

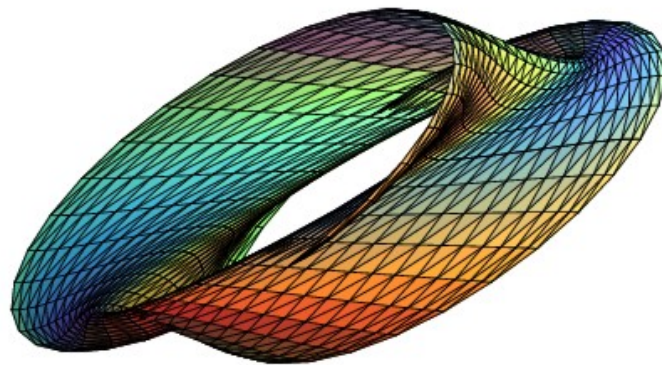
---

---

BOLETIM DE INICIAÇÃO CIENTÍFICA EM  
MATEMÁTICA · BICMAT

---

---



VOLUME XXI  
SETEMBRO DE 2024  
DEPARTAMENTO DE MATEMÁTICA  
IGCE · RIO CLARO

BOLETIM DE INICIAÇÃO CIENTÍFICA EM  
MATEMÁTICA · BICMAT

*Comissão editorial*

Elíris Cristina Rizzioli  
Renata Zotin Gomes de Oliveira  
Nativi Viana Pereira Bertolo  
Thiago de Melo

*Editoração gráfica*

Thiago de Melo

*Realização*

Departamento de Matemática  
IGCE · Unesp Rio Claro

## EDITORIAL

O Boletim de Iniciação Científica em Matemática · BICMat é uma publicação que se destina a difundir prioritariamente trabalhos de Iniciação Científica em Matemática que fazem parte de projetos desenvolvidos por alunos do Curso de Graduação em Matemática do IGCE, Unesp Rio Claro. Eventualmente trabalhos de Iniciação Científica realizados em outras instituições poderão também ser publicados neste Boletim.

O BICMat foi criado em 1998 e nessa época foram publicados dois volumes; o primeiro no ano de criação e o segundo em 2000.

Considerando a importância da Iniciação Científica para o graduando, e o sempre crescente número de projetos desta natureza desenvolvidos em nossa instituição, resolvemos reativar a publicação do BICMat em 2006, com ISSN 1980-024X.

Destacamos que a autoria dos trabalhos apresentados no BICMat é dos alunos. O orientador figura apenas como responsável científico.

Este Boletim também está aberto à divulgação de trabalhos que não sejam frutos de projetos de Iniciação Científica, mas que sejam de interesse dos alunos do curso de graduação em Matemática. Estes trabalhos serão selecionados pelos Editores.

Este volume está disponibilizado eletronicamente na página do Departamento de Matemática no endereço

[www.rc.unesp.br/igce/matematica/bicmat/](http://www.rc.unesp.br/igce/matematica/bicmat/)

ou através do código QR



## SUMÁRIO

<i>Equações Diferenciais Ordinárias e Teoria de Floquet</i>	
Danielle Assunção da Silva .....	5
<i>Aplicação de Corpos Finitos na Criptografia: Um Estudo do Algoritmo AES</i>	
Lídia Campelo da Silva .....	18
<i>Estabilidade de Equações Diferenciais com Retardamento via Teoremas de Ponto Fixo</i>	
Maitê Borges Fiorini dos Anjos .....	27
<i>A integral de Kurzweil para a caracterização de EDO's generalizadas</i>	
Wellington Moisés de Oliveira .....	37

# Equações Diferenciais Ordinárias e Teoria de Floquet

Danielle Assunção da Silva<sup>†</sup>

Orientador(a): Profa. Dra. Marta Cilene Gadotti

**Resumo:** Este trabalho aborda a teoria qualitativa das equações diferenciais ordinárias, focando em sistemas periódicos e suas soluções. Inicia-se com a introdução aos sistemas lineares não homogêneos e a apresentação do Teorema de Floquet, que é essencial para transformar sistemas periódicos em sistemas com coeficientes constantes. A matriz fundamental  $\Phi(t)$  é definida, e as propriedades dos autovalores e expoentes característicos são exploradas.

A partir do Teorema de Floquet, é demonstrado que a mudança de variável  $y = P(t)u$  transforma um sistema periódico em um sistema linear com coeficientes constantes, facilitando a análise de suas soluções. A relação entre os multiplicadores e os autovalores da matriz  $R$  é estabelecida, e a condição para a existência de soluções periódicas é discutida.

Um dos principais resultados é que uma solução do sistema não homogêneo  $y' = A(t)y + g(t)$  é periódica se, e somente se, as condições sobre o sistema homogêneo associado são atendidas. O trabalho inclui a análise de uma equação escalar como exemplo, mostrando a aplicação prática das teorias discutidas.

**Palavras-chave:** sistemas lineares; coeficientes periódicos; Teorema de Floquet

## 1 Introdução

Vários fenômenos físicos e biológicos são descritos por sistemas de equações diferenciais ordinárias (EDOs) com coeficientes periódicos, como vibrações em circuitos elétricos, sistemas mecânicos e até a dinâmica de fluidos.

Uma equação bastante utilizada é a de Hill. As equações de Hill são EDOs homogêneas de segunda ordem com coeficientes periódicos. Tem-se a forma geral:

$$y'' + a(t)y' + b(t)y = 0 \quad (1.1)$$

com  $a(t)$  e  $b(t)$  periódicas. Essa equação é utilizada na Mecânica Celeste, aplicações de circuitos elétricos e condutividade elétrica de metais. A Teoria de Floquet é importante para o estudo destes tipos de equações. Assim, neste trabalho será introduzido, de forma simples, os conceitos e resultados referentes à essa Teoria.

## 2 Preliminares

Apresentamos a seguir, um importante resultado para garantir a existência e unicidade de uma solução de um sistema linear.

**Lema 2.1** (Desigualdade de Gronwall). *Tendo uma constante  $k \geq 0$ , sendo as funções  $f$  e  $g$  contínuas e não negativas em algum intervalo  $\alpha \leq t \leq \beta$ , e satisfazendo a desigualdade:*

$$f(t) \leq k + \int_{\alpha}^t f(s)g(s) ds,$$

<sup>†</sup>FAPESP: 2024/00903-5

para  $\alpha \leq t \leq \beta$ , então

$$f(t) \leq k \exp \left( \int_{\alpha}^t g(s) ds \right),$$

para  $\alpha \leq t \leq \beta$ .

*Demonstração.* Definimos a função  $U(t) = k + \int_{\alpha}^t f(s)g(s) ds$ . Como  $U(\alpha) = k$ , temos pela hipótese que  $f(t) \leq U(t)$  para todo  $t \in [\alpha, \beta]$ .

Pelo Teorema Fundamental do Cálculo, temos

$$U'(t) = f(t)g(t) \leq U(t)g(t), \text{ para } \alpha \leq t \leq \beta.$$

A partir da desigualdade  $U'(t) \leq U(t)g(t)$ , podemos escrever

$$\frac{U'(t)}{U(t)} \leq g(t).$$

Integrando ambos os lados dessa desigualdade de  $\alpha$  até  $t$ , obtemos

$$\int_{\alpha}^t \frac{U'(s)}{U(s)} ds \leq \int_{\alpha}^t g(s) ds.$$

A integral do lado esquerdo é a derivada do logaritmo de  $U(s)$ , então temos

$$\ln U(t) - \ln U(\alpha) \leq \int_{\alpha}^t g(s) ds.$$

Como  $U(\alpha) = k$ , isso se torna

$$\ln U(t) - \ln k \leq \int_{\alpha}^t g(s) ds.$$

Simplificando, obtemos

$$\ln \left( \frac{U(t)}{k} \right) \leq \int_{\alpha}^t g(s) ds.$$

Exponenciando ambos os lados, temos

$$\frac{U(t)}{k} \leq \exp \left( \int_{\alpha}^t g(s) ds \right),$$

ou seja,

$$U(t) \leq k \exp \left( \int_{\alpha}^t g(s) ds \right).$$

Finalmente, como  $f(t) \leq U(t)$ , obtemos

$$f(t) \leq k \exp \left( \int_{\alpha}^t g(s) ds \right).$$

Isso conclui a demonstração da Desigualdade de Gronwall. ■

**Teorema 2.2.** *Existência e Unicidade.* Suponha que  $A(t)$  e  $b(t)$  sejam funções Riemann integráveis em  $t$  em um intervalo  $(a, b)$ , isto é, as integrais de Riemann existem em algum intervalo  $[c, d] \subset (a, b)$ , para cada  $a_{ij}$ ,  $i, j = 1, \dots, n$  em  $A(t)$  e cada  $b_j$ ,  $j = 1, \dots, n$  em  $b(t)$ , e suponha também que existe uma função  $k(t)$ , contínua em  $(a, b)$ , tal que:

1.  $k(t)$  é contínua em  $(a, b)$  e existe  $M > 0$  tal que  $|k(t)| \leq M$ ;

2.  $|A(t)| \leq k(t)$  e  $|b(t)| \leq k(t)$ ,  $a < t < b$ .

Considere  $t_0 \in (a, b)$  e  $y^0$  um vetor dado. Então o sistema de equações lineares não homogêneo, representado por

$$\begin{cases} y_1' = a_{11}(t)y_1 + a_{12}(t)y_2 + \cdots + a_{1n}(t)y_n + b_1(t), \\ y_2' = a_{21}(t)y_1 + a_{22}(t)y_2 + \cdots + a_{2n}(t)y_n + b_2(t), \\ \vdots \\ y_n' = a_{n1}(t)y_1 + a_{n2}(t)y_2 + \cdots + a_{nn}(t)y_n + b_n(t), \end{cases} \quad (2.1)$$

tem uma única solução  $y(t)$  em  $(a, b)$  tal que  $y(t_0) = y^0$  e  $y(t)$  satisfaz, para todo  $t \in (a, b)$ , a igualdade:

$$y(t) = y^0 + \int_{t_0}^t A(s) \cdot y(s) ds + \int_{t_0}^t b(s) ds. \quad (2.2)$$

*Demonstração.* A ideia da prova é construir uma sequência de aproximações sucessivas que converge para a solução da equação. Começamos definindo a sequência da seguinte maneira:

$$\begin{aligned} y_0(t) &= y^0, \\ y_1(t) &= y^0 + \int_{t_0}^t A(s) \cdot y_0(s) ds + \int_{t_0}^t b(s) ds, \\ y_2(t) &= y^0 + \int_{t_0}^t A(s) \cdot y_1(s) ds + \int_{t_0}^t b(s) ds, \\ &\vdots \\ y_n(t) &= y^0 + \int_{t_0}^t A(s) \cdot y_{n-1}(s) ds + \int_{t_0}^t b(s) ds. \end{aligned}$$

Nosso objetivo é provar que a sequência  $\{y_n(t)\}$  converge para uma função  $y(t)$ , que será a solução da equação original. Para isso, vamos provar que a sequência  $\{y_n(t)\}$  é de Cauchy em  $[c, d] \subset (a, b)$ , garantindo, assim, a convergência.

Primeiro, vamos estimar  $|y_n(t) - y_{n-1}(t)|$ :

$$|y_n(t) - y_{n-1}(t)| = \left| \int_{t_0}^t A(s) \cdot (y_{n-1}(s) - y_{n-2}(s)) ds \right|.$$

Usando a hipótese que  $|A(t)| \leq k(t)$ , temos:

$$|y_n(t) - y_{n-1}(t)| \leq \int_{t_0}^t |A(s)| \cdot |y_{n-1}(s) - y_{n-2}(s)| ds \leq \int_{t_0}^t k(s) \cdot |y_{n-1}(s) - y_{n-2}(s)| ds.$$

Agora, vamos proceder por indução para obter uma estimativa geral de  $|y_n(t) - y_{n-1}(t)|$ .

Para  $n = 1$ , temos:

$$|y_1(t) - y_0(t)| = \left| \int_{t_0}^t A(s) \cdot y_0(s) ds + \int_{t_0}^t b(s) ds \right| \leq \int_{t_0}^t k(s) ds \cdot (1 + |y^0|),$$

onde usamos que  $|b(s)| \leq k(s)$  e  $|y_0(s)| = |y^0|$ .

Para  $n = 2$ , temos:

$$|y_2(t) - y_1(t)| \leq \int_{t_0}^t k(s) \cdot |y_1(s) - y_0(s)| ds \leq (1 + |y^0|) \int_{t_0}^t k(s) \cdot \int_{t_0}^s k(u) du ds.$$

Essa estimativa pode ser reescrita em termos da função acumulada  $K(t) = \int_{t_0}^t k(s) ds$ , de modo que:

$$|y_2(t) - y_1(t)| \leq (1 + |y^0|) \frac{K(t)^2}{2!}.$$

Seguindo esse padrão, usando o argumento indutivo, temos que para um  $n \geq 1$ , vale a seguinte estimativa:

$$|y_n(t) - y_{n-1}(t)| \leq (1 + |y^0|) \frac{K(t)^n}{n!}.$$

Agora, somamos essas diferenças para obter a estimativa para  $|y_n(t) - y_m(t)|$ , com  $m < n$ :

$$|y_n(t) - y_m(t)| = |(y_n(t) - y_{n-1}(t)) + (y_{n-1}(t) - y_{n-2}(t)) + \cdots + (y_{m+1}(t) - y_m(t))|.$$

Aplicando a estimativa anterior, obtemos:

$$|y_n(t) - y_m(t)| \leq (1 + |y^0|) \sum_{j=m+1}^n \frac{K(t)^j}{j!}.$$

Como a série  $\sum_{j=1}^{\infty} \frac{K(t)^j}{j!}$  converge, concluímos que  $\{y_n(t)\}$  é uma sequência de Cauchy e, portanto, converge para uma função contínua  $y(t)$ . Agora, verifiquemos que  $y(t)$  é de fato solução do sistema. Sabemos que  $y_n(t) \rightarrow y(t)$  e que a função  $y(t)$  é contínua, portanto:

$$y(t) = \lim_{n \rightarrow \infty} y_n(t) = y^0 + \lim_{n \rightarrow \infty} \int_{t_0}^t A(s) \cdot y_{n-1}(s) ds + \int_{t_0}^t b(s) ds.$$

Pelo Teorema da Convergência Dominada, temos:

$$y(t) = y^0 + \int_{t_0}^t A(s) \cdot y(s) ds + \int_{t_0}^t b(s) ds.$$

Assim,  $y(t)$  satisfaz a equação integral, o que implica que é uma solução do sistema de equações diferenciais. A unicidade segue diretamente da Desigualdade de Gronwall. Se existissem duas soluções  $y_1(t)$  e  $y_2(t)$ , então a diferença  $z(t) = y_1(t) - y_2(t)$  satisfaria a equação homogênea

$$z(t) = \int_{t_0}^t A(s) \cdot z(s) ds.$$

Aplicando a Desigualdade de Gronwall, obtemos  $z(t) = 0$ , ou seja,  $y_1(t) = y_2(t)$ , provando a unicidade da solução. ■

**Teorema 2.3.** *Dada uma matriz  $A_{n \times n}(t)$ , cujas entradas são contínuas, o conjunto solução de*

$$y'(t) = A(t)y(t) \tag{2.3}$$

*é um espaço vetorial de dimensão  $n$ .*

*Demonstração.* Não é difícil mostrar que o conjunto de todas as soluções de (2.3) é um espaço vetorial, pois basta mostrar que é um subespaço vetorial do espaço de todas as funções  $x : I \rightarrow \mathbb{R}^n$ .

Mostremos que a dimensão é  $n$ . Denotando  $\{e_1, \dots, e_n\}$ , a base canônica de  $\mathbb{R}^n$ , considere os seguintes  $n$  PVIs:



1º:

$$y' = A(t)y$$

$$y(t_0) = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = e_1$$

2º:

$$y' = A(t)y$$

$$y(t_0) = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = e_2$$

nº:

$$y' = A(t)y$$

$$y(t_0) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} = e_n$$

Pelo Teorema de Existência e Unicidade, existe uma única solução para cada PVI, denotadas por  $\phi_1, \phi_2, \dots, \phi_n$ , respectivamente.

Mostremos que  $\{\phi_1, \phi_2, \dots, \phi_n\}$  é base do conjunto solução de (2.3).

Primeiro, mostremos que  $\{\phi_1, \phi_2, \dots, \phi_n\}$  é linearmente independente. De fato, considere a combinação linear

$$\alpha_1\phi_1 + \dots + \alpha_n\phi_n = 0_v \Rightarrow \alpha_1\phi_1(t) + \dots + \alpha_n\phi_n(t) = 0, \forall t \in I.$$

Logo, para  $t = t_0$ , tem-se:

$$\alpha_1\phi_1(t_0) + \dots + \alpha_n\phi_n(t_0) = 0.$$

Como  $\{e_1, e_2, \dots, e_n\}$  é linearmente independente, pois forma a base canônica de  $\mathbb{R}^n$ , segue que  $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ . Portanto,  $\{\phi_1, \phi_2, \dots, \phi_n\}$  é linearmente independente.

Agora, mostremos que  $\{\phi_1, \phi_2, \dots, \phi_n\}$  gera o conjunto solução de (2.3). De fato, seja  $\psi : I \rightarrow \mathbb{R}^n$  uma solução de (2.3), basta mostrar que  $\psi$  se escreve como combinação linear dos elementos de  $\{\phi_1, \phi_2, \dots, \phi_n\}$ .

Para mostrar isso, considere então

$$\psi(t_0) = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

e a combinação linear

$$\phi(t) = \beta_1\phi_1(t) + \dots + \beta_n\phi_n(t), \quad \forall t \in I.$$

Como  $\phi_1, \phi_2, \dots, \phi_n$  são soluções de (2.3), segue que  $\beta_1\phi_1 + \dots + \beta_n\phi_n$  é também solução, pois o conjunto solução é espaço vetorial. Note que,

$$\phi(t_0) = \beta_1\phi_1(t_0) + \dots + \beta_n\phi_n(t_0) = \beta_1e_1 + \dots + \beta_ne_n = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

Portanto,  $\phi$  e  $\psi$  são soluções do mesmo PVI:

$$\begin{aligned} y' &= A(t)y \\ y(t_0) &= \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}. \end{aligned}$$

Pela unicidade da solução do PVI, conclui-se que  $\phi = \psi$ , ou seja,

$$\psi = \beta_1\phi_1 + \dots + \beta_n\phi_n.$$

Portanto,  $\{\phi_1, \phi_2, \dots, \phi_n\}$  gera o conjunto solução de (2.3).

Assim, segue que  $\{\phi_1, \phi_2, \dots, \phi_n\}$  é base e, portanto, a dimensão é  $n$ . ■

**Teorema 2.4** (Fórmula de Abel). *Se  $\Phi$  é solução da matriz de*

$$y' = A(t)y, \tag{2.4}$$

em  $I$  e se  $t_0$  é um ponto qualquer de  $I$ , então,  $\forall t \in I$ ,

$$\det \Phi(t) = \det \Phi(t_0) \exp \left[ \int_{t_0}^t \sum_{j=1}^n a_{jj}(s) ds \right]. \tag{2.5}$$

Podemos afirmar, por  $t_0$  ser arbitrário, que ou  $\det \Phi(t) \neq 0$  para cada  $t \in I$  ou  $\det \Phi(t) = 0$ ,  $\forall t \in I$ .

*Demonstração.* Assumindo que as colunas de  $\Phi$  são  $\phi_1, \phi_2, \dots, \phi_n$ , sendo  $\phi_j$  os elementos  $(\phi_{1j}, \phi_{2j}, \dots, \phi_{nj})$ . Então podemos escrever a afirmação de que  $\phi_j$  é uma solução de (2.4) em  $I$ , em termos de elementos como

$$\phi'_{ij} = \sum_{k=1}^n a_{ik}\phi_{kj}, \quad \text{para } (i, j = 1, \dots, n). \tag{2.6}$$

Agora, precisamos lembrar que a derivada do determinante de  $\Phi$  em relação a  $t$  é a soma de  $n$  determinantes, isto é,

$$(\det \Phi)' = \begin{vmatrix} \phi'_{11} & \phi'_{12} & \cdots & \phi'_{1n} \\ \phi'_{21} & \phi'_{22} & \cdots & \phi'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \phi'_{n1} & \phi'_{n2} & \cdots & \phi'_{nn} \end{vmatrix} + \begin{vmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1n} \\ \phi'_{21} & \phi'_{22} & \cdots & \phi'_{2n} \\ \phi_{31} & \phi_{32} & \cdots & \phi_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{n1} & \phi_{n2} & \cdots & \phi_{nn} \end{vmatrix} + \cdots + \begin{vmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1n} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{n-1,1} & \phi_{n-1,2} & \cdots & \phi_{n-1,n} \\ \phi'_{n1} & \phi'_{n2} & \cdots & \phi'_{nn} \end{vmatrix}.$$

Esse fato é fácil de ser provado por indução. Usando (2.6), obtemos

$$\begin{aligned}
 (\det \Phi)' = & \begin{vmatrix} \sum_{k=1}^n a_{1k}\phi_{k1} & \sum_{k=1}^n a_{1k}\phi_{k2} & \cdots & \sum_{k=1}^n a_{1k}\phi_{kn} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \phi_{n1} & \phi_{n2} & \cdots & \phi_{nn} \end{vmatrix} \\
 + & \begin{vmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1n} \\ \sum_{k=1}^n a_{2k}\phi_{k1} & \sum_{k=1}^n a_{2k}\phi_{k2} & \cdots & \sum_{k=1}^n a_{2k}\phi_{kn} \\ \phi_{31} & \phi_{32} & \cdots & \phi_{3n} \\ \vdots & \vdots & \cdots & \vdots \\ \phi_{n1} & \phi_{n2} & \cdots & \phi_{nn} \end{vmatrix} \\
 + \cdots & \\
 + & \begin{vmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ \phi_{n-1,1} & \phi_{n-1,2} & \cdots & \phi_{n-1,n} \\ \sum_{k=1}^n a_{nk}\phi_{k1} & \sum_{k=1}^n a_{nk}\phi_{k2} & \cdots & \sum_{k=1}^n a_{nk}\phi_{kn} \end{vmatrix}.
 \end{aligned}$$

Usando operações elementares sobre as linhas, podemos avaliar cada determinante. Por exemplo, no primeiro determinante, multiplicamos a segunda linha por  $a_{12}$ , a terceira por  $a_{13}$ , e assim por diante, até a  $n$ -ésima por  $a_{1n}$ , adicionando essas  $(n-1)$  linhas e, em seguida, subtraindo o resultado da primeira linha. Isso deixa  $a_{11}$  como um fator da primeira linha resultante. Fazendo o mesmo procedimento para os outros determinantes, obtemos,  $\forall t \in I$ ,

$$(\det \Phi)' = a_{11} \det \Phi + a_{22} \det \Phi + \cdots + a_{nn} \det \Phi,$$

ou, equivalentemente,

$$(\det \Phi)' = \left( \sum_{k=1}^n a_{kk}(t) \right) \det \Phi, \quad (2.7)$$

que é uma equação escalar linear homogênea de primeira ordem para  $\det \Phi$ . Sua solução é dada por (2.5) sem dificuldade. ■

**Observação 2.5.** A matriz fundamental de solução é uma matriz formada por soluções linearmente independentes de um sistema de equações diferenciais lineares homogêneas da forma

$$y' = A(t)y.$$

**Teorema 2.6.** A matriz solução  $\Phi$  de (2.4), em um intervalo  $I$ , é a matriz fundamental de (2.4) em  $I$  se, e somente se,  $\det \Phi(t) \neq 0$ ,  $\forall t \in I$ .

*Demonstração.* ( $\Rightarrow$ ) Se  $\det \Phi(t) \neq 0$ ,  $\forall t \in I$ , as colunas da matriz são linearmente independentes em  $I$  e, além disso,  $\Phi$  é a matriz fundamental de (2.4) em  $I$ .

( $\Leftarrow$ ) Por outro lado, se é uma matriz fundamental, então toda solução  $\psi$  de (2.4), em  $I$ , tem a forma  $\psi(t) = \Phi(t)c$  para algum vetor constante  $c$ . Para cada  $t_0$  fixado em  $I$  e qualquer vetor  $\psi(t_0)$ , por  $\Phi(t)$  ser a matriz fundamental, o sistema de equações algébricas  $\psi(t_0) = \Phi(t_0)c$  tem uma única solução para  $c$ .

Portanto,  $\det \Phi(t_0) \neq 0$ . Agora, a Fórmula de Abel nos diz que  $\det \Phi(t) \neq 0$ ,  $\forall t \in I$ . ■

**Observação 2.7.** Logo, a matriz  $\Phi(t)$  é chamada de matriz fundamental de solução se:

- Suas colunas forem soluções linearmente independentes do sistema em  $I$ .

- O determinante da matriz  $\Phi(t)$  for diferente de zero, ou seja,  $\det \Phi(t) \neq 0$ , para todo  $t \in I$ .

Essa matriz é fundamental porque qualquer solução do sistema pode ser escrita como uma combinação linear das colunas de  $\Phi(t)$ . Assim, todas as soluções do sistema homogêneo podem ser expressas como

$$y(t) = \Phi(t)c,$$

onde  $c$  é um vetor constante.

**Teorema 2.8.** *Se  $\Phi$  é uma matriz fundamental para (2.4) em  $I$  e  $C$  é uma matriz constante não singular, então  $\Phi \cdot C$  também é uma matriz fundamental para (2.4) em  $I$ . Cada matriz fundamental de (2.4) é desta forma, para alguma matriz não singular  $C$ .*

*Demonstração.* Para provar isso, precisamos mostrar que  $\Phi \cdot C$  também é uma matriz fundamental para (2.4) em  $I$ , onde  $\Phi$  é uma matriz fundamental para o sistema.

Primeiro, vamos verificar se  $\Phi \cdot C$  é solução do sistema. Para isso, derivamos  $\Phi \cdot C$  em relação a  $t$  e verificamos se é igual a  $A(t) \cdot \Phi \cdot C$ . Calculemos então a derivada de  $\Phi \cdot C$  em relação a  $t$ :

$$\frac{d}{dt}(\Phi \cdot C) = \frac{d\Phi}{dt} \cdot C.$$

Sabemos que  $\Phi$  é solução do sistema, então  $\frac{d\Phi}{dt} = A(t) \cdot \Phi$ .

Substituindo:

$$\frac{d}{dt}(\Phi \cdot C) = A(t) \cdot \Phi \cdot C.$$

Agora, precisamos verificar se isso é igual a  $A(t) \cdot \Phi \cdot C$ . Ou seja, precisamos mostrar que  $\Phi \cdot \frac{dC}{dt} = 0$ . Dado que  $C$  é constante, temos:

$$\frac{dC}{dt} = 0, \quad \text{portanto,} \quad \Phi \cdot \frac{dC}{dt} = \Phi \cdot 0 = 0.$$

Assim,  $\Phi \cdot C$  é de fato solução do sistema (2.4).

Em relação à segunda parte da afirmação, para mostrar que cada matriz fundamental para (2.4) pode ser expressa como  $\Phi \cdot C$  para alguma matriz não singular  $C$ , podemos considerar  $C = \Phi(t_0)^{-1}$ , onde  $\Phi$  é uma matriz fundamental para o sistema. Isso ocorre porque  $\Phi$  é invertível, pois é uma matriz fundamental, então  $\Phi(t_0)^{-1}$  existe e é não singular. Portanto,  $\Phi \cdot \Phi(t_0)^{-1}$  é uma matriz fundamental expressa como  $\Phi \cdot C$  para uma matriz não singular  $C$ . ■

### 3 Sistemas lineares com coeficientes periódicos

Primeiro consideramos o sistema linear

$$y' = A(t)y, \tag{3.1}$$

no qual  $A(t)$  é uma matriz  $n \times n$  periódica de período  $\omega$ , ou seja,  $A(t + \omega) = A(t)$ , em  $-\infty < t < \infty$ . Temos que se  $\Phi(t)$  é a matriz fundamental de (3.1) então

$$\Phi'(t + \omega) = A(t + \omega)\Phi(t + \omega) = A(t)\Phi(t + \omega).$$

Dessa forma,  $\Phi(t + \omega)$  é uma matriz solução de (3.1) e, pela Fórmula de Abel, temos que  $\det \Phi(t + \omega) \neq 0$ . Então, pelo Teorema 2.6,  $\Phi(t + \omega)$  também é uma matriz fundamental

de (3.1) e, portanto, pelo Teorema 2.8 existe uma matriz constante não singular  $C$ , em  $-\infty < t < \infty$ , tal que

$$\Phi(t + \omega) = \Phi(t)C. \quad (3.2)$$

Pode-se mostrar que, correspondendo a toda matriz constante não singular  $C$ , existe uma matriz  $R$ , tal que  $C = e^{\omega R}$ . Notamos que se  $\Phi(0) = I$ , então, por (3.2)

$$\Phi(\omega) = e^{\omega R}. \quad (3.3)$$

Agora, podemos estabelecer o Teorema de Floquet.

**Observação 3.1.** Pode-se observar que se  $A(t)$  é uma matriz constante, portanto, periódica de qualquer período  $\omega$ , o resultado a seguir se reduz ao caso já estudado em que  $A(t)$  é constante para coeficientes constantes com  $P(t) = I$  e  $R = A$ .

**Teorema 3.2** (Teorema de Floquet). *Seja  $A(t)$  uma matriz periódica contínua de período  $\omega$  e seja  $\Phi(t)$  qualquer matriz fundamental do sistema (3.1). Notamos que existe uma matriz periódica não singular  $P(t)$  de período  $\omega$  e uma matriz constante  $R$  tal que*

$$\Phi(t) = P(t)e^{tR}. \quad (3.4)$$

*Demonstração.* Seja  $\Phi(t)$  uma matriz fundamental arbitrária do sistema (3.1). Seja  $R$  a matriz determinada por  $\Phi(\omega)$  através da equação (3.2), que satisfaz  $\Phi(\omega) = \Phi(0)e^{\omega R}$ . Agora, definimos, para todo  $t \in \mathbb{R}$ ,

$$P(t) = \Phi(t)e^{-tR}. \quad (3.5)$$

Claramente,  $P(t)$ , sendo o produto de duas matrizes não singulares ( $\Phi(t)$  e  $e^{-tR}$ ), é não singular. Além disso, verificamos que:

$$P(t + \omega) = \Phi(t + \omega)e^{-(t+\omega)R}.$$

Como  $\Phi(t)$  é uma matriz fundamental do sistema periódico e  $\Phi(t + \omega) = \Phi(t)e^{\omega R}$ , temos:

$$P(t + \omega) = \Phi(t)e^{\omega R}e^{-(t+\omega)R} = \Phi(t)e^{-tR} = P(t).$$

Assim,  $P(t)$  é periódica com período  $\omega$ . Finalmente, resolvendo (3.5) para  $\Phi(t)$ , obtemos:

$$\Phi(t) = P(t)e^{tR},$$

conforme desejado. ■

**Observação 3.3.** Se  $A(t)$  é real, seu período  $\omega$  é real, então mesmo que  $\Phi(t)$  seja real, não é necessariamente verdade que a matriz  $R$  seja real. Note, por exemplo, que se  $n = 1$  e se  $C$  em (3.2) for qualquer número real negativo, então  $C$  não tem um logaritmo real, de modo que  $R$  não pode ser. Neste caso, usamos

$$\Phi(t + 2\omega) = \Phi(t + \omega)C = \Phi(t)C^2,$$

definimos  $S$  por

$$C^2 = e^{2\omega S} \quad (3.6)$$

e pode ser mostrado que  $S$  é real. Pode-se então mostrar ainda que existe uma matriz real não singular  $Q(t)$  de período  $2\omega$  tal que

$$\Phi(t) = Q(t)e^{tS}. \quad (3.7)$$

O Teorema de Floquet pode ser usado para transformar o sistema (3.1) em um sistema linear com coeficientes constantes como segue. Deixemos

$$y = P(t)u, \quad (3.8)$$

onde  $P(t)$  é a matriz periódica do Teorema 3.2. Já que, de (3.1),

$$\left[ P(t)e^{tR} \right]' = P'(t)e^{tR} + P(t)e^{tR}R = A(t)P(t)e^{tR}$$

segue que

$$P'(t) = A(t)P(t) - P(t)R.$$

Assim,

$$y' = P(t)u' + P'(t)u = P(t)u' + (A(t)P(t) - P(t)R)u = A(t)P(t)u$$

e, portanto,

$$P(t)u' - P(t)Ru = 0$$

ou

$$u' = Ru, \quad (3.9)$$

que é um sistema linear de coeficientes constantes.

Com isso, acabamos de provar o seguinte resultado.

**Corolário 3.4.** *A mudança da variável  $y = P(t)u$  transforma o sistema periódico (3.1) no sistema (3.9) com coeficientes constantes, conforme provado acima. Costuma-se chamar os autovalores  $\lambda_i$  da matriz não singular  $e^{\omega R}$  de multiplicadores do sistema (3.1), e chamar os autovalores  $\rho_i$  da matriz  $R$  de expoentes característicos do sistema (3.1).*

A prova, segue-se, também, do teorema do logaritmo de uma matriz, enunciado a seguir, como resultado auxiliar:

**Teorema 3.5.** *Seja  $B$  uma matriz  $n \times n$  não singular. Então existe uma matriz  $A$   $n \times n$ , chamada logaritmo de  $B$ , tal que*

$$e^A = B.$$

Temos que

$$\rho_i = \frac{1}{\omega} \log \lambda_i, \quad \text{com } i = 1, \dots, n. \quad (3.10)$$

Vamos apresentar, agora, mais algumas consequências do Teorema 3.2:

**Corolário 3.6 (do Teorema 3.2).** *Uma solução  $\phi(t)$  do sistema (3.1) tem a propriedade  $\phi(t + \omega) = K\phi(t)$ , em  $-\infty < t < \infty$ , onde  $K$  é uma constante se, e somente se,  $K$  for um autovalor de  $\Phi(\omega) = e^{\omega R}$ .*

**Corolário 3.7 (do Teorema 3.2).** *Se os expoentes característicos do sistema (3.1) tiverem partes reais negativas, ou equivalentemente, se os multiplicadores do sistema (3.1) tiverem magnitude estritamente menor do que 1, então todas as soluções do sistema (3.1) se aproximam de zero.*

**Exemplo 3.8.** Considere a equação escalar

$$u'' = p(t)u' + q(t)u = 0, \quad (3.11)$$

onde  $p$  e  $q$  são funções contínuas de período  $\omega$  em  $t$ . Determine uma equação satisfeita pelos multiplicadores.

*Resolução:* Denotando  $y_1 = u$  e  $y_2 = u'$ , obtemos o sistema equivalente

$$\begin{cases} y_1' = y_2, \\ y_2' = -q(t)y_1 - p(t)y_2. \end{cases} \quad (3.12)$$

Seja  $\Phi(t)$  a matriz fundamental que é a identidade em  $t = 0$ . Então,

$$\Phi(t) = \begin{pmatrix} \phi_1(t) & \phi_2(t) \\ \phi_1'(t) & \phi_2'(t) \end{pmatrix}, \quad (3.13)$$

onde  $\phi_1$  e  $\phi_2$  são as soluções de (3.11) tais que  $\phi_1(0) = \phi_2'(0) = 1$ ,  $\phi_2(0) = \phi_1'(0) = 0$ . De acordo com a definição de multiplicadores e a equação (3.13), os multiplicadores são os autovalores de  $\Phi(\omega)$  e, portanto, usando (3.13), eles satisfazem a equação

$$\det(\Phi(\omega) - \lambda I) = \lambda^2 - (\phi_1(\omega) + \phi_2'(\omega))\lambda + \det \Phi(\omega) = 0.$$

Pela fórmula de Abel,

$$\det \Phi(\omega) = \det \Phi(0) \exp\left(-\int_0^\omega p(s) ds\right) = \exp\left(-\int_0^\omega p(s) ds\right).$$

Assim, os multiplicadores são as raízes da equação

$$\lambda^2 - (\phi_1(\omega) + \phi_2'(\omega))\lambda + \exp\left(-\int_0^\omega p(s) ds\right) = 0.$$

Voltando para o sistema não homogêneo,

$$y' = A(t)y + g(t), \quad (3.14)$$

onde assumimos ao longo do processo que  $A(t)$  e  $g(t)$  são contínuos e periódicos em  $t$  do mesmo período  $\gamma$ . Note que o caso de  $A(t)$  ser uma matriz constante não está excluído.

Um caso especial importante de (3.14) é a equação escalar

$$u'' + a_1u' + a_2u = A \cos(Kt),$$

onde  $a_1$  e  $a_2$  são constantes, o que surge em diversas aplicações. Também é conhecida como a equação do oscilador harmônico.

Queremos estudar a questão da existência de soluções periódicas de (3.14).

**Teorema 3.9.** *Uma solução  $\phi(t)$  de (3.14) é periódica de período  $\omega$  em  $t$  se, e somente se,  $\phi(\omega) = \phi(0)$ .*

*Demonstração.* Se for periódica de período  $\omega$ , é óbvio que  $\phi(\omega) = \phi(0)$ . Por outro lado, suponha que  $\phi(t)$  é uma solução de (3.14) tal que  $\phi(\omega) = \phi(0)$ . Considere as funções  $\phi(t)$  e  $\psi(t) = \phi(t + \omega)$ . Então  $\phi$  e  $\psi$  são ambas soluções de (3.14) e  $\psi(0) = \phi(\omega) = \phi(0)$ . Assim, as soluções  $\phi$  e  $\psi$  têm os mesmos valores iniciais e, pelo teorema da unicidade,  $\phi(t) \equiv \psi(t) = \phi(t + \omega)$ , em  $-\infty < t < \infty$ , o que comprova a periodicidade. ■

**Teorema 3.10.** *O sistema (3.14) tem uma solução periódica de período  $\gamma$  para qualquer vetor forçante periódico  $g$  de período  $\gamma$  se, e somente se, o sistema homogêneo  $y' = A(t)y$  não tem solução periódica de período  $\omega$  exceto a solução trivial  $y \equiv 0$ .*

*Demonstração.* Seja  $\Phi(t)$  a matriz fundamental do sistema homogêneo (3.1) que é a matriz identidade em  $t = 0$ . Na verdade,  $\Phi$  é dada por (3.4). Pela Fórmula da Variação de Constantes, toda solução  $\psi(t)$  de (3.14) tem a forma

$$\psi(t) = \Phi(t)\psi(0) + \Phi(t) \int_0^t \Phi^{-1}(s)g(s) ds.$$

Pelo Teorema 3.9, a solução  $\psi$  será periódica se, e somente se,  $\psi(0) = \psi(\omega)$ . Mas

$$\psi(\omega) = \Phi(\omega)\psi(0) + \Phi(\omega) \int_0^\omega \Phi^{-1}(s)g(s) ds$$

e a condição de periodicidade  $\psi(\omega) = \psi(0)$  torna-se

$$[I - \Phi(\omega)] \psi(0) = \Phi(\omega) \int_0^\omega \Phi^{-1}(s)g(s) ds.$$

Este é um sistema linear não homogêneo de equações algébricas para os componentes do vetor  $\psi(0)$ , que deve ser solucionável para cada vetor forçante periódico  $g$ . Isso é possível se, e somente se,  $\det(I - \Phi(\omega)) \neq 0$ . Assim, (3.3) e a definição de multiplicadores dizem que a solução de (3.14) é periódica se, e somente se, 1 não for um multiplicador do sistema homogêneo  $y' = A(t)y$ . Combinado com o Corolário 3.7 do Teorema 3.2, usando  $K = 1$ , temos o resultado. ■

## 4 Considerações Finais

Neste trabalho, abordamos a teoria das equações diferenciais ordinárias, com foco em sistemas periódicos e suas características fundamentais. Através da análise do Teorema de Floquet, demonstramos como a transformação de variáveis pode converter sistemas complexos em modelos com coeficientes constantes, facilitando a identificação de soluções periódicas.

**Agradecimentos:** Ao apoio financeiro da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) pelo financiamento deste trabalho.

*Abstract:* This work addresses the qualitative theory of ordinary differential equations, focusing on periodic systems and their solutions. It begins with an introduction to non-homogeneous linear systems and presents Floquet's Theorem, which is essential for transforming periodic systems into systems with constant coefficients. The fundamental matrix  $\Phi(t)$  is defined, and the properties of eigenvalues and characteristic exponents are explored.

From Floquet's Theorem, it is demonstrated that the variable change  $y = P(t)u$  transforms a periodic system into a linear system with constant coefficients, facilitating the analysis of its solutions. The relationship between the multipliers and the eigenvalues of matrix  $R$  is established, and the condition for the existence of periodic solutions is discussed.

One of the main results is that a solution of the non-homogeneous system  $y' = A(t)y + g(t)$  is periodic if and only if the conditions on the associated homogeneous system are met. The work includes the analysis of a scalar equation as an example, demonstrating the practical application of the discussed theories.

*Keywords:* linear systems; periodic coefficients; Floquet's Theorem

## Referências Bibliográficas

- [1] Brauer, F.; Nohel, J. A. *The Qualitative Theory of Ordinary Differential Equations*. W.A. Benjamin, 1969.



- [2] Silva, T. R. V. *A Influência De Uma Ação Impulsiva no Comportamento De Soluções De Equações Diferenciais*. UNESP, 2011.

# Aplicação de Corpos Finitos na Criptografia: Um Estudo do Algoritmo AES

Lídia Campelo da Silva

Orientador(a): Profa. Dra. Sara Díaz Cardell

**Resumo:** O objetivo deste trabalho consiste em realizar uma análise aprofundada do algoritmo de criptografia simétrica AES (Advanced Encryption Standard) e estudar a aplicação de corpos finitos na construção deste algoritmo, com ênfase na camada de substituição.

**Palavras-chave:** Advanced Encryption Standard (AES); criptografia; corpos finitos; camada de substituição.

---

## 1 Introdução

A criptografia é a arte de proteger informações por meio da transformação de dados de forma que não possam ser facilmente compreendidos por terceiros. Atualmente, a criptografia é a base de muitas das tecnologias de segurança que usamos diariamente, como transações bancárias online, comunicação por e-mail e armazenamento de dados, entre outros. Com o crescimento exponencial das comunicações eletrônicas, a criptografia tem-se tornado essencial para garantir a privacidade e a integridade das informações.

A criptografia pode ser dividida em duas categorias: simétrica e assimétrica [1, 2]. A criptografia simétrica utiliza a mesma chave tanto para criptografar quanto para descriptografar os dados. Embora seja rápida e eficiente, especialmente para grandes volumes de informações, enfrenta o desafio de como distribuir essa chave de maneira segura antes da comunicação. Já a criptografia assimétrica, que surgiu como uma solução para esse problema, usa um par de chaves: uma chave pública para criptografar os dados e uma chave privada para descriptografá-los. Esse método melhora a segurança, pois elimina a necessidade de compartilhar a chave privada entre as partes envolvidas na comunicação, porém os algoritmos assimétricos usam chaves muito maiores e são computacionalmente mais lentos que os algoritmos simétricos. Neste trabalho, estudamos o (Advanced Encryption Standard), um algoritmo de bloco simétrico, ou seja, um algoritmo que usa a mesma chave para criptografar a descriptografar e cifra a mensagem em blocos de tamanho constante.

O algoritmo AES surgiu como uma resposta à carência de um padrão de criptografia mais seguro e eficiente. Nos anos 1990, o algoritmo de criptografia padrão na época, o DES (Data Encryption Standard) [1, Capítulo 3], começou a ser considerado vulnerável devido ao aumento da capacidade computacional e ao surgimento de novas técnicas de criptoanálise. O DES não era mais adequado para garantir a segurança necessária em um cenário de crescente uso da internet [1, Seção 3.5].

Por conta dessas preocupações, o NIST (National Institute of Standards and Technology) dos Estados Unidos iniciou, em 1997, um processo público para desenvolver um novo padrão de criptografia que substituísse o DES. Esse processo envolveu a submissão de vários algoritmos. Ao final do processo, em 2000, o algoritmo Rijndael, desenvolvido pelos criptógrafos belgas Joan Daemen e Vincent Rijmen, foi escolhido como o novo padrão e recebeu o nome de AES [1, Capítulo 4]. Neste trabalho fazemos uma análise aprofundada da estrutura interna

do algoritmo AES e estudamos o uso de corpos finitos de característica dois na camada de substituição do algoritmo.

## 2 Preliminares

Para compreender melhor todos os processos envolvidos no AES, nesta seção, relembramos alguns resultados importantes sobre corpos finitos, polinômios e operações. Para o desenvolvimento desta parte, utilizamos as referências [3, 4].

**Definição 2.1.** Um anel  $(R, +, \cdot)$  é um conjunto  $R$  munido de duas operações binárias, adição e multiplicação, tal que

- (a)  $(R, +)$  é um grupo abeliano;
- (b)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  para quaisquer  $a, b, c \in R$ ;
- (c)  $a \cdot (b + c) = a \cdot b + a \cdot c$ ,  $(b + c) \cdot a = b \cdot a + c \cdot a$  para quaisquer  $a, b, c \in R$ .

**Definição 2.2.** Seja  $R$  um anel.

1. Denotamos o elemento neutro da operação “+” como  $0_R$ , por conveniência, neste trabalho, vamos usar apenas 0.
2.  $R$  é um anel com identidade se o anel possuir elemento neutro para a operação “ $\cdot$ ”, chamado identidade e denotado por  $1_R$ ;
3.  $R$  é comutativo se a operação “ $\cdot$ ” for comutativa;
4.  $R$  é um domínio de integridade se for comutativo, com identidade e se  $a \cdot b = 0$  implicar que  $a = 0$  ou  $b = 0$ , para quaisquer  $a, b \in R$ ;
5.  $R$  é um anel com divisão se os elementos não nulos de  $R$  formarem um grupo sob a operação “ $\cdot$ ”;
6.  $R$  é um corpo se for um anel com divisão comutativo.

**Definição 2.3.** A ordem de um corpo  $\mathbb{F}$  é a quantidade de elementos diferentes que o conjunto  $\mathbb{F}$  possui. No caso de um corpo finito, sua ordem é sempre uma potência de um número primo.

**Definição 2.4.** Seja  $R$  é um anel e seja  $n$  o menor inteiro positivo tal que  $nr = 0$ , para todo  $r \in R$ , onde  $nr = r + r + \dots + r$ ,  $n$  vezes. Então dizemos que  $R$  tem característica finita e  $n$  é a característica de  $R$ . Caso contrário, dizemos que  $R$  tem característica zero.

**Teorema 2.5** ([4, Theorem 1.44]). *Um anel  $R \neq \{0\}$  com característica positiva, identidade e sem divisores de zero deve ter característica prima.*

**Prova:** Se  $n$  não fosse primo, poderíamos escrever  $n = km$  com  $k, m \in \mathbb{Z}$  e  $1 < k, m < n$ . Então,

$$0 = n1_R = (km)1_R = (k1_R) \cdot (m1_R),$$

o que implica que ou  $k1_R = 0$  ou  $m1_R = 0$ , já que  $R$  não tem divisores de zero. Isso implica que ou  $kr = (k1_R) \cdot r = 0$  para todo  $r \in R$ , ou  $mr = (m1_R) \cdot r = 0$  para todo  $r \in R$ , em contradição com a minimalidade da característica  $n$ . ■

**Corolário 2.6** ([4, Corolário 1.45]). *Todo corpo finito tem característica prima.*

**Definição 2.7.** Um corpo (de Galois) primo é um corpo finito que possui ordem  $p$ , onde  $p$  é um número primo. Este corpo é denotado por  $\mathbb{F}_p$  ou  $GF(p)$ , os elementos são  $\{0, 1, 2, \dots, p-1\}$ , e as operações de soma e produto são realizadas módulo  $p$ . Além disso, a característica do corpo é  $p$ .

**Exemplo 2.8.** Considere o corpo finito  $\mathbb{F}_2 = \{0, 1\}$ , conhecido como o corpo binário. A aritmética neste corpo é realizada módulo 2, resultando nas seguintes tabelas de operações:

Adição:	Multiplicação:																		
<table style="border-collapse: collapse; margin: auto;"> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">+</td> <td style="padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">1</td> <td style="padding: 5px 10px;">1</td> <td style="padding: 5px 10px;">0</td> </tr> </table>	+	0	1	0	0	1	1	1	0	<table style="border-collapse: collapse; margin: auto;"> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">·</td> <td style="padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">0</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px 10px;">1</td> <td style="padding: 5px 10px;">0</td> <td style="padding: 5px 10px;">1</td> </tr> </table>	·	0	1	0	0	0	1	0	1
+	0	1																	
0	0	1																	
1	1	0																	
·	0	1																	
0	0	0																	
1	0	1																	

**Definição 2.9.** Um corpo  $\mathbb{F}$  é uma extensão finita de  $\mathbb{K}$  se  $\mathbb{K} \subseteq \mathbb{F}$  e  $\mathbb{F}$  é um espaço vetorial de dimensão finita sobre  $\mathbb{K}$ . Nesse caso, referimo-nos à dimensão  $m$  de  $\mathbb{F}$  sobre  $\mathbb{K}$  como o grau da extensão, e escrevemos  $[\mathbb{F} : \mathbb{K}] = m$ .

**Definição 2.10.** Um polinômio  $f$  sobre  $\mathbb{F}_p$  é uma expressão da forma  $f(x) = \sum_{i=0}^n a_i x^i$ , onde  $n$  é um número inteiro não negativo e  $a_i \in \mathbb{F}_p$  para  $i = 0, 1, \dots, n$ . Um polinômio é dito mônico se o coeficiente da maior potência de  $x$  for 1. O anel formado pelos polinômios sobre  $\mathbb{F}_p$ , com a soma e o produto de polinômios usual, é chamado de anel de polinômios sobre  $\mathbb{F}_p$  e é denotado por  $\mathbb{F}_p[x]$ .

**Definição 2.11.** Um polinômio  $f \in \mathbb{F}_p[x]$  é um polinômio irredutível sobre  $\mathbb{F}_p$  se  $f$  tiver grau positivo e  $f = gh$ , com  $g, h \in \mathbb{F}_p[x]$ , implicar que ou  $g$  ou  $h$  é um polinômio constante.

Agora, estamos prontos para definir os elementos e as operações em uma extensão de  $\mathbb{F}_p$ . Na extensão  $\mathbb{F}_{p^m}$ ,  $m$  inteiro positivo, os elementos não são representados como inteiros, mas como polinômios de grau menor que  $m$ , com coeficientes em  $\mathbb{F}_p$ :

$$\mathbb{F}_{p^m} = \{a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1} \mid a_i \in \mathbb{F}_p\}.$$

As operações soma e produto são realizadas módulo um polinômio irredutível de grau  $m$  em  $\mathbb{F}_p$ , para garantir que as operações sejam fechadas. Sejam  $A(x) = \sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}_{p^m}$  e  $B(x) = \sum_{i=0}^{m-1} b_i x^i \in \mathbb{F}_{p^m}$ . A soma dos dois elementos é então computada de acordo com:

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i,$$

onde  $c_i \equiv (a_i + b_i) \pmod p$ . Por outro lado, a diferença é computada de acordo com:

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i,$$

onde  $c_i \equiv a_i - b_i \pmod p$ . Note que quando  $p = 2$ , tem-se que  $A(x) - B(x) = A(x) + B(x)$ .

Dado  $P(x) \in \mathbb{F}_p[x]$  um polinômio irredutível de grau  $m$ , definimos o produto dos dois elementos  $A(x), B(x) \in \mathbb{F}_{p^m}$  como:

$$C(x) \equiv A(x) \cdot B(x) \pmod{P(x)}.$$

**Exemplo 2.12.** O corpo  $\mathbb{F}_4$  pode ser construído sobre  $\mathbb{F}_2$  usando o polinômio irredutível  $Q(x) = x^2 + x + 1$ . Este corpo contém 4 elementos,  $\mathbb{F}_4 = \{0, 1, x, x + 1\}$ , e as tabelas das duas operações são dadas a continuação:

**Adição:**

+	0	1	$x$	$x + 1$
0	0	1	$x$	$x + 1$
1	1	0	$x + 1$	$x$
$x$	$x$	$x + 1$	0	1
$x + 1$	$x + 1$	$x$	1	0

**Multiplicação:**

×	0	1	$x$	$x + 1$
0	0	0	0	0
1	0	1	$x$	$x + 1$
$x$	0	$x$	$x + 1$	1
$x + 1$	0	$x + 1$	1	$x$

Corpos finitos de característica 2 são amplamente usados na criptografia por sua eficiência em hardware. As operações como a soma e a multiplicação, são rápidas e fáceis de implementar em circuitos digitais. Isso é útil em algoritmos como o AES [5] e em criptografia baseada em curvas elípticas (ECC) [1, Capítulo 9], onde a eficiência é crucial. Em particular, o AES trabalha com o corpo  $\mathbb{F}_{2^8}$ , onde cada elemento  $A \in \mathbb{F}_{2^8}$  é representado como

$$A(x) = a_0 + a_1x + \dots + a_7x^7, \quad a_i \in \mathbb{F}_2,$$

e as operações são realizadas módulo o polinômio irreduzível  $P(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$  (mais detalhes na Seção 4).

### 3 Estrutura interna do AES

O Advanced Encryption Standard é um algoritmo de criptografia simétrica que opera em blocos de 128 bits e pode usar chaves de 128, 192 ou 256 bits. Os algoritmos de bloco precisam oferecer as propriedades de difusão e confusão para garantir sua segurança. A difusão assegura que pequenas alterações no texto original (texto claro) resultem em grandes mudanças no texto cifrado, espalhando o impacto por todo o bloco cifrado. Já a confusão cria uma relação complexa entre a chave e o texto cifrado, tornando difícil deduzir a chave com base em padrões estatísticos

O processo de criptografia do AES envolve múltiplas rodadas de iterações, variando de 10 a 14 rodadas, dependendo do tamanho da chave. Cada rodada inclui operações como SubBytes (substituição de bytes), ShiftRows (permutação dos elementos das linhas), MixColumns (multiplicação de matrizes) e AddRoundKey (adição da chave da rodada). Na Figura 2.1 é possível observar a estrutura iterativa do algoritmo. No AES o processo de confusão ocorre na etapa de SubBytes, enquanto a difusão ocorre nas etapas de ShiftRows e MixColumns.

O AES é um cifrador orientado a bytes. A entrada de 16 bytes  $A_0, \dots, A_{15}$  é processada byte a byte pela S-Box. A saída de 16 bytes  $B_0, \dots, B_{15}$  é permutada byte a byte na camada ShiftRows e misturada pela transformação MixColumns. Finalmente, a subchave de 128 bits  $k_i$  é adicionada com o resultado intermediário. Na Figura 2.2 é possível observar a estrutura interna de cada rodada do algoritmo.

Para entender como os dados se movem através do AES, primeiramente notemos que o estado  $A$  é composto por 16 bytes em formato hexadecimal,  $A_0, A_1, \dots, A_{15}$ , e estes bytes estão dispostos em uma matriz de tamanho  $4 \times 4$ :

$$\begin{pmatrix} A_0 & A_4 & A_8 & A_{12} \\ A_1 & A_5 & A_9 & A_{13} \\ A_2 & A_6 & A_{10} & A_{14} \\ A_3 & A_7 & A_{11} & A_{15} \end{pmatrix}$$

O AES opera sobre elementos, colunas ou linhas da matriz de estado atual. Da mesma forma, os bytes da chave são dispostos em uma matriz com quatro linhas e quatro (para chave de 128 bits), seis (para chave de 192 bits) ou oito (para chave de 256 bits) colunas.

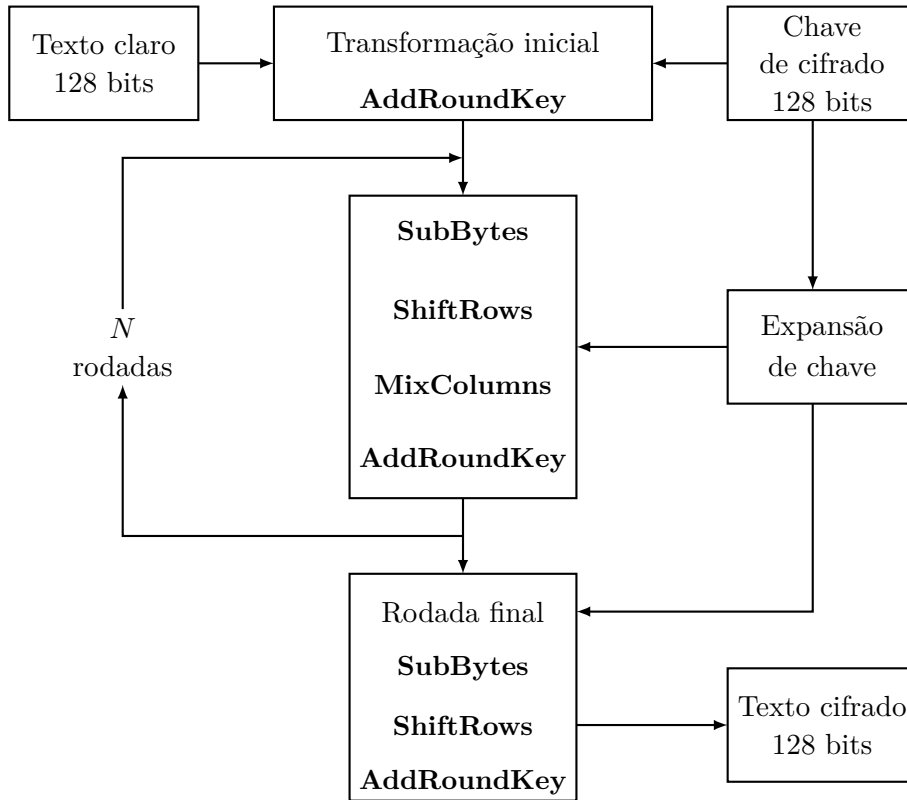


Figura 2.1: Estrutura do AES

### 3.1 SubBytes

A camada de substituição pode ser vista como uma fila de 16 S-Boxes paralelas, como podemos observar na Figura 2.2, cada uma com 8 bits (1 byte) de entrada e saída.

Todas as 16 S-Boxes são idênticas. Nesta camada, cada byte de estado  $A_i$  é substituído por outro byte  $B_i$ , ou seja,  $S(A_i) = B_i$ , para  $i = 0, 1, \dots, 15$ .

A S-Box é o único elemento não linear do AES. A caixa pode ser invertida de forma única, o que é necessário para a descryptografia. Nas implementações de software, a S-Box geralmente é realizada como uma tabela de consulta (vide Tabela 2.1). Note que os bytes de entrada e saída da S-Box estão em formato hexadecimal.

### 3.2 ShiftRows

A transformação ShiftRows desloca ciclicamente as linhas da matriz de estados. A segunda linha da matriz de estado é deslocada três bytes para a direita, a terceira linha dois bytes para a direita e a quarta linha um byte para a direita. A primeira linha não é alterada pela transformação ShiftRows. O objetivo da transformação ShiftRows é aumentar as propriedades de difusão no AES. Se a entrada da subcamada ShiftRows for dada como uma matriz de estado  $B$ , obtemos:

$$B = \begin{pmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_1 & B_5 & B_9 & B_{13} \\ B_2 & B_6 & B_{10} & B_{14} \\ B_3 & B_7 & B_{11} & B_{15} \end{pmatrix} \xrightarrow{\text{ShiftRows}} \begin{pmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_5 & B_9 & B_{13} & B_1 \\ B_{10} & B_{14} & B_2 & B_6 \\ B_{15} & B_3 & B_7 & B_{11} \end{pmatrix}$$

A matriz à esquerda é o estado de entrada, enquanto a matriz à direita é o estado de saída

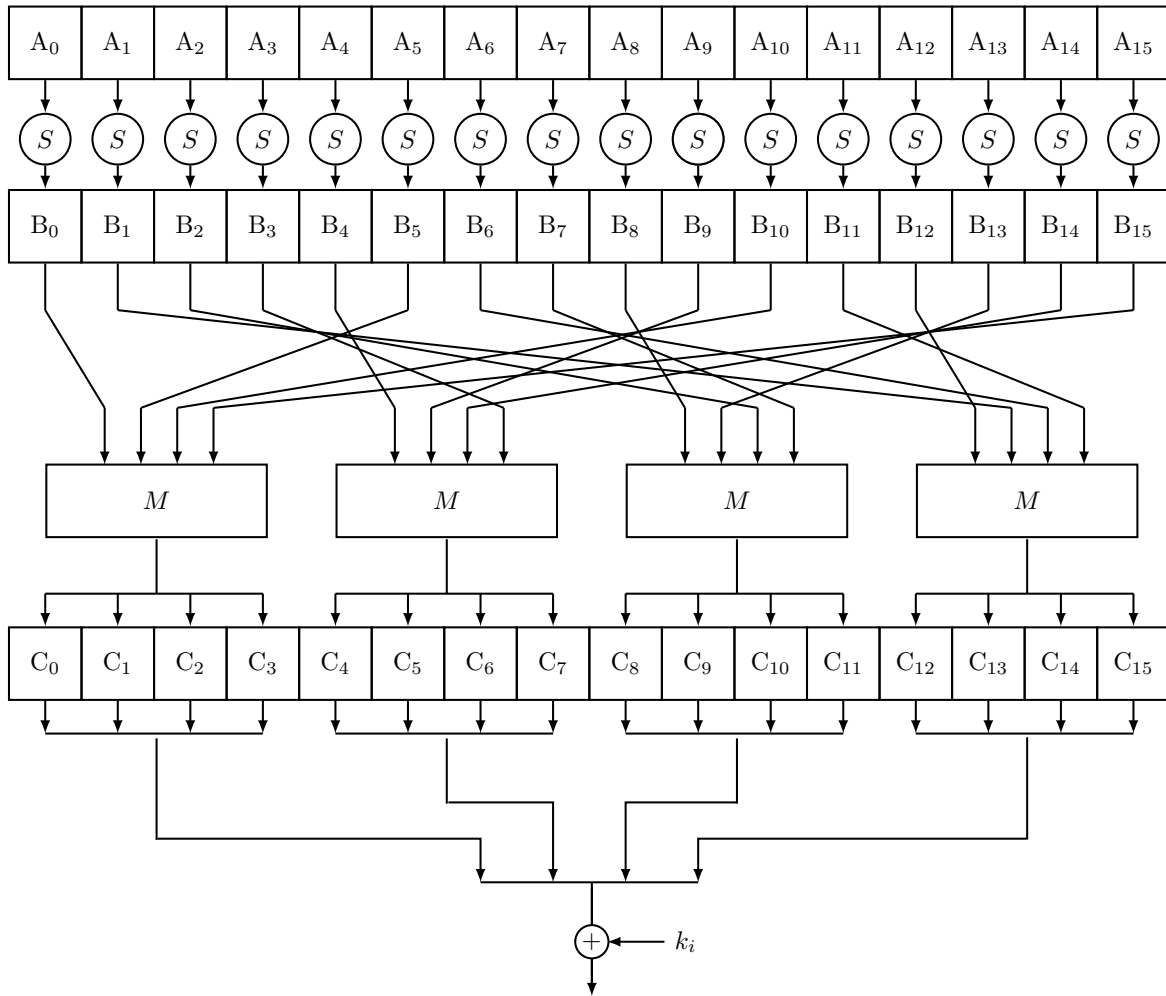


Figura 2.2: Estrutura interna de cada rodada do AES

após a transformação ShiftRows, onde as linhas são deslocadas conforme descrito acima.

### 3.3 MixColumns

A operação MixColumns é o principal elemento de difusão no AES, pois cada byte de entrada influencia quatro bytes de saída. A combinação das camadas ShiftRows e MixColumns torna possível que, após apenas três rodadas, cada byte da matriz de estado dependa de todos os 16 bytes do texto claro (texto original sem cifrar).

Denotamos o estado de entrada de 16 bytes por  $B$  e o estado de saída de 16 bytes por  $C$ ,  $\text{MixColumns}(B) = C$ , onde  $B$  é o estado após a operação ShiftRows. Agora, cada coluna de 4 bytes de  $B$  é considerada como um vetor e multiplicada por uma matriz  $M$  fixa de tamanho  $4 \times 4$  dada por:

$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

As entradas da matriz  $M$  são denotadas usando uma notação hexadecimal e a aritmética envolvendo os coeficientes de  $B$  e  $M$  é realizada no corpo finito  $\mathbb{F}_{2^8}$ , com polinômio irredutível

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
10	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
20	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
30	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
40	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
50	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
60	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
70	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
80	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
90	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A0	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B0	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C0	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D0	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E0	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F0	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tabela 2.1: S-Box do AES

$P(x) = x^8 + x^4 + x^3 + x + 1$ . Na Tabela 2.2 podemos ver os polinômios de  $\mathbb{F}_{2^8}$  correspondentes a cada entrada de  $M$ .

Constante Hexadecimal	Representação binária	Elemento em $\mathbb{F}_{2^8}$
01	00000001	1
02	00000010	$x$
03	00000011	$x + 1$

Tabela 2.2: Constantes e polinômios correspondentes no corpo  $\mathbb{F}_{2^8}$

**Exemplo 3.1.** Vejamos, por exemplo, como os primeiros quatro bytes de saída (primeira coluna de  $C$ ) são calculados:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

Aqui, cada saída  $C_i$ ,  $i = 0, 1, 2, 3$ , é obtida multiplicando os valores de entrada  $B_0, B_5, B_{10}, B_{15}$  pelos coeficientes constantes da matriz, utilizando operações no corpo  $\mathbb{F}_{2^8}$ :

$$\begin{aligned} C_0 &= 02B_0 + 03B_5 + 01B_{10} + 01B_{15} \\ C_1 &= 01B_0 + 02B_5 + 03B_{10} + 01B_{15} \\ C_2 &= 01B_0 + 01B_5 + 02B_{10} + 03B_{15} \\ C_3 &= 03B_0 + 01B_5 + 01B_{10} + 02B_{15} \end{aligned}$$

### 3.4 AddRoundKey

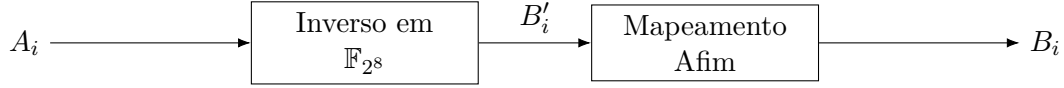
Os dados de entrada para a camada de Adição de Chave são a matriz de estado atual  $C$  de 16 bytes e uma subchave que também consiste em 16 bytes (128 bits). As duas entradas são combinadas por meio de uma operação XOR bit a bit.



## 4 Aplicação de corpos finitos no AES

Podemos observar as aplicações dos corpos finitos em duas etapas muito importantes, SubBytes e MixColumns. As operações envolvendo corpos finitos na etapa de MixColumns foi explicada anteriormente, agora vamos ver a aplicação na S-Box que se encontra na etapa de SubBytes, que é o principal objetivo deste trabalho.

A S-Box do AES pode ser vista como uma transformação matemática em duas etapas:



A primeira parte da substituição é uma inversão no corpo  $\mathbb{F}_{2^8}$ . Para cada elemento de entrada  $A_i$  calcula-se o inverso multiplicativo  $B'_i = A_i^{-1}$ , onde tanto  $A_i$  quanto  $B'_i$  são considerados elementos do corpo  $\mathbb{F}_{2^8}$ , usando o polinômio  $P(x) = x^8 + x^4 + x^3 + x + 1$  como polinômio irredutível fixo.

Na segunda parte da substituição, cada byte  $B'_i$  é multiplicado por uma matriz de bits constante, seguida da adição de um vetor constante de 8 bits. A operação é descrita por:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \pmod 2 \quad (4.1)$$

Na maioria das implementações do AES, as saídas da S-Box são computadas usando a Tabela 2.1.

**Exemplo 4.1.** Consideremos o byte dado por  $A = 01010011_2 = 83_{10} = 53_{16}$ . O polinômio correspondente é dado por  $p(x) = x^6 + x^4 + x + 1$ .

Queremos calcular o inverso multiplicativo de  $p(x)$ . Para isso, usamos o algoritmo estendido de Euclides e obtemos:

$$\begin{aligned} p(x) \cdot q(x) &= (x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x) \\ &= x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x \\ &= (x^8 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + x) + 1 \\ &= 1 \pmod{(x^8 + x^4 + x^3 + x + 1)} \end{aligned}$$

Portanto,  $q(x) = x^7 + x^6 + x^3 + x$  é o inverso multiplicativo de  $p(x)$  e temos que  $B' = 11001010$ .

Agora, realizamos o mapeamento afim descrito em (4.1):

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Para finalizar, temos que  $B = 11101101_2 = 237_{10} = ED_{16}$ . Conferindo na Tabela 2.1, podemos confirmar que a imagem do byte  $A = 53$  através da S-Box é exatamente o byte  $B = ED$ .

## 5 Considerações finais

Neste trabalho, foi possível analisar de maneira mais aprofundada a estrutura interna do algoritmo de criptografia simétrica AES e a aplicação de corpos finitos, com ênfase na camada de substituição. Observamos que o AES se apoia fortemente em operações aritméticas baseadas em corpos finitos, particularmente no corpo  $\mathbb{F}_{2^8}$ .

Podemos notar que a criptografia AES é composta por diversas camadas que garantem tanto a confusão quanto a difusão dos dados ao longo das várias rodadas do processo de cifrado. Em especial, a camada SubBytes, que utiliza a S-Box, introduz uma não-linearidade essencial ao algoritmo, dificultando os ataques por criptoanálise. Além disso, a eficiência do AES em lidar com grandes volumes de dados, devido ao uso de operações modulares simples, como a soma e multiplicação em corpos de característica dois, demonstra a importância dos corpos finitos.

Assim, concluímos que o uso de corpos finitos no AES é um exemplo claro de como conceitos matemáticos abstratos podem ser aplicados de maneira prática e eficaz em tecnologias modernas de segurança da informação. A substituição baseada em corpos finitos no AES fornece uma estrutura robusta que contribui significativamente para a segurança e o desempenho deste algoritmo.

**Agradecimentos:** Agradeço à Profa. Dra. Sara Díaz Cardell, pela orientação e incentivo.

*Abstract: The objective of this work is to conduct an in-depth analysis of the AES (Advanced Encryption Standard) algorithm and to investigate the application of finite fields in cryptography, with a focus on the construction of the substitution layer of AES.*

*Keywords: Advanced Encryption Standard (AES); cryptography; finite fields; substitution layer*

---

## Referências Bibliográficas

- [1] C. Paar e J. Pelz, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Berlin, Heidelberg (2010).
- [2] N. P. Smart, *Cryptography Made Simple*. Springer Berlin, Heidelberg (2016).
- [3] G. L. Mullen e D. Panario Smart, *Handbook of finite fields*. CRC Press, (2013).
- [4] R. Lidl e H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, Cambridge (1986).
- [5] Federal Information Processing Standards Publication, *Advanced Encryption Standard (AES)*, 2001, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf> [Accessed: (Setembro, 2024)].

# Estabilidade de Equações Diferenciais com Retardamento via Teoremas de Ponto Fixo

Maitê Borges Fiorini dos Anjos<sup>†</sup>

Orientador(a): Profa. Dra. Suzete Maria Silva Afonso

**Resumo:** Este trabalho busca apresentar uma ferramenta poderosa para a análise qualitativa das equações diferenciais com retardamento: Teoremas de Ponto Fixo. Por meio dos Teoremas de Ponto Fixo de Banach e de Schauder obteremos resultados que garantem a estabilidade de soluções de equações diferenciais com retardamento.

**Palavras-chave:** equações diferenciais com retardamento; estabilidade; teorema do ponto fixo de Banach; teorema do ponto fixo de Schauder

---

## 1 Introdução

As equações diferenciais ordinárias e parciais são ferramentas amplamente utilizadas para modelar fenômenos reais. Contudo, existe uma grande quantidade de sistemas em que a taxa de variação do estado em cada instante depende, não somente do estado do processo nesse instante, mas também do histórico de estados do fenômeno. Assim sendo, para tais casos, torna-se apropriada a utilização das equações diferenciais com retardamento (EDRs), ferramentas capazes de descrever processos que envolvem atrasos de tempo de forma mais realística.

Todavia, a dinâmica das equações diferenciais com retardamento é bastante complexa, tornando a obtenção de soluções exatas uma tarefa desafiadora na maioria dos casos. Portanto, é fundamental identificar propriedades qualitativas que permitam uma compreensão mais profunda desses sistemas. Neste trabalho, apresentamos uma análise da estabilidade de equações diferenciais com retardamento (EDRs) por meio da aplicação de dois teoremas de ponto fixo, o Teorema do Ponto Fixo de Banach e o Teorema do Ponto Fixo de Schauder, que nos permitem estabelecer condições precisas para garantir a estabilidade das soluções.

## 2 Preliminares sobre as Equações Diferenciais com Retardamento

Nesta seção, temos como objetivo apresentar a definição de uma equação diferencial funcional (EDF) com retardamento e o teorema de existência e unicidade de solução para tal tipo de equação.

Sejam  $r \geq 0$  um número real,  $\mathbb{R} = (-\infty, \infty)$ ,  $\mathbb{R}^n$  o espaço vetorial real  $n$ -dimensional com norma  $|\cdot|$  e  $C([a, b], \mathbb{R}^n)$  o espaço de Banach das aplicações contínuas  $\phi$  de  $[a, b]$  em  $\mathbb{R}^n$  com a norma da convergência uniforme, dada por

$$\|\phi\| = \sup_{a \leq \theta \leq b} |\phi(\theta)|.$$

---

<sup>†</sup>Bolsista FAPESP, Processo: 2022/07722-0

Se  $t_0 \in \mathbb{R}$ ,  $A \geq 0$  e  $x \in C([t_0 - r, t_0 + A], \mathbb{R}^n)$ , então, para qualquer  $t \in [t_0, t_0 + A]$ , a notação  $x_t$  representa a função de  $[-r, 0]$  em  $\mathbb{R}^n$  definida por

$$x_t(\theta) = x(t + \theta), \quad -r \leq \theta \leq 0.$$

No que segue, denotaremos o espaço  $C([-r, 0], \mathbb{R}^n)$  por  $C$ .

**Definição 2.1.** Seja  $f: \mathbb{R} \times C \rightarrow \mathbb{R}^n$  uma aplicação. A equação

$$\dot{x}(t) = f(t, x_t) \tag{2.1}$$

é chamada uma equação diferencial funcional de primeira ordem com retardamento.

Observamos que a equação (2.1) inclui equações diferenciais ordinárias, pois para  $r = 0$  temos  $\theta = 0$  e, portanto,  $x_t(\theta) = x_t(0) = x(t)$ , obtendo  $\dot{x}(t) = f(t, x(t))$ .

**Definição 2.2.** Dizemos que a equação (2.1) é *autônoma* se  $f(t, \phi) = g(\phi)$ , onde  $g$  não depende de  $t$ ; *linear* se  $f(t, \phi) = L(t)\phi + h(t)$ , onde  $L(t)$  é uma função linear; *linear homogênea* se  $h \equiv 0$  e *linear não-homogênea* se  $h \not\equiv 0$ .

**Definição 2.3.** Dizemos que uma aplicação  $x$  é solução da equação (2.1) em  $[t_0 - r, t_0 + A]$  se existem  $t_0 \in \mathbb{R}$  e  $A > 0$  tais que  $x \in C([t_0 - r, t_0 + A], \mathbb{R}^n)$ ,  $(t, x_t) \in \mathbb{R} \times C$  e  $x(t)$  satisfaz a equação (2.1) para  $t \in [t_0, t_0 + A]$ .

**Definição 2.4.** Sejam  $t_0 \in \mathbb{R}$  e  $\phi \in C$ , dizemos que  $x$  é solução da equação (2.1) com função inicial  $\phi$  em  $t_0$  se existe  $A > 0$  tal que  $x(t)$  é solução da equação (2.1) em  $[t_0 - r, t_0 + A]$  e  $x_{t_0} = \phi$ .

**Lema 2.5.** Se  $t_0 \in \mathbb{R}$ ,  $\phi \in C$  e  $f(t, \phi)$  é contínua, então encontrar uma solução da equação (2.1) com função inicial  $\phi$  em  $t_0$  é equivalente a resolver ao problema de valor inicial para a seguinte equação integral:

$$x_{t_0} = \phi \tag{2.2}$$

$$x(t) = \phi(0) + \int_{t_0}^t f(s, x_s) ds, \quad t \geq t_0. \tag{2.3}$$

**Lema 2.6.** Se  $x \in C([t_0 - r, t_0 + A], \mathbb{R}^n)$  então  $x_t$  é uma função contínua de  $t$  para  $t \in [t_0, t_0 + A]$ .

**Teorema 2.7.** (Teorema de Existência e Unicidade para EDFRs). Seja  $f(t, \phi)$  contínua e localmente lipschitziana com relação a  $\phi$  em  $\mathbb{R} \times C$ . Então, para qualquer  $t_0 > 0$  e  $\varphi \in C$ , existem  $A > 0$  e uma função  $x(t)$  definida em  $[t_0 - r, t_0 + A]$  que é solução da equação (2.1) com função inicial  $\varphi$  em  $t_0$ . Além do mais, esta solução é única.

### 3 Noções de Estabilidade

Seja  $f: C([-r, 0], \mathbb{R}^n) \times \mathbb{R} \rightarrow \mathbb{R}^n$  uma aplicação contínua. Consideremos a EDFR com retardamento

$$x'(t) = f(x_t, t). \tag{3.1}$$

Esta seção será dedicada a conceitos sobre estabilidade da solução trivial  $\bar{x} \equiv 0$  de (3.1). No que segue, suporemos que  $f(0, t) = 0$  para todo  $t \in \mathbb{R}$ , para que a função  $\bar{x} \equiv 0$  seja, de fato, uma solução de (3.1).

**Definição 3.1.** A solução trivial  $\bar{x} \equiv 0$  de (2.1) será dita

- (i) *Estável*, se para quaisquer  $\sigma \in \mathbb{R}$  e  $\varepsilon > 0$ , existir  $\delta = \delta(\varepsilon, \sigma) > 0$  tal que se  $x(\sigma, \phi, f)$  for uma solução de (2.1) tal que  $x_\sigma(\sigma, \phi, f) = \phi$  e

$$\|\phi\| < \delta,$$

então

$$\|x_t(\sigma, \phi, f)\| < \varepsilon, \quad t \geq \sigma.$$

- (ii) *Uniformemente estável*, se o número  $\delta$  no item (i) for independente de  $\sigma$ .
- (iii) *Assintoticamente estável*, se existir  $\delta_0 = \delta_0(\sigma) > 0$  e para todo  $\varepsilon > 0$ , existir  $T = T(\varepsilon) \geq 0$  tal que se  $x(\sigma, \phi, f)$  for uma solução de (2.1) tal que  $x_\sigma(\sigma, \phi, f) = \phi$  e

$$\|\phi\| < \delta_0,$$

então

$$\|x_t(\sigma, \phi, f)\| < \varepsilon, \quad t \geq \sigma + T.$$

- (iv) *Uniformemente assintoticamente estável*, se o número  $\delta$  no item (iii) for independente de  $\sigma$ .

**Observação 3.2.** Se  $y$  for uma solução qualquer da equação (2.1), então  $y$  será dita *estável*, se a solução nula da equação

$$z'(t) = f(z_t + y_t, t) - f(y_t, t). \quad (3.2)$$

for estável. Os outros conceitos de estabilidade para  $y(t)$  são definidos de forma análoga.

Nas duas seções seguintes apresentaremos resultados que garantem a estabilidade de EDRs sob certas condições, aplicando a teoria de ponto fixo. Em geral, seguimos um conjunto de passos que representa o caminho pelo qual a estabilidade da solução nula de uma equação diferencial funcional é estabelecida por meio da teoria de ponto fixo. Esse conjunto de passos é dado por:

1. Uma análise da equação diferencial revela que, para algum  $t_0$  dado, existe um intervalo inicial  $E_{t_0}$  e uma função inicial  $\psi : E_{t_0} \rightarrow \mathbb{R}^n$ . Em seguida, podemos determinar um conjunto de funções  $\mathcal{M}$  da seguinte forma:

$$\mathcal{M} = \{\phi : E_{t_0} \cup [t_0, \infty) \rightarrow \mathbb{R}^n : \phi(t) = \psi(t), t \in E_{t_0}\},$$

que abrigaria soluções aceitáveis da equação. Em geral, isso significa que nós poderíamos exigir que se  $\phi \in \mathcal{M}$ , então  $\phi$  é limitada e  $\phi(t) \rightarrow 0$  quando  $t \rightarrow \infty$ .

2. Para resolver  $\dot{x} = f(t, x_t)$ , obtemos uma equação integral do tipo

$$x(t) = a(t) + \int_{t_0}^t G(t, s, x(\cdot), \psi) ds,$$

onde  $a : [t_0, \infty) \rightarrow \mathbb{R}^n$  e  $G(t, s, \varphi(\cdot), \psi)$  dependem de  $t, s, \varphi$ , e  $\psi$ .

Definimos a aplicação  $P : \mathcal{M} \rightarrow \mathcal{M}$  como:

$$(P\varphi)(t) = \psi(t) \text{ em } E_{t_0},$$

e

$$(P\varphi)(t) = a(t) + \int_{t_0}^t G(t, s, \varphi(\cdot), \psi) ds \text{ para } t \geq t_0.$$

Um ponto fixo de  $P$  resolve o problema de valor inicial  $\dot{x} = f(t, x_t)$  e  $x(t) = \psi(t)$  em  $E_{t_0}$ .

3. Finalmente, escolhemos um teorema de ponto fixo adequado, que mostrará que a aplicação  $P$  possui um ponto fixo em  $\mathcal{M}$ . Este ponto fixo será a solução aceitável para a equação analisada.

#### 4 Estabilidade via Teorema do Ponto Fixo de Banach

Nesta seção apresentaremos o Teorema do Ponto Fixo de Banach e o aplicaremos para obter resultados sobre estabilidade de EDFRs. Consideremos a seguinte equação diferencial com retardamento

$$\dot{x}(t) = -ax(t) + bx(t-r), \quad t \geq 0, \quad (4.1)$$

onde  $a, b$  são constantes positivas e  $r \geq 0$ .

**Teorema 4.1** (Teorema do Ponto Fixo de Banach). *Seja  $(S, \rho)$  um espaço métrico completo e considere  $P: S \rightarrow S$  uma aplicação. Se  $P: S \rightarrow S$  é uma contração, isto é, se existe uma constante  $0 \leq \alpha < 1$  tal que, para cada par  $\phi_1, \phi_2 \in S$ ,  $\rho(P\phi_1, P\phi_2) \leq \alpha\rho(\phi_1, \phi_2)$  então  $P$  admitirá um único ponto fixo  $\phi \in S$ , ou seja, existirá um único  $\phi \in S$  tal que  $P\phi = \phi$ .*

*Demonstração.* Para  $\phi_0 \in S$  tomado arbitrariamente vamos definir a sequência  $(\phi_n)_{n \in \mathbb{N}} \subset S$  pela iteração:

$$\phi_0, \phi_1 = P\phi_0, \phi_2 = P\phi_1 = P^2\phi_0, \dots, \phi_n = P^n\phi_0.$$

Note que,

$$\begin{aligned} \rho(\phi_{m+1}, \phi_m) &= \rho(P\phi_m, P\phi_{m-1}) \\ &\leq \alpha\rho(\phi_m, \phi_{m-1}) \\ &= \alpha\rho(P\phi_{m-1}, P\phi_{m-2}) \\ &\leq \alpha^2\rho(\phi_{m-1}, \phi_{m-2}) \\ &= \alpha^2\rho(P\phi_{m-2}, P\phi_{m-3}) \\ &\vdots \\ &\leq \alpha^m\rho(\phi_1, \phi_0). \end{aligned}$$

Pela Desigualdade Triangular e pela fórmula da soma dos termos de uma progressão geométrica, obtemos, para  $n > m$ ,

$$\begin{aligned} \rho(\phi_m, \phi_n) &\leq \rho(\phi_m, \phi_{m+1}) + \rho(\phi_{m+1}, \phi_{m+2}) + \dots + \rho(\phi_{n-1}, \phi_n) \\ &\leq (\alpha^m + \alpha^{m+1} + \dots + \alpha^{n-1})\rho(\phi_0, \phi_1) \\ &= \alpha^m \frac{1 - \alpha^{n-m}}{1 - \alpha} \rho(\phi_0, \phi_1). \end{aligned}$$

Como  $0 < \alpha < 1$ , temos que  $1 - \alpha^{n-m} < 1$ . Logo,

$$\rho(\phi_m, \phi_n) \leq \frac{\alpha^m}{1 - \alpha} \rho(\phi_0, \phi_1).$$

Assim, para  $m$  suficientemente grande podemos tornar o lado direito dessa desigualdade tão pequeno quanto se queira. Portanto,  $(\phi_n)_{n \in \mathbb{N}}$  é uma sequência de Cauchy e, como  $S$  é completo, concluímos que  $\phi_n \rightarrow \phi$  quando  $n \rightarrow \infty$ , para algum  $\phi \in S$ .

Agora, pela Desigualdade Triangular e pelo fato de  $P$  ser uma contração (e, portanto, uma aplicação contínua), segue que

$$\rho(\phi, P\phi) \leq \rho(\phi, \phi_m) + \rho(\phi_m, P\phi) = \rho(\phi, \phi_m) + \rho(P\phi_{m-1}, P\phi) \leq \rho(\phi, \phi_m) + \alpha\rho(\phi_{m-1}, \phi),$$

ou seja,

$$\rho(\phi, P\phi) \leq \rho(\phi, \phi_m) + \alpha\rho(\phi_{m-1}, \phi).$$

Como  $\phi_m \rightarrow \phi$  quando  $m \rightarrow \infty$ , o lado direito dessa última desigualdade fica tão pequeno quanto se queira e isso nos mostra que  $P\phi = \phi$ , isto é,  $\phi$  é um ponto fixo de  $P$ .

Por fim, vamos supor que existam  $\phi_1$  e  $\phi_2$  em  $(S, \rho)$  tais que  $P\phi_1 = \phi_1$  e  $P\phi_2 = \phi_2$ . Então, temos que  $\rho(\phi_1, \phi_2) = \rho(P\phi_1, P\phi_2) \leq \alpha\rho(\phi_1, \phi_2)$ , de onde concluímos que  $\rho(\phi_1, \phi_2) = 0$ , pois  $\alpha < 1$ . Portanto,  $\phi_1 = \phi_2$  e a prova está completa. ■

Para estudar a estabilidade da solução nula da equação (4.1) usando o Teorema 4.1, precisaremos garantir que o espaço métrico das funções contínuas e limitadas  $f: [-r, \infty) \rightarrow \mathbb{R}$ , equipado com a métrica do supremo, é completo. Faremos isso a seguir.

**Proposição 4.2.** *Seja  $(S, \rho)$  o espaço métrico das funções contínuas e limitadas  $f: [-r, \infty) \rightarrow \mathbb{R}$  com a métrica do supremo,*

$$\rho(f, g) = \sup_{t \in [-r, \infty)} |f(t) - g(t)|, \text{ com } f, g \in S, \quad (4.2)$$

e  $d(x, y) = |x - y|$  é uma métrica em  $\mathbb{R}$ . Então,  $(S, \rho)$  é completo.

*Demonstração.* Seja  $(f_n)_{n \in \mathbb{N}} \subset (S, \rho)$  uma sequência de Cauchy. Então, para todo  $\varepsilon > 0$ , existe  $N \in \mathbb{N}$  tal que se  $m, n > N$  tem-se

$$\sup_{t \in [-r, \infty)} |f_n(t) - f_m(t)| \leq \frac{\varepsilon}{2}.$$

Em particular, para cada  $t_0 \in \mathbb{R}$ ,  $(f_n(t_0))_{n \in \mathbb{N}}$  é uma sequência de Cauchy em  $\mathbb{R}$  e como  $\mathbb{R}$  é completo,  $(f_n(t_0))_{n \in \mathbb{N}}$  tem um limite em  $\mathbb{R}$ , o qual denotaremos por  $f(t_0)$ . Para todo  $m \in \mathbb{N}$ , temos

$$|f(t_0) - f_m(t_0)| = \lim_{n \rightarrow \infty} |f_n(t_0) - f_m(t_0)| \leq \frac{\varepsilon}{2} < \varepsilon,$$

e, portanto, a convergência da sequência  $(f_n)_{n \in \mathbb{N}}$  para a função  $f$  é uniforme, uma vez que  $t_0 \in \mathbb{R}$  é arbitrário. Consequentemente,  $f: [-r, \infty) \rightarrow \mathbb{R}$  é contínua, pois todas as funções  $f_n$  da sequência o são. Observe, agora, que

$$\sup_{t \in [-r, \infty)} |f(t)| \leq \sup_{t \in [-r, \infty)} |f(t) - f_{n_0}(t)| + \sup_{t \in [-r, \infty)} |f_{n_0}(t)|,$$

para algum  $n_0 \in \mathbb{N}$  suficientemente grande.

Como  $f_{n_0} \in (S, \rho)$ , segue que  $\sup_{t \in [-r, \infty)} |f_{n_0}(t)| \leq K_1$  para algum  $K_1 > 0$ . Além disso, como  $\rho(f, f_n) \rightarrow 0$  se  $n \rightarrow \infty$ , temos que  $\sup_{t \in [-r, \infty)} |f(t) - f_{n_0}(t)| \leq K_2$  para algum  $K_2 > 0$ . Logo,

$$\sup_{t \in [-r, \infty)} |f(t)| \leq K_1 + K_2,$$

de onde segue que  $f \in (S, \rho)$ , garantindo que o espaço  $(S, \rho)$  é completo. ■

Cabe lembrar que todo espaço normado  $(M, \|\cdot\|)$  é um espaço métrico, com a métrica induzida pela norma:  $\rho(x, y) = \|x - y\|$ , para  $x, y \in M$ . Portanto, pela Proposição 4.2, podemos inferir que o espaço normado das funções contínuas e limitadas  $f: [-r, \infty) \rightarrow \mathbb{R}$ , com a norma do supremo, é um espaço métrico completo, com a métrica dada em (4.2).

**Teorema 4.3.** *Se  $a > 0$  e  $|b| < a$ , então a solução nula da equação (4.1) é uniformemente assintoticamente estável para  $r \geq 0$ .*

*Demonstração.* Sejam  $\psi: [-r, 0] \rightarrow \mathbb{R}$  uma função inicial contínua e  $(M, \|\cdot\|)$  o espaço de Banach das aplicações contínuas e limitadas  $\phi: [-r, \infty) \rightarrow \mathbb{R}$ , com a norma do supremo (induzida pela métrica do supremo vista na Proposição 4.2). Consideremos o seguinte conjunto:

$$S = \{\phi \in M: \phi(t) = \psi(t) \text{ para } t \in [-r, 0], \text{ e } \phi \rightarrow 0 \text{ quando } t \rightarrow \infty\}.$$

Com a norma do supremo, pela Proposição 4.2, podemos inferir que  $S$  é completo. Reescrevendo (4.1) pela fórmula da variação dos parâmetros, obtemos

$$x(t) = \psi(0)e^{-at} + \int_0^t e^{-a(t-s)}bx(s-r)ds, \quad t > 0.$$

Seja  $P: S \rightarrow M$  a aplicação definida por

$$P(\phi)(t) = \begin{cases} \psi(t), & \text{se } -r \leq t \leq 0, \\ \psi(0)e^{-at} + \int_0^t e^{-a(t-s)}b\phi(s-r)ds, & \text{se } t > 0. \end{cases}$$

Note que  $P(S) \subset S$ . De fato, seja  $\phi \in S$ . Dado  $\varepsilon > 0$ , como  $\phi \rightarrow 0$  quando  $t \rightarrow \infty$ , existe  $t_1 > 0$  tal que  $|\phi(t-r)| < \varepsilon/2$  para  $t > t_1$ . E como  $e^{-at} \rightarrow 0$  quando  $t \rightarrow \infty$ , existe  $t_2 > t_1$  tal que  $|\psi(0)e^{-at}| < \varepsilon/2$ , se  $t > t_2$ . Portanto, para  $t > t_2$ , temos

$$\begin{aligned} |P(\phi)(t)| &\leq |\psi(0)e^{-at}| + \left| \int_0^t e^{-a(t-s)}b\phi(s-r) ds \right| \\ &< \frac{\varepsilon}{2} + \int_0^t e^{-a(t-s)}|b|\frac{\varepsilon}{2} ds \\ &= \frac{\varepsilon}{2} + \frac{\varepsilon}{2}|b|\frac{1}{a} [1 - e^{-at}] \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \left[ \frac{|b|}{a} \right] \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon, \end{aligned}$$

visto que  $1 - e^{-at} < 1$  (para  $t > 0$ ) e  $|b| < a$ . Então,  $P(\phi) \in S$ , pois  $P(\phi)$  é limitada,  $P(\phi)(t) = \psi(t)$  para  $-r \leq t \leq 0$  e  $P(\phi)(t) \rightarrow 0$  quando  $t \rightarrow \infty$ .

Agora, se  $\phi, \eta \in S$ , então

$$|(P\phi)(t) - (P\eta)(t)| \leq \|\phi - \eta\| \int_0^t |b|e^{-a(t-s)}ds \leq \|\phi - \eta\| \frac{|b|}{a},$$

para qualquer  $t > 0$ . Portanto,  $P$  é uma contração, dado que  $|b| < a$ . Pelo Teorema do Ponto Fixo da Contração (Teorema 4.1),  $P$  possui um único ponto fixo  $\phi$  em  $S$ , tal que  $\phi(t) \rightarrow 0$  quando  $t \rightarrow \infty$ . Por fim,

$$\|\phi\| \leq \|\psi\| + \frac{|b|}{a}\|\phi\| \implies \|\phi\| \leq \frac{\|\psi\|}{1 - \frac{|b|}{a}}.$$

Assim, dado  $\varepsilon > 0$ , tomando  $\delta = \varepsilon \left(1 - \frac{|b|}{a}\right)$ , segue a estabilidade uniforme e a estabilidade assintótica de  $x = 0$ . ■

**Exemplo 4.4.** Pelo Teorema 4.3, temos que a solução nula de  $\dot{x}(t) = -3x(t) - 2x(t-1)$ ,  $t > 0$ , é uniformemente assintoticamente estável, uma vez que  $|b| = 2 < a = 3$  e  $a = 3 > 0$ .



## 5 Estabilidade via Teorema do Ponto Fixo de Schauder

Sejam  $C = C([-r, 0], \mathbb{R})$  e  $\mathbb{R}^+ = \{x \in \mathbb{R} : x \geq 0\}$ . Nesta seção, vamos estudar a estabilidade da equação

$$\dot{x}(t) = -a(t, x_t)x(t) + f(t, x_t) \quad (5.1)$$

onde  $a, f: \mathbb{R}^+ \times C \rightarrow \mathbb{R}$  são funções contínuas, utilizando o Teorema do Ponto Fixo de Schauder, demonstrado na sequência.

**Teorema 5.1** (Teorema do Ponto Fixo de Schauder). *Sejam  $(X, \|\cdot\|)$  um espaço de Banach e  $S \subset X$  um conjunto compacto e convexo. Se  $f: S \rightarrow S$  é uma função contínua, então  $f$  possui pelo menos um ponto fixo.*

*Demonstração.* Dado  $\varepsilon > 0$ , temos que  $\bigcup_{x \in S} B(x, \varepsilon)$  é uma cobertura por abertos de  $S$ . Como

$S$  é compacto, existem  $x_1, x_2, \dots, x_n \in S$  tais que  $S \subset \bigcup_{i=1}^n B(x_i, \varepsilon)$ . Vamos definir  $g: S \rightarrow S$  por

$$g(x) = \frac{\sum_{i=1}^n m_i(x)x_i}{\sum_{i=1}^n m_i(x)},$$

onde  $m_i: S \rightarrow \mathbb{R}$  é definida por

$$m_i(x) = \begin{cases} \varepsilon - \|x - x_i\|, & \text{se } \|x - x_i\| < \varepsilon, \\ 0, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases}$$

Note que  $g$  está bem definida, pois se  $\sum_{i=1}^n m_i(x^*) = 0$  para algum  $x^* \in S$ , o fato de  $m_i(x) \geq 0$  para todo  $x$  implica que  $m_i(x^*) = 0$  para todo  $i$ . Pela definição de  $m_i$ , temos que  $\|x^* - x_i\| \geq \varepsilon$  e, portanto,  $x^* \notin \bigcup_{i=1}^n B(x_i, \varepsilon) \supset S$ , o que é absurdo, visto que  $x^* \in S$ .

Para mostrar que  $g$  é contínua, basta mostrar que  $m_i$  é contínua para todo  $i$ . Dado  $a \in S$ , mostremos que  $m_i$  é contínua em  $a$ . De fato, dado  $\varepsilon > 0$ , se  $\|a - x_i\| \geq \varepsilon$ , então  $m_i(a) = 0$ . Portanto, para todo  $\delta > 0$ , se  $\|x - a\| < \delta$ , então  $\|m_i(x) - m_i(a)\| = \|m_i(x)\| < \varepsilon$ , pois  $m_i(x) = \varepsilon - \|x - x_i\| < \varepsilon$ .

Suponha que  $\|a - x_i\| < \varepsilon$ . Tomando  $\delta < \varepsilon$ , temos que se  $\|x - a\| < \delta$  então

$$\begin{aligned} |m_i(x) - m_i(a)| &= \begin{cases} |\varepsilon - \|x - x_i\| - (\varepsilon - \|a - x_i\|)|, & \text{se } \|x - x_i\| < \varepsilon, \\ |m_i(a)|, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \\ &= \begin{cases} |-\|x - x_i\| + \|a - x_i\||, & \text{se } \|x - x_i\| < \varepsilon, \\ |m_i(a)|, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \\ &\leq \begin{cases} \|a - x_i - (x - x_i)\|, & \text{se } \|x - x_i\| < \varepsilon, \\ |m_i(a)|, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \\ &= \begin{cases} \|x - a\|, & \text{se } \|x - x_i\| < \varepsilon, \\ |m_i(a)|, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \\ &< \begin{cases} \delta, & \text{se } \|x - x_i\| < \varepsilon, \\ |m_i(a)|, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \\ &< \begin{cases} \varepsilon, & \text{se } \|x - x_i\| < \varepsilon, \\ \varepsilon, & \text{se } \|x - x_i\| \geq \varepsilon. \end{cases} \end{aligned}$$

Portanto,  $|m_i(x) - m_i(a)| < \varepsilon$  se  $\|x - a\| < \delta$ . Como  $a$  foi tomado arbitrariamente em  $S$ , obtemos a continuidade de  $m_i$  em  $S$  e, por conseguinte, a de  $g$ . Note também que, para todo  $x \in S$ , tem-se

$$\|g(x) - x\| = \left\| \frac{\sum_{i=1}^n m_i(x)(x_i - x)}{\sum_{i=1}^n m_i(x)} \right\| \leq \left| \frac{\sum_{i=1}^n m_i(x)}{\sum_{i=1}^n m_i(x)} \right| = \varepsilon. \quad (5.2)$$

Seja  $S_n$  a envoltória complexa de  $\{x_1, \dots, x_n\}$ . Vamos definir, para cada  $n \in \mathbb{N}$ , a aplicação  $g \circ f: S_n \rightarrow S_n$ . Mostremos que  $g \circ f$  tem um ponto fixo.

É sabido que  $S_n$  é homeomorfo a um subconjunto compacto e convexo de  $\mathbb{R}^n$ , que denotaremos por  $K$ . Seja  $h: K \rightarrow S_n$  tal homeomorfismo entre  $K$  e  $S_n$ .

Defina  $F: K \rightarrow K$  por  $F = h^{-1} \circ (g \circ f) \circ h$ . Temos que  $F$  é contínua e pelo Teorema do Ponto Fixo de Brouwer<sup>††</sup>,  $F$  tem um ponto fixo  $x^*$  em  $K$ . Agora, veja que  $h(x^*)$  é ponto fixo de  $g \circ f$ . Com efeito, pela definição de  $F$ , temos que  $g \circ f = h \circ F \circ h^{-1}$  e, conseqüentemente,

$$\begin{aligned} g \circ f(h(x^*)) &= h \circ F \circ h^{-1} \circ (h(x^*)) \\ &= h \circ F(x^*) \\ &= h(x^*). \end{aligned}$$

Portanto, para cada  $n \in \mathbb{N}$ , a aplicação  $g \circ f: S_n \rightarrow S_n$  possui um ponto fixo, que denotaremos por  $p_0^n$ . Considere a seqüência de pontos fixos  $(p_0^n)_{n \in \mathbb{N}}$  de  $g \circ f$ . Como a seqüência  $(p_0^n)_{n \in \mathbb{N}}$  está contido em  $S$  e  $S$  é compacto, existe uma subseqüência  $(p_0^{n'})_{n' \in \mathbb{N}}$  de  $(p_0^n)_{n \in \mathbb{N}}$  tal que  $p_0^{n'} \rightarrow p_0 \in S$  quando  $n' \rightarrow \infty$ .

Ademais, como  $p_0^{n'} = g \circ f(p_0^{n'})$  para todo  $n' \in \mathbb{N}'$ , obtemos

$$\begin{aligned} \|p_0^{n'} - f(p_0^{n'})\| &= \|p_0^{n'} - g \circ f(p_0^{n'}) + g \circ f(p_0^{n'}) - f(p_0^{n'})\| \\ &\leq \|p_0^{n'} - g \circ f(p_0^{n'})\| + \|g \circ f(p_0^{n'}) - f(p_0^{n'})\| \\ &= \|g \circ f(p_0^{n'}) - f(p_0^{n'})\| \\ &\leq \varepsilon, \end{aligned}$$

onde a última desigualdade se deve a (5.2).

Portanto,  $\lim_{n' \rightarrow \infty} \|p_0^{n'} - f(p_0^{n'})\| \leq \varepsilon$ . Da convergência de  $(p_0^{n'})_{n' \in \mathbb{N}}$  e da continuidade de  $f$ , obtemos  $\|p_0 - f(p_0)\| \leq \varepsilon$  para todo  $\varepsilon > 0$ , de onde concluímos que  $f(p_0) = p_0$ , ou seja,  $f$  tem um ponto fixo em  $S$ , conforme queríamos demonstrar. ■

A demonstração do próximo resultado será omitida aqui, mas pode ser encontrada em [5, Teorema 2.32]. Cabe mencionar que  $C(\mathbb{R}, \mathbb{R}^+)$  denotará o espaço vetorial das funções contínuas  $x: \mathbb{R} \rightarrow \mathbb{R}^+$ .

**Teorema 5.2.** *Suponha que existem funções contínuas  $a_1, a_2 \in C(\mathbb{R}, \mathbb{R})$  tais que*

$$a_1(t) \leq a(t, x_t) \leq a_2(t).$$

*Além disso, vamos considerar satisfeitas as seguintes condições:*

(H<sub>1</sub>)  $f(t, 0) = 0$ , *existem uma constante positiva  $L$  e uma função contínua  $b_1: \mathbb{R} \rightarrow \mathbb{R}^+$  tais que*

$$|f(t, \phi) - f(t, \psi)| \leq b_1 |\phi - \psi|,$$

<sup>††</sup>**Teorema do Ponto Fixo de Brouwer.** Seja  $X \subset \mathbb{R}^n$  um conjunto não vazio, compacto e convexo. Se  $f: X \rightarrow X$  é uma função contínua, então  $f$  tem um ponto fixo.

para  $\phi, \psi \in C_L = \{x \in C(\mathbb{R}, \mathbb{R}^+): \|x\| \leq L\}$ .

Existe uma função  $b_2 \in C(\mathbb{R}, \mathbb{R})$  tal que

$$(H_2) \quad |f(t, x_t)| \leq |b_2(t)||x(t)|, \text{ para } t > 0 \text{ e } x \in C;$$

$$(H_3) \quad \lim_{t \rightarrow \infty} \int_0^t (a(s) - |b_2(s)|) ds = \infty.$$

Então, a solução nula de (5.1) é assintoticamente estável.

A demonstração do próximo resultado segue diretamente do Teorema 5.2 e também pode ser encontrada em [5] (veja o Corolário 2.34).

**Corolário 5.3.** *Considere a generalização do modelo proposto por Mackey e Glass para o processo de Hematopoiese, isto é, a produção de células sanguíneas na medula óssea:*

$$\dot{x}(t) = -a(t)x(t) + \frac{b(t)\theta^n x(t - r(t))}{\theta^n + x^n(t - r(t))}, \quad (5.3)$$

em que  $a, b, r \in C(\mathbb{R}, \mathbb{R}^+)$ ,  $\theta$  é uma constante positiva e  $n$  é um inteiro positivo dado. Em (5.3),  $r$  representa o tempo entre a produção de células imaturas na medula óssea e sua maturação quando é lançada na corrente sanguínea, por fim  $x(t)$  denota a densidade de células maduras na corrente sanguínea no tempo  $t$ .

Se  $\lim_{t \rightarrow \infty} \int_0^t (a(s) - b(s)) ds = \infty$ , então a solução nula de (5.3) é assintoticamente estável.

## 6 Considerações Finais

O estudo qualitativo das EDRs é essencial porque nos oferece uma visão clara de como os sistemas com retardamento se comportam. Ele também ajuda a escolher as ferramentas matemáticas mais adequadas para lidar com a complexidade dessas equações. O uso de teoremas de ponto fixo é uma forma eficaz para identificar condições de estabilidade e entender a dinâmica dos sistemas com atrasos temporais.

Além dos teoremas de ponto fixo de Banach e Schauder, que utilizamos para estabelecer condições de estabilidade, cabe destacar a existência de outros teoremas importantes, como o Teorema do Ponto Fixo de Krasnoselskii. Esse teorema, que combina aspectos dos teoremas de Banach e Schauder, também é útil para analisar a estabilidade das soluções e pode ampliar nossa compreensão acerca desses sistemas.

**Agradecimentos:** Agradeço à Profa. Dra. Suzete Maria Silva Afonso, pela orientação e incentivo durante a realização deste trabalho e à FAPESP pelo apoio financeiro.

*Abstract: This work aims to present a powerful tool for the qualitative analysis of delay differential equations: Fixed Point Theorems. By using the Banach and Schauder Fixed Point Theorems, we will obtain results that ensure the stability of solutions to delay differential equations.*

*Keywords: delay differential equations; stability; Banach fixed point theorem; Schauder fixed point theorem.*

## Referências Bibliográficas

- [1] J. K. Hale; S. M. V. Lunel. *Introduction to Functional Differential Equations*, volume 99 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 1993.

- [2] K. Gopalsamy. *Stability and Oscillations in Delay Differential Equations of Population Dynamics*. Mathematics and Its Applications. Springer Netherlands, 1992.
- [3] Y. Kuang. *Delay Differential Equations: With Applications in Population Dynamics*. Mathematics in Science and Engineering. Elsevier Science, 1993.
- [4] T. A. Burton. *Stability by fixed point theory for functional differential equations*. Dover Publications, Inc., Mineola, NY, 2006.
- [5] R. Lima. *Estabilidade de equações diferenciais funcionais com retardamento via teoria de pontos fixos*. Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto. 107 p. 2019.

# A integral de Kurzweil para a caracterização de equações diferenciais ordinárias generalizadas

Wellington Moisés de Oliveira<sup>†</sup>

Orientador(a): Profa. Dra. Suzete Maria Silva Afonso

**Resumo:** A partir do interesse em estudar equações diferenciais ordinárias, muitos pesquisadores contribuíram para o campo da teoria de integração. Nomes como Riemann, Lebesgue, Perron, Henstock e Kurzweil possuem muitas contribuições para a área. Mais especificamente, para a caracterização e estudo das equações diferenciais ordinárias generalizadas, precisamos trabalhar com as integrais de Kurzweil. Para apresentar esta integral, partiremos da construção familiar da integral de Riemann e buscaremos refinar alguns conceitos que estimam a soma de Riemann para caracterizar a integral de Kurzweil. Apresentaremos, também, resultados importantes como a existência e unicidade desta integral e algumas propriedades dessa nova ferramenta. Finalizaremos apresentando o conceito de equação diferencial ordinária generalizada e explorando algumas de suas propriedades iniciais, que são base para a construção de resultados mais gerais na teoria de equações diferenciais.

**Palavras-chave:** Integral de Riemann; Integral de Kurzweil; Equações diferenciais ordinárias generalizadas

## 1 Introdução

Este artigo tem como objetivo fundamentar a teoria das equações diferenciais ordinárias generalizadas (EDOs generalizadas). Mais especificamente, definiremos a integral de Kurzweil para poder apresentar as EDOs generalizadas e, por fim, exploraremos algumas de suas propriedades básicas.

Uma das principais motivações para estudar as EDOs generalizadas deve-se ao fato de que é possível obter resultados bastante gerais concernentes a propriedades qualitativas de suas soluções e traduzi-los para as teorias dos outros tipos de equações diferenciais por meio das correspondências que existem entre elas.

O artigo irá se estruturar de forma que contemple as discussões de dois grandes tópicos, a citar:

- (I) Revisão de conceitos e teoria básica necessária de Análise Real e Espaços Métricos para compreender a definição e as propriedades fundamentais da integral de Kurzweil;
- (II) Estudo da teoria básica de EDOs generalizadas: existência, unicidade e dependência contínua das soluções;

Em busca de situar nosso trabalho, iniciaremos com uma breve contextualização histórica acerca das integrais de Riemann, de Lebesgue e de Perron, apresentando um exemplo que contribuirá para compreendermos a importância da construção das integrais de Kurzweil.

Então, a partir de sua definição, exploraremos algumas propriedades sobre essa ferramenta.

<sup>†</sup>Bolsista: Fundação de Amparo à Pesquisa do Estado de São Paulo. Processo: 2023/10170-2

Por fim, caracterizaremos as EDOs generalizadas, apresentando alguns de seus resultados iniciais, que servem de base para a construção das correspondências entre as EDOs generalizadas e os outros tipos de equações diferenciais.

## 2 Panorama histórico

Esta seção foi elaborada com o auxílio das referências [3] e [4].

### 2.1 As integrais de Riemann e Lebesgue

A integral de Riemann, definida por Bernhard Riemann em 1854, é uma ferramenta clássica usada na resolução de muitos problemas matemáticos até hoje, uma vez que se relaciona com taxas de variações, sendo essencial para os estudos de diferenciabilidade contínua. Justamente por este fato, no final do século XIX, matemáticos constataram algumas desvantagens ao se trabalhar com a integral de Riemann ou, simplesmente, a R-integral.

Quando estudamos uma função não-limitada em algum intervalo da reta, percebemos que ela não é R-integrável, ou ainda, no Teorema Fundamental do Cálculo faz-se necessário a continuidade de uma função para que sua derivada seja R-integrável.

Contudo, 50 anos depois, Henri Léon Lebesgue generalizou o conceito de integral de Riemann de modo que a integral de Lebesgue apresentasse diversas vantagens em relação à integral de Riemann, sobretudo em relação aos cálculos envolvendo limites. Um dos principais ganhos, e de nosso interesse, é que no Teorema Fundamental do Cálculo para integral de Lebesgue, garantimos que a derivada de uma função é Lebesgue integrável se ela for absolutamente contínua.

### 2.2 A integral de Kurzweil

Os principais resultados do estudo de integrais não-absolutamente convergentes foram desenvolvidas independentemente tanto por Jaroslav Kurzweil, em 1957, quanto por Ralph Henstock, em 1961, cerca de 50 anos depois das publicações de Lebesgue.

Em 1957, Jaroslav Kurzweil obteve um novo conceito de integração baseado nas ideias de Riemann, que generaliza as integrais de Riemann e Lebesgue. A integral de Kurzweil ou K-integral, como é conhecida, é definida para funções de duas variáveis e surgiu com o intuito de solucionar algumas dificuldades encontradas na teoria de EDOs, envolvendo, por exemplo, funções oscilatórias, descontínuas ou funções que não são de variação limitada.

Em 1961, Ralph Henstock desenvolveu o mesmo conceito que Kurzweil, mas para funções de uma variável.

Como a integral de Kurzweil engloba a de Henstock, encontramos em algumas referências o nome de integral de Henstock-Kurzweil ou HK-integral para o conceito que exploraremos, uma vez que eles trabalharam independentemente um do outro, numa época de divulgação científica restrita.

Neste trabalho, por seguirmos as notações de Kurzweil, manteremos somente o seu nome, por simplicidade.

A integral de Kurzweil, que generaliza o conceito de integral de Riemann para que toda derivada de uma função seja integrável, será nosso foco principal, uma vez que, a fim de explorar importantes características de EDOs generalizadas como a existência e unicidade de suas soluções e suas propriedades qualitativas, termos a garantia de que podemos trabalhar com as integrais do processo é muito importante.

Isto posto, primeiro, revisitaremos um pouco a ideia da integral de Riemann.

### 3 A integral de Riemann

Por ser vista em qualquer curso de cálculo diferencial e integral, bem como em cursos de análise real, a integral de Riemann é amplamente conhecida na comunidade matemática, tendo suma importância para nossa formação e em nossas práticas.

Contudo, como ela não é nosso foco, apenas enunciaremos a sua definição e qual é a condição para que uma função seja R-integrável, a seguir, apresentaremos um exemplo de função que não é Riemann integrável no intervalo  $[0, 1]$  da reta real, indicando nossa necessidade em buscar algo mais geral e que garanta a integrabilidade de mais casos.

Para a elaboração desta seção, utilizamos, principalmente, [2].

#### 3.1 Definição da integral de Riemann

**Definição 3.1.** Seja  $[a, b] \subset \mathbb{R}$ . Uma *partição* de  $[a, b]$  é um conjunto finito de pontos  $\mathcal{P} = \{x_0, x_1, \dots, x_n\}$  tal que  $x_0 = a$ ,  $x_n = b$  e  $x_{i-1} < x_i$  para  $i = 1, \dots, n$ . Para cada subintervalo  $[x_{i-1}, x_i]$  definimos que o tamanho  $l$  do subintervalo é  $l([x_{i-1}, x_i]) = x_i - x_{i-1}$ . A *norma* ou *métrica*  $\mu$  da partição será o maior subintervalo, ou seja,  $[x_{i-1}, x_i]$

$$\mu(\mathcal{P}) = \max\{x_i - x_{i-1} : i = 1, \dots, n\}.$$

Dessa forma, os pontos  $\{x_0, x_1, \dots, x_n\}$  formam uma sequência crescente de números em  $[a, b]$  que o divide em subintervalos contínuos.

Sejam  $f : [a, b] \rightarrow \mathbb{R}$ ,  $\mathcal{P} = \{x_0, x_1, \dots, x_n\}$  uma partição  $[a, b]$  e  $t_i \in [x_{i-1}, x_i]$  para cada  $i$ . Consideraremos

$$S(f, \mathcal{P}, \{t_i\}_{i=1}^n) = \sum_{i=1}^n f(t_i)(x_i - x_{i-1})$$

como a aproximação da soma de Riemann com respeito a partição  $\mathcal{P}$  e o conjunto de pontos  $\{t_i\}_{i=1}^n$ .

A integral de Riemann de uma função  $f$  sobre  $[a, b]$  será o limite da soma  $S(f, \mathcal{P}, \{t_i\}_{i=1}^n)$  quando a norma da partição tende a 0.

**Definição 3.2.** Uma função  $f : [a, b] \rightarrow \mathbb{R}$  é Riemann integrável sobre  $[a, b]$  se há um  $I \in \mathbb{R}$  tal que para todo  $\varepsilon > 0$  existe um  $\delta > 0$  para que, se  $\mathcal{P}$  é uma partição qualquer de  $[a, b]$  com  $\mu(\mathcal{P}) < \delta$  e  $t_i \in [x_{i-1}, x_i]$  para todo  $i$ , então

$$|S(f, \mathcal{P}, \{t_i\}_{i=1}^n) - I| < \varepsilon.$$

Denotamos por

$$I = \int_a^b f = \int_a^b f(t) dt$$

a integral de  $f$ , em relação à partição  $\mathcal{P}$ , sobre o intervalo  $[a, b]$ .

#### 3.2 Uma função que não é Riemann integrável

Vejamos, então, um exemplo de função que não é R-integrável em um intervalo da reta.

**Exemplo 3.3.** Sejam  $f : [0, 1] \rightarrow \mathbb{R}$

$$f(x) = \begin{cases} 1, & \text{se } x \in \mathbb{Q} \cap [0, 1], \\ 0, & \text{se } x \notin \mathbb{Q} \cap [0, 1] \end{cases}$$

a função de Dirichlet e  $\mathcal{P} = \{x_0, x_1, \dots, x_n\}$  uma partição arbitrária de  $[0, 1]$ .

Para todo subintervalo produzido pela partição, podemos afirmar que existe um número racional  $r_i$  e um número irracional  $q_i$ . Assim,

$$\begin{aligned} S(f, \mathcal{P}, \{r_i\}_{i=1}^n) &= \sum_{i=1}^n f(r_i)(x_i - x_{i-1}) \\ &= \sum_{i=1}^n x_i - x_{i-1} \\ &= x_n - x_0 = 1 - 0 = 1 \end{aligned}$$

enquanto,

$$\begin{aligned} S(f, \mathcal{P}, \{q_i\}_{i=1}^n) &= \sum_{i=1}^n f(q_i)(x_i - x_{i-1}) \\ &= \sum_{i=1}^n 0(x_i - x_{i-1}) = 0. \end{aligned}$$

Agora, vamos supor que  $f$  seja Riemann integrável e com integral  $I$ .

Se fixarmos  $\varepsilon < 1/2$  e escolhermos um  $\delta$  correspondente, veremos que, se  $\mathcal{P}$  é uma partição qualquer com norma menor que  $\delta$ , então

$$\begin{aligned} 1 &= |S(f, \mathcal{P}, \{q_i\}_{i=1}^n) - S(f, \mathcal{P}, \{r_i\}_{i=1}^n)| \\ &= |(S(f, \mathcal{P}, \{q_i\}_{i=1}^n) - I) - (S(f, \mathcal{P}, \{r_i\}_{i=1}^n) - I)| \\ &\leq |(S(f, \mathcal{P}, \{q_i\}_{i=1}^n) - I)| + |(S(f, \mathcal{P}, \{r_i\}_{i=1}^n) - I)| \\ &< \varepsilon + \varepsilon \\ &< \frac{1}{2} + \frac{1}{2} \\ &= 1 \end{aligned}$$

o que é um absurdo e, portanto, uma contradição com a hipótese de que  $f$  é Riemann integrável sobre  $[a, b]$ .

## 4 Introdução à integral de Kurzweil

Nesta seção, apresentaremos a definição da integral de Kurzweil. Para isso, [3] e [4] foram as principais fontes de pesquisa.

Daqui em diante, denotaremos por  $X$  um espaço de Banach com norma  $\|\cdot\|$  e  $\mathcal{K}([a, b], X)$  o espaço vetorial de todas as funções Kurzweil integráveis no espaço de Banach  $X$ .

### 4.1 Preliminares

Aqui, enunciaremos algumas definições preliminares que são necessárias para definir a integral de Kurzweil. Também, veremos um teorema de análise real para demonstrar o Lema de Cousin.

**Definição 4.1.** Uma divisão  $D = \{J_1, J_2, \dots, J_k\}$  de  $[a, b]$  é uma coleção finita de subintervalos compactos  $J_i$  de  $[a, b]$ ,  $i = 1, 2, \dots, k$ , com  $k \in \mathbb{N}$ , tais que  $[a, b] = \bigcup_{i=1}^k J_i$  e  $\text{int}(J_i) \cap \text{int}(J_j)$  seja vazio sempre que  $i \neq j$ .



**Definição 4.2.** Um intervalo marcado é um par  $(\tau, J)$  que consiste de um ponto  $\tau \in \mathbb{R}$  e um intervalo  $J$  em  $\mathbb{R}$ . Dizemos que  $\tau$  é uma marca de  $J$ .

**Definição 4.3.** Uma divisão marcada ou uma partição de  $[a, b]$  é uma coleção finita de pares  $D = \{(\tau_i, J_i) : i = 1, 2, \dots, k\}$ , em que  $D = \{J_1, J_2, \dots, J_k\}$  é uma divisão de  $[a, b]$  e  $\tau_i \in J_i$  para cada  $i = 1, 2, \dots, k$ .

**Definição 4.4.** Um calibre em  $[a, b]$  é qualquer função positiva  $\delta : [a, b] \rightarrow (0, +\infty)$ .

**Definição 4.5.** Seja  $\delta$  um calibre em  $[a, b]$ . Uma divisão marcada ou partição  $D$  é dita  $\delta$ -fina se, para todo  $i = 1, 2, \dots, k$ , tem-se  $J_i \subset [\tau_i - \delta(\tau_i), \tau_i + \delta(\tau_i)]$ .

Também, enunciaremos um resultado de análise real que será necessário em breve.

**Teorema 4.6** (Teorema dos intervalos encaixados). *Seja  $J_1 \subset J_2 \subset \dots \subset J_n \subset \dots$  uma seqüência decrescente de intervalos limitados e fechados  $J_n = [a_n, b_n]$ . A interseção  $\bigcap_{n=1}^{\infty} J_n$  não é vazia, isto é, existe pelos menos um número real  $x$  tal que  $x \in J_n$  para todo  $n \in \mathbb{N}$ . Mais precisamente temos  $\bigcap J_n = [a, b]$ , onde  $a = \sup a_n$  e  $b = \inf b_n$ .*

Para detalhes da demonstração desse teorema, o leitor pode consultar [1]. A seguir, usá-lo-emos como resultado auxiliar para a demonstração do Lema de Cousin.

**Lema 4.7** (Lema de Cousin). *Se  $\delta$  é um calibre em  $[a, b]$ , então existe uma divisão marcada  $\delta$ -fina em  $[a, b]$ .*

*Demonstração.* Sejam  $\delta > 0$  e  $J = [a, b]$  um intervalo na reta, tal que  $J$  não admite uma divisão marcada  $\delta$ -fina. Tomemos

$$D = \left\{ \left[ a, \frac{a+b}{2} \right]; \left[ \frac{a+b}{2}, b \right] \right\}$$

uma divisão marcada em que, por hipótese, um de seus intervalos não satisfaz ser  $\delta$ -fino. Vamos denotar esse subintervalo por  $[a_1, b_1]$ .

Analogamente, construímos

$$D_1 = \left\{ \left[ a_1, \frac{a_1+b_1}{2} \right]; \left[ \frac{a_1+b_1}{2}, b_1 \right] \right\}$$

que pela hipótese assumida, um de seus subintervalos não satisfaz ser  $\delta$ -fino e o denotaremos por  $[a_2, b_2]$ .

Indutivamente, construímos uma seqüência de intervalos decrescentes, limitados e fechados de  $[a, b]$  satisfazendo as seguintes condições:

1.  $[a_n, b_n] \subset [a_{n+1}, b_{n+1}], \forall n \in \mathbb{N}$ ;
2.  $b_n - a_n = \frac{b-a}{2^n}, n \in \mathbb{N}$ ;
3. não há divisão marcada  $\delta$ -fina em  $[a_n, b_n], \forall n \in \mathbb{N}$ .

Pelo Teorema 4.6, através da condição 1 podemos afirmar que  $\bigcap_{n=1}^{\infty} [a_n, b_n] = \{c\}$ , para algum  $c \in J$ . Por outro lado, da condição 2 temos que

$$\lim_{n \rightarrow \infty} (b_n - a_n) = \lim_{n \rightarrow \infty} \left( \frac{b-a}{2^n} \right) = 0,$$

ou seja, pela definição de limite, para  $\varepsilon = \delta(c) > 0$ , existe  $n_0 \in \mathbb{N}$  tal que, se

$$n \geq n_0 \Rightarrow |(b_n - a_n) - 0| < \delta(c) \Rightarrow b_n - a_n < \delta(c).$$

Em particular,  $b_{n_0} - a_{n_0} < \delta(c)$  e disso seguem duas desigualdades e implicações:

- i.  $c - a_{n_0} < b_{n_0} - a_{n_0} < \delta(c) \Rightarrow a_{n_0} > c - \delta(c)$ ;
- ii.  $b_{n_0} - c < b_{n_0} - a_{n_0} < \delta(c) \Rightarrow b_{n_0} < c + \delta(c)$ .

Como  $a_{n_0} < b_{n_0}$ , podemos afirmar que  $[a_{n_0}, b_{n_0}] \subset [c - \delta(c), c + \delta(c)]$  que é a definição de ser uma divisão marcada  $\delta$ -fina, o que contradiz a condição 3.

Deste modo, concluímos que, para todo intervalo  $[a, b]$  e um calibre  $\delta$ , existe uma divisão marcada  $\delta$ -fina em  $[a, b]$ . ■

Esse lema é muito importante pois assegura que podemos realizar as somas de Riemann em uma partição  $\delta$ -fina qualquer, uma vez que a divisão marcada  $\delta$ -fina sempre existe e nossos elementos estão bem definidos. Aliás, a demonstração é bem construtiva, se tornando quase um método para realizar isso, caso seja do nosso interesse.

## 4.2 A integral de Kurzweil

Munidos dos conceitos enunciados, agora somos capazes de definir a integral no sentido de Kurzweil.

**Definição 4.8.** Seja  $U : [a, b] \times [a, b] \rightarrow X$  uma função. Usaremos a notação  $S(U, D)$  para representar a soma de Riemann correspondente à função  $U$  e à divisão marcada  $D$  de  $[a, b]$ .

Além disso,

$$S(U, D) = \sum_{j=1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})].$$

**Definição 4.9** (A integral de Kurzweil). Uma função  $U : [a, b] \times [a, b] \rightarrow X$  é Kurzweil integrável ou, simplesmente, K-integrável, se existe um elemento  $I \in X$  e, para todo  $\varepsilon > 0$ , existe um calibre  $\delta$  em  $[a, b]$ , tal que

$$\|S(U, D) - I\| = \left\| \sum_{j=1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] - I \right\| < \varepsilon$$

para toda divisão marcada  $\delta$ -fina  $D = \{(\tau_j, [\alpha_{j-1}, \alpha_j]) : j = 1, \dots, k\}$  de  $[a, b]$ .

Denotaremos

$$S(U, D) = \int_a^b DU(\tau, t) = I$$

como a integral de Kurzweil de  $U$ , em relação a divisão marcada  $D$ , sobre o intervalo  $[a, b]$ .

Vamos mostrar que  $I$  é única no intervalo  $[a, b]$ .

**Teorema 4.10.** (Unicidade da Integral de Kurzweil) Se  $U \in \mathcal{K}([a, b], X)$ , então  $\int_a^b DU(\tau, t)$  é única.

*Demonstração.* Sejam  $I_1$  e  $I_2$  valores da integral de Kurzweil de  $U$  em  $[a, b]$ . Dado  $\varepsilon > 0$ , existem calibres  $\delta_1$  e  $\delta_2$  em  $[a, b]$ , tais que

$$\|S(U, D_1) - I_1\| < \frac{\varepsilon}{2} \quad \text{e} \quad \|S(U, D_2) - I_2\| < \frac{\varepsilon}{2},$$

para todas divisões marcadas  $\delta_1$ -fina  $D_1$  e  $\delta_2$ -fina  $D_2$ , respectivamente.

Definimos o calibre  $\delta$  em intervalo  $[a, b]$  por

$$\delta(x) = \min\{\delta_1(x), \delta_2(x)\},$$

para todo  $x \in [a, b]$ . Com o Lema de Cousin, podemos garantir a existência de uma divisão marcada  $\delta$ -fina  $D$ , que pela escolha de  $\delta$ , é também  $\delta_1$  e  $\delta_2$  finas.

Consequentemente,

$$\begin{aligned} \|I_1 - I_2\| &= \|S(U, D) - I_2 - (S(U, D) - I_1)\| \\ &\leq \|S(U, D) - I_1\| + \|S(U, D) - I_2\| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Como  $\varepsilon > 0$  é arbitrário, podemos concluir que  $I_1 = I_2$ . ■

A integrabilidade de  $U : [a, b] \rightarrow \mathbb{R}^n$  em cada uma das suas componentes é muito importante para a demonstração do critério de Cauchy, por isso, enunciaremos esse teorema e a seguir, veremos o critério de Cauchy para a integral de Kurzweil. Para mais detalhes sobre ele, o leitor pode consultar [3].

**Teorema 4.11.** *Uma função  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$ ,  $U = (U_1, U_2, \dots, U_n)$ , é Kurzweil integrável se, e somente se, cada uma das componentes  $U_j$  é integrável, no sentido de Kurzweil, para  $j = 1, \dots, n$ .*

Agora, vamos demonstrar o critério de Bolzano-Cauchy para a existência da integral  $\int_a^b DU(\tau, t)$ .

**Teorema 4.12** (Critério de Bolzano-Cauchy para existência da integral de Kurzweil). *A função  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  é integrável sobre  $[a, b]$  se, e somente se, para cada  $\varepsilon > 0$ , existe um calibre  $\delta : [a, b] \rightarrow (0, \infty)$  tal que*

$$\|S(U, D_1) - S(U, D_2)\| < \varepsilon$$

para quaisquer partições  $D_1$  e  $D_2$   $\delta$ -finas de  $[a, b]$ .

*Demonstração.* Pelo Teorema 4.11, podemos reduzir nossa demonstração para  $\mathbb{R}$ , apenas.

Vamos assumir que o critério de Bolzano-Cauchy seja válido. Isto é, existe um calibre  $\delta$  em  $[a, b]$  tal que, para quaisquer partições  $D_1$  e  $D_2$  de  $[a, b]$ , temos

$$|S(U, D_1) - S(U, D_2)| < \frac{\varepsilon}{2}.$$

Vamos denotar por  $\mathcal{M}$  o conjunto de todos os  $s \in \mathbb{R}$  tais que existe um calibre  $\omega$  em  $[a, b]$  que, para toda partição  $\omega$ -fina  $D$ , segue que  $s \leq S(U, D)$ .

Assuma que  $D_0$  seja uma partição  $\delta$ -fina arbitrária de  $[a, b]$ . Pelo Critério de Cauchy, para toda partição  $\delta$ -fina  $D$  de  $[a, b]$ , temos que

$$\begin{aligned} |S(U, D) - S(U, D_0)| &< \frac{\varepsilon}{2} \Rightarrow \\ -\frac{\varepsilon}{2} &< S(U, D) - S(U, D_0) < \frac{\varepsilon}{2} \Rightarrow \\ S(U, D_0) - \frac{\varepsilon}{2} &< S(U, D) < S(U, D_0) + \frac{\varepsilon}{2}. \end{aligned}$$

Portanto,

$$\left(-\infty, S(U, D) - \frac{\varepsilon}{2}\right) \subset \mathcal{M} \quad \text{e} \quad \mathcal{M} \subset \left(-\infty, S(U, D_0) + \frac{\varepsilon}{2}\right),$$

isto é, o conjunto  $\mathcal{M}$  é não-vazio e limitado superiormente, logo, admite supremo, digamos,  $\sup \mathcal{M}$ .

Consequentemente, temos que

$$S(U, D_0) - \frac{\varepsilon}{2} \leq \sup \mathcal{M} \leq S(U, D_0) + \frac{\varepsilon}{2} \Rightarrow |\sup \mathcal{M} - S(U, D_0)| < \frac{\varepsilon}{2}.$$

Sendo assim,

$$\begin{aligned} |S(U, D) - \sup \mathcal{M}| &= |(S(U, D) - S(U, D_0)) - (\sup \mathcal{M} - S(U, D_0))| \\ &\leq |S(U, D) - S(U, D_0)| + |\sup \mathcal{M} - S(U, D_0)| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} < \varepsilon \end{aligned}$$

para toda divisão marcada  $D$  de  $[a, b]$ .

Pela definição da integral de Kurzweil, a função  $U$  é Kurzweil integrável no intervalo  $[a, b]$  e

$$\int_a^b DU(\tau, t) = \sup \mathcal{M}.$$

Por outro lado, se a integral em questão existe, pela definição, dado  $\varepsilon > 0$ , existe um calibre  $\delta > 0$  em  $[a, b]$ , tal que

$$\|S(U, D) - I\| < \varepsilon$$

para toda divisão  $\delta$ -fina  $D$  de  $[a, b]$ , em que  $I$  é o resultado da integral.

Agora, se esse resultado é válido para quaisquer divisões marcadas  $\delta$ -fina de  $[a, b]$ , tomemos  $D_1$  e  $D_2$ , em específico. Dessa forma, temos

$$\|S(U, D_1) - I\| < \frac{\varepsilon}{2}$$

e

$$\|S(U, D_2) - I\| < \frac{\varepsilon}{2}.$$

Portanto,

$$\begin{aligned} \|S(U, D_1) - S(U, D_2)\| &= \|(S(U, D_1) - I) - (S(U, D_2) - I)\| \\ &\leq \|S(U, D_1) - I\| + \|S(U, D_2) - I\| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon, \end{aligned}$$

concluindo o desejado. ■

A seguir, iremos explorar e demonstrar algumas das propriedades fundamentais da integral de Kurzweil.

### 4.3 Propriedades fundamentais da integral de Kurzweil

**Teorema 4.13 (Linearidade).** *Sejam  $U, V \in \mathcal{K}([a, b], X)$  e  $c_1, c_2 \in \mathbb{R}$ . Então  $c_1U + c_2V \in \mathcal{K}([a, b], X)$  e*

$$\int_a^b D [c_1U(\tau, t) + c_2V(\tau, t)] = c_1 \int_a^b DU(\tau, t) + c_2 \int_a^b DV(\tau, t).$$

*Demonstração.* Sejam  $D = \{(\tau_i, [\alpha_{i-1}, \alpha_i]) : i = 1, \dots, k\}$  uma divisão marcada arbitrária de  $[a, b]$  e  $S(U, D)$  e  $S(V, D)$  as somas de Riemann das funções  $U$  e  $V$ , respectivamente.

Então,

$$\begin{aligned} S(c_1U + c_2V, D) &= \sum_{i=1}^k [(c_1U + c_2V)(\tau_i, \alpha_i) - (c_1U + c_2V)(\tau_i, \alpha_{i-1})] \\ &= \sum_{i=1}^k [c_1U(\tau_i, \alpha_i) + c_2V(\tau_i, \alpha_i) - c_1U(\tau_i, \alpha_{i-1}) - c_2V(\tau_i, \alpha_{i-1})] \\ &= \sum_{i=1}^k [(c_1U(\tau_i, \alpha_i) - c_1U(\tau_i, \alpha_{i-1})) + (c_2V(\tau_i, \alpha_i) - c_2V(\tau_i, \alpha_{i-1}))] \\ &= \sum_{i=1}^k [c_1U(\tau_i, \alpha_i) - c_1U(\tau_i, \alpha_{i-1})] + \sum_{i=1}^k [c_2V(\tau_i, \alpha_i) - c_2V(\tau_i, \alpha_{i-1})] \\ &= c_1 \sum_{i=1}^k [U(\tau_i, \alpha_i) - U(\tau_i, \alpha_{i-1})] + c_2 \sum_{i=1}^k [V(\tau_i, \alpha_i) - V(\tau_i, \alpha_{i-1})] \\ &= c_1S(U, D) + c_2S(V, D). \end{aligned}$$

Isto é,

$$\int_a^b D [c_1U(\tau, t) + c_2V(\tau, t)] = c_1 \int_a^b DU(\tau, t) + c_2 \int_a^b DV(\tau, t). \quad \blacksquare$$

Para detalhes da demonstração dos próximos dois resultados, Teoremas 4.14 e 4.15, o leitor pode consultar [3].

**Teorema 4.14.** *Seja  $U \in \mathcal{K}([a, b], X)$ . Então para todo subintervalo  $[c, d] \subset [a, b]$ , temos  $U \in \mathcal{K}([c, d], X)$ .*

**Teorema 4.15.** *Se  $U \in \mathcal{K}([a, b])$ , então, para todo intervalo  $[c, d] \subset [a, b]$  teremos que  $U \in \mathcal{K}([c, d])$ .*

**Teorema 4.16 (Integrabilidade em subintervalos).** *Se  $c \in (a, b)$  e  $U : [a, b] \times [a, b] \rightarrow X$  é tal que  $U \in \mathcal{K}([a, c], X) \cap \mathcal{K}([c, b], X)$ , então  $U \in \mathcal{K}([a, b], X)$  e*

$$\int_a^b DU(\tau, t) = \int_a^c DU(\tau, t) + \int_c^b DU(\tau, t)$$

*Demonstração.* Seja  $\varepsilon > 0$  dado e sejam  $I_1 = \int_a^c DU(\tau, t)$  e  $I_2 = \int_c^b DU(\tau, t)$ .

Pelo Lema de Cousin (Lema 4.7), existe um calibre  $\delta_1$  em  $[a, c]$  tal que para toda partição  $\delta_1$ -fina  $D_1$  de  $[a, c]$ , temos que

$$\|S(U, D_1) - I_1\| < \frac{\varepsilon}{2}.$$

De forma similar, pelo Lema de Cousin, podemos garantir que existe um calibre  $\delta_2$  em  $[c, b]$  tal que para toda partição  $\delta_2$ -fina  $D_2$  de  $[c, b]$ , temos que

$$\|S(U, D_2) - I_2\| < \frac{\varepsilon}{2}.$$

Vamos definir um calibre  $\mu$  da seguinte maneira

$$\mu(\tau) = \begin{cases} \delta_1(\tau), & \text{se } \tau \in [a, c), \\ \min\{\delta_1(c), \delta_2(c)\}, & \text{se } \tau = c, \\ \delta_2(\tau), & \text{se } \tau \in (c, b] \end{cases}$$

e vamos escolher  $\delta : [a, b] \rightarrow (0, \infty)$  tal que

$$\begin{aligned} \delta(\tau) &< \min\{\mu(\tau), |\tau - c|\} \text{ se } \tau \neq c, \\ \delta(c) &= \min\{\delta_1(c), \delta_2(c)\} \text{ se } \tau = c. \end{aligned}$$

Da forma com a qual escolhemos  $\delta$ , temos que  $\delta$  é um calibre em  $[a, b]$ .

Seja  $D = (\alpha_0, \tau_1, \alpha_1, \dots, \tau_k, \alpha_k)$  uma partição  $\delta$ -fina de  $[a, b]$ . Assim, existe um índice  $m$  tal que  $c \in [\alpha_{m-1}, \alpha_m]$ . Ademais,

$$c \in [\alpha_{m-1}, \alpha_m] \subset [\tau_m - \delta(\tau_m), \tau_m + \delta(\tau_m)] \Rightarrow |c - \tau_m| \leq \delta(\tau_m).$$

Contudo, se assumirmos  $c \neq \tau_m$ , como  $[\alpha_{m-1}, \alpha_m]$  é  $\delta$ -fino, segue que

$$|\tau_m - c| \leq \delta(\tau_m) < |\tau_m - c|$$

o que é uma contradição, logo,  $\tau_m = c$ , necessariamente.

Com isso, obtemos que

$$\begin{aligned} S(U, D) &= \sum_{j=1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] \\ &= \sum_{j=1}^{m-1} [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] + U(c, \alpha_m) \\ &\quad - U(c, \alpha_{m-1}) + \sum_{j=m+1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] \\ &= \sum_{j=1}^{m-1} [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] + U(c, c) - U(c, \alpha_{m-1}) \\ &\quad + U(c, \alpha_m) - U(c, c) + \sum_{j=m+1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] \\ &= S(U, D_1) + S(U, D_2). \end{aligned}$$

Assim, para uma partição  $\delta$ -fina  $D$  de  $[a, b]$ , temos:

$$\begin{aligned} \|S(U, D) - I_1 - I_2\| &= \|S(U, D_1) + S(U, D_2) - I_1 - I_2\| \\ &= \|S(U, D_1) - I_1 + S(U, D_2) - I_2\| \\ &\leq \|S(U, D_1) - I_1\| + \|S(U, D_2) - I_2\| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon. \end{aligned}$$

Como  $\varepsilon > 0$  é arbitrário, da definição de integral de Kurzweil, concluímos o resultado desejado. ■

**Lema 4.17** (Lema de Saks-Henstock). *Sejam  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  uma função integrável sobre  $[a, b]$  e  $\varepsilon > 0$  dado. Existe um calibre  $\delta$  em  $[a, b]$ , tal que*

$$\left\| \sum_{j=1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] - \int_a^b DU(\tau, t) \right\| < \varepsilon$$

para toda partição  $\delta$ -fina  $D = \{\alpha_0, \tau_1, \alpha_1, \dots, \tau_k, \alpha_k\}$  do intervalo  $[a, b]$ .

Se

$$a \leq \beta_1 \leq \xi_1 \leq \lambda_1 \leq \beta_2 \leq \xi_2 \leq \lambda_2 \leq \dots \leq \beta_m \leq \xi_m \leq \lambda_m \leq b$$

representa um sistema  $\delta$ -fina  $\{(\xi_j, [\beta_j, \lambda_j]) : j = 1, \dots, m\}$ , isto é, para  $j = \{1, \dots, m\}$ ,

$$\xi_j \in [\beta_j, \lambda_j] \subset [\xi_j - \delta(\xi_j), \xi_j + \delta(\xi_j)],$$

então

$$\left\| \sum_{j=1}^m \left[ U(\xi_j, \lambda_j) - U(\xi_j, \beta_j) - \int_{\beta_j}^{\lambda_j} DU(\tau, t) \right] \right\| < \varepsilon. \quad (4.1)$$

*Demonstração.* Sem perda de generalidade, podemos assumir que  $\beta_j < \lambda_j$ , para todo  $j = \{1, 2, \dots, m\}$ .

Vamos tomar  $\lambda_0 = a$  e  $\beta_{m+1} = b$ . Se  $\lambda_j < \beta_{j+1}$ , para algum  $j = \{0, 1, \dots, m\}$ , então, pelo Teorema 4.15, sabemos que a integral  $\int_{\lambda_j}^{\beta_{j+1}} DU(\tau, t)$  existe, portanto, para cada  $\eta > 0$ , existe um calibre  $\delta_j$  em  $[\lambda_j, \beta_{j+1}]$  tal que  $\delta_j(\tau) < \delta(\tau)$ , para  $\tau \in [\lambda_j, \beta_{j+1}]$  e para toda partição  $\delta_j$ -fina  $D_j$  de  $[\lambda_j, \beta_{j+1}]$ , teremos que

$$\left\| S(U, D_j) - \int_{\lambda_j}^{\beta_{j+1}} DU(\tau, t) \right\| < \frac{\eta}{m+1}.$$

Se  $\lambda_j = \beta_{j+1}$ , então,

$$S(U, D_j) = 0.$$

Ainda, a expressão

$$\sum_{j=1}^m [U(\xi_j, \lambda_j) - U(\xi_j, \beta_j)] + \sum_{j=1}^m S(U, D_j)$$

representa uma soma integral correspondente a uma certa partição  $\delta$ -fina, conseqüentemente,

$$\left\| \sum_{j=1}^m \left[ U(\xi_j, \lambda_j) - U(\xi_j, \beta_j) + \sum_{j=1}^m S(U, D_j) \right] - \int_a^b DU(\tau, t) \right\| < \varepsilon$$

Por isso,

$$\begin{aligned} & \left\| \sum_{j=1}^m \left[ U(\xi_j, \lambda_j) - U(\xi_j, \beta_j) - \int_{\beta_j}^{\lambda_j} DU(\tau, t) \right] \right\| \leq \\ & \leq \left\| \sum_{j=1}^m [U(\xi_j, \lambda_j) - U(\xi_j, \beta_j)] + \sum_{j=1}^m S(U, D_j) - \int_a^b DU(\tau, t) \right\| + \\ & \quad + \sum_{j=1}^m \left\| S(U, D_j) - \int_a^b DU(\tau, t) \right\| < \end{aligned}$$

$$\begin{aligned} &< \varepsilon + (m+1) \frac{\eta}{m+1} \\ &= \varepsilon + \eta. \end{aligned}$$

Como a desigualdade vale para qualquer  $\eta > 0$ , obtemos o resultado desejado. ■

Além deste teorema, também usaremos alguns fatos envolvendo desigualdades entre integrais. Vamos enunciá-los na próxima seção.

#### 4.4 Desigualdades para a integral de Kurzweil

Nesta seção estudaremos dois resultados envolvendo desigualdades e a integral de Kurzweil. ■ A principal referência para esse estudo foi o Capítulo 1 de [3].

**Teorema 4.18.** *Sejam  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  e  $V : [a, b] \times [a, b] \rightarrow \mathbb{R}$  funções em que as integrais  $\int_a^b DU(\tau, t)$  e  $\int_a^b DV(\tau, t)$  existem. Se existe um calibre  $\delta$  em  $[a, b]$  tal que*

$$|t - \tau| \cdot \|U(\tau, t) - U(\tau, \tau)\| \leq (t - \tau) (V(\tau, t) - V(\tau, \tau))$$

para todo  $t \in [\tau - \delta(\tau), \tau + \delta(\tau)]$ , podemos garantir que ocorre a desigualdade

$$\left\| \int_a^b DU(\tau, t) \right\| \leq \int_a^b DV(\tau, t).$$

Note que, mais particularmente, tomando  $V(\tau, t) = f(\tau)g(t)$  em que  $f, g : [a, b] \rightarrow \mathbb{R}$  são funções reais, temos que

$$\left\| \int_a^b DU(\tau, t) \right\| \leq \int_a^b f(s)dg(s).$$

O próximo resultado é lido como corolário direto do Teorema 4.18 e o enunciaremos aqui.

**Teorema 4.19.** *Sejam  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  e  $V : [a, b] \times [a, b] \rightarrow \mathbb{R}$  funções em que as integrais  $\int_a^b DU(\tau, t)$  e  $\int_a^b f(s)dg(s)$  existem, em que  $f, g : [a, b] \rightarrow \mathbb{R}$ . Se existe um calibre  $\delta$  em  $[a, b]$  tal que*

$$|t - \tau| \cdot \|U(\tau, t) - U(\tau, \tau)\| \leq (t - \tau) \cdot f(\tau)(g(t) - g(\tau))$$

para todo  $t \in [\tau - \delta(\tau), \tau + \delta(\tau)]$  e podemos garantir que ocorre a desigualdade

$$\left\| \int_a^b DU(\tau, t) \right\| \leq \int_a^b f(s)dg(s).$$

Usaremos esse corolário para o estudo de algumas propriedades de EDOs generalizadas que exploraremos mais adiante neste artigo. Por enquanto, iremos enunciar alguns teoremas relacionando a integral de Kurzweil e o estudo de limites.

#### 4.5 Relações com a existência e cálculo de limites

**Teorema 4.20.** *Seja a função  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  tal que  $U \in \mathcal{K}([a, c])$  para todo  $c \in [a, b]$  e existe o limite finito*

$$\lim_{c \rightarrow b^-} \left[ \int_a^c DU(\tau, t) - U(b, c) + U(b, b) \right] = I.$$

Então, a função  $U$  é integrável sobre  $[a, b]$  e

$$\int_a^b DU(\tau, t) = I.$$



**Teorema 4.21.** *Seja a função  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  tal que  $U \in \mathcal{K}([a, c])$  para todo  $c \in (a, b)$  e existe o limite finito*

$$\lim_{c \rightarrow a^+} \left[ \int_c^b DU(\tau, t) - U(b, c) + U(b, b) \right] = I.$$

Então, a função  $U$  é integrável sobre  $[a, b]$  e

$$\int_a^b DU(\tau, t) = I.$$

**Teorema 4.22.** *Seja a função  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}^n$  tal que  $U \in \mathcal{K}([a, c])$  para todo  $c \in [a, b]$  e existe o limite finito*

$$\lim_{s \rightarrow c} \left[ \int_a^s DU(\tau, t) - U(b, c) + U(b, b) \right] = \int_a^c DU(\tau, t).$$

Para detalhes das demonstrações dos três teoremas enunciados, o leitor pode consultar a referência [3].

#### 4.6 Métodos de integração

Agora, veremos dois métodos de resolução de integrais muito importantes para a integral de Kurzweil, que também funcionam para as integrais de Riemann, com suas devidas adaptações e particularidades.

**Teorema 4.23 (Teorema da Substituição).** *Assuma que  $-\infty < c < d < +\infty$  e que  $\varphi : [c, d] \rightarrow \mathbb{R}$  é uma função contínua estritamente monótona em  $[c, d]$ .*

*Seja  $U : [\varphi(c)] \times [\varphi(d)] \rightarrow \mathbb{R}^n$ . Se uma das integrais*

$$\int_{\varphi(c)}^{\varphi(d)} DU(\tau, t), \int_c^d DU(\varphi(\sigma), \varphi(s))$$

*existe, então, a outra também existe e*

$$\int_{\varphi(c)}^{\varphi(d)} DU(\tau, t) = \int_c^d DU(\varphi(\sigma), \varphi(s)).$$

*Demonstração.* Sem perda de generalidade, vamos assumir que  $\varphi$  é crescente. Também, vamos assumir que uma das integrais existe e vamos demonstrar que isso implica na existência da outra.

Aqui, faremos a prova com a hipótese da existência de  $\int_c^d DU(\varphi(\sigma), \varphi(s))$ . Podemos encontrar detalhes sobre a demonstração assumindo a existência de  $\int_{\varphi(c)}^{\varphi(d)} DU(\tau, t)$  em [2].

Dado  $\varepsilon > 0$ , existe um calibre  $\omega$  em  $[c, d]$  tal que, para cada partição  $\omega$ -fina

$$\{\beta_0, \sigma_1, \beta_1, \dots, \beta_{k-1}, \sigma_k, \beta_k\}$$

desse intervalo, temos

$$\left\| \sum_{j=1}^k [U(\varphi(\sigma_j), \varphi(\beta_j)) - U(\varphi(\sigma_j), \varphi(\beta_{j-1}))] - \int_c^d DU(\varphi(\sigma), \varphi(s)) \right\| < \varepsilon.$$

Como  $\varphi$  é monótona crescente,  $\varphi([c, d]) = [\varphi(c), \varphi(d)]$ , logo, bijetora nesse intervalo. Sendo assim, admite uma inversa  $\varphi^{-1} : [\varphi(c), \varphi(d)] \rightarrow [c, d]$ , naturalmente contínua e crescente em  $[\varphi(c), \varphi(d)]$ .

Por isso, para cada  $\tau \in [\varphi(c), \varphi(d)]$ , existe exatamente um  $\sigma = \varphi^{-1}(\tau) \in [c, d]$ . Vamos definir  $\delta(\tau) > 0$ , para cada  $\tau \in [\varphi(c), \varphi(d)]$ , tal que

$$[\tau - \delta(\tau), \tau + \delta(\tau)] \cap [\varphi(c), \varphi(d)] \subset \varphi([\sigma - \omega(\sigma), \sigma + \omega(\sigma)]) \cap [c, d].$$

Seja  $\{\alpha_0, \tau_1, \alpha_1, \dots, \alpha_{k-1}, \tau_k, \alpha_k\}$  uma partição arbitrária  $\delta$ -fina de  $[\varphi(c), \varphi(d)]$ . Também, tomemos  $\beta_j = \varphi^{-1}(\alpha_j), j = 0, 1, \dots, k$  e  $\sigma_j = \varphi^{-1}(\tau_j), j = 1, \dots, k$ .

Então, pela monotonicidade de  $\varphi^{-1}$ , temos que

$$\beta_0 = \varphi^{-1}(\alpha_0) = c < \beta_1 < \beta_2 < \dots < \beta_{k-1} < \beta_k = \varphi^{-1}(\alpha_k) = d$$

e

$$\beta_{j-1} < \sigma_j < \beta_j, j = 1, 2, \dots, k.$$

Assim, garantimos que  $\{\beta_0, \sigma_1, \beta_1, \dots, \beta_{k-1}, \sigma_k, \beta_k\}$  é uma partição de  $[c, d]$ .

Como  $\{\alpha_0, \tau_1, \alpha_1, \dots, \alpha_{k-1}, \tau_k, \alpha_k\}$  é  $\delta$ -fina em  $[\varphi(c), \varphi(d)]$ , segue que

$$\tau_j - \delta(\tau_j) \leq \alpha_{j-1} \leq \tau_j \leq \alpha_j \leq \tau_j + \delta(\tau_j) \Rightarrow$$

$$\varphi(\sigma_j - \omega(\sigma_j)) \leq \alpha_{j-1} \leq \alpha_j \leq \varphi(\sigma_j + \omega(\sigma_j)).$$

Aplicando  $\varphi^{-1}$  nas últimas desigualdades (uma vez que  $\varphi^{-1}$  é crescente), concluímos que a partição  $\{\beta_0, \sigma_1, \beta_1, \dots, \beta_{k-1}, \sigma_k, \beta_k\}$  é  $\omega$ -fina, também.

Portanto, seja  $\{\beta_0, \sigma_1, \beta_1, \dots, \beta_{k-1}, \sigma_k, \beta_k\}$  uma partição  $\delta$ -fina. Se a integral  $\int_c^d DU(\varphi(\sigma), \varphi(s))$  existe, então,

$$\left\| \sum_{j=1}^k [U(\tau_j, \alpha_j) - U(\tau_j, \alpha_{j-1})] - \int_c^d DU(\varphi(\sigma), \varphi(s)) \right\| < \varepsilon \Rightarrow$$

$$\left\| \sum_{j=1}^k [U(\varphi(\sigma_j), \varphi(\beta_j)) - U(\varphi(\sigma_j), \varphi(\beta_{j-1}))] - \int_{\varphi(c)}^{\varphi(d)} DU(\tau, t) \right\| < \varepsilon$$

e a integral  $\int_{\varphi(c)}^{\varphi(d)} DU(\varphi(\tau), t)$  também existe.  $\blacksquare$

Agora, vamos generalizar a fórmula da integração por partes para a integral de Kurzweil. Antes, vamos enunciar um breve lema.

**Lema 4.24.** *Assuma que  $V : [a, b] \times [a, b] \rightarrow \mathbb{R}$  é tal que*

$$V(\tau, t) = V(t, \tau) \text{ para } t, \tau \in [a, b].$$

*Vamos definir  $W(\tau, t) = V(t, \tau)$ . Então se uma das integrais*

$$\int_a^b DV(\tau, t), \int_a^b DW(\tau, t)$$

*existe, então, a outra existe também e*

$$\int_a^b DV(\tau, t) = \int_a^b DW(\tau, t) = \int_a^b DV(t, \tau).$$

A demonstração desse lema decorre imediatamente da análise das somas de Riemann, em relação a uma partição  $\delta$ -fina  $D$  qualquer em  $[a, b]$ , para as funções  $V$  e  $W$  fazendo uso da propriedade de simetria das funções.

**Teorema 4.25 (Integração por Partes).** *Suponha que  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}$  é uma função dada. Vamos definir  $U^*(\tau, t) = U(t, \tau)$  e  $V(\tau, t) = U(\tau, \tau) - U(\tau, t) - U(t, \tau) + U(t, t)$ .*

*Se duas das integrais*

$$\int_a^b DU(\tau, t), \int_a^b DU^*(\tau, t), \int_a^b DV(\tau, t)$$

*existem, então, a terceira também existe e segue a igualdade*

$$\int_a^b DU(\tau, t) + \int_a^b DU^*(\tau, t) = U(b, b) - U(a, a) - \int_a^b DV(\tau, t).$$

A demonstração desse teorema consiste em realizar manipulações da norma das somas de Riemann da função (definição da integral de Kurzweil e desigualdade triangular), utilizando as propriedades de  $V$  satisfazer a hipótese de simetria do Lema 4.24. Para mais detalhes, pode-se consultar [3].

A seguir, apresentaremos um teorema de convergência para a integral de Kurzweil, tendo como referência o Capítulo 1 de Schwabik [3].

**Teorema 4.26.** *Seja  $U, U_m : [a, b] \times [a, b] \rightarrow \mathbb{R}$  para  $m \in \mathbb{N}$ , em que  $U_m \in \mathcal{K}([a, b])$ . Vamos assumir que a sequência  $(U_m)$  satisfaz as condições descritas a seguir.*

*Existe um calibre  $\delta$  em  $[a, b]$  tal que, para todo  $\varepsilon > 0$ , haverá  $p : [a, b] \rightarrow \mathbb{N}$  e uma função positiva  $\Phi$ , definida em um intervalo  $J \subset [a, b]$  fechado, satisfazendo*

$$\Phi(x + y) \geq \Phi(x) + \Phi(y)$$

*para todos  $x, y \in J$  e  $\Phi([a, b]) < \varepsilon$ , tal que, para todo  $\tau \in [a, b]$ , temos*

$$|U_m(\tau, J) - U(\tau, J)| < \Phi(J)$$

*caso  $m > p(\tau)$  e  $(\tau, J)$  é um intervalo marcado  $\delta$ -fino com  $\tau \in J \subset [a, b]$ .*

*Assuma, ainda, que para duas funções  $V, W : [a, b] \times [a, b] \rightarrow \mathbb{R}$ , em que  $V, W \in \mathcal{K}([a, b])$ , existe um calibre  $\theta$  em  $[a, b]$  tal que para todo  $m \in \mathbb{N}$ ,  $\tau \in [a, b]$  temos*

$$V(\tau, J) \leq U_m(\tau, J) \leq W(\tau, J)$$

*para todo intervalo marcado  $\theta$ -fino  $(\tau, J)$ .*

*Então,  $U \in \mathcal{K}([a, b])$  e*

$$\lim_{m \rightarrow \infty} \int_a^b DU_m(\tau, J) = \int_a^b DU(\tau, J).$$

## 5 Teorema Fundamental do Cálculo para Integral de Henstock-Kurzweil

Antes de apresentar e estudar alguns exemplos de funções reais Kurzweil integráveis, vamos enunciar e demonstrar o Teorema Fundamental do Cálculo para a Integral de Henstock-Kurweil de funções reais.

Primeiro, vamos enunciar a definição usual de integral de Henstock-Kurzweil.

**Definição 5.1.** *Sejam  $f : [a, b] \rightarrow \mathbb{R}$  uma função e  $D = \{(\tau, [\alpha_{i-1}, \alpha_i] : i = 1, \dots, k)\}$  uma divisão de  $[a, b]$ . Se  $U : [a, b] \times [a, b] \rightarrow \mathbb{R}$  for tal que*

$$U(\tau, t) = f(\tau) \cdot t, \text{ com } \tau, t \in [a, b],$$

*então,*

$$S(U, D) = \sum_{i=1}^k [U(\tau_i, \alpha_i) - U(\tau_i, \alpha_{i-1})] = \sum_{i=1}^k f(\tau_i)[\alpha_i - \alpha_{i-1}].$$

**Teorema 5.2** (Teorema Fundamental do Cálculo generalizado). *Seja  $F : [a, b] \rightarrow \mathbb{R}$  uma primitiva de  $f$ , isto é, existe uma função  $f : [a, b] \rightarrow \mathbb{R}$  tal que  $f(x) = F'(x)$ , para todo  $x \in [a, b]$ . Então,  $f$  é Henstock-Kurzweil integrável e*

$$(HK) \int_a^b f(s) ds = F(b) - F(a).$$

Sendo  $(HK) \int_a^b f(s) ds$  a integral de Henstock-Kurzweil da função  $f$  no intervalo  $[a, b]$ .

*Demonstração.* Seja  $\varepsilon > 0$  dado. Queremos construir um calibre  $\delta$  em  $[a, b]$ , tal que, para toda divisão marcada  $\delta$ -fina  $D = \{(\tau_i, [t_{i-1}, t_i]) : i = 1, 2, \dots, k\}$ , tenhamos

$$\left| \sum_{i=1}^k f(\tau_i)[t_i - t_{i-1}] - (F(b) - F(a)) \right| < \varepsilon(b - a).$$

Por hipótese,  $F'(\tau) = f(\tau)$ , para todo  $\tau \in [a, b]$ . Logo, para cada  $\tau \in [a, b]$ , existem constantes  $r, s \in [a, b]$  tais que

$$|F(r) - F(\tau) - f(\tau)(r - \tau)| < \varepsilon|r - \tau|;$$

$$|F(\tau) - F(s) - f(\tau)(\tau - s)| < \varepsilon|\tau - s|,$$

sempre que  $\tau - \delta(\tau) < s < \tau < r < \tau + \delta(\tau)$ .

Portanto,

$$|F(r) - F(s) - f(\tau)(r - s)| < \varepsilon|r - s|.$$

Note que a função acima  $\delta : [a, b] \rightarrow \mathbb{R}$  é o calibre que desejávamos, uma vez que

$$\begin{aligned} \left| \sum_{i=1}^k f(\tau_i)[t_i - t_{i-1}] - (F(b) - F(a)) \right| &= \left| \sum_{i=1}^k f(\tau_i)[t_i - t_{i-1}] - (F(t_i) - F(t_{i-1})) \right| \\ &< \sum_{i=1}^k \varepsilon(t_i - t_{i-1}) \\ &= \varepsilon(b - a). \end{aligned}$$

Logo, a função  $f$  é Henstock-Kurzweil integrável. ■

Imediatamente, como consequência deste teorema, podemos afirmar que qualquer função  $f : [a, b] \rightarrow \mathbb{R}$ , que seja a derivada de outra função  $F : [a, b] \rightarrow \mathbb{R}$ , é Henstock-Kurzweil integrável.

Vejamos alguns exemplos na próxima seção.

## 6 Exemplos de funções Kurzweil integráveis

Vamos explorar alguns exemplos de funções Kurzweil integráveis encontrados na literatura, tendo como principais materiais de pesquisa as referências [2] e [4].

### 6.1 Função de Dirichlet

**Exemplo 6.1.** Vamos retomar à função de *Dirichlet*, como vimos no Exemplo 3.3.

Sabemos que  $f : [0, 1] \rightarrow \mathbb{R}$ , tal que

$$f(x) = \begin{cases} 1, & \text{se } x \in \mathbb{Q} \cap [0, 1], \\ 0, & \text{se } x \notin \mathbb{Q} \cap [0, 1], \end{cases}$$

não é Riemann integrável. Contudo, mostraremos que  $f$  é Kurzweil integrável.

Além disso, mostraremos que

$$\int_0^1 f(x) dx = 0.$$

De fato, dado  $\varepsilon > 0$ , tomemos o calibre  $\delta : [0, 1] \rightarrow \mathbb{R}$ , tal que

$$\delta(x) = \begin{cases} \frac{\varepsilon}{2^{n+1}}, & \text{se } x = x_n, \forall n \in \mathbb{N}, \\ 1, & \text{se } x \text{ é irracional em } [0, 1] \end{cases}$$

em que  $(x_n)_{n \in \mathbb{N}}$  é uma enumeração dos racionais em  $[0, 1]$ .

Desse modo, se

$$D = \{(\tau_j, [\alpha_{j-1}, \alpha_j]) : j = 1, 2, \dots, k\}$$

é uma partição  $\delta$ -fina qualquer em  $[0, 1]$ , obtemos

$$\begin{aligned} |S(f, D) - 0| &= |S(f, D)| \\ &= \left| \sum_{j=1}^k f(\tau_j)(\alpha_j - \alpha_{j-1}) \right| \\ &\leq \left| \sum_{\substack{j=1 \\ \tau_j \in [0,1] \cap \mathbb{Q}}}^k f(\tau_j)(\alpha_j - \alpha_{j-1}) \right| + \left| \sum_{\substack{j=1 \\ \tau_j \in [0,1] \cap (\mathbb{R} - \mathbb{Q})}}^k f(\tau_j)(\alpha_j - \alpha_{j-1}) \right| \\ &= \left| \sum_{\substack{j=1 \\ \tau_j \in [0,1] \cap \mathbb{Q}}}^k f(\tau_j)(\alpha_j - \alpha_{j-1}) \right| = \left| \sum_{\substack{j=1 \\ \tau_j \in [0,1] \cap \mathbb{Q}}}^k (\alpha_j - \alpha_{j-1}) \right|. \end{aligned}$$

Como a partição  $D$  é  $\delta$ -fina, a distância entre cada  $\alpha_j$  e  $\alpha_{j-1}$  é sempre inferior ao dobro do calibre, ou seja,

$$\left| \sum_{\substack{j=1 \\ \tau_j \in [0,1] \cap \mathbb{Q}}}^k (\alpha_j - \alpha_{j-1}) \right| \leq \sum_{j=1}^k 2 \frac{\varepsilon}{2^{j+1}} = 2 \sum_{j=1}^k \frac{\varepsilon}{2^{j+1}} = 2 \left( \frac{\varepsilon}{2} \right) = \varepsilon$$

para toda divisão  $\delta$ -fina  $D$  em  $[0, 1]$ . Isto é,

$$|S(f, D) - 0| < \varepsilon,$$

que pela definição da integral de integral de Kurzweil implica que

$$\int_0^1 f(x) dx = 0.$$

## 6.2 Exemplo de funções que não são Riemann nem Lebesgue integrável

**Exemplo 6.2.** Seja  $f : [0, 1] \rightarrow \mathbb{R}$  tal que

$$f(x) = \begin{cases} 2x \cos\left(\frac{\pi}{x^2}\right) + \frac{2\pi}{x} \operatorname{sen}\left(\frac{\pi}{x^2}\right), & x \in (0, 1], \\ 0, & x = 0. \end{cases}$$

Note que  $f$  não é Lebesgue integrável, uma vez que não é absolutamente integrável e, portanto, também não é Riemann integrável, como podemos constatar em [1].

Contudo, sabemos que  $f$  é a derivada da função  $F : [0, 1] \rightarrow \mathbb{R}$

$$F(x) = \begin{cases} x^2 \cos\left(\frac{\pi}{x^2}\right), & x \in (0, 1], \\ 0, & x = 0. \end{cases}$$

Portanto, pelo Teorema 5.2,  $f$  é Henstock-Kurzweil integrável em  $[0, 1]$ . Mais precisamente,

$$\int_0^1 f(x) dx = F(1) - F(0) = \cos(\pi) - 0 = -1.$$

**Exemplo 6.3.** Consideramos, agora, a função  $f : [0, 1] \rightarrow \mathbb{R}$ , na qual

$$f(x) = \begin{cases} \frac{(-1)^k}{x}, & \text{para } \frac{1}{k+1} < x \leq \frac{1}{k}, \\ 0, & \text{se } x = 0. \end{cases}$$

Sabemos que, para  $x > 0$ ,  $\ln x$  é a primitiva da função  $\frac{1}{x}$ . Assim, para todo  $k \in \mathbb{N}$ , temos

$$\int_{\frac{1}{k+1}}^{\frac{1}{k}} f(s) ds = (-1)^k \int_{\frac{1}{k+1}}^{\frac{1}{k}} \frac{1}{s} ds = (-1)^k \ln\left(\frac{k+1}{k}\right)$$

como vimos no Teorema 5.2.

Então, para  $n \in \mathbb{N}$  obtemos

$$\int_{\frac{1}{n}}^1 f(s) ds = \sum_{k=1}^{n-1} \int_{\frac{1}{k+1}}^{\frac{1}{k}} f(s) ds = \sum_{k=1}^{n-1} (-1)^k \ln\left(\frac{k+1}{k}\right).$$

Como

$$(a_k)_{k \in \mathbb{N}}, a_k = \ln\left(\frac{k+1}{k}\right)$$

é uma sequência positiva de termos decrescentes, em que  $a_k \rightarrow 0$  quando  $k \rightarrow +\infty$ , o teste de Leibniz garante a convergência da série. Vamos chamar o resultado desta convergência de  $L$ .

Daí, segue que

$$\lim_{c \rightarrow 0^+} \int_c^1 f(s) ds = L < \infty.$$

Deste modo,  $f$  é Kurzweil integrável em  $[0, 1]$ . Também podemos notar que a série não convergiria absolutamente, portanto,  $f$  não é Lebesgue integrável e, por consequência, nem Riemann integrável.

Assim, encerramos o primeiro grande tópico que este artigo pretendia abordar e iniciaremos as discussões sobre as EDOs generalizadas.

## 7 Equações Diferenciais Ordinárias generalizadas

Nesta seção, iremos discutir como se dá a caracterização de EDOs generalizadas, bem como discutir resultados e propriedades importantes que decorrem desta caracterização.

Para a escrita desta seção, utilizamos como referência o capítulo 3 de Schwabik [3]. Bem como ele, denotaremos por  $G \subset \mathbb{R}^{n+1}$  um conjunto aberto e  $F : G \rightarrow \mathbb{R}^{n+1}$  uma função dada.

### 7.1 Definindo EDOs generalizadas e suas soluções

**Definição 7.1.** Uma função  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$  é dita solução de uma EDO generalizada

$$\frac{dx}{d\tau} = DF(x, t) \quad (7.1)$$

no intervalo  $[\alpha, \beta] \subset \mathbb{R}$ , se  $(x(t), t) \in G$  para todo  $t \in [\alpha, \beta]$  satisfazendo

$$x(s_2) - x(s_1) = \int_{s_1}^{s_2} DF(x(\tau), t) \quad (7.2)$$

para todos  $s_1, s_2 \in [\alpha, \beta]$ .

Vale ressaltar que a integral do lado direito da igualdade deve ser lida no sentido de Kurzweil, como definimos em 4.9.

**Observação 7.2.** As notações de (7.1) são puramente simbólicas. Mais incisivamente, os símbolos diferenciais do lado esquerdo da igualdade não indicam que se trata da derivada da função  $x$ . “D” do lado direito é apenas uma referência de que se trata de uma EDO generalizada. Vamos explorar um pouco essa observação.

Seja  $r : [0, 1] \rightarrow \mathbb{R}$  uma função contínua não diferenciável sobre todo o intervalo  $[0, 1]$ .

Faça  $F(x, t) = r(t)$  e tome  $D = \{(\tau_j, [s_{j-1}, s_j]) : j = 1, 2, \dots, n\}$  uma divisão marcada de  $[0, 1]$ .

Então,

$$\int_{s_1}^{s_2} DF(x(\tau), t) = \int_{s_1}^{s_2} Dr(t) = \sum_{j=1}^n [r(s_j) - r(s_{j-1})] = r(s_n) - r(s_0) = r(s_2) - r(s_1).$$

Desse modo,  $x : [0, 1] \rightarrow \mathbb{R}$  tal que  $x(t) = r(t)$ , para todo  $t \in [a, b]$ , é uma solução para (7.1) e não é diferenciável em nenhum ponto de seu domínio.

**Teorema 7.3.** Uma função  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$  é solução de uma EDO generalizada (7.1) em  $[\alpha, \beta]$  se, e somente se, para todo  $\gamma \in [\alpha, \beta]$  fixado temos

$$x(s) = x(\gamma) + \int_{\gamma}^s DF(x(\tau), t), s \in [\alpha, \beta]. \quad (7.3)$$

*Demonstração.* Supondo que  $x$  seja solução de (7.1), então

$$x(s_2) - x(s_1) = \int_{s_1}^{s_2} DF(x(\tau), t)$$

para todo  $s_1, s_2 \in [\alpha, \beta]$ .

Tomemos, então,  $s_1 = \gamma$  e  $s_2 = s$  decorrendo, imediatamente, que

$$x(s) = x(\gamma) + \int_{\gamma}^s DF(x(\tau), t).$$

Reciprocamente, se vale que

$$x(s) = x(\gamma) + \int_{\gamma}^s DF(x(\tau), t)$$

para qualquer  $s \in [\alpha, \beta]$  e  $\gamma \in [\alpha, \beta]$  fixado, então

$$\begin{aligned} x(s_2) - x(s_1) &= x(\gamma) + \int_{\gamma}^{s_2} DF(x(\tau), t) - x(\gamma) - \int_{\gamma}^{s_1} DF(x(\tau), t) \\ &= \int_{s_1}^{\gamma} DF(x(\tau), t) + \int_{\gamma}^{s_2} DF(x(\tau), t) \\ &= \int_{s_1}^{s_2} DF(x(\tau), t), \end{aligned}$$

o que implica que  $x$  é solução da EDO generalizada. ■

**Teorema 7.4.** *Se  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$  é solução para a EDO generalizada (7.1) em  $[\alpha, \beta]$ , então*

$$\lim_{s \rightarrow \sigma} [x(s) - F(x(\sigma), s) + F(x(\sigma), \sigma)] = x(\sigma)$$

para todo  $\sigma \in [\alpha, \beta]$ .

Este teorema pode ser demonstrado utilizando o Teorema 7.3 juntamente do Teorema 4.22. Para mais detalhes, o leitor pode consultar [3].

A partir de agora, vamos introduzir uma nova classe de funções e exploraremos alguns resultados com mais detalhes.

## 7.2 A classe de funções $\mathcal{F}(G, h, \omega)$

Sejam  $B_r = \{x \in \mathbb{R}^n : \|x\| < r\}$ , com  $r > 0$  e  $(a, b)$  um intervalo aberto da reta, com  $-\infty < a < b < +\infty$ .

Definiremos, então, o conjunto  $G$  como o produto cartesiano entre  $B_r$  e  $(a, b)$ , ou seja,  $G = B_r \times (a, b)$ .

Além disso, também definiremos  $h : [a, b] \rightarrow \mathbb{R}$  sendo uma função não-decrescente em  $[a, b]$  e  $\omega : [0, +\infty) \rightarrow \mathbb{R}$  uma função contínua em que  $\omega(0) = 0$ .

**Definição 7.5.** Uma função  $F : G \rightarrow \mathbb{R}^n$  pertence à classe  $\mathcal{F}(G, h, \omega)$  se satisfaz as seguintes propriedades:

$$\|F(x, t_2) - F(x, t_1)\| \leq |h(t_2) - h(t_1)| \quad (7.4)$$

para todo  $(x, t_1), (x, t_2) \in G$  e

$$\|F(x, t_2) - F(x, t_1) - F(y, t_2) + F(y, t_1)\| \leq \omega(\|x - y\|)|h(t_2) - h(t_1)| \quad (7.5)$$

para todo  $(x, t_1), (x, t_2), (y, t_1), (y, t_2) \in G$ .

Vamos explorar alguns resultados.

**Lema 7.6.** *Sejam  $[\alpha, \beta] \subset [a, b]$  e  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$  uma função tal que  $(x(t), t) \in G$  para todo  $t \in [\alpha, \beta]$ . Vamos considerar  $F : G \rightarrow \mathbb{R}^n$  uma função satisfazendo (7.4). Além disso, se a integral  $\int_{\alpha}^{\beta} DF(x(\tau), t)$  existe, então, para todos  $s_1, s_2 \in [\alpha, \beta]$  vale a desigualdade*

$$\left\| \int_{s_1}^{s_2} DF(x(\tau), t) \right\| \leq |h(s_2) - h(s_1)|.$$

*Demonstração.* Como  $F$  satisfaz (7.4), temos que

$$\|F(x, t_2) - F(x, t_1)\| \leq |h(t_2) - h(t_1)| \Rightarrow$$



$$|t - \tau| \cdot \|F(x(\tau), t) - F(x(\tau), \tau)\| \leq |(t - \tau)(h(t) - h(\tau))|$$

para quaisquer  $t, \tau \in [\alpha, \beta]$ . Assim, a integral  $\int_{\alpha}^{\beta} dh(t)$  existe e

$$\int_{s_1}^{s_2} dh(t) = h(s_2) - h(s_1)$$

para todos  $s_1, s_2 \in [\alpha, \beta]$ . Portanto, como consequência do Teorema 4.19, temos que

$$\left\| \int_{s_1}^{s_2} DF(x(\tau), t) \right\| \leq |h(s_2) - h(s_1)|. \quad \blacksquare$$

Observe que, pela equação (7.2), podemos relacionar a integral do lado esquerdo da última desigualdade com a diferença de duas imagens da função  $x$  e esse será nosso próximo resultado.

**Lema 7.7.** *Sejam  $[\alpha, \beta] \subset [a, b]$  e  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$  uma função tal que  $(x(t), t) \in G$  para todo  $t \in [\alpha, \beta]$ . Vamos considerar  $F : G \rightarrow \mathbb{R}^n$  uma função satisfazendo (7.4). Então, para todos  $s_1, s_2 \in [\alpha, \beta]$  vale a desigualdade*

$$\|x(s_2) - x(s_1)\| \leq |h(s_2) - h(s_1)|.$$

*Demonstração.* Como  $x$  é solução de (7.1), temos que

$$x(s_2) - x(s_1) = \int_{s_1}^{s_2} DF(x(\tau), t),$$

para quaisquer  $s_1, s_2 \in [\alpha, \beta]$ . Agora, pelo Lema 7.6, conseguimos concluir que

$$\left\| \int_{s_1}^{s_2} DF(x(\tau), t) \right\| \leq |h(s_2) - h(s_1)| \Rightarrow \|x(s_2) - x(s_1)\| \leq |h(s_2) - h(s_1)|. \quad \blacksquare$$

**Teorema 7.8.** *Sejam  $F \in \mathcal{F}(G, h, \omega)$  e  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$ , com  $[\alpha, \beta] \subset [a, b]$ , o limite pontual de uma sequência de funções  $x_k : [\alpha, \beta] \rightarrow \mathbb{R}^n$  tais que  $(x(s), s) \in G$  e  $(x_k(s), s) \in G$  para todo  $k \in \mathbb{N}$ ,  $s \in [a, b]$  e existe  $\int_{\alpha}^{\beta} DF(x_k(\tau), t)$  para todo  $k$  natural. Então, a integral  $\int_{\alpha}^{\beta} DF(x(\tau), t)$  existe e vale a igualdade*

$$\int_{\alpha}^{\beta} DF(x(\tau), t) = \lim_{k \rightarrow \infty} \int_{\alpha}^{\beta} DF(x_k(\tau), t)$$

*Demonstração.* Vamos assumir, sem perda de generalidade, que  $F$  é uma função real.

Por (7.5), temos que

$$\begin{aligned} & |F(x_k(\tau), t_2) - F(x_k(\tau), t_1) - F(x(\tau), t_2) + F(x(\tau), t_1)| \leq \\ & \omega(\|x_k(\tau) - x(\tau)\|) \cdot |h(t_2) - h(t_1)| \end{aligned}$$

para todo  $\tau \in [\alpha, \beta]$ ,  $t_1 \leq \tau \leq t_2$ ,  $[t_1, t_2] \subset [\alpha, \beta]$ .

Primeiramente, recordemos que  $h$  é uma função não-decrescente e, portanto, pela definição de intervalo real,

$$t_1 \leq t_2 \Rightarrow 0 \leq h(t_2) - h(t_1).$$

Com isso, podemos omitir o módulo na última expressão:

$$\begin{aligned} & |F(x_k(\tau), t_2) - F(x_k(\tau), t_1) - F(x(\tau), t_2) + F(x(\tau), t_1)| \leq \\ & \omega(\|x_k(\tau) - x(\tau)\|) \cdot (h(t_2) - h(t_1)). \end{aligned}$$

Agora, vamos definir a função

$$\mu(t) = \frac{\varepsilon}{h(\beta) - h(\alpha) + 1} h(t)$$

para todo  $t \in [\alpha, \beta]$  e  $\varepsilon > 0$  dado.

Como  $\omega$  é contínua e  $x$  é o limite pontual da sequência de funções, temos que

$$\lim_{k \rightarrow \infty} x_k(\tau) - x(\tau) = 0 \Rightarrow \omega \left( \lim_{k \rightarrow \infty} x_k(\tau) - x(\tau) \right) = \omega(0) = 0.$$

Isso significa que, dado  $\varepsilon > 0$ , existe  $p(\tau) \in \mathbb{N}$  tal que

$$k \geq p(\tau) \Rightarrow \omega(x_k(\tau) - x(\tau)) < \frac{\varepsilon}{h(\beta) - h(\alpha) + 1}.$$

Voltando, podemos afirmar que, para  $k \geq p(\tau)$ , temos

$$\begin{aligned} |F(x_k(\tau), t_2) - F(x_k(\tau), t_1) - F(x(\tau), t_2) + F(x(\tau), t_1)| &\leq \\ &\leq \mu(t_2) - \mu(t_1). \end{aligned}$$

o que, por (7.4) juntamente do Teorema 4.26, implica o desejado, uma vez que as integrais existem e a igualdade segue imediatamente. ■

**Corolário 7.9.** *Sejam  $F \in \mathcal{F}(G, h, \omega)$  e  $x : [\alpha, \beta] \rightarrow \mathbb{R}^n$ , com  $[\alpha, \beta] \subset [a, b]$ , o limite pontual de uma sequência de funções regradas finitas tais que  $(x(s), s) \in G$  para todo  $s \in [\alpha, \beta]$ . Então, a integral  $\int_{\alpha}^{\beta} DF(x(\tau), t)$  existe.*

Para detalhes deste corolário, consultar [3].

## 8 Considerações

A teoria de integral teve avanços substanciais durante o último século através das contribuições de muitas pessoas. Uma delas, e que é particularmente especial para aquilo que discutimos, foi Jaroslav Kurzweil.

Paralelamente à Ralph Henstock, Kurzweil criou um novo universo de possibilidades no campo das EDOs ao generalizar as integrais de Riemann e Lebesgue.

Da maneira com que a integral de Kurzweil é definida, podemos a utilizar para caracterizar as EDOs generalizadas.

O termo “EDO generalizada” é justificável, no sentido que, dada uma equação diferencial ordinária, podemos encontrar uma EDO generalizada tal que as duas equações tenham o mesmo conjunto solução.

Além disso, que é possível obter resultados bastante gerais concernentes a propriedades qualitativas de suas soluções e traduzi-los para as teorias de outros tipos de equações diferenciais por meio das correspondências que existem entre elas.

Neste trabalho, buscamos apresentar a base da teoria das EDOs generalizadas para, posteriormente, estudar essas correspondências.

**Agradecimentos:** Agradecemos à Fundação de Amparo à Pesquisa do Estado de São Paulo pelo financiamento da pesquisa de iniciação científica.

*Abstract: From the interest in studying Ordinary Differential Equations, numerous researchers have contributed to the field of integral theory. Prominent figures such as Riemann, Lebesgue, Perron, Henstock, and Kurzweil have made significant contributions to this area. More specifically, in order to characterize and study generalized ordinary differential equations, it is essential to work with Kurzweil integrals. To introduce this integral, we will start with the familiar construction of the Riemann integral and seek to refine certain concepts that approximate the Riemann sum in order to characterize the Kurzweil integral. We will also present important results, such as the existence and uniqueness of this integral, as well as some properties of this new tool. Finally, we will introduce the concept of generalized ordinary differential equations and explore some of their initial properties, which serve as a foundation for constructing more general results in the theory of differential equations.*

*Keywords: Riemann integral; Kurzweil integral; Generalized ordinary differential equations*

---

## Referências Bibliográficas

- [1] Lima, E. L. *Análise Real*, vol. 1, 8a edição, Coleção Matemática Universitária, IMPA, 2004.
- [2] Kurtz, D. S.; Swartz, C. W. *Theories of integration. The integrals of Riemann, Lebesgue, Henstock-Kurzweil, and Mcshane, Series in Real Analysis*. 9. World Scientific Publishing, 2004.
- [3] Schwabik, Š. *Generalized Ordinary Differential Equations*. World Scientific, Series in Real Analysis, vol. 5, 1992.
- [4] Souto, G. M. *Equações diferenciais funcionais com retardamento e impulsos via equações diferenciais ordinárias generalizadas*. Maringá, 2013.

## BOLETIM DE INICIAÇÃO CIENTÍFICA EM MATEMÁTICA · BICMAT

### *Orientação aos autores*

Ao redigir o material a ser divulgado o autor deve observar que o alvo principal é o aluno de graduação, devendo a redação ser clara e objetiva incentivando-o à leitura.

O trabalho deve ser enviado à Comissão Editorial, via e-mail, na linguagem  $\text{\LaTeX}$ , usando a classe `bicmat`. Mais informações sobre a formatação do trabalho podem ser encontradas em [www.rc.unesp.br/igce/matematica/bicmat](http://www.rc.unesp.br/igce/matematica/bicmat), assim como o endereço para o envio do trabalho.

A responsabilidade de cada artigo é exclusiva do autor e respectivo orientador.