base de Hilbert [2, Theorem 2.5.4] nos assegura que $V(I)$ é uma variedade afim, pois de acordo com esse teorema, existe um conjunto finito de polinômios $f_1, \ldots, f_s \in I$ tais que $I = \langle f_1, \ldots, f_s \rangle$, e [2, Proposition 2.5.9] mostra que $V(I)$ é o conjunto das raízes comuns desses polinômios.

O primeiro ponto a ressaltar é que ideais diferentes podem ter a mesma variedade. Por exemplo, $\langle x \rangle$ e $\langle x^2 \rangle$ são ideais diferentes em $\mathbb{R}[x]$ que têm a mesma variedade $V(x) = V(x^2) = \{0\}$.

Outro problema sério pode ocorrer quando $\mathbb{K}$ não é algebricamente fechado: Considere os três polinômios $1, 1 + x^2, 1 + x^2 + x^4$ em $\mathbb{R}[x]$. Cada um desses gera um ideal diferente

$$I_1 = \langle 1 \rangle = \mathbb{R}[x], \qquad I_2 = \langle 1 + x^2 \rangle, \qquad I_3 = \langle 1 + x^2 + x^4 \rangle,$$

mas cada polinômio não tem raiz. Então, as variedades correspondentes são todas vazias:

$$V(I_1) = V(I_2) = V(I_3) = \emptyset.$$

Será que esse problema de ter ideais diferentes representando a variedade vazia desaparece se o corpo $\mathbb{K}$ é algebricamente fechado? Para provar o Teorema Fraco dos Zeros de Hilbert, precisamos do seguinte resultado:

Lema 3.1. *Dado $\mathbb{K}$ um corpo algebricamente fechado, seja $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ e assuma que para algum i, f_i é da forma*

$$cx_1^N + \text{ termos em } x_1 \text{ que tenham grau total menor que } N.$$

onde $c \neq 0$ é um elemento de $\mathbb{K}$ e $N > 0$. Se $I_1 = I \cap \mathbb{K}[x_2, \ldots, x_n]$, e $(a_2, \ldots, a_n) \in V(I_1)$, então existe $a_1 \in \mathbb{K}$ tal que $(a_1, \ldots, a_n) \in V(I)$.

Demonstração. Ver [2, Corollary 3.1.4]. Observe que na demonstração desse resultado, é possível substituir $\mathbb{C}$ por um corpo $\mathbb{K}$ algebricamente fechado. ■

Teorema 3.2 (Teorema Fraco dos Zeros de Hilbert)**.** *Seja $\mathbb{K}$ um corpo algebricamente fechado e seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal satisfazendo $V(I) = \emptyset$. Então, $I = \mathbb{K}[x_1, \ldots, x_n]$.*

Demonstração. Para provar que um ideal é igual a $\mathbb{K}[x_1, \ldots, x_n]$, a estratégia principal consiste em mostrar que o polinômio constante 1 está em I, pois se $1 \in I$, então I é todo o anel de polinômios.

No caso de uma variável, isto é, quando o anel de polinômios é $\mathbb{K}[x]$, por [1, Teorema 1.3.8] e [1, Teorema 2.2.2] $\mathbb{K}[x]$ é um domínio principal. Então, podemos escrever $I = \langle f \rangle$, para algum polinômio $f \in \mathbb{K}[x]$. Logo, $V(I)$ é o conjunto das raízes de f em $\mathbb{K}$. Já que $\mathbb{K}$ é algebricamente fechado, cada polinômio não constante em $\mathbb{K}[x]$ tem uma raiz. Isso significa que se $V(I) = \emptyset$, então f é uma constante não nula. Nesse caso, $\frac{1}{f} \in \mathbb{K}$ e, portanto, $g = (\frac{1}{f})g \cdot f \in I$, para todo $g \in \mathbb{K}[x]$. Isso mostra que $I = \mathbb{K}[x]$.

Agora assuma que o resultado foi provado para os anéis de polinômios em $n-1$ variáveis, que escreveremos por $\mathbb{K}[x_2, \ldots, x_n]$. Considere qualquer ideal $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ para o qual $V(I) = \emptyset$. Podemos assumir que f_1 não é constante, pois, caso fosse, não teríamos nada a provar. Então, suponha que f_1 tenha grau total $N \geq 1$. Em seguida, mudaremos as coordenadas para que f_1 tenha uma forma especialmente agradável. Ou seja, considere a mudança linear de variáveis

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1, \end{aligned} \tag{1}$$

onde os a_i são constantes em $\mathbb{K}$, ainda a serem determinadas. Realizando a substituição (1) em f_1, obtemos

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \ldots, \tilde{x}_n + a_n\tilde{x}_1) \\ &= c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{ termos em } \tilde{x}_1 \text{ que tenham grau total menor que } N. \end{aligned}$$

É possível mostrar que $c(a_2, \ldots, a_n)$ é uma expressão não nula em $a_2, \ldots, a_n$ seguindo o passo a passo do exercício 4.1.3 de [2]. Por conta do espaço que essa demonstração ocupa, iremos omití-la.

De [2, Proposition 1.1.5], podemos escolher $a_2, \ldots, a_n \in \mathbb{K}$ tais que $c(a_2, \ldots, a_n) \neq 0$. Com essa escolha de $a_2, \ldots, a_n$, sob a mudança de variáveis (1), todo polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ pode ser reescrito como um polinômio $\tilde{f} \in \mathbb{K}[\tilde{x}_1, \ldots, \tilde{x}_n]$. É possível mostrar que $\tilde{I} = \{\tilde{f} : f \in I\}$ é um ideal em $\mathbb{K}[\tilde{x}_1, \ldots, \tilde{x}_n]$.

Note ainda que $V(\tilde{I}) = \emptyset$ pois, se as equações transformadas tivessem solução(ões), as originais também teriam. Além disso, se pudermos mostrar que $1 \in \tilde{I}$, então $1 \in I$ seguirá, já que as constantes não são alteradas pela operação $\tilde{}$.

Logo, é suficiente provar que $1 \in \tilde{I}$. Pelo parágrafo anterior, $f_1 \in I$ se torna $\tilde{f}_1 \in \tilde{I}$ com a propriedade

$$\tilde{f}_1(\tilde{x}_1, \ldots, \tilde{x}_n) = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{ termos em } \tilde{x}_1 \text{ com grau total menor que } N,$$

onde $c(a_2, \ldots, a_n) \neq 0$. Seja agora

$$\pi_1 : \mathbb{K}^n \to \mathbb{K}^{n-1}$$

o mapeamento de projeção nas últimas $n-1$ coordenadas. Se definimos $\tilde{I}_1 = \tilde{I} \cap \mathbb{K}[\tilde{x}_2, \ldots, \tilde{x}_n]$, então, pelo Lema 3.1, temos que soluções parciais em $\mathbb{K}^{n-1}$ sempre se estendem, isto é, $V(\tilde{I}_1) = \pi_1(V(\tilde{I}))$. Isso implica que $V(\tilde{I}_1) = \pi_1(V(\tilde{I})) = \pi_1(\emptyset) = \emptyset$. Pela hipótese de indução, segue que $\tilde{I}_1 = \mathbb{K}[\tilde{x}_2, \ldots, \tilde{x}_n]$. Mas isso implica que $1 \in \tilde{I}_1 \subset \tilde{I}$, e a prova está completa. ■

(Problema da Consistência): Agora, será que é possível determinar se $V(f_1, \ldots, f_s) = \emptyset$, isto é, se as equações $f_1 = \cdots = f_s = 0$ têm uma solução em comum?

Observe que o Teorema Fraco dos Zeros de Hilbert nos ajuda a resolver o problema: Os polinômios falham em ter uma solução em comum se, e só se $V(f_1, \ldots, f_s) = \emptyset$. Pelo Teorema Fraco dos Zeros de Hilbert, essa última sentença vale se e só se $1 \in \langle f_1, \ldots, f_s \rangle$. Assim, para resolver esse problema, precisamos estar aptos a determinar se 1 pertence a um ideal. Isso é facilitado pela observação de que, para qualquer ordenação monomial, $\{1\}$ é a única Base de Gröbner reduzida para o ideal $\langle 1 \rangle$ (ver [2, página 172]).

Resumindo, temos o seguinte algoritmo de consistência: Se tivermos polinômios $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, nós computamos uma Base Reduzida de Gröbner do ideal que eles geram com respeito a qualquer ordenação. Se essa Base for $\{1\}$, os polinômios não têm raiz comum em $\mathbb{K}^n$; se a base não é $\{1\}$, eles devem ter um zero em comum. Note que esse algoritmo funciona apenas em corpos algebricamente fechados. Enunciemos o Teorema dos Zeros de Hilbert:

Teorema 3.3 (Teorema dos Zeros de Hilbert)**.** *Seja $\mathbb{K}$ um corpo algebricamente fechado. Se $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots x_n]$ são tais que $f \in I(V(f_1, \ldots, f_s))$, então existe um inteiro $m \geq 1$ tal que $f^m \in \langle f_1, \ldots, f_s \rangle$ e vice-versa.*

Demonstração. Dado um polinômio f não nulo que se anula em todo zero comum dos polinômios $f_1, \ldots, f_s$, temos que mostrar que existe um inteiro $m \geq 1$ e polinômios $A_1, \ldots, A_s$ tais que

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Considere o ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y]$, onde $f, f_1, \ldots, f_s$ são como acima. Afirmamos que $V(\tilde{I}) = \emptyset$. Para ver isso, observe que para $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$ tem-se

- $(a_1, \ldots, a_n)$ é uma raiz comum de $f_1, \ldots, f_s$, ou
- $(a_1, \ldots, a_n)$ não é uma raiz comum de $f_1, \ldots, f_s$.

No primeiro caso $f(a_1, \ldots, a_n) = 0$, pois f desaparece em qualquer zero comum de $f_1, \ldots, f_s$. Então, o polinômio $1 - yf$ assume o valor $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$ no ponto $(a_1, \ldots, a_n, a_{n+1})$. Em particular, $(a_1, \ldots, a_n) \notin V(\tilde{I})$. No segundo caso, para algum i, $1 \leq i \leq s$, nós temos que ter $f_i(a_1, \ldots, a_n) \neq 0$. Em particular, concluímos novamente que $(a_1, \ldots, a_n, a_{n+1}) \notin V(\tilde{I})$. Como $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$ foi arbitrário, concluímos que $V(\tilde{I}) = \emptyset$, como afirmado. Agora aplique o

Teorema Fraco dos Zeros de Hilbert para concluir que $1 \in \tilde{I}$. Ou seja,

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

para polinômios $p_i, q \in \mathbb{K}[x_1, \ldots, x_n, y]$. Agora, defina $y = \frac{1}{f(x_1, \ldots, x_n)}$. Então, a relação acima implica que

$$1 = \sum_{i=1}^{s} p_i \left(x_1, \ldots, x_n, \frac{1}{f} \right) f_i.$$

Multiplicando os dois lados da igualdade por uma potência f^m, onde m é escolhido suficientemente grande para limpar todos os denominadores, obtemos

$$f^m = \sum_{i=1}^{s} A_i f_i$$

para polinômios A_i quaisquer em $\mathbb{K}[x_1, \ldots, x_n]$, como queríamos demonstrar. ■

4 Considerações finais

O Teorema dos Zeros de Hilbert nos afirma que, sobre um corpo $\mathbb{K}$ algebricamente fechado, a única forma de dois ideais diferentes definirem a mesma variedade é que para todo polinômio do conjunto de geradores de um dos ideais, alguma potência desse polinômio pertença ao outro ideal, e vice-versa. Sobretudo, cabe dizer ainda que o foco desse trabalho foi examinar o que acontece caso uma variedade de um ideal é vazia.

Agradecimentos

Na condição de bolsista do PET Matemática da Universidade Federal de Uberlândia, agradeço ao Programa de Eduação Tutorial da SESu/MEC pelo fomento e por todos que me apoiaram até aqui. O segundo autor agradece à FAPEMIG pelo apoio financeiro do projeto APQ-00470-22.

Referências

[1] GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**, 6a Ediçao. Editora SBM, 2015.

[2] COX, David et al. **Ideals, varieties, and algorithms**. American Mathematical Monthly, v. 101, n. 6, p. 582-586, 1994.

Sobre duas definições de completude para corpos ordenados

Bruno Henrique Viana de Morais
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
brunohvmorais@ufu.br

Jean Venato Santos
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
jvenatos@ufu.br

Palavras-chave

Corpos
Corpos ordenados
Corpos ordenados completos

Resumo

Apresentamos duas maneiras de introduzir a noção de corpos ordenados completos, mostramos que tais noções são distintas e provamos uma relação entre elas.

1 Introdução

Dado um corpo ordenado $\mathbb{K}$, nos textos de análise real, tais como [2], é comum introduzir a completude do corpo pela existência (em $\mathbb{K}$) de supremo para qualquer subconjunto limitado superiormente. Por outro lado, em [1], Aragona considera $\mathbb{K}$ completo se toda sequência de Cauchy converge em $\mathbb{K}$. Para diferenciar tais noções, diremos neste caso que o corpo ordenado é Cauchy completo. Aragona observa que as duas definições de completude são distintas e que a definição Cauchy completa, tem a vantagem de ser estendível de maneira natural para contextos mais gerais, tais como para "espaços métricos" e "espaços topológicos", tal facilidade não ocorre com a existência de supremo, para a qual a ordem em K é imprescindível.

Ainda em [1], Aragona enuncia, sem demonstração, que para um corpo ordenado $\mathbb{K}$ ser completo via existência de supremo equivale a $\mathbb{K}$ Cauchy completo e arquimediano. Mencionaremos mais adiante a existência de uma corpo ordenado não arquimediano que é Cauchy completo. Em particular, isto mostra que a propriedade Cachy completo para corpos ordenados é mais fraca que a completude via existência de supremo.

Na próxima seção serão introduzidas as noções necessárias para enunciar este resultado que relaciona as duas definições de completude para corpos ordenados e em seguida será apresentada uma demonstração deste resultado.

2 Noções preliminares e resultado principal

Um *corpo* é um conjunto $\mathbb{K}$ munido de duas operações $(a,b) \in \mathbb{K}\times\mathbb{K} \mapsto a+b \in \mathbb{K}$ e $(a,b) \in \mathbb{K}\times\mathbb{K} \mapsto ab \in \mathbb{K}$ chamadas *adição* e *multiplicação*, respectivamente, ambas comutativas e associativas, havendo elemento neutro da adição $0 \in \mathbb{K}$ e elemento neutro da multiplicação $1 \in \mathbb{K}$, para cada $x \in \mathbb{K}$ existe $-x \in \mathbb{K}$ tal que $x+(-x)=0$, para cada $x \in \mathbb{K}$, $x \neq 0$ existe $\frac{1}{x} \in \mathbb{K}$ tal que $x\frac{1}{x}=1$ e dados quaisquer $x,y,z \in \mathbb{K}$ vale $x(y+z)=xy+xz$.

Um corpo $\mathbb{K}$ é dito *ordenado* se possui um subconjunto P, chamado conjunto dos elementos positivos em $\mathbb{K}$, verificando as seguintes duas condições: se $x,y \in P$ então $x+y \in P$ e $xy \in P$; para cada $x \in \mathbb{K}$ ocorre uma e apenas uma das três alternativas: ou $x=0$ ou $x \in P$ ou $-x \in P$. Num corpo ordenado a expressão $x<y$, ou x é menor que y, significa que $y-x \in P$, o mesmo pode ser também expresso por $y>x$ e dito y é maior que x. Já a expressão $x \leq y$, ou x é menor ou igual a y, significa que $y-x \in P$ ou $y=x$, e também pode ser expresso por $y \geq x$ e dito y é maior ou igual a x.

É bem conhecido que os conjuntos dos números racionais $\mathbb{Q}$ e dos números reais $\mathbb{R}$ com as operações usuais de adição e multiplicação são exemplos de corpos ordenados com uma noção de ordem também usual. Já ao corpo dos números complexos $\mathbb{C}$, com adição e multiplicação usuais, não é possível munir com uma noção de ordem (ver, por exemplo, [3]).

O conceito de ordem permite definir a noção de *valor absoluto* para qualquer elemento x de $\mathbb{K}$ por $|x|=\max\{x,-x\}$. Uma *sequência em* $\mathbb{K}$, que denotaremos por (x_m), é uma função que a cada

elemento $m \in \mathbb{N}$ associa um único $x_m \in \mathbb{K}$.

A partir do conceito de valor absoluto é possível introduzir as seguintes noções sobre uma sequência (x_m) em $\mathbb{K}$: Uma sequência (x_m) em $\mathbb{K}$ é dita *limitada* se existir $M \in \mathbb{K}$ tal que $|x_m| < M$ para todo $m \in \mathbb{N}$. Uma sequência (x_m) é *convergente* em $\mathbb{K}$, se existe $a \in \mathbb{K}$ tal que, para todo $0 < \varepsilon \in \mathbb{K}$, existe $m_0(\varepsilon) \in \mathbb{N}$ de forma que $|x_m - a| < \varepsilon$ sempre que $m > m_0(\varepsilon)$. Neste caso diz-se que (x_m) *converge para* a e denota-se por $x_m \to a$. Uma sequência (x_m) em $\mathbb{K}$ é dita de *Cauchy*, se para cada $0 < \varepsilon \in \mathbb{K}$, existe $m_0(\varepsilon) \in \mathbb{N}$ tal que $|x_m - x_n| < \varepsilon$ sempre que $m, n \geq m_0(\varepsilon)$.

Tais noções são suficientes para a primeira definição de corpo ordenado completo, a ser considerado nesta nota, que é a definição apresentada por Aragona em [1, pg. 126]:

Definição 2.1. Um corpo ordenado $\mathbb{K}$ é dito *Cauchy completo* se suas sequências de Cauchy são convergentes em $\mathbb{K}$.

Ainda da noção de ordem num corpo $\mathbb{K}$, dado um subconjunto $A \subset \mathbb{K}$, diz-se que um elemento $b \in \mathbb{K}$ é uma *cota superior* de A se $a \leq b$ para cada $a \in A$. Quando A possui uma cota superior, diz-se que A é *limitado superiormente*. Se $A \subset \mathbb{K}$ é limitado superiormente, um elemento $x \in \mathbb{K}$ é chamado *supremo* de A, denotado por $\sup A$ se x é a menor cota superior de A, ou seja, se x satisfaz as duas condições seguintes.

(S1) $a \leq x, \forall a \in A$.

(S2) $x \leq b$, onde b é uma cota superior de A.

Isso permite formular outra definição de corpo ordenado completo, que é geralmente utilizada nos textos clássicos de análise real, tal como [2]:

Definição 2.2. Um corpo ordenado $\mathbb{K}$ é dito *completo* se todo subconjunto de $\mathbb{K}$ não vazio e limitado superiormente possuir supremo.

Outro conceito que segue da propriedade de ordem num corpo $\mathbb{K}$ é a noção de *corpo arquimediano* que ocorre quando dados quaisquer $a, b \in \mathbb{K}$, com $a > 0$, existir $n \in \mathbb{N}^*$ tal que $na > b$.

Dos livros textos de análise, tais como [1, 2], sabe-se que o corpo ordenado dos reais $\mathbb{R}$ é tanto completo quanto Cauchy completo além de arquimediano, enquanto o corpo ordenado dos racionais $\mathbb{Q}$ é arquimediano porém não é completo e nem Cauchy completo. Outro fato menos conhecido, é que existe corpo ordenado Cauchy completo que não é arquimediano, a saber o corpo de Levi-Civita (veja, por exemplo, [4]).

Em [1, pg. 157], Aragona observa que as duas definições de corpos ordenados completos são distintas e ressalta que a noção utilizada na Definição 2.1, ou seja, que toda sequência de Cauchy é convergente, tem a vantagem de ser estendível de maneira natural para contextos mais gerais, tais como para "espaços métricos" e "espaços topológicos". Tal facilidade não ocorre com a propriedade utilizada na Definição 2.2, para a qual a ordem em $\mathbb{K}$ é imprescindível. Ainda em [1, pg. 157], Aragona enuncia, sem demonstração, o seguinte resultado sobre a relação entre as duas noções de completude num corpo ordenado:

Teorema 2.3. *Seja $\mathbb{K}$ um corpo ordenado, as seguintes condições são equivalentes:*

(i) Todo subconjunto de $\mathbb{K}$ limitado superiormente possui supremo.

(ii) $\mathbb{K}$ é arquimediano e Cauchy completo.

Em particular, este resultado revela que a Definição 2.2 é mais restritiva que Cauchy completo, uma vez que um corpo ordenado pode ser Cauchy completo sem ser arquimediano.

Utilizando raciocínios clássicos da análise real encontrados em [1, 2], a seguir apresentamos uma demonstração para este teorema.

3 Demonstração do Teorema 2.3

Para demonstrar o Teorema 2.3 utilizamos o seguinte:

Lema 3.1. *Toda sequência de Cauchy num corpo ordenado é limitada.*

Demonstração. Sejam (x_n) uma sequência de Cauchy e $\varepsilon = 1$. Assim existe $n_0 \in \mathbb{N}$ tal que $m, n \geq n_0 \Rightarrow |x_m - x_n| < 1$. Em particular, $n \geq n_0 \Rightarrow |x_{n_0} - x_n| < 1$, ou seja, $n \geq n_0 \Rightarrow x_n \in (x_{n_0} - 1, x_{n_0} + 1)$. Considere $X = \{x_1, x_2, ..., x_{n_0-1}, x_{n_0} - 1, x_{n_0} + 1\}$, a o menor e b o maior elementos de X. Fazendo M o maior entre $|a|$ e $|b|$, segue que $|x_n| < M + 1, \forall n \in \mathbb{N}$, ou seja, que (x_n) é limitada. ■

Demonstração do Teorema 2.3. $(i) \Rightarrow (ii)$ Comecemos mostrando que $\mathbb{K}$ é arquimediano. Suponha por absurdo que existam $a, b \in \mathbb{K}$, com $a > 0$ tais que $\forall n \in \mathbb{N}, na \leq b$. Então $n \leq b/a$, $\forall n \in \mathbb{N}$, ou seja, $\mathbb{N}$ é limitado superiormente em $\mathbb{K}$. Por (i), existe $\overline{b} = \sup \mathbb{N}$ em $\mathbb{K}$. Assim, $n \leq \overline{b}, \forall n \in \mathbb{N}$ e portanto,

$$n - 1 \leq \overline{b} - 1, \forall n \in \mathbb{N} \Rightarrow n \leq \overline{b} - 1, \forall n \in \mathbb{N},$$

ou seja, $\overline{b}$ não é o menor majorante, logo não é $\sup \mathbb{N}$, o que absurdo. Portanto, temos que para quaisquer $a, b \in \mathbb{K}, a > 0$, existe $n \in \mathbb{N}$ tal que $na > b$, isto é, $\mathbb{K}$ é arquimediano.

Mostremos agora que dada (x_n) uma sequência de Cauchy em $\mathbb{K}$, então (x_n) converge em $\mathbb{K}$. Primeiro, vamos mostrar que (x_n) possui subsequência convergente. Pelo Lema 3.1, (x_n) é limitada, então existe $M > 0$ tal que $x_n \in [-M, M]$. Seja $A = \{t \in \mathbb{R};\, t \leq x_n$ para infinitos valores de $n\}$. De $-M \leq x_n \leq M, \forall n \in \mathbb{N}$, segue que $-M \in A$ e $t \leq M, \forall t \in A$, logo A é não-vazio e limitado superiormente. Por (i), existe $c = \sup A$. Dado $\varepsilon > 0$, existe $t \in A$ tal que $c - \varepsilon < t$, logo, para infinitos índices n, $c - \varepsilon \leq x_n$. Por outro lado, $c + \varepsilon \notin A$, então há apenas um número finito de índices n tais que $c + \varepsilon \leq x_n$. Podemos concluir que, dado $\varepsilon > 0$, para um número infinito de valores de n, temos $c - \varepsilon < x_n < c + \varepsilon$. Assim, para todo $k > 0$ existe $x_{n_k} \in \left(c - \frac{1}{k},\, c + \frac{1}{k}\right)$, portanto (x_{n_k}) é uma subsequência de (x_n) que converge para c, quando $k \to \infty$.

Segundo, vamos mostrar que sendo (x_n) de Cauchy a sequência converge para o mesmo limite da subsequência acima. Dado $\varepsilon > 0$, existe n_0 tal que $m, n \geq n_0 \Rightarrow |x_m - x_n| < \frac{\varepsilon}{2}$. Como $x_{n_k} \to c$,

existe k_0 tal que $n_{k_0} > n_0$ e $|x_{n_{k_0}} - c| < \frac{\varepsilon}{2}$. Assim, para todo $m > n_0$ temos

$$|x_m - c| \leq |x_m - x_{n_{k_0}}| + |x_{n_{k_0}} - c| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

O que mostra que $x_n \to c$.

$(ii) \Rightarrow (i)$ Seja $X \subset \mathbb{K}$ um subconjunto não vazio e limitado superiormente. No intuito de mostrar que X possui supremo defina:

$$B := \{b \in \mathbb{K};\ b \text{ é uma cota superior de } X\} \text{ e } B^C := \mathbb{K} \setminus B.$$

De X ser limitado superiormente segue que $B \neq \emptyset$. Dados $x \in X \neq \emptyset$ e $a \in \mathbb{K}$ tais que $a < x$ segue que $a \in B^C$, donde $B^C \neq \emptyset$. Note que se $a \in B^C$ e $b \in B$ então $a < b$. De fato, se $b \leq a$ então a seria cota superior de X e portanto seria um elemento de B, o que não ocorre pela definição de B^C.

A seguir, vamos provar que existe $\lambda \in \mathbb{K}$ tal que $a \leq \lambda \leq b$ para quaisquer $a \in B^C$ e $b \in B$. Posteriormente mostraremos que $\lambda = \sup X$.

Afirmação: Dado $n \in \mathbb{N}$, existem $a_n \in B^C$ e $b_n \in B$ tais que $b_n - a_n < \frac{1}{n}$.

Com efeito, dados quaisquer $a \in B^C$ e $b \in B$, sendo $\mathbb{K}$ um corpo ordenado arquimediano existe $m \in \mathbb{N}$ tal que $b - a < m \cdot \dfrac{1}{n}$. Defina $\delta := \dfrac{b-a}{m}$ e observe que $0 < \delta < \frac{1}{n}$. A partir destes ingredientes, defina a sequência $(r_i)_{0 \leq i \leq m}$ no corpo $\mathbb{K}$ por: $r_i := a + i\delta,$ para cada $i = 0, 1, \ldots, m$.

Como $r_0 = a + 0\delta = a \in B^C$ e $r_m = a + m\delta = a + m\frac{b-a}{m} = a + b - a = b \in B$, segue que existe $l \in \{0, 1 \ldots, m-1\}$ tal que $r_l \in B^C$ e $r_{l+1} \in B$, senão teríamos que $r_i \in B^C$ para todo $i \in \{0, 1, \ldots, m\}$, contradizendo $r_m \in B$.

Para concluir a afirmação, basta fazer $a_n = r_l \in B^C$ e $b_n = r_{l+1} \in B$, pois

$$b_n - a_n = r_{l+1} - r_l = a + (l+1)\delta - (a + l\delta) = \delta < \frac{1}{n}.$$

Pela afirmação, existem sequências (a_n) em B^C e (b_n) em B tais que $0 < b_n - a_n < \frac{1}{n}, \forall n \in \mathbb{N}^*$.

Assim, dados quaisquer $p, q \in \mathbb{N}^*$, de $a_q \leq b_p$ segue que $a_q - a_p \leq b_p - a_p < \frac{1}{p}$, e analogamente, trocando p e q obtém-se $a_p - a_q < \frac{1}{q}$. Logo,

$$|a_p - a_q| = \max\{a_p - a_q,\ a_q - a_p\} < \max\left\{\frac{1}{p},\ \frac{1}{q}\right\}, \forall\, p, q \in \mathbb{N}^*,$$

o que implica que a sequência (a_n) é de Cauchy, pois dado $\varepsilon > 0$ basta tomar $p_0 \in \mathbb{N}$ tal que $\frac{1}{p_0} < \varepsilon$, assim $p, q \geq p_0$ implica $|a_p - a_q| < \max\left\{\frac{1}{p},\ \frac{1}{q}\right\} \leq \frac{1}{p_0} < \varepsilon$. Por (ii), segue que (a_n) é convergente em $\mathbb{K}$, ou seja, existe $\lambda \in \mathbb{K}$ tal que $a_n \to \lambda$.

Por outro lado, temos que (b_n) também converge para λ, pois:

$$|b_n - \lambda| \leq |b_n - a_n| + |a_n - \lambda| < \frac{1}{n} + |a_n - \lambda|.$$

Portanto, $|b_n - \lambda| \to 0$ o que implica $b_n \to \lambda$, quando $n \to \infty$.

Assim, dados quaisquer $a \in B^C$ e $b \in B$, temos:

$$a \leq b_n \text{ e } a_n \leq b, \, \forall \, n \in \mathbb{N}^*$$

que, passando ao limite quando $n \to \infty$, implica

$$a \leq \lim b_n = \lambda = \lim a_n \leq b,$$

o que mostra a existência do $\lambda \in \mathbb{K}$ previamente mencionada.

Note que λ é cota superior de X. Com efeito, se existisse $x \in X$ tal que $x > \lambda$, ou, $x - \lambda > 0$, uma vez que $b_n \to \lambda$, existiria n_0 tal que $0 \leq b_{n_0} - \lambda < x - \lambda$ o que implicaria $b_{n_0} < x$ com $b_{n_0} \in B$, o que é absurdo. Por outro lado, como $\lambda \leq b$ para todo $b \in B$, temos que λ é, pela definição de B, a menor das cotas superiores de X, finalizando a prova de que $\lambda = \sup X$. ■

4 Considerações finais

Neste trabalho são apresentadas duas formas de se introduzir completude em corpos ordenados. Foi observado que a noção Cauchy completo é mais geral pela citação do corpo de Levi-Civita, que é ordenado Cauchy completo mas não arquimediano e portanto, pelo Teorema 2.3, não é completo. O conjunto dos reais $\mathbb{R}$, é dado exemplo como corpo ordenado Cauchy completo arquimediano e (consequentemente) completo, um fato relevante e talvez menos conhecido é que este é o único corpo com tais caraterísticas. Tal afirmação é apresentada, sem demonstração, por Aragona em [1, pg. 127].

Agradecimentos

Na condição de bolsista do PICME, agradeço ao CNPq pelo fomento.

Referências

[1] ARAGONA, Jorge, **Números Reais**. São Paulo: Editora Livraria da Física, 2010.

[2] LIMA, Elon Lages, **Curso de Análise. Volume 1**. Rio de Janeiro: Projeto Euclides, 1989.

[3] LIMA, Elon Lages, **Meu Professor de Matemática e outras histórias**. Rio de Janeiro: Editora SBM, 1991.

[4] BERZ, Martin, Calculus and numerics on Levi-Civita fields. **Computational Differentiation: Techniques, Applications, and Tools**,1996, 89, 19–37, 1996.

Planaridade e Coloração de Grafos

Gabriel Teles
UFU, FAMAT, Uberlândia, MG, Brasil
gabriel.teles1@ufu.br

Germano Abud de Rezende
UFU, FAMAT, Uberlândia, MG, Brasil
germano.abud@ufu.br

Palavras-chave

Grafo.
Planaridade.
Coloração de Grafos.

Resumo

Neste trabalho introduzimos a teoria de grafos e apresentamos alguns resultados clássicos sobre planaridade e coloração de vértices. São inúmeras as aplicações da teoria em problemas concretos e existem ainda várias conjecturas sobre o assunto. O famoso "problema das 4 cores" desafiou gerações de matemáticos por mais de um século e ainda hoje desperta interesse e curiosidade. Em sua formulação original, o teorema afirma que qualquer mapa pode ser colorido com no máximo 4 cores. Nosso objetivo é apresentar resultados teóricos e clássicos da teoria, finalizando o texto com alguns exemplos de aplicações. As referências citadas neste texto servem como um guia para um estudo mais detalhado e também para outras referências correlatas.

1 Introdução

Formalmente, um **grafo** é definido como um par ordenado $G = (V, E)$, onde V é um conjunto finito de vértices e $E \subset V \times V$ é um conjunto de arestas. As arestas podem ser direcionadas (setas que indicam uma direção) e temos um grafo direcionado. Neste trabalho trataremos apenas de grafos não-direcionados.

Se para um dado par de vértices existe mais de uma aresta associada, dizemos que o grafo é um **multigrafo**. Um grafo sem laços e sem arestas múltiplas é dito ser um **grafo simples**. Neste texto, o termo "grafo" será usado apenas para grafos simples. Um **grafo completo** é um grafo em que todos os vértices estão conectados por uma aresta. É uma classe importante de grafos e frequentemente usada em várias aplicações práticas e teóricas da teoria dos grafos. Denotamos o grafo completo com n vértices por K_n. Um **grafo bipartido** é um grafo em que o conjunto de vértices pode ser particionado em dois subconjuntos disjuntos, de forma que todas as arestas conectem apenas vértices de conjuntos diferentes. Em outras palavras, não há arestas entre vértices do mesmo subconjunto. Os grafos bipartidos são usados em várias aplicações práticas, como modelagem de sistemas de recomendação, análise de redes sociais e em problemas de emparelhamento. Por exemplo, em um sistema de recomendação de filmes, os vértices de um grafo bipartido podem representar usuários e filmes, e uma aresta pode representar uma avaliação positiva do usuário para o filme. O objetivo é encontrar pares de usuários e filmes que formem uma boa recomendação. Um **grafo bipartido completo** é um grafo bipartido tal que cada vértice de um subconjunto da partição de V está conectado a todos os vértices do outro subconjunto. Se V foi particionado em dois subconjuntos com m e p elementos cada um, denotamos o grafo bipartido completo por $K_{m,p}$. Um **caminho** em um grafo G é uma sequência de vértices tais que dois vértices consecutivos estão conectados e não há repetição de arestas. Se o primeiro e o último vértices forem iguais, o caminho é **fechado**. Se não houver repetições de vértices (exceto possivelmente o primeiro e o último), o caminho é **simples**. Um **ciclo** é um caminho simples fechado. Denotamos um ciclo com n vértices por C_n. Um grafo é **conexo** se existir um caminho ligando quaisquer dois vértices deste grafo. Uma **árvore** é um grafo conexo e acíclico (sem ciclos). Esta também é uma importante classe de grafos, com aplicações em construções de rodovias, instalações de redes em geral, dente outras. Também é comum quando se deseja verificar a validade de certos resultados para grafos, demonstrar inicialmente o resultado para árvores. Existem muitos resultados teóricos "clássicos" de propriedades e caracterização de grafos nas classes elencadas acima, entretanto omitiremos a maioria destes resultados por não se relacionarem diretamente com o assunto principal deste texto.

2 Grafos Planares

Um grafo é dito **planar** se admitir uma representação gráfica no plano, sem que suas arestas se cruzem. No estudo de grafos planares, podemos nos restringir aos grafos simples. Um exemplo de grafo planar é o grafo K_4 que pode ser desenhado em um plano sem que suas arestas se cruzem,

conforme ilustrado na Figura 1.

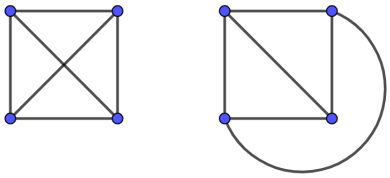


Figura 1: O grafo K_4 e sua representação planar.

Todavia afirmar o que um grafo é planar, muitas vezes não é uma tarefa trivial. Para isso existem vários teoremas importantes relacionados a grafos planares. Enunciaremos alguns destes resultados clássicos, sem demostrá-los. Existem dois grafos não planares que são muito importantes no estudo de planaridade: o K_5 (completo sobre cinco vértices) e o $K_{3,3}$ (bipartido completo).

Teorema 2.1. *Os grafos K_5 e $K_{3,3}$ não são planares.*

A demonstração "clássica" pode ser encontrada em [2].

Toda representação planar de um grafo planar divide o plano em regiões, chamadas faces, sendo uma destas faces ilimitada (chamada face infinita). O número de faces de um grafo está relacionado com o número de arestas e vértices do grafo através da fórmula de Euler, cuja demonstração pode ser encontrada em [2]:

Teorema 2.2 (Fórmula de Euler)**.** *Em um grafo planar conexo, o número de vértices (n), o número de arestas (m) e o número de faces (f) satisfazem a equação $n - m + f = 2$.*

O teorema anterior tem dois corolários importantes que podem ser úteis para se determinar a não planaridade de um grafo. As demosntrações podem ser encontradas em [4].

Corolário 2.3. *Se G é um grafo simples, conexo e planar com m arestas e $n \geq 3$ vértices, então, $m \leq 3n - 6$.*

Observe que K_5 tem 10 arestas e 5 vértices e, portanto, não satisfaz a relação do corolário acima.

Corolário 2.4. *Se G é um grafo simples, conexo e planar com m arestas, n vértices e nenhum ciclo de tamanho 3, então $m \leq 2n - 4$.*

Observe que $K_{3,3}$ tem 9 arestas e 6 vértices e, portanto, não satisfaz a relação do corolário acima.

Para se determinar se um grafo é planar, processos de redução ou subdivisão (veja em [4] ou [1]) podem ser aplicados ao grafo original até se obter um grafo "mais simples" que não cumpra certas condições de planaridade. Um teorema importante sobre planaridade foi demonstrado pela primeira vez pelo matemático polonês Kuratowski em 1930. A demostração pode ser encontrada em [1].

Teorema 2.5 (Kuratowski)**.** *Um grafo G é planar se, e somente se, não contém um subgrafo que é uma configuração do grafo K_5 ou do grafo $K_{3,3}$.*

A verificação do teorema de Kuratowski tem um alto preço computacional, pois é um problema de complexidade $NP - completo$ ou seja, é um tipo de problema computacional para o qual não se conhece um algoritmo eficiente para encontrar a solução. Um problema NP-Completo tem um alto preço computacional porque os únicos algoritmos conhecidos para resolvê-lo exigem um tempo que é uma função exponencial do tamanho do problema. Na prática, existem algoritmos eficientes para verificar a planaridade de grafos de tamanho moderado, mas para grafos maiores, esses algoritmos podem ser impraticáveis em termos de tempo de execução e uso de memória. O Teorema de Whitney afirma que qualquer grafo planar pode ser construído a partir do grafo completo de quatro vértices K_4 por meio de subdivisões de arestas. Mais detalhes sobre este resultado podem ser encontrados em [1].

3 Coloração de Grafos

Dado um grafo qualquer, realizar uma coloração do mesmo, significa atribuir rótulos a certos elementos (faces, vértices ou arestas), os quais chamamos de "cores". No caso de uma coloração de vértices, dois vértices adjacentes não devem receber a mesma cor e desejamos utilizar uma quantidade mínima de cores, dita número cromático do grafo G, denotado por $\chi(G)$. Uma k-coloração de um grafo é uma coloração com k cores, isto é, uma função $c : V(G) \to \{1, 2, \ldots, k\}$ tal que vértices adjacentes possuem imagens distintas. O grafo é dito k-cromático se admite uma k-coloração e k é mínimo. Vejamos alguns exemplos:

- o grafo nulo ($E = \emptyset$) é 1-cromático;
- o gafo completo K_n é $(n-1)$-cromático;
- o ciclo C_n é 2-cromático para n par e 3-cromático para n ímpar.
- uma árvore com $n \geq 2$ vértices e um grafo bipartido com $m \geq 1$ arestas são 2-cromáticos;

Existem diversos teoremas importantes sobre coloração de vértices e número cromático em grafos. A seguir enunciaremos alguns deles. As demonstrações podem ser encontradas em [3].

Teorema 3.1. *Um grafo é 2-cromático se, e somente se ele é bipartido.*

Teorema 3.2. *Se Δ é grau máximo dos vértices de G então o número cromático de G é menor ou igual a $\Delta + 1$.*

Teorema 3.3 (Teorema (Brooks, 1941))**.** *Seja G uma grafo simples, conexo, $G \neq K_n$. Se Δ é grau máximo dos vértices de G então $\chi(G) \leq \Delta$.*

Observe que o resultado acima nem sempre fornece uma "limitação razoável", visto que aplicado ao grafo bipartido completo $K_{1,n}$ obtém-se $\chi \leq n$ e sabemos que $\chi = 2$ para esta classe de grafos.

O teorema seguir é um dos mais famosos resultados sobre coloração de vértices. Ele surgiu de um dos mais famosos problemas em aberto (até 1976) da matemática: o problema das quatro cores.

O problema foi posto em 1852 pelo matemático britânico Francis Guthrie, que se perguntou se seria possível colorir um mapa de forma que países vizinhos tivessem cores diferentes usando no máximo quatro cores. Embora sua hipótese fosse verdadeira para muitos casos, ninguém conseguiu provar essa conjectura por mais de um século. Kenneth Appel e Wolfgang Haken apresentaram uma prova em 1976, usando um algoritmo computacional que verificou todas as possíveis configurações de mapas planares e provou que todo mapa planar pode ser colorido com no máximo quatro cores. Embora essa prova tenha sido controversa devido ao uso de computadores, desde então foram apresentadas outras provas independentes, algumas das quais mais elegantes e acessíveis do que a prova original.

Teorema 3.4 (Teorema das Quatro Cores)**.** *Seja G um grafo simples e planar. Então $\chi(G) \leq 4$.*

O Teorema das Quatro Cores tem implicações importantes em várias áreas, incluindo ciência da computação, teoria dos jogos e planejamento de redes de comunicação. Além disso, é um dos resultados mais conhecidos da teoria dos grafos e é frequentemente mencionado em livros didáticos de matemática e popularizados em cultura popular.

4 Aplicações

Nesta seção apresentaremos alguns exemplos em que os resultados sobre coloração de grafos podem ser aplicados. Uma pergunta óbvia seria: mas e o algoritmo para colorir? Neste trabalho apresentaremos apenas um algoritmo "guloso" de coloração. O leitor interessado pode encontrar várias referências que tratam do assunto. Seja G um grafo com n vértices.

1. Ordene os vértices de G em uma ordem não-crescente de graus.
2. Faça $S_1 = S_2 = \cdots = S_n = \emptyset$.
3. Inclua v_1 em S_1.
4. Para $j = 2, \ldots, n$:
    - Encontre um conjunto S_k tal que v_j não seja a nenhum dos vértices em S_k e k é o menor índice possível.
    - Inclua v_j em S_k.

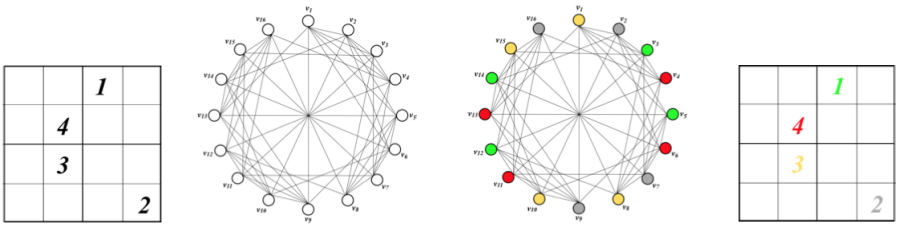
Exemplo 4.1. *Pode-se mostrar que o número cromático do mapa do Brasil é 4 (veja [4]).*

Exemplo 4.2. *A tabela abaixo mostra a alocação de alunos nos exames finais que eles devem realizar:*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
MATEM	X							X				X			X	
PORT	X			X							X					X
INGLÊS						X	X			X					X	
GEOG				X	X		X		X				X			
HIST			X							X		X		X		X
FIS			X		X								X			
QUIM		X						X	X		X			X		
BIOL		X				X										

Duas disciplinas só podem ter exames realizados simultaneamente se não houver alunos comuns. Podemos construir um grafo com as disciplinas como vértices $\{M, P, I, G, H, F, Q, B\}$ *e dois vértices serão adjacentes se tiverem um aluno em comum. Assim, o problema é equivalente a obter uma coloração mínima. Os exames podem ser realizados em dois horários: um para* $\{B, G, H, M\}$ *e outro para* $\{F, I, P, Q\}$.

Exemplo 4.3. *Vamos resolver o sudoku* 4×4 *a seguir, obtendo uma 4-coloração do grafo correspondente. Enumeramos os vértices a partir de cada quadradinho do sudoku, de cima para baixo e da esquerda para a direita. A partir da partição em quatro cores* $S_1 = \{1, 8, 10, 15\}, S_2 = \{2, 7, 9, 16\}, S_3 = \{3, 5, 12, 14\}, S_4 = \{4, 6, 11, 13\}$ *preencheremos com o número 1 os quadradinhos associados a cor verde, 2 para a cor cinza, 3 para a cor amarela e 4 para a cor vermelha.*



Fonte: https://ri.ufs.br/bitstream/riufs/9211/2/DIOGENES_SANTANA_VASCONCELOS.pdf

Com este trabalho percebemos o grande número de aplicações da teoria de grafos em diversas áreas, em particular teoria de coloração de grafos. Para trabalhos futuros, pretendemos estudar os polinômios cromáticos e suas aplicações na determinação de números cromáticos em grafos.

Agradecimentos

Na condição de bolsista do PICME (Programa de Iniciação Científica e Mestrado), agradeço Conselho Nacional de Desenvolvimento Científico e Tecnológico pelo fomento.

Referências

[1] BERGE, C. **The theory of graphs**. Courier Corporation, 2001.

[2] BONDY, J.A.; MURTY, U.S.R. **Graph theory with applications**. Vol. 290. London: Macmillan, 1976.

[3] WILSON, R.J. **Introduction to graph theory**. Pearson Education India, 1979.

[4] RANGEL,S.; ANTUNES,V.; ARAUJO,S. **Teoria de Grafos - Notas de Aula**. Disponível em: <https://www.ibilce.unesp.br/#!/departamentos/matematica-aplicada/docentes/socorro/disciplinas/teoria-dos-grafos/>. Acesso em: 12 abr. 2023.

Estudo comparativo entre as linguagens de programação Julia e C na resolução numérica de PVC unidimensionais.

Gabriel Melo Gomes Pereira
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brail
gabriel.pereira3@ufu.br

Santos Alberto Enriquez Remigio
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brail
santos.er@ufu.br

Palavras-chave

Linguagem C.
Linguagem Julia.
Método das diferenças finitas.
Problemas de valor de contorno linear.

Resumo

O presente trabalho tem como objetivo comparar o tempo computacional das linguagens Julia e C na solução de um sistema linear associado a um Problema de Valor de Contorno (PVC). Para isso, foram implementados programas nas duas linguagens utilizando o Método das Diferenças Finitas (MDF). Os resultados obtidos demonstraram que a linguagem Julia se compara em velocidade às linguagens de baixo nível, sendo capaz de ser mais rápida que C em alguns casos. Esses resultados aparentam indicar que a implementação de códigos, usando a linguagem de programação Julia, para resolução numérica de modelos matemáticos cujo processo de obtenção das soluções exija alta demanda computacional, seja um procedimento indicado para obtenção de soluções numéricas dos referidos .

1 Introdução

Ao estudar fisica, engenharia e áreas afim, depara-se com fenômenos físicos modelados por equações diferenciais. São exemplos: escoamento de fluidos; transferência de calor em uma barra; queda de um objeto; deflexão de vigas, etc. Estas equações diferenciais podem ser ordinárias ou parciais. No caso de equações diferenciais ordinárias, a função incógnita é uma função que depende de uma única variável independente. Um caso particular dessas equações são os chamados Problemas de Valor de Contorno modelados por equações diferenciais ordinárias (EDO) de segunda ordem, com

algum tipo de informação nos extremos do domínio de solução ($[a, b]$) denominadas condições de contorno. O PVC linear modelado a ser trabalho no presente trabalho é dado por

$$\begin{cases} \dfrac{d^2u}{dx} = f(x), \quad a < x < b & (1) \\ u(a) = v_a & (2) \\ u(b) = v_b & (3) \end{cases}$$

onde f é uma função conhecida, sendo v_a e v_b constantes. A EDO acima é linear. A determinação da solução analítica de um PVC é simples desde que seja possível integrar analiticamente a função f(x). Porém, a maioria das equações encontradas nos problemas práticos não possui solução analítica, sendo necessário então o uso de métodos numéricos para a solução das mesmas.

O objetivo do presente estudo é verificar a viabilidade do uso da linguagem de programação Julia como uma linguagem científica para a implementação computacional de códigos para resolução numérica para Problemas de Valor de Contorno lineares. Para fins de comparação, um código foi implementado nas linguagens Julia e C para resolver numericamente, via Método de Diferenças Finitas, o referido PVC. Os resultados obtidos foram analisados e comparados em termos de eficiência e facilidade de implementação computacional.

2 Linguagem Julia

Julia é uma linguagem de programação dinâmica de alto nível, lançada em 2012, que se destaca por ser projetada especificamente para computação científica e numérica. A linguagem foi desenvolvida por um grupo de pesquisadores do MIT, com a intenção de criar uma linguagem que pudesse ser tão fácil de usar quanto o Matlab ou Python, porém tão rápida quanto o C ou Fortran.

A linguagem de programação Julia tem como inspiração várias outras linguagens, como Python, Matlab, R, Lua e Lisp. Ela adota a sintaxe do Python e o conceito de pacotes (módulos) do R. Além disso, a linguagem possui recursos avançados como manipulação de dados em larga escala, compilação just-in-time (JIT), computação paralela e distribuída, que a tornam adequada para aplicações científicas complexas.

A grande vantagem da Julia é sua eficiência, que é comparável à de linguagens de programação de baixo nível, como C ou Fortran, mas com uma sintaxe muito mais simples e intuitiva. No entanto, a Julia ainda é uma linguagem relativamente nova e, portanto, pode ter limitações em relação a outras linguagens já validadas, testadas e com maior tempo de uso, como Python ou R.

3 Linguagem C

A linguagem C foi criada em 1972, por Dennis M. Ritchie, e se tornou uma das linguagens de programação mais populares e influentes na história da computação. Ela foi projetada para permitir que os programadores escrevam programas eficientes e que possam ser executados em uma ampla variedade de sistemas operacionais e arquiteturas de hardware.

Uma das principais vantagens da linguagem C é sua velocidade e eficiência, permitindo que os programadores escrevam programas que executam rapidamente e usem recursos do sistema de forma eficiente. No entanto, aprender a linguagem C pode ser desafiador no início e isso pode afastar o aluno ou aluna do mundo da programação.

4 Método de Diferenças Finitas

A ideia geral do Método de Diferenças Finitas é a discretização do domínio e a substituição das derivadas presentes na equação diferencial por aproximações denominadas diferenças finitas.

A discretização do domínio consiste na escolha de pontos do intervalo $[a, b]$ onde se deseja aproximar a solução. Podemos, por exemplo, dividir o intervalo em um número finito de subintervalos de tamanhos diferentes e escolher pontos em cada um desses intervalos. No caso de considerar-se subintervalos do mesmo tamanho e os pontos como sendo os extremos desses subintervalos, o conjunto de pontos definidos é denominado de malha homogênea (pontos igualmente espaçados).

A figura abaixo representa uma malha homogênea dividida em n partes e com espaçamento h. Observe que os x, representam os valores numéricos do domínio discretizado.

Figura 1: Malha Homogênea ou Regular

O segundo passo é a discretização da equação que consiste em substituir as derivadas presentes na equação por aproximações dadas por diferenças finitas, obtidas através da expansão em série de Taylor da função incógnita. Para nosso caso, a derivada de segunda ordem foi aproximada pela seguinte diferença centrada de segunda ordem:

$$\frac{d^2u_i}{dx^2} = \frac{u_{i+1} - 2u_i + u_{i-1}}{h^2} + O(h^2) \tag{4}$$

4.1 MDF Aplicado a PVC Lineares

Para a resolução do problema dado em (1-3), o primeiro passo é a discretização do intervalo, para isso dividi-se o intervalo em n partes iguais, com espaçamento dado por:

$$h = \frac{b-a}{n} \tag{5}$$

obtendo assim, uma malha com $n+1$ pontos. Cada um desses pontos é obtido pela expressão $x_i = a + ih$, com $i = 0, \ldots, n$.

Para a discretização da equação (1), utilizou-se as fórmulas de diferenças centrais para aproximar a primeira e segunda derivada de u.

$$\frac{u_{i+1} - 2u_i + u_{i-1}}{h^2} = f(x_1) \tag{6}$$

Colocando em evidência os valores de u_{i-1}, u_i e u_{i+1} obtém-se:

$$u_{i-1} - 2u_i + u_{i+1} = h^2 f(x_i), \tag{7}$$

com $u_0 = v_a$ e $u_n = v_b$.

Desenvolvendo a equação (7) em cada ponto u_i, do domínio discretizado e utilizando u_o e u_n, como acima, obtem-se o seguinte sistema linear tridiagonal da forma $Ax = b$

$$A = \begin{bmatrix} -2 & 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -2 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & -2 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & -2 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & -2 \end{bmatrix}, \quad x = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ \vdots \\ u_{n-2} \\ u_{n-1} \end{bmatrix} \quad e \quad b = \begin{bmatrix} h^2 f(x_1) - u_a \\ h^2 f(x_2) \\ h^2 f(x_3) \\ h^2 f(x_4) \\ \vdots \\ h^2 f(x_{n-2}) \\ h^2 f(x_{n-1}) - u_b \end{bmatrix} \tag{8}$$

5 Metodologia

O método utilizado para avaliação neste trabalho foi a implementação de um programa utilizando as ferramentas mais básicas de ambas as linguagens, C e Julia, em um computador com processador Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz, que conta com 4 núcleos e 8 processadores lógicos, além de uma memória RAM de 8 GB. O sistema operacional utilizado foi o Microsoft Windows 11 Pro. Ambas implementavam o método de Gauss-Seidel para resolver o sistema linear $Ax = b$. Os resultados foram enviados para um arquivo para visualizar as aproximações obtidas por ambos códigos. Além disso, foi medido o tempo de execução do programa em ambas as linguagens. No contexto dos

problemas que serão apresentados ϵ_r refere-se ao erro relativo máximo e ϵ_R do resíduo.

Três Problemas de Valor de Contorno do tipo (1)-(3) foram resolvidas:

- Problema 1: $f(x) = 0$ com solução exata do dada por $u(x) = 2x + 3$ para $-1 \leq x \leq 1$.
- Problema 2: $f(x) = -4\pi^2 sen(2\pi x)$ com solução analítica $u(x) = sen(2\pi x)$ para $-1 \leq x \leq 1$.
- Problema 3: $f(x) = (-4\pi^2 sen(2\pi x) + 4\pi cos(2\pi x) + sen(2\pi x))e^x$ com solução da EDO $u(x) = sen(2\pi x)e^x + x$ para $0 \leq x \leq 2$.

Nos três problemas, dividimos o intervalo em $N = 1000$ partes iguais. O número máximo de iterações foi definido como 100.000, com um valor de erro máximo de $1e^{-8}$ $(= 10^{-8})$ e uma tolerância de erro relativo de $1e^{-5}$ $(= 10^{-5})$.

Nas tabelas 1 a 3 aparecem os números de iterações do método de Gauss-Seidel realizadas pelos códigos (coluna 2), erros relativos atingidos (coluna 3), erros dos resíduos obtidos (coluna 4) e tempos computacionais gastos (coluna 5), para os problemas 1, 2 e 3, respectivamente.

Linguagem	Número de Iterações	ϵ_r	ϵ_R	Tempo(seg)
Julia	100.000	2,843035e-6	1,419065e-5	2,050
, C	100.000	1,419065e-5	1,419065e-5	5,228

Tabela 1: Tabela de resultados do Problema 1

Linguagem	Número de Iterações	ϵ_r	ϵ_R	Tempo(seg)
Julia	66.962	9,999738e-9	1,000490e-8	2,262
C	66.968	9,999412e-9	9,999413e-9	11,706

Tabela 2: Tabela de resultados do Problema 2

Linguagem	Número de Iterações	ϵ_r	ϵ_R	Tempo(seg)
Julia	100.000	9,740593e-7	4,303828e-6	8,582
C	100.000	4,303828e-6	4,303828e-6	53,280

Tabela 3: Tabela de resultados do Problema 3

Na Figura 2 mostram-se as aproximações obtidas por ambos códigos. Ambos resultados estão próximos entre eles e da solução exata.

6 Conclusão

Em suma, a implementação do método de Diferenças Finitas para resolver um Problema de Valor de Contorno linear em ambas as linguagens, C e Julia, mostrou-se eficiente e produziu resultados consistentes. A comparação dos tempos de execução entre as duas linguagens revelou que a implementação em Julia foi mais rápida do que em C. Além disso, a facilidade de implementação em Julia foi

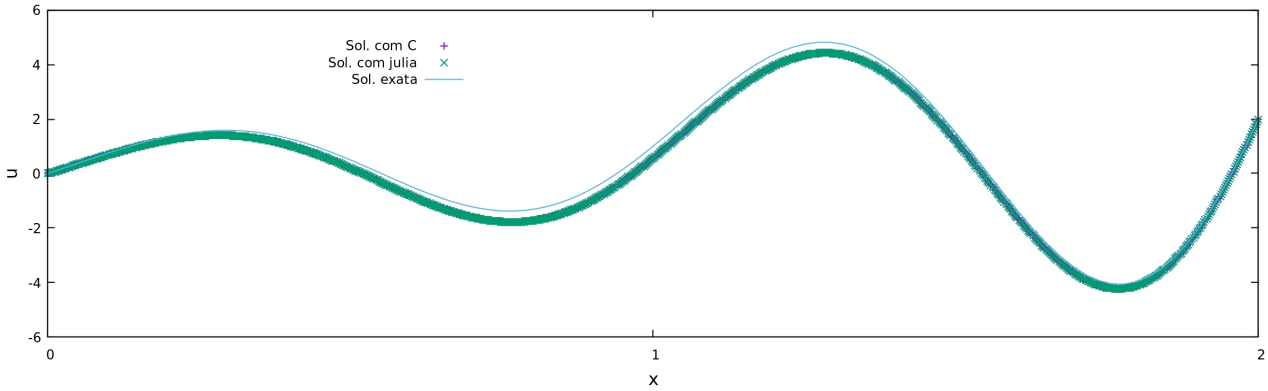


Figura 2: Soluções aproximadas, usando Julia e C, e solução exata do Problema 3

destacada pela sua sintaxe clara e concisa, facilitando o desenvolvimento do programa. No entanto, os resultados também mostraram que a margem de erro em ambas as linguagens era similar. Portanto, dependendo do contexto e dos objetivos do projeto, a escolha da linguagem pode variar, mas, sim Julia tem um alto potencial como uma linguagem científica.

Referências

[1] Boyce, W.E. and DiPrima, R.C. **Equações diferenciais elementares e problemas de valores de contorno**. Grupo Gen - LTC, 2010.

[2] Burden, A.M. and Burden, R.L. and Faires, D.J. **Análise Numérica**. CENGAGE DO BRASIL, 2016.

[3] Humes, A. F. P. C; Melo, I. S. H; Yoshida, L. K; MARTINS, W. T. **Noção de Cálculo Numérico**. São Paulo: USP, 1984.

[4] JULIA DOCUMENTATION. **Julia Language Documentation**. Disponível em: https://docs.julialang.org/en/v1/. Acesso em: 10 jan. 2023.

[5] SCHILDT, H.; MAYER, R.C. C completo e total. Makron Books, 1997.

Uma Introdução ao Método SIMPLEX

Fernanda de Carvalho Pinto
UFU, FEELT, Uberlândia, MG, Brasil
fernanda.carvalho@ufu.br

Germano Abud de Rezende
UFU, FAMAT, Uberlândia, MG, Brasil
germano.abud@ufu.br

Palavras-chave

Programação linear.
SIMPLEX.
Otimização.

Resumo

Neste trabalho faremos uma breve introdução ao método SIMPLEX para a resolução de certos problemas de programação linear. Inicialmente uma pequena introdução é feita: definimos e apresentamos a forma padrão de um problema linear de otimização e exemplificamos como problemas mais gerais podem ser colocados na forma padrão. Em seguida, o método SIMPLEX na forma de tableau é apresentado a partir de um exemplo. As principais referências para a teoria e exemplos neste trabalho foram [1],[2] e [3].

1 Introdução

Um problema de otimização linear trata-se de um conjunto de funções lineares, sendo uma delas a **função objetivo** que desejamos maximizar/minimizar e as demais são as restrições, que podem ser de igualdade ou desigualdades. Ou seja, problemas de otimização linear necessitam de uma função principal, que em problemas cotidianos poderia ser, por exemplo, uma função que relaciona o ganho com uma certa quantidade de produtos, e as restrições representariam a quantidade máxima de matéria prima ou horas de trabalho a serem gastas. Assim, nesse exemplo, ao maximizar o ganho, deve-se levar em consideração o total de material disponível ou a carga horária. A programação linear consiste em um método de otimização matemática, que envolve problemas lineares de maximização ou minimização. As questões de otimização linear envolvem elementos como as **variáveis de decisão**, as quais representam quantidades que precisam ser determinadas, e as **restrições** que limitam a quantidade de recursos disponíveis.

Exemplo 1.1. *Uma empresa fabrica dois tipos de produto X_1 e X_2. O produto X_1 leva 1 hora para ser produzido, possui uma pintura especial que leva 2 horas para ser feita e é vendido por R$300,00, enquanto o produto X_2 leva 2 horas para ser produzido, possui uma pintura especial que leva 1 hora para ser feita e é vendido por R$200,00. Em uma semana, a empresa desfruta de 100 horas de produção e 90 horas para pintura especial. Desejamos determinar as quantidades dos produtos X_1 e X_2 a serem produzidas de modo que o lucro seja o maior possível dentro das restrições impostas.*
O problema pode ser modelado matematicamente da seguinte maneira:

$$\begin{aligned} \textit{maximize} \quad & z = 300x_1 + 200x_2 \\ \textit{restrições} \quad & x_1 + 2x_2 \leq 100 \\ & 2x_1 + x_2 \leq 90 \\ & x_1, x_2 \geq 0 \end{aligned}$$

Dessa forma, a função z é um exemplo de função objetivo, enquanto as demais inequações representam as restrições para o problema. As variáveis x_1, x_2 que correspondem às quantidades dos produtos X_1 e X_2 a serem produzidas, respectivamente, são as variáveis de decisão.

2 Forma Padrão

Os problemas de programação linear podem ser colocados em uma forma padrão antes de serem resolvidos. Um problema está na forma padrão se os seguintes critérios são satisfeitos:

- a função objetivo deve ser maximizada;
- as restrições devem ser igualdades;
- as variáveis devem ser não negativas;
- as restrições devem ser não negativas.

A forma padrão do problema é apresentada da seguinte forma:

$$\begin{aligned} \textit{max} \quad & c^T x \\ \textit{restrições} \quad & Ax = b \\ & x \geq 0 \end{aligned} \tag{1}$$

Entretanto, caso um problema não esteja em sua forma padrão há alguns passos simples que podem ser efetuados para se obter tais condições necessárias:

- Se nas restrições $Ax = b$ ocorrer algum linha onde o coeficiente b_i é negativo, multiplica-se esta linha por -1.
- Há situações, como os exemplo 1.1 e 1.2, em que as restrições estão na forma de desigualdade, Neste caso é necessário adicionar certas variáveis chamadas de **variáveis de folga (ou excesso)** que transformam uma restrição de desigualdade em uma restrição equivalente de igualdade.

  Exemplo 2.1.

  $$\begin{aligned} \textit{maximize} \quad & x_2 + 2x_2 \\ \textit{restrições} \quad & 4x_1 + 2x_2 \leq 10 \\ & x_1 + 3x_2 \geq 18 \\ & x_1, x_2 \geq 0 \end{aligned}$$

  Adicionam-se variáveis de folga y_i's, não negativas, caso a restrição seja do tipo "$\leq$" e subtraem-se as variáveis de excesso z_i's, não negativas, caso a restrição seja do tipo "$\geq$":

  $$\begin{aligned} \textit{maximize} \quad & x_1 + 2x_2 \\ \textit{restrições} \quad & 4x_1 + 2x_2 + y_1 = 10 \\ & x_1 + 3x_2 - z_2 = 18 \\ & x_1, x_2, y_1, z_2 \geq 0 \end{aligned}$$

- Se o problema tiver uma ou mais variáveis que não precisam ser necessariamente não negativas, isto é, se não houver a restrição $x_i \geq 0, \forall i$, então têm-se variáveis livres. Para tornar essa variável não negativa, uma opção é escrevê-la na forma de diferença de outras duas variáveis não negativas:

  $$x_i = u_i - v_i, \text{ onde } u_i \geq 0 \text{ e } v_i \geq 0.$$

  Exemplo 2.2.

  $$\begin{aligned} \textit{minimize} \quad & x_1 + 2x_2 + 3x_3 \\ \textit{restrições} \quad & 4x_1 + 2x_2 + x_3 = 10 \\ & x_1 + 3x_2 + 5x_3 = 18 \\ & x_2, x_3 \geq 0 \end{aligned}$$

Substituindo x_1 por $u_1 - v_1$, obtém-se:

$$\begin{aligned} \textit{minimize} \quad & u_1 - v_1 + 2x_2 + 3x_3 \\ \textit{restrições} \quad & 4u_1 - 4v_1 + 2x_2 + x_3 = 10 \\ & u_1 - v_1 + 3x_2 + 5x_3 = 18 \\ & u_1, v_1, x_2, x_3 \geq 0 \end{aligned}$$

Outra opção para tornar a variável não negativa é tirá-la do problema, a isolando-a em uma das equações e colocando a variável em função das demais, assim, excluir a equação isolada do problema e substituir o seu valor nas outras. Isolando-se x_1 na segunda restrição do exemplo 2.2 tem-se $x_1 = 18 - 3x_2 - 5x_3$. Substituindo-se essa igualdade na função objetivo, obtem-se:

$$\begin{aligned} \textit{minimize} \quad & 18 - x_2 - 2x_3 \\ \textit{restrições} \quad & 10x_2 + 19x_3 = 62 \\ & x_2, x_3 \geq 0. \end{aligned}$$

Após a solução do problema ter sido encontrada para x_2 e x_3, basta substituir os valores na expressão para x_1 determinando-se o seu valor.

3 O Método SIMPLEX

O método SIMPLEX, desenvolvido por George Dantzig em 1947, é um procedimento iterativo que utiliza-se de uma solução básica viável e, a partir dela, realiza-se repetidas operações em busca de uma solução ótima para um problema de programação linear.

Como todo problema de minimização pode ser transformado em um problema de maximização, vamos apresentar o método SIMPLEX para problemas de maximização. Para isto, apresentaremos o método a partir de um exemplo. Considere o seguinte problema (na forma padrão):

Exemplo 3.1.

$$\begin{aligned} \textit{maximize} \quad & z = 5x_1 + 2x_2 \\ \textit{restrições} \quad & x_1 + F_1 = 3 \\ & x_2 + F_2 = 4 \\ & x_1 + 2x_2 + F_3 = 9 \\ & x_1, x_2, F_1, F_2, F_3 \geq 0 \end{aligned}$$

onde x_1 e x_2 variáveis de decisão e F_1, F_2 e F_3 variáveis de folga.

Observe que o sistema linear $Ax = b$, dado pelas equações das restrições, tem 5 variáveis e 3 equações e, portanto, tem infinitas soluções. Queremos encontrar aquela que maximiza a função z. Uma solução básica viável "óbvia" consiste em zerar as variáveis x_1, x_2 (variáveis não básicas) e assim as variáveis de folga assumem seus valores máximos e não nulos (variáveis básicas), ou seja

$(F_1, F_2, F_3) = (3, 4, 9)$, mas $z = 0$ com certeza não deve ser a solução ótima! A partir da escolha da solução básica viável, escrevemos a função objetivo em termos das variáveis não básicas (z já está em função de x_1 e x_2). Se pelo menos uma delas tem coeficiente positivo (problemas de maximização) então a solução não é ótima! Se a solução básica proposta não for ótima, é necessário selecionar uma das variáveis não básicas (variáveis de decisão) para entrar na base, a qual será aquela que, dentro da função objetivo, apresente o maior coeficiente positivo. Após a escolha da variável que entra na base, verificar qual das variáveis de folga deve sair da base. No exemplo, x_1 entra na base e deve assumir o maior valor possível, sem que as variáveis básica fiquem negativas. Portanto, obtém-se $x_1 = 3$ e $x_2 = 0$. Ainda, $F_1 = 3 - x_1 = 3 - 3 = 0$ e assim, F_1 sai da base. A nova solução básica será $(x_1, F_2, F_3) = (3, 4, 6)$. E continuamos o processo até que nenhuma das variáveis não básicas possua coeficiente positivo. Uma maneira mais "econômica" de apresentar o método SIMPLEX é através do **"tableau"**, que consiste de uma tabela com os coeficientes de todas as variáveis do problema. No nosso exemplo, inciamos com:

base	x_1	x_2	F_1	F_2	F_3	termos independentes
z	-5	-2	0	0	0	0
F_1	1	0	1	0	0	3
F_2	0	1	0	1	0	4
F_3	1	2	0	0	1	9

Tabela 1: Tableau para o exemplo 3.1

Observe que escrevemos $z - 5x_1 - 2x_2 + 0F_1 + 0F_2 + 0F_3 = 0$ para a função objetivo (teremos solução ótima se todos os coeficientes para a equação de z forem não negativos), e começamos com a solução básica viável $(F_1, F_2, F_3) = (3, 4, 9)$. Ao analisarmos se a solução que foi proposta é uma solução ótima, percebemos que nem todos os coeficientes da equação para z são não-negativos. Portanto uma solução ótima ainda não foi encontrada.

O coeficiente de maior valor absoluto é -5, o qual está associado a variável x_1. Portanto a coluna da variável x_1 é a coluna pivô (x_1 entra na base). Em seguida, identifica-se a variável que sai da base: aquela cuja a divisão dos termos independentes pela sua correspondente na coluna pivô possua o menor valor(apenas divisões finitas e não negativas devem ser consideradas). Nesse caso, tem-se:

$$F_1 = \frac{3}{1} = 3; \quad F_2 = \frac{4}{0} = \text{indeterminado (desconsiderar)}; \quad F_3 = \frac{9}{1} = 9.$$

Portanto, a variável F_1 deixará a base. Realiza-se o processo de pivoteamento (linha e coluna de x_1), resultando na tabela 2.

Como ainda restam coeficientes negativos na linha da função objetivo, a análise é feita novamente (x_2 entra e F_3 sai da base) e todo o processo de pivoteamento (linha e coluna de x_2) é repetido, resultando na tabela 3.

Obtendo, desse modo, a solução ótima com valores das variáveis:

$$x_1 = 3, x_2 = 3, F_1 = 0, F_2 = 1, F_3 = 0, z = 21$$

	x_1	x_2	F_1	F_2	F_3	termos independentes
Z	0	-2	5	0	0	15
x_1	1	0	1	0	0	3
F_2	0	1	0	1	0	4
F_3	0	2	-1	0	1	6

Tabela 2: Tableau para o exemplo 3.1 após x_1 entrar na base.

	x_1	x_2	F_1	F_2	F_3	termos independentes
Z	0	0	4	0	1	21
x_1	1	0	1	0	0	3
F_2	0	0	1/2	1	-1/2	1
x_2	0	1	-1/2	0	1/2	3

Tabela 3: Tableau para o exemplo 3.1, após x_2 entrar na base.

4 Conclusão

O método simplex provou-se como um procedimento muito eficiente para a resolução de muitos problemas de programação linear. Sua estruturação na forma de tableau é fácil de ser implementada e executada. A partir do estudo de casos mais simples, iremos ampliar nosso estudo para casos particulares: empate na escolha de variáveis que entram ou saem da base, problemas com múltiplas soluções, solução ilimitada, e o dual-simplex. Desejamos ainda implementar o método e resolver alguns problemas aplicados.

Agradecimentos

Na condição de bolsista do PICME (Programa de Iniciação Científica e Mestrado), agradeço Conselho Nacional de Desenvolvimento Científico e Tecnológico pelo fomento.

Referências

[1] MARINS, F. A. S.; **Introdução à pesquisa operacional**. São Paulo: Cultura Acadêmica, 2011.

[2] PUCCINI, A. de L.; **Introdução à programação linear**. Rio de Janeiro: Livros Técnicos e Científicos, 1987.

[3] SCHNEIDER. R. M.; **Trabalho de Conclusão de Curso - Método Simplex Para Programação Linear**. Universidade Federal de Santa Catarina. Florianópolis, 2013.

Álgebra linear aplicada no controle de um braço robótico

Vitor Hugo Leite Caetano
UFU, Faculdade de Mecatrônica, Uberlândia, Minas Gerais, Brasil
vitor.caetano@ufu.br

Profa. Luciana Aparecida Alves
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
luciana.alves@ufu.br

Palavras-chave

Robótica
Álgebra Linear
Matrizes de rotação

Resumo

O presente trabalho explora a aplicação da Álgebra Linear na cinemática direta, cinemática inversa e robótica móvel. Apresentaremos um exemplo prático de como a Álgebra Linear é usada para resolver problemas em robótica e destacando a importância da matemática nesse campo.

1 Introdução

A Álgebra Linear é uma ferramenta essencial na robótica moderna, permitindo o controle de braços robóticos e outras aplicações diversas, como manufatura, automação e exploração espacial. Um exemplo importante do uso de matrizes nesse caso são as matrizes de rotação, amplamente utilizadas para controlar a posição e orientação de braços robóticos. Neste resumo, caracterizaremos as matrizes de rotação e as aplicaremos no controle desses mecanismos.

2 Transformações ortogonais

Definição 2.1. (a) *Considere $M(m,n)$ o espaço das matrizes reais com m linhas e n colunas. Uma matriz $A \in M(m,n)$ é ortogonal se $A^tA = I_n$, onde I_n denota a matriz identidade de ordem n.*
(b) *Sejam V e W espaços vetoriais reais de dimensão finita munidos de produto interno. Uma transformação linear $T : V \longrightarrow W$ é dita ortogonal quando $\langle T(u), T(v)\rangle = \langle u, v\rangle$, para todo $u, v \in V$.*

Observe que a igualdade $A^tA = I_n$ significa que as colunas das matriz A formam um conjunto de m vetores ortonormais em $\mathbb{R}^n$. Além disso, no caso das matrizes quadradas ortogonais, temos que $A^{-1} = A^t$.

As transformações ortogonais possuem diversas propriedades geométricas interessantes, muitas das quais estão contidas no seguinte resultado.

Teorema 2.2. *Seja $T : V \longrightarrow W$ uma transformação linear entre espaços vetoriais reais de dimensão finita providos de produto interno. As seguintes afirmações são equivalentes:*

a. T é transformação linear ortogonal;

b. T preserva norma, isto é, $\|T(u)\| = \|u\|$, para todo $u \in V$;

c. T preserva distância, isto é, $\|T(u) - T(v)\| = \|u - v\|$, para todo $u, v \in V$;

d. A matriz da transformação T relativa a qualquer par de bases ortonormais de V e W é uma matriz ortogonal;

e. A transformação T transforma conjuntos ortonormais de V em conjuntos ortonormais de W.

Demonstração. Veja [2], Teorema 14.1, pag. 184. ■

No presente estudo, trabalharemos apenas com as matrizes quadradas ortogonais. O próximo exemplo caracteriza todas as matrizes quadradas de ordem 2.

Exemplo 2.3. *Seja*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

uma matriz ortogonal 2×2. *Seja* $u_1 = (a, c) \in \mathbb{R}^2$ *um vetor unitário de* $\mathbb{R}^2$, *logo existe* $\theta \in \mathbb{R}$ *tal que* $a = \cos\theta$, $c = \operatorname{sen}\theta$. *Temos que* $u_2 = (b, d)$ *é um vetor unitário perpendicular a* u_1, *assim:* $u_2 = \pm(-\operatorname{sen}\theta, \cos\theta)$. *Logo, existem duas possibilidades para a matriz* A*:*

$$A = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{bmatrix} \; ou \; A = \begin{bmatrix} \cos\theta & \operatorname{sen}\theta \\ \operatorname{sen}\theta & -\cos\theta \end{bmatrix}$$

No primeiro caso, observe que o polinômio característico de A *é dado por* $p(\lambda) = \lambda^2 - (2\cos\theta)\lambda + 1$, *o qual não possui raízes reais salvo se* $\theta = 0°$ *ou* $= 180°$, *ou seja,* $A = \pm I_2$. *Além disso, no caso no qual a matriz não possui autovalores reais, ela representa a rotação de um ângulo* θ.

Para o segundo caso, temos $p(\lambda) = \lambda^2 - 1$ *que possui raízes* ± 1. *Então, dado o operador* $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ *cuja matriz na base canônica é* A, *temos que* T *admite autovetores* v_1, v_2 *com* $T(v_1) = v_1$ *e* $T(v_2) = -v_2$. *Nesse caso, a matriz* A *representa uma reflexão em torno do eixo que contém* v_1, *paralelamente a* v_2.

De forma geral, os operadores ortogonais podem ser caracterizados da seguinte forma.

Teorema 2.4. *Seja* $A : E \longrightarrow E$ *um operador ortogonal num espaço vetorial de dimensão finita munido de produto interno. Existe uma base ortogonal de E relativamente a qual a matriz A tem a forma:*

$$\begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & \cos\alpha_1 & -\operatorname{sen}\alpha_1 & \\ & & & & & & \operatorname{sen}\alpha_1 & \cos\alpha_1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & \cos\alpha_k & -\operatorname{sen}\alpha_k \\ & & & & & & & & & \operatorname{sen}\alpha_k & \cos\alpha_k \end{bmatrix}$$

Figura 1: Fonte [2] pag. 189

Demonstração. Veja [2], Teorema 14.3, pag. 189. ■

3 Exemplo aplicado

Usando como base para o estudo, usaremos um exemplo retirado do artigo [1]. Seguindo nesse exemplo, entenderemos mais sobre as transformações lineares empregadas no controle de um braço

robótico, o qual rotaciona em torno do próprio eixo z.

Para tanto, é essencial definir alguns tipos de junta, tais como a junta prismática ou linear, responsável por movimentos em linha reta, e a junta rotacional, que realiza movimentos circulares em torno do seu próprio eixo.

3.1 Rotação em $\mathbb{R}^3$

As rotações de um ângulo θ em $\mathbb{R}^3$ podem ser descritas pelas matrizes:

$$R_x = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta & 0 \\ \operatorname{sen}\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad R_y = \begin{bmatrix} \cos\theta & 0 & -\operatorname{sen}\theta \\ 0 & 1 & 0 \\ \operatorname{sen}\theta & 0 & \cos\theta \end{bmatrix}, \quad R_z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\operatorname{sen}\theta \\ 0 & \operatorname{sen}\theta & \cos\theta \end{bmatrix}.$$

Denotaremos por R_{01} a rotação do sistema 0 para o sistema 1. logo, a posição de um determinado ponto p_0 relativo ao referencial 1 é dada por:

$$R_{01} \cdot p_0 = p_1.$$

A rotação inversa do sistema 1 para o sistema 0 pode ser obtida por: $p_0 = (R_{01})^t \cdot p_1$. Agora se o referencial sofrer uma sequência finita de rotações, essa sequência pode ser representada por: $R_{01} \cdot R_{12} \ldots R_{n,n-1}$.

3.2 Translação

A translação de um ponto por uma dada distância é definida por

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} + D_{01} = \begin{bmatrix} x \\ y \\ z \end{bmatrix} + \begin{bmatrix} d_{x0} \\ d_{y0} \\ d_{z0} \end{bmatrix}.$$

Define-se a *matriz homogênea* de ordem 4 da seguinte forma:

$$T_{01} = \begin{bmatrix} R_{01} & D_{01} \\ 0 & 1 \end{bmatrix},$$

sendo D_{01} a matriz de translação e R_{01} a matriz de rotação. Note que a linha inferior da matriz não oferece nenhuma informação, já que não foram consideradas perspectiva e escala.

3.3 Controle do braço robótico

Considere o problema de descrever o movimento de um braço robótico cuja base gira em torno do eixo z. A distância do referencial fixo 0 para o referencial 1 é de uma unidade ao longo do eixo z.

Podemos descrever o movimento da garra através de uma função com parâmetro nas coordenadas das juntas q, ou seja,

$$u = f(q)$$

, onde

- u vetor que permite descrever a posição da garra;
- $q = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \end{bmatrix}$, vetor das variáveis das juntas, sendo $q_i = \theta_i$ para uma junta rotativa e $q_i = d_i$ para uma junta prismática.

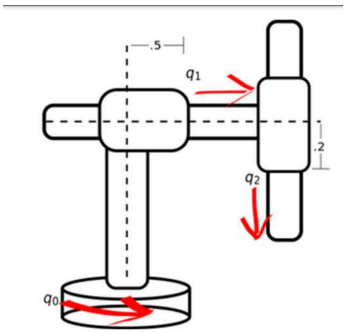


Figura 2: Fonte [1]

A matriz rotação do referencial fixo 0 para o referencial 1 é dada por:

$$R_{01} = \begin{bmatrix} \cos(q_0) & -\text{sen}\,(q_0) & 0 \\ \text{sen}\,(q_0) & \cos(q_0) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Obtém-se, assim, a matriz transformação homogênea do referencial fixo 0 para o referencial 1:

$$T_{01} = \begin{bmatrix} \cos(q_0) & -\text{sen}\,(q_0) & 0 & 0 \\ \text{sen}\,(q_0) & \cos(q_0) & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Quanto à transformação do referencial 1 para o referencial 2, não se verifica rotação (é uma junta prismática), ocorrendo uma translação de $0,5 + q_1$ ao longo do eixo y do referencial 1. Deste modo, a matriz transformação é dada por:

$$T_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0,5 + q_1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

A última transformação (do referencial 2 para o referencial da garra) obtém-se da translação ao longo do eixo z:

$$T_{2F} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -0,2 - q_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Assim, a transformação do referencial fixo 0 para o referencial da garra F obtém-se através da composição das transformações anteriormente enunciadas, isto é:

$$T_{0F} = T_{01}T_{12}T_{2F} = \begin{bmatrix} \cos(q_0) & -\text{sen}\,(q_0) & 0 & -\text{sen}\,(q_0)(0,5 + q_1) \\ \text{sen}\,(q_0) & \cos(q_0) & 0 & \cos(q_0)(0,5 + q_1) \\ 0 & 0 & 1 & 1,8 - q_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Assim, é possível calcular a posição de qualquer ponto da garra relativamente ao referencial fixo 0. Por exemplo, tomando $p_0 = (0, 0, 0, 1)$ e $q = (\pi/3, 0.3, 0.4)$, temos que

$$T_{0F} \cdot p_0 = \begin{bmatrix} -0.693 \\ 0.4 \\ 1.4 \\ 1 \end{bmatrix}.$$

Agradecimentos

Agradecimento ao CNPq pelo fomento da Bolsa de Iniciação Científica do PICME.

Referências

[1] COSTA, A. L. da S.. **Álgebra linear aplicada no controlo de um braço robótico**. 2020. Disponível em :https://fenix.tecnico.ulisboa.pt/downloadFile/1126518382274862/AL_Ana.pdf. Acesso em 02 de maio de 2023.

[2] LIMA, E. L.. **Álgebra Linear**. Coleção Matemática Universitária. 3ª Edição. Rio de Janeiro: SBM, 1999.

Pseudoprimos e números de Carmichael

Natan Gonçalves de Lyra
UFU, Faculdade de Computação, Uberlândia, MG, Brasil
natanglyra@gmail.com

Dylene Agda Souza de Barros
UFU, Faculdade de Matemática, Uberlândia, MG, Brasil
dylene@ufu.br

Palavras-chave

Pseudoprimos.
Números de Carmichael.
Teste de Miller.

Resumo

O Pequeno Teorema de Fermat diz que se p é primo, então b^p é congruente a b módulo p onde b é um inteiro, o que acontece na verdade é que existem números compostos que também satisfazem essa condição, a esses números damos o nome de *pseudoprimos* com base b. Existem também os números de Carmichael que são pseudoprimos para várias bases diferentes. No decorrer do resumo são mostrados as características desses números e diferentes testes de primalidade que foram sendo desenvolvidos com o tempo para testar se n é composto ou se provavelmente é primo, visto que existem números compostos (pseudoprimos) que passam nos testes para certas bases. O estudo dos números primos e pseudoprimos é de suma importância para algoritmos criptográficos como a criptografia RSA, principalmente o Teste de Miller, que até nos dias atuais, acerta a primalidade de números com relativa eficiência.

1 Introdução

O estudo de números primos é uma área fascinante da matemática, suas características únicas e distribuição bastante complexa, desde à antiguidade, foram motivos de estudo para matemáticos ao longo da história. *Pierre de Fermat* em especial, bastante conhecido pelo "Último Teorema de Fermat", desenvolveu um teste de primalidade que ficou conhecido como Pequeno Teorema de Fermat.

Teorema 1.1 (Pequeno Teorema de Fermat)**.** *Seja p um número primo e a um número inteiro, então*

$$a^p \equiv a(mod\ p)$$

Por meio deste teste sabemos que se p é primo e a é um inteiro qualquer, então a condição do teorema sempre será satisfeita. O problema acarretado de usar esse teorema como teste de primalidade é que existem números compostos que também satisfazem essas condições, tais números são chamados *pseudoprimos*, e são o tema desse resumo.

2 Pseudoprimos

2.1 Teste de Leibniz

Existem resultados interessantes derivados do Pequeno Teorema de Fermat (1.1) que ajudam na detecção de números compostos e primos, um exemplo disso é usarmos a contrapositiva do teorema. Se por acaso encontramos algum a tal que $a^n \not\equiv a(mod\ n)$, então n é composto, já que essa inequação viola o Pequeno Teorema de Fermat. Na verdade, é possível polir esse teste com algumas considerações adicionais.

Como no teste está sendo usado congruências módulo n, e qualquer inteiro é congruente a um inteiro no intervalo de 0 a $n-1$, e os números 0, 1 e $n-1$ sempre satisfazem a equação do Teorema (1.1), podemos limitar as bases a no intervalo $1 < a < n-1$. Já que sabemos agora que a é necessariamente menor que n, é possível usar uma variante do Pequeno Teorema de Fermat para os casos de n não dividir a.

Teorema 2.1 (Pequeno Teorema de Fermat II)**.** *Seja p um número primo e a um número inteiro que não é divisível por p, então*

$$a^{p-1} \equiv 1(mod\ p)$$

Isso significa que, se encontrarmos algum a no intervalo $1 < a < n-1$, tal que $a^{n-1} \not\equiv a(mod\ n)$, então n é composto.

O Teste de Leibniz consiste no inverso deste teste para números primos, ou seja, se um número ímpar n satisfaz o Teorema (2.1), para algum a no intervalo $1 < a < n-1$ então n é primo.

Exemplo 2.2. *Vamos testar o número 17 na base 2.*

$$2^{16} \equiv 65536 \equiv 3885 \cdot 17 + 1 \equiv 1(mod\ 17)$$

Dessa forma, usando 2 como base, o Teste de Leibniz retorna 17 como possível primo.

No entanto, existem alguns números que não são primos que passam no Teste de Leibniz usando 2 como base, um exemplo desses números é o 341, onde $2^{340} \equiv 1(mod\ 341)$, mesmo que $341 = 11 \cdot 31$ seja composto.

Quando um número inteiro positivo, ímpar e composto n passa no Teste de Leibniz, dizemos que ele é um *pseudoprimo* para a base $1 < b < n - 1$ se atender as condições do Teorema (2.1), isto é $b^{n-1} \equiv 1(mod\ n)$. Neste caso, 341 é um pseudoprimo para a base 2.

Para deixar o teste mais eficiente, podemos testar o mesmo número n para várias bases diferentes. Se colocarmos o número 341 novamente no Teste de Leibniz agora com base 3 teremos que $3^{340} \equiv 56(mod\ 341)$.

Dessa forma, usando 3 como base, o Teste de Leibniz retorna 341 como composto. Neste caso, dizemos que 3 é uma *testemunha* de que 341 é composto.

Aumentar a quantidade de bases testadas é uma boa forma de aumentar a eficiência do Teste de Leibniz, contudo, existem números que são *pseudoprimos* para todas as bases coprimas a n, esses números são conhecidos como *números de Carmichael*.

2.2 Números de Carmichael

Um número é de Carmichael se ele for um número composto ímpar $n > 0$ que satisfaz a equação do Pequeno Teorema de Fermat (1.1) para todas as bases b no intervalo $1 < b < n - 1$. O menor número dessa forma é o 561 e foi encontrado por *Robert Daniel Carmichael* em 1912.

Existem algumas formas de mostrar que 561 é um número de Carmichael, a primeira delas é pela definição dos números de Carmichael, ou seja, mostrar para todo b no intervalo $1 < b < 560$ que $b^{561} \equiv b(mod\ 561)$.

A segunda e mais simples forma de verificar que 561 é um número de Carmichael é mostrando que $b^{561} \equiv b(mod\ 561)$ que é equivalente a dizer que $b^{561} - b \equiv 0(mod\ 561)$. Ou seja, mostrar que $b^{561} - b$ é divisível por 561. É possível fatorar 561 da seguinte maneira $561 = 3 \cdot 11 \cdot 17$. Como cada um dos fatores de 561 são distintos entre si, podemos usar o seguinte lema que pode ser encontrado em [2]

Lema 2.3. *Sejam a, b e c inteiros positivos e suponhamos que a e b são primos entre si.*

1. *Se b divide o produto ac então b divide c;*

2. *Se a e b dividem c então o produto ab divide c;*

Isso significa que o produto destes primos (3, 11 e 17) divide $b^{561} - b$, basta mostrar que cada fator de 561 divide $b^{561} - b$.

Começando pelo número 3, queremos mostrar que

$$b^{561} \equiv b(mod\, 3)$$

Se por acaso 3 dividir b então a congruência será verificada, digamos que 3 não divide b. De acordo com o Teorema (2.1), $b^2 \equiv 1(mod\, 3)$ e como $561 = 2 \cdot 280 + 1$, então

$$b^{561} \equiv (b^2)^{280} \cdot b \equiv b(mod\, 3)$$

Podemos repetir o processo para o 11, onde $561 = 10 \cdot 56 + 1$ e consequentemente para o 17, onde $561 = 16 \cdot 35 + 1$. Logo

$$b^{561} \equiv (b^{10})^{56} \cdot b \equiv b(mod\, 11)$$

$$b^{561} \equiv (b^{16})^{35} \cdot b \equiv b(mod\, 17)$$

Como $b^{561} - b$ é divisível por 3, 11 e por 17, então o número 561 é de Carmichael.

Duas características desse número permitiram usar tanto a variante do Pequeno Teorema de Fermat (2.1) quanto o lema de produto de primos (2.3).

1. O **resto** da divisão de 561 por cada um de seus fatores menos um é igual a **1**;

2. A **multiplicidade** de cada fator de 561 é **1**;

Na verdade, *Alwin Reinhold Korselt* observou que existem infinitos números de Carmichael e que todos eles possuem essas mesmas duas características que o número 561 obedece.

2.3 Teorema de Korselt

O resultado obtido por Korselt mencionado anteriormente pode ser enunciado no seguinte Teorema

Teorema 2.4 (Teorema de Korselt)**.** *Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes:*

1. p^2 ***não divide*** n*;*

2. $p - 1$ ***divide*** $n - 1$*;*

É possível mostrar a veracidade desse Teorema por meio dos mesmos passos usados para verificar que 561 é um número de Carmichael, ou seja, queremos mostrar que

$$b^n \equiv b(mod\, n)$$

onde p é um fator primo de n. Caso p dividir b então a congruência será verificada, digamos que p não divide b. De acordo com o Teorema (2.1), $b^{p-1} \equiv 1(mod\, p)$, e pelo Teorema de Korselt (2.4), $p - 1$

divide $n-1$, e como $n = (n-1)+1$, então temos que

$$n = (n-1)+1 = (p-1)q+1$$

para algum q inteiro positivo, substituindo no Teorema de Fermat (2.1) teremos que

$$b^n \equiv b^{(p-1)q+1} \equiv (b^{p-1})^q \cdot b \equiv b(mod\ p)$$

Concluímos que, para qualquer inteiro b, se por acaso p é um dos fatores primos de n então a equação do Teorema (1.1) será satisfeita.

Como de acordo com o Teorema de Korselt (2.4), p^2 não divide n, ou seja, a multiplicidade de todos os fatores primos de n é igual a 1, então podemos escrever n como o produto dos primos p_1, p_2, $\cdots$ até p_k, onde $p_1 < \cdots < p_k$. Como cada um dos fatores de n são distintos entre si, segue do Lema (2.3) que se $b^n - b$ é divisível por cada um dos fatores de n, então o produto $n = p_1 \cdots p_k$ divide $b^n - b$, que é equivalente a dizer que $b^n \equiv b(mod\ n)$. Concluímos que se n satisfaz as condições do Teorema de Korselt (2.4), então n é um número de Carmichael. A prova da ida pode ser encontrada em [1].

2.4 Teste de Miller

Como mostrado anteriormente, os números de Carmichael passam no Teste de Leibniz para várias bases b diferentes. Surge então a necessidade de um teste que consegue verificar se um número inteiro positivo ímpar é composto mesmo entre os pseudoprimos e os números de Carmichael. Em 1976, *Garry L. Miller* desenvolveu um teste que consegue detectar números compostos com maior eficiência comparado ao de Leibniz.

Seja n o número ímpar a ser testado e a b uma base no intervalo $1 < b < n-1$, podemos escrever $n-1$ como $2^k q$ (visto que se n é ímpar então $n-1$ é par), onde k representa a multiplicidade de 2 na fatoração de $n-1$ e q é um inteiro ímpar. O Teste de Miller se resume em testar o módulo n na base b escolhida para todas as potências de b^q, b^{2q}, $b^{2^2 q}$, $b^{2^3 q}$, $\cdots$, $b^{2^{k-1} q}$ e $b^{2^k q}$, se por acaso nenhuma dessas potências forem congruentes a 1 módulo n, então o teste retorna n como composto.

Se por acaso o número n testado for primo, então pelo menos uma das potências da sequência deve ser congruente a 1 módulo n, visto que, de acordo com o Teorema de Fermat (2.1), $b^{2^k q} \equiv b^{n-1} \equiv 1(mod\ n)$. Diremos que j é o menor expoente tal que $b^{2^j q} \equiv 1(mod\ n)$, ou seja, j é o menor expoente tal que $b^{2^j q} - 1$ é divisível por n. Fazendo uma limitação tal que o expoente da base b seja par, ou seja, $j \geq 1$, podemos escrever $b^{2^j q} - 1$ usando produtos notáveis

$$b^{2^j q} - 1 = (b^{2^{j-1} q} - 1)(b^{2^{j-1} q} + 1)$$

Como n divide $b^{2^j q} - 1$, então n divide $b^{2^{j-1} q} - 1$ ou $b^{2^{j-1} q} + 1$, mas como j é o menor expoente tal que $b^{2^j q} - 1$ é divisível por n, então n não divide $b^{2^{j-1} q} - 1$, logo n divide $b^{2^{j-1} q} + 1$, o que é equivalente a dizer que $b^{2^{j-1} q} \equiv -1(mod\ n)$.

Por fim, temos que se n é primo, então ou pelo menos uma das potências b^{2q}, b^{2^2q}, b^{2^3q}, $\cdots$, $b^{2^{k-1}q}$ é congruente a -1 módulo n ou, para o caso de $j = 0$, $b^q \equiv 1(mod\, n)$, caso contrário, n é retornado como composto. No entanto, existem números compostos tais que $b^{2^{j-1}q} \equiv -1(mod\, n)$ ou $b^q \equiv 1(mod\, n)$, como será mostrado em um dos exemplos a seguir

Exemplo 2.5. *Vamos testar o número 341 na base 2, como* $340 = 2^2 \cdot 85$ *então,* $2^{85} \equiv 32(mod\, 341)$*, e* $2^{2\cdot 85} \equiv 32^2 \equiv 1(mod\, 341)$*, logo o número* ***341 é composto****.*

Exemplo 2.6. *Vamos testar o número de Carmichael 561 na base 2, como* $560 = 2^4 \cdot 35$ *então,* $2^{35} \equiv 263(mod\, 561)$*, e* $2^{2\cdot 35} \equiv 263^2 \equiv 166(mod\, 561)$*, e* $2^{2^2\cdot 35} \equiv 166^2 \equiv 67(mod\, 561)$*, e* $2^{2^3\cdot 35} \equiv 67^2 \equiv 1(mod\, 561)$ *logo o número* ***561 é composto****.*

Exemplo 2.7. *Vamos testar o número 25 na base 7, como* $24 = 2^3 \cdot 3$ *então,* $7^3 \equiv 18(mod\, 25)$*, e* $7^{2\cdot 3} \equiv 18^2 \equiv -1(mod\, 25)$ *logo o teste é* ***inconclusivo****.*

Dizemos que n é um *pseudoprimo forte* para uma base b caso o número composto ímpar n retornar inconclusivo para o Teste de Miller. Neste caso, 25 é um **pseudoprimo forte** para a base 7.

3 Considerações finais

O estudo dos números primos e de diferentes testes de primalidade são de suma importância para o desenvolvimento e manutenção de muitos algoritmos criptográficos usados na segurança de informações, como por exemplo, na criptografia RSA, que é a motivação principal do estudo dos Pseudoprimos e Números de Carmichael. Produzimos uma versão simplificada do Teste de Miller em linguagem C que foi disponibilizada na plataforma Replit pelo link <https://replit.com/@NatanOmega/Teste-De-Miller>.

Agradecimentos

Na condição de bolsista do PICME da Universidade Federal de Uberlândia, agradeço ao Programa de Iniciação Científica (CNPq) do IMPA pelo fomento.

Referências

[1] COUTINHO, S. C.; **Números Inteiros e Criptografia RSA**. 2ª Edição. Rio de Janeiro: IMPA, 2013.

[2] SANTOS, J. P. O.; **Introdução à Teoria dos Números**. 3ª Edição. Rio de Janeiro: IMPA, 2020.

Primeiros passos na mecânica quântica através de algoritmos quânticos

Filipe Caetano Oliveira de Resende
UFU, FEELT, Uberlândia, Minas Gerais, Brasil
filipe.resende@ufu.br

Ivan da Silva Sendin
UFU, FACOM, Uberlândia, Minas Gerais, Brasil
sendin@ufu.br

Palavras-chave

Mecânica quântica.
Algoritmos quânticos.
Bits quânticos.

Resumo

Este trabalho discute conceitos iniciais de mecânica quântica por meio de uma abordagem algorítmica: explicando o que são bits quânticos e como portas lógicas quânticas atuam sobre eles. Com o uso do kit de desenvolvimento de software Qiskit, para Python, e da plataforma de computação quântica IBM Quantum Experience, pode-se programar e executar circuitos quânticos em simuladores e computadores quânticos reais da empresa IBM. Indivíduos com conhecimentos básicos de álgebra linear e programação podem facilmente assimilar o conteúdo do trabalho e através disso construir uma base em física quântica.

1 Introdução

Entre o fim do Século XIX e o início do Século XX, uma série de problemas foram surgindo na Física. As teorias até então vigentes previam fenômenos incompatíveis com a realidade. Tal crise propiciou o surgimento da mecânica quântica [1]. Tal teoria lida com sistemas físicos cujas dimensões estão na escala subatômica. Na década de 1980, um novo campo promissor surgia: a computação quântica. Com ela, acredita-se que tarefas intangíveis para um computador tradicional serão realizadas pelos chamados computadores quânticos, que tiram vantagem de fenômenos da física quântica em prol de um ganho exponencial de eficiência [2]. Neste trabalho, é apresentada a experiência de aprendizado da mecânica quântica por meio do uso de algoritmos quânticos. São abordados conceitos básicos da mecânica quântica por meio de uma abordagem didática, utilizando a biblioteca Qiskit [3], para Python, e a plataforma IBM Quantum Experience [4]. Apresentamos a experiência de aprendizagem da mecânica quântica voltada para pessoas leigas em Física, porém com familiaridade com álgebra linear básica e programação.

2 Programação quântica

A IBM Quantum Experience é um serviço de computação quântica via nuvem da IBM. Por meio desta plataforma, é possível executar algoritmos quânticos, remotamente, em sistemas quânticos reais da IBM. O Qiskit é um kit de desenvolvimento de software open-source para Python. Ele foi criado pela IBM a fim de se possibitar a programação de algoritmos quânticos para a execução via nuvem. Para a implementação dos códigos nesse trabalho, fez-se uso do Jupyter Notebook, uma plataforma de computação interativa baseada na web e comumente utilizada para o uso do Qiskit.

3 Sobreposição quântica

3.1 O bit quântico

Os bits clássicos são unidades de informação que podem assumir os valores 0 ou 1. Diferentemente deles, os bits quânticos (qubits) podem estar em uma sobreposição dos dois valores. É como se estivessem em uma mistura de 0 e 1. No ato de medir/ler um qubit, seu estado de "mistura"colapsa para o estado 0 ou 1. À grosso modo, é como se a leitura feita por um observador forçasse o qubit a se decidir entre 0 ou 1. Dizemos que um qubit está em uma sobreposição quântica dos estados $|0\rangle$ e $|1\rangle$. A cada um dos dois valores está associado um número complexo denominado amplitude de probabilidade. O estado $|\psi\rangle$ de um qubit arbitrário é representado por um vetor normalizado em $\mathbb{C}^2$ [5]:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Os complexos α e β são as amplitudes de probabilidade. No processo de medição, as probabilidades de o qubit colapsar para $|0\rangle$ e $|1\rangle$ são, respectivamente, $|\alpha|^2$ e $|\beta|^2$.

4 Portas quânticas

No mundo clássico, as portas lógicas recebem como entrada um ou mais bits clássicos e produzem, como saída, geralmente 0 ou 1 (embora existam portas clássicas com mais de um bit de saída). Entre elas temos, por exemplo, a porta NOT:

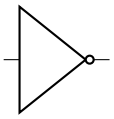


Figura 1: Porta lógica NOT

Entrada	Saída
0	1
1	0

Tabela 1: Tabela verdade da porta NOT

Podemos representar portas lógicas por meio de matrizes. A matriz correspondente a porta NOT é:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Multiplicando-se essa matriz à esquerda do vetor correspondente ao bit de entrada, obtém-se o bit de saída. Observe o caso em que a entrada é o bit 1:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

O vetor de saída corresponde ao bit 0. A representação matricial não se restringe apenas às portas, mas pode ser usada para representar circuitos lógicos por inteiro. Podemos representar qualquer circuito clássico por uma matriz. Se a entrada do circuito é composta por m bits e a saída por n bits, temos que: a entrada é representada por um vetor $2^m \times 1$, a saída por um vetor $2^n \times 1$ e o circuito em si por uma matriz $2^n \times 2^m$ [5].

Na porta lógica NOT, pode-se determinar qual foi o bit de entrada sabendo-se a saída: se a saída for 0, a entrada é 1, e se for 1, a entrada é 0. Trata-se de uma porta reversível. A porta OR, por outro lado, possui três configurações de entrada que resultam na saída 1 (0 e 1, 1 e 0, 1 e 1), e portanto não é reversível. Nos circuitos lógicos quânticos, todas as portas têm que ser reversíveis. As portas quânticas são representadas por matrizes unitárias, e uma das mais utilizadas é a porta Hadamard, representada pela matriz H [1]:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

A seguir, mostra-se a saída da porta para as entradas $|0\rangle$ e $|1\rangle$:

$$H|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$

$$H|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$$

As notações $|+\rangle$ e $|-\rangle$ são frequentemente utilizadas para se referir aos estados obtidos acima. Em ambos os casos, a porta Hadamard fez com que um qubit em um estado clássico (0 ou 1) entrasse em uma sobreposição "meio-a-meio"de 0 e 1. Tanto em $|+\rangle$ quanto em $|-\rangle$, a probabilidade de se medir 0 é a mesma de se medir 1 (50%).

4.1 Implementação da porta Hadamard

No nosso primeiro código, o seguinte circuito será projetado:

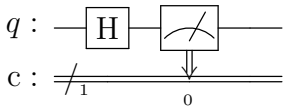


Figura 2: Circuito da porta Hadamard

Neste circuito, uma porta Hadamard é aplicada ao bit quântico q (que inicialmente está no estado $|0\rangle$), o qual é em seguida medido. O valor medido é armazenado na forma de um bit clássico em c. Como Jupyter Notebook é um ambiente interativo, pode-se exibir a saída de uma linha de código individualmente, logo abaixo dela.

Código para a implementação da porta Hadamard

```
1 from qiskit import *
2 circuit = QuantumCircuit(1, 1)
3 circuit.h(0)
4 circuit.measure(0, 0)
```

Na primeira linha do código, importamos todas as funções, classes e módulos da biblioteca Qiskit. Em seguida, criamos um circuito quântico composto por um qubit e um bit clássico. Este é utilizado para armazenar o valor medido para o bit quântico após a aplicação da porta Hadamard. Nas linhas 3 e 4, aplica-se uma porta Hadamard no qubit e uma medição no qubit resultante.

```
7 simulator = Aer.get_backend('qasm_simulator')
8 result = execute(circuit,backend=simulator,shots=10000).result()
```

```
9  from qiskit.tools.visualization import plot_histogram
10 plot_histogram(result.get_counts(circuit))
```

A fim de simular o circuito quântico em nosso computador local, importamos, por meio da linha 7, o simulador, e em seguida executamos a simulação do circuito. Conforme especificado no parâmetro "shots" da função "execute", o circuito foi simulado 10 mil vezes. Usou-se a função "plot_histogram" para visualizar o resultado das simulações em um histograma. Este nos mostra que, em 50,1% das vezes o resultado medido foi 0, e em 49,9% da vezes foi 1. Conforme o esperado, a distribuição dos resultados foi aproximadamente meio a meio (Figura 3a).

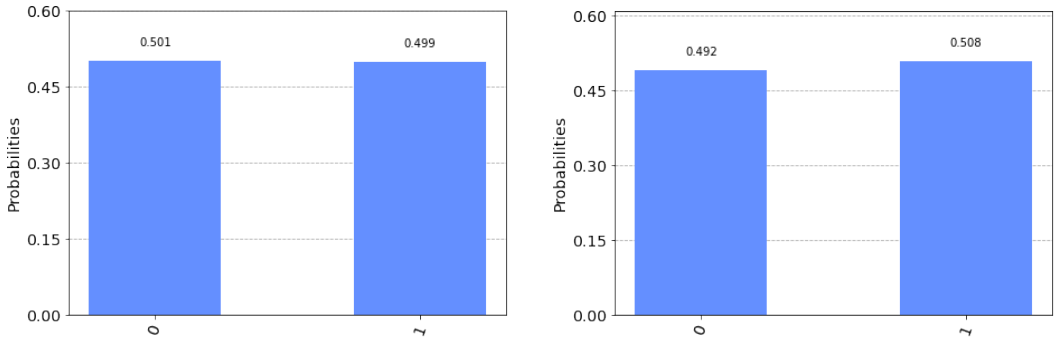
Após a simulação do circuito em nosso coputador local, executamos o circuito remotamente em um dispositivo quântico real da empresa IBM:

```
11 IBMQ.load_account()
12 provider = IBMQ.get_provider('ibm-q')
13 qcomp = provider.get_backend('ibm_oslo')
14 job = execute(circuit, backend = qcomp)
15 from qiskit.tools.monitor import job_monitor
16 job_monitor(job)
17 result = job.result()
18 plot_histogram(result.get_counts(circuit))
```

Para executarmos um circuito em um dispositivo da IBM, precisamos criar uma conta na IBM Quantum Experience e salvar suas informações em nosso computador (esta etapa não será mostrada). Feito isso, devemos carregar nossa conta com o comando "IBMQ.load_account()" sempre que quisermos executar circuitos quânticos remotamente nos computadores da IBM.

O dispositivo escolhido foi "ibm_oslo", constituído por 7 qubits. As linhas 12 e 13 preparam o circuito para ser executado nesse computador. Subsequentemente, o circuito é enviado para ser executado e o resultado da execução é armazenado no objeto "result" (linha 17).

Como não foi passado um valor para o parâmetro "shots" na função da linha 14, o número de execuções foi 4 mil, padrão do dispositivo ibm_oslo. A linha 18 plota a distribuição dos resultados das medições feitas. Em 49,2% das execuções, o qubit colapsou para $|0\rangle$ na etapa de medição e, em 50,8% das vezes, colapsou para $|1\rangle$. Novamente a distribuição está de acordo com o que se esperava: aproximadamente meio a meio (Figura 3b).



(a) Execuções do simulador (b) Execuções reais do ibm_oslo

Figura 3: Distribuição de resultados

5 Considerações finais

Conceitos básicos de física quântica podem ser assimilados de maneira didática por meio da implementação de circuitos quânticos. No trabalho original, foram abordados vários conceitos, contudo apenas o primeiro deles (sobreposição) foi discutido neste resumo. A leitura do trabalho permite que indivíduos com conhecimento básico de álgebra linear e programação sejam introduzidos à mecânica quântica mesmo sem ter experiência prévia em física.

Referências

[1] NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. 10^{th} Anniversary Edition. Cambridge: Cambridge University Press, 2010.

[2] FEYNMAN, R. P. Simulating physics with computers. **International journal of theoretical physics**. 21, 467–488, 1982.

[3] Qiskit contributors, "Qiskit: An Open-source Framework for Quantum Computing", 2023, doi: 10.5281/zenodo.2573505.

[4] IBM. IBM Quantum Experience [Plataforma Online]. Disponível em: https://quantum-computing.ibm.com/. Acesso em: 10 abr. 2023.

[5] YANOFSKY, N. S.; MANNUCCI, M. A. **Quantum Computing for Computer Scientists**. Cambridge: Cambridge University Press, 2008.

O *software* GeoGebra na formação do professor de matemática

Matheus Carvalho Carrijo Silveira
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
matheuscarrijo@ufu.br

Fabiana Fiorezi de Marco Matos
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
fabiana.marco@ufu.br

Érika Maria Chioca Lopes
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
erikalopes@ufu.br

Resumo

Este trabalho é parte de um projeto de pesquisa financiado pela FAPEMIG e tem como objetivo apresentar a oferta de um projeto de extensão sobre o software GeoGebra para professores e futuros professores de matemática. Foram realizados seis encontros em laboratório de informática na UFU, Campus Santa Mônica, possibilitando a instrumentalização dos participantes e a discussão sobre a inserção de tecnologias digitais no processo de ensino-aprendizagem de matemática. Os quatro primeiros encontros foram voltados à familiarização com o software e, os dois últimos procuraram relacionar o software ao ensino de conteúdos matemáticos e suas possibilidades. Ao final dos encontros foram realizadas entrevistas com alguns participantes com o intuito de obter informações acerca do aprendizado ocorrido e da importância de movimentos como esse para a formação dos professores e de futuros professores. As entrevistas ainda estão em análises e serão alvo de discussão em futuro artigo.

Palavras-chave: Educação Matemática, Tecnologias digitais, GeoGebra.

1 Introdução

Apesar de sempre estar cercado de pessoas, mais especificamente, alunos, a profissão do professor é uma profissão solitária. Quando volta para casa, planeja aulas, corrige provas e trabalhos, se dedica a criar propostas para suas turmas e, muitas vezes, não tem com quem compartilhar um desafio ou conquista numa aula. Entende-se solitária pela ausência de uma rede de apoio e diálogo.

A rede de apoio que surge, ganha força atualmente e pode ser analisada de várias perspectivas diferentes. A oficina relatada neste trabalho é um exemplo e pode demonstrar e discutir como essa rede pode influenciar e beneficiar a formação do professor e do futuro professor de matemática, tendo as tecnologias digitais, como o software GeoGebra, como auxiliares no sentido de prepará-los para utilizar essas ferramentas com cautela e proveito.

O uso de tecnologias digitais no processo de ensino-aprendizagem de matemática pode promover uma rede de apoio que auxilie professores e futuros professores. Nesse sentido, apresentamos neste trabalho a oferta de um projeto de extensão, por meio de oficinas sobre o software GeoGebra, para professores e futuros professores de matemática.

2 A Oficina

O projeto de extensão “Oficina: o software GeoGebra na formação do professor de matemática” é parte de um projeto de pesquisa financiado pela FAPEMIG (APQ-03108-17), sendo bolsista de IC o primeiro autor deste texto. O projeto de extensão contou com a colaboração do primeiro autor, da segunda autora, orientadora deste no projeto de pesquisa e das professoras Ana Cláudia Molina Zaqueu Xavier e Érika Maria Chioca Lopes, no sentido de divulgação do projeto e elaboração das oficinas, respectivamente.

Foram realizados 6 encontros às quartas-feiras, das 19h00 às 20h30, no primeiro semestre de 2023, em laboratório de informática na UFU-Campus Santa Mônica, bloco 1B, sala 218 (laboratório 03), o qual dispõe de 23 máquinas.

Das 18 vagas oferecidas, foram reservadas 9 delas para alunos do curso de Matemática, 4 para alunos de graduação de outras áreas e pós-graduação e, 5 para professores que ensinam matemática em qualquer nível de ensino.

As oficinas foram divididas em dois momentos: os quatro primeiros encontros foram voltados ao conhecimento inicial do software e, os dois últimos procuraram relacioná-lo ao ensino de conteúdos matemáticos e suas possibilidades como a criação de propostas, o conhecimentos do GeoGebra Classroom, a discussão dos conhecimentos docentes relacionados às tecnologias digitais e a sua utilização em sala de aula. Ao final dos encontros foram realizadas entrevistas com alguns participantes com o intuito de compreender sobre o aprendizado ocorrido e a importância de movimentos como esse para a formação dos professores e de futuros professores. Tais entrevistas serão alvo de análise em outros artigos.

2.1 Desenvolvimento

Os quatro primeiros encontros se basearam na familiarização dos participantes com o software, ou seja, a apresentação do software GeoGebra, suas ferramentas, potencialidades e possibilidades.

A temática do primeiro encontro foi o Teorema de Morley[1], tendo uma construção relativamente básica em relação à sua execução e às ferramentas usadas, de modo que fosse uma oficina introdutória. O segundo encontro trabalhou a semelhança de triângulos e o Teorema de Tales, introduzindo o

[1] Segundo o Teorema de Morley, em qualquer triângulo, as interseções das trissetrizes adjacentes formam um triângulo equilátero.

controle deslizante do software, além de repetir o uso de muitas ferramentas utilizadas no primeiro encontro.

A temática do terceiro encontro foi a esfera e suas interseções com planos, sendo o objetivo do encontro apresentar a janela 3D e algumas de suas ferramentas, tendo em vista que os dois encontros anteriores e o quarto encontro ocorreram na janela de visualização 2D. O quarto encontro explorou o Triângulo de Reuleaux, exemplo do conceito de figuras de largura constante da geometria plana e pouco conhecido, que inclui muitas ferramentas utilizadas nos encontros anteriores e algumas ferramentas mais sofisticadas, como lugares geométricos por ponto e controles deslizantes, botões de exibir/esconder objetos, criação de retas pelo campo de entrada e botões de programação, que controlam algum movimento na janela de visualização.

No quinto encontro, foi apresentada a plataforma do GeoGebra, a criação de conta nesta, a opção de pesquisar trabalhos publicados por outras pessoas e outros aplicativos que não foram usados nas construções anteriores. Foi trabalhada uma atividade de função definida a partir de parâmetros manipuláveis pelo usuário, com a criação de questões abertas e fechadas, *applets* configurados para os alunos e textos. Em seguida, foi introduzida a tela de criação de tarefa, que pode ser registrada no GeoGebra Classroom e então, explorou-se a tela do professor e seus mecanismos, como ocultar nome dos alunos que entrarem na tarefa, cronometrar e pausar a tarefa, e a tela do aluno, a fim de realizar a exploração completa.

O sexto encontro foi baseado em uma proposta de construção coletiva de atividade, cada participante em um computador criando a sua, mas dessa vez, o ministrante não esteve como tutor da construção, ou seja, não houve passo a passo, por isso na coletividade foi envolvida também participação do ministrante, que circulou entre os participantes, ajudando-os no que era preciso. Foi proposta a construção de uma atividade na plataforma

geogebra.org que proporcionasse a exploração ou investigação de algum conceito matemático pelo aluno por meio de algum tipo de questionário com exercícios acerca do tema, utilizando ferramentas da criação de atividades e tarefas na própria plataforma para inserir essas questões, antecedidas por uma construção.

Os dois últimos encontros objetivaram relacionar as potencialidades do software GeoGebra ao ensino de matemática, por meio da criação de propostas, atividades, GeoGebra Classroom e discussão dos conhecimentos docentes relacionados às tecnologias digitais e à administração do seu uso em sala de aula.

3 Entrevistas

Ao final do último encontro, a fim de obter informações sobre as percepções dos participantes sobre a oficina, foi proposta uma entrevista com participantes voluntários que permitisse aos autores melhor compreender as respostas registradas em um formulário de avaliação sobre o projeto, complementando a avaliação sobre o aprendizado do participante e do impacto para a sua formação.

4 Considerações finais

A proposição da oficina aqui apresentada, parte da IC do primeiro autor, bolsista do projeto FAPEMIG (APQ-03108-17), trata do relato de uma experiência extensionista que envolveu alunos de graduação do curso de Matemática da UFU, alguns alunos de pós-graduação em outras áreas e professores de escolas públicas e particulares, diferentes níveis de ensino, possibilitando diferentes vivências e pontos de vista na oficina, o que com certeza colaborou para o maior desenvolvimento tanto dos participantes quanto do ministrante.

Assim como na pesquisa de Zulatto (2002), acerca da percepção de professores sobre as potencialidades do GeoGebra no ensino de matemática,

os participantes comentaram, durante os encontros da oficina, sobre o impacto do uso de softwares de geometria dinâmica como o GeoGebra em construção, investigação, visualização, dinamismo e motivação de alunos. Os professores mencionaram perceber a relação entre todas essas potencialidades e as oportunidades que surgem no uso delas para *o* e *no* ensino-aprendizagem de matemática.

É importante ressaltar que o professor não é total responsável pela inserção dessas tecnologias na educação, porém é parte fundamental do processo, pois as propostas dentro de sala de aula ocorrem sobre sua supervisão. Além disso, segundo Zulatto (2002), é essencial o professor se aproprie do conhecimento e do propósito de situações como as construídas na oficina.

Agradecimentos

Os autores agradecem o apoio da Fundação de Amparo à Pesquisa do Estado de Minas Gerais pelo fomento em forma de bolsa destinado ao primeiro autor por meio do projeto APQ-03108-17.

Referências

BORBA, Marcelo. PENTEADO, Miriam. **Informática e Educação Matemática.** 1ª ed. Belo Horizonte: Autêntica, 2001.

ZULATTO, R. B. A. **Professores de matemática que utilizam softwares de geometria dinâmica: suas características e perspectivas**. 2002. 316 p. Dissertação (Mestrado). Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista, outubro de 2002.

Investigando como a Modelagem vem sendo mobilizada na Educação do Campo

Andréia Figueredo
UFU, Faculdade de Matemática, Uberlândia, MG, Brasil
andreia.figueredo@ufu.br

Douglas Marin
UFU, Faculdade de Matemática, Uberlândia, MG, Brasil
douglasmarin@ufu.br

Palavras-chave

Encontro Nacional de Educação Matemática.
Análise de Conteúdo.
Modelagem Matemática.

Resumo

Com esse estudo temos o objetivo em ampliar nossas compreensões sobre a Modelagem Matemática e a sua relação com o processo de ensino e aprendizagem nas escolas do campo. Como metodologia usaremos a Análise de Conteúdo, a partir dos anais do Encontro Nacional de Educação Matemática. Apresentamos como resultados algumas considerações sobre os artigos que foram pesquisados.

1 Introdução

O presente relato é um recorte de uma pesquisa[1] mais ampla, que tem como objetivo elaborar um mapeamento de pesquisas brasileiras que abordam o ensino de Matemática em escolas campo. Para esse texto, o objetivo está em elaborar compreensões sobre como a Modelagem Matemática vem sendo mobilizado em escolas do campo no contexto brasileiro.

Para atingir esse objetivo, tomamos como *corpus* analítico os anais[2] dos últimos dez anos do Encontro Nacional de Educação Matemática (ENEM). Escolhemos esse evento pois, ocorre a cada três anos e é organizado pela Sociedade Brasileira de Educação Matemática (SBEM) e, é um local que ocorre grande número de circulação de pesquisas em âmbito nacional e que tem o objetivo de difundir informações e conhecimento sobre o ensino e aprendizagem da Matemática.

Nossas preocupações estão ligadas as escolas campo que estão localizadas no Campo. Entendemos esse espaço, como um lugar cultural, de trabalho e permeado de saberes matemáticos. Nele, a Educação do Campo, apresenta suas especificidades, sua ciência, suas próprias 'matemáticas' que estão presentes na arroba, no milho ou café que são medidos por litro ou por saca, no plantio por palmos e a 'cerca' por passos. Tais saberes e experiências precisam ser valorizados e a matemática ressignificada (FIGUEREDO; MARIN, 2022).

Nesse contexto nossos entendimentos sobre Modelagem Matemática, vão ao encontro de Bassanezi, quando ele diz que ela "[...] consiste na arte de transformar situações da realidade em problemas matemáticos cujas soluções devem ser interpretadas na linguagem do mundo real" (BASSANEZI, 2022, p. 16).

Nesse sentido, Barbosa (2001, p. 29) aponta que as atividades de Modelagem "[...] são consideradas como um meio de indagar e questionar situações reais por meio de métodos matemáticos, evidenciando o caráter cultural e social da matemática".

Uma vez delineado o contexto de nossa pesquisa, passaremos no que segue, a apresentar os procedimentos metodológicos.

2 Procedimentos metodológicos

A pesquisa qualitativa tem o foco em estudar e compreender fenômenos subjetivos, sociais e humanos através da descrição dos autores. Para a composição dos procedimentos metodológicos que utilizamos neste artigo, optamos pela Análise de Conteúdo pois, conforme Bardin (1977), ela contribui para a descrição e interpretação do conteúdo dos textos que são submetidos a uma análise criteriosa e rigorosa.

Segundo Moraes (1999, p. 2), a Análise de Conteúdo conduz a "descrições sistemáticas, qualitativas

[1]Trata-se de uma iniciação científica registrada no Programa de Estudos Tutorado (PET) do curso de Matemática da Universidade Federal de Uberlândia.

[2]As edições estudas foram a XIV ENEM que ocorreu em 2022, edição online; XIII ENEM realizada em 2019, Cuiabá - MT; XII concluída em 2016, São Paulo - SP; XI que aconteceu em 2013, Curitiba – PR.

ou quantitativas, ajuda a reinterpretar as mensagens e a atingir uma compreensão de seus significados num nível que vai além de uma leitura comum".

Assim, a Análise de Conteúdo é um instrumento de análise interpretativa, que com um conjunto de técnicas, busca compreender, interpretar e explicar o conteúdo da mensagem contribuindo para a construção do conhecimento após o tratamento dos dados.

Após as primeiras inspirações que fomentaram nossas intenções de pesquisa, passamos por constituir o *corpus*[3] de análise. Como consideramos inviável a leitura na íntegra de todos os artigos[4] publicados nos anais dos ENEMs, iniciamos a construção de filtros de seleção. Para essa pesquisa, selecionamos trinta e dois textos, com os seguintes filtros: "Educação do/no campo", "escola do campo" e "escola rural". A aplicação dos filtros deu-se, primeiramente, nos títulos dos artigos e, posteriormente nos artigos todos.

Em posse dos artigos fizemos a leitura integral e para o agrupamento excluimos os textos que não traziam no título a Modelagem Matemática, assim foram selecionados quatro[5] que dialogam que mobilizam a Modelagem Matemática com a escola do campo. Os quais passamos a expor na próxima sessão.

3 Análise

Tabela 1: Título, autores e edição ENEM

Título	**autores**	**código**
Modelagem matemática na educação do campo: alunas(os) em movimento	Maria Carolina Machado Magnus (UFSC)	13.1
Enlaces entre Modelagem Matemática, estágio supervisionado e educação do campo: relato de Uma experiência formativa	Matheus Cardoso da Cunha (UFSC) Débora Regina Wagner (UFSC)	13.2
Etnomodelagem e Educação do Campo: Tecendo saberes	Luana Oliveira Moreira de Jesus (UESC) Zulma Elizabete de Freitas Madruga (UFRB)	14.3
Modelagem Matemática na Educação do Campo: implicações sociais	Kátia da Costa Leite (UFSC) Everaldo Silveira (UFSC)	14.4

Fonte: Dados da pesquisa

[3]"O corpus é o conjunto dos documentos tidos em conta para serem submetidos aos procedimentos analíticos" (BARDIN, 1977, p.96).

[4]Entendemos por artigo as comunicações científicas, os relatos de experiência, os pôsteres, as conferências, as palestras, os minicursos e os textos referentes às mesas redondas. Todos os textos que compõem os anais foram considerados artigos.

[5]Observamos que usando essas palavras-chave, não foram localizados artigos no XI ENEM e XII ENEM.

Organizamos os QUATRO artigos selecionados em uma tabela (Tabela 1), explicitando seus títulos, autores e um código[6] de identificação.

Ao analisar os artigos selecionados percebemos indícios em que a Modelagem vem sendo mobilizada em escolas do campo. Como foi o caso do artigo 13.1, que tem como cenário uma disciplina de curso de Licenciatura em Educação do Campo, onde o autora discute a contribuição para a "visibilidade e compreensão da realidade campesina em seus diversos aspectos: sociais, culturais, políticos, econômicos, gênero, geração, etnia, ... Possibilitando, desta maneira, discussões sobre as práticas cotidianas das(os) sujeitas(os) do campo e, principalmente, como a matemática pode auxiliá-los(as) nos estudos destas".

O relato de experiência de Estágio Supervisionado, no artigo 13.2, tem o objetivo de relacionar a matemática e a agroecologia por meio da Modelagem Matemática, que contribui para que gradativamente se vá superando o tratamento estanque e compartimentalizado que tem caracterizado o seu ensino nesses espaços, favorecendo a ação investigativa como forma de conhecer, compreender, atuar e transformar a realidade em que vivem.

O objetivo do artigo 14.3, está em investigar as pesquisas realizadas sobre Etnomodelagem nas relações estabelecidas com a Educação do Campo, a partir de levantamento de pesquisas publicadas na CAPES[7] , na BDTD[8] e no ENEM[9] . Para as autoras a Etnomodelagem é um caminho que pode possibilitar o envolvimento dos estudantes em práticas formativas, considerando o campo como local de produção de conhecimento, o que pode contribuir na valorização da identidade dos educandos como camponeses.

Por fim, o texto 14.4 também vai nessa direção e busca em teses e dissertações, o desenvolvimento de atividades de Modelagem no âmbito da educação básica em escolas do campo e discussões das práticas desenvolvidas. Os autores apontam que na Modelagem os estudantes têm a oportunidade de construir o conhecimento matemático a partir de temas do seu interesse e, portanto, pode contribuir com sua vida e trabalho nas propriedades rurais, ao usar temas que envolvam a produção agrícola, ou mesmo a gestão da propriedade rural.

4 Considerações finais

Nesse relato elaboramos uma síntese de uma pesquisa, em que teve o propósito de apresentar compreensões sobre como a Modelagem Matemática vem sendo mobilizada em escolas do campo no contexto brasileiro. E mesmo com a escassez de trabalhos na temática, notamos que a Modelagem Matemática é um metodologia que articula com o ensino pautado na construção do conhecimento e na

[6]Os códigos devem ser entendidos da seguinte forma: o número anterior ao ponto refere-se à edição do evento, isto é, o número 13 diz respeito à 13ª edição do ENEM; e o número após o ponto à numeração do artigo que fizemos aqui, de 1 a 4 (visto que 4 é o total de artigos selecionados), iniciando dos eventos mais antigos para os mais recentes.

[7]CAPES - Catálogo de Teses e Dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

[8]BDT - Biblioteca Digital Brasileira de Teses e Dissertações.

[9]ENEM - Encontro Nacional de Educação Matemática (2010 – 2019).

valorização dos saberes dos estudantes campesinos.

Agradecimentos

Na condição de bolsista do PET Matemática da Universidade Federal de Uberlândia, agradeço ao Programa de Eduação Tutorial da SESu/MEC pelo fomento.

Referências

[1] BARBOSA, J. **Modelagem matemática**: concepções e experiências de futuros professores. 2001. Tese (Doutorado em Educação Matemática) – Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista, Rio Claro, 2001.

[2] BARDIN, L. **Análise de Conteúdo**. Lisboa: Edições 70, 1977.

[3] BASSANEZI, R.C. **Ensino-aprendizagem com modelagem matemática**: uma nova estratégia. São Paulo: Contexto, 2002.

[4] FIGUEREDO, A; MARIN, D. Relações entre a Educação do Campo e a Educação Matemática. In: XXII SEMAT e XII SEMEST, 2022, Uberlândia. **Anais** eletrônicos [....] Minas Gerais: Uberlândia, 2022. p. 24-28. Disponível em: <https://sites.google.com/view/anais-da-semat-e-semest/home/edi%C3%A7%C3%A3o-atualh.qt9hbb91qey5>. Acesso em: 31 mar. 2023

[5] MORAES, R. Análise de conteúdo. **Revista Educação** , Porto Alegre: PUC- RS, v. 22, n. 37, p. 7-32, 1999

Oferta e Demanda

Maria Cecilia Alcântara Neiva Cunha
Escola Estadual Antônio Thomaz Ferreira de Rezende, Uberlãndia, MG, Brasil
ceciliaalc13@gmailcom

Hernán Roberto Montúfar López
UFU, Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, MG, Brasil
montufar@ufu.br

Palavras-chave

Oferta.
Demanda.
Equilibrio de Mercado.

Resumo

Neste trabalho focaremos um aspecto particular conhecido como equilíbrio de mercado, no qual oferta e demanda se equilibram. Desta forma apresentamos as condições de oferta e o comportamento da demanda em diferentes situações. Primeramente descrevemos o comportamento da curva de demanda, estudaremos as suas características, determinantes e procura de mercado. Analogamente faremos para a curva da oferta. Finalmente, em economia para definir um preço criamos um equilíbrio para cada mercado.

1 Introdução

Uma **função** é uma relação de dependência entre duas ou mais variáveis em que a cada valor da variável independente associamos um único valor da variável dependente. Agora a quantidade demandada Q de um bem depende de varios fatores, incluindo: o preço do mercado, P, Renda dos consumidores, Y, o preço de produtos substituíveis, P_s, o preço de produtos complementares, P_c, os gastos com propaganda, P_p e preferência dos consumidores, C. Matematicamente, temos a **função demanda** que é a relação entre a quantidade demandada e vários fatores que afetam a demanda, [1].

$$Q = f(P, Y, P_s, P_c, P_p, C).$$

Neste caso específico, podemos assumir implicitamente que as variáveis Y, P_s, P_c, P_p e C são fixas e as chamaremos de **variáveis exógenas**, por serem constantes e estarem fora do modelo. As variáveis Q e P as chamaremos de **variáveis endógenas**, por poderem variar e estar dentro do modelo. Podemos expresar isso da seguinte forma: $Q = f(P)$. Uma vez que Q está relacionado com P, inversamente P deve estar relacionado com Q:

$$Q = f(P) \quad \Rightarrow \quad P = g(Q).$$

As duas funções, f e g, são funções inversas. Em muitas funções microeconômicas como receita orçamentaria, custo médio e lucro, é convencional representá-las graficamente com Q no eixo horizontal, então faz sentido fazer o mesmo aqui.

A **função oferta** é a relação entre a quantidade ofertada e os diversos fatores que afetam a oferta. Portanto, temos

$$Q = f(P, T, K, L, E, L_A, T_e),$$

onde: Q é a quantidade ofertada,P é o preço do mercado, T a terra, K o capital, L o trabalho, E o empreendimento, L_A os lucros obtidos com bens alternativos e T_e a tecnologia. Consideremos o caso em que P e Q são variáveis endógenas e as outras variáveis sejam exógenas, $P = f(Q)$, então a função oferta é a relação entre a quantidade, Q, de um bem que os produtores planejam trazer ao mercado ao preço, P, do bem.

Neste trabalho será discutido e analisado o caso linear da função oferta e função demanda. Para isso, utilizamos

- **Oferta:** $P = aQ + b$ com $a > 0$ e $b > 0$.
- **Demanda:** $P = cQ + d$ com $c < 0$ e $d > 0$.

A figura 1 indica uma curva linear típica de oferta. A teoria econômica indica que, quando o preço cresce a oferta também cresce. Matematicamente, P é considerado uma **função crescente** de Q.

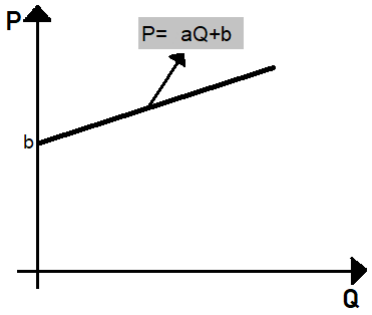


Figura 1: Análise gráfica de $P = aQ + b$.

A figura 2 mostra um gráfico de uma função demanda linear típica. A teoria elementar nos mostra que a demanda geralmente cai quando o preço de um bem aumenta, e então a inclinação da reta é negativa. Matematicamente, P é então uma ***função decrescente*** *de Q*

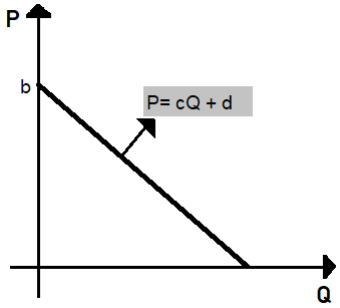


Figura 2: Análise gráfica de $P = cQ + d$.

Comparando esses dois gráficos, obtemos o equilíbrio da oferta e demanda.

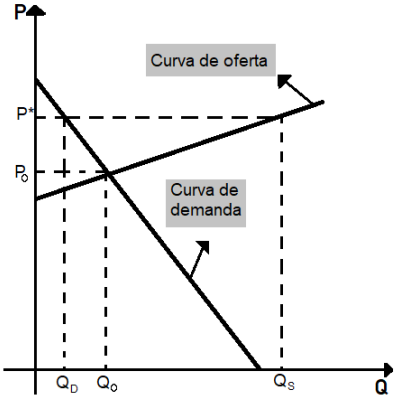


Figura 3: Análise gráfica do equilíbrio

Exemplo: As funções oferta e demanda de um bem são dadas por:

$$\begin{cases} P = -5Q_D + 80 \\ P = \ \ 2Q_S + 10 \end{cases}$$

onde P, Q_D e Q_S indicam respectivamente, preço, quantidade demandada e quantidade ofertada. Encontremos o preço e quantidade de equílibrio: algebricamente e graficamente. Agora, se o governo diminuir em 15% o imposto do preço de mercado de cada bem, determinamos o novo preço e a nova quantidade de equilíbrio.
Em equilíbrio temos: $Q_D = Q_S$. Então

$$\begin{cases} P = -5Q_D + 80 \\ P = \ \ 2Q_S + 10 \end{cases} \Rightarrow -5Q + 80 = 2Q + 10 \Rightarrow Q = 10$$

De onde $P = 2(10) + 10 \Rightarrow P = 30$.

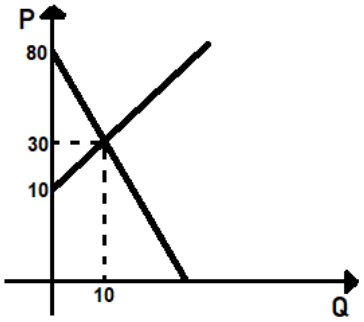


Figura 4: Análise gráfica de $P = -5Q_D + 80$ e $P = 2Q_S + 10$.

Se o imposto diminui 15%:

$$\begin{cases} P = -5Q_D + 80 \\ P - 15 = \ \ 2Q_S + 10 \end{cases} \Rightarrow -5Q + 80 = 2Q + 10 + 15 \Rightarrow Q = 7,85$$

De onde $P = 2(7,85) + 10 + 15 \Rightarrow P = 40,7$.

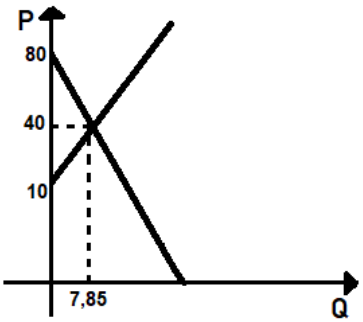


Figura 5: Análise gráfica de $P = -5Q_D + 80$ e $P - 15 = 2Q_S + 10$.

2 Duas commodities independentes

Nesta seção, abordamos um modelo mais realista de oferta e demanda, considerando a substitutibilidade e complementaridade de bens. Suponhamos que haja dois bens relacionados, chamados de bem 1 e bem 2, e que a demanda por cada bem dependa dos preços tanto do bem 1 quanto do bem 2. Se as funções de demanda forem lineares, podemos expressá-las da seguinte forma:

$$Q_{D_1} = a_1 + b_1 P_1 + c_1 P_2.$$

$$Q_{D_2} = a_2 + b_2 P_1 + c_2 P_2.$$

Nessas equações, P_1 e P_2 representam os preços do bem 1 e do bem 2, respectivamente, e Q_{D_1} e Q_{D_2} representam as quantidades demandadas de cada bem. Os parâmetros a_1, b_1, c_1, a_2, b_2, e c_2 são constantes que influenciam a demanda. Podemos inferir algumas características dos bens com base nos sinais dos parâmetros. Por exemplo, $a_1 > 0$, pois há uma demanda positiva quando o preço de ambos os bens é zero. O parâmetro b_1 é negativo, pois a demanda por um bem tende a diminuir quando seu preço aumenta. O sinal de c_1 depende da natureza dos bens. Se os bens são substituíveis, c_1 será positivo, indicando que um aumento no preço do bem 2 levará os consumidores a mudarem para o bem 1, resultando em um aumento na quantidade demandada de bem 1. Por outro lado, se os bens forem complementares, c_1 será negativo, pois um aumento no preço de ambos os bens levará a uma diminuição na demanda. Resultados semelhantes se aplicam aos sinais dos parâmetros a_2, b_2 e c_2. O cálculo do preço e da quantidade de equilíbrio em um modelo de mercado com dois bens será demonstrado no próximo exemplo.

Exemplo: As funções demanda e oferta para dois bens interpendentes são dadas por

$$\begin{cases} Q_{D_1} = 50 - 2P_1 + P_2 \\ Q_{D_2} = 10 + P_1 - 4P_2 \\ Q_{S_1} = -20 + P_1 \\ Q_{S_2} = -10 + 5P_2 \end{cases};$$

Mostremos que os preços de equilíbrio satisfazem $\begin{pmatrix} 3 & -1 \\ -1 & 9 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 70 \\ 20 \end{pmatrix}$, e encontremos o inverso da matriz 2×2 para depois determinar os preços de equilíbrio.
Reagrupando as equações de oferta e demanda temos:

$$\begin{cases} Q_{D_1} = 50 - 2P_1 + P_2 \\ Q_{S_1} = -20 + P_1 \end{cases} \quad e \quad \begin{cases} Q_{D_2} = 10 + P_1 - 4P_2 \\ Q_{S_2} = -10 + 5P_2 \end{cases};$$

$$\begin{cases} Q_{D_1} = Q_{S_1} \quad \Rightarrow \quad 50 - 2P_1 + P_2 = -20 + P_1 \quad \Rightarrow \quad -3P_1 + P_2 = -70 \\ Q_{D_2} = Q_{S_2} \quad \Rightarrow \quad 10 + P_1 - 4P_2 = -10 + 5P_2 \quad \Rightarrow \quad P_1 - 9P_2 = -20 \end{cases};$$

$$\begin{cases} -3P_1 + P_2 = -70 \\ P_1 - 9P_2 = -20 \end{cases} \Rightarrow \begin{pmatrix} 3 & -1 \\ -1 & 9 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 70 \\ 20 \end{pmatrix}$$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ -1 & 9 \end{pmatrix}^{-1} \begin{pmatrix} 70 \\ 20 \end{pmatrix}.$$

Se $A = \begin{pmatrix} 3 & -1 \\ -1 & 9 \end{pmatrix} \Rightarrow \begin{pmatrix} 3 & -1 & 1 & 0 \\ -1 & 9 & 0 & 1 \end{pmatrix} \backsim \begin{pmatrix} -1 & 9 & 0 & 1 \\ 3 & -1 & 1 & 0 \end{pmatrix} \backsim \begin{pmatrix} 1 & -9 & 0 & -1 \\ 3 & -1 & 1 & 0 \end{pmatrix} \backsim$
$\begin{pmatrix} 1 & -9 & 0 & -1 \\ 0 & 26 & 1 & 3 \end{pmatrix} \backsim \begin{pmatrix} 1 & -9 & 0 & -1 \\ 0 & 1 & 1/26 & 3/26 \end{pmatrix} \backsim \begin{pmatrix} 1 & 0 & 9/26 & 1/26 \\ 0 & 1 & 1/26 & 3/26 \end{pmatrix} \Rightarrow A^{-1} = \begin{pmatrix} 9/26 & 1/26 \\ 1/26 & 3/26 \end{pmatrix}.$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = 1/26 \begin{pmatrix} 9 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 70 \\ 20 \end{pmatrix} = 1/26 \begin{pmatrix} 650 \\ 130 \end{pmatrix}. \qquad Logo: \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 25 \\ 5 \end{pmatrix}.$$

3 Conclusão

Em sua essência o mercado é um grupo de indivíduos que compram e vendem determinados bens ou serviços. A oferta, por sua vez, diz respeito à quantidade de produto que os vendedores desejam e estão dispostos a disponbilizar para venda. Dessa forma, a oferta é influenciada por fatores como insumos, tecnologia, custo de produção entre outros. Por outro lado, a demanda refere-se à quantidade de produto que os consumidores querem e estão dispostos a adquirir. Em outras palavras, a demanda é determinada pelos compradores e é influenciada por fatores como renda dos consumidores, preços, produtos similiares e substitutos, dentre outros. O Equilíbrio de mercado acontece quando a quantidade de bens e serviços que os consumidores desejam comprar é igual à quantidade de bens e serviços que os produtores desejam vender, resultando em um cenário sem excesso ou escassez de oferta ou demanda.

Agradecimentos

O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil (CNPq) através do programa PIBIC-EM.

Referências

[1] Ian Jacques-Mathematics for Economics and Business (5ª Edição)-Prentice Hall (2006).

Transformações geométricas do plano no plano e suas matrizes associadas

Luiz Fernando Goulart Fonseca Junior
E. E. Frei Egídio Parisi, Uberlândia, Minas Gerais, Brasil
luizgamer362.com@gmail.com

Ana Paula Tremura Galves
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
ana.galves@ufu.br

Palavras-chave

Palavra-chave 1. Transformações geométricas
Palavra-chave 2. Matrizes
Palavra-chave 3. Plano cartesiano

Resumo

Transformações geométricas do plano no plano são operações fundamentais da geometria que estuda as mudanças de forma, posição e orientação de objetos no plano. Essas transformações podem ser usadas em diversas aplicações práticas, como engenharia, computação gráfica, física, matemática e outras áreas de ciência e tecnologia. O objetivo deste trabalho é fornecer uma visão geral das transformações geométricas do plano no plano e explorá-las por meio de suas matrizes associadas.

1 Introdução

As transformações geométricas do plano no plano são operações que alteram a posição, orientação, forma ou tamanho dos objetos geométricos no plano, enquanto mantém a propriedade de que as linhas retas permanecem retas.

Este trabalho irá abordar as seguintes transformações geométricas definidas no plano cartesiano: expansão, contração e escala não uniforme, reflexões em torno dos eixos coordenados, reflexão em torno da origem, reflexão em torno da reta $y = x$, translação e rotações em torno de um ponto fixo no sentido horário e no sentido anti–horário. Em seguida serão utilizadas matrizes para representar cada uma dessas transformações geométricas. Conceituaremos translação, uma transformação que não pode ser representada através de matrizes. Todas essas transformações geométricas serão apresentadas com um exemplo geométrico para facilitar a compreensão.

2 Representação matricial das transformações do plano

O objetivo desta seção é mostrar, de maneira intuitiva, como é possível representar as transformações geométricas do plano através de matrizes de ordem 2×2. Vale observar também que certas transformações não podem ser representadas por uma matriz, como será justificado mais adiante.

Exemplo 2.1. *Considere a matriz A de ordem 2×2 dada por $A = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}$ e a transformação do plano numérico, denotada por $T : \mathbb{R}^2 \to \mathbb{R}^2$, definida pela matriz A, que leva o ponto $P = (a, b)$ no ponto $Q = (c, d)$ definida da seguinte forma $\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix} . \begin{bmatrix} a \\ b \end{bmatrix}$.*
Assim $T(P) = Q$, ou seja, $T(a, b) = (c, d)$. O ponto Q é a imagem do ponto P pela transformação T.

Por exemplo, dado o ponto $P = (3, 2)$ a sua imagem pela transformação T, definida pela matriz A, é o ponto $Q = (4, 1)$.

As transformações do plano no plano definidas através de uma matriz de ordem 2×2, como no exemplo acima, tem duas propriedades bem particulares que são dadas por:
(a) $T(P_1 + P_2) = T(P_1) + T(P_2)$, para todo $P_1, P_2 \in \mathbb{R}^2$.
(b) $T(\lambda P) = \lambda T(P)$, para todo $P \in \mathbb{R}^2$ e $\lambda \in \mathbb{R}$.

Transformações do plano no plano que possuem estas duas propriedades são denominadas **transformações lineares**.

De um modo geral, pode-se representar as transformações lineares na forma matricial.

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix}$.

Logo, a transformação T é representada pela matriz $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$.

Nas subseções a seguir serão apresentadas as transformações geométricas do plano no plano e as matrizes de ordem 2×2 a elas associadas. Em cada caso, será explicitado um exemplo geométrico para melhorar o entendimento.

2.1 Expansão, contração e escala não uniforme

Definição 2.2. *Considere o plano cartesiano $\mathbb{R}^2$ e um escalar $\lambda \in \mathbb{R}$ fixo. A transformação $T : \mathbb{R}^2 \to \mathbb{R}^2$, dada por $T(x, y) = \lambda(x, y) = (\lambda x, \lambda y)$ é uma **contração** para $|\lambda| < 1$. Quando $|\lambda| > 1$, dizemos que T é uma **expansão**.*

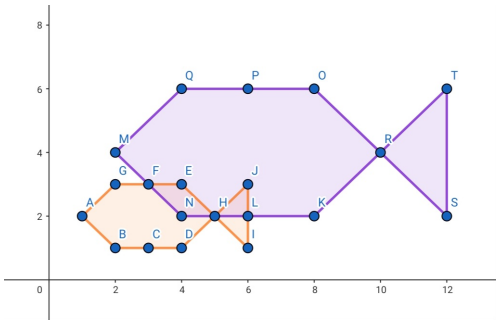


Figura 1: Exemplo de expansão com $\lambda = 2$.

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \lambda x \\ \lambda y \end{bmatrix}$.

Assim, a transformação T é representada pela matriz $\begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$.

Se na transformação da Definição 2.2 ocorrer $T(x, y) = (\lambda_1 x, \lambda_2 y)$, com $\lambda_1, \lambda_2 \in \mathbb{R}$ escalares fixos, porém arbitrários, tal transformação é denominada **escala**. Dizemos que a transformação é uma **escala não uniforme** quando λ_1 é diferente de λ_2, e dizemos que é uma **escala uniforme** quando $\lambda_1 = \lambda_2$. Note que na escala uniforme podemos ter uma contração ou uma expansão. Nesse caso, a escala é representada pela matriz $\begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$.

2.2 Reflexões em torno dos eixos coordenados

Definição 2.3. *Considere o plano cartesiano $\mathbb{R}^2$. A transformação $T : \mathbb{R}^2 \to \mathbb{R}^2$, definida por $T(x, y) = (x, -y)$ é denominada uma **reflexão em torno do eixo x**.*

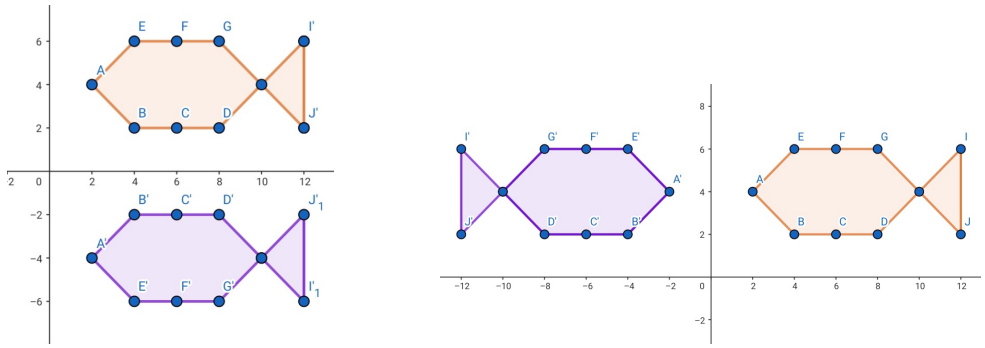
Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}$.

Deste modo, a reflexão em torno do eixo x é representada pela matriz $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Definição 2.4. *Considere o plano cartesiano* $\mathbb{R}^2$. *A transformação* $T : \mathbb{R}^2 \to \mathbb{R}^2$, *definida por* $T(x, y) = (-x, y)$ *é denominada uma* ***reflexão em torno do eixo y***.

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ y \end{bmatrix}$.

Logo, a reflexão em torno do eixo y é representada pela matriz $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$.



(a) Reflexão em torno do eixo x

(b) Reflexão em torno do eixo y

Figura 2: Exemplos de reflexões em torno dos eixos coordenados.

2.3 Reflexão em torno da origem e em torno da reta $y = x$

Definição 2.5. *Considere o plano cartesiano* $\mathbb{R}^2$. *A transformação* $T : \mathbb{R}^2 \to \mathbb{R}^2$, *definida por* $T(x, y) = (-x, -y)$ *é denominada uma* ***reflexão em torno da origem***.

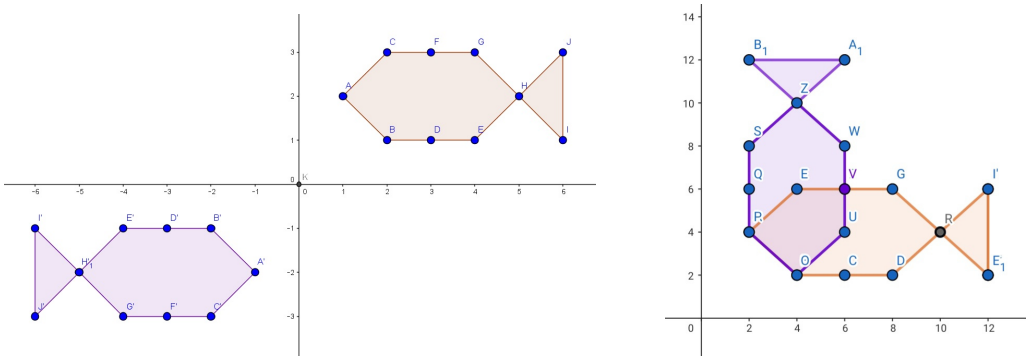
Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ -y \end{bmatrix}$.

Logo, a reflexão em torno da origem é representada pela matriz $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

Definição 2.6. *Considere o plano cartesiano* $\mathbb{R}^2$. *A transformação* $T : \mathbb{R}^2 \to \mathbb{R}^2$, *definida por* $T(x, y) = (y, x)$, *é denominada uma* ***reflexão em torno da reta y=x***.

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} y \\ x \end{bmatrix}$.

Deste modo, a reflexão em torno da reta $y = x$ é representada pela matriz $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.



(a) Reflexão em torno da origem (b) Reflexão em torno da reta y=x

Figura 3: Exemplos de reflexão em torno da origem e em torno da reta y=x.

2.4 Translação

Definição 2.7. *Considere o plano cartesiano* $\mathbb{R}^2$ *e um elemento fixo, porém arbitrário,* $(a, b) \in \mathbb{R}^2$. *A transformação* $T : \mathbb{R}^2 \to \mathbb{R}^2$, *dada por* $T(x, y) = (x, y) + (a, b) = (x + a, y + b)$ *é denominada uma* ***translação***.

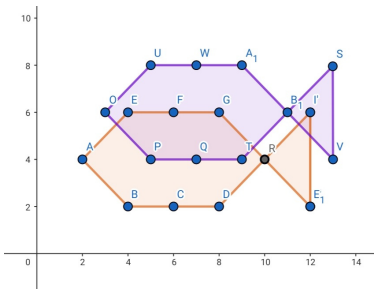


Figura 4: Exemplo de translação com $(x, y) = (2, 1)$ e $(a, b) = (1, 2)$.

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x + a \\ y + b \end{bmatrix}$.

Podemos verificar facilmente que a translação não é uma transformação linear, pois não transforma a origem nela mesma. Assim, não podemos representá–la através de uma matriz. A translação é denominada uma transformação afim.

2.5 Rotação

Definição 2.8. *Considere o plano cartesiano* $\mathbb{R}^2$. *A transformação geométrica* $T : \mathbb{R}^2 \to \mathbb{R}^2$, *definida por* $T(x, y) = (xcos(\theta) - ysen(\theta), xsen(\theta) + ycos(\theta))$ *é denominada uma* ***rotação de um ângulo*** θ ***no sentido anti–horário*** *e de centro na origem do sistema de coordenadas.*

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix}$.

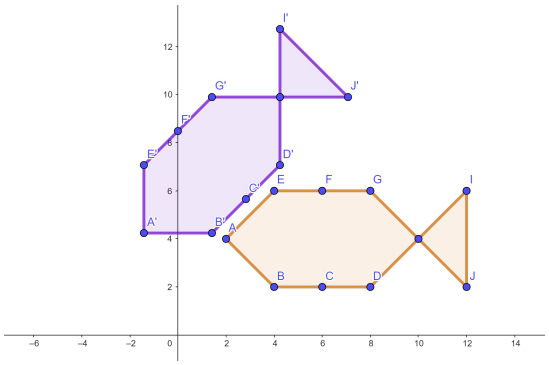


Figura 5: Exemplo de rotação de um ângulo $\theta = 45°$ no sentido anti–horário.

Assim, a rotação de um ângulo θ no sentido anti–horário é representada pela matriz $\begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix}$, denominada **matriz de rotação**.

3 Considerações finais

As transformações geométricas têm uma ampla gama de aplicações em diversas áreas. As principais áreas de aplicação incluem modelagem 3D, animação, processamento de imagem, realidade aumentada, desenvolvimento de jogos e sistemas de navegação. O estudo das transformações geométricas e suas aplicações pode levar a avanços significativos em áreas como a computação gráfica, engenharia, arquitetura, física e outras áreas relacionadas.

Agradecimentos

Na condição de bolsista do Programa Institucional de Bolsas de Iniciação Científica da Universidade Federal de Uberlândia, agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo fomento.

Referências

[1] HAZZAN, S.; IEZZI, G. **Fundamentos de matemática elementar - Sequências, Matrizes, Determinantes e Sistemas**. Volume 4. São Paulo: Editora Atual, 1977.

[2] PULINO, P.; RODRIGUES, C. I. **Transformações geométricas: aplicação nos movimentos de braços robóticos**. 2017. 128 p. Ciência e arte nas férias - Instituto de Matemática Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2017.

A cinemática e o movimento de um braço robótico

Maria Eduarda de Lima Diniz
E. E. Antônio Thomaz Ferreira de Rezende, Uberlândia, Minas Gerais, Brasil
dudalima0210@gmail.com

Ana Paula Tremura Galves
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
ana.galves@ufu.br

Palavras-chave

Palavra-chave 1. Cinemática direta
Palavra-chave 2. Cinemática inversa
Palavra-chave 3. Robótica

Resumo

Cinemática é o estudo dos movimentos sem levar em conta as causas que os geram, ou seja, sem considerar as forças envolvidas. A cinemática é fundamental em muitas áreas da engenharia e ciência, incluindo robótica, mecânica, física, entre outras. Nesse contexto, a cinemática direta e a cinemática inversa são dois conceitos importantes para a análise de movimentos em sistemas mecânicos. O objetivo deste trabalho é utilizar a cinemática em exemplos de movimentos de um braço robótico com dois graus de liberdade.

1 Introdução

A cinemática direta e a cinemática inversa são dois conceitos importantes na análise de movimentos em sistemas mecânicos. A cinemática direta é usada para determinar a posição, a velocidade e a aceleração de um objeto ou sistema com base em seus parâmetros geométricos e dinâmicos. Já a cinemática inversa é usada para calcular as configurações necessárias para que um objeto ou sistema alcance uma determinada posição desejada.

Na prática, a cinemática direta e a cinemática inversa são usadas em conjunto para controlar o movimento de sistemas mecânicos. Por exemplo, um robô pode ser programado para seguir uma trajetória específica, usando a cinemática direta para determinar a posição, a velocidade e a aceleração em cada ponto da trajetória. Em seguida, a cinemática inversa é usada para calcular as configurações das juntas do braço robótico que permitem que ele siga a trajetória desejada.

Este trabalho tem como objetivo apresentar brevemente os conceitos de cinemática direta e de cinemática inversa e aplicá-los em exemplos de movimento de um braço robótico com dois graus de liberdade.

As principais referências utilizadas no trabalho são [1] e [2].

2 Cinemática Direta

Na robótica, a cinemática direta é usada para determinar a posição final de um braço robótico, com base nas coordenadas do ponto de origem, no comprimento dos braços e na orientação das juntas.

Conhecendo as coordenadas do ponto P e o ângulo θ, vamos determinar as coordenadas do ponto P', isto é, vamos obter a matriz de rotação. Para auxiliar na dedução da matriz de rotação, denotamos por r o comprimento dos segmentos $0P$ e $0P'$, isto é, $r = \overline{OP} = \overline{OP'}$. Utilizamos para a dedução da matriz de rotação, basicamente, as relações trigonométricas no triângulo retângulo, seno e cosseno da soma de dois ângulos.

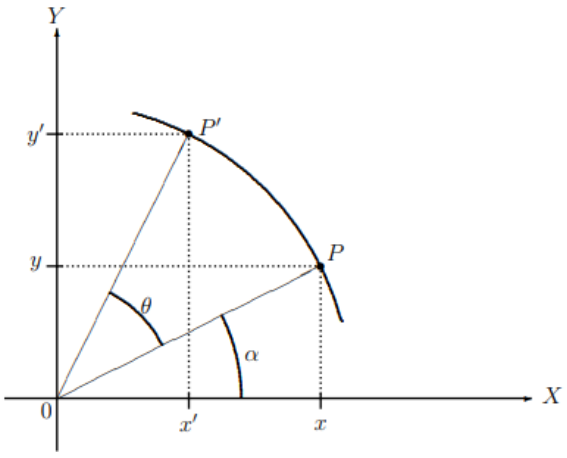


Figura 1: Rotação de um ângulo θ no sentido anti-horário.

Na Figura 1, temos os pontos $P = (x, y)$, $P' = (x', y')$, $A = (x, 0)$ e $A' = (x', 0)$. Assim, utilizando relações trigonométricas nos triângulos retângulos $0PA$ e $0P'A'$, obtemos

$$\begin{cases} x &= rcos(\alpha) \\ y &= rsen(\alpha) \end{cases} \quad e \quad \begin{cases} x' &= rcos(\alpha + \theta) \\ y' &= rsen(\alpha + \theta) \end{cases}$$

Utilizando agora, as relações para seno e cosseno da soma de dois ângulos, temos

$$x' = rcos(\alpha)cos(\theta) - rsen(\alpha)sen(\theta) = xcos(\theta) - ysen(\theta). \tag{1}$$

$$y' = rsen(\alpha)cos(\theta) + rcos(\alpha)sen(\theta) = xsen(\theta) + ycos(\theta). \tag{2}$$

Assim, temos a seguinte definição:

Definição 2.1. *Considere o plano cartesiano $\mathbb{R}^2$. A transformação geométrica $T : \mathbb{R}^2 \to \mathbb{R}^2$, definida por $T(x, y) = (xcos(\theta) - ysen(\theta), xsen(\theta) + ycos(\theta))$ é denominada uma* ***rotação de um ângulo*** *θ* ***no sentido anti–horário*** *e de centro na origem do sistema de coordenadas.*

Dado um ponto $P = (x, y) \in \mathbb{R}^2$ a sua imagem, denotada pelo ponto $P' = (x', y')$, pela transformação T é definida da forma $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix} . \begin{bmatrix} x \\ y \end{bmatrix}$.

Logo, a rotação de um ângulo θ no sentido anti-horário é representada pela matriz $\begin{bmatrix} cos(\theta) & -sen(\theta) \\ sen(\theta) & cos(\theta) \end{bmatrix}$, denominada **matriz de rotação**.

É importante observar, uma vez que estamos realizando uma rotação, que as coordenadas dos pontos $P = (x, y)$ e $P' = (x', y')$ satisfazem a seguinte equação

$$x^2 + y^2 = (x')^2 + (y')^2. \tag{3}$$

3 Cinemática Inversa

Na robótica a cinemática inversa é uma técnica utilizada para determinar as posições das juntas de um braço robótico a partir da posição final desejada do efetuador. Ela é fundamental em aplicações de programação de robôs, permitindo que o operador do robô especifique uma posição desejada para o efetuador e o controlador do robô determine as posições das juntas necessárias para alcançar essa posição.

Pelas equações (1) e (2), temos $x' = xcos(\theta) - ysen(\theta)$ e $y' = xsen(\theta) + ycos(\theta)$.

Multiplicando a primeira equação anterior por x e multiplicando a segunda equação anterior por y , obtemos

$$xx' = x^2cos(\theta) - xysen(\theta) \quad \text{e} \quad yy' = xysen(\theta) + y^2cos(\theta).$$

Somando membro a membro as duas equações acima, ficamos com

$$xx' + yy' = (x^2 + y^2)cos(\theta) \tag{4}$$

Finalmente da equação (4), obtemos

$$cos(\theta) = \frac{xx' + yy'}{x^2 + y^2} \iff \theta = \pm arccos\left(\frac{xx' + yy'}{x^2 + y^2}\right). \tag{5}$$

Assim, conhecendo os pontos $P = (x, y)$ e $P' = (x', y')$ que satisfazem a equação (3), obtemos o ângulo θ com o qual realizamos a rotação. Note que a escolha do sinal do ângulo θ depende se realizamos uma rotação no sentido horário ou no sentido anti-horário.

4 Aplicações da cinemática direta e da cinemática inversa

Serão apresentados três exemplos simples para ilustrar a cinemática direta e a cinemática inversa em movimento de um braço robótico com dois graus de liberdade.

Exemplo 4.1. *Sejam $P = (x, y) = (\sqrt{2}, \sqrt{2})$ e $P' = (x', y') = (0, 2)$ pontos que satisfazem a condição dada pela equação (3), como ilustra a Figura 2. Vamos determinar o ângulo θ com o qual podemos realizar uma rotação entre os pontos.*

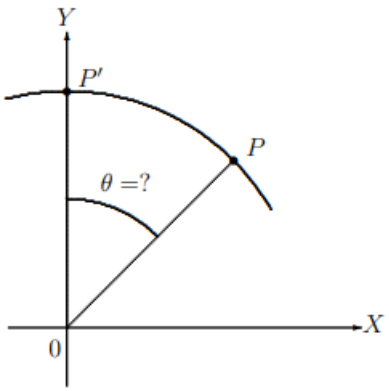


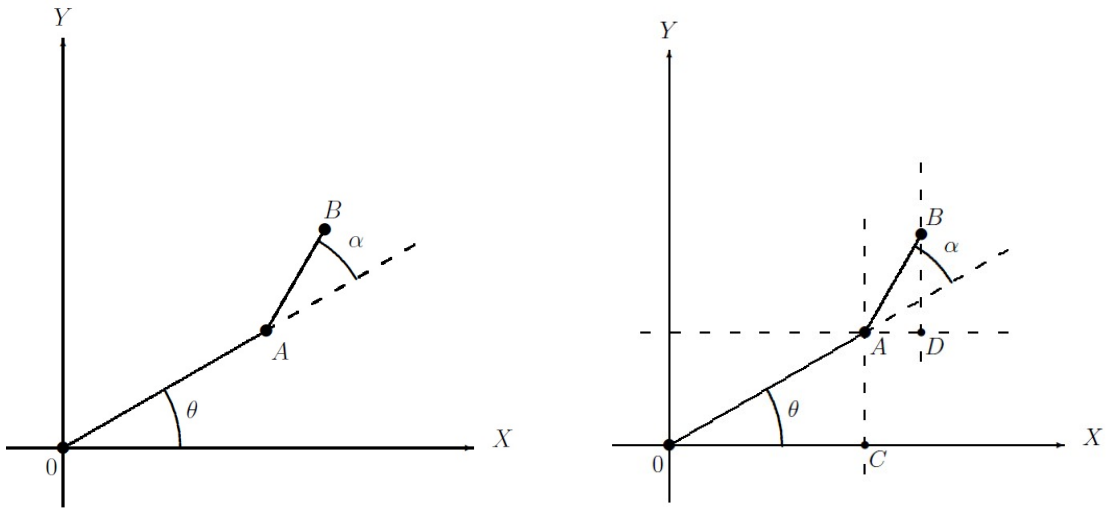
Figura 2: Cinemática inversa.

Sabemos que o ângulo θ é obtido pela equação (5). Assim, temos

$$\theta = \pm arccos\left(\frac{0.\sqrt{2} + 2.\sqrt{2}}{2 + 2}\right) = \pm arccos\left(\frac{\sqrt{2}}{2}\right) = \pm\frac{\pi}{4}.$$

Finalmente, o sinal do ângulo θ será determinado de acordo com o sentido da rotação. Assim, escolhemos o sinal positivo para uma rotação no sentido anti-horário, quando estamos levando o ponto P no ponto P', e escolhemos o sinal negativo para uma rotação no sentido horário, quando estamos levando o ponto P' no ponto P.

Exemplo 4.2. *Considere a Figura 3(a) como sendo a representação de um braço robótico com dois graus de liberdade com movimentos no plano xy.*



(a) Ilustração de um braço robótico (b) Cinemática direta

Figura 3: Cinemática direta de um braço robótico com dois graus de liberdade.

(a) Determine as coordenadas do ponto $B = (c, d)$ em funçao de $L_1 = \overline{OA}$, $L_2 = \overline{AB}$, θ e α, como descritos na Figura 3(a).

(b) Utilize a fórmula obtida no item (a) para encontrar as coordenadas do ponto $B = (c, d)$ quando $L_1 = \overline{OA} = 40cm$, $L_2 = \overline{AB} = 20cm$, $\theta = 30°$ e $\alpha = 30°$.

O ponto B pode ser interpretado como sendo a posição no espaço da extremidade do braço robótico.

Resolução. (a) Aplicando relações trigonométricas no triângulo retângulo OCA, da Figura 3(b), obtemos as coordenadas do ponto $A = (a, b)$ da forma:

$$sen(\theta) = \frac{\overline{AC}}{\overline{OA}} = \frac{b}{L_1} \Longrightarrow b = L_1.sen(\theta) \quad \text{e} \quad cos(\theta) = \frac{\overline{OC}}{\overline{OA}} = \frac{a}{L_1} \Longrightarrow a = L_1.cos(\theta)$$

Assim, $A = (a, b) = (L_1.cos(\theta), L_1.sen(\theta))$.

Resta agora encontrar as coordenadas do ponto $B = (c, d)$.

Consideremos $\beta = \theta + \alpha$. Aplicando relações trigonométricas no triângulo retângulo BAD, obtemos as coordenadas do ponto B da seguinte forma:

$$sen(\beta) = \frac{\overline{DB}}{\overline{AB}} = \frac{m}{L_2} \Longrightarrow m = L_2.sen(\beta) \quad \text{e} \quad cos(\beta) = \frac{\overline{AD}}{\overline{AB}} = \frac{n}{L_2} \Longrightarrow n = L_2.cos(\beta)$$

Desta forma, $c = a + n = L_1.cos(\theta) + L_2.cos(\beta)$ e $d = b + m = L_1.sen(\theta) + L_2.sen(\beta)$.

Equivalentemente, podemos encontrar $B = (c, d)$ por uma transformação linear da seguinte forma:

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} cos(\theta) & cos(\beta) \\ sen(\theta) & sen(\beta) \end{bmatrix} \cdot \begin{bmatrix} L_1 \\ L_2 \end{bmatrix}.$$

Lembrando que $\beta = \theta + \alpha$.

Portanto, descrevemos acima a cinemática direta de um braço robótico, isto é, conhecendo os ângulos θ e α determinamos de modo único a posição do cotovelo que é o ponto A e a posição da extremidade do braço robótico que é o ponto B.

(b) Pelo item (a), obtemos as coordenadas do ponto $B = (c, d)$ da seguinte forma:

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} cos(30°) & cos(60°) \\ sen(30°) & sen(60°) \end{bmatrix} \cdot \begin{bmatrix} 40 \\ 20 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix} \cdot \begin{bmatrix} 40 \\ 20 \end{bmatrix} = \begin{bmatrix} 20\sqrt{3} + 10 \\ 20 + 10\sqrt{3} \end{bmatrix}.$$

Portanto o ponto $B = \left(20\sqrt{3} + 10, 20 + 10\sqrt{3}\right)$.

5 Considerações finais

As aplicações da cinemática direta e da cinemática inversa abrangem uma ampla gama de setores, desde a fabricação de produtos em grande escala até a cirurgia assistida por robôs, passando por aplicações em veículos autônomos, robótica móvel, sistemas de segurança e vigilância, entre outras. Esses conceitos são fundamentais para o desenvolvimento de sistemas automatizados e para a compreensão do movimento em sistemas mecânicos.

Agradecimentos

Na condição de bolsista do Programa Institucional de Bolsas de Iniciação Científica da Universidade Federal de Uberlândia, agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo fomento.

Referências

[1] COSTA, C. G. **Utilização de matrizes no estudo de orientação e posição de um braço robótico por meio das coordenadas de Denavit-Hartenberg**. 2014. 97 p. Dissertação de Mestrado - Departamento de Matemática, Universidade Federal de Goiás, Catalão, 2014.

[2] PULINO, P.; RODRIGUES, C. I. **Transformações geométricas: aplicação nos movimentos de braços robóticos**. 2017. 128 p. Ciência e arte nas férias - Instituto de Matemática Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas, 2017.

Matrizes e a criptografia de dados

Alexssander Farias Vieira

E. E. Antônio Thomaz Ferreira de Rezende, Uberlândia, Minas Gerais, Brasil
alexssanderfariasvieira.4112@gmail.com

Ana Paula Tremura Galves

UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
ana.galves@ufu.br

Palavras-chave

Palavra-chave 1. Criptografia
Palavra-chave 2. Matrizes
Palavra-chave 3. Algoritmos

Resumo

A criptografia surgiu da necessidade de proteger mensagens secretas, consideradas importantes, onde somente o remetente e o destinatário poderiam interpretá-las, tornando difícil o acesso por indivíduos não autorizados. Atualmente ela é constituída por estudos de algoritmos criptográficos seguros e robustos que podem ser implantados em computadores. Podemos utilizar a criptografia em situações nas quais é necessária uma comunicação privada como, por exemplo, via internet, em transações eletrônicas, cartões de crédito, mensagens eletrônicas, entre outros. Este trabalho tem como objetivo analisar e comparar alguns dos principais métodos criptográficos existentes e apresentar um exemplo da utilização de matrizes para a criptografia.

1 Introdução

A criptografia é uma técnica que tem sido utilizada desde os tempos antigos para proteger informações sensíveis. Tal palavra vem do Grego, *Kryptósque*, significa secreto *egrápheinque* significa escrever um código ou mensagem de modo que somente quem envia e quem recebe a mensagem original são capazes de interpretá-la.

Os códigos secretos foram bastante utilizados nas guerras, para transmitir mensagens sem que o inimigo conseguisse compreendê-las.

A criptografia moderna se desenvolveu com a chegada da computação, e atualmente é uma área de grande importância para a segurança da informação em diversas áreas, como finanças, governo, militar e comércio eletrônico.

O interesse pela criptografia tem aumentado significativamente devido a necessidade de manter a privacidade de dados e informações.

Uma série de técnicas e algoritmos são utilizados na criptografia para proteger a confidencialidade, integridade e autenticidade das informações. Uma técnica comum utilizada na criptografia é a utilização de matrizes, que permite a criação de algoritmos seguros e robustos.

Este trabalho tem como objetivo analisar os métodos criptográficos existentes e apresentar uma utilização das matrizes para a criptografia.

As principais referências utilizadas no trabalho são [1] para conceitos preliminares de matrizes e [2] para o estudo de matrizes aplicada a criptografia.

2 Tipos de criptografia

Existem dois principais tipos de criptografia: simétrica e assimétrica.

A criptografia simétrica é uma técnica em que a mesma chave é utilizada tanto para criptografar quanto para descriptografar uma mensagem. Isso significa que o remetente e o destinatário devem compartilhar a mesma chave secreta para garantir a segurança da mensagem. A chave simétrica é gerada por um algoritmo de criptografia e, se alguém conseguir obter a chave, a segurança da mensagem será comprometida. Um exemplo de algoritmo de criptografia simétrica é o *Advanced Encryption Standard* (AES), que é amplamente utilizado em aplicações de segurança.

A criptografia assimétrica, também conhecida como criptografia de chave pública, é uma técnica em que o remetente e o destinatário possuem duas chaves diferentes, uma pública e outra privada. A chave pública é utilizada para criptografar a mensagem e a chave privada é utilizada para descriptografar a mensagem. A chave pública pode ser compartilhada com qualquer pessoa, mas a chave privada deve ser mantida em segredo. Dessa forma, a criptografia assimétrica fornece uma segurança maior do que a criptografia simétrica, pois é necessário obter a chave privada para descriptografar a mensagem. Um exemplo de algoritmo de criptografia assimétrica é o RSA, que é amplamente utilizado em aplicações de segurança.

Ambas as técnicas têm suas vantagens e desvantagens. A criptografia simétrica é mais rápida e eficiente do que a criptografia assimétrica, mas é menos segura, pois a chave deve ser compartilhada entre o remetente e o destinatário. Por outro lado, a criptografia assimétrica é mais segura do que a criptografia simétrica, mas é mais lenta e ineficiente, pois envolve a utilização de duas chaves diferentes.

Em muitas aplicações, é comum utilizar uma combinação de criptografia simétrica e assimétrica para obter o melhor dos dois mundos. Por exemplo, a criptografia simétrica pode ser utilizada para criptografar a mensagem e a chave simétrica pode ser criptografada com a chave pública do destinatário, que é depois enviada junto com a mensagem criptografada. Dessa forma, o destinatário pode usar

sua chave privada para descriptografar a chave simétrica e, em seguida, usar a chave simétrica para descriptografar a mensagem. Essa abordagem é conhecida como criptografia híbrida e é amplamente utilizada em aplicações de segurança.

3 Métodos criptográficos

Existem vários métodos criptográficos disponíveis para proteger informações e garantir a privacidade e segurança de dados sensíveis. Cada método tem seus próprios pontos fortes e fracos, e o método escolhido dependerá das necessidades específicas de segurança e privacidade de cada aplicação. Alguns dos principais métodos criptográficos serão citados nas subseções a seguir:

3.1 Cifras de HILL

A cifra de Hill é um algoritmo de criptografia que usa matrizes para criptografar e descriptografar informações. Ela foi inventada por Lester S. Hill em 1929 e é considerada uma das primeiras cifras lineares.

O algoritmo de Hill é uma cifra de substituição que usa matrizes para transformar cada letra do texto original em uma letra cifrada. Essa matriz é chamada de "matriz de cifra"e é uma matriz quadrada de ordem $n \times n$, onde n é um inteiro positivo.

Para criptografar uma mensagem usando a cifra de Hill, cada letra do texto original é convertida em um número correspondente à sua posição no alfabeto. Esses números são colocados em uma matriz de tamanho $n \times 1$, e a matriz de cifra é multiplicada pela matriz resultante. O resultado é uma nova matriz que contém os números correspondentes às letras cifradas. Esses números são então convertidos de volta em letras para criar a mensagem cifrada.

Para descriptografar, a mensagem cifrada é colocada em uma matriz de tamanho $n \times 1$ e multiplicada pela matriz inversa da matriz de cifra. O resultado é uma matriz que contém os números correspondentes às letras originais. Esses números são então convertidos de volta em letras para criar a mensagem original.

Uma das principais vantagens da cifra de Hill é que ela é resistente a ataques de força bruta. Isso ocorre porque é muito difícil determinar a matriz de cifra a partir da mensagem cifrada sem a chave de descriptografia correta. No entanto, a cifra de Hill é vulnerável a ataques de criptoanálise diferencial e outros tipos de ataques sofisticados.

Em resumo, a cifra de Hill é uma cifra de substituição que usa matrizes para criptografar e descriptografar informações. Embora tenha algumas limitações, ela continua sendo uma técnica criptográfica importante e influente.

3.2 Cifras de substituição

Cifras de substituição são algoritmos de criptografia que substituem cada letra ou símbolo de um texto original por outra letra ou símbolo, de acordo com uma chave de criptografia. Existem vários tipos de cifras de substituição, como a cifra de César, a cifra de Vigenère e a cifra de Playfair. Essas cifras são vulneráveis a ataques de criptoanálise, como a análise de frequência, mas ainda são amplamente usadas em aplicações simples e de baixa segurança.

3.3 Método Matriz

Semelhante ao de substituição e transposição, com ênfase diferente. Tem como objetivo tornar o algoritmo mais complexo e pode ser aplicado como introdução às matrizes.

3.4 Método Permutacional

O método permutacional era o método mais utilizado antes da existência do computador. É um algoritmo de criptografia que reorganiza as letras ou símbolos do texto original de acordo com uma chave de permutação. Existem diferentes tipos de técnicas permutacionais, como a cifra de transposição e a cifra de rearranjo de colunas. A cifra de transposição permuta as letras ou símbolos do texto original de acordo com uma sequência predefinida, enquanto a cifra de rearranjo de colunas permuta as colunas de uma matriz que contém as letras do texto original. A criptografia permutacional é resistente a ataques de análise de frequência e ataques de força bruta, mas ainda é vulnerável a outros tipos de ataques sofisticados.

3.5 Método RSA (Rivest-Shamir-Adleman)

O método RSA na criptografia é um algoritmo de criptografia assimétrica que usa um par de chaves (pública e privada) para criptografar e descriptografar mensagens. Para criptografar a mensagem, a chave pública do destinatário é usada para transformar a mensagem original em uma sequência de números que são incompreensíveis sem a chave privada correspondente. A descriptografia da mensagem é realizada pelo destinatário usando sua chave privada correspondente para transformar os números cifrados de volta na mensagem original. O método RSA é seguro e é amplamente utilizado em aplicações de segurança digital, como transações financeiras e comunicações de dados sensíveis.

3.6 SSL (Secure Sockets Layer) e TLS (TransportLayer Security)

SSL (Secure Sockets Layer) e TLS (Transport Layer Security) são protocolos de segurança usados na criptografia de comunicações na internet, como e-mails, transações financeiras e navegação em sites seguros. Ambos os protocolos usam algoritmos de criptografia simétrica e assimétrica para proteger a confidencialidade, integridade e autenticidade dos dados transmitidos entre um cliente e um servidor. A principal diferença entre SSL e TLS é que TLS é a versão mais recente e segura, desenvolvida como uma atualização do SSL. Além disso, o TLS usa um processo de negociação de chave mais seguro do que o SSL, chamado de Protocolo de Troca de Chave Difie-Hellman. TLS é amplamente usado hoje em dia para garantir a segurança das comunicações na internet.

4 Matrizes e criptografia

Uma forma de usar matrizes na criptografia é envolvendo matrizes inversas. O exemplo a seguir descreve uma dessas formas.

Seja $A = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}$ uma matriz quadrada de ordem 2×2 com inversa $B = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$.

A matriz A irá codificar uma mensagem e o destinatário usará a matriz B para decodificar .

O primeiro passo para codificar a mensagem é fazer sua conversão da forma alfabética para forma numérica. Para isso, a tabela a seguir será utilizada.

Tabela 1: Tabela alfanumérica

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	.	!	#	
21	22	23	24	25	26	27	28	29	30

Tanto o remetente quanto o destinatário devem estar cientes desta tabela.
Vamos codificar a seguinte frase: “MEU FUTURO DEPENDE DE MIM”.

MEU#FUTURO#DEPENDE#DE#MIM

13 5 21 29 6 21 20 21 18 15 29 4 5 16 5 14 4 5 29 4 5 29 13 9 13

O símbolo $\#$ serve para não haver erros de leitura na língua portuguesa após a decodificação da mensagem.

Vamos colocar a sequência de números dispostos em uma matriz M de duas linhas. Se o número de elementos da matriz for ímpar, deve-se acrescentar um caractere vazio.

$$M = \begin{bmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{bmatrix}$$

Para codificar a mensagem, multiplicamos a matriz A pela matriz M, obtendo a matriz $N = A.M$

$$N = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{bmatrix}$$

$$N = \begin{bmatrix} 55 & 20 & 77 & 91 & 23 & 92 & 64 & 68 & 83 & 58 & 96 & 25 & 45 \\ 42 & 15 & 56 & 62 & 17 & 71 & 44 & 47 & 65 & 43 & 67 & 21 & 40 \end{bmatrix}$$

A matriz N apresenta a mensagem codificada:

55 20 77 91 23 92 64 68 83 58 96 25 45 42 15 56 62 17 71 44 47 65 43 67 21 40

O destinatário, no momento em que receber a mensagem codificada, usará a matriz B para decodificar e ler a mensagem.

Sabendo que $B.N = B.A.M = I.M = M$, temos que $M = B.N$.

Multiplicando a matriz B pela matriz N, obtemos o seguinte resultado

$$N = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 55 & 20 & 77 & 91 & 23 & 92 & 64 & 68 & 83 & 58 & 96 & 25 & 45 \\ 42 & 15 & 56 & 62 & 17 & 71 & 44 & 47 & 65 & 43 & 67 & 21 & 40 \end{bmatrix}$$

$$N = \begin{bmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{bmatrix}$$

Enfim chegamos à matriz $M = B.N$ do remetente que é a mensagem original.

Em seguida, é só reverter os números utilizando novamente a tabela alfanumérica.

13 5 21 29 6 21 20 21 18 15 29 4 5 16 5 14 4 5 29 4 5 29 13 9 13

MEU#FUTURO#DEPENDE#DE#MIM

5 Considerações finais

A criptografia é uma técnica essencial para garantir a segurança e privacidade das informações em um mundo cada vez mais digital e conectado.

A escolha do método criptográfico adequado depende do contexto de aplicação e dos requisitos de segurança necessários. Além disso, a segurança da criptografia também depende da força das chaves de criptografia usadas, bem como da segurança do armazenamento e da transmissão dessas chaves.

Com a crescente demanda por segurança digital, a criptografia continuará a ser uma área de pesquisa e desenvolvimento em constante evolução. Novos métodos criptográficos estão sendo desenvolvidos para atender às necessidades de segurança cada vez mais rigorosas em ambientes digitais, e a adoção de técnicas avançadas de criptografia se tornará ainda mais importante para garantir a segurança dos dados em um mundo cada vez mais conectado.

Agradecimentos

Na condição de bolsista do Programa Institucional de Bolsas de Iniciação Científica da Universidade Federal de Uberlândia, agradeço ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo fomento.

Referências

[1] HAZZAN, S.; IEZZI, G. **Fundamentos de matemática elementar - Sequências, Matrizes, Determinantes e Sistemas**. Volume 4. São Paulo: Editora Atual, 1977.

[2] OLIVEIRA, F.N.S. **Ensino de matrizes aplicado a criptografia com o uso de ferramentas digitais**. 2015. 33 p. Trabalho de Conclusão de Curso - Instituto Universidade Virtual, Universidade Federal do Ceará, Maranguape, 2015.

A família quadrática $\mathbf{F}_{\mu}(\mathbf{x}) = \mu\mathbf{x}(\mathbf{1} - \mathbf{x})$

Luís Otávio de Oliveira Alvarenga

UFTM, Engenharia Mecânica, Universidade Federal do Triângulo Mineiro, Uberaba, MG, Brasil
alvarengaluis443@gmail.com

Hernán Roberto Montúfar López

UFU, Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, MG, Brasil
montufar@ufu.br

Palavras-chave

Sistemas dinâmicos.
Comportamento caótico.
Aplicação quadrática.

Resumo

A dinâmica por trás de sistemas caóticos é utilizada para prever o comportamento futuro de diversos problemas práticos como a previsão do tempo ou o comportamento de um fluido turbulento no espaço. Para compreender melhor o comportamento de tais fenômenos é necessário o conhecimento teórico sobre sistemas dinâmicos e suas propriedades. Assim, o trabalho em questão apresenta técnicas e ferramentas para analisar a dinâmica de uma ampla classe de aplicações quadráticas. Inicialmente, são avaliados os pontos fixos da função e analisada sua dinâmica para todo x no intervalo unitário $[0, 1]$. Por fim, é realizada uma análise da dinâmica global da aplicação, onde é mostrado que ela pode apresentar comportamento caótico para determinados valores do parâmetro μ.

1 Introdução

Neste trabalho será discutida e analisada a aplicação quadrática $F_\mu(x) = \mu x(1-x)$ com $\mu > 1$. O comportamento dessa função sob iteração foi compreendido na década dos anos 90 e ilustra muitos dos fenômenos importantes que ocorrem em sistemas dinâmicos. Usando a composição de funções obtemos a lista de números

$$x_0, F_\mu(x_0), F_\mu(F_\mu(x_0)), F_\mu(F_\mu(F_\mu(x_0))) \cdots$$

Esse será nosso sistema dinâmico e analisaremos como a dinâmica desta função mudará a medida que o parâmetro μ varia, [1].Veremos que a dinâmica simbólica é um modelo muito importante para entender estas iterações.

Proposição 1.1. *Supondo* $\mu > 1$.

1. *Se* $x < 0$, *então* $F_\mu^n(x) \to -\infty$ *quando* $n \to \infty$.
2. $F_\mu(0) = 0$.
3. $0 < p_\mu < 1$, $F_\mu(p_\mu) = p_\mu$ *quando* $p_\mu = \frac{\mu-1}{\mu}$.
4. $F_\mu(1) = 0$.
5. *Se* $x > 1$, *então* $F_\mu^n(x) \to -\infty$ *quando* $n \to \infty$.

Demonstração. Os items 2 e 4 são imediatos.

1. Se $x < 0$, então $\mu x(1-x) < \mu x < x$. Assim $F_\mu(x) < x$. Logo $F_\mu^n(x) \to -\infty$.
3. Se $\mu > 1$ então $0 < \mu - 1 < \mu$. Logo $0 < p_\mu < 1$ e se verifica que $F_\mu(p_\mu) = p_\mu$.
5. Se $x > 1$, então $1 - x < 0$. Assim $F_\mu(x) < 0$. Logo $F_\mu^n(x) \to -\infty$.

■

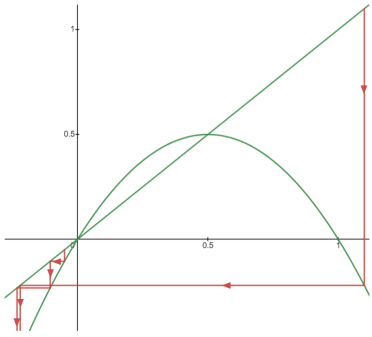


Figura 1: Análise gráfica de $F_\mu(x) = \mu x(1-x)$ quando $\mu > 1$.

Segue-se da proposição acima, que as dinâmicas interesantes de F_μ occorrem no intervalo $I = \{x \mid 0 \leq x \leq 1\}$, uma vez que todos os pontos que não se encontram em I tendem para $-\infty$, figura 1.

Proposição 1.2. *Seja* $1 < \mu < 3$.

1. *F_μ possui um ponto fixo atrator em $p_\mu = \frac{(\mu-1)}{\mu}$ e um ponto fixo repulsor em* 0.

2. *Se* $0 < x < 1$, *então*

$$\lim_{n\to\infty} F_\mu^n(x) = p_\mu.$$

Demonstração.

1. Pela proposição 1.1 F_μ possui dois pontos fixos: 0 e p_μ. Perceba que $F'_\mu(0) = \mu$ e $F'_\mu(p_\mu) = 2-\mu$. Logo, 0 é ponto fixo repulsor para $\mu > 1$ e p_μ é ponto fixo atrator para $1 < \mu < 3$.

2. Consideremos o caso em que $1 < \mu < 2$, figura 2a. Se $x \in (0, 1/2]$. Então uma análise gráfica mostra imediatamente que: $\mid F_\mu(x) - p_\mu \mid < \mid x - p_\mu \mid$ se $x \neq p_\mu$. Consequentemente, $F_\mu^n(x) \to p_\mu$ quando $n \to \infty$. Por outro lado, se $x \in (1/2, 1)$, então $F_\mu(x) \in (0, 1/2)$, de modo que o argumento anterior implica que $F_\mu^n(x) = F_\mu^{n-1}(F_\mu(x)) \to p_\mu$, quando $n \to \infty$.

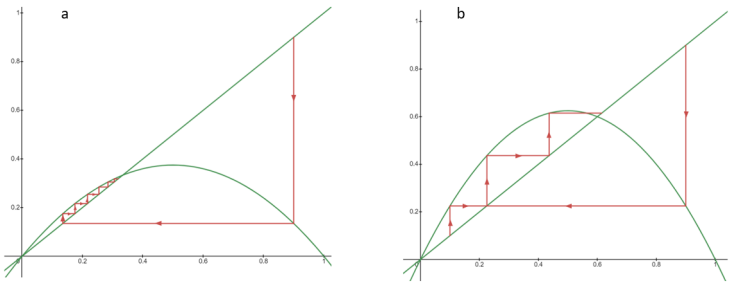


Figura 2: Análise gráfica de $F\mu = \mu x(1-x)$ quando a) $1 < \mu < 2$, b) $2 < \mu < 3$.

Para o caso $2 < \mu < 3$ a análise gráfica é diferente, figura 2b. Note que $1/2 < p_\mu < 1$. Considere que $\hat{p}_\mu$ seja o único ponto do intervalo $(0, 1/2)$ que é mapeado em p_μ por F_μ. Assim, podemos dizer que F_μ^2 mapeia o intervalo $[\hat{p}_\mu, p_\mu]$ dentro de $[1/2, p_\mu]$. Isso segue que $F_\mu^n(x) \to p_\mu$ quando $n \to \infty$ para todo $x \in [\hat{p}_\mu, p_\mu]$. Agora supomos $x < \hat{p}_\mu$. Novamente a análise gráfica mostra que existe um $k > 0$ de modo que $F_\mu^k(x) \in [\hat{p}_\mu, p_\mu]$. Portanto, $F_\mu^{k+n}(x) \to p_\mu$ quando $n \to \infty$. Finalmente, do mesmo modo que anteriormente, F_μ mapeia o intervalo $(p_\mu, 1)$ para $(0, p_\mu)$. Como, $(0, 1) = (0, \hat{p}_\mu) \bigcup [\hat{p}_\mu, p_\mu] \bigcup (p_\mu, 1)$, finalizamos a análise para o caso $2 < \mu < 3$.

■

Assim, para $1 < \mu < 3$, F_μ possui apenas dois pontos fixos e todos os outros pontos em I são assintóticos para p_μ. Assim podemos dizer que a dinâmica da aplicação quadrática F_μ foi completamente compreendida no intervalo analisado.

2 Estrutura dinâmica de F_μ com $\mu > 4$

Como dito anteriormente a dinâmica de F_μ acontece no intervalo unitário I. Observe que com $\mu > 4$, o valor máximo $\mu/4$ de F_μ é maior que 1. Por isso pontos saem de I após uma iteração de F_μ. Denotamos o conjunto de tais pontos por A_0. Claramente A_0 é um intervalo aberto com centro em $1/2$ e possui a propriedade em que, se $x \in A_0$, então $F_\mu(x) > 1$, assim $F_\mu^2(x) < 0$ e $F_\mu^n(x) \to -\infty$. A_0 é o conjunto de pontos que escapam imediatamente de I. Todos os outros pontos de I permanecem em I após uma iteração de F_μ. Seja $A_1 = \{x \in I \mid F_\mu(x) \in A_0\}$. Se $x \in A_1$, então $F_\mu^2(x) > 1$, $F_\mu^3(x) < 0$, e assim como antes, $F_\mu^n(x) \to -\infty$. Por dedução,

$$A_n = \left\{x \in I \mid F_\mu^n(x) \in A_0\right\}.$$

Isto é, $A_n = \left\{x \in I \mid F_\mu^i(x) \in I \ \ para \ \ i \leq n \ \ mas \ \ F_\mu^{n+1}(x) \notin I\right\}$, de modo que A_n consiste em todos os pontos que escapam de I na $n+1$ iteração. Como anteriormente, se x se encontra em A_n, sua órbita enventualmente tenderá para $-\infty$. Agora que já conhecemos o destino de todos os pontos que se encontram em A_n, nos resta analizar o comportamento dos pontos restantes, ou seja, os pontos que nunca escapam de I; esse conjunto de pontos se encontra em

$$\Lambda = I - \left(\bigcup_{n=0}^{\infty} A_n\right)$$

Para entender exatamente qual é esse conjunto de pontos, descreveremos com mais cuidado a construção recursiva. Visto que A_0 é um intervalo aberto centrado em $1/2$, $I - A_0$ consiste em dois intervalos fechados, I_0 na esquerda e I_1 na direita. Observe a figura 3.

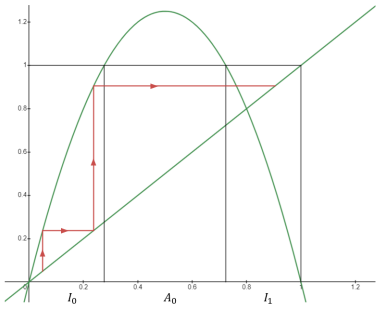


Figura 3: Análise gráfica de $F_\mu = \mu x(1-x)$ quando $\mu > 4$ com intervalos A_0, I_0 e I_1

Observe que F_μ é crescente em I_0 e decrescente em I_1. Desde que $F_\mu(I_0) = F_\mu(I_1) = I$, existe um par de intervalos abertos, um em I_0 e outro em I_1 que são mapeados em A_0 por F_μ. Esse par de intervalos é precisamente o conjunto A_1. Agora consideremeos $I - (A_0 \bigcup A_1)$. Esse conjunto consiste de 4 intervalos fechados e F_μ mapeia cada um monotonicamente em I_0 ou I_1. Consequentemente F_μ^2 mapeia cada um em I. Portanto podemos ver que cada um dos quatro intervalos em $I - (A_0 \bigcup A_1)$ contém um subintervalo que possui imagem em A_0 por F_μ^2. Logo, pontos de tais intervalos escapam

de I após a terceira iteração de F_μ. Esse conjunto de subintervalos é denominado A_2. Podemos dizer que o conjunto A_n consiste em 2^n intervalos abertos e disjuntos. Além disso, F_μ^n possui no mínimo 2^n pontos fixos ou, equivalentemente, $Per_n(F_\mu)$ possui 2^n pontos em I.

A construção do conjunto Λ ocorre de maneira semelhante à construção do conjunto de terços médios de Cantor. Λ é obtido pela sucessiva remoção de intervalos abertos dos meios de um conjunto de intervalos fechados.

Teorema 2.1. *Se $\mu > 2 + \sqrt{5}$, então Λ é um conjunto de Cantor.*

Portanto, para $\mu > 4$ qualquer ponto tende a $-\infty$ quando aplicado F_μ ou então órbitas inteiras se encontram em Λ. Para compreender a estrutura de $F_\mu|_\Lambda$, iremos utilizar um modelo simbólico que descreve a dinâmica de F_μ da maneira mais simples possível. Consideremos o espaço $\Sigma_2 = \{s = (s_0 s_1 s_2 \dots) \mid s_i = 0 \text{ ou } 1\}$ chamado de **espaço sequência** que possui infinitas cadeias de inteiros como $(000\dots)$ ou $(0101\dots)$. Definamos neste espaço a **aplicação shift** $\sigma : \Sigma_2 \to \Sigma_2$ dada por $\sigma(s_0 s_1 s_2 \dots) = (s_1 s_2 s_3 \dots)$. Esta aplicação tem as seguintes propriedades: a cardinalidade de $Per_n(\sigma)$ é 2^n. $Per(\sigma)$ é denso em Σ_2 e existe uma órbita densa para σ em Σ_2.

Relacionaremos agora a aplicação shift com a função quadrática $F\mu(x) = \mu x(1-x)$ quando μ é grande o suficiente. O itinerário de x é uma sequência $S(x) = s_0 s_1 s_2 \dots$ onde $s_i = 0$ se $F^i(x) \in I_0$ e $s_i = 1$ se $F^i(x) \in I_1$. Isso é, $S(x)$ é um ponto no espaço sequência Σ_2. Logo, considera-se

$$S : \Lambda \to \Sigma_2$$

Se $\mu > 2 + \sqrt{5}$, então $S : \Lambda \to \Sigma_2$ é um homeomorfismo. Logo, Λ e Σ_2 são os mesmos. Além de que S proporciona uma equivalência entre as dinâmicas de F_μ sobre Λ e σ sobre Σ_2, já que $S \circ F_\mu = \sigma \circ S$. Funções topologicamente[1] conjugadas são equivalentes em termos de suas dinâmicas. Assim a função quadrática possui as mesmas propriedades descritas para σ.

Teorema 2.2. *Seja $F_\mu(x) = \mu x(1-x)$ com $\mu > 2 + \sqrt{5}$. Então: A cardinalidade de $Per_n(F_\mu)$ é 2^n, $Per(F_\mu)$ é denso em Λ e F_μ possui órbita densa em Λ.*

3 Comportamento Caótico

Existem inúmeras definições de caos, adotaremos aqui uma abordagem topológica. Seja J um espaço métrico. A função $f : J \to J$ é **topologicamente transitiva** se para qualquer par de intervalos abertos $U, V \in J$ existe $n > 0$ de modo que $f^n(U) \cap V \neq \emptyset$. Intuitivamente, f possui pontos que eventualmente se movem sob iteração, de uma pequena vizinhança arbitrária para outra. Consequentemente, o sistema dinâmico não pode ser decomposto em dois intervalos abertos e disjuntos invariantes por f. Perceba que se a função possui uma órbita densa, então claramente ela é transitiva.

[1] Seja $f : A \to A$ e $g : B \to B$ duas funções. f e g são topologicamente conjugadas se existe um homeomorfismo $h : A \to B$ de modo que $h \circ f = g \circ h$.

$f : J \to J$ possui **dependência sensitiva das condições iniciais** se existe $\delta > 0$ tal que, para todo $x \in J$ e qualquer vizinhança N de x existe $y \in N$ e $n \geq 0$ de modo que $\mid f^n(x) - f^n(y) \mid > \delta$. Isto é, existem pontos perto de x que eventualmente são separados de x por pelo menos δ sob a iteração de f.

Definição 3.1. *$f : J \to J$ é dita **caótica** em J se: f possui dependência sensitiva das condições iniciais, f é topologicamente trasitiva e pontos periódicos são densos em J.*

Afirmamos que uma função caótica possui três componentes: imprevisibilidade, indecomponibilidade e um elemento de regularidade. Um sistema caótico é imprevisível por causa de sua dependência sensitiva das condições iniciais. Ele não pode ser decomposto em subsistemas que não interagem sob f pois são topologicamente transitivos. E, por fim, existe um elemento de regularidade: os pontos periódicos, que são densos.

Observe que $F_\mu = \mu x(1-x)$ com $\mu > 2 + \sqrt{5}$ possui dependência sensitiva das condições iniciais em Λ. De fato, escolhemos δ menor que o diâmetro de A_0, onde A_0 é o espaço entre I_0 e I_1. Seja $x, y \in \Lambda$. Se $x \neq y$, então as imagens de x e y devem diferir em pelo menos um ponto, digamos no $n-$ésimo ponto. Logo, em um determinado momento da iteração, $F_\mu^n(x)$ e $F_\mu^n(y)$ estarão em lados opostos de A_0, de modo que $F_\mu^n(x) - F_\mu^n(y) > A_0 > \delta$. É possível afirmar também que a aplicação $F_\mu = \mu x(1-x)$ com $\mu > 2 + \sqrt{5}$ é topologicamente transitiva, uma vez que, segundo o teorema 2.2, F_μ possui órbita densa em Λ. Assim, podemos dizer que a aplicação $F_\mu = \mu x(1-x)$ apresenta comportamento caótico com $\mu > 2 + \sqrt{5}$.

4 Conclusão

O teorema 2.2 mostra o poder da dinâmica simbólica e da conjugação topológica. A conjugação topológica garante que as órbitas de ambas as funções são as mesmas e, além disso, a dinâmica simbólica fornece uma medida aproximada da complexidade das órbitas em Λ. Assim, essas duas noções comprovam que a aplicação shift é um modelo preciso para a família quadrática.

Agradecimentos

O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil (CNPq) através do programa de Iniciação Ciêntífica e Mestrado (PICME).

Referências

[1] R.L DEVANEY. **An Introduction To Chaotic Dynamical Systems**. 2a. ed. Addison-Wesley Publishing Company, 1986. isbn:0-201-13046-7

A dinâmica de aplicações no círculo unitário

Luís Otávio de Oliveira Alvarenga

UFTM, Engenharia Mecânica, Universidade Federal do Triângulo Mineiro, Uberaba, MG, Brasil
alvarengaluis443@gmail.com

Hernán Roberto Montúfar López

UFU, Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, MG, Brasil
montufar@ufu.br

Palavras-chave

Sistemas dinâmicos.
Comportamento caótico.
Círculo unitário.

Resumo

A dinâmica de aplicações no círculo unitário é um campo de estudo que envolve o estudo de funções que mapeiam o círculo unitário em si mesmo, e os comportamentos que essas funções apresentam. Neste trabalho, explorou-se alguns dos conceitos fundamentais da dinâmica de aplicações no círculo unitário, incluindo o comportamento caótico, pontos periódicos, pontos fixos e pontos eventualmente periódicos. No final, esperamos oferecer uma visão geral clara e concisa desse campo de estudo que tem aplicações em diversas áreas da matemática.

1 Introdução

Para modelar um fenômeno natural é necesário introduzir um espaço que descreva seus estados possíveis e uma lei de evolução que descreva como esse fenômeno evolui no tempo. A teoria dos sistemas dinâmicos busca compreender o comportamento de longo prazo destes sistemas em evolução. Se o tempo t é um número inteiro, dizemos que o sistema dinâmico é discreto e será descrito por uma aplicação f no espaço de estados M.

$$f : M \to M$$

As composições desta aplicação gera a dinâmica do sistema. Assim, ao estudar sistemas dinâmicos discretos estamos interessados em conhecer todas as iterações de um ponto e seu comportamento.

Uma órbita de $x \in M$ é o conjunto $\mathcal{O}(x) = \{f^n(x) : n \in \mathbb{Z}\}$. O ponto x é um ponto fixo de f se $f(x) = x$. Se $f^n(x) = x$ o ponto x é um ponto periódico de período n. O conjunto de pontos periódicos de período n é denotado como $Per_n(f)$. Já o conjunto de pontos fixos são denominados por $Fix(f)$. O conjunto de todas as interações de um ponto periódico formam uma órbita periódica.

Consideremos o cículo unitário S^1: pontos de S^1 são determinados de forma padrão pelo ângulo θ em radianos. Assim, um ponto pode ser denotado por qualquer ângulo na forma $\theta + 2k\pi$, onde k é um número inteiro. Agora considere o homeomorfismo[1]

$$f : S^1 \to S^1$$

dada por $f(\theta) = 2\theta$. Como $f^n(\theta) = 2^n\theta$, θ é periódico de período n se e somente se $2^n\theta = \theta + 2k\pi$ para qualquer k inteiro, ou seja, se e somente se $\theta = \frac{2k\pi}{2^n-1}$, onde $0 \leq k \leq 2^n - 2$ é um inteiro.

- Se $n = 1$, temos $2\theta = \theta + 2k\pi$. Logo $Fix(f) = \{0\}$.
- Se $n = 2$, temos $2^2\theta = \theta + 2k\pi \Leftrightarrow \theta = \frac{2k\pi}{3}$. Logo $Per_2(f) = \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$.
- Se $n = 3$, temos $2^3\theta = \theta + 2k\pi \Leftrightarrow \theta = \frac{2k\pi}{7}$. Logo $Per_3(f) = \{0, \frac{2\pi}{7}, \frac{4\pi}{7}, \frac{6\pi}{7}, \frac{8\pi}{7}, \frac{10\pi}{7}, \frac{12\pi}{7}\}$.

Logo, os pontos periódicos de período n para f são as $(2^n - 1)$ raízes unitárias.

Um ponto x é eventualmente periódico com período n se x não é periódico mas existe um $m > 0$ de modo que $f^{n+i}(x) = f^i(x)$ para todo $i \geq m$. Consideremos a mesma função $f(\theta) = 2\theta$ no círculo. Note que $f(0) = 0$ é fixo. Se $\theta = 2k\pi/2^n$ então $f^n(\theta) = 2k\pi$ de modo que θ é eventualmente fixo.

- Se $n = 1$, temos $\theta = k\pi$. Logo $\theta = \pi$ eventualmente fixo.
- Se $n = 2$, temos $\theta = \frac{k\pi}{2}$. Logo $\theta = \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ são eventualmente fixos.
- Se $n = 3$, temos $\theta = \frac{k\pi}{4}$. Logo $\theta = \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}, \pi, \frac{5\pi}{4}, \frac{3\pi}{2}, \frac{7\pi}{4}$ são eventualmente fixos.

[1] Um homeomorfismo é uma função contínua, invertível e com inversa contínua.

E isso significa que pontos eventualmente fixos são densos em S^1.

Desta forma, homeomorfismos no círculo podem ter pontos de qualquer período. Isto não acontece na reta onde só podem existir pontos periódicos de no máximo período dois.

Proposição 1.1. *Seja $f : \mathbb{R} \to \mathbb{R}$ um homeomorfismo. Então não existe $x \in Per_n(f)$ com $n > 2$.*

Demonstração. Afirmamos que f é estritamente crescente ou estritamente decrescente. De fato: suponha que não é estritamente crescente então existem $x < y < z$ tais que $f(x) < f(y)$ e $f(z) < f(y)$. Pelo teorema do valor intermediário, existe $a \in (x, y)$ e $b \in (y, z)$ tais que $f(a) = f(b)$. Mas $a \neq b$, assim f não é injetiva. Contradicão, já que por hipótese f é homeomorfismo. Analogamente para o caso que não é estritamente decrescente.

Para f estritamente crescente temos: $f(x) < x$, $f(x) = x$ ou $x < f(x)$. Se $f(x) < x$ então $f^2(x) < f(x) < x$. Por indução, $f^n(x) < x$ para $n \in \mathbb{N}$. Portanto, x não é ponto periódico. Se $f(x) = x$ então x é um ponto fixo. Se $x < f(x)$, por indução $x < f^n(x)$ para $n \in \mathbb{N}$. Portanto, x não é ponto periódico.

Para f estritamente decrescente temos: $x < y \Rightarrow f(x) > f(y) \Rightarrow f^2(x) < f^2(y)$. Assim, f^2 é estritamente crescente. Logo existe x tal que $f^2(x) = x$, ponto períodico de período 2. Portanto, não existem pontos periódicos de período maior que 2. ■

2 Comportamento de S^1

O objetivo de sisemas dinâmicos é compreender a natureza de todas as órbitas, além de indentificar o conjunto de órbitas que são periódicas, eventualmente periódicas, assintóticas, etc. Por ser uma tarefa impossível de se resolver, na prática, optamos por uma abordagem unicamente qualitativa e geométrica para entender a dinâmica dos sistemas dados, [1].

Definição 2.1. *Seja p um ponto periódico de período n. O ponto p é hiperbólico se $\mid (f^n)'(p) \mid \neq 1$. O ponto p é chamado de ponto periódico atrator se $\mid (f^n)'(p) \mid < 1$. Se $n = 1$, o ponto p é dito ponto fixo. O ponto fixo hiperbólico p com $\mid f'(p) \mid > 1$ é chamado de ponto fixo repulsor.*

Pontos periódicos atratores de período n apresentam vizinhança localizada dentro de si por f^n. Essa vizinhança é denominada como conjunto estável local e é denotada por W^s_{loc}. Já para os pontos fixos repulsores, existe um intervalo aberto U de p de modo que, se $x \in U$, $x \neq p$, existe $k > 0$ tal que $f^k(x) \notin U$. A vizinhança U de p é denominada conjunto instável local e é denotado por W^u_{loc}.

O gráfico de uma função real proporciona informações sobre a primeira iteração e apenas informações simplificadas sobre as iterações subsequentes. Para entender as iterações mais altas poderíamos tentar traçar cada um dos gráficos, mas esse é um processo complexo. Portanto, utiliza-se um método mais eficiente, o retrato de fase. O retrato de fase consiste em uma representação geométrica das trajetórias de um sistema dinâmico. Basicamente, para esboçar o retrato de fase da dinâmica no círculo unitário, traçamos um círculo de raio 1, escrevemos a função na forma polar, marcamos o ponto

incial que desejamos analisar, definimos e traçamos os pontos fixos existentes e analisamos quais são atratores ou repulsores. Em seguida desenhamos uma seta que sai dos pontos repulsores para os pontos atratores. Com esta representação é possível determinar de forma qualitativa onde determinado ponto se encontrará após n iterações.

Exemplo 1: Seja $f(\theta) = \theta + \epsilon \sin(2\theta)$ para $0 < \epsilon < 1/2$. Note que f possui pontos fixos em 0, $\pi/2$, π e $3\pi/2$. $f'(0) = f'(\pi) = 1 + 2\epsilon > 1$ e $f'(\pi/2) = f'(3\pi/2) = 1 - 2\epsilon < 1$. Logo 0 e π são pontos fixos repulsores enquanto $\pi/2$ e $3\pi/2$ são pontos fixos atratores. Analogamente, quando $f(\theta) = \theta + \epsilon \sin(4\theta)$, f possui pontos fixos repulsores em 2π, $\pi/2$, π, $3\pi/2$ e pontos fixos atratores em $\pi/4$, $3\pi/4$, $5\pi/4$, $7\pi/4$. Os retratos de fase dessas funções podem ser vistos na figura 1.

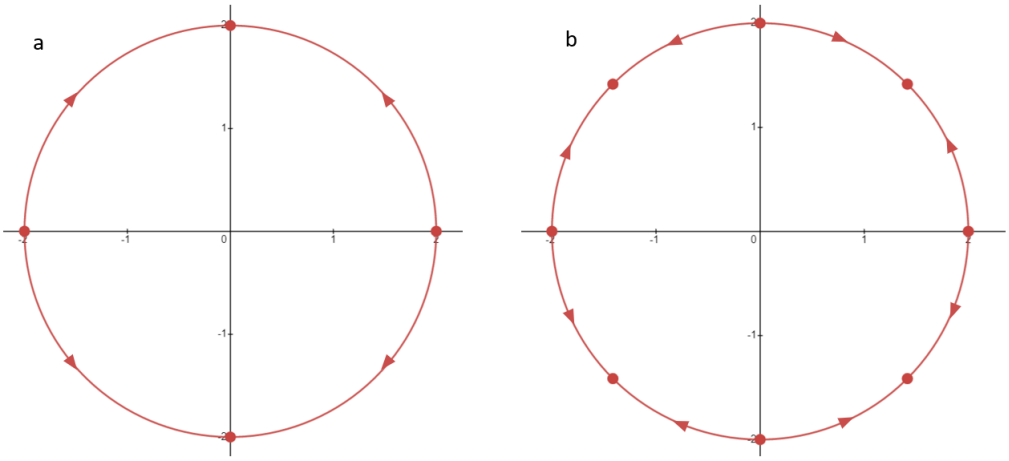


Figura 1: Retrato de fase de a) $f(\theta) = \theta + \epsilon \sin(2\theta)$ e b) $f(\theta) = \theta + \epsilon \sin(4\theta)$

Exemplo 2: Translação no círculo. Seja $\lambda \in \mathbb{R}$ e $T_\lambda(\theta) = \theta + 2\pi\lambda$. A função T_λ apresenta comportamento bastante diferente de acordo com a racionalidade ou irracionalidade de λ. Se $\lambda = p/q$, onde p e q são inteiros, então $T_\lambda^q(\theta) = \theta + 2\pi p = \theta$ de modo que todos os ponto sejam fixos por T_λ^q. Quando λ é irracional, a situação é diferente, como pode ser visto no teorema abaixo.

Teorema 2.2. *Cada órbita T_λ é densa em S^1 se λ é irracional.*

Demonstração. Seja $\theta \in S^1$. Os pontos na órbita de θ são distintos se $T_\lambda^n(\theta) = T_\lambda^m(\theta)$, então temos $(n-m)\lambda \in \mathbb{Z}$, de modo que $n = m$. Qualquer conjunto infinito de pontos no círculo deve possuir um ponto limite. Assim, dado qualquer $\epsilon > 0$, devem existir inteiros n e m de modo que $\mid T_\lambda^n(\theta) - T_\lambda^m(\theta) \mid < \epsilon$. Seja $k = n - m$. Então $\mid T_\lambda^k(\theta) - \theta \mid < \epsilon$. Assim T_λ preserva comprimentos em S^1. Consequentemente, T_λ^k mapeia o círculo conectanto θ a $T_\lambda^k(\theta)$, $T_\lambda^k(\theta)$ a $T_\lambda^{2k}(\theta)$ que possui comprimento menor que ϵ. Isso mostra que os pontos θ, $T_\lambda^k(\theta)$, $T_\lambda^{2k}(\theta)\ldots$ dividem S^1 em arcos de comprimento menor que ϵ. ■

3 Caos em S^1

Analisada a dinâmica básica de funções no círculo e definidos os pontos fixos e periódicos, podemos verificar se seu comportamento é caótico ou não. Para isso, seja J um espaço métrico e consideremos as definições abaixo.

Definição 3.1. *A função $f : J \to J$ é topologicamente transitiva se para qualquer par de intervalos abertos $U, V \in J$ existe $n > 0$ de modo que $f^n(U) \cap V \neq \emptyset$.*

Intuitivamente, uma função topologicamente transitiva possui pontos que eventualmente se movem sob uma iteração, de uma pequena vizinhança arbitrária para outra. Consequentemente, o sistema dinâmico não pode ser decomposto em dois intervalos abertos e disjuntos que não variam com a função. Perceba que se a função possui uma órbita densa, então claramente ela é transitiva.

Definição 3.2. *$f : J \to J$ possui uma dependência sensitiva das condições iniciais se existe $\delta > 0$ de modo que, para todo $x \in J$ e qualquer vizinhança N de x existe $y \in N$ e $n \geq 0$ de modo que $\mid f^n(x) - f^n(y) \mid > \delta$.*

Logo, uma função possui dependência sensitiva das condições iniciais se existem pontos perto de x que eventualmente são separados de x por pelo menos δ sob a iteração de f.

Definição 3.3. *A função f é dita caótica em J se: f possui dependência sensitiva das condições iniciais; f é topologicamente trasitiva; pontos periódicos são densos em J.*

Resumindo, podemos afirmar que uma função caótica possui três componentes: imprevisibilidade, indecomponibilidade e algum elemento de regularidade. Um sistema caótico é imprevisível por causa de sua dependência sensitiva das condições iniciais. Ele não pode ser decomposto em subsistemas que não sofrem iteração de f pois são topologicamente transitivos. E, por fim, durante o comportamento, existe um elemento de regularidade, ou seja, os pontos periódicos, que são densos.

Exemplo 3: Uma rotação irracional do círculo é topologicamente transitiva, mas não possui dependência das condições iniciais, uma vez que todos os pontos matêm a mesma distância após a iteração. Logo a rotação irracional no círculo não apresenta comportamento caótico.

Exemplo 4: A função $f : S^1 \to S^1$ dada por $f(\theta) = 2\theta$ apresenta comportamento caótico. A distância angular entre dois pontos é dobrada com a iteração de f. Isso significa que f possui depedência sensitiva das condições iniciais. A transitividade topológica também segue desta observação, uma vez que qualquer arco pequeno em S^1 é eventualmente expandido por algum f^k para cobrir todo S^1 e, em particular, qualquer outro arco em S^1. Podemos dizer que a função também possui uma forte forma de dependência sensível chamada expansividade.

4 Conclusão

A partir da proposição 1.1, do teorema 2.2 e das definições apresentadas neste trabalho, é possível concluir que aplicações no círculo unitário apresentam rica dinâmica. Apresentando comportamento caótico ou não, podemos afirmar que aplicações em S^1 oferecem diversas oportunidades para o estudo de sistemas dinâmicos complexos e para a descoberta de novos comportamentos. Espera-se que este trabalho tenha fornecido uma introdução útil e acessível a esse campo da matemática.

Agradecimentos

O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brasil (CNPq) através do programa de Iniciação Ciêntífica e Mestrado (PICME).

Referências

[1] R.L DEVANEY. **An Introduction To Chaotic Dynamical Systems**. 2a. ed. Addison-Wesley Publishing Company, 1986. isbn:0-201-13046-7

Em intervalos transitividade implica caos

Vitor Eduardo Pereira

Universidade Federal de Uberlândia, Faculdade de Engenharia Mecânica, Uberlândia, Minas Gerais, Brasil

vitor.eduardo@ufu.br

Jean Venato Santos

Universidade Federal de Uberlândia, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil

jvenatos@ufu.br

Palavras-chave

Dinâmicas caóticas.
Caos segundo Devaney.
Redução no caos de Devaney.

Resumo

A definição de caos segundo Devaney diz que pra uma função ser caótica ela deve satisfazer três propriedades: ter densidade de pontos periódicos, ser transitiva e sensível às condições iniciais. Contudo, é possível propor algumas reduções para a ocorrência do caos, de forma que duas ou apenas uma das propriedades já seja suficiente para implicar a caoticidade. E uma delas, provada por Berglund e Vellekoop, é que, em intervalos, a transitividade irá implicar no caos. Neste trabalho, tal redução é apresentada e, por meio de exemplos, é estabelecido que outras reduções não são possíveis.

1 Introdução

A definição de caos para funções $f\colon X \to X$ definidas num espaço métrico X, introduzida por Devaney em [3] envolve três condições. A primeira delas se refere ao conjunto dos pontos periódicos de f, ou seja, pontos $x \in X$ tais que $f^n(x) = x$, para algum natural n. A propriedade é que o *conjunto dos pontos periódicos seja denso* em X. A segunda característica de sistemas caóticos é a *transitividade*, a qual estabelece que para qualquer par de pontos x e y em X, e qualquer $\varepsilon > 0$, existem n natural e um ponto $z \in X$ que está ε-próximo de x e tal que $f^n(z)$ está ε-próximo de y. A condição final é a *sensibilidade às condições iniciais* que ocorre se existir um $\beta > 0$ tal que para quaisquer x em X e $\varepsilon > 0$, há um y que está ε-próximo de x e um n natural tais $f^n(x)$ e $f^n(y)$ distam pelo menos β. Em resumo:

Definição 1.1. ***[Caos de Devaney [3]]*** *Seja X um espaço métrico. Uma função $f\colon X \to X$ é dita caótica em X se:*

1. *os pontos periódicos de f são densos em X,*
2. *f é transitiva,*
3. *f depende sensivelmente das condições iniciais.*

Em [1] Banks et al mostraram a seguinte redução na Definição 1.1:

Teorema 1.2 (Banks et al [1])**.** *Seja X um espaço métrico. Se uma função contínua $f\colon X \to X$ é transitiva e possui densas órbitas periódicas então f depende sensivelmente das condições iniciais.*

Para funções contínuas definidas em intervalos, Berglund e Vellekoop obtiveram a seguinte redução:

Teorema 1.3 (Berglund e Vellekoop [2])**.** *Sejam I um intervalo, não necessariamente limitado, e $f\colon I \to I$ uma função contínua. Se f é transitiva em I então f é caótica em I.*

Baseados em [2], no que segue, apresentaremos a demonstração deste resultado. Note que, pelo Teorema 1.2, será suficiente mostrar que a transitividade de f implica densidade de pontos periódicos de f em I. Ainda em [2], Berglund e Vellekoop deram exemplos que ilustram a impossibilidade de outras reduções no caos de Devaney para funções contínuas definidas em intervalos. Tais exemplos serão apresentados na Seção 3.

2 Demonstração do Teorema 1.3

Para demonstrar o teorema faz-se necessário o uso do seguinte lema:

Lema 2.1. *Sejam I um intervalo, não necessariamente limitado, e $f : I \to I$ uma função contínua. Se $J \subset I$ for um intervalo que não contém pontos periódicos de f e $z \in J$ é tal que $f^m(z)$ e $f^n(z) \in J$ com $0 < m < n$, então $z < f^m(z) < f^n(z)$ ou $z > f^m(z) > f^n(z)$.*

Demonstração. Suponha por absurdo que exista um $z \in J$ satisfazendo $f^m(z),\ f^n(z) \in J, z < f^m(z)$ e $f^m(z) > f^n(z)$, com $0 < m < n$. Defina a função $g(x) = f^m(x)$. Sabe-se que $z < g(z)$, vamos provar que isso implica que $z < g(z) < g^{(k+1)}(z)$, para todo natural $k \geq 1$. Com efeito, se isto não ocorre, seja k_0 o menor natural tal que $g^{(k_0+1)}(z) < g(z)$. Assim, para a função $g^{k_0}(x) - x$, teríamos $g^{k_0}(z) > g(z) > z$, ou seja, $g^{k_0}(z) - z > 0$ e também que $g^{k_0}(g(z)) - g(z) < 0$. Mas, pelo Teorema do Valor Intermediário, isto implica que existe um ponto $c \in]z,\ g(z)[\subset J$ com $g^{k_0}(c) - c = 0$, fornecendo um ponto $k_0 m$-periódico de f em J. Então, $z < g^k(z)$ para todo $k > 0$, em particular para $k = n - m > 0$, segue que $z < f^{((n-m)m)}(z)$, ou seja, $0 < f^{((n-m)m)}(z) - z$.

Agora usando $f^n(z) = f^{(n-m)}(f^m(z)) < f^m(z)$, tomando $h = f^{(n-m)}$ vamos mostrar que $h^{(k+1)}(f^m(z)) < h(f^m(z)) < f^m(z)$, para todo natural $k \geq 1$. De fato, do contrário, tome k_0 o menor natural tal que $h^{(k_0+1)}(f^m(z)) > h(f^m(z))$. Neste caso, para a função $h^{k_0}(x) - x$, temos $h^{k_0}(f^m(z)) - f^m(z) < 0$ e $h^{k_0}(h(f^m(z))) - h(f^m(z)) > 0$. Assim, pelo Teorema do Valor Intermediário, existe $d \in]f^m(z),\ h(f^m(z))[\subset J$ tal que $h^{k_0}(d) = d$, fornecendo um ponto $k_0(n-m)$-periódico de f em J. Tal contradição mostra que $h^k(f^m(z)) < f^m(z)$, para todo natural $k \geq 1$. Em particular, se $k = m$ segue que $f^{((n-m)m)}(f^m(z)) - f^m(z) < 0$.

Dos parágrafos acima e do Teorema do Valor Intermediário existe $y \in]z,\ f^m(z)[\subset J$ tal que $f^{((n-m)m)}(y) - y = 0$, fornecendo um ponto periódico de f em J, tal contradição prova o Lema. ■

Este resultado é suficiente para a:

Demonstração do Teorema 1.3.

Pelo Teorema 1.2 é suficiente provar que se I é um intervalo e $f : I \to I$ é uma função contínua, a transitividade de f implica que o conjunto dos pontos periódicos de f será denso em I.

Suponha, por absurdo, que exista um intervalo aberto $J \subset I$ sem pontos periódicos de f. Tome um $x \in J$, um conjunto aberto $N \subsetneq J$ contendo x e outro intervalo aberto $E \subset J \setminus N$. Se f é transitiva em I, então existe um $m > 0$, para o qual $f^m(N) \bigcap E \neq \varnothing$ e então um $y \in J$ com $f^m(y) \in E \subset J$. Como J não contém pontos periódicos, segue que $y \neq f^m(y)$ e como f é contínua existe uma vizinhança U de y com $f^m(U) \bigcap U = \varnothing$. Se U é um intervalo aberto, pela transitividade, novamente, pode-se encontrar um $n > m$ e um $z \in U$ com $f^n(z) \in U$. Mas então teríamos $0 < m < n$ e $z, f^n(z) \notin U$ e isso viola o lema acima. De fato, temos $z,\ f^m(z),\ f^n(z) \in J$ com $0 < m < n$, tais que $f^m(z)$ nunca está entre z e $f^n(z)$, uma vez que os dois últimos estão no intervalo U e $f^m(z)$ está fora de U. ■

3 Exemplos

A seguir são apresentados exemplos, dados em [2], que estabelecem a impossibilidade de outras reduções na definição de caos além das mencionadas acima.

Iniciamos observando que a função identidade ($y = x$), fornece uma dinâmica contínua num intervalo com densidade de pontos periódicos porém sem apresentar transitividade e nem sensibilidade às condições iniciais.

O próximo exemplo mostra que para uma função contínua num intervalo, sensibilidade às condições iniciais e densidade de pontos periódicos, não garantem transitividade.

Exemplo 3.1. *Defina em $I = \mathbb{R}_+$ a função*

$$f(x) = \begin{cases} 3x & \textit{se} \quad 0 \leq x < \frac{1}{3} \\ -3x + 2 & \textit{se} \quad \frac{1}{3} \leq x < \frac{2}{3} \\ 3x - 2 & \textit{se} \quad \frac{2}{3} \leq x < 1 \\ f(x-1) + 1 & \textit{se} \quad 1 \leq x \end{cases} .$$

Com o esboço de parte do gráfico de f, visto na Figura 1, induz-se que o comportamento de f no quadrado $[0,1] \times [0,1]$ irá se repetir em cada quadrado $[n, n+1] \times [n, n+1]$ do plano xy. Sendo assim, é suficiente entender a dinâmica da função no primeiro destes quadrados.

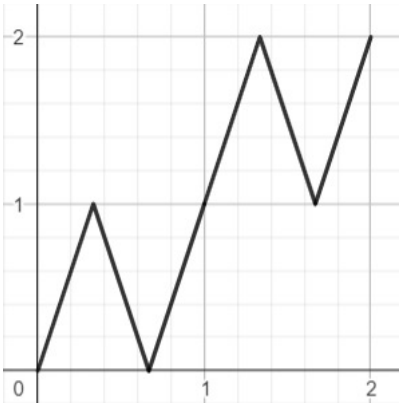


Figura 1: Gráfico de $f(x)$

Na Figura 2 é exposto o comportamento do gráfico de f^2 no intervalo $[0,1]$.

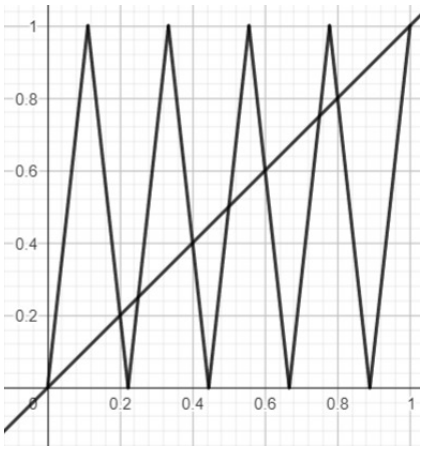


Figura 2: Gráfico de $f^2(x)$ para o intervalo $[0,1]$ sobreposto pela função identidade

Note que enquanto o gráfico da f em $[0,1]$ é constituído de 3 segmentos de retas, o gráfico da f^2 é constituído por 9 segmentos de retas o que permite induzir que quando a f é iterada, a quantidade de

tais segmentos de retas é multiplicado por três, e o intervalo no eixo x associado a cada segmento é divido por três sendo todos uniformemente distribuídos no intervalo $[0, 1]$.

Assim, pode ser induzido que o número de segmentos de retas da n-ésima iterada f^n de f é dado por 3^n com intervalos de comprimento $1/3^n$. Isto permite concluir que dado um subintervalo qualquer $J \subset [0, 1]$ de raio ϵ existirá um $n \in \mathbb{N}$ para o qual a imagem $f^n(J) = [0, 1]$, o que implicará na interseção entre os gráficos de f^n e a identidade ocorrendo dentro do intervalo J, o que prova a densidade de pontos periódicos. Além disto, fazendo $\beta = 1/2$ e dado $x \in J$ existirá um $y \in J$, que estará ϵ-próximo de x, para o qual $f^n(y)$ estará a, pelo menos, β de distância de $f^n(x)$, o que mostra a sensibilidade às condições iniciais.

Ainda observando o gráfico de f, concluímos que para $f([0, 1]) = [0, 1]$, isto implica que $f : [0, 2] \to [0, 2]$ não é transitiva.

A seguir é apresentada uma função contínua num intervalo com sensibilidade às condições iniciais sem densidade de pontos periódicos.

Exemplo 3.2. *Considere a função $g(x)$ definida no intervalo $I = [0, \frac{3}{4}]$ por*

$$g(x) = \begin{cases} \frac{3}{2}x & \text{se} \quad 0 \leq x < \frac{1}{2} \\ \frac{3}{2}(1-x) & \text{se} \quad \frac{1}{2} \leq x \leq \frac{3}{4} \end{cases} .$$

O gráfico dessa função pode ser visualizado na Figura 3.

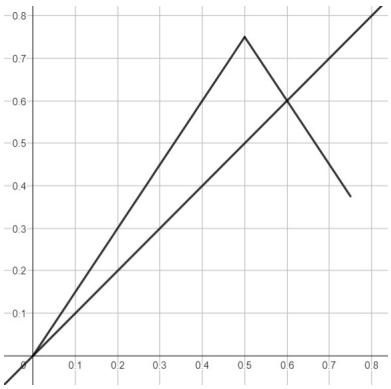


Figura 3: Gráfico de $g(x)$ sobreposto pela função identidade

Analisando os gráficos de g e de $g^2(x)$, que pode ser visto na Figura 4, é possível induzir que dado um ponto no intervalo $]0, 3/8[$ em algum momento sua órbita irá cair no intervalo $[3/8, 3/4]$ e a partir daí tal órbita nunca mais retorna ao intervalo $]0, 3/8[$.

Uma primeira consequência desta propriedade é que g não terá pontos periódicos em $]0, 3/8[$ e portanto não apresentará densidade de pontos periódicos.

Outra consequência é que g será invariante no intervalo $[3/8, 3/4]$, ou seja, as iteradas de pontos neste intervalo permanecem nele. Sendo assim, como ambas partes da função tem fator multiplicativo $3/2 > 1$, dado qualquer subintervalo J de $[0, 1]$, para n suficientemente grande, sua iterada $g^n(J)$

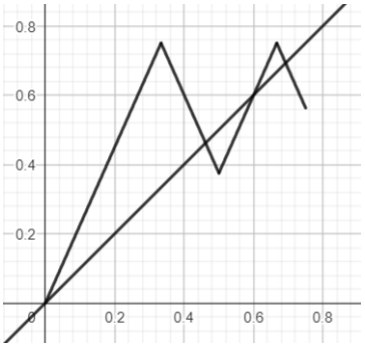


Figura 4: Gráfico de $g^2(x)$ sobreposto pela função identidade

conterá o intervalo $[3/8, 3/4]$. *Portanto, por raciocínio análogo ao do exemplo anterior, é possível concluir que* g *é sensível com* $\beta = (3/8 + 3/4)/2 = 9/16$.

4 Considerações finais

Com base em [2], foi demonstrado que para funções contínuas definidas em intervalos da reta real, a transitividade é suficiente para obter a caoticidade da função. Para isto, foi usado uma redução dada em [1] que diz que densidade de pontos periódicos e transitividade implicam sensibilidade às condições iniciais. Além disso, por meio de exemplos, ficou estabelecida a impossibilidade de outras reduções na definição de caos além destas.

Agradecimentos

Na condição de bolsista do PIBIC, agradeço ao CNPq pelo fomento.

Referências

[1] BANKS, J.; BROOKS, J.; CAIRNS, G.; DAVIS, G.; STACEY, P. On Devaney's definition of chaos, **The American Mathematical Monthly**. 99, 332-334, 1992.

[2] BERGLUND, R.; VELLEKOOP, M. On Intervals, Transitivity = Chaos. **The American Mathematical Monthly**. 101, 353-355, 1994.

[3] DEVANEY, R. L. **An introduction to chaotic dynamical systems**. Addison-Wesley, 1989.

A definição de Entropia de Boltzmann

Keoma Hermenegildo Kurashima
UFU, Instituo de Física, Uberlândia, MG, Brasil
keoma.kurashima@ufu.br

Juliano Gonçalves Oler
UFU, Departamento de Matemática, Uberlândia, MG, Brasil
jgoler@ufu.br

Palavras-chave

Entropia.
Logaritmo.
Boltzmann.

Resumo

A Entropia é uma grandeza Física abstrata que foi estudada e dado uma formulação estatística por Ludwig Eduard Boltzmann. Em um primeiro contato com a formula de Boltzmann, nos cursos de física básica, parece intuitiva a sua definição. Contudo uma pergunta interessante seria: existe uma outra função que possa representar os pré-requisitos do *gedankenexperiment* da expansão livre de um gás? Nesse trabalho daremos a resposta para tal questão.

1 Introdução

Nos cursos básicos de física se encontra o primeiro contato com a Segunda Lei da termodinâmica a "entropia", onde a variação da entropia em sistemas fechados é estudado. Podemos atribuir a lei ao estudo empírico dos físicos e engenheiros que trabalhavam na área da termodinâmica. Graças ao *gedankenexperiment* da expansão livre de um gás, a saber:

> "Há um paralelismo completo entre a evolução do macroestado de um sistema no sentido da probabilidade crescente e o princípio de aumento da entropia, o que nos leva a inferir que a entropia deve ser uma medida de probabilidade termodinâmica." [1].

Na mecânica estatística, a fórmula de entropia de Boltzmann (também conhecida como equação de Boltzmann-Planck) é uma equação que permite calcular a entropia e o número de micro-estados de um sistema específico. A fórmula de Boltzmann mostra a relação entre a entropia e o número de maneiras pelas quais os átomos e moléculas de um sistema termodinâmico podem ser organizados.

Através de estudos empirícos, Boltzmann observou que a entropia é uma grandeza que pode ser representada por uma função real $f(x)$, tal que para todo $x \in \mathbb{R}$ é crescente, isto é,

i) f é crescente, isto é $x < y \Leftrightarrow f(x) < L(y)$,

e aditiva, ou seja,

ii) $f(x \cdot y) = f(x) + f(y)$,

uma vez que a entropia dos sistemas resultantes S é a soma das entropias, porém como os sistemas são independentes a probabilidade P é o produto das probabilidades. Logo,

$$P = P_1 \cdot P_2 \Rightarrow S = S_1 + S_2$$

Nesse contexto, dizemos que f é uma função de Entropia de Boltzmann, se f satistaz as condições (i) e (ii) definidas anteriormente, mais precisamente, se o conjunto

$$E = \left\{ f \in F(\mathbb{R}^+, \mathbb{R}) \quad | \quad f \text{ satifaz (i) e (ii)} \right\},$$

é não vazio.

Pergunta. Após os estudos de Boltzmann, uma questão natural a ser respondida é: o conjunto E é não vazio? Ou seja, existem funções que satisfazem as duas propriedades observadas por Boltzmann?.

O próximo resultado dá uma resposta positiva a esta pergunta. Seja $f \in F(\mathbb{R}, \mathbb{R})$. O conjunto gerado por f, denotado por $< f >$, é definido por:

$$< f >= \{ g \in F(\mathbb{R}, \mathbb{R}) \quad | \quad g = kf, \text{com } k \in \mathbb{R} \}.$$

Nestas condições, temos o seguinte resultado:

Teorema 1.1. *Se $f \in F(\mathbb{R}, \mathbb{R})$, então $E =< \ln(x) >$.*

2 Prova do Resultado

Prova do Teorema 1. Para provar o Teorema 1, temos que mostrar que

(a) $< \ln x > \subset E$;

(b) $E \subset < \ln x >$.

Para verificarmos a inclusão do item (a) temos que mostrar que todo elemento de $< \ln x >$ é crescente e aditivo. A prova do item (b) será feito mostrando que, qualquer função do conjunto E pode se gerada a partir de uma outra função do conjunto.

Lema 2.1. A função $\log x$ é crescente e aditiva. Logo $< \ln x >$ também compartilha da mesma propriedades.

Demonstração. Seja $f \in < \ln x >$. então $f(x) = k \ln x$, onde $k \in \mathbb{R}$. Definimos o $\ln x$ como

$$\ln x = \int_1^x (1/t)\, dt.$$

Primeiramente, vamos mostrar que $f(x)$ é crescente. De fato, se $x_1 < x_2$, usando a definição de $\ln x$, bem como e as propriedades de integrais, temos

$$\begin{aligned} \log x_2 - \log x_1 &= \int_1^{x_2} (1/t)\, dt - \int_1^{x_1} (1/t)\, dt \\ &= \int_1^{x_2} (1/t)\, dt + \int_1^{x_1} (1/t)\, dt \\ &= \int_{x_1}^{x_2} (1/t)\, dt. \end{aligned}$$

Como $1/t \geq 1/x_2$, para todo $t \in [x_1, x_2]$, usando o Corolário do Teorema 1 de [2]. pág. 346-348. Temos

$$0 < (1/x_2)(x_2 - x_1) \leq \int_{x_1}^{x_2} (1/t)\, dt = \log x_2 - \log x_1.$$

Logo, $\log x_2 > \log x_1$, se $x_2 > x_1$.

Agora, vamos provar que f é aditiva. Se a e b são reais positivos, então

$$\log (ab) = \log a + \log b.$$

Considere a função $g(x) = \log(ax)$, $\forall x > 0$. g é uma função composta $g = \log \circ h$, onde $h(x) = ax$. Pelo teorema sobre derivação de funções compostas, temos:

$$g'(x) = (\log)'(h(x)) - h'(x),$$

ou seja

$$g'(x) = \frac{1}{ax} \cdot a = \frac{1}{x}.$$

Logo

$$(g(x) - \log(x))' = g'(x) - \log'(x) = \frac{1}{x} - \frac{1}{x} = 0,$$

o que implica que $g(x) = \log x + k$, onde k é uma constante, portanto

$$\log(ax) = \log x + k$$

para todo $x > 0$. Fazendo $x = 1$, temos

$$\log(a) = \log 1 + k = \int_1^1 (1/t)\, dt + k = 0 + k.$$

Logo,

$$\log(ax) = \log a + \log x$$

para todo $x > 0$. Em particular, para $x = b$ temos (2.1). ■

Logo, como $f(x)$ é crescente e aditiva, então temos que $f(x) \in E$. Dessa forma, $< \ln x > \subset E$ o que mostra (a). Resta mostrarmos o item (b). O item (b) segue do próximo lema:

Lema 2.2. *Se $f_1, f_2 \in E$, então existe $k > 0$ tal que $f_2(x) = k \cdot f_1(x)$ para todo $x > 0$.*

Demonstração. Suponha que exista um número $a \neq 1$ tal que $f_1(a) = f_2(a)$. Para fixar ideias, digamos que $a > 1$. Logo temos que $f_1(a^r) = f_2(a^r), \forall r \in \mathbb{Q}$. Pela propriedade 6 de [3], temos que $f_1(a^r) = r f_1(a) = r f_2(a) = f_2(a^r)$. Suponhamos que exista algum $b > 0$ tal que $f_1(b) \neq f_2(b)$. Por exemplo $f_1(b) < f_2(b)$. Escolha um $n \in \mathbb{Z}$ de tal modo que

$$f_1(a) < n \cdot [f_2(b) - f_1(b)].$$

Então

$$f_1(a^{1/n}) = \frac{1}{n} \cdot f_1(a) < f_2(b) - f_1(b).$$

Por simplicidade, escrevemos $c = f_1(a^{1/n})$. Os numeros $c, 2c, 3c, ...$ dividem $\mathbb{R}$ em invervalos justapostos de mesmo comprimento c. Como $c < f_2(b) - f_1(b)$, pelo menos um desses números, digamos $m \cdot c$, pertence ao interior do intervalos $(f_1(b), f_2(b))$, ou seja, $f_1(b) < m \cdot c < f_2(b)$.
Assim temos,

$$m \cdot c = m \cdot f_1(a^{1/n}) = f_1(a^{m/n}) = f_2(a^{m/n})$$

Então

$$f_1(b) < f_1(a^{m/n}) = f_2(a^{m/n}) < f_2(b).$$

Como f_1 e f_2 são crescentes, pela propriedade i), temos da primeira parte da desigualdade que $f_1(b) < f_1(a^{m/n}) \Rightarrow b < a^{m/n}$, e da segunda parte $f_1(a^{m/n}) < f_2(b) \Rightarrow a^{m/n} < b$. Logo $b = a$, contrariando a nossa hipótese incial, $f_1(b) \neq f_2(b)$. Esta contradição mostra que b não existe. Assim se $\exists a \neq 1 \in \mathbb{R}^+$ tal que $f_1(a) = f_2(a) \Rightarrow f_1(x) = f_2(x), \forall x > 0$.

Agora, $f_1, f_2 \in \mathcal{C}$. Seja $k = f_2(a)/f_1(a), \forall a \neq 1$. Pegue $f_3 \in \mathcal{C}$, definido por $f_3(x) = k \cdot f_1(x)$. Como $f_3(a) = k \cdot f_1(a) = [f_2(a)/f_1(a)] \cdot f_1(a) = f_2(a)$, segue-se do que foi provado acima que, $f_3(x) = f_2(x), \forall x > 0$, ou seja, que $f_2(x) = k \cdot f_1(x), \forall x > 0$, como queríamos demostrar. ■

Como $\ln x, f \in E$. Segue que existe um $k \in \mathbb{R}$. tal que $f(x) = k \ln x$. Logo, $f \in < \ln x >$ o que mostra que $E \subset < \ln x >$. Portanto, por (a) e (b) concluímos a prova do Teorema 1 ■

3 Conclusão

Assim concluímos que o conjunto E é não vazio e gerado pela função logarítmica. Contudo ainda existe muitas questões em aberto sobre o conceito e a função de Entropia. Quais são suas propriedades e significado? E quais são as relações das diversas definições de Entropia em outras áreas do conhecimento?

Referências

[1] NUSSENZVEIG, H. M. **Curso de Física Básica: Fluidos, Oscilações e Ondas, Calor**. 4ª Edição. Rio de Janeiro: Blucher, 2002.

[2] LIMA, E. L. **Curso de análise volume 2**. 11ª Edição. Rio de Janeiro: IMPA, 2010.

[3] LIMA, E. L. **Logaritmos**. 2ª Edição. Rio de Janeiro: GRAFTEX Comunicação Visual Ltda, 1996.

Códigos Reed-Solomon

Guilherme Cabral de Menezes
Faculdade de Computação, UFU, Uberlândia-MG, Brasil
guilherme.cabral@ufu.br

Alonso Sepúlveda Castellanos
Faculdade de Matemática, UFU, Uberlândia-MG, Brasil
alonso.castellanos@ufu.br

Palavras-chave

Códigos corretores
Códigos cíclicos
Códigos Reed-Solomon

Resumo

Podemos garantir que a computação só está muito evoluida hoje por conta da matemática, e um grande exemplo disso são os códigos corretores de erros, vendo que a matemática auxília a computação a realizar tarefas como envio de mensagens que ao nosso ver não produz erros. Dessa forma, esse trabalho tem a finalidade de mostrar de uma forma detalhada e compreensiva como esse processo é realizado em um código conhecido como Reed-Solomon.

1 Introdução

Às vezes temos a sensação de que não ocorre erros no computador, sempre ocorre tudo dentro do esperado, mas será que erros ocorrem no computador? Claro que ocorrem, principalmente em meios de comunicação como a televisão, por conta de interferências. Porém quando uma mensagem por exemplo é enviada de uma pessoa a outra não é um simples processo de mandar a mensagem, é nessário fazer alguns ajustes na mensagem com a possibilidade de corrigilá, e assim entramos em um tópico muito importante na computação, os códigos corretores de erros.

2 Conceitos básicos

Os códigos corretores de erros simplesmente codificam e depois decodificam a mensagem, dessa forma vamos discutir sobre um tipo especifíco de código, os códigos de Reed-Solomon, porém vamos primeiramente entender alguns conceitos básicos sobre códigos corretores de erros antes de continuarmos.

Nos preocupamos agora em códigos lineares $C \subseteq \mathbb{F}_q^n$, que são subespaços vetoriais sobre o corpo finito $\mathbb{F}_q$ (ver [1, Capítulo 3]).

Definição 2.1 *Dado um código linear* $C \subseteq \mathbb{F}_q^n$ *com* $x, y \in C$*, a distância de Hamming, denotada* $d(x, y)$*, é o número de posições em que essas palavras do código diferem.*

Definição 2.2 *A distância miníma de um código* C *é definada como:*

$$d = \min\{d(x, y) : x, y \in C, x \neq y\}$$

Definição 2.3 *Um código linear* C *é descrito como* $[n, k, d]$ *sobre um alfabeto* $\mathbb{F}_q$*, onde* n *é o comprimento da palavra codificada,* k *a dimensão do código e* d *a distâcia miníma do código.*

Quando estivermos em códigos cíclicos é bem comum não saber d facilmente, assim vamos denotar um código também como $[n, k]$, ou seja, omitindo a distância miníma do código.

Definição 2.4 *Dado um código linear* C *descrito como* $[n, k, d]$*, vale a seguinte desigualdade*

$$d \leq n - k + 1$$

conhecida como Cota de Singleton, onde os códigos que valem a igualdade são conhecidos como MDS *(Maximum Distance Separable).*

Exemplo 2.5 *Vamos criar um código* $C = [5, 2, d]$ *com quatro elementos sobre* $\mathbb{F}_2$

$$p_1 = (00000),\ p_2 = (11100),\ p_3 = (00111),\ p_4 = (11011)$$

Tomando a definição de distância de Hamming vamos encontrar distância mínima do código.

$$d(p_1, p_2) = 3,\ d(p_1, p_3) = 3,\ d(p_1, p_4) = 4,\ d(p_2, p_3) = 4,\ d(p_2, p_4) = 3,\ d(p_3, p_4) = 3$$

Assim a distância mínima do código C *é* $d = 3$*.*

Com essa definição de *distância miníma de Hamming* já é possível definir nossa estratégia de decodificação: para qualquer n-tupla r recebida após passar pelo canal de comunicação, existe uma única palavra $c \in C$ tal que

$$d(r, c) = \min\{d(r, x) : x \in C\}$$

onde podemos então decodificar r como c.

Teorema 2.6 *Dado* $C \subseteq \mathbb{F}_q^n$ *um código linear na forma* $[n, k, d]$*, conseguimos corrigir no máximo* $\left\lfloor \frac{d-1}{2} \right\rfloor$ *erros, e detectar no maximo* $d - 1$ *erros.*

3 Matrizes geradoras e teste de paridade

Até o momento não realizamos nada que realmente codifica nossa mensagem m de tamanho k para uma palavra de tamanho n, pois a escolha desse processo pode variar muito, vendo que afetará bastante na distância miníma do nosso código.

Definição 3.1 *A matriz geradora* G *de um código linear* $C \subseteq \mathbb{F}_q^n$ *é uma matriz de tamanho* $k \times n$ *onde suas linhas são formadas por uma base ordenada* $\beta = \{v_1, v_2, \ldots, v_k\}$ *tal que*

$$\begin{aligned} T : \mathbb{F}_q^k &\to \mathbb{F}_q^n \\ a &\mapsto aG \end{aligned}$$

A matriz geradora de um código $C - [n, k, d]$ serve para codificar uma mensagem de tamanho k para uma palavra de tamanho n. Para nos auxiliar a decodificar a mensagem transmitida, vamos agora definir os códigos duais.

Definição 3.2 *Seja* $C \subseteq \mathbb{F}_q^n$ *um código linear* $[n, k, d]$ *sobre* $\mathbb{F}_q$*, existe um código* $C^\perp$ *tal que*

$$C^\perp = \{v \in \mathbb{F}_q^n : \sum_{i=0}^{n-1} v_i u_i = 0, \forall u \in C\}$$

Corolário 3.3 $(C^\perp)^\perp = C$.

Lema 3.4 *Seja* $a \in C^\perp \Leftrightarrow Ga^T = 0$.

Seja H uma matriz geradora de $C^\perp$ temos pelo **Corolário 3.3** e **Lema 3.4** que $v \in C \Leftrightarrow v \in (C^\perp)^\perp \Leftrightarrow Hv^T = 0$. A matriz H que gera $C^\perp$ é chamada teste de paridade de C, e com ela fica mais fácil saber se $v \in C$, além disso essa matriz será fundamental na parte da decodificação da palavra.

Definição 3.5 *Seja* C *um código linear com matriz teste de paridade* H*, dado* $v \in C$*, chamaremos o vetor* Hv^T *de síndrome de v.*

Com essa definição de síndrome, poderemos definir como realmente ocorrerá a decodificação: dado que queremos enviar uma mensagem m, codificamos a mensagem para c, porém após passar pelo canal de comunicação recebemos r, então $e = r - c$, sendo e nosso vetor erro, e como por definição temos $Hc^T = 0$, temos que

$$He^T = H(r^T - c^T)^T = Hr^T - Hc^T = Hr^T = s$$

Dado um código que pode corrigir até t erros, se o número de coordenadas não nulas do vetor e for menor que t, então pode-se provar a unicidade de e, assim já temos o suficiente para codificar e decodificar uma mensagem, porém ainda é bem complicado de encontrar essas matrizes e utilizá-las com facilidade, assim vamos tentar melhorar a forma como essas matrizes estão estruturadas.

Proposição 3.6 *Seja* $G = (A|I_k)$ *uma matriz geradora de* C*, então* $H = (I_{n-k}| - A^T)$ *é uma matriz geradora de* $C^\perp$*. Essa forma de orgranizar as matrizes é conhecida como forma padrão.*

Agora apesar de não nos preocuparmos ainda em realmente codificar e decodificar, já possuimos ferramentas para tal, agora podemos utilizá-las para ver alguns tipos específicos de códigos.

4 Códigos cíclicos

Definição 4.1 *Um código* $C-[n,k,d]$ *sobre* $\mathbb{F}_q$ *é denominado cíclico se, e somente se,* $\forall a \in C$*, é verdade que* $a' \in C$*, onde* $a=(a_0,a_1,\ldots,a_{n-1})$ *e* $a'=(a_{n-1},a_0,a_1,\ldots,a_{n-2})$*.*

Porém essa definição de códigos cíclicos é bem díficil de concluir algumas informações, com isso vamos definir a seguinte transformação linear

$$\begin{gathered} T:\mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n-1\rangle \\ (a_0,a_1,\ldots,a_{n-1}) \mapsto [a_0+a_1x+\cdots+a_{n-1}x^{n-1}] \end{gathered}$$

Levando em consideração polinômios de $\mathbb{F}_q[x]$ sobre o polinômio $f(x)=x^n-1$, a operação de *shift* (que transforma a em a') é simplesmente multiplicar o polinômio associado por x, pois $x^n \equiv 1 (\mathrm{mod}\ f(x))$, dessa forma

$[x\cdot[a_0+a_1x+\cdots+a_{n-1}x^{n-1}] \equiv [a_0x+a_1x^2+\cdots+a_{n-2}x^{n-1}+a_{n-1}x^n] \equiv [a_{n-1}+a_0x+a_1x^2+\cdots+a_{n-2}x^{n-1}]$

O espaço gerado pelo polinômio $g(x) \in \mathbb{F}_q[x]/\langle x^n-1\rangle$ é um subespaço de $\mathbb{F}_q[x]/\langle x^n-1\rangle$. Quando o polinômio $g(x)$ for um divisor mônico de $f(x)$, esse subespaço será cíclico.

Exemplo 4.2 *Considerando* $f(x)=x^4-1$ *e* $g(x)=1+x^2$ *será gerado o seguinte subespaço cíclico*

$S=T^{-1}(\langle g(x)\rangle)=\{(0000),(1010),(0101),(1111)\}$

Teorema 4.3 *Dado* $g(x)$ *um divisor mônico de* $f(x)=x^n-1$ *de grau* $n-k$*, então* $g(x)$ *gera um subespaço cíclico* S *de* $\mathbb{F}_q[x]$ *de dimensão* k*.*

A base $\beta=\{g(x),xg(x),\ldots,x^kg(x)\}$ já seria o suficiente para codificar a mensagem, porém como explicado no capítulo anterior, para facilitar vamos encontrar uma base β' tal que nossa matriz geradora seja da forma $G=(I_k|A)$. Dessa forma, encontraremos a matriz teste de paridade com mais facilidade.

Proposição 4.4 *Seja* $g(x)$ *um polinômio gerador de um código cíclico* $C-[n,k,d]$ *sobre* $\mathbb{F}_q$*. Assim, podemos obter uma matriz geradora* G *de* C *com a seguinte base*

$$\beta'=\left\{\tfrac{x^{n-k+i}}{g(x)} : 0\le i\le k-1\right\}.$$

O conjunto $\beta'=\left\{\frac{x^{n-k+i}}{g(x)} : 0\le i\le k-1\right\}$ é uma base que gera o mesmo subespaço cíclico que $g(x)$, logo teremos que o código C terá matriz geradora e matriz teste de paridade definadas da forma $G=(A|I_k)$ e $H=(I_{n-k}|-A^T)$, respectivamente, onde A é uma matriz $k\times(n-k)$.

Dado que ao codificar a mensagem obtivemos c e recebemos a mensagem r após passar pelo meio de comunicação, a síndrome $s=Hr^T$ nos ajudará na decodificação da mensagem, porém na representação polinomial o cálculo da síndrome é um pouco mais fácil de se realizar.

Teorema 4.5 *Dados* $r(x)$ *e* $s(x)$ *os polinômios que representam a mensagem recebida* r *e a síndrome de* r *após realizar a transformação linear, temos que* $s(x)$ *é o resto da divisão de* $r(x)$ *por* $g(x)$*.*

Teorema 4.6 *Seja um código* $C-[n,k]$ *sobre* $\mathbb{F}_q$ *gerado por* $g(x)$*, dado* $r(x)$*, que representa a mensagem recebida, com síndrome* $s(x)=\sum_{i=0}^{n-k-1} s_ix^i$*, temos que a síndrome de* $xr(x)$ *é*

1. $xs(x)$*, se* $\mathrm{grau}(s(x))<n-k-1$
2. $xs(x)-s_{n-k-1}g(x)$*, se* $\mathrm{grau}(s(x))=n-k-1$

Como último pré-requisito para estudarmos os códigos Reed-Solomon devemos aprender uma maneira de decodificar dado um código cíclico qualquer.

Definição 4.7 *Um burst error cíclico de tamanho* t *é um vetor tal que todas as posições não nulas estão dentro de* t *posições ciclicamente consecutivas no vetor, sendo a primeira e a última posição obrigatoriamente não nulas.*

Exemplo 4.8

$v_1 = (0000\mathbf{10011}000)$ *tem burst cíclico de tamanho* 5
$v_2 = (000000\mathbf{111001})$ *tem burst cíclico de tamanho* 6
$v_3 = (\mathbf{01}0000000\mathbf{110})$ *tem burst cíclico de tamanho* 5

A ideia de *burst errors* são interresante por conta que quando ocorrem erros na passagem do canal de comunicação, geralmente esses erros estão em sequência (alguma interfência naquele momento em especifíco por exemplo), assim a ideia é que se um código tem fator de correção t, ele consegue corrigir até t erros em sequência.

Exemplo 4.9 *Um código* $C-[7,3]$ *que é gerado por* $g(x) = 1+x+x^2+x^4$ *tem fator de correção* $t = 2$*, assim teremos que cada burst é de tamanho no máximo* 2 *e deverão ser associados a síndromes diferentes.*

burst error	*síndrome*	*burst error*	*síndrome*
x^0	*1000*	$x^0(1+x)$	*1100*
x^1	*0100*	$x^1(1+x)$	*0110*
x^2	*0010*	$x^2(1+x)$	*0011*
x^3	*0001*	$x^3(1+x)$	*1111*
x^4	*1110*	$x^4(1+x)$	*1001*
x^5	*0111*	$x^5(1+x)$	*1010*
x^6	*1101*	$x^6(1+x)$	*0101*

Vamos supor que após codificar uma mensagem m obtivemos c, porém após passar pelo canal de comunicação obtemos r com síndrome s, assim temos que $e = r - c$, e por consequência da **Definição 3.6** temos que $s = He^T$, porém mostramos acima que $H = (I_{n-k}| - A^T)$, assim caso $e = (s^T, 0)$, onde 0 é uma k-upla nula, temos que $s = (I_{n-k}s^t, -A^T0) = He^T$. Porém unicidade de e só ocorre quando $w(e) \leq l$, onde l é a quantidade máxima de erros que podemos corrigir, assim para que tal ocorra devemos garantir que $w(s) \leq l$.

Assim vamos definir $s_i(x)$ como a síndrome de $x^i r(x)$, então quando $w(s_i(x)) \leq l$, teremos que $x^i e(x) = (s_i, 0) \implies e(x) = x^{n-i}(s_i, 0)$.

Porém para *burst errors* devemos analizar se $e(x)$ é um *burst* $\leq t$, sendo t o maior *burst* corrigível, logo devemos garantir que $s_i(x)$ seja um *burst* não cíclico (pois se fosse cíclico não é verdade que *burst* de $e(x) = (s_i(x), 0) \leq t$), agora basta encontrar o menor i tal que tem *burst* $\leq t$ e $e(x) = (s_i, 0)$.

Exemplo 4.10 *Dado o código do* ***Exemplo 4.9*** *vamos supor que foi recebida uma mensagem* $r = (0101110)$
$r(x) = 1 + x^5 + x^6 = xg(x) + (1 + x + x^2)$*, assim temos que*
$s_0(x) = 1 + x + x^2$
$s_1(x) = x + x^2 + x^3$
$s_2(x) = 1 + x + x^3$
$s_3(x) = 1$
Assim temos que $e(x) = x^{7-3}s_3(x) = x^4 \cdot 1 = x^4 \implies e = (0000100) \implies c = r - e = (1001010) - (000100) = (1001110)$.

Apesar de conseguirmos fazer todo o processo de codificação e decodificação, ainda não se sabe muito bem como conseguir a distância mínima de um código cíclico, e realmente é uma tarefa difícil de se analisar, por conta disso veremos certos tipos específicos de códigos que nos auxiliarão a encontrar essa distância e também a quantidade de *burst errors* que podemos corrigir.

5 Códigos Reed-Solomon

Vimos na seção anterior que é relativamente fácil codificar e decoficar mensagens em códigos cíclicos, agora nesse capítulo vamos discutir sobre o código de Reed-Solomon, um dos mais utilizados por ser MDS e fácil de conseguir a quantidade de *burst errors* corrigíveis. Dado $\beta \in \mathbb{F}_q$, vamos supor que a ordem de β seja n, isto é, $\beta^n = 1$ e $\beta^s \neq 1$ para $s < n$. Vamos definir como Reed-Solomon os códigos gerados pelo seguinte polinômio

$g(x) = (x - \beta)(x - \beta^2) \cdots (x - \beta^{\delta-1})$

Os códigos Reed-Solomon são um caso particular de códigos BCH (ver [2, Chapter 6]). Dadas algumas propriedades dessa classe de códigos, é possível provar que $g(x)$ será um divisor de $x^n - 1$, sendo assim gerador de um subespaço cíclico de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Além do mais temos que $\mathrm{grau}(g(x)) = \delta - 1 = n - k \implies \delta = n - k + 1$, com isso já podemos anunciar o seguinte teorema.

Teorema 5.1 *Dado um código Reed-Solomon* $[n, k, d]$ *temos que* $d = n - k + 1 = \delta$

Exemplo 5.2 *Dado um código* C *sobre* $\mathbb{F}_{2^4}$*, com* α *sendo uma raiz de* $f(x) = 1 + x + x^4$*, temos que* $\beta = \alpha^5$ *será* 3^a *raiz de unidade, logo*

$g(x) = (x - \beta)(x - \beta^2)$

dessa forma $n = 3$ *e* $\delta = 3$*, então* $n - k + 1 = \delta \implies 3 - k + 1 = 3 \implies k = 1$*, dessa forma* $g(x)$ *gera um código Reed-Solomon* $[3, 1]$ *sobre* $\mathbb{F}_{2^4}$*.*

Como visto no teorema acima os códigos de Reed-Solomon são MDS, porém estamos mais preocupados em aplicar decodificação em *burst errors*, logo temos o seguinte teorema para nos auxiliar.

Teorema 5.3 *Um código de Reed-Solomon* $[n, k]$ *sobre* $\mathbb{F}_{2^m}$ *pode ser transformado em um código cíclico* $[nm, km]$ *sobre* $\mathbb{F}_2$ *com capacidade de corrigir* $m\left(\left\lfloor \frac{n-k}{2} \right\rfloor - 1\right) + 1$ *burst errors.*

6 Conclusão

Com esse trabalho vimos que não é tão complexo mandar uma mensagem apartir de um meio de comunicação utilizando um código Reed-Solomon para correção de erros. Atualmente o código de Reed-Solomon e algumas variações do mesmo são muito utilizados em meios que possuem bastante interferência, pois como visto na seção 5, esses códigos conseguem corrigir razoalmente muitos *burst errors*, diferente de outros códigos até mais complexos que corrigem uma quantidade menor deste tipo de erro. Com isso podemos afirmar que o Reed-Solomon é um dos principais códigos corretores utilizados atualmente, vendo que vivemos num mundo que cada dia mais cresce tecnologicamente, e como consequência produz mais interferências.

Agradecimento

Na condição de bolsista do Programa de Iniciação Científica, agradeço ao CNPq pelo apoio financeiro.

Referências

[1] H. ABRAMO, T. MARIA LÚCIA VILLELA. **Códigos Corretores de Erros**. 2ªed.. Rio de Janeiro: IMPA, 2017.

[2] A. SCOTT VANSTONE, C. PAUL VAN OORSCHOT. **An Introduction to Error Correcting Codes with Applications**. Boston/Dordrecht/London: Kluwer Academic Publishers, 1989.

Criptografia - Cifras de Hill

Eduardo Oliveira de Sousa
UFU, Faculdade de Gestão e Negócios, Uberlândia, Minas Gerais, Brasil
eduardooliveira@ufu.br

Elisa Regina dos Santos
UFU, Faculdade de Matemática, Uberlândia, Minas Gerais, Brasil
elisars@ufu.br

Palavras-chave

Criptografia.
Álgebra Linear.
Aritmética modular.

Resumo

Este estudo aborda a criptografia e métodos de codificação e decodificação de textos utilizando matrizes, transformações lineares, independência linear, operações matriciais e eliminação gaussiana. Além disso, serão apresentados conceitos de aritmética modular e técnicas para quebrar mensagens cifradas.

1 Introdução

A **criptografia** consiste no estudo da codificação e da decodificação de mensagens secretas. Desde as primeiras civilizações da Mesopotâmia, Egito, Grécia e Roma, essa era utilizada para proteger mensagens confidenciais e segredos militares. Nesse estudo os códigos são denominados **cifras**, as mensagens não codificadas são **textos comuns** e as mensagens codificadas são **textos cifrados**. O processo de transformar um texto comum em um texto cifrado é denominado **cifrar** e o processo inverso é denominado **decifrar**.

Na Grécia Antiga, a cifra mais conhecida era a chamada "Cifra de César" e foi utilizada pelo famoso líder militar Júlio César. Nessa cifra, cada letra do alfabeto era substituída por outra letra que se encontrava a um determinado número de posições à frente na ordem alfabética. Esse tipo de cifra é conhecida por **cifra de substituição**, pois consiste em substituir cada letra do alfabeto por outra letra. As cifras de substituição possuem a grande desvantagem de manter a frequência das letras individuais, facilitando a quebra do código. O objetivo deste trabalho é apresentar uma maneira de superar esse problema, dividindo o texto em blocos e cifrando os blocos em vez de cada letra separadamente.

Nos dias de hoje, a criptografia é amplamente utilizada em diversas áreas para proteger informações confidenciais. Desde o uso de senhas em dispositivos eletrônicos até a troca de informações em sistemas bancários e governamentais, a criptografia garante a segurança e a privacidade das informações. Além disso, a criptografia também é usada em comunicações online, como em e-mails e mensagens instantâneas, para proteger a privacidade dos usuários.

2 Cifras de Hill

Em 1929, o matemático Lester S. Hill [2, 3] introduziu sistemas criptográficos baseados em transformações matriciais. Tais sistemas são conhecidos atualmente como **cifras de Hill**. Nas cifras de Hill cada letra do alfabeto corresponde a um número de 0 a 25 da seguinte forma:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Tabela 1: Correspondentes numéricos

No caso de cifras de Hill com blocos de tamanho n, ciframos o texto da seguinte forma:

1. Escolha uma matriz quadrada de tamanho $n \times n$, onde n é um número inteiro positivo. Essa matriz será a **chave de cifragem** ou **chave**. Mais adiante veremos que tal matriz deverá satisfazer algumas condições.

2. Divida o texto em blocos de n letras. Se o texto não tiver um número inteiro de blocos de tamanho n, adicione letras fictícias para completar o último bloco.

3. Para cada bloco de n letras, crie um vetor coluna de tamanho n, onde cada elemento é o número associado à letra correspondente segundo a Tabela 1. Esses vetores serão chamados **vetores comuns**.

4. Multiplique os vetores coluna pela matriz chave (utilizaremos aritmética modular para manter os resultados dentro do intervalo de 0 a 25). Esses vetores serão chamados **vetores cifrados**.

5. Converta cada elemento dos vetores resultantes de volta para sua letra correspondente.

6. Junte os blocos cifrados para formar o texto cifrado.

Exemplo 2.1 (2-cifra de Hill)**.** *Vamos cifrar a mensagem "MOSTRA IC" utilizando a matriz chave*

$$\boldsymbol{A} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}.$$

Dividindo o texto em blocos de tamanho 2*, temos*

$$MO \quad ST \quad RA \quad IC.$$

Assumindo a correspondência de letras e números segundo a Tabela 1, criamos os vetores coluna para cada bloco:

$$P_1 = \begin{bmatrix} 13 \\ 15 \end{bmatrix}, \; P_2 = \begin{bmatrix} 19 \\ 20 \end{bmatrix}, \; P_3 = \begin{bmatrix} 18 \\ 1 \end{bmatrix}, \; P_4 = \begin{bmatrix} 9 \\ 3 \end{bmatrix}.$$

Ao multiplicar cada um deles pela matriz chave **A***, obtemos os seguintes vetores coluna:*

$$C_1 = \begin{bmatrix} 177 \\ 170 \end{bmatrix}, \; C_2 = \begin{bmatrix} 251 \\ 235 \end{bmatrix}, \; C_3 = \begin{bmatrix} 166 \\ 97 \end{bmatrix}, \; C_4 = \begin{bmatrix} 93 \\ 66 \end{bmatrix}.$$

Para manter as entradas dos vetores coluna entre 0 *e* 25*, vamos substituir cada inteiro pelo seu respectivo resto na divisão por* 26*, obtendo assim:*

$$C_1 = \begin{bmatrix} 21 \\ 14 \end{bmatrix}, \; C_2 = \begin{bmatrix} 17 \\ 1 \end{bmatrix}, \; C_3 = \begin{bmatrix} 10 \\ 19 \end{bmatrix}, \; C_4 = \begin{bmatrix} 15 \\ 14 \end{bmatrix}.$$

Agora substituindo cada número pela respectiva letra, temos a mensagem "UNQAJSON".

No exemplo acima, substituímos os inteiros maiores que 25 pelo seu resto na divisão por 26. Essa é a base da **aritmética modular**. Apresentaremos a seguir alguns conceitos dessa área que serão essenciais para a compressão de como decifrar uma mensagem codificada por uma cifra de Hill.

3 Aritmética Modular

Por trabalharmos na Cifra de Hill com números de 0 a 25, vamos usar neste estudo a aritmética modular, que é uma ramificação da aritmética que lida com a divisão de números inteiros em conjuntos

chamados classes de congruência. Essa divisão é baseada em um número inteiro fixo chamado módulo. No estudo vamos usar o módulo do número 26, mas outros módulos podem ser usados.

Definição 3.1. *Seja m um número inteiro positivo. Dois inteiros a e b são* ***congruentes*** *módulo m se a diferença entre eles é um múltiplo de m. Isso é denotado por $a \equiv b \pmod{m}$.*

Exemplo 3.2. $7 \equiv 2 \pmod{5}$, $19 \equiv 3 \pmod{2}$, $-1 \equiv 25 \pmod{26}$ *e* $12 \equiv 0 \pmod{4}$.

Dado um módulo m, como os possíveis restos na divisão por m são $0, 1, 2, \ldots, m-1$, temos que qualquer inteiro a é congruente módulo m a exatamente um dos inteiros $0, 1, 2, \ldots, m-1$. Esse inteiro é denominado **resíduo** de a módulo m. Denotaremos por

$$\mathbb{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$$

o conjunto dos resíduos módulo m. O teorema a seguir nos mostra como determinar o resíduo módulo m de um inteiro qualquer.

Teorema 3.3 ([1], Teorema 11.16.1)**.** *Dados um inteiro a e um módulo m quaisquer, definindo R como sendo o resto da divisão de $|a|$ por m, o resíduo r de a módulo m é dado por:*

$$r = \begin{cases} R, & \text{se } a \geq 0, \\ m - R, & \text{se } a < 0 \text{ e } R \neq 0, \\ 0, & \text{se } a < 0 \text{ e } R = 0. \end{cases}$$

Exemplo 3.4. *Pelo Teorema 3.3, temos que o resíduo de* 97 *módulo* 26 *é* 19*, o resíduo de* -38 *módulo* 26 *é* 14 *e o resíduo de* -26 *módulo* 26 *é* 0.

Definição 3.5. *Dado um número a em Z_m, dizemos que um número a^{-1} em Z_m é um* ***recíproco*** *ou* ***inverso multiplicativo*** *de a módulo m se $a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{m}$.*

É possível provar que a possui um único recíproco módulo m se, e somente se, a e m não têm fatores primos em comum. A seguir apresentamos uma tabela de recíprocos módulo 26.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Tabela 2: Recíprocos módulo 26

Para um estudo detalhado de Aritmética Modular sugerimos a referência [4].

4 Decifrando as Cifras de Hill

Para decifrar as cifras de Hill, vamos precisar da matriz inversa (módulo 26) da matriz chave. Se m é um inteiro positivo, dizemos que uma matriz **A**, com entradas em $\mathbb{Z}_m$, é **invertível módulo** m se

existir uma matriz **B**, com entradas em $\mathbb{Z}_m$, tal que

$$\mathbf{A}\,\mathbf{B} \equiv \mathbf{B}\,\mathbf{A} \equiv \mathbf{I}\ (\mathrm{mod\ m}).$$

Suponha que a matriz chave **A** seja invertível módulo 26 e seja P um vetor comum. Então o vetor cifrado é dado por $C = \mathbf{A}P$ e vale $P = \mathbf{A}^{-1}C$. Logo, podemos recuperar os vetores comuns multiplicando os vetores cifrados à esquerda por $\mathbf{A}^{-1}$. A seguir apresentamos um resultado que nos diz quando uma matriz é invertível módulo 26.

Proposição 4.1 ([1], Corolário 11.16.4)**.** *Uma matriz quadrada **A**, com entradas em $\mathbb{Z}_{26}$, é invertível módulo 26 se, e somente se, o resíduo de $\det(\boldsymbol{A})$ módulo 26 não é divisível por 2 ou 13.*

Exemplo 4.2. *Vejamos que a matriz **A** do Exemplo 2.1 é invertível módulo 26. Observe que*

$$\det(\boldsymbol{A}) = a_{11}a_{22} - a_{12}a_{21} = (9 \cdot 7) - (5 \cdot 4) = 43 \equiv 17\ (\mathrm{mod}\ 26).$$

*Como 17 não é divisível por 2 nem por 13, temos que **A** é invertível módulo 26 pela proposição anterior. Daí, a matriz inversa de **A** é*

$$\boldsymbol{A}^{-1} \equiv \det(A)^{-1} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \equiv 17^{-1} \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \equiv 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}\ (\mathrm{mod}\ 26).$$

Vamos utilizar essa matriz para decifrar a mensagem "UNQAJSON" obtida no Exemplo 2.1. Para facilitar o cálculo, vamos juntar todos os vetores cifrados associados à mensagem em uma matriz com colunas de tamanho 2. Temos então:

$$C = \begin{bmatrix} 21 & 17 & 10 & 15 \\ 14 & 1 & 19 & 14 \end{bmatrix}.$$

Multiplicando $\boldsymbol{A}^{-1}$ por C, obtemos a matriz de vetores comuns

$$P = \boldsymbol{A}^{-1}C = 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \begin{bmatrix} 21 & 17 & 10 & 15 \\ 14 & 1 & 19 & 14 \end{bmatrix} = 23 \begin{bmatrix} 91 & 115 & -6 & 49 \\ 21 & -76 & 121 & 51 \end{bmatrix}$$

$$= \begin{bmatrix} 2093 & 2645 & -138 & 1127 \\ 483 & -1748 & 2783 & 1173 \end{bmatrix} \equiv \begin{bmatrix} 13 & 19 & 18 & 9 \\ 15 & 20 & 1 & 3 \end{bmatrix}\ (\mathrm{mod}\ 26),$$

resultando na mensagem "MOSTRA IC".

5 Quebrando as Cifras de Hill

Vale ressaltar que a cifra de Hill não é uma cifra perfeita e existem algumas formas de quebrá-la. Uma delas consiste em utilizar uma técnica na qual é necessário possuir tanto a mensagem cifrada

quanto um trecho da mensagem original, a partir das quais é possível obter a matriz chave utilizada na cifragem. O teorema a seguir nos fornece uma maneira de fazer isso.

Teorema 5.1 ([1], Teorema 11.16.5)**.** *Sejam $P_1, P_2, \ldots, P_n$ vetores comuns linearmente independentes e sejam $C_1, C_2, \ldots, C_n$ os vetores cifrados correspondentes de uma n-cifra de Hill. Se*

$$\boldsymbol{P} = \begin{bmatrix} P_1^T \\ \vdots \\ P_n^T \end{bmatrix} \quad e \quad \boldsymbol{C} = \begin{bmatrix} C_1^T \\ \vdots \\ C_n^T \end{bmatrix}$$

são as matrizes $n \times n$ dos vetores $P_1^T, \ldots, P_n^T$ e dos vetores $C_1^T, \ldots, C_n^T$, respectivamente, então a sequência de operações elementares sobre linhas que reduz $\boldsymbol{C}$ a identidade $\boldsymbol{I}$ transforma $\boldsymbol{P}$ em $(A^{-1})^T$.

6 Considerações finais

Ao longo deste estudo, vimos o funcionamento da cifra de Hill e suas vantagens e desvantagens. Entre as vantagens, podemos destacar a simplicidade da implementação, a dificuldade de quebra da criptografia e a capacidade de cifrar tanto textos curtos como longos. Por outro lado, uma desvantagem da cifra de Hill é a vulnerabilidade a ataques que exploram as propriedades algébricas da cifra para quebrá-la.

É importante notar que a cifra de Hill não é usada em sistemas de criptografia modernos, mas possui valor histórico e é uma técnica fundamental para entender os princípios básicos da criptografia.

Agradecimentos

Na condição de bolsista do PICME, agradeço ao CNPq pelo apoio financeiro.

Referências

[1] ANTON, H.; RORRES, C. **Álgebra Linear com Aplicações**. 8ª edição. Porto Alegre: Bookman, 2001.

[2] HILL, L. S. Cryptography in an Algebraic Alphabet. **Amer. Math. Monthly.** 36, 306-312, 1929.

[3] HILL, L. S. Concerning Certain Linear Transformation Apparatus of Cryptography. **Amer. Math. Monthly.** 38, 135-154, 1931.

[4] SANTOS, J. P. O. **Introdução à teoria dos números**. 3ª edição. Rio de Janeiro: IMPA, 2020.

Indução Matemática e a Torre da Hanói

João Victor Rezende Amaro
UFU, Faculdade de Engenharia Mecânica, Uberlândia, MG, Brasil
joao.amaro@ufu.br

Dylene Agda Souza de Barros
UFU, Faculdade de Matemática, Uberlândia, MG, Brasil
dylene@ufu.br

Palavras-chave

Indução Matemática.
Torre de Hanói.
Discos.

Resumo

O trabalho é baseado no estudo do livro "Indução Matemática"de Abramo Hefez, com foco nos capítulos de indução matemática e do problema da Torre de Hanói. O problema de Hanói consiste em uma plataforma com 3 pinos, no qual um deles possui discos empilhadas, do maior ao menor, e o desafio é mover a torre para outro pino, um disco por vez, e nunca ter um disco maior sobre um menor. Existe um método para se resolver a Torre com a menor quantidade de movimentos, e a indução matemática foi a ferramenta utilizada para demonstrar que a quantidade mínima de movimentos para resolver o problema com n discos é $P(n) = 2^n - 1$.

1 Introdução

A Indução Matemática é um artifício utilizado para demonstrar proposições que podem ser ditas em função de números naturais, ou seja, o conjunto $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$. O princípio consiste em provar que a relação é valida para algum termo inicial, por exemplo, provar que $P(1)$ é verdade. A partir daí, supõe-se que a proposição é válida para angum n, ou seja, $P(n)$ é verdade e, com esta suposição, deve-se provar que $P(n + 1)$ também é verdadeiro.

Por tratar de números naturais, a Indução Matemática tem diversas aplicações e, neste trabalho, é apresentado uma delas: mostra-se que a quantidade mínima de movimentos para resolver o problema da Torre de Hanói com n discos é $P(n) = 2^n - 1$.

Esse tranalho foi inspirado nas seguintes referências [1] - [4].

2 A Torre de Hanói

O problema da Torre de Hanói foi um jogo criado em 1882 pelo matemático francês Edouard Lucas, sendo uma plataforma com 3 pinos fixados, e uma torre de discos com um furo no meio e diâmetros diferentes, empilhados em um dos pinos, sempre com o disco de diâmetro menor sobre um de diametro maior. O objetivo é mover a torre para outro pino, um disco por vez, e nunca colocar um disco maior sobre um menor.

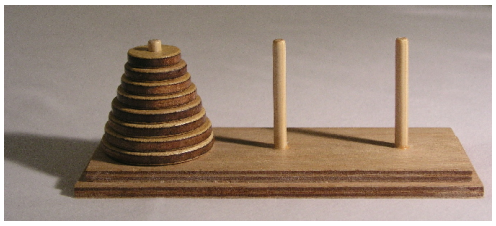


Figura 1: Torre de Hanói

Uma tática para resolver o problema é projetar onde os discos devem ficar, para isso dividí-los em subtorres, em que se precisa resolver a anterior para fazer a próxima. Tomando como exemplo a figura acima, para se resolver a torre com 8 discos, antes deve-se resolver com 7 discos, 6, 5, e assim até 2 e 1 discos. Dessa forma, para que a torre passe para a direita, a subtorre anterior, de 7 discos, deve ficar no meio, para isso a de 6 fica na direita, de 5 no pino central, até a subtorre de 2 discos fivar na direita e por fim a de um disco no meio. Outra tática é, ao longo do jogo, dividir mais as torres já divididas, redeterminar onde a subtorre deve ficar, mover os discos de acordo com a ideia anterior e, assim, avançar mais. Logo, os conjuntos de discos vão mudar entre o disco da esquerda, direita e meio a medida que forem necessários.

Com essa lógica aplicada para cada disco e subtorre, o problema é solucionado para n discos e com a menor quantidade de movimentos.

3 Indução Matemática e Torre de Hanói

O método para resolver a Torre pode ser utilizado para sugeririr uma equação que fornece a quantidade mínima de movimentos para solucionar o problema em função da quantidade de discos empilhados. Como a quantidade de discos pertence ao conjunto dos números naturais, isso é um caso que pode ser demonstrado por indução matemática.

Para uma torre com 1 disco, é necessário apenas 1 movimento. Para uma torre com 2 discos, são necessários 3 movimentos, esses casos são fáceis de perceber. Para uma torre com 3 discos, são necessários 3 movimentos para mover a subtorre de dois discos, mais um movimento para mover o maior disco, mais 3 movimentos para mover a subtorre novamente para o disco maior, ou seja, 7 movimentos. Generalizando, como o maior disco deve ficar no pino da direita, deve se mover todos os n-1 pinos restantes para o pino do meio. Observe que nesse momento, resolvemos o jogo para a subtorre de n-1 discos. Daí transportamos o disco maior para a direita e então resolvemos novamente o jogo para n-1 pinos. Com isso, conclui-se que são nessessárias 2 vezes a quantidade de movimentos de (n-1) discos, mais 1. Uma forma mais fácil de visualizar é por uma tabela:

nº discos	Movimentos	Operação
1	1	1
2	$2 \cdot 1 + 1 = 3$	$(1 \cdot 2) + 1$
3	$2 \cdot 3 + 1 = 7$	$((1 \cdot 2) + 1)2 + 1$
4	$2 \cdot 7 + 1 = 15$	$(((1 \cdot 2) + 1)2 + 1)2 + 1$
5	$2 \cdot 15 + 1 = 31$	$((((1 \cdot 2) + 1)2 + 1)2 + 1)2 + 1$

Tabela 1: Número de discos, quantidade mínima de movimentos e operação completa

Ao analisar a tabela nota-se que a quantidade de movimentos é a soma

$$2^{n-1} + 2^{n-2} + 2^{n-3} + ... + 2^1 + 1$$

A hipótese é que a soma seja igual a $2^n - 1$, para provar isso vamos usar Indução Matemática.

Primeiro, temos que $P(1) = 1 = 2^1 - 1 = 1$ logo, o P(1) é verdade. Com o passo inicial, pode-se supor que $P(n)$ é verdadeira **para algum** $n \geq 1$, ou seja $P(n) = 2^n - 1$, como representado na figura abaixo.

Agora, basta provar que o próximo passo também é verdade, ou seja, que $P(n+1) = 2^{n+1} - 1$. Observando a tabela acima, temos que $P(n+1) = 2 \cdot P(n) + 1$ e, portanto, usando nossa hipótese de indução, temos

$$P(n+1) = 2 \cdot P(n) + 1 = 2 * (2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1, \quad (1)$$

donde tiramos que $P(n) = 2^n - 1$, **para todo** $n \geq 1$.

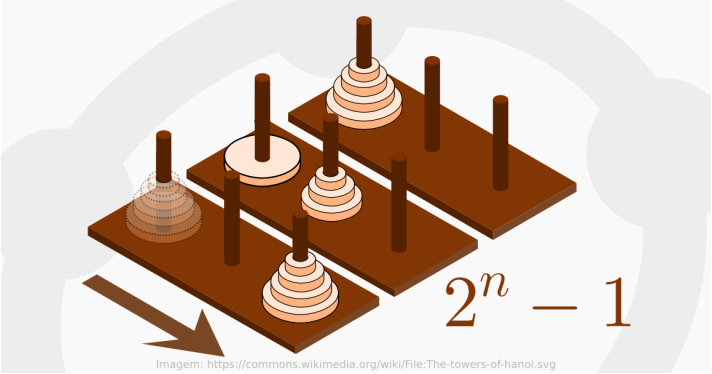


Figura 2: Torre de Hanói

4 Considerações finais

A matemática está presente em vários jogos. Um exemplo é o da Torre de Hanói, que desafia a lógica e o raciocínio rápido de quem tenta resolvê-la. Este é um problema simples de explicar e aprender a jogar, mas é necessário um número mínimo de passos para solunioná-lo. Mostramos que para solucionar o problema da torre com n discos são necessários pelo menos $2^n - 1$ movimentos. Por exemplo, para solucionar o problema com 64 discos, são necessários no mímino 18446073709551615 movimentos.

Referências

[1] Hefez, A. **Indução Matemática**. Rio de Janeiro: Editora SBM, 2007.

[2] MANOEL, L. R. S. Torre de Hanói. **Artigos do Laboratório de Matemática - Ibilce - Unesp** . Uberlândia, 2021. Disponível em: <https://www.ibilce.unesp.br/Home/Departamentos/Matematica/labmat/torre_de_hanoi.pdf>. Acesso em: 12 de abril de 2023.

[3] Figura 1: Disponível em: <https://pt.wikipedia.org/wiki/Torre_de_Han%C3%B3i>. Acesso em: 12 de abril de 2023.

[4] Figura 2: Disponível em: <https://www.prof-edigleyalexandre.com/2018/04/jogo-torre-de-hanoi-criado-com-o-geogebra.html>. Acesso em: 12 de abril de 2023.