ISSN 1518-0352

Revista Ciências Exatas e Naturais

Volume 19 - Número 2 Julho/Dezembro 2017

Universidade Estadual do Centro-Oeste - UNICENTRO
Rua Simeão Camargo Varela de Sá,3
85040-080 - Guarapuava,Paraná
Brasil

Revista Ciências Exatas e Naturais

Publicação do
Setor de Ciências Exatas e de Tecnologia - UNICENTRO Campus
CEDETEG

Rua Simeão Camargo Varela de Sá, 3
85040-080 - Guarapuava, Paraná
Brasil
Fone: (42)3629-8116
Fax: (42)3629-8100
E-mail: recen.unicentro@gmail.com

FICHA CATALOGRÁFICA
(Catalogação na publicação - Biblioteca da UNICENTRO)

Revista Ciências Exatas e Naturais/Setor de
Ciências Exatas e de Tecnologia da Universidade Estadual do Centro-Oeste
-PR.-v.1,n.1 (1999) - Guarapuava: UNICENTRO, 2017-

Semestral

Até o n.1: Revista de Ciências Exatas e Naturais.
ISSN 1518-0352
1. Universidade Estadual do Centro-Oeste.
Setor de Ciências Exatas e de Tecnologia.

Indexada no Latindex, Sumários.org e PKP Harvester
e-ISSN 2175-5620

Revista Ciências Exatas e Naturais

Reitor
Aldo Nelson Bona

Vice-Reitor
Osmar Ambrósio de Souza

Diretora da Editora UNICENTRO
Denise Gabriel Witzel

Diretora do Setor de Ciências Exatas e de Tecnologia
Karina Worm Beckmann

Publicação aprovada pelo Conselho Editorial da UNICENTRO

Revista Ciências Exatas e Naturais

Edição
Editora UNICENTRO

Impressão
Gráfica da UNICENTRO

Diagramação
Thiago Kfouri De Angelis

Capa
Fernanda Pacheco de Moraes

Editorial

O Mestrado Profissional em Matemática em Rede Nacional – PROFMAT é um programa de mestrado na área de Matemática com oferta nacional, destinado a Professores de Matemática em exercício na Educação Básica, especialmente àqueles que atuam na rede pública de ensino.

O PROFMAT surgiu em 2011 em resposta a uma ação induzida pela CAPES junto à comunidade científica da área de Matemática, representada e coordenada pela Sociedade Brasileira de Matemática, responsável pela Coordenação Nacional do Programa desde então. Precursor no Brasil, esse programa proporcionou as bases de trabalho para implantação de outros programas de mestrado profissional da mesma natureza, como o ProfFis e o ProfHistória.

Atualmente, o PROFMAT conta com uma rede de 75 instituições associadas distribuídas em todas as regiões do Brasil, totalizando 100 cidades atendidas, contando com mais de três mil e quinhentos trabalhos concluídos. O PROFMAT é recomendado pela CAPES, reconhecido pelo Conselho Nacional de Educação e validado pelo Ministério da Educação com nota 5 (nota máxima para programas de mestrado).

O volume temático "PROFMAT" da Revista de Ciências Exatas e Naturais (RECEN) apresenta 9 artigos cujas pesquisas foram desenvolvidas durante a realização do mestrado profissional PROFMAT. Esses trabalhos versam sobre aspectos teóricos pertinentes ao ensino de Matemática; muitos deles trazem propostas didáticas ou exemplos para serem usados em sala de aula da Educação Básica e Superior. Todos artigos foram analisados por pareceristas ad hoc.

O artigo Diagrama de Voronoi nas Métricas Euclidiana e do Táxi: Uma Exploração em GeoGebra apresenta resultados teóricos relacionados ao Diagrama de Voronoi, ilustrando-os na ferramenta de geometria dinâmica citada. Os autores Paula Roberta Scaburi dos Santos e Andres David Baez-Sanchez finalizam o texto expondo sua crença na ligação entre as ideias apresentadas e conceitos desenvolvidos no Ensino Médio.

No texto Paradoxos Geométricos nas Aulas de Geometria, Rudimar Luiz Nós e Francielle Gonçalves Sentone expõem alguns paradoxos e resultados de aplicações em uma turma do Ensino Médio e uma da graduação (Licenciatura em Matemática), envolvendo os paradoxos de Curry e de Hooper. Concluem o artigo discutindo evidências da desvalorização da geometria nos currículos escolares.

No artigo Cifra de Hill: Uma Aplicação ao Estudo de Matrizes, Lucas Diego Antunes Barbosa e Mariana Garabini Cornelissen propõe aos professores de matemática do Ensino Médio a aplicação de matrizes a uma técnica de criptografia (codificação/decodificação). Os autores finalizam o trabalho examinando a potencialidade do uso de aplicações no ensino de Matemática.

José Silvino Dias e Mariana Garabini Cornelissen trazem o código corretor de erros usado pela nave espacial Mariner 9 ao transmitir fotos do planeta Marte à Terra, quando foi enviada ao espaço em 1971 pela NASA (National Aeronautics and Space Administration). Eloy Nicotera Junior e Sinuê Dayan Barbero Lodovici, no trabalho Uma Apresentação do Teorema de Mamikon, discutem alternativas geométricas para o cálculo de áreas com ilustrações construídas no aplicativo GeoGebra. Os autores entendem suas ideias como uma possibilidade de apresentação do Cálculo aos alunos do Ensino Médio, a qual poderia motivá-los no caminho das ciências exatas.

O trabalho Uma Introdução à Teoria dos Jogos, desenvolvido por David Jonnes Francez, procura mostrar, por meio de jogos, conceitos de soma-zero, estratégias, matriz de ganhos,

jogos estritamente e não estritamente determinados.

Em nosso sexto artigo, A Equação de Condução de Calor Uni e Bidimensional: Solução Usando Transformada Integral e o Método da Separação de Variáveis, Reynaldo D'Alessandro Neto e Antonio Luís Venezuela trazem um problema de matemática aplicada pertinente ao Ensino Superior, elucidando duas técnicas de resolução.

No trabalho Sistemas de Identificação Modular: Uma Aplicação no Ensino Fundamental, Fernanda Rodrigues Alves Costa e Marcelo Oliveira Veloso exploram sistemas de identificação modular na detecção de erros. Os autores encerram propondo uma sequência didática para o Ensino Fundamental, que usaria blocos lógicos.

No último artigo dessa edição, Igor Alvarenga da Silva Nascimento e Mário César Martins de Lima expõem aplicações de funções exponenciais para serem trabalhadas no Ensino Médio. Eles acreditam que por meio do ensino aplicado, conectado ao cotidiano, pode-se proporcionar interesse pelo conteúdo de Matemática.

Essa edição temática mostra uma pequena fração da diversidade dos trabalhos desenvolvidos no PROFMAT. Outros artigos estão sendo analisados e abrimos espaço para novas submissões para edições futuras. Desejamos que sejam proveitosos aos leitores.

Karine Feverzani Magnago
Comissão Editorial

Sumário

Diagrama de Voronoi nas Métricas Euclidiana e do Táxi: Uma Exploração em GeoGebra

Voronoi Diagram in Euclidian and Taxicab Metric: An Exploration Using GeoGebra

Paula Roberta Scaburi dos Santos
Secretaria de Estado da Educação, Santa Catarina
prof.paulascaburi@gmail.com

Andres David Baez-Sanchez
Universidade Tecnológica Federal do Paraná, Curitiba
adavidbaez@gmail.com

Resumo: Este trabalho apresenta uma exploração do conceito de diagrama de Voronoi na métrica Euclidiana e na métrica do táxi com a ajuda do ambiente de geometria dinâmica GeoGebra. São descritas visualizações dinâmicas para alguns resultados teóricos relacionados ao diagrama de Voronoi na métrica Euclidiana, assim como ilustrações dos conceitos de táxi-circunferência e táxi-mediatriz. Finalmente é implementado um procedimento para a representação das regiões de influência do diagrama de Voronoi na métrica do táxi.

Palavras-chave: diagrama de Voronoi; métrica Euclidiana; métrica do táxi; GeoGebra.

Abstract: This work presents an exploration of the Voronoi diagram in Euclidean and Taxicab metrics using the dynamic geometry environment GeoGebra. Using dynamic visualizations, some theoretical results related to Voronoi diagram in Euclidean metric are illustrated as well as the concepts of taxi-circumference and taxicab-bisector. Finally, a procedure is implemented to represent the regions of influence of the Voronoi diagram in the taxicab metric.

Key words: Voronoi diagram; Euclidian metric; táxicab metric; GeoGebra.

1 Introdução

A noção de diagrama de Voronoi de um conjunto de pontos P, pode ser relacionada à divisão do plano em um conjunto de regiões de influência, cada uma determinada pela *proximidade* entre os pontos da região e os pontos do conjunto P. As seguintes definições formalizam esta ideia:

Definição 1 *Dado um conjunto $P = \{p_1, p_2, ..., p_n\}$ de pontos e uma métrica d em $\mathbb{R}^2$, a* ***célula de Voronoi*** *$V_d(p_i)$ é definida como*

$$V_d(p_i) = \{q \in \mathbb{R}^2 : d(q, p_i) \leq d(q, p_j) \text{ para } j = 1, \ldots, n\}.$$

Recebido em 13/08/2017 - Aceito em 02/10/2017

Caso não haja lugar a equívocos em relação à métrica, será usada a notação $V(p_i)$ no lugar de $V_d(p_i)$. A seguinte definição introduz o conceito de diagrama de Voronoi de um conjunto de pontos.

Definição 2 *O* ***diagrama de Voronoi*** *de* $P = \{p_1, p_2, ..., p_n\}$*, denotado por* $Vor(P)$ *é definido como a união das fronteiras de todas as células de Voronoi* $V(p_i)$ *correspondentes aos pontos do conjunto* P*.*

Assim, cada célula de Voronoi $V(p_i)$ é o conjunto dos pontos que estão mais próximos ou à mesma distância de p_i do que de qualquer outro ponto de P e o diagrama de Voronoi $Vor(P)$ é a união das fronteiras de todas as células de Voronoi. As Figuras 1 e 2 ilustram estes conceitos considerando a métrica euclidiana.

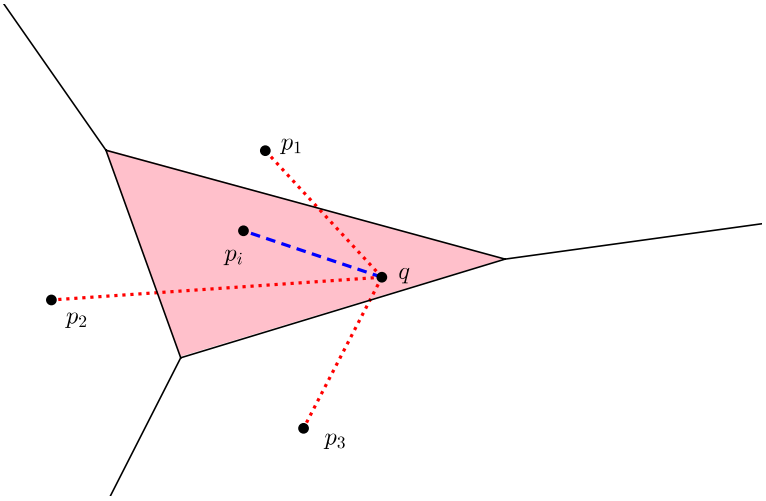


Figura 1. Célula de Voronoi $V(p_i)$

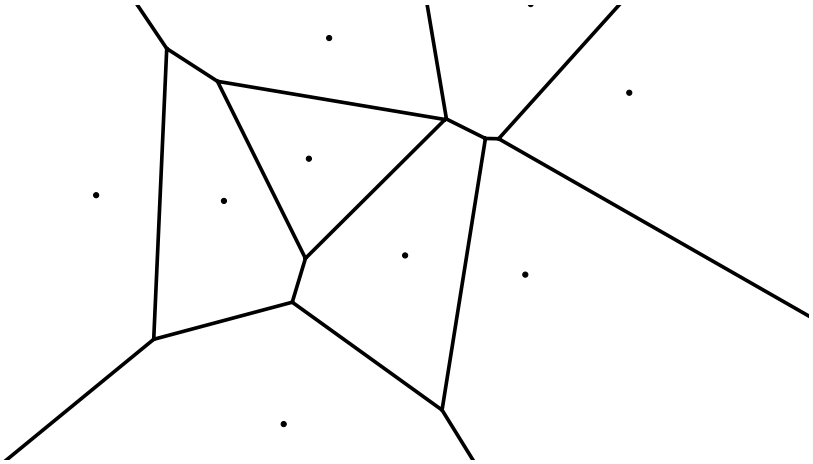


Figura 2. Diagrama de Voronoi $Vor(P)$

É possível encontrar na literatura definições diferentes das aqui apresentadas. Em [1] por exemplo, o diagrama de Voronoi é definido como o conjunto das células e não como a união

das fronteiras. Em [2] as células são definidas usando a desigualdade estrita $d(q, p_i) < d(q, p_j)$ no lugar da desigualdade $d(q, p_i) \leq d(q, p_j)$. Neste trabalho as definições apresentadas seguem as consideradas em [3].

Segundo [4], as primeiras apresentações formais do conceito do diagrama de Voronoi aparecem em trabalhos de Peter Gustav Lejeune Direchlet (1805-1859) e George Fedoseevich Voronoy (ou Voronoi) (1868-1908). Em 1854, o médico britânico John Snow utilizou uma ideia similar ao diagrama de Voronoi, para concluir que a maioria das pessoas que morreram na epidemia de cólera em Soho, distrito de Londres, moravam mais perto da bomba de água de Broad Street do que de qualquer outra bomba, mostrando assim a relação entre a água consumida e o surto da doença. Este fato é considerado como o início da epidemiologia moderna [5].

Estruturas relacionadas ao diagrama de Voronoi aparecem em várias áreas do conhecimento: astronomia, arqueologia, planejamento urbano, física, fisiologia, estudo de epidemias, ecologia, entre outras áreas [1]. O diagrama de Voronoi também é estudado na área de geometria computacional [3].

Este trabalho considera o uso do ambiente de geometria dinâmica GeoGebra para a exploração do conceito de diagrama de Voronoi na métrica Euclidiana e na métrica do táxi. Serão descritas algumas construções dinâmicas para ilustrar resultados teóricos relacionados ao diagrama na métrica Euclidiana, assim como visualizações dos conceitos de táxi-circunferência e táxi-mediatriz. Finalmente será considerado um procedimento para a representação das regiões de influência do diagrama de Voronoi na métrica do táxi.

2 Diagrama de Voronoi na métrica Euclidiana

A determinação explícita do diagrama de Voronoi na métrica Euclidiana, pode ser feita usando alguns dos vários algorítmos descritos na literatura [1, 2, 3] mas quando for considerado um conjunto com um, dois ou três pontos, é possível determinar o diagrama de Voronoi de forma simples.

2.1 Diagrama de Voronoi para um, dois ou três pontos

Quando houver apenas um ponto, a célula de Voronoi será o plano todo e o diagrama de Voronoi será vazio. Para dois pontos A e B, basta construir a mediatriz do segmento $\overline{AB}$. Sobre a mediatriz de $\overline{AB}$ estão os pontos que ficam a mesma distância dos dois pontos e as células de Voronoi são justamente os semiplanos fechados definidos pela mediatriz. O diagrama de Voronoi correspondente resulta ser a própria mediatriz do segmento formado pelos dois pontos.

Para três pontos, tem-se dois casos possíveis: pontos colineares ou não colineares. Considere primeiro o caso do diagrama de Voronoi para três pontos A, B, e C não colineares. Inicialmente são determinadas as mediatrizes dos segmentos $\overline{AB}$, $\overline{BC}$ e $\overline{CA}$ como ilustrado na Figura 3.

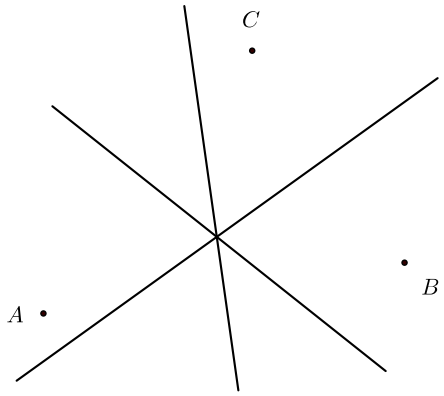


Figura 3. Construção das mediatrizes.

O ponto de encontro das mediatrizes é o ponto que está a mesma distância dos pontos A, B e C e será chamado de vértice do diagrama de Voronoi. Note que este ponto é justamente o circuncentro do triângulo ABC. Para determinar como serão as células de Voronoi para cada ponto, note que sobre a mediatriz do segmento formado por dois pontos, há pontos que estão mais próximos do terceiro ponto do que dos dois pontos que formam o segmento, assim esses pontos pertencem à região de influência do terceiro ponto. Basta eliminar então esses pontos em cada mediatriz para obter a representação adequada das células de Voronoi. Note, por exemplo, que para o ponto de influência A na Figura 3, a parte *inferior à esquerda* da mediatriz do segmento $\overline{BC}$ será desconsiderada, pois estes pontos estão mais próximos do ponto A e portanto pertencem a região de influência de A. O mesmo será feito com as outra mediatrizes conforme a Figura 4:

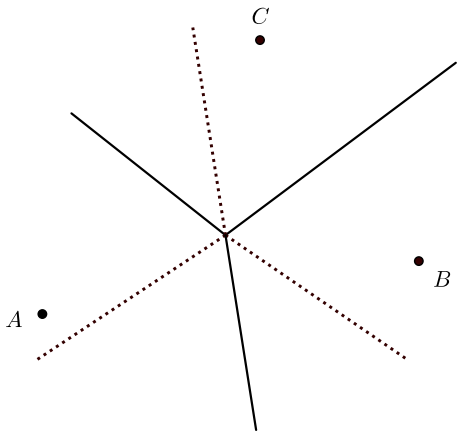


Figura 4. Eliminação dos segmentos que *invadem* as regiões de influência.

A figura restante, após a eliminação dos segmentos, será o diagrama de Voronoi para estes três pontos no plano.

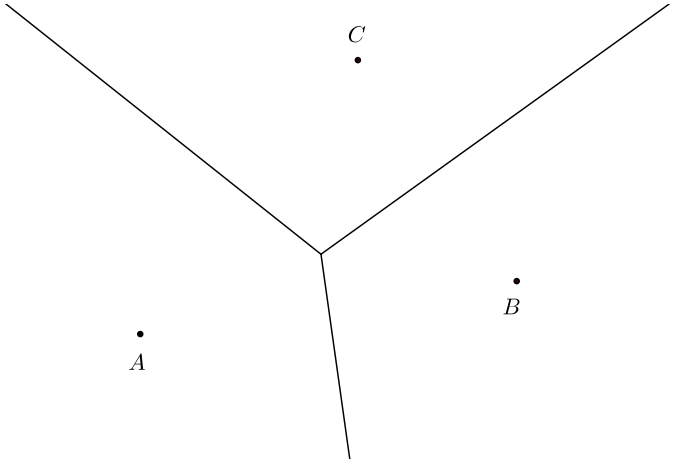


Figura 5. Diagrama de Voronoi para os pontos não colineares A, B e C.

Se os três pontos forem colineares, o diagrama de Voronoi será formado por retas (mediatrizes) paralelas. Isto será enunciado e ilustrado no Teorema 3.

Todas as figuras consideradas na discussão anterior foram geradas usando o GeoGebra, mas é possível usar este software para uma exploração mais dinâmica de outras propriedades do diagrama de Voronoi.

2.2 Usando o GeoGebra para explorar o diagrama de Voronoi na métrica Euclidiana

O diagrama de Voronoi na métrica Euclidiana pode ser gerado no GeoGebra usando os comandos **DiagramaDeVoronoi** ou **Voronoi** como é ilustrado na Figura 6.

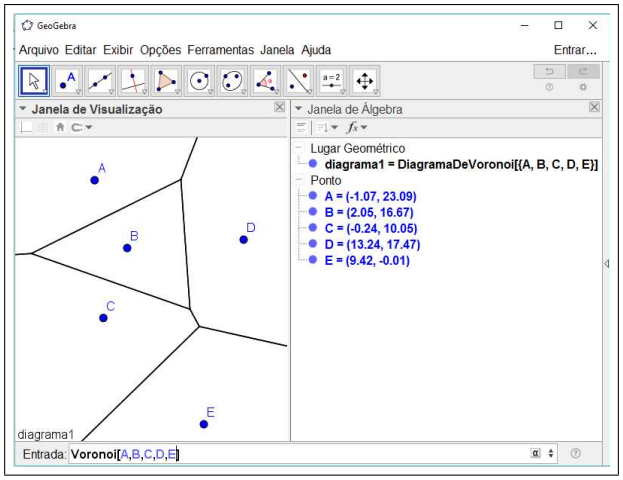


Figura 6. Diagrama de Voronoi na métrica Euclidiana no GeoGebra.

A seguir serão exploradas algumas propriedades do diagrama de Voronoi na métrica Euclidiana. As demonstrações das propriedades consideradas podem ser encontradas em [3]

ou [6].

Teorema 3 *Seja $P = \{p_1, p_2, ..., p_n\}$ um conjunto de pontos no plano. Se todos os pontos forem colineares o $Vor(P)$ consiste em $n-1$ linhas paralelas. Caso contrário, $Vor(P)$ é formado por segmentos de reta ou semirretas.*

Este resultado pode ser ilustrado com facilidade no GeoGebra manipulando diretamente os pontos considerados e o comando **Voronoi** ou com ajuda de um controle deslizante.

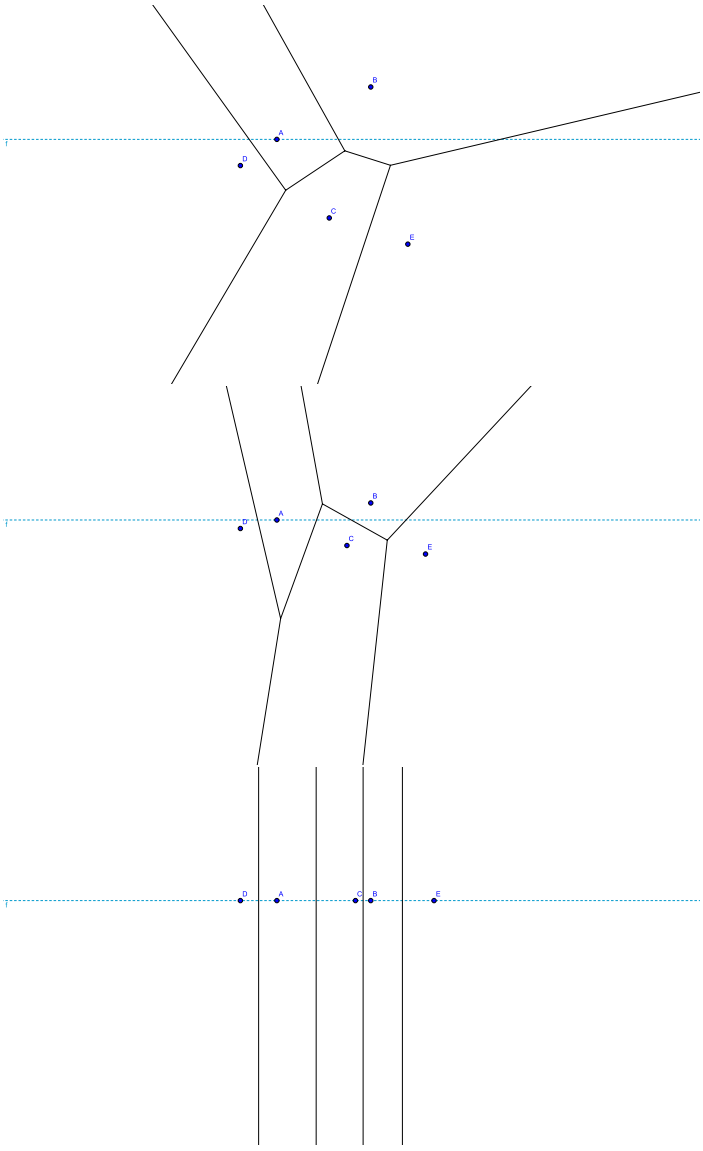


Figura 7. Diagrama de Voronoi: Pontos Não Colineares e Colineares.

Na Figura 7, note como quanto mais próximos os pontos encontram-se da reta f, os segmentos de reta no diagrama de Voronoi vão mudando sua inclinação até se tornarem retas paralelas. Uma construção dinâmica correspondente pode ser acessada em https://ggbm.at/c9E3hgjG.

Os próximos três teoremas permitem determinar, através de circunferências, se um ponto qualquer do plano é ponto interior de alguma célula, está sobre uma única aresta, ou é um dos vértices do diagrama de Voronoi de um conjunto de pontos $P = \{p_1, p_2, \ldots, p_n\}$. Para estabelecer a classificação, dado um ponto $p \notin P$ será usada a notação C_p para denotar um **círculo com centro p que não tem nenhum dos pontos do conjunto P no seu interior**.

Teorema 4 *Um ponto p é um ponto interior de $V(p_i)$ se e somente se existe um círculo C_p tal que p_i é o único ponto de P na fronteira de C_p.*

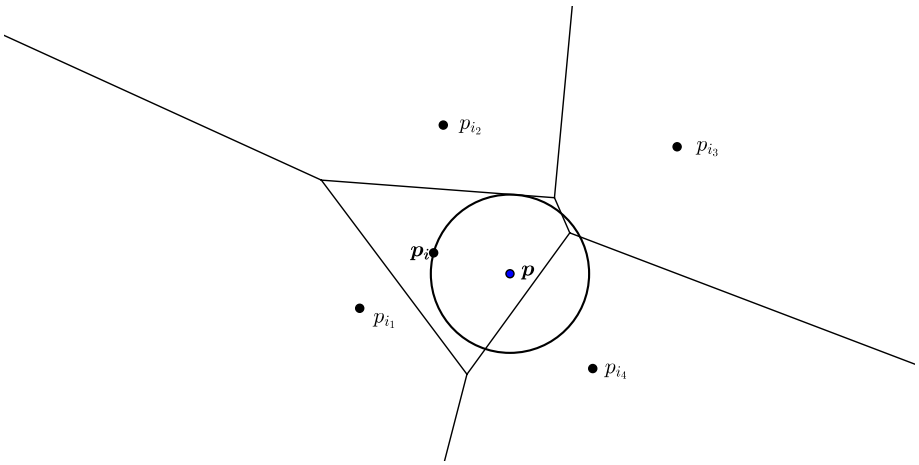


Figura 8. Ponto interior a p_i.

Note na Figura 8, que a circunferência em destaque, é a única com centro em p, que possui um ponto de P na fronteira e nenhum ponto de P no interior.

O Teorema 5 carateriza os pontos que pertencem exatamente a duas células de Voronoi, isto é, são pontos no interior relativo a uma das arestas e não são vértices.

Teorema 5 *Um ponto p é um ponto interior da aresta $V(p_i) \cap V(p_j)$ se, e somente se, existe um círculo C_p tal que exatamente os pontos p_i e p_j de P, estão na fronteira de C_p.*

Na Figura 9, é ilustrado o fato de que para um ponto p no interior da aresta é possível construir um círculo C_p com exatamente os pontos p_i e p_j na fronteira de C_p. A figura também ilustra o fato de que esta mesma propriedade é satisfeita por pontos p' e p'' sobre a aresta que estejam suficientemente *próximos* de p.

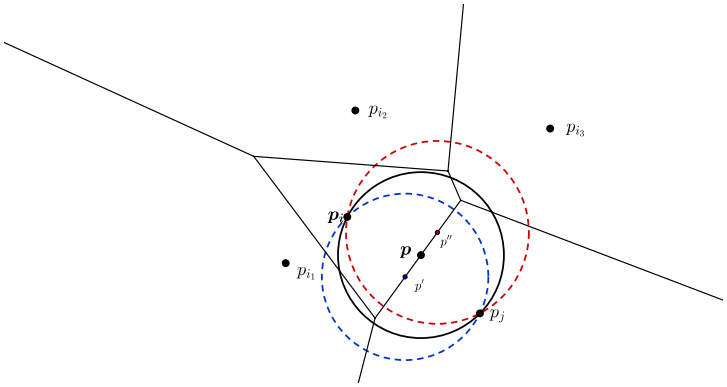


Figura 9. Pontos interiores a aresta de Voronoi.

Teorema 6 *Um ponto p é um vértice de Voronoi se, e somente se existe um círculo C_p tal que há pelo menos três pontos de P na fronteira de C_p.*

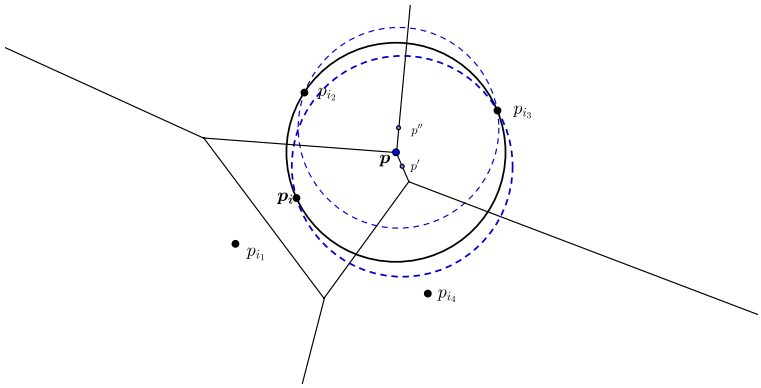


Figura 10. Ponto sobre o vértice de Voronoi.

Na Figura 10, é ilustrado o fato de que para um ponto p que seja vértice do diagrama é possível construir um círculo C_p com três ou mais pontos de P na fronteira. Note que os pontos p' e p'' *próximos* de p, não têm esta propriedade.

Além de usar o GeoGebra para a construção de gráficos, é possível utilizar as suas ferramentas para ilustrar dinamicamente os três teoremas anteriores simultaneamente. Um exemplo de uma construção dinâmica simples neste sentido pode ser encontrada em https://ggbm.at/JpnqZnPr.

O seguinte resultado, carateriza as células de Voronoi em termos do fecho convexo do conjunto P.

Teorema 7 *A célula de Voronoi $V(p_i)$ é ilimitada se, e somente se, p_i está na fronteira do fecho convexo de P.*

A demonstração deste resultado utiliza os teoremas anteriores de caraterização de pontos via circunferências [3]. É possível utilizar ferramentas básicas do GeoGebra para ilustrar diversas partes da demonstração [6] ou construir uma ilustração dinâmica do resul-

tado. Um exemplo de uma construção dinâmica neste sentido pode ser encontrada em https://ggbm.at/PdBm5BvQ.

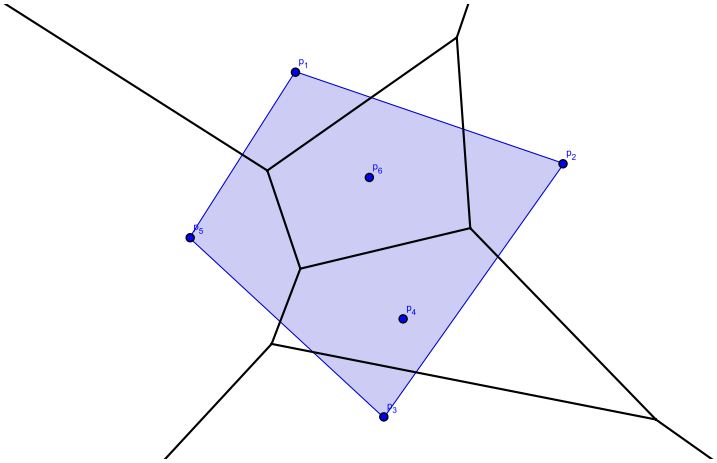


Figura 11. Células de Voronoi e Fecho Convexo de P.

3 Métrica do Táxi

Nesta seção será considerada a métrica do táxi. A métrica ou distância do táxi (também conhecida como métrica de Manhattan ou métrica L_1) d_T entre dois pontos $A = (x_a, y_a)$ e $B = (x_b, y_b)$ é definida como

$$d_T(A, B) = |x_a - x_b| + |y_a - y_b| \tag{1}$$

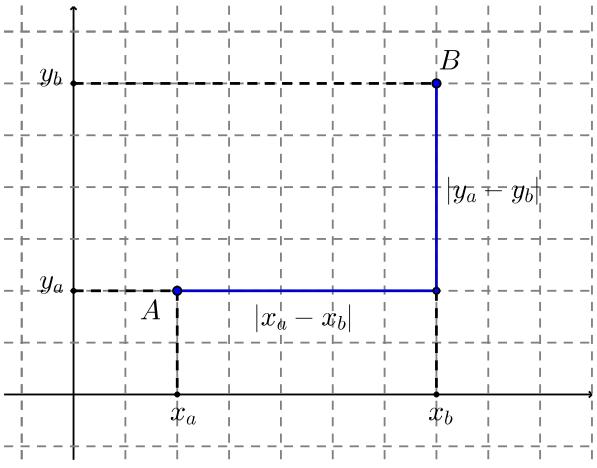


Figura 12. Distância ou métrica do táxi.

O nome de métrica do táxi é associado a esta métrica, pois numa região com ruas sempre paralelas ou ortogonais entre si, a distância total percorrida para ir de táxi do ponto A ao

ponto B é igual a soma das distâncias percorridas em deslocamentos *horizontais* mais a soma das distâncias percorridas em deslocamentos *verticais*. Mas no plano, esta soma é justamente a soma definida na Equação 1 como é ilustrado na Figura 12. Nosso objetivo final é utilizar o GeoGebra para visualizar o diagrama de Voronoi de um conjunto de pontos na métrica do táxi, mas como não existe uma ferramenta pronta em GeoGebra para este propósito, na seção seguinte será desenvolvido um procedimento de representação aproximado. Para entender adequadamente este procedimento, nesta seção serão considerados os conceitos correspondentes à circunferência e mediatriz entre dois pontos na métrica do táxi e com a ajuda do GeoGebra, serão exploradas algumas das suas características. Mais detalhes dos conceitos e demonstrações dos resultados considerados ao longo desta seção podem ser encontrados em [6, 8].

3.1 Táxi-Circunferência

A táxi-circunferência de centro C e raio r é o lugar geométrico dos pontos no plano que na métrica do táxi distam r unidades do ponto $C = (x_c, y_c)$. Assim, uma *táxi-circunferência* de raio r e centro $C = (x_c, y_c)$ é formada pelos pontos (x, y) que solucionam a equação:

$$|x - x_c| + |y - y_c| = r. \tag{2}$$

A seguinte proposição caracteriza este lugar geométrico.

Proposição 8 *A táxi-circunferência de centro $C = (x_c, y_c)$ e raio r é o quadrilátero de vértices $(x_c, y_c + r)$, $(x_c + r, y_c)$, $(x_c, y_c - r)$ e $(x_c - r, y_c)$.*

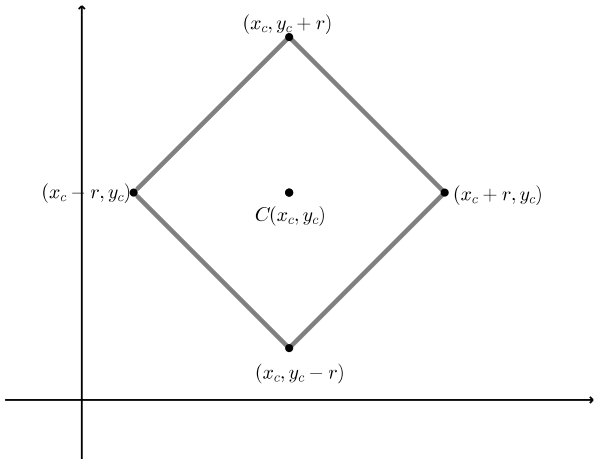


Figura 13. Táxi-circunferência.

A representação gráfica de uma táxi-circunferência também pode ser obtida no GeoGebra utilizando a expressão 2 como é ilustrado na Figura 14

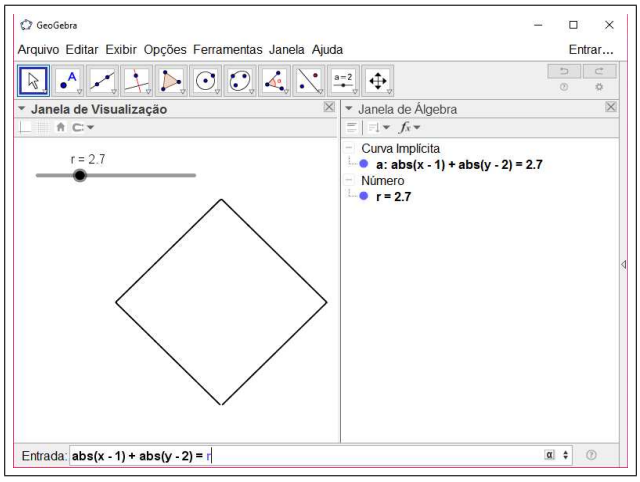


Figura 14. Táxi-circunferência no GeoGebra.

3.2 Táxi-mediatriz

A mediatriz entre os pontos A e B (ou mediatriz do segmento $\overline{AB}$) é definida como o lugar geométrico dos pontos P tais que $d(P, A)$ é igual a $d(P, B)$. Considerando a definição da métrica do Táxi, para $P = (x, y)$, $A = (x_a, y_a)$ e $B = (x_b, y_b)$ temos que P pertence à táxi-mediatriz de $\overline{AB}$ se, e somente se

$$|x - x_a| + |y - y_a| = |x - x_b| + |y - y_b|. \tag{3}$$

Em princípio, parece natural usar diretamente a expressão anterior para gerar no GeoGebra a táxi-mediatriz entre dois pontos, no entanto, veremos que esta implementação direta pode produzir uma representação um tanto confusa em certos casos. Nas Figuras 15 e 16 é ilustrado o uso direto da expressão 3 para gerar a representação da táxi-mediatriz em GeoGebra.

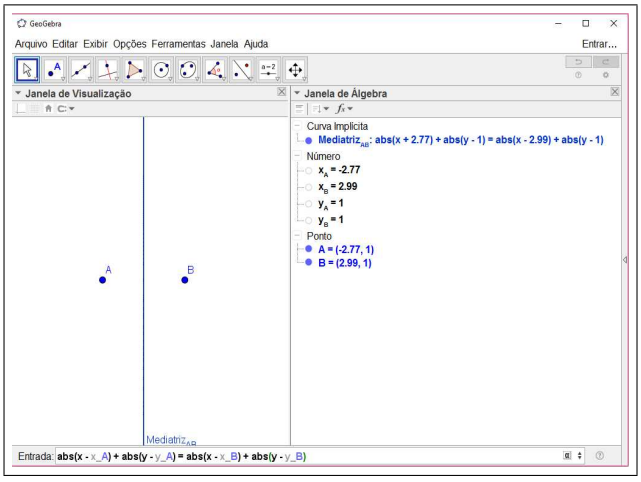


Figura 15. Táxi-Mediatriz no GeoGebra.

Note que, dependendo da posição relativa entre os pontos A e B, a táxi-mediatriz entre A e B pode ou não ser igual à mediatriz na métrica Euclidiana. Na Figura 15 a táxi-mediatriz coincide com a mediatriz na métrica Euclidiana, mas na Figura 16, a táxi-mediatriz é formada por um segmento de reta unido a duas semirretas. A representação específica dependerá da inclinação m entre os pontos A e B.

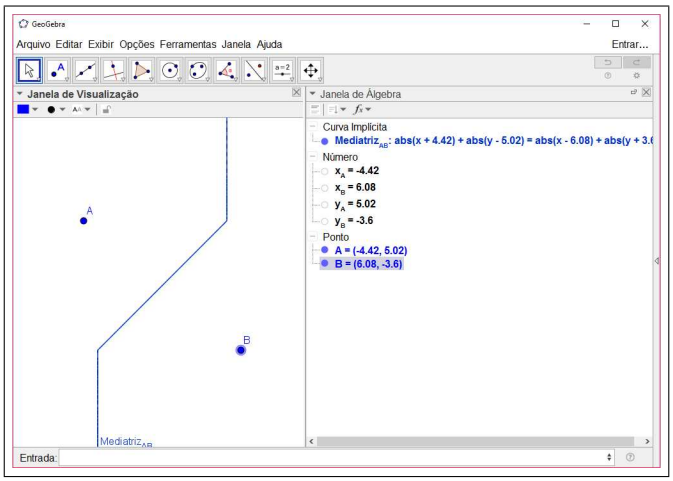


Figura 16. Táxi-Mediatriz no GeoGebra.

Usando diretamente a expressão (3) para gerar a representação da táxi-mediatriz no caso em que esta inclinação é igual a 1 ou -1 o resultado no GeoGebra pode parecer confuso, como sugerem as Figuras 17 e 18.

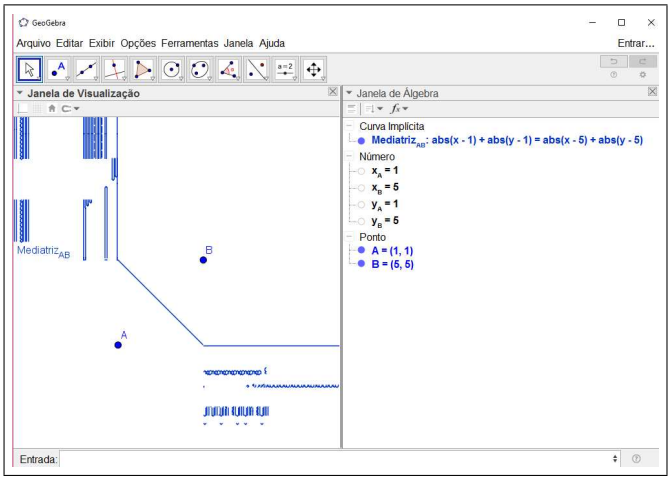


Figura 17. Táxi-Mediatriz em GeoGebra para $m = 1$.

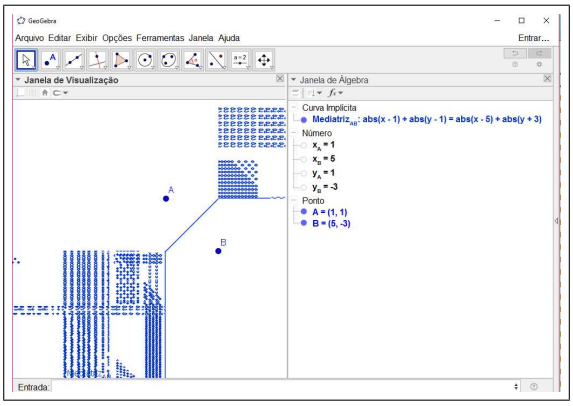


Figura 18. Táxi-Mediatriz no GeoGebra para $m = -1$.

Sem nenhum resultado teórico adicional, as representações apresentadas nas Figuras 17 e 18 são no mínimo confusas e podem até parecer fruto de algum erro. A implementação direta e simples da equação da táxi-mediatriz no GeoGebra, não permite identificar adequadamente o que acontece com a táxi-mediatriz quando $m = 1$ ou $m = -1$, como pode ser verificado na construção dinâmica disponível em https://ggbm.at/RVCjwEjB. A seguir, serão apresentados os resultados teóricos que estabelecem adequadamente as caraterísticas da táxi-mediatriz.

Proposição 9 *Dados dois pontos $A = (x_a, y_a)$ e $B = (x_b, y_b)$, seja m a inclinação do segmento $\overline{AB}$. Se $m = 0$ então a táxi-mediatriz entre A e B será a reta $x = \dfrac{x_a + x_b}{2}$. Se o segmento $\overline{AB}$ é vertical então m é indefinida e a táxi-mediatriz será a reta $y = \dfrac{y_a + y_b}{2}$.*

Note que neste caso a táxi-mediatriz coincide com a mediatriz na métrica Euclidiana. A Figura 19 ilustra este fato considerando dois pontos A e B e as distâncias entre os pontos P_1 e P_2 sobre a táxi-mediatriz e os pontos A e B.

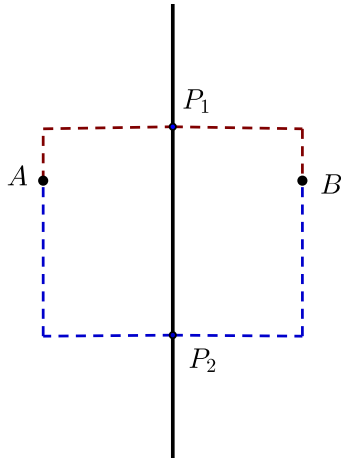


Figura 19. Táxi-mediatriz quando $m = 0$.

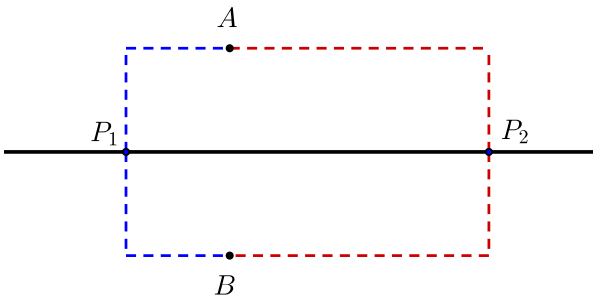


Figura 20. Táxi-mediatriz quando m é indefinido.

O seguinte resultado considera os casos em que $|m| \neq 1$ e $m \neq 0$. As Figuras 21 e 22 representam as típicas táxi-mediatrizes para $m > 1$ e $0 < m < 1$. Para um desenvolvimento mais construtivo deste resultado veja [6].

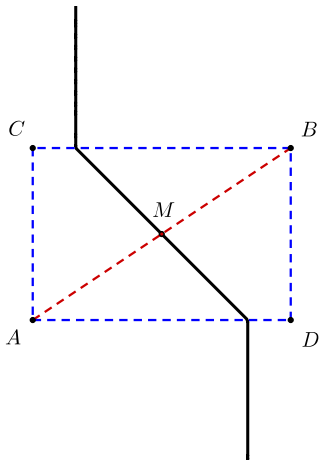


Figura 21. Táxi-mediatriz para $0 < m < 1$.

Proposição 10 *Dados dois pontos $A = (x_a, y_a)$ e $B = (x_b, y_b)$, seja m a inclinação do segmento $\overline{AB}$.*

- *Se $0 < m < 1$ então a táxi-mediatriz entre A e B é formada pelo segmento de reta entre os pontos $\left(x_a + \frac{(x_b - x_a)(1-m)}{2}, y_b\right)$ e $\left(x_a - \frac{(x_b - x_a)(1-m)}{2}, y_a\right)$, a parte da reta $x = x_a + \frac{(x_b - x_a)(1-m)}{2}$ correspondente a $y \geq y_b$ e a parte da reta $x = x_b - \frac{(x_b - x_a)(1-m)}{2}$ correspondente a $y \leq y_a$.*
- *Se $1 < m$ então a táxi-mediatriz entre A e B é formada pelo segmento de reta entre os pontos $\left(x_a, y_b - \frac{(x_b - x_a)(m-1)}{2}\right)$ e $\left(x_b, y_a + \frac{(x_b - x_a)(m-1)}{2}\right)$, a parte da reta*

$y = y_a + \frac{(x_b - x_a)(m-1)}{2}$ *correspondente a* $x \geq x_b$ *e a parte da reta* $y = y_b - \frac{(x_b - x_a)(m-1)}{2}$ *correspondente a* $x \leq x_a$.

- *Se* $-1 < m < 0$ *então a táxi-mediatriz entre* A *e* B *é formada pelo segmento de reta entre os pontos* $\left(x_a + \frac{(x_b - x_a)(1+m)}{2}, y_b\right)$ *e* $\left(x_a - \frac{(x_b - x_a)(1+m)}{2}, y_a\right)$, *a parte da reta* $x = x_a + \frac{(x_b - x_a)(1+m)}{2}$ *correspondente a* $y \leq y_b$ *e a parte da reta* $x = x_b - \frac{(x_b - x_a)(1+m)}{2}$ *correspondente a* $y \geq y_a$.

- *Se* $m < -1$ *então a táxi-mediatriz entre* A *e* B *é formada pelo segmento de reta entre os pontos* $\left(x_a, y_b + \frac{(x_b - x_a)(-m-1)}{2}\right)$ *e* $\left(x_b, y_a - \frac{(x_b - x_a)(-m-1)}{2}\right)$, *a parte da reta* $y = y_a - \frac{(x_b - x_a)(-m-1)}{2}$ *correspondente a* $x \geq x_b$ *e a parte da reta* $y = y_b + \frac{(x_b - x_a)(-m-1)}{2}$ *correspondente a* $x \leq x_a$.

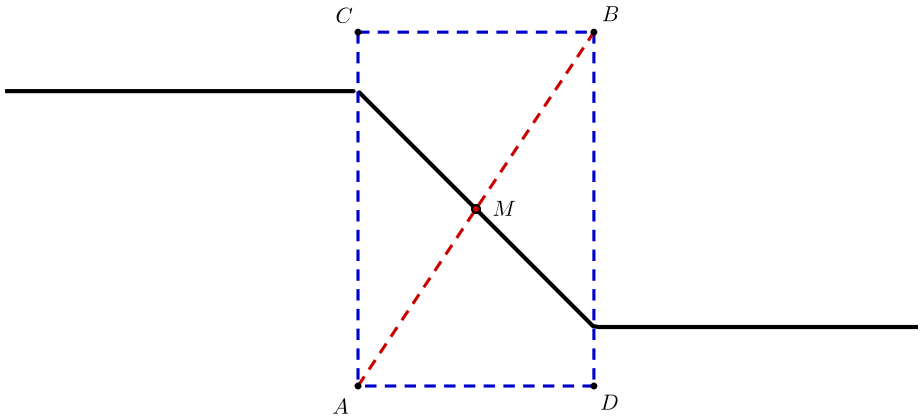


Figura 22. Táxi-mediatriz para $m > 1$.

A proposição seguinte considera o caso em que $|m| = 1$. Nesta situação a táxi-mediatriz não é formada apenas por retas ou segmentos de reta, sendo formada por um segmento de reta unido a dois *quadrantes do plano* como é ilustrado nas Figuras 23 e 24

Proposição 11 *A táxi-mediatriz de um segmento com inclinação* $|m| = 1$ *é formada pela união de um segmento de reta e dois quadrantes conforme os dois casos a seguir:*

- *Se* $m = 1$ *a táxi-mediatriz é formada pelos quadrantes* $(x \leq x_a,\ y \geq y_b)$ *e* $(x \geq x_b,\ y \leq y_a)$, *e pelo segmento da reta* $y = \frac{x_a + y_a + x_b + y_b}{2} - x$ *para* $x_a < x < x_b$.

- *Se* $m = -1$ *a táxi-mediatriz é formada pelos quadrantes* $(x \leq x_a,\ y \leq y_b)$ *e* $(x \geq x_b,\ y \geq y_a)$, *e pelo segmento da reta* $y = \frac{-x_a + y_a - x_b + y_b}{2} + x$ *para* $x_a < x < x_b$.

Com os conceitos anteriores sobre a táxi-mediatriz, é possível construir uma ilustração mais completa no GeoGebra, como por exemplo a disponível em https://ggbm.at/aAwc9pdJ [1].

[1] Autoria de Marco Antônio Manneta

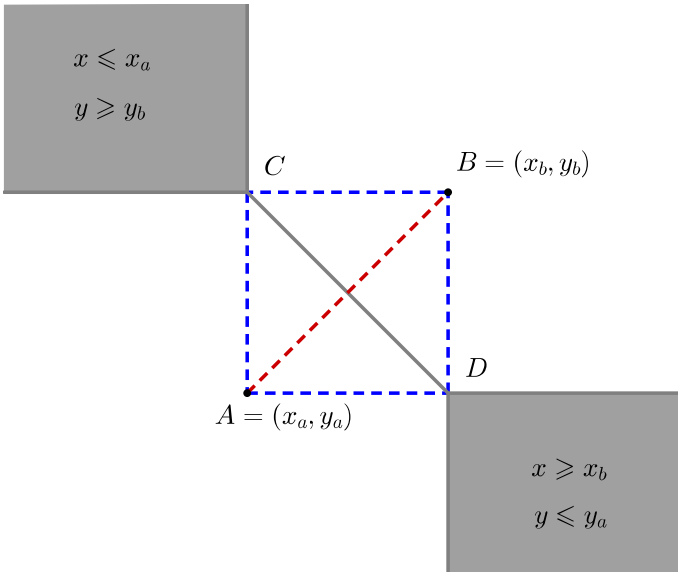


Figura 23. Táxi-mediatriz para $m = 1$.

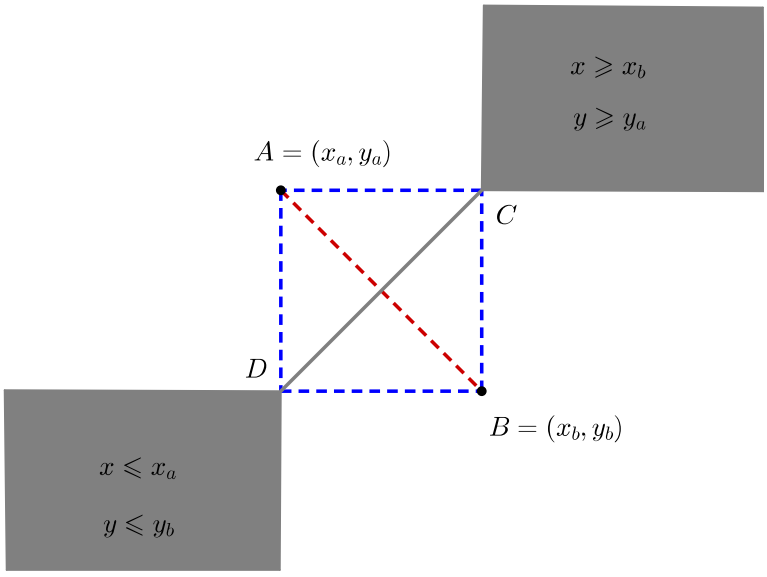


Figura 24. Táxi-mediatriz para $m = -1$.

4 Representação do diagrama de Voronoi na Métrica do Táxi

Nesta seção será apresentado um procedimento para obter uma representação do diagrama de Voronoi na métrica do táxi. A ideia é a seguinte: Inicialmente considere para cada ponto do conjunto $P = \{p_1, p_2, \cdots, p_n\}$ uma táxi-circunferência de centro em p_i e raio r.

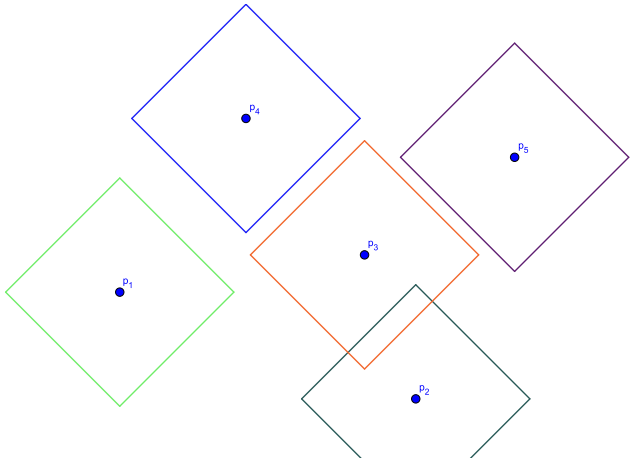


Figura 25. Táxi-Circunferências de centro em p_i e raio r.

Considere também que o raio r varia de forma contínua sobre o intervalo $[0, \infty)$. Quando $r = 0$, o único ponto sobre a táxi-circunferência é o próprio ponto p_i, mas quando r vai aumentando, qualquer ponto p do plano estará em algum momento sobre a circunferência correspondente ao ponto p_i.

A primeira vez que p estiver sobre a táxi-circunferência de centro em p_i, para algum i, isto seria equivalente a dizer que p está mais próximo ou pelo menos a mesma distância de p_i do que de qualquer outro ponto p_j, ou seja, p pertence à célula de Voronoi $V(p_i)$ se é atingido primeiro pela circunferência correspondente a p_i. Por outro lado, se fosse possível que r toma-se como valor inicial ∞ e fosse decrescendo até 0, então todos os pontos estariam em algum momento sobre cada táxi-circunferências, mas só a última vez que um ponto p fosse *tocado* por uma táxi-circunferência com centro em algum p_i, isto significaria que p seria um elemento da célula associada ao ponto p_i.

É possível emular esta ideia no GeoGebra com o uso de cores dinâmicas e utilizando a opção de rastro para as táxi-circunferências. É claro que não é possível inicializar r no valor ∞ mas para uma escolha inicial suficientemente grande, é possível obter uma representação aproximada do diagrama de Voronoi.

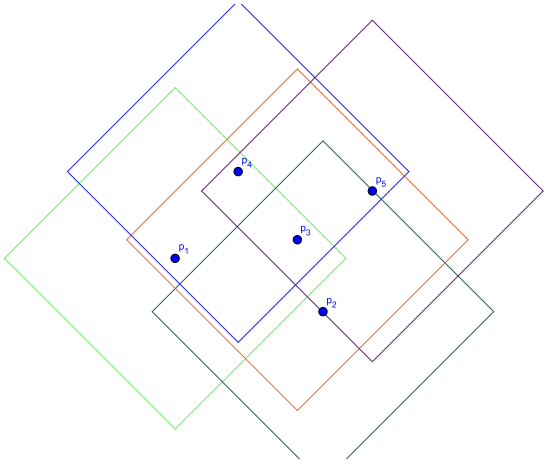


Figura 26. Representação do Diagrama de Voronoi na métrica do Táxi

No exemplo ilustrado na Figura 26 foi considerado r com valor inicial 13. A Figura 27 mostra a situação quando quando $r = 4$, e é possível notar como o rastro deixado pelas táxi-circunferências vai colorindo diversos pontos do plano e as células correspondentes a cada ponto começam a ser esboçadas. Um mesmo ponto pode ter diferentes cores em diferentes momentos, mas a cor deixada pela última circunferência que o atinge, indicará a célula de Voronoi a qual pertence.

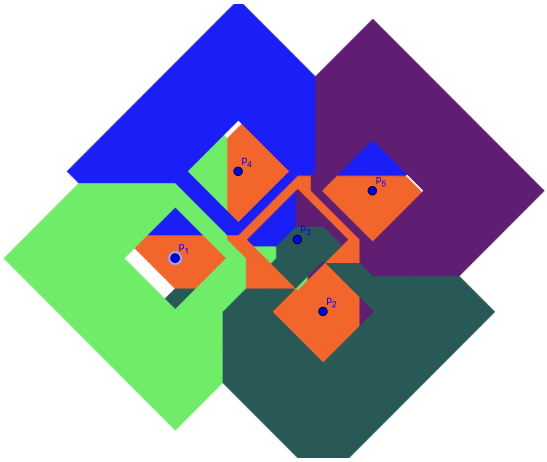


Figura 27. Representação do Diagrama de Voronoi na métrica do Táxi.

Na Figura 28 aparece o resultado final deste processo: uma representação aproximada do diagrama de Voronoi na métrica do táxi para $P = \{p_1, p_2, p_3, p_4, p_5\}$.

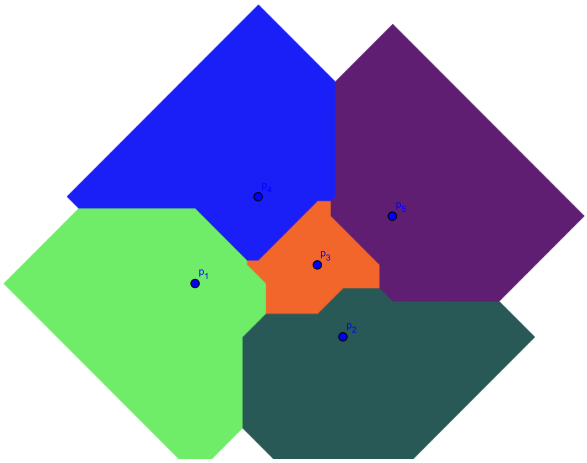


Figura 28. Representação do Diagrama de Voronoi na métrica do Táxi.

A partir da Figura 28, é possível ver que no caso da métrica do táxi, as células não são necessariamente regiões convexas. A Figura 28 parece sugerir também que as células ilimitadas correspondem a pontos p_i na fronteira do fecho convexo de P, mas como é ilustrado na Figura 29, esto não é necessariamente verdade. O procedimento descrito anteriormente pode ser explorado na animação disponível em https://ggbm.at/US6vBbV4.

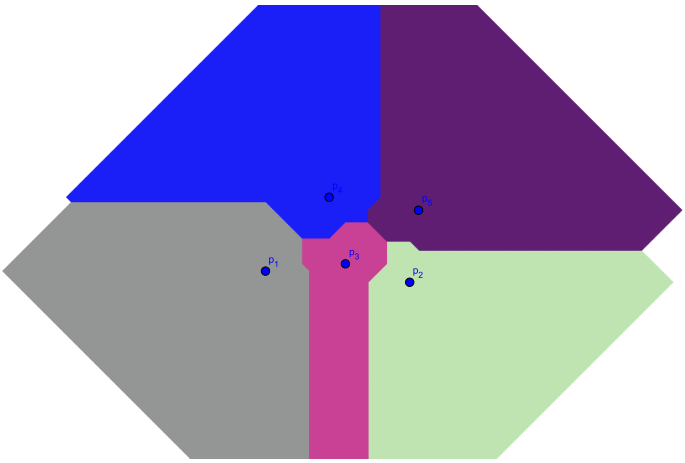


Figura 29. Célulás ilimitadas não correspondem a pontos na fronteira do fecho convexo.

5 Comentários Finais

Ao longo do trabalho foi descrita a utilização do GeoGebra, tanto para ilustrar resultados teóricos relacionados ao diagrama de Voronoi na métrica euclidiana, como para a exploração dos conceitos de táxi-circunferência e táxi-mediatriz. Estes resultados e conceitos estão baseados em ideias simples, mas nem sempre é imediata a sua compreensão. O uso do GeoGebra permite aprimorar a compreensão destes conceitos. Foi ilustrado também, que uma implementação direta no GeoGebra da equação da táxi-mediatriz, poderia levar a confusões sem

a adequada fundamentação teórica. Foi descrito também como GeoGebra pode ser usado para produzir uma representação do diagrama de Voronoi na métrica do táxi. É importante destacar que este procedimento de representação pode ser estendido a outras métricas, se há uma construção adequada da circunferência correspondente. Finalmente, queremos destacar que as ligações entre as ideias aqui discutidas e alguns conceitos considerados no ensino médio, permitem ao professor de Matemática estabelecer situações-problemas interessantes, com aplicações diretas de conceitos geométricos e que quando desenvolvidas com ajuda de ferramentas computacionais como GeoGebra, podem estimular o processo de aprendizado.

Referências

[1] OKABE, A.; BOOTS, B.; SUGIHARA, K.; CHIU, S. N. Spatial Tessellations: Concepts and Applications of Voronoi Diagrams. Wiley Series in Probability and Statistics, 2009.

[2] BERG, M. Computational Geometry: Algorithms and Applications. Springer, 2008.

[3] FIGUEIREDO, L. H.; CARVALHO, P. C. P. Notas de Geometria Computacional. IMPA, 2009.

[4] LIEBLING, T. M.; POURNIN, L. Voronoi Diagrams and Delaunay Triangulations: Ubiquitous Siamese Twins. *Documenta Mathematica*, Extra Volume ISMP, p.419-431, 2012.

[5] JOHNSON, S. O mapa fantasma: Como a luta de dois homens contra a cólera mudou o destino de nossas metrópoles. Zahar, 2008.

[6] SANTOS, P. S. Diagrama de Voronoi: Uma exploração nas distâncias Euclidiana e do táxi. Dissertação de Mestrado, Mestrado Profissional em Matemática em Rede Nacional PROFMAT, 2016.

[7] KRAUSE, E. F. Taxicab Geometry: An Adventure in Non-Euclidean Geometry. Dover Publications, 1986.

[8] WANDERLEY A. J. M.; CARNEIRO J. P. Q. e WAGNER E. Como melhorar a vida de um casal usando geometria não-euclidiana. *Revista do Professor de Matemática*, v.50, p.23-30, 2001.

Paradoxos Geométricos nas Aulas de Geometria

Geometric Paradoxes in Geometry Classes

Rudimar Luiz Nós
Universidade Tecnológica Federal do Paraná - UTFPR, Curitiba, PR
rudimarnos@utfpr.edu.br

Francielle Gonçalves Sentone
Escola Estadual Professora Abigail dos Santos Corrêa, Matinhos, PR
fran.sentone@gmail.com

Resumo: Apresentamos neste trabalho alguns paradoxos geométricos, assim como as atividades sobre os paradoxos de Curry e de Hooper aplicadas em turmas da Educação Básica e do Ensino Superior com o intuito de investigar, através de uma atividade recreativa e de um questionário, como os estudantes empregam conceitos e definições para solucionar problemas geométricos. As atividades evidenciaram a formação deficiente dos estudantes do Ensino Fundamental e do Ensino Médio em Geometria Plana e em Geometria Analítica e concluímos que os professores de matemática poderiam empregar a Matemática Recreativa para motivar a aprendizagem.

Palavras-chave: Matemática Recreativa; paradoxo do tabuleiro; paradoxo de Curry; paradoxo de Hooper.

Abstract: We present in this work some geometric paradoxes as well as the activities about the Curry and Hooper paradoxes applied in classes of basic and higher education in order to investigate, through a recreational activity and a questionnaire, how students use concepts and definitions to solve geometric problems. The activities revealed the deficient formation of the elementary and high school students in Plane Geometry and in Analytic Geometry and we concluded that mathematics teachers could use Recreational Mathematics to motivate learning.

Key words: Recreational Mathematics; the checkerboard paradox; Curry's paradox; Hooper's paradox.

1 Introdução

Um paradoxo é uma declaração que vai contra o senso comum, expectativas ou definições; é uma proposição que, apesar de aparentar um raciocínio coerente, demonstra falta de lógica. A palavra paradoxo provém do grego *paradoksos*: o prefixo *para* significa contrário a, ou oposto de, e o sufixo *doxo*, opinião. No latim, *paradoxum* é uma sentença que se opõe à opinião comum. Bons exemplos são o paradoxo do mentiroso, cuja primeira versão conhecida é atribuída a Eubulides de Mileto (século IV a.C.) [1], o paradoxo do altruísta e o paradoxo do Tangram, este um paradoxo geométrico.

Paradoxo 1.1 (Paradoxo do mentiroso) *Um homem diz que está mentindo. O que ele*

Recebido em 08/08/2017 - Aceito em 29/09/2017
RECEN 19(2) p.134-151 jul/dez 2017 DOI:10.5935/RECEN.2017.02.02

diz é verdadeiro ou falso?

- Se o homem está mentindo, o que ele diz é verdadeiro. Logo, ele não é mentiroso. Contraditório!
- Se o homem não está mentindo, o que ele diz é falso. Logo, ele é mentiroso. Contraditório novamente.

Paradoxo 1.2 (Paradoxo do altruísta) *Uma pessoa é altruísta se não pensa em si mesma. Considere um indivíduo que pensa em uma pessoa somente se ela é altruísta.*

- Se o indivíduo é altruísta, então ele pensa em si mesmo. Logo, ele não é altruísta. Contraditório!
- Se o indivíduo não é altruísta, então ele não pensa em si mesmo. Logo, ele é altruísta. Novamente, contraditório.

Paradoxo 1.3 (Paradoxo do Tangram) *Na Figura 1, qual das duas gravuras de um chinês tem a maior área?*

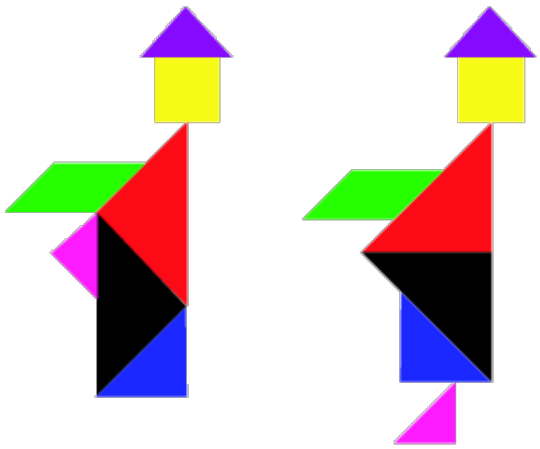


Figura 1. Paradoxo do Tangram [2]

- O Tangram é um antigo quebra-cabeça chinês composto por sete peças que formam um quadrado. O mesmo conjunto de peças do Tangram pode produzir duas figuras com áreas aparentemente diferentes, uma das quais é um subconjunto apropriado da outra, como na Figura 1. Essa contradição foi denominada *paradoxo do Tangram* [3].

Para [4], os melhores paradoxos são os mais fáceis de afirmar e os mais difíceis de resolver. Então, solucionar um paradoxo seria como desvendar um truque? Seria mágica? Poderíamos, enquanto professores de matemática, empregar paradoxos para introduzir/investigar conceitos, principalmente geométricos? Segundo [5], a resposta é sim, pois "Os Paradoxos Geométricos são tratados na Matemática Recreativa, desenvolvendo habilidades de raciocínio matemático por parte do aluno, tornando a Matemática e o raciocínio lógico dedutivo mais atrativos".

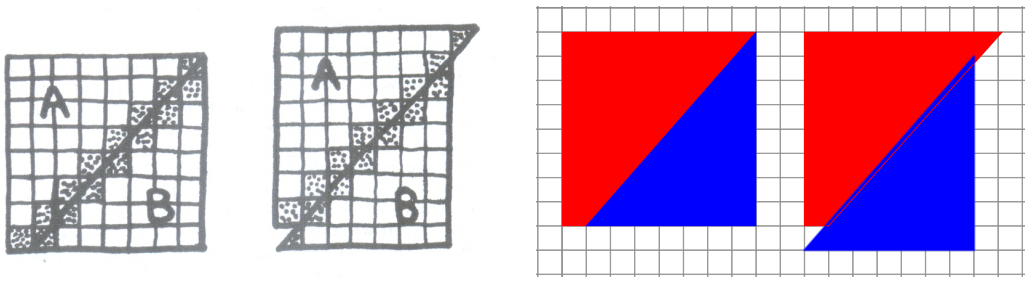
Dessa forma, inspirados principalmente por [6], propusemo-nos a apresentar alguns paradoxos geométricos para estudantes da Educação Básica e do Ensino Superior. O objetivo do trabalho é investigar como os estudantes do Ensino Fundamental, do Ensino Médio e do Curso de Licenciatura em Matemática empregam conceitos de Geometria Plana e de Geometria Analítica, tais como área, o Teorema de Pitágoras e o coeficiente angular da reta, para desvendar os paradoxos ou truques geométricos e, também, motivá-los para o estudo desses conceitos. Todas as figuras empregadas no texto para desvendar os truques geométricos foram construídas no GeoGebra [7].

2 Desenvolvimento

2.1 O paradoxo do tabuleiro

O paradoxo do tabuleiro (*The checkerboard paradox*) é um paradoxo no qual o princípio da distribuição oculta [6, 8] é responsável por misteriosos "ganhos" ou "perdas" de áreas.

Na Figura 2(a), temos à esquerda um tabuleiro quadrado 8×8 com área igual a 64. Esse tabuleiro é cortado em duas partes que, reencaixadas, formam a figura à direita com área igual a 63. Na manipulação, uma unidade de área some.



(a) Paradoxo do tabuleiro [6] (b) Construção do paradoxo do tabuleiro

Figura 2. Desvendando o paradoxo do tabuleiro

A explicação para o truque é que o tabuleiro não é cortado segundo sua diagonal. Ele é cortado do último quadrado da primeira linha até o segundo quadrado da última linha. Devido a este corte, cada quadrado cortado não foi cortado ao meio, mas sim de maneira que, quando deslocados, pareçam quadrados como os demais, mas não são. E quando deslocamos as peças de maneira que se encaixem, percebemos, como na Figura 2(b), que as duas peças se sobrepõem e a área da região sobreposta é a área do quadrado que sumiu.

2.2 O paradoxo de Curry

O paradoxo de Curry é uma ilusão de ótica com figuras geométricas planas criado pelo famoso mágico amador norte-americano Paul Jerome Curry (1917-1986). Devido à ilusão, muitos autores não o consideram um paradoxo geométrico. No paradoxo do quadrado perdido, como também é chamado, quatro figuras são reagrupadas de maneira a faltar um quadrado, como ilustra a Figura 3.

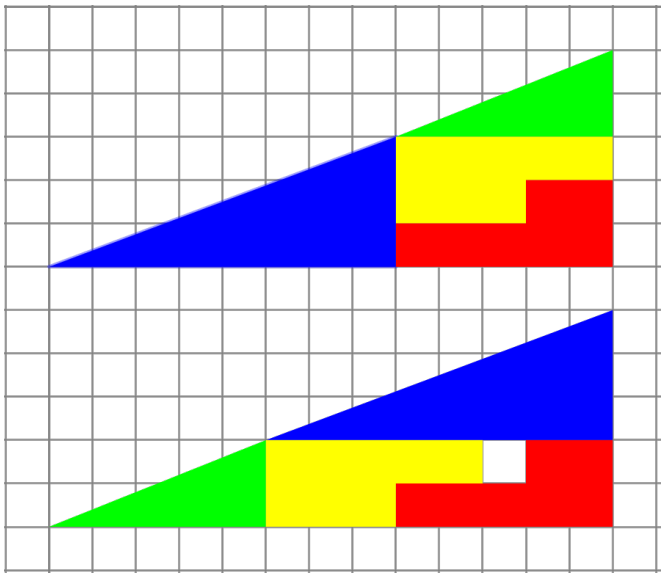


Figura 3. Paradoxo de Curry: o enigma do quadrado perdido

Para desvendar o paradoxo de Curry, podemos empregar conceitos geométricos, tais como o cálculo de áreas, o Teorema de Pitágoras, a semelhança de triângulos e a declividade da reta, e de Teoria dos Números, como a sequência de Fibonacci. O emprego destes conceitos conduz à conclusão de que os triângulos retângulos de catetos de medidas $5uc$ e $13uc$ da Figura 3 são uma ilusão de ótica. Na verdade, eles são quadriláteros é há uma diferença de áreas, como comprova a Figura 4.

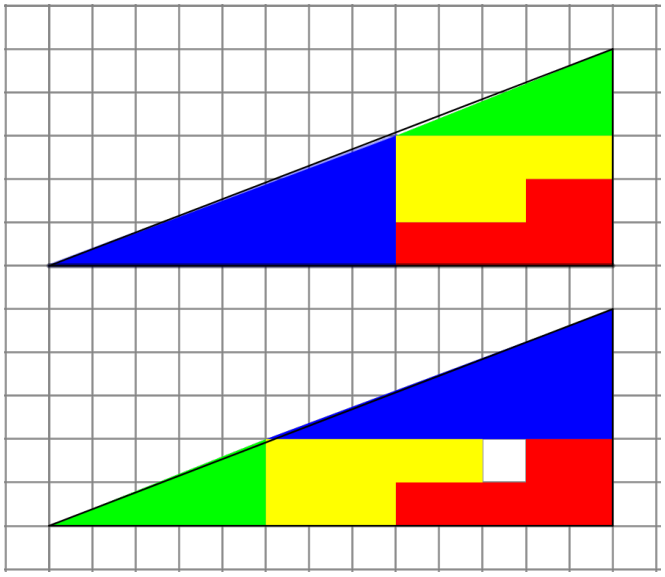


Figura 4. Desvendando o paradoxo de Curry

2.2.1 Área

Na Figura 3, temos, a princípio, dois triângulos retângulos de medidas congruentes, compostos pelas mesmas quatro peças, porém com um quadrado a menos. Mas como é possível dois triângulos com as mesmas medidas terem áreas diferentes?

Para [9, 10] isto não é possível.

> "Intuitivamente, a área de uma região no plano é um número positivo que associamos à mesma e serve para quantificar o espaço por ela ocupado. Para encontrar a área de uma figura F, devemos comparar sua superfície, espaço ocupado, com a de outra figura tomada como unidade. O resultado será um número que exprime quantas unidades de área está contida na figura F. Para o conceito de área ter validade, uma das propriedades válidas afirma que polígonos congruentes têm áreas iguais".

Considerando os triângulos da Figura 3, "para que sejam congruentes devemos deslocar um deles no espaço, sem deformá-lo, até coincidir com o outro" [9]. Ao deslocarmos um triângulo de maneira a fazê-lo coincidir com o outro, a área do quadrado faltante não será comum a ambos os triângulos. Logo, os triângulos não são congruentes uma vez que não têm a mesma área.

Para calcular as áreas das partes dos triângulos da Figura 3 usaremos como unidade de medida o quadrado unitário, ou seja, o quadrado que tem o lado medindo uma unidade de comprimento, representada por $1uc$, e área igual a uma unidade de área, representada por $1ua$. Assim, o triângulo retângulo cujos catetos medem $5uc$ e $13uc$, doravante denominado triângulo 5×13, tem $32,5$ quadrados unitários, ou seja, tem área igual a $32,5ua$. Calculando a área de todas as partes desse triângulo, temos que:

1. Área do triângulo retângulo 3×8: $\dfrac{3\times8}{2}=12ua$;
2. Área do triângulo retângulo 2×5: $\dfrac{2\times5}{2}=5ua$;
3. Área dos polígonos não-convexos: $3+5=8ua$ e $2+5=7ua$.

Somando as áreas das peças, determinamos uma área total de $32ua$. Há uma falta de $0,5ua$ para a área do triângulo 5×13. Portanto, essas quatro peças não podem formar o triângulo 5×13.

2.2.2 O Teorema de Pitágoras

Já temos uma primeira inconsistência em relação às áreas. Verifiquemos então se a hipotenusa h_1 do triângulo retângulo 5×13 equivale à soma das hipotenusas h_2 e h_3 dos triângulos retângulos 3×8 e 2×5, respectivamente. Usaremos para tanto o Teorema de Pitágoras. Este teorema é enunciado em [10] como "um dos mais belos e importantes teoremas da Matemática de todos os tempos".

Teorema 2.1 (Teorema de Pitágoras) *Em qualquer triângulo retângulo, a área do quadrado cujo lado é a hipotenusa é igual à soma das áreas dos quadrados que têm como lados cada um dos catetos.*

Empregando o Teorema 2.1, constatamos que:

1. Hipotenusa h_1 do triângulo retângulo 5×13: ${h_1}^2 = 5^2 + 13^2 \Rightarrow h_1 = \sqrt{194}$;
2. Hipotenusa h_2 do triângulo retângulo 3×8: ${h_2}^2 = 3^2 + 8^2 \Rightarrow h_2 = \sqrt{73}$;
3. Hipotenusa h_3 do triângulo retângulo 2×5: ${h_3}^2 = 2^2 + 5^2 \Rightarrow h_3 = \sqrt{29}$.

Estamos supondo que $h_1 = h_2 + h_3$. Logo:

$$\begin{aligned} h_1 &= h_2 + h_3; \\ \sqrt{194} &= \sqrt{73} + \sqrt{29}; \\ \left(\sqrt{194}\right)^2 &= \left(\sqrt{73} + \sqrt{29}\right)^2; \\ 194 &= 73 + 29 + 2\sqrt{73 \times 29}; \\ 194 - 73 - 29 &= 2\sqrt{73 \times 29}; \\ \frac{92}{2} &= \sqrt{73 \times 29}; \\ 46^2 &= \left(\sqrt{73 \times 29}\right)^2; \\ 2116 &= 2117. \end{aligned} \tag{1}$$

A igualdade (1) é uma contradição. Assim, a hipotenusa h_1 do triângulo retângulo 5×13 não equivale à soma das hipotenusas h_2 e h_3 dos triângulos retângulos 3×8 e 2×5, respectivamente.

2.2.3 Semelhança de triângulos

Após constatarmos outra inconsistência de medidas, investiguemos agora se os triângulos retângulos 5×13, 3×8 e 2×5 são semelhantes. A semelhança de triângulos é definida em [11] como a seguir.

Definição 2.1 *Dois triângulos são semelhantes se, e somente se, possuem os três ângulos internos ordenadamente congruentes e os lados homólogos proporcionais.*

Dessa forma, se dois pares de lados correspondentes forem proporcionais, então os ângulos internos correspondentes serão congruentes e dois triângulos serão semelhantes. Comparemos os três triângulos retângulos da Figura 3.

1. Triângulos retângulos 5×13 e 3×8:

$$\frac{5}{3} = \frac{13}{8}. \tag{2}$$

A igualdade (2) não é verdadeira, uma vez que para tal, 40 deveria ser igual a 39.

2. Triângulos retângulos 5×13 e 2×5:

$$\frac{5}{2} = \frac{13}{5}. \tag{3}$$

A igualdade (3) não é verdadeira, uma vez que para tal, 25 deveria ser igual a 26.

3. Triângulos retângulos 3×8 e 2×5:

$$\frac{3}{2} = \frac{8}{5}. \tag{4}$$

A igualdade (4) não é verdadeira, uma vez que para tal, 15 deveria ser igual a 16.

As igualdades (2), (3) e (4) são falsas. Dessa forma, os triângulos retângulos não são semelhantes.

2.2.4 Declividade da reta

Depois da terceira inconsistência de medidas, analisemos se a reta suporte da hipotenusa h_1 do triângulo retângulo 5×13 é a reta suporte das hipotenusas h_2 e h_3 dos triângulos retângulos 3×8 e 2×5, respectivamente. Isto equivale a verificar inicialmente se as retas suportes têm a mesma declividade. Os triângulos retângulos da Figura 3 sugerem que a reta suporte das três hipotenusas é a mesma. O coeficiente angular de uma reta r, ilustrada na Figura 5, é definido por [12] da forma que segue.

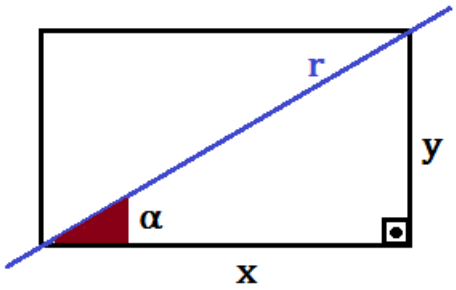


Figura 5. Declividade da reta r: coeficiente angular $m = \tan\alpha = \dfrac{y}{x} = \dfrac{sen\alpha}{cos\alpha}$

Definição 2.2 *O coeficiente angular de uma reta r não perpendicular ao eixo das abcissas é o número real m tal que*

$$m = \tan\alpha = \frac{sen\alpha}{cos\alpha}. \tag{5}$$

A partir da igualdade (5), podemos determinar a medida do ângulo α de inclinação da reta r:

$$\alpha = \arctan\left(\frac{y}{x}\right). \tag{6}$$

Empregando as relações (5) e (6), obtemos:

1. Coeficiente angular m_1 da reta suporte da hipotenusa h_1: $m_1 = \dfrac{5}{13} \approx 0,385$;

   Ângulo de inclinação α_1 da reta suporte de h_1: $\alpha_1 = \arctan\left(\dfrac{5}{13}\right) \approx 21,04°$;

2. Coeficiente angular m_2 da reta suporte da hipotenusa h_2: $m_2 = \dfrac{3}{8} = 0,375$;
   Ângulo de inclinação α_2 da reta suporte de h_2: $\alpha_2 = \arctan\left(\dfrac{3}{8}\right) \approx 20,56°$;

3. Coeficiente angular m_3 da reta suporte da hipotenusa h_3: $m_3 = \dfrac{2}{5} = 0,4$;
   Ângulo de inclinação α_3 da reta suporte de h_3: $\alpha_3 = \arctan\left(\dfrac{2}{5}\right) \approx 21,80°$.

Como os coeficientes angulares são diferentes, as hipotenusas dos triângulos retângulos 5×13, 3×8 e 2×5 têm retas suportes distintas.

2.2.5 A sequência de Fibonacci

Os números 2, 3, 5, 8 e 13, medidas dos catetos dos três triângulos retângulos da Figura 3, são termos consecutivos da sequência de Fibonacci

$$S_n = \begin{cases} 0, & n = 0, \\ 1, & n = 1, \\ S_{n-1} + S_{n-2}, & n \geq 2. \end{cases} \tag{7}$$

Em [6], o sistema de equações (8) é descrito para calcular os ganhos ou perdas de área em figuras que têm os números da sequência de Fibonacci como medida dos lados.

Proposição 2.1 *Sejam A, B e C três números consecutivos da sequência de Fibonacci e X a perda ou ganho de área. As equações do sistema*

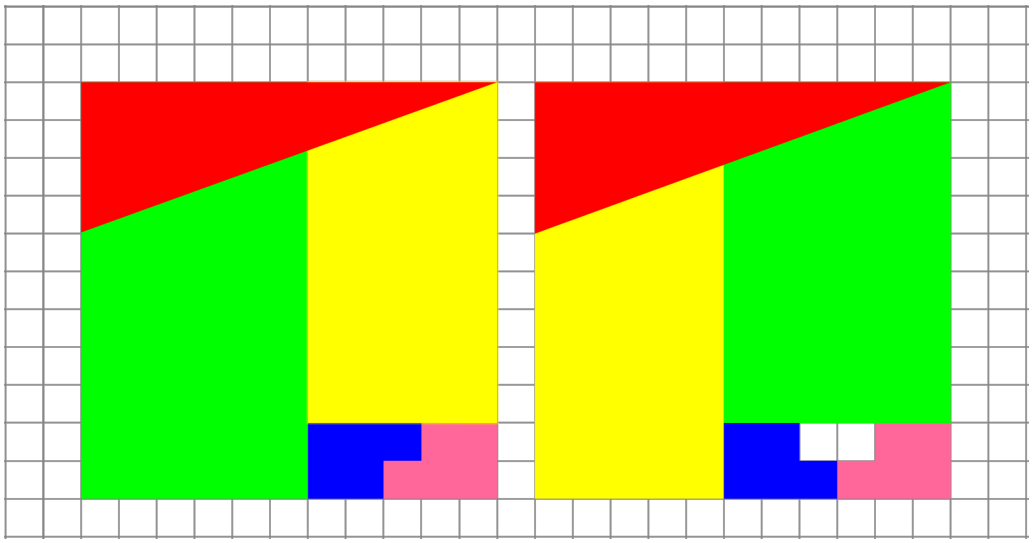
$$\begin{cases} A + B = C, \\ B^2 = A \cdot C \pm X, \end{cases} \tag{8}$$

relacionam A, B, C e X.

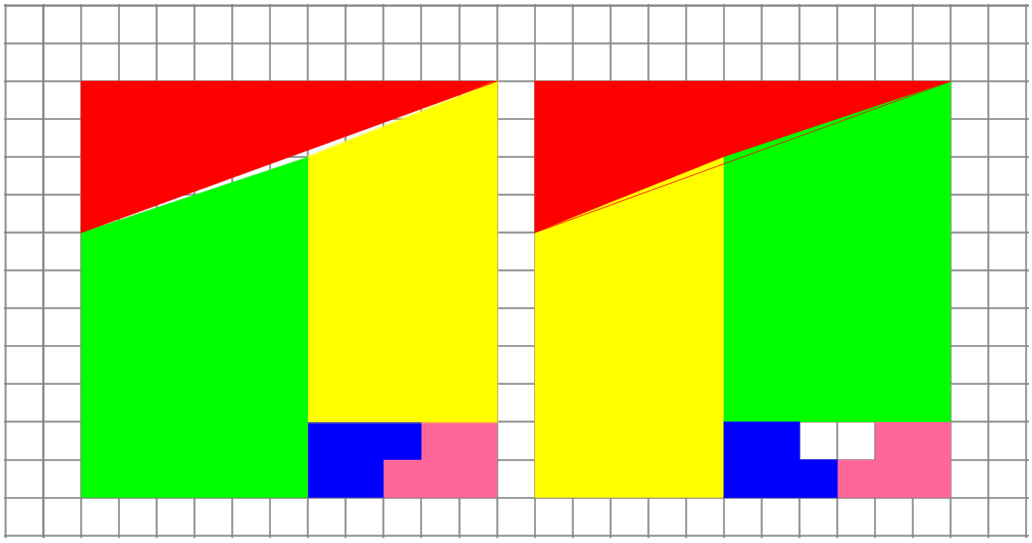
No sistema (8), a segunda equação é a Identidade de Cassini (Jean-Dominique Cassini (1625-1712)). Considerando nesse sistema $A = 5$, $B = 8$ e $C = 13$, obtemos $X = -1$. Desse modo, $X = -1$ significa que o reagrupamento das peças na Figura 3 provocou o ganho de um quadrado unitário.

2.3 Outras formas para o paradoxo de Curry

Outra forma do paradoxo de Curry é a forma quadrada. Nesta, um quadrado de lado ℓ é divido em peças que formam outro "quadrado" de lado ℓ, porém com um "buraco". Curry trabalhou em muitas variações de quadrados, mas não conseguiu construir um quadrado que pudesse ser dividido em menos de cinco peças e ainda produzisse um "buraco" que não tocasse a borda. As Figuras 6 e 7 ilustram duas das formas quadradas propostas por Curry.

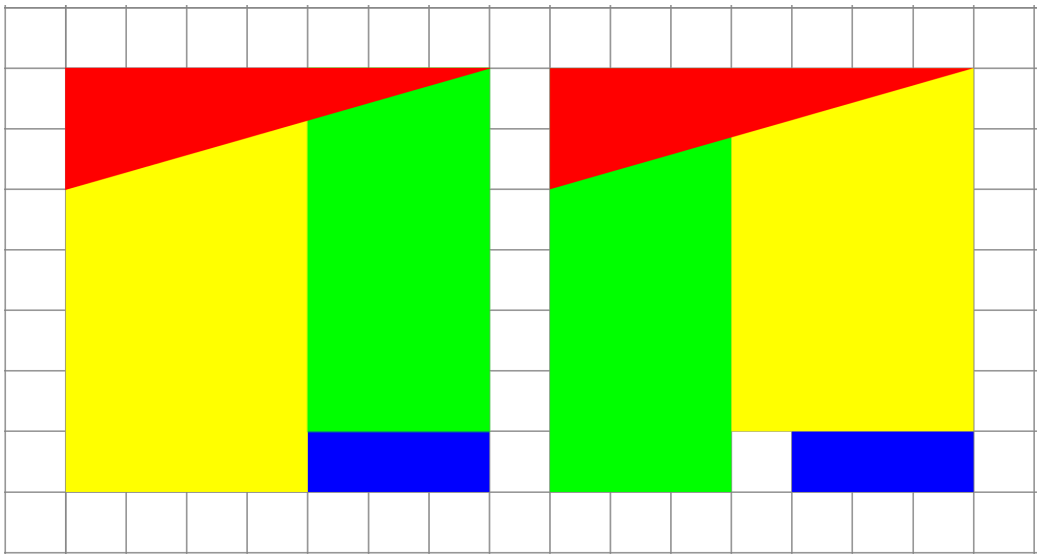


(a) Forma quadrada do paradoxo de Curry com cinco peças

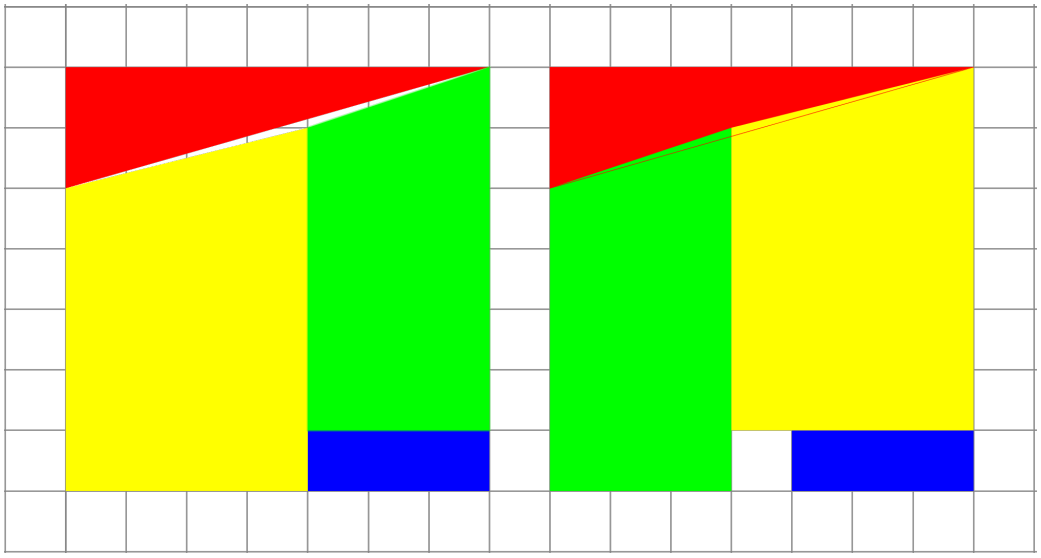


(b) Desvendando a forma quadrada do paradoxo de Curry com cinco peças

Figura 6. Construção da forma quadrada do paradoxo de Curry com cinco peças



(a) Forma quadrada do paradoxo de Curry com quatro peças



(b) Desvendando a forma quadrada do paradoxo de Curry com quatro peças

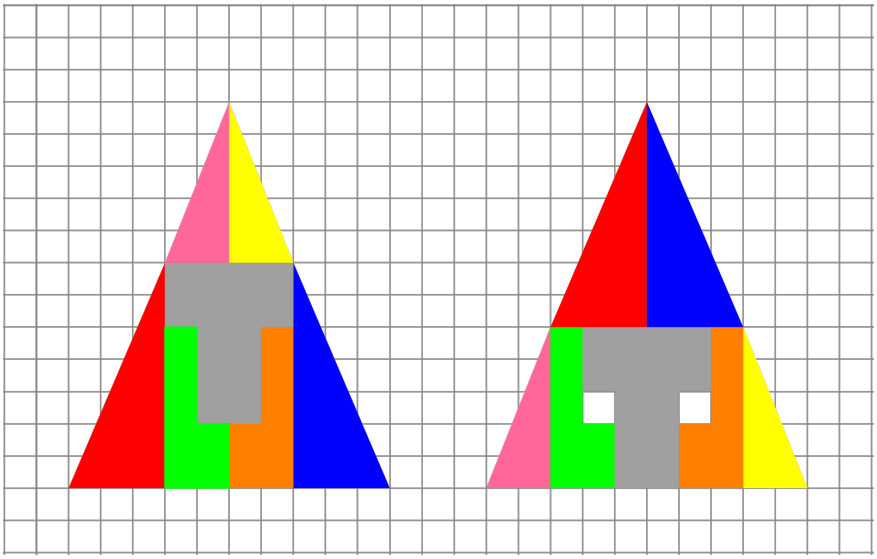
Figura 7. Construção da forma quadrada do paradoxo de Curry com quatro peças

No paradoxo de Curry, além do triângulo retângulo há uma variedade interessante de triângulos isósceles divididos em quatro, cinco, seis ou sete peças que formam um "buraco" de dois, quatro ou seis quadrados unitários [6, 8]. Esses triângulos podem ser construídos de duas maneiras:

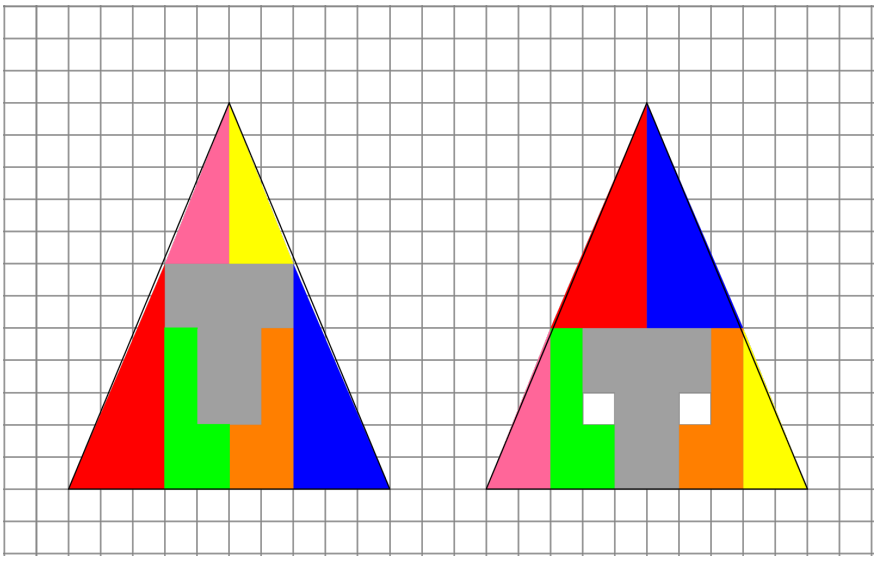
1. os lados congruentes do triângulo isósceles não coincidem com os lados das peças;

2. as peças se sobrepõem.

A explicação para estes paradoxos, os triângulos isósceles de Curry, continua a mesma: as figuras são uma ilusão de ótica. Podemos observar as falhas na Figura 8.



(a) Forma triangular do paradoxo de Curry



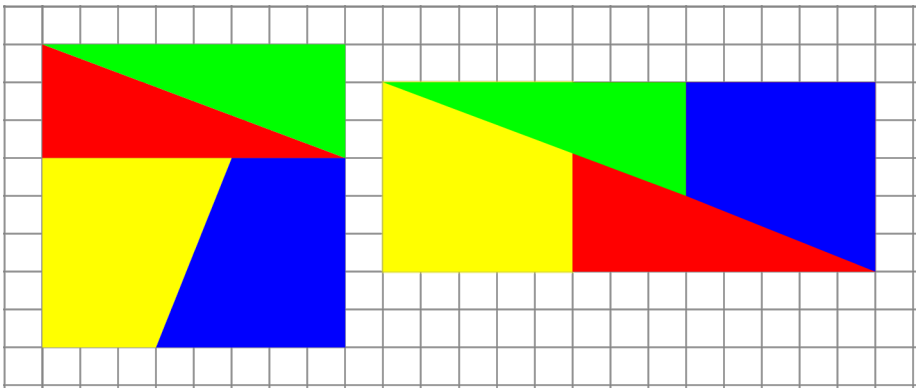
(b) Desvendando a forma triangular do paradoxo de Curry

Figura 8. Construção da forma triangular do paradoxo de Curry

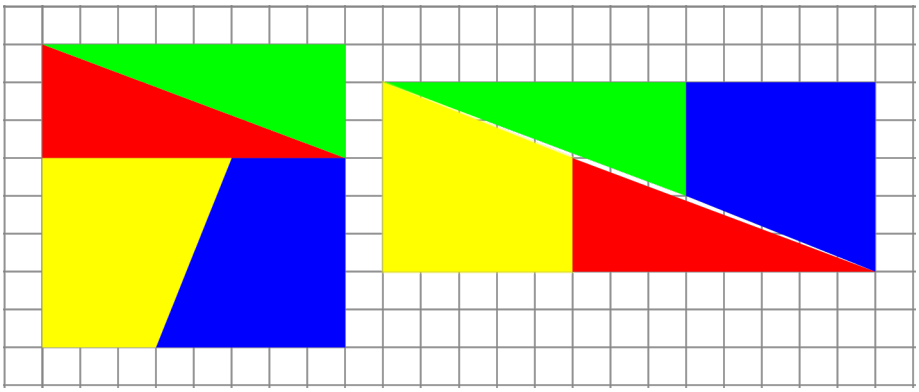
2.4 O paradoxo de Hooper

Segundo [6], outro paradoxo que provoca a perda ou o ganho de área é encontrado originalmente em *Rational Recreations* de William Hooper, uma obra de quatro volumes publicada em Londres em 1774. O paradoxo de Hooper consiste na divisão de uma figura

em peças e no reagrupamento destas para formar outra figura, porém com área diferente da figura original. Em [6, 13] esse paradoxo á apresentado da seguinte forma: um quadrado com lado medindo $8uc$, de área $64ua$, é transformado em um retângulo de dimensões $5uc$ e $13uc$, de área $65ua$, como ilustra a Figura 9(a). Neste caso, podemos observar na Figura 9(b) que o quadrado de lado $8uc$ não tem falhas, enquanto no retângulo falta uma área próxima à diagonal. Esta área meda $1ua$, exatamente o que o quadrado tem a menos do que o retângulo. Novamente, podemos utilizar conceitos geométricos para investigar a ilusão provocada pelo reagrupamento das peças.



(a) Paradoxo de Hooper: $64 = 65$?



(b) Desvendando o paradoxo de Hooper: $64 = 65$?

Figura 9. Construção do paradoxo de Hooper

3 Resultados e discussão

As atividades foram propostas com o intuito de mensurar o domínio de conceitos de Geometria Plana e/ou de Geometria Analítica por partes dos estudantes dos três níveis de ensino. Nas turmas do Ensino Fundamental e do Ensino Médio, apresentamos o paradoxo de Curry para os estudantes construindo os triângulos no GeoGebra - Figura 10, e em Etil Vinil Acetato (EVA) - Figura 11.

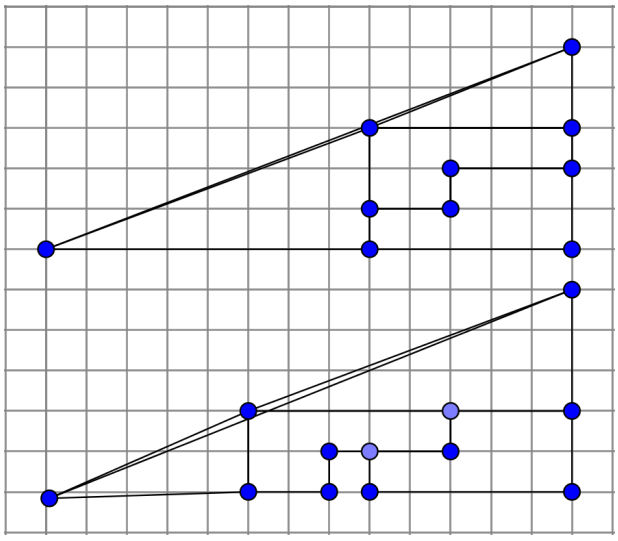


Figura 10. Triângulos de Curry construídos no GeoGebra

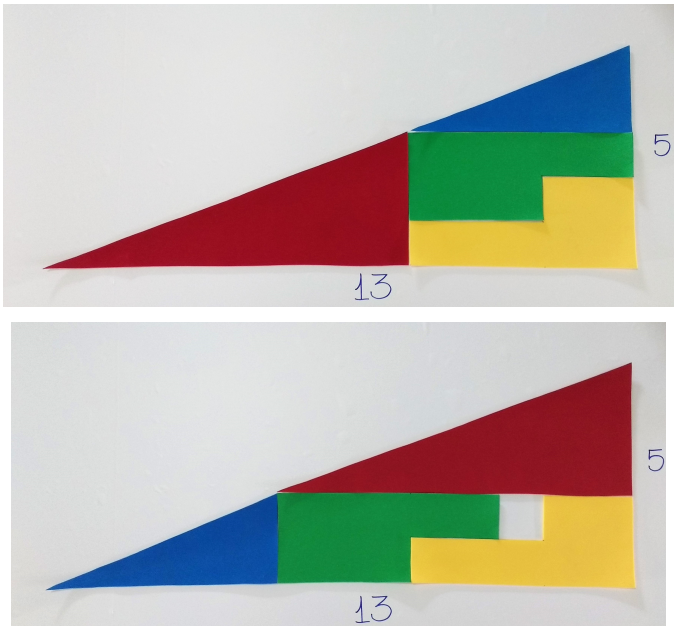


Figura 11. Triângulos de Curry construídos em EVA

3.1 Ensino Fundamental

A atividade com quatro questões foi aplicada em uma turma do nono ano do Ensino Fundamental de uma escola pública estadual em Matinhos-PR. Dos 22 estudantes dessa turma, 17 estavam presentes. Discutimos com os estudantes, de maneira similar à introdução deste trabalho, o que seria um paradoxo e apresentamos o paradoxo de Curry. Conceitos

geométricos como a área de algumas figuras planas e o Teorema de Pitágoras foram revistos. Essa parte durou 50 minutos, o tempo de uma aula. Na aula seguinte, durante mais 50 minutos, os estudantes responderam, trabalhando individualmente, às questões que seguem. A Figura 12 mostra os resultados gerais da atividade.

Questão 3.1 (1ª **questão)** *A soma das áreas de cada peça é igual à área dos triângulos formados pelas peças?*

Questão 3.2 (2ª **questão)** *Utilizando o Teorema de Pitágoras, calcule a medida da hipotenusa dos três triângulos retângulos. O que você conclui? Empregue a máquina calculadora para justificar sua conclusão.*

Questão 3.3 (3ª **questão)** *Observando a figura e a sua construção no GeoGebra, o que você conclui sobre os triângulos formados pelas peças e sobre o quadrado perdido?*

Questão 3.4 (4ª **questão)** *Com base nas conclusões sobre o paradoxo de Curry, o que você tem a dizer sobre o paradoxo de Hooper?*

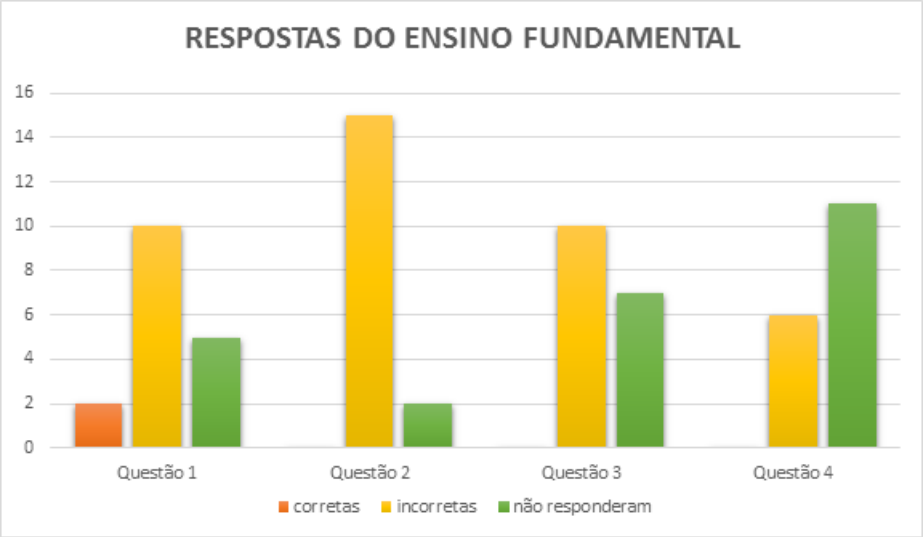


Figura 12. Respostas às questões da atividade para o Ensino Fundamental [8]

3.2 Ensino Médio

A atividade com cinco questões foi aplicada em uma turma do terceiro ano do Ensino Médio de um colégio público estadual em Matinhos-PR. Dos 39 estudantes dessa turma, 30 estavam presentes, sendo que 24 responderam às questões propostas e 6 não devolveram o questionário com as respostas. Discutimos com os estudantes, de maneira análoga à introdução deste trabalho, o que seria um paradoxo e apresentamos o paradoxo de Curry. Conceitos de Geometria Analítica, como a equação geral da reta e o coeficiente angular da reta, foram revisados. Essa parte durou uma aula de 50 minutos. Na aula seguinte, durante mais 50 minutos, os estudantes responderam, trabalhando individualmente, às questões listadas a seguir. A Figura 13 ilustra os resultados gerais da atividade.

Questão 3.5 (1ª **questão**) *Determine a equação geral* $y = mx + n$ *da reta suporte da diagonal dos retângulos de dimensões* 13×5, 8×3 *e* 5×2. *Use a máquina calculadora para determinar o ângulo de inclinação das retas.*

Questão 3.6 (2ª **questão**) *No primeiro triângulo formado pelas quatro peças, calcule: a)* $y(0)$ *; b)* $y(8)$*; c)* $y(13)$. *As imagens calculadas coincidem com os valores verificados na figura?*

Questão 3.7 (3ª **questão**) *No segundo triângulo formado pelas quatro peças, calcule: a)* $y(0)$*; b)* $y(5)$*; c)* $y(13)$. *As imagens calculadas coincidem com os valores verificados na figura?*

Questão 3.8 (4ª **questão**) *Observando a figura e a sua construção no GeoGebra, o que você conclui sobre os triângulos formados pelas peças e sobre o quadrado perdido?*

Questão 3.9 (5ª **questão**) *Com base nas conclusões sobre o paradoxo de Curry, o que você tem a dizer sobre o paradoxo de Hooper?*

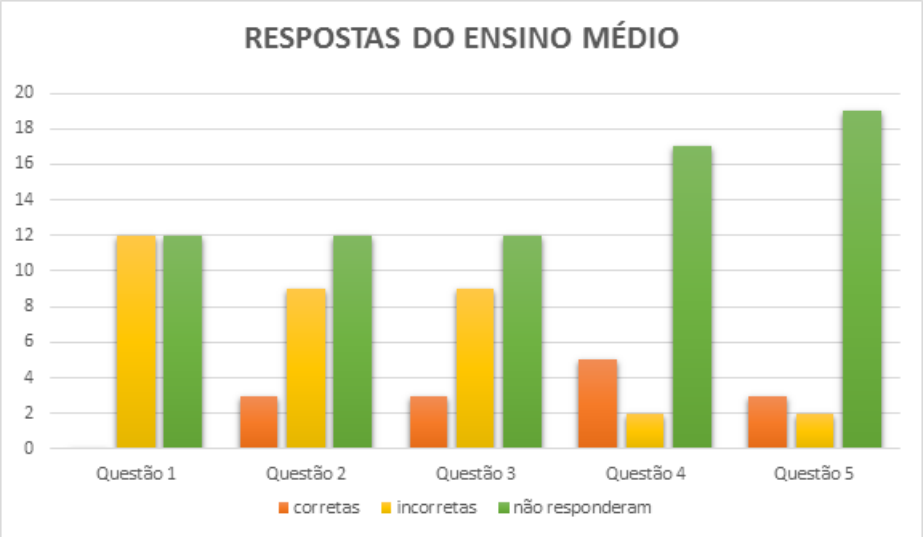


Figura 13. Respostas às questões da atividade para o Ensino Médio [8]

3.3 Ensino Superior

A atividade foi aplicada em uma turma do segundo período do Curso de Licenciatura em Matemática de uma universidade pública federal, na disciplina de Geometria Espacial. Dos 37 estudantes dessa turma, 13 estavam presentes. Discutimos com os estudantes o que seria um paradoxo, exemplificando com paradoxos lógico-matemáticos e com os paradoxos geométricos de Curry e de Hooper. Os estudantes trabalharam em duplas durantes duas aulas de 50 minutos. O roteiro de atividades proposto para o Ensino Superior é praticamente o mesmo proposto para o Ensino Fundamental, uma vez que os estudantes já haviam cursado Geometria Plana no semestre anterior. A Figura 14 mostra os resultados gerais da atividade.

Questão 3.10 (1ª **questão**) *A soma das áreas de cada peça é igual à área dos triângulos formados pelas peças?*

Questão 3.11 (2ª **questão**) *Utilizando o Teorema de Pitágoras, calcule a medida da hipotenusa dos três triângulos retângulos. O que você conclui?*

Questão 3.12 (3ª **questão**) *Qual é sua explicação para o quadrado perdido?*

Questão 3.13 (4ª **questão**) *Com base nas conclusões sobre o Paradoxo de Curry, o que você tem a dizer sobre o Paradoxo de Hooper?*

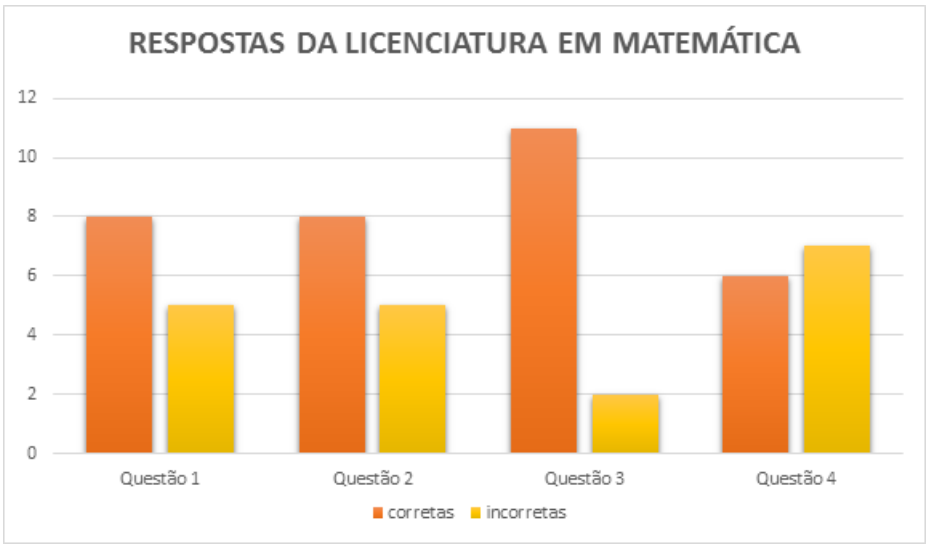


Figura 14. Respostas às questões da atividade para o Ensino Superior [8]

3.4 Análise das atividades

A partir da análise das respostas dos roteiros de atividades que aplicamos em sala de aula, verificamos que os estudantes das turmas do Ensino Fundamental e do Ensino Médio têm dificuldades para empregar conceitos e definições; uma minoria é capaz de efetuar os cálculos associados corretamente e, ainda, uma parte desta minoria não sabe como usar esses cálculos para justificar a solução dos problemas propostos. Quanto ao Ensino Superior, os resultados foram satisfatórios. Mesmo assim, constatamos a falta de rigor matemático nas soluções apresentadas, assim como o mau uso da linguagem escrita.

4 Conclusões

Apresentamos neste trabalho alguns paradoxos geométricos e empregamos os paradoxos de Curry e de Hooper para avaliar a aprendizagem de conteúdos de Geometria Plana e de Geometria Analítica.

Os resultados das atividades aplicadas na Educação Básica, principalmente no que diz respeito ao cálculo de áreas, nos fazem pensar que a Geometria, mesmo constando nos Parâmetros Curriculares Nacionais para Matemática, é negligenciada ou pouco abordada/explorada em sala de aula no Ensino Fundamental e no Ensino Médio. Em 1989, [14] já afirmava/questionava:

> Quanto ao ensino de Geometria, o problema torna-se ainda mais grave: constata-se que ele vem gradualmente desaparecendo do currículo real das escolas. Será que este conhecimento não é necessário ao homem moderno? Terá a geometria perdido sua importância do ponto de vista educacional? Que outros motivos fizeram com que ela fosse praticamente expulsa da sala de aula?

Transcorridos quase trinta anos, a situação nos parece a mesma ou pior. Estamos cientes de que os resultados de duas turmas são insuficientes para fazermos inferências representativas sobre o ensino de Geometria na Educação Básica brasileira. Contudo, os resultados da prova de Matemática e suas Tecnologias do ENEM - Exame Nacional do Ensino Médio, que apresenta um número expressivo de questões sobre Geometria Plana e Geometria Espacial, parecem corroborar essa conclusão.

Assim, devemos, enquanto professores de Matemática, trabalhar para incluir efetivamente a Geometria no currículo da Educação Básica. E nesse processo inclusivo, poderíamos empregar a Matemática Recreativa para estabelecer/explorar conceitos geométricos.

Agradecimentos

À CAPES, pela recomendação do PROFMAT por meio do parecer do Conselho Técnico Científico da Educação Superior e pelo incentivo financeiro.

Referências

[1] APROSIO, A. P. Pinóquio no país dos paradoxos. Zahar, Rio de Janeiro, 2015.

[2] WOLFRAMMATHWORLD Tangram Paradox.
Disponível em: http://mathworld.wolfram.com/TangramParadox.html

[3] DUDENEY, H. Amusements in mathematics, Dover, New York, 1958.

[4] FARLOW, S. J. Paradoxes in mathematics. Dover, New York, 2014.

[5] ALVES, E. C. A.; MORAIS FILHO, D. C. de. Paradoxos geométricos recreativos como recurso didático. VII Semana de Matemática, Universidade Federal de Campina Grande, Paraíba, 2013.

[6] GARDNER, M. Mathematics, magic and mystery. Dover, New York, 1956.

[7] GEOGEBRA. Discover math with geogebra.
Disponível em: https://www.geogebra.org

[8] SENTONE, F. G. Paradoxos geométricos em sala de aula. Dissertação de Mestrado, UTFPR, Curitiba, 2017.

[9] NETO, A. C. M. Geometria. *Coleção PROFMAT*, v.9, n.1, Rio de Janeiro, 2013.

[10] LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. Temas e problemas elementares. *Coleção PROFMAT*, v.5, n.3, Rio de Janeiro, 2012.

[11] DOLCE, O.; POMPEO, J. N. Fundamentos de matemática elementar: geometria plana. v.9, n.9, São Paulo, 2013.

[12] IEZZI, G. Fundamentos de matemática elementar: geometria analítica. v.7, n.6, São Paulo, 2013.

[13] MELLO e SOUZA, J. C. de. Matemática divertida e curiosa. Rio de Janeiro, 2001.

[14] PAVANELLO, R. M. O abandono do ensino de geometria: uma visão histórica. Dissertação de Mestrado, Unicamp, 1989.

Cifra de Hill: Uma Aplicação ao Estudo de Matrizes

Hill Cipher: an Application to the Study of Matrices

Lucas Diego Antunes Barbosa
Instituto Federal de Educação, Ciência e Tecnologia do Norte de MG - IFNMG, Salinas, MG
lucas.barbosa@ifnmg.edu.br

Mariana Garabini Cornelissen
Universidade Federal de São João del Rei - UFSJ, Ouro Branco, MG
mariana@ufsj.edu.br

Resumo: O aprendizado de um conteúdo matemático pode se tornar mais atrativo para o estudante se estiver associado a alguma aplicação. Partindo desse princípio, esse trabalho apresenta aos professores de matemática do Ensino Médio uma proposta de aplicação do conteúdo de matrizes à uma técnica criptográfica, ou seja, uma técnica para codificar e decodificar mensagens, chamada Cifra de Hill. Além de mostrar uma aplicação de um conteúdo matemático, esse trabalho também apresenta uma possibilidade de trabalhar a integração de diferentes disciplinas em sala de aula, já que fazemos uso de conhecimentos básicos de programação de computadores, conteúdo essencial para os estudantes no dia de hoje, na proposta de aula aqui apresentada.

Palavras-chave: criptografia; matrizes; Hill; cifra.

Abstract: Learning mathematical content may become more attractive to students if they are associated with an application. Based on this principle, this work presents to teachers of high school mathematics a proposal to apply matrix content to a cryptographic technique, that is, a technique for encoding and decoding messages, called Hill Cipher. In addition to showing an application of mathematical content, this work also presents a possibility of working the integration of different disciplines in the classroom, since we make use of basic knowledge of computer programming, essential content for students today, in the lesson proposal presented here.

Key-words: encryption; matrices; Hill; cipher.

1 Introdução

O mundo está sofrendo várias transformações, mas alguns aspectos permanecem iguais. Hoje, assim como no passado, para muitos jovens, aprender matemática na escola é uma experiência difícil e, às vezes, desestimulante. Segundo D'Ambrosio [1] os professores em geral mostram a matemática como um corpo de conhecimentos acabado e polido. "Ao aluno não é dado em nenhum momento a oportunidade ou gerada a necessidade de criar nada, nem mesmo uma solução mais interessante. O aluno assim, passa a acreditar que na aula de Matemática o seu papel é passivo e desinteressante"[1].

Recebido em 30/08/2017 - Aceito em 20/11/2017

Aprender não é a simples aquisição de técnicas e habilidades e nem a memorização de algumas explicações e teorias [2]. Por isso, sempre que possível, sugere-se que o professor mostre uma aplicação com o objetivo de estimular e facilitar o aprendizado de um determinado conteúdo. "A possibilidade de compreender conceitos e procedimentos matemáticos é necessária tanto para tirar conclusões e fazer argumentações, quanto para o cidadão agir como consumidor prudente ou tomar decisões em sua vida pessoal e profissional"[3]. Nesta mesma direção, Charlot [4] aponta que a educação não consiste em transmitir conhecimentos acabados, mas em propor aos alunos situações e problemas que desencadeiam uma atividade intelectual que, com a ajuda do professor, leve ao conhecimento. E ainda, que essas situações provoquem o aluno a despertar algum conhecimento anterior, no contexto da aprendizagem significativa. A aprendizagem significativa, conforme Moreira [5], é aquela em que as ideias expressas simbolicamente interagem de maneira substantiva e não arbitrária com aquilo que o aluno já sabe.

Partindo dessa teoria de aprendizagem, esse trabalho tem o objetivo de apresentar aos professores de matemática uma proposta de aplicação do conteúdo de matrizes à uma técnica de criptografia, ou seja, um procedimento para codificar e decodificar mensagens. Atualmente, existem diversos trabalhos já publicados sobre esse tema. Abaixo escolhemos três pesquisas que mais se aproximam do nosso estudo.

O trabalho de mestrado intitulado "Criptografia matricial aplicada ao ensino médio", Schurman [6] teve como objetivo geral apresentar uma sequência didática para trabalhar o conteúdo matrizes com alunos do ensino médio. O autor aponta que o conceito de matrizes é amplamente utilizado em diversas áreas do conhecimento, tais como Economia, Engenharia, Tecnologia, dentre outros. E ainda mais importante que entender o conceito de matrizes é "preciso atribuir sentindo a ele, pois com isso os alunos poderão perceber a necessidade de representação matricial nos diversos fenômenos que os cercam"[6].

Já na dissertação intitulada "Criptografia: uma engenharia didática com funções matrizes e cifra de Hill para o ensino médio", Marinho [7] propôs a implementação de uma engenharia didática para o tratamento do tema criptografia, associado aos conteúdos de matemática trabalhados no ensino médio. O pesquisador afirma que "atividades envolvendo o tema criptografia abrem caminho para a introdução, em sala de aula, de tecnologias da informação e comunicação" [7].

A pesquisa intitulada "Uma proposta para ampliar a perspectiva de professores e alunos em relação ao estudo de matrizes", teve como objetivo proporcionar a professores da rede estadual de São Paulo e alunos de licenciatura em matemática, uma alternativa eficiente e significativa para o estudo de matrizes com foco em transformação geométricas. Neste estudo, Oliveira [8] aponta que a matemática sem dúvida alguma está entre as disciplinas mais rejeitadas por alunos do ensino regular. No entanto, provavelmente na maioria dos casos essa rejeição está associada a abordagens inadequadas de conteúdos, as quais não permitem que os alunos percebam as possíveis aplicações e transformações dos conhecimentos estudados em ferramentas utilizadas por toda sociedade.

No caso desse trabalho, a técnica criptográfica escolhida é a chamada Cifra de Hill em homenagem ao seu criador, o americano Lester S. Hill, que desenvolveu essa técnica em 1929. A justificativa para esta escolha são as possibilidades de abordar diversos conteúdos matemáticos com esse método, como será visto adiante. Conforme Conceição [9] a criptografia, por fazer parte do cotidiano dos alunos, se torna um método muito eficaz para o desenvolvimento de conceitos matemáticos, não somente no Ensino Médio, como também no Ensino Fundamental e a partir daí, torna-se um motivador para a aprendizagem da matemática.

Dessa forma, esse trabalho apresenta uma aplicação de um conteúdo matemático que permite trabalhar os conteúdos de matrizes, determinantes, máximo divisor comum, noções

de aritmética modular, criptografia e programação de computadores em sala de aula, mostrando assim uma possível relação entre teoria e prática matemática. Espera-se que esse trabalho instigue a curiosidade dos professores e dos alunos na relação de teoria e prática matemática, com o intuito de melhorar a relação de ensino e de aprendizagem.

2 Criptografia

Desde o surgimento da humanidade existe a necessidade de se obter maior segurança na transmissão de informações que são enviadas por diversos meios de comunicação. Em tempos passados de guerra se observou o uso de técnicas especiais para o envio de mensagens secretas para as tropas, como foi o caso de Júlio César, imperador de Roma, quando suas tropas estavam pela Europa em guerra [10]. O imperador deslocava o alfabeto três casas adiante para codificar suas mensagens, como pode ser visualizado pela tabela abaixo.

Tabela 1. *Cifra de César*

letra → letra correspondente
A → D
B → E
C → F
D → G
E → H
F → I
e assim por diante

Neste caso, se a mensagem a ser enviada fosse: ACABEM COM O INIMIGO, as tropas receberiam a seguinte mensagem cifrada DFDEHPFRPRNQNPNLR. De acordo com a pesquisa realizada por Fiarresga [11], o relato mais grotesco de transmissão de mensagens codificadas foi usado por Histieu ao transmitir uma mensagem a Aristágoras de Mileto. Histieu raspou a cabeça de um indivíduo, escreveu no seu couro cabeludo a mensagem que queria enviar, esperou que o cabelo do indivíduo voltasse a crescer e enviou-o em viagem até Aristágoras. O indivíduo quando chegou, raspou novamente a cabeça e mostrou a mensagem à Aristágoras de Mileto.

Essa transmissão de informações de forma oculta é conhecida por criptografia. Portanto, criptografia é a técnica de esconder uma escrita e o seu significado é de origem grega (*kripto* = escondido, oculto e *grápho* = grafia, escrita). Segundo Evaristo e Perdigão [12] a criptografia pode ser entendida como a ação de reescrever um texto de modo que apenas as pessoas autorizadas pelo autor do texto sejam capazes de compreendê-lo. O texto normalmente é chamado de mensagem, uma pessoa autorizada a ler a mensagem é chamada destinatário e o autor da mensagem é chamado de remetente. Chamamos de chave criptográfica algo necessário para a codificação ou decodificação da mensagem. Dessa forma, podemos dizer que a criptografia estuda os métodos para codificar uma mensagem de modo que só o seu destinatário legítimo consiga interpretá-la.

Uma vez que a comunicação entre as pessoas é inevitável no atual momento de grande avanço tecnológico, percebemos o quão sério é a transmissão de informações sigilosas. Por exemplo, uma instituição financeira possui informações particulares e importantes de muitas pessoas e tais informações podem ser acessadas caso não haja um sistema de segurança eficaz.

Informações secretas como senhas podem ser interceptadas por pessoas inescrupulosas e utilizadas de forma prejudicial aos proprietários, causando grande prejuízo a estes, pois, com a senha de uma conta bancária, podem ser realizados saques e empréstimos em favor de terceiros. Além do prejuízo com contas bancárias, como no exemplo das instituições financeiras, podemos também citar como exemplo a possibilidade de quebra de sigilo de e-mails, tratando-se de informações compartilhadas via internet, caso um sistema criptográfico não seja utilizado. A quebra do sigilo de e-mails pode provocar grandes danos, como a descoberta de endereço, telefone, local de trabalho, o que pode ser perigoso quando dados tão particulares forem parar na mão de pessoas maldosas. Neste sentido, a criptografia assume um importante papel.

Existem dois tipos de criptografia: simétrica e assimétrica. Na criptografia simétrica, a forma de codificar e decodificar uma mensagem é a mesma. Já na criptografia assimétrica a maneira de codificar não é a mesma de decodificar. No caso da criptografia assimétrica, a chave de codificação é pública e no caso da criptografia simétrica essa chave é privada. São exemplos de métodos criptográficos simétricos: Cifra de César, Cifra de Hill, Data Encryption Standard (DES)e Advanced Encryption Standard (AES). Como método criptográfico assimétrico, podemos citar o método mais famoso e utilizado hoje em dia, que é o método RSA, desenvolvido em 1978 por Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman (daí o nome RSA), pesquisadores na época do Instituto de Tecnologia de Massachusetts. Mais adiante, falaremos um pouco sobre cada um desses métodos.

De acordo com Coutinho [13] estes códigos foram criados para o uso em aplicações comerciais, e não na comunicação entre espiões. Por isso, os códigos modernos são todos de chave pública. Esta é uma ideia introduzida em 1976 por W. Diffie e M.E. Hellman da Universidade da Califórnia. Em um código de chave pública saber codificar não implica saber decodificar! Isto parece impossível: se sei codificar, para decodificar basta desfazer o que fiz. Desfazer o processo de codificação pode não ser tão simples quanto parece.

O DES é um método criptográfico que foi designado, pelos Estados Unidos da América, como algoritmo padrão de criptografia em 1977 e foi amplamente utilizado internacionalmente. É um algoritmo de cifra em blocos, isto é, tal algoritmo opera sobre agrupamentos de tamanho fixo, chamado de blocos. Atualmente, o DES sozinho é considerado inseguro para muitas aplicações e, em 1997, foi substituído pelo AES, mas ainda continuou a ser utilizado em larga escala até 2004 com algumas modificações. O AES tornou-se o algoritmo padrão em 2002 e em 2006 já era um dos algoritmos mais populares utilizados para criptografia simétrica. O AES também é um algoritmo de cifra em bloco, porém com um tamanho de chave maior que o DES. Uma descrição detalhada de tais algoritmos pode ser encontrada em [10]. A criptografia RSA é um método de chave pública cuja codificação baseia-se em um determinado número que é o produto de dois números primos e a decodificação por esse método depende da fatoração desse número, ou seja, dos números primos que o originou. Portanto, sua segurança é garantida com a escolha de um par de números primos grandes. Ao leitor interessado nesse método criptográfico recomenda-se o livro [13]. A cifra de Hill, que é uma técnica de criptografia simétrica, com chave privada, será o assunto de uma próxima seção. Antes, será necessário revisar alguns conceitos e resultados sobre matrizes e aritmética modular.

3 Preliminares

Apresentamos nesta seção algumas definições e resultados sobre matrizes e também sobre aritmética modular que serão necessários para o entendimento do método de Hill. Uma

leitura mais detalhada sobre esses conteúdos pode ser encontrada em [14] e [15].

Definição 3.1 *Seja $k \in \mathbb{N} - \{0\}$. Dizemos que dois números inteiros a e b são congruentes módulo k se os restos da divisão euclidiana de a e b por k são iguais. Neste caso, escrevemos $a \equiv b \ mod \ k$.*

Pode-se mostrar que $\equiv$ é uma relação de equivalência em $\mathbb{Z}$ cuja classe de equivalência módulo k de $a \in \mathbb{Z}$ é dada por

$$[a] = \{x \in \mathbb{Z}; x \equiv a \bmod k\} = \{x = a + kq | q \in \mathbb{Z}\}$$

Além disso, para cada $a \in \mathbb{Z}$ existe um e somente um $r \in \mathbb{Z}, 0 \leq r < k$, tal que $[a] = [r]$. Logo, existem exatamente k classes de equivalência módulo k distintas:

$$[0], [1], [2], \ldots, [k-1]$$

O conjunto de todas essas classes módulo k será representado por $\mathbb{Z}_k$. O leitor interessado pode consultar esse conteúdo em [16].

Definição 3.2 *Um elemento $[a] \in \mathbb{Z}_k$ será dito invertível, quando existir $[b] \in \mathbb{Z}_k$ tal que $[a][b] = [1]$. O elemento $[b] \in \mathbb{Z}_k$ é único (ver demonstração em [17]) e é dito o inverso de $[a]$.*

Proposição 3.1 *$[a] \in \mathbb{Z}_k$ é invertível se, e somente se, $mdc(a, k) = 1$*
Demonstração: *Suponha que $[a] \in \mathbb{Z}_k$ é invertível, logo, existe $[b] \in \mathbb{Z}_k$ tal que:*

$$[a].[b] = [1] \Leftrightarrow a.b \equiv 1 \ mod \ k \Leftrightarrow a.b - 1 \equiv 0 \ mod \ k$$

o que implica que existe $q \in \mathbb{Z}$ tal que $a.b - 1 = q.k$. Logo, $a.b - q.k = 1$ donde $mdc(a, k) = 1$.
Suponha agora que $mdc(a, k) = 1$. Então existem $q, b \in \mathbb{Z}$ tais que:

$$a.b + q.k = 1.$$

Portanto, $a.b \equiv 1 \ mod \ k$, ou seja, $[a][b] = [1]$, como queríamos demonstrar.

■

Veremos agora como encontrar o inverso de um número em $\mathbb{Z}_k$.
Suponha $a \in \mathbb{Z}_k$ invertível e seja $a^{-1} \in \mathbb{Z}_k$ o seu inverso; então $\text{mdc}(a, k) = 1$, o que implica que existem $b, q \in \mathbb{Z}$ tais que:

$$1 = a.b + k.q$$

donde

$$1 \equiv a.b \bmod k$$

Multiplicando os dois membros da igualdade por a^{-1}, obtemos:

$$a^{-1} \equiv b \bmod k$$

Precisamos portanto encontrar b. Os valores de b e q podem ser encontrados utilizando o algoritmo de Euclides, como pode ser visto no exemplo abaixo.

Exemplo 3.1 *Neste exemplo iremos encontrar o inverso de 55 em* $\mathbb{Z}_{26}$*. Como* $mdc(55, 26) = 1$*, sabemos que 55 é invertível em* $\mathbb{Z}_{26}$ *e, além disso, existem* $b, q \in \mathbb{Z}$ *tais que*

$$55.b + 26.q = 1$$

Para encontrarmos b que, conforme dito anteriormente, será o inverso de 55 em $\mathbb{Z}_{26}$*, devemos inicialmente dividir 55 por 26, através da divisão euclidiana, obtendo um quociente e um resto:*

$$55 = 26.2 + 3$$

Agora, devemos dividir 26 pelo resto encontrado, no caso 3, e continuar esse processo, ou seja, de dividir o dividendo pelo resto, até encontrarmos resto nulo.

$$26 = 3.8 + 2$$

$$3 = 2.1 + 1$$

$$2 = 1.2 + 0$$

Observe que esse é o processo que utilizamos para determinar o máximo divisor comum (mdc) entre dois números. O último resto não nulo encontrado é o mdc entre 55 *e* 26*. Agora, partindo da última equação cujo resto é não nulo, e utilizando as equações acima, conseguimos encontrar b e q. Vejamos:*

$$1 = 3 - 2.1$$

Mas, das equações anteriores, temos que $2 = 26 - 3.8$ *e* $3 = 55 - 26.2$*, donde*

$$1 = 3 - 2.1 = 3 - (26 - 3.8).1 = 3 - 26.1 + 3.8.1 = 3.9 - 26.1$$

$$1 = (55 - 26.2).9 - 26.1 = 55.9 - 26.2.9 - 26.1 = 55.9 - 26.19$$

donde

$$1 = 55.9 - 26.19$$

o que implica que 9 é o inverso de 55 em $\mathbb{Z}_{26}$*.*

Definição 3.3 *Dada uma matriz quadrada A de ordem n, chama-se de inversa de A à matriz quadrada B de ordem n tal que:*

$$A.B = B.A = I_n$$

onde I_n *é a matriz identidade de ordem n. Se uma matriz A possui inversa, então sua inversa é única (ver demonstração em [14]) e será denotada por* A^{-1}*.*

Definição 3.4 *Seja* $A = (a_{ij})_{n \times n}$ *uma matriz quadrada de ordem n. O determinante da matriz A, denotado por* $det\,(A)$*, é o número real dado por:*

$$det\,(A) = \sum_{i=1}^{n} a_{ij}.(-1)^{i+j}\, det\,(A(i|j))$$

onde j é qualquer inteiro fixo entre 1 *e n e* $A(i|j)$ *é a matriz formada a partir da matriz A suprimindo sua i-ésima linha e sua j-ésima coluna.*

Sabemos que uma matriz é invertível se, e somente se, seu determinante é não nulo. Uma demonstração desse fato pode ser encontrada em [18].

Definição 3.5 *Define-se o cofator do elemento a_{ij} da matriz A como*

$$\Delta_{ij}(A) = (-1)^{i+j} det(A(i|j)).$$

A matriz $B = (\Delta_{ij}(A))_{n\times n}$ será chamada de matriz dos cofatores da matriz A e sua transposta será chamada de matriz adjunta de A e denotada por adj(A).

Lema 3.1 *Se A é uma matriz quadrada de ordem n, então*

$$a_{k1}\Delta_{i1} + a_{k2}\Delta_{i2} + ... + a_{kn}\Delta_{in} = 0 \text{ se } k \neq i \tag{1}$$

$$a_{1k}\Delta_{1j} + a_{2k}\Delta_{2j} + ... + a_{nk}\Delta_{nj} = 0 \text{ se } k \neq j \tag{2}$$

para i, j = 1,...,n.

Demonstração: Definimos a matriz A' como sendo a matriz obtida de A substituindo a i-ésima linha de A por sua k-ésima linha, ou seja,

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_k \\ \vdots \\ A_n \end{pmatrix} \text{ e } A' = \begin{pmatrix} A_1 \\ \vdots \\ A_k \\ \vdots \\ A_k \\ \vdots \\ A_n \end{pmatrix}$$

Como a matriz A' possui duas linhas iguais, logo det $A' = 0$. O desenvolvimento do determinante de A' segundo a i-ésima linha é exatamente a equação 1. De modo análogo prova-se a equação 2, ainda usando o fato que det $(A) =$ det (A^t) onde A^t é matriz transposta de A. ■

Proposição 3.2 *Seja A um matriz quadrada de ordem n. Então:*

$$adj(A).A = det(A).I_n$$

Demonstração: *O produto da matriz adjunta de A pela matriz A é dado por:*

$$\begin{pmatrix} \Delta_{11} & \cdots & \Delta_{n1} \\ \vdots & \vdots & \vdots \\ \Delta_{1i} & \cdots & \Delta_{ni} \\ \vdots & \vdots & \vdots \\ \Delta_{1n} & \cdots & \Delta_{nn} \end{pmatrix} . \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}$$

O elemento da posição i, j de adj(A).A é

$$(adj(A).A)_{ij} = \sum_{k=1}^{n} a_{ik}\Delta_{jk} = a_{i1}\Delta_{j1} + a_{i2}\Delta_{j2} + ... + a_{in}\Delta_{jn}$$

Pelo lema 3.1, equação 2, e pela definição 3.4 temos que:

$$(adj(A).A)_{ij} = \begin{cases} det(A), \, se \, i = j \\ 0, \, se \, i \neq j \end{cases}$$

Assim,

$$adj(A).A = \begin{pmatrix} det\,(A) & 0 & \cdots & 0 \\ 0 & det\,(A) & \cdots & 0 \\ \vdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & det\,(A) \end{pmatrix} = det\,(A).I_n$$

■

Proposição 3.3 *Se A é uma matriz invertível, então*

$$A^{-1} = \frac{1}{detA}.adj(A)$$

.

Demonstração: *Se A é invertível então $det(A) \neq 0$. Logo, segue pela proposição 3.2 que*

$$\left(\frac{1}{det(A)}\, adj(A)\right).A = I_n$$

donde $A^{-1} = \frac{1}{det(A)}\, adj(A)$

■

Corolário 3.1 *Dada uma matriz $A = (a_{ij})_{n\times n}$, o determinante da matriz A será invertível em $\mathbb{Z}_k$ se o $mdc(det\, A, k) = 1$.*

A demonstração desse corolário é direta pelo que foi visto na proposição 3.1. Com isso, estamos prontos para entender o método de Hill.

4 Cifra de Hill

A cifra de Hill faz parte da época das cifras com papel e lápis, ele é inseguro contra ataque via computador e pode ser decodificado facilmente. Abaixo, segue um roteiro detalhando passo a passo desse algoritmo de codificação e decodificação, assim como um exemplo.

1. Inicialmente devemos converter as letras da mensagem a ser criptografada em números. Isso pode ser feito de diversas maneiras, dependendo de qual número será associado a cada letra. Aqui neste trabalho, usaremos a tabela ASCII (American Standard Code for Interchange Information) na base decimal para essa conversão, que é a tabela mais utilizada na área computacional. Sem perda de generalidade, podemos trabalhar somente com as letras maiúsculas.

Tabela 2. *Conversão das letras maiúsculas para o sistema decimal, conforme a tabela ASCII*

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

2. Agora devemos agrupar a sequência numérica obtida em vetores coluna de tamanho n onde n pode ser qualquer número natural não nulo. Caso o último vetor tenha tamanho menor que n, repita o último número do vetor até completar o tamanho n.

3. O terceiro passo é escolher uma matriz $A = (a_{ij})_{n\times n}$ que será a chave de codificação. O determinante da matriz A deve ser invertível em $\mathbb{Z}_k$, isto é, de acordo com o corolário 3.1, devemos escolher A de forma que mdc(det $A, k) = 1$. Aqui k é o número de símbolos possíveis de acordo com a tabela utilizada. No nosso caso, que estamos trabalhando só com as letras maiúsculas, $k = 26$.

4. Em seguida, iniciamos a codificação que consiste simplesmente em multiplicar à esquerda a matriz chave A por uma matriz B cujas colunas são formadas pelos vetores coluna do passo 2 com cada entrada subtraída de 65. Deve-se subtrair o número 65, pois assim tem-se a classe residual módulo 26.

$$A.B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{n1} \\ a_{21} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ b_{21} & \cdots & b_{n2} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix}$$

5. Após efetuar o produto das matrizes, caso alguma entrada da matriz final seja maior ou igual a 26, devemos trocar esse número pelo seu resto na divisão por 26.

6. Finalmente some 65 a cada uma das entradas dessa matriz obtida e transforme seus vetores coluna em letras de acordo com a tabela 2. Essa mensagem formada é a codificação da mensagem original.

Faremos agora um exemplo desse algoritmo de codificação. Como estamos utilizando a tabela 2, só utilizamos as letras maiúsculas sem os espaços e os acentos.

Exemplo 1
Mensagem original: CIFRADEHILL

Passo 1: Conversão da mensagem de acordo com a tabela 2

C	I	F	R	A	D	E	H	I	L	L
67	73	70	82	65	68	69	72	73	76	76

Passo 2: Agrupando a sequência numérica em vetores coluna de tamanho $n = 3$ e repetindo o último número do vetor coluna:

$$\begin{pmatrix} 67 \\ 73 \\ 70 \end{pmatrix}, \begin{pmatrix} 82 \\ 65 \\ 68 \end{pmatrix}, \begin{pmatrix} 69 \\ 72 \\ 73 \end{pmatrix}, \begin{pmatrix} 76 \\ 76 \\ 76 \end{pmatrix}$$

Passo 3: Escolha da chave de codificação. Neste caso, uma matriz A de ordem 3 dada por

$$A = \begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix}$$

Observe que det A = 55 e mdc$(55, 26) = 1$.

Passo 4: Multiplicando a matriz A à esquerda pela matriz formada pelos vetores coluna com cada entrada subtraída de 65, obtemos:

$$\begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix} . \begin{pmatrix} 2 & 17 & 4 & 11 \\ 8 & 0 & 7 & 11 \\ 5 & 3 & 8 & 11 \end{pmatrix} = \begin{pmatrix} 64 & 35 & 80 & 121 \\ 33 & 15 & 47 & 66 \\ 38 & 75 & 69 & 110 \end{pmatrix}$$

Passos 5: Agora devemos determinar os restos da divisão euclidiana de cada entrada por 26, obtendo:

$$\begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

Passo 6: E finalmente, somando 65 a cada entrada da matriz anterior, chegamos à matriz abaixo

$$\begin{pmatrix} 77 & 74 & 67 & 82 \\ 72 & 80 & 86 & 79 \\ 77 & 88 & 82 & 71 \end{pmatrix}$$

Fazendo a conversão dos números obtidos em letras de acordo com a tabela 2 concluímos que o destinatário receberá a seguinte mensagem codificada: MHMJPXCVRROG
Agora, passaremos ao processo de decodificação. Segue abaixo um roteiro detalhando passo a passo o que deve ser feito para decodificar uma mensagem codificada utilizando o processo de Hill.

1. Além da mensagem codificada, o remetente também deve enviar para o destinatário a matriz chave de codificação, $A = (a_{ij})_{n\times n}$ utilizada. O destinatário ao receber a mensagem codificada precisará converter as letras em números conforme a tabela utilizada pelo remetente, subtrair 65 de cada um desses números e formar uma matriz $C = (c_{ij})_{n\times m}$, ou seja, ele deve agrupar a sequência numérica obtida em vetores coluna de tamanho n.

2. Agora, o destinatário precisa determinar o inverso do determinante da matriz A em $\mathbb{Z}_{26}$ e, em seguida, determinar a matriz adjunta de A.

3. O próximo passo é multiplicar o inverso do determinante em $\mathbb{Z}_{26}$ e a matriz adjunta de A encontrados no passo anterior pela matriz C. Observe que aqui estamos simplesmente fazendo o produto $A^{-1}.C$.

4. Em seguida, encontre o resto da divisão euclidiana de cada uma das entradas dessa matriz por 26.

5. E finalmente, some 65 a cada uma das entradas.

Dessa forma, o destinatário descobrirá a mensagem original enviada. Após a codificação e decodificação podemos perceber de fato que o método é inseguro. Pela codificação e por alguns cálculos matemáticos, a decodificação é feita de forma fácil.

Vamos aplicar esse algoritmo para recuperar a mensagem do exemplo 1.

Exemplo 2

Passo 1: Suponha que o destinatário recebeu a matriz chave de ordem 3 e a mensagem abaixo:

MHMJPXCVRROG

$$A = \begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix}$$

Tomando como referência a tabela 2, o destinatário pode transformar esse bloco de letras na seguinte matriz:

$$B = \begin{pmatrix} 77 & 74 & 67 & 82 \\ 72 & 80 & 86 & 79 \\ 77 & 88 & 82 & 71 \end{pmatrix}$$

Subtraindo 65 de cada entrada da matriz anterior obtém-se a matriz:

$$C = \begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

Passo 2 : Como o determinante da matriz chave é 55, precisamos encontrar o inverso de 55 em $\mathbb{Z}_{26}$. Pelo exemplo 3.1, temos que o inverso de 55 em $\mathbb{Z}_{26}$ é 9.

Obtendo a matriz adjunta de A, tem-se a matriz:

$$\text{adj}(A) = \begin{pmatrix} 13 & -38 & 14 \\ 15 & -10 & -5 \\ -3 & 13 & 1 \end{pmatrix}$$

Passo 3: O próximo passo agora é multiplicar 9.adj$(A).C$:

$$9.\begin{pmatrix} 13 & -38 & 14 \\ 15 & -10 & -5 \\ -3 & 13 & 1 \end{pmatrix}.\begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

$$=\begin{pmatrix} 117 & -342 & 126 \\ 135 & -90 & -45 \\ -27 & 117 & 9 \end{pmatrix}.\begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

$$=\begin{pmatrix} 522 & -1179 & -4806 & -2043 \\ 450 & -1170 & -2385 & 765 \\ 603 & 1719 & 2556 & 1233 \end{pmatrix}$$

Passo 4: Em seguida, encontre o resto da divisão euclidiana de cada uma das entradas dessa matriz por 26

$$=\begin{pmatrix} 2 & 17 & 4 & 11 \\ 8 & 0 & 7 & 11 \\ 5 & 3 & 8 & 11 \end{pmatrix}$$

Passo 5: Somando 65 a cada entrada da matriz acima e consultando a tabela 2, obtém-se a mensagem codificada.

$$=\begin{pmatrix} 67 & 82 & 69 & 76 \\ 73 & 65 & 72 & 76 \\ 70 & 68 & 73 & 76 \end{pmatrix}$$

$$=\begin{pmatrix} C & R & E & L \\ I & A & H & L \\ F & D & I & L \end{pmatrix}$$

Portanto o destinatário encontrará a seguinte mensagem original: CIFRADEHILLL

5 Proposta de aula

Nesta seção sugerimos uma proposta de aula que pode ser aplicada no Ensino Médio, no curso técnico em Informática, no curso de licenciatura em matemática ou em qualquer outro curso em que são ministrados os conteúdos de matrizes e programação de computadores. Esta proposta é baseada na aprendizagem significativa de David Ausubel. Nesta concepção, a aprendizagem se caracteriza pela interação entre os conhecimentos prévios e os conhecimentos novos, dando ao sujeito novos significados para os conhecimentos prévios.

Conforme Moreira [5], este conhecimento prévio pode ser um símbolo já significativo, um conceito, uma proposição, um modelo mental ou uma imagem chamado de *subsunçor*. Este é um "conhecimento específico, existente na estrutura do indivíduo, que permite dar significados a um novo conhecimento que lhe é apresentado ou por ele descoberto"[5].

O autor aponta que o conhecimento prévio é a variável que mais influencia a aprendizagem significativa de novos conhecimentos. Neste estudo, apontamos como o subsunçor

os conhecimentos de lógica e programação de computadores, pois avaliamos como fundamentais para execução e compreensão desta proposta e são esses conhecimentos que darão "significados"ao conceito de matrizes.

Proposta de atividade: Construir um algoritmo para codificar e decodificar mensagens através do método de Hill.

Público-alvo: Alunos do Ensino Médio, do curso técnico em Informática ou do curso de licenciatura em matemática

Material necessário: Essa proposta de aula deve ser aplicada com o auxílio do laboratório de informática e, preferencialmente, com a participação dos professores de informática da escola. Será necessário quadro branco, pincel, retroprojetor, e ainda sugerimos que os computadores do laboratório de informática tenham a linguagem de programação C++ ou PHP.

Pré-Requisitos: Inicialmente o professor de matemática deve desenvolver com esses alunos os seguintes conteúdos matemáticos: matrizes, determinante, MDC e noções de aritmética modular.

Objetivos:

- Despertar o interesse dos alunos para o aprendizado da matemática.
- Associar teoria e prática matemática.
- Desenvolver a integração das disciplinas de matemática e programação de computadores.
- Aprender a trabalhar em equipe.
- Mostrar aplicações de conteúdos matemáticos no dia-a-dia.

Metodologia: Após o desenvolvimento dos conteúdos listados acima em pré-requisitos por meio de aula expositiva e dialogada, será explicado para os alunos o histórico da criptografia e o método aplicável em sala de aula, a cifra de Hill. Após o ensino dos conteúdos teóricos necessários, o professor pedirá que o alunos formem grupos de 5 membros e construam um algoritmo, em qualquer linguagem de programação, para codificar e decodificar uma mensagem utilizando o método de Hill.

Carga-horária prevista: Segue abaixo um cronograma com o tempo estimado de aula e o conteúdo a ser trabalhado. O tempo de uso do laboratório de informática fica a critério do professor envolvido com essa proposta de aula.

6 Aplicação e resultados

Nos meses de outubro e novembro de 2014, essa proposta de aula foi aplicada para os alunos do 3^0 ano do curso técnico em informática do ensino integrado do Instituto Federal do Norte de Minas Gerais-IFNMG Campus: Arinos. No primeiro momento, os alunos assustaram-se quando ouviram as palavras algoritmo e programação dentro de um trabalho de matemática. A disciplina de programação de computadores foi vista somente no 1^0 ano,

Tabela 3. *Sugestão de cronograma para a proposta de aula*

Tempo estimado	**Conteúdo**
4h/a	Divisão euclidiana, MDC, noções de aritmética modular.
1h/a	Números inversíveis em $\mathbb{Z}_k$.
1h/a	Matrizes: exemplos e operações.
4h/a	Determinante e Matriz Inversa.
3h/a	Criptografia e Cifra de Hill.

ou seja, dois anos antes. Apesar disso, muitos alunos mostraram um grande interesse em participar do trabalho, já que cada integrante do grupo seria contemplado com 10 pontos dos 35 pontos distribuídos naquela etapa.

O primeiro passo foi explicar os conteúdos teóricos necessários. Noções de aritmética modular e números inversíveis foram novidade para os alunos, pois os mesmos nunca tinham visto esses temas. Os alunos mostraram grande dificuldade em efetuar divisões usando o algoritmo de divisão euclidiana. Uma situação que pode justificar essa dificuldade, é o fato dos alunos estarem acostumados a efetuar operações básicas de matemática em aparelhos eletrônicos. No conteúdo matrizes e determinantes, os alunos não tiveram muita dificuldade, pois muitos deles já tinham estudado o conteúdo no 2^0 ano do curso. Quando foram citados os métodos de criptografia existentes e a importância da criptografia no contexto atual, foi o momento que os alunos mais prestaram atenção na aula, pois naquele momento eles estavam estudando conteúdos matemáticos associados à uma aplicação. Nesse momento percebe-se a importância de mostrar conteúdos matemáticos associados com fatos decorrentes do dia-a-dia.

O segundo passo foi dividir a turma em grupos de 5 membros, aleatoriamente, para que os alunos pudessem ter interação entre eles. Em seguida, foi agendado o laboratório de informática para que os alunos pudessem todos os dias após as aulas regulares, se reunirem e confeccionarem o trabalho proposto. Os alunos mostraram grande dificuldade em traduzir as expressões matemáticas para a linguagem em que o seu algoritmo estava sendo construído. Nesse momento, a presença do professor de matemática é fundamental. As dificuldades de programação que iam surgido eram encaminhadas aos professores de informática, que participaram desses encontros que os alunos realizaram durante uma semana no laboratório.

O terceiro passo, após terem criado o algoritmo de codificação pela cifra de Hill, foi apresentar o trabalho em sala de aula. Os alunos criaram uma interface, entregaram os códigos dos trabalhos feitos na linguagem C++ e PHP, e ainda hospedaram o mesmo no servidor. Ao final da apresentação dos trabalhos, alguns alunos julgaram o algoritmo como trabalhoso, mas afirmaram que puderam relembrar códigos de programação e ainda aprenderam matemática.

Neste trabalho, os alunos utilizaram a tabela 4 abaixo, dos caracteres minúsculos (ao invés dos maiúsculos como fizemos na seção anterior) para fazerem a conversão das letras em números e ainda limitaram o tamanho da mensagem para apenas 9 caracteres.

Tabela 4. *Conversão das letras minúsculas em sistema decimal sugerida pelos alunos*

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

7 Conclusão

Existem várias tópicos da matemática que podem ser trabalhados com aplicações como o que foi proposto acima. Isso ajudaria a responder a pergunta clássica de uma aula de matemática: "Para que isso servirá em minha vida?". O algoritmo construído pelos alunos teve um aspecto positivo, pois, contribuiu para o desenvolvimento dos alunos no estudo de matrizes e na programação, auxiliando o aprendizado dessas disciplinas. Esse trabalho não esgotará o estudo sobre aplicações na matemática, espera-se que a partir dele possam surgir novas ideias para associar a teoria à prática em sala de aula, podendo assim melhorar o aprendizado em matemática.

Referências

[1] D'AMBROSIO, B. S. Como Ensinar Matemática Hoje? SBEM, Brasília, ano 2, n.2, p.15-19, 1989.

[2] D'AMBROSIO, Ubiratan. Ação pedagógica e Etnomatemática como marcos conceituais de Matemática. In: BICUDO, M.A.V.; Educação Matemática. Editora Centauro. 2ª ed. 2005.

[3] BRASIL, Ministério da Educação, Parâmetros Curriculares Nacionais: ensino médio. Secretaria de Educação Média e Tecnológica. Brasília: 1999.

[4] CHARLOT, B. Da relação com o saber às práticas educativas. São Paulo: Cortez, 2013.

[5] MOREIRA, M. A. Aprendizagem significativa: a teoria e textos complementares. São Paulo: Editora Livraria de Física, 2011.

[6] SCHURMANN, H. Criptografia matricial aplicada ao ensino médio. 2013. 75 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática, 2013.

[7] MARINHO FILHO, E. R. Criptografia: uma engenharia didática com funções matrizes e cifra de Hill, para o ensino médio. 2015. 128 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Oeste do Pará, Instituto de Ciências da Educação, Programa de Ciências Exatas.

[8] OLIVEIRA, W. F. Uma proposta para ampliar a perspectiva de professores e alunos em relação ao estudo se matrizes. 2017. 129 f.Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas.

[9] CONCEIÇÃO, M. R. F. Transformações no Plano: Uma Aplicação do Estudo de Matrizes com o Uso de Planilhas Eletrônicas. 2013. 64 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT). Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande, 2013.

[10] FALEIROS, A. C. Criptografia. São Carlos-SP: SBMAC,2011.

[11] FIARRESGA, V. M. C. Criptografia e Matemática. (Dissertação do Mestrado em Matemática para Professores). Departamento de Matemática, Universidade Federal de Lisboa,2010.

[12] EVARISTO, J.; PERDIGÂO, E. Introdução à Álgebra Abstrata. Maceió: EDUFAL,2002.

[13] COUTINHO, S.C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2014.

[14] SEYMOUR, L. Álgebra Linear: teorema e problemas.São Paulo: Pearson Makron Books, 1994.-(Coleção Schaum)

[15] HEFEZ, A. Aritmética.Rio de Janeiro: SBM,2013.

[16] DOMINGUES, H. H.;IEZZI, G. Álgebra Moderna.São Paulo: Atual,2003.

[17] SHOKRANIAN, S. Uma introdução à Teoria dos números. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

[18] HEFEZ, A.; FERNANDEZ, C. S. Introdução à Álgebra Linear. Rio de Janeiro: SBM,2012.

[19] LIMA, E. L. Álgebra linear.Rio de Janeiro:SBM,2003.

[20] RIBENBOIM, P. Números Primos: Velhos Mistérios e Novos Recordes. Rio de Janeiro: IMPA, 2012.

[21] SANTOS, R. J. Introdução a Álgebra Linear. Departamento de Matemática-ICEx.Universidade Federal de Minas Gerais, 2010.

O Código da Nave Espacial Mariner 9

The Code of the Spacecraft Mariner 9

José Silvino Dias
Instituto Federal de Minas Gerais - IFMG, São João Evangelista, MG
jose.silvino@ifmg.edu.br

Mariana Garabini Cornelissen
Universidade Federal de São João del Rei - UFSJ, Ouro Branco, MG
mariana@ufsj.edu.br

Resumo: Este trabalho apresenta e descreve o código corretor de erros pertencente a uma família de códigos lineares, chamado Código de Reed-Muller de primeira ordem utilizado pela nave espacial Mariner 9 ao transmitir fotos do planeta Marte à Terra, quando foi enviada ao espaço em 1971 pela NASA (National Aeronautics and Space Administration).

Palavras-chave: código; mensagem; erro; Mariner 9.

Abstract: This paper presents and describes the error corrector code belonging to a family of linear codes, called the first-order Reed-Muller code used by the Mariner 9 spacecraft when transmitting photos of the planet Mars to Earth, when it was sent into space in 1971 by NASA (National Aeronautics and Space Administration).

Key words: code; message; error; Mariner 9.

1 Introdução

O presente trabalho descreve o código corretor de erros utilizado pela nave espacial Mariner 9, enviada ao espaço pela NASA em 30 de maio de 1971 com o objetivo de transmitir fotos do planeta Marte à Terra.

O Programa Mariner, segundo [1], teve o seu primeiro lançamento fracassado com a nave Mariner 1. A Mariner 2 foi a primeira missão que obteve sucesso, passou a 35 mil quilômetros do planeta Vênus em 14 de dezembro de 1962 e enviou informações da atmosfera de Vênus. A Mariner 3 lançada em 5 de novembro de 1964, tinha como objetivo alcançar o planeta Marte, porém pouco depois do lançamento surgiram problemas técnicos que inviabilizaram a missão. Após o fracasso da missão Mariner 3, foi enviada em 28 de novembro de 1964 a Mariner 4 que passou a 9920 quilômetros de Marte e transmitiu à Terra as primeiras fotografias da superfície marciana. A Mariner 5 sobrevoou Marte em 19 de outubro de 1967, coletou e transmitiu informações do planeta vermelho. A Mariner 6, passou por Marte em 31 de julho de 1969, tirou fotos e analisou a composição e pressão atmosférica de Marte. A Mariner 7 enviou fotografias do pólo sul de Marte. O lançamento da Mariner 8 não foi bem sucedido, levando a NASA lançar a nave Mariner 9, cujo código corretor de erros será estudado neste artigo. Esta nave entrou na órbita de Marte em 13 de novembro de 1971, 167 dias após o lançamento.

Recebido em 30/08/2017 - Aceito em 18/10/2017

Nesta missão foi fotografado um majestoso vulcão com 27 km de altura, denominado "Monte Olimpo", que já havia sido observado por telescópio, pelo astrônomo italiano Giovanni Schiaparelli (1835-1910), que descreveu como uma região de intenso brilho na superfície de Marte.

A teoria de códigos corretores de erros, foi fundada pelo matemático Claude Shannon (1916-2001), do Laboratório Bell de Nova Jersey, Estados Unidos da América (EUA), num trabalho publicado em 1948. Tal teoria tornou-se muito ativa a partir da década de 70 com a corrida espacial e a popularização dos computadores, sendo, até hoje, amplamente utilizada em diversas áreas do conhecimento: matemática, computação, engenharia elétrica, engenharia espacial, estatística entre outras.

Esta teoria é utilizada sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade em setores como: comunicação via satélite, comunicações internas de um computador, armazenamento ótico de dados. Contudo, na transmissão ou armazenamento de dados, pode ocorrer interferências eletromagnéticas ou equívocos humanos (erros de digitação) que são chamados de ruídos, possibilitando que a mensagem recebida seja diferente da mensagem transmitida. A referida teoria tem como objetivo corrigir tais erros e fazer com que a mensagem transmitida pelo emissor seja de fato a mesma mensagem recebida pelo usuário.

Atualmente existem diversos trabalhos já publicados e disponíveis sobre a Teoria dos Códigos Corretores de Erros, por exemplo [2], [3], [4] e [5], que citam o código utilizado pela Mariner 9, mas de maneira superficial, apenas como exemplo de uma classe de códigos. O objetivo desse trabalho é explicar de maneira clara e completa o código específico utilizado pela Mariner 9, que pertence à classe dos códigos de Reed Muller ([6], [7], [8] e [9]) começando pela apresentação dos pré requisitos da Teoria de Códigos Corretores de Erros necessários para o total entendimento dessa codificação (Seção 2), passando pela apresentação, descrição e demonstração dos principais parâmetros dos Códigos de Reed Muller de Primeira Ordem (Seção 3) até a explicação em si da codificação e decodificação utilizada por essa nave espacial no envio de fotos de Marte para a Terra (Seção 4). Com isso, espera-se que esse texto sirva de material didático para alunos dos cursos de matemática, computação ou até mesmo engenharia, para profissionais da área de tecnologia da informação e também para professores de matemática e física tanto do Ensino Médio como do Ensino Superior aprenderem uma aplicação importante da matemática.

2 Conteúdos Básicos

Nesta seção são apresentadas as principais definições e os principais resultados da teoria dos códigos corretores de erros necessários para que o leitor entenda o código utilizado pela Mariner 9. Todos os resultados desta seção podem ser encontrados em [2] e [3].

Entende-se por código, de acordo com a teoria da comunicação, o conjunto de símbolos que devem ser conhecidos tanto pelo emissor quanto pelo receptor, de modo que a mensagem seja compreendida. Codificar a informação inicial, adicionando informação redundante, de tal forma que, ao receber o sinal modificado pelo "ruído" seja possível, de alguma forma, recuperar a mensagem original, esta é a ideia básica da teoria de códigos corretores de erros.

O ponto de partida para a construção de um código corretor de erros é construir um conjunto de símbolos finito $\mathcal{F}$, chamado alfabeto. O número de elementos de $\mathcal{F}$ será denotado por q.

Definição 2.1 (Códigos Corretores de Erros) *Um código corretor de erros é um sub-*

conjunto próprio qualquer de $\mathcal{F}^n$*, para algum* n *natural, onde* $\mathcal{F}^n = \underbrace{\mathcal{F} \times \mathcal{F} \times \ldots \times \mathcal{F}}_{n \text{ vezes}}$.

O exemplo a seguir ilustra a definição acima.

Exemplo 2.1 *O idioma português é um exemplo de um código corretor de erros. Dado o alfabeto* $\mathcal{F}$ *da língua portuguesa, formado por* 26 *letras, bem como o espaço em branco, também considerado como uma letra, o "c" cedilha e as vogais acentuadas: à, á, â, ã, é, ê, í, ó, ô, õ e ú (neste caso, o número de elementos de* $\mathcal{F}$ *é* $q = 39$*), uma palavra desta língua pode ser considerada como um elemento de* $\mathcal{F}^{46}$*, já que* 46 *é o comprimento da palavra mais longa da mesma, "pneumoultramicroscopicossilicovulcanoconiótico", segundo [10]. As outras palavras que não possuem* 46 *letras são completadas com espaços em branco do lado direito ao término da palavra, omitindo-os na escrita. Assim, o conjunto* $\mathcal{C}$ *de todas as palavras da língua portuguesa é um subconjunto próprio de* $\mathcal{F}^{46}$ *e, portanto, um código corretor de erros. Suponha que, ao escrever uma palavra, produza a sequência de letras "espatial". Como esta palavra não é um elemento de* $\mathcal{C}$*, percebe-se imediatamente que houve erro e, nesse caso, a correção é possível pois, a palavra de* $\mathcal{C}$ *que mais se assemelha a "espatial" é "espacial". Percebe-se, porém, que este código não é muito eficiente, uma vez que, se a palavra "nave" for erroneamente escrita como "neve", ou ainda, como "nove", não se conseguiria detectar e muito menos corrigir o erro.*

Neste artigo trabalharemos apenas com códigos binários, isto é, códigos definidos sobre o alfabeto $\mathcal{F}$ igual ao corpo $\mathbb{F}_2 = \{0, 1\}$ cujas operações de soma e produto são dadas pela tabela abaixo.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Tabela 1. Adição e multiplicação em $\mathbb{F}_2$

Segue abaixo outro exemplo de código, desta vez sobre o corpo $\mathbb{F}_2$.

Exemplo 2.2 (Código da Nave) *Supõe-se que um protótipo de uma nave espacial se mova a 20 metros de altura (acima do solo), de modo que, ao dar um dos comandos: Para Cima, Leste, Sudeste, Sul, Oeste, Noroeste, Norte ou Para Baixo, ele se desloca em uma destas direções. Estes oito comandos podem ser codificados como elementos de* $\mathbb{F}_2^3$*, como abaixo:*

$Para\ Cima \longrightarrow 000$
$Leste \longrightarrow 001$
$Sudeste \longrightarrow 010$
$Sul \longrightarrow 011$
$Oeste \longrightarrow 100$
$Noroeste \longrightarrow 101$
$Norte \longrightarrow 110$
$Para\ Baixo \longrightarrow 111$

Tabela 2. Codificação da fonte do código da nave

O código acima é chamado de "código da fonte". Suponha que estes ternos ordenados devam ser transmitidos via rádio e que o sinal no caminho sofra interferências. Imagine que a mensagem 111*(Para Baixo) possa, na chegada, ser recebida como* 011*(Sul), o que faria com que o protótipo, em vez de ir Para Baixo, fosse para o Sul. Numa tentativa de corrigir tal erro, pode-se fazer uma recodificação das palavras, de modo que permita detectar e corrigir os erros ocorridos na transmissão, acrescentando redundâncias nos códigos da fonte. Como na tabela abaixo:*

$Para\ Cima \longrightarrow 000 \longrightarrow 0000000$
$Leste \longrightarrow 001 \longrightarrow 0010111$
$Sudeste \longrightarrow 010 \longrightarrow 0101010$
$Sul \longrightarrow 011 \longrightarrow 0111101$
$Oeste \longrightarrow 100 \longrightarrow 1001100$
$Noroeste \longrightarrow 101 \longrightarrow 1011011$
$Norte \longrightarrow 110 \longrightarrow 1100110$
$Para\ Baixo \longrightarrow 111 \longrightarrow 1110001$

Tabela 3. Codificação de canal do código da nave

Recodificando desta maneira, observe que os três primeiros símbolos reproduzem o código da fonte, enquanto os quatro restantes são redundâncias inseridas. O novo código inserido na recodificação é um código detector e corretor de erros, chamado de "código de canal".

Suponha que seja inserido um erro ao transmitir uma das palavras, por exemplo, a palavra 1110001*(Para Baixo), de modo que a mensagem recebida seja* 1110000*. Comparando essa mensagem com as palavras do código de canal, nota-se que ela não faz parte do mesmo e, portanto, detectam-se erros. A palavra deste código mais próxima da referida mensagem (a que tem menor número de elementos diferentes) é* 1110001*, que é, portanto, a palavra transmitida.*

A teoria dos códigos corretores de erros consiste em transformar o código da fonte em código de canal, em detectar e corrigir erros na recepção das palavras e em decodificar o código de canal em código da fonte.

Consideram-se, neste trabalho, apenas canais simétricos, isto é, todos os símbolos transmitidos do código têm a mesma probabilidade de serem recebidos de forma errada.

Será apresentada a seguir uma forma de medir a distância entre palavras de um código em $\mathbb{F}_2^n$.

Definição 2.2 (Distância de Hamming) *Dados dois elementos* $u = (u_1, u_2, \ldots, u_n)$ *e* $v = (v_1, v_2, \ldots, v_n)$ *com* $u, v \in \mathbb{F}_2^n$*, chama-se distância de Hamming entre* u *e* v *ao número de posições em que estes dois elementos diferem, isto é:*

$$d(u, v) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$$

Dado um código $\mathcal{C} \subset \mathbb{F}_2^n$ *chama-se de "distância mínima"do código* $\mathcal{C}$ *o número:*

$$d = min\{d(u, v) : u, v \in \mathcal{C}, u \neq v\}$$

Exemplo 2.3 *No código da nave temos que:*

$$d(0101010, 1110001) = 5$$
$$d(0111101, 1011011) = 4$$
$$d(0000000, 1001100) = 3$$

Observe que, a distância mínima do código da nave é $d = 3$.

A distância de Hamming, conforme definida acima, é uma métrica. Portanto, para todo $u, v, w \in \mathbb{F}_2^n$, temos as seguintes propriedades:

(i) Positividade: $d(u, v) \geq 0$, a igualdade acontece, se e somente se, $u = v$;

(ii) Simetria: $d(u, v) = d(v, u)$;

(iii)Desigualdade Triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

A seguir, o Teorema 2.1 apresenta um dos principais resultados da teoria de códigos corretores de erros. Para a demonstração desse teorema necessitaremos, anteriormente, de duas definições e de um lema.

Definição 2.3 (Menor Inteiro) *Dado um código* $\mathcal{C} \subset \mathbb{F}_2^n$ *com distância mínima* d*, considere* η *a parte inteira de* $\frac{d-1}{2}$*, que será denotada por* $\eta = \left[\frac{d-1}{2}\right]$.

Definição 2.4 (Disco) *Dado um elemento* $x \in \mathbb{F}_2^n$ *e um número real* $\eta > 0$*, definimos disco de centro* x *e raio* η *como sendo o conjunto:*

$$D(x, \eta) = \{u \in \mathbb{F}_2^n : d(u, x) \leq \eta\}$$

Lema 2.1 *Sejam* $\mathcal{C} \subset \mathbb{F}_2^n$ *um código com distância mínima* d*,* $\eta = [\frac{d-1}{2}]$ *e* c *e* c' *duas palavras de* $\mathcal{C}$ *. Então* $D(c, \eta) \cap D(c', \eta) = \emptyset$.

Demonstração: Suponha que exista $x \in D(c, \eta) \cap D(c', \eta)$. Assim $d(c, x) \leq \eta$ e $d(c', x) \leq \eta$. Como $d(c', x) = d(x, c')$ e, pela desigualdade triangular temos que

$$\begin{aligned} d(c, c') &\leq d(c, x) + d(x, c') \\ &\leq \eta + \eta \\ &\leq 2\eta \\ &\leq d - 1 \\ &< d \end{aligned}$$

Agora, isto é um absurdo, pois as palavras c e $c' \in \mathcal{C}$ tem distância maior ou igual a d, já que d é a distância mínima de $\mathcal{C}$. Portanto $D(c, \eta) \cap D(c', \eta) = \emptyset$. ■

Teorema 2.1 *Seja* $\mathcal{C} \subset \mathbb{F}_2^n$ *um código com distância mínima* d*. Então:*

(i) $\mathcal{C}$ *detecta até* $d - 1$ *erros;*

(ii) $\mathcal{C}$ *corrige até* $\eta = \left[\frac{d-1}{2}\right]$ *erros.*

Demonstração:

(i) Se d é a distância mínima do código $\mathcal{C}$ então qualquer palavra que tenha até $d-1$ erros não pertence a $\mathcal{C}$ e, portanto, seu erro será detectado;

(ii) Seja c a palavra do código $\mathcal{C}$ a ser transmitida e r a palavra recebida sendo cometidos t erros, com $t \leq \eta$, então $d(r,c) = t \leq \eta$, assim $r \in D(c,\eta)$. Logo, basta trocar r por c já que, pelo Lema 2.1, não há outra palavra de $\mathcal{C}$ em $D(c,\eta)$ que não seja c.

■

Observe que se c é a palavra a ser transmitida e foi recebida a palavra r com t erros, sendo $t \leq \eta$, como c é a palavra mais próxima do código $\mathcal{C}$ então troca-se r por c. Mas não se tem garantia total de que a palavra transmitida foi c, pois poderia ter sido cometido mais que t erros o que levaria a outra palavra do código $\mathcal{C}$ diferente de c.

Exemplo 2.4 *Suponha que se queira mover a nave do exemplo* 2.2 *para cima. Neste caso, a mensagem a ser transmitida é* $c = 0000000$ *(Para Cima). Mas, a mensagem recebida pelo receptor foi* $r = 1000000$*, ocorrendo* 1 *erro na transmissão. Como a distância mínima do código da nave é* $d = 3$ *então este código detecta até* 2 *erros e corrige até* $\eta = \left[\frac{d-1}{2}\right] = 1$ *erro. Portanto, esse erro será detectado e corrigido pelo código que trocará* r *por* c*.*

Pelo item (ii) do Teorema 2.1, segue uma definição importante para a correção de erros de um código.

Definição 2.5 (Capacidade de Correção do Código) *Dado um código* $\mathcal{C}$ *com distância mínima* d*, a capacidade de correção do código é dada por:*

$$\eta = \left[\frac{d-1}{2}\right]$$

Interessa-nos códigos que tenham um número M de palavras relativamente grande, para que se possa transmitir muita informação e que tenha uma distância mínima d também grande, para se ter uma boa capacidade de correção de erros.

A seguir, vamos definir uma classe de códigos muito importante que será utilizado neste trabalho. Lembre-se que $\mathbb{F}_2^n$ é um espaço vetorial sobre $\mathbb{F}_2$ com soma e multiplicação por escalar usuais.

Definição 2.6 (Códigos Lineares) *Um código* $\mathcal{C} \subset \mathbb{F}_2^n$ *é chamado de código linear se for um subespaço vetorial de* $\mathbb{F}_2^n$*.*

Observação 2.1 *Todo código linear é por definição um espaço vetorial de dimensão finita. Sejam* k *a dimensão do código* $\mathcal{C}$*,* $\{v_1, v_2, \ldots, v_k\}$ *uma de suas bases e* $a_1, a_2, \ldots, a_k$ *escalares em* $\mathbb{F}_2$*. Todo vetor* $v \in \mathcal{C}$ *se escreve como combinação linear dos vetores* $\{v_1, v_2, \ldots, v_k\}$ *de forma única, isto é:*

$$v = a_1v_1 + a_2v_2 + a_3v_3 + \cdots + a_kv_k$$

Logo, um código linear $\mathcal{C} \subset \mathbb{F}_2^n$ *de dimensão* k *possui* 2^k *elementos.*

Exemplo 2.5 *O código da nave*

$$\mathcal{C} = \{0000000, 0010111, 0101010, 0111101, 1001100, 1011011, 1100110, 1110001\}$$

é um código linear pois o conjunto $\mathcal{C}$ acima é fechado com relação à adição, ou seja, a soma de quaisquer duas palavras desse conjunto resulta em uma palavra de $\mathcal{C}$, fechado com relação à multiplicação por elementos de $\mathbb{F}_2$ e também contém o elemento nulo. Logo, $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_2^7$.

Definição 2.7 (Parâmetros de um Código) *Um código $\mathcal{C} \subset \mathbb{F}_2^n$ possui três parâmetros fundamentais $[n, M, d]$, que são, respectivamente, o seu comprimento (o número n corresponde ao espaço ambiente $\mathbb{F}_2^n$ onde $\mathcal{C}$ se encontra), o seu número de elementos M e a sua distância mínima d.*

Exemplo 2.6 *Vimos no exemplo 2.5 que o código da nave*

$$\mathcal{C} = \{0000000, 0010111, 0101010, 0111101, 1001100, 1011011, 1100110, 1110001\}$$

é um código linear. Seus parâmetros são: $n = 7$, $M = 8$ e $d = 3$. Tal código também pode ser visto como a imagem da seguinte aplicação linear $T : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^7$

$$(x_1, x_2, x_3) \mapsto (x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3, x_3)$$

Por exemplo, a codificação $(0, 1, 1)$ que denotaremos por 011 (código da fonte) é $T(011) = 0111101$ (código de canal).

Veremos a seguir que a distância mínima pode ser calculada utilizando o peso de um código linear.

Definição 2.8 (Peso de um Código Linear) *O peso de um código linear $\mathcal{C}$, que denominaremos por $w(\mathcal{C})$, é o peso mínimo de todas as palavras não nulas de $\mathcal{C}$, isto é,*

$$w(\mathcal{C}) = min\{w(u) : u \in \mathcal{C} \setminus \{0\}\}$$

onde $w(u) = |\{i : u_i \neq 0\}|$ representa o número de caracteres não nulos da palavra u.

Observe que $w(u) = d(u, 0)$.

Proposição 2.1 *Seja $\mathcal{C} \subset \mathbb{F}_2^n$ um código linear com distância mínima d. Então:*

(i) $d(u, v) = w(u - v),\ \forall u, v \in \mathbb{F}_2^n$;

(ii) $d = w(\mathcal{C})$.

Demonstração:

(i) Segue $\forall u, v \in \mathbb{F}_2^n$, com $u = (u_1, u_2, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$ que

$$\begin{aligned} w(u - v) &= |\{i : u_i - v_i \neq 0,\ 1 \leq i \leq n\}| \\ &= |\{i : u_i \neq v_i,\ 1 \leq i \leq n\}| \\ &= d(u, v). \end{aligned}$$

(ii) Para todo par de elementos $u, v \in \mathcal{C}$, com $u \neq v$, tem-se $z = u - v \in \mathcal{C} \setminus \{0\}$. Assim, temos

$$\begin{aligned} d &= min\{i : u_i \neq v_i,\ 1 \leq i \leq n\} \\ &= min\{i : u_i - v_i \neq 0,\ 1 \leq i \leq n\} \\ &= min\{i : z_i \neq 0,\ 1 \leq i \leq n\} \\ &= min\{w(z) : z \in \mathcal{C} \setminus \{0\}\} \\ &= w(C) \end{aligned}$$

■

Observe que, como demonstrado na proposição 2.1, nos códigos lineares o peso coincide com a distância mínima do código, isto é, $w(\mathcal{C}) = d$. Em um código linear com M elementos, podemos calcular a distância mínima d, deste código, a partir do seu peso com $M - 1$ cálculos de distâncias, em vez dos $\binom{M}{2} = \frac{M(M-1)}{2}$ cálculos que deveriam ser feitos em um código qualquer, não linear, para o cálculo de d.

Veremos, na definição a seguir, que é usual colocar os elementos da base de um código linear $\mathcal{C}$ numa matriz.

Definição 2.9 (Matriz Geradora de um Código) *Dados um código linear $\mathcal{C} \subset \mathbb{F}_2^n$ de dimensão k sobre $\mathbb{F}_2^n$ e $\beta = \{u_1, u_2, \ldots, u_k\}$ uma base ordenada de $\mathcal{C}$, considere a matriz G, cujas linhas são os vetores $u_i = (u_{i1}, u_{i2}, \ldots, u_{in})$, com $i = 1, 2, \ldots, k$:*

$$G = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ u_{21} & u_{22} & \cdots & u_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ u_{k1} & u_{k2} & \cdots & u_{kn} \end{pmatrix}_{k \times n}$$

Tal matriz G é denominada "matriz geradora"do código $\mathcal{C}$, a qual não é única, dependendo da escolha da base β.

Dada a matriz G, matriz geradora de um código $\mathcal{C}$, para se codificar uma mensagem x utilizando tal código, basta fazermos $x.G$.

Exemplo 2.7 *O conjunto $\beta = \{1001100, 0101010, 0010111\}$ é uma base do código $\mathcal{C}$ da nave, já que os vetores de β são linearmente independentes e geram o conjunto $\mathcal{C}$. Disso temos a matriz geradora de $\mathcal{C}$ como abaixo*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}_{3 \times 7}$$

De acordo com o exemplo 2.6, observe que a codificação de 011 *é $T(011) = 0111101$, que nada mais é do que* $(011).G$.

Agora, para decodificar a palavra 0111101 *do código $\mathcal{C}$, isto é, achar a palavra $x \in \mathbb{F}_2^3$, tal que, $T(x) = 0111101$, basta resolver a equação $(x_1, x_2, x_3).G = 0111101$, o que implica: $x_1 = 0$, $x_2 = 1$, e $x_3 = 1$.*

3 Códigos de Reed-Muller de 1ª Ordem

Os códigos de Reed-Muller foram criados em 1954, por David Eugene Muller (1924 – 2008). Neste mesmo ano, Irving Stoy Reed (1923 – 2012) descobriu o algoritmo de decodificação destes códigos. Estes códigos formam uma classe de códigos lineares sobre $\mathbb{F}_2$ que possuem várias maneiras de serem definidos. Vamos, a seguir, dar uma definição recursiva para estes códigos.

Os códigos Reed-Muller de 1ª ordem - $R(1,m)$ são códigos binários lineares definidos, recursivamente, por:

- $R(1,0) = \{0,1\} = \mathbb{F}_2$.
- $R(1,1) = \mathbb{F}_2 \times \mathbb{F}_2 = \{00,01,10,11\} = \mathbb{F}_2^2$.
- *Para* $m > 1$, defina :

$$R(1,m) = \left\{ u\ u, u\ (u+\bar{1}) \mid u \in R(1,m-1) \text{ e } \bar{1} = \text{vetor } \underbrace{11\ldots1}_{2^{m-1}} \right\}$$

Por exemplo,

$$R(1,2) = \{u\ u, u\ (u+\bar{1}) \mid u \in R(1,1)\} = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$$

Utilizando $R(1,2)$, obtemos:

$$R(1,3) = \left\{ \begin{array}{cccc} 00000000 & 01010101 & 10101010 & 11111111 \\ 00110011 & 01100110 & 10011001 & 11001100 \\ 00001111 & 01011010 & 10100101 & 11110000 \\ 00111100 & 01101001 & 10010110 & 11000011 \end{array} \right\}$$

Através do $R(1,3)$, obtemos o $R(1,4)$ e assim sucessivamente.

3.1 Parâmetros do Código de Reed-Muller de 1ª Ordem

De acordo com a definição 2.7, os parâmetros de um código são: $[n, M, d]$, onde n é o comprimento do código, M é a cardinalidade desse código e d é sua distância mínima.

Pela definição dos códigos de Reed-Muller de primeira ordem, temos que

$$R(1,0) \subset \mathbb{F}_2^1 = \mathbb{F}_2^{2^0}$$

$$R(1,1) \subset \mathbb{F}_2^2 = \mathbb{F}_2^{2^1}$$

$$R(1,2) \subset \mathbb{F}_2^4 = \mathbb{F}_2^{2^2}$$

$$R(1,3) \subset \mathbb{F}_2^8 = \mathbb{F}_2^{2^3}$$

Continuando esse raciocínio, teremos $R(1,4) \subset \mathbb{F}_2^{16} = \mathbb{F}_2^{2^4}$ e assim sucessivamente, obtendo:

$$R(1,m) \subset \mathbb{F}_2^{2^m}$$

Logo, o comprimento dos Códigos de Reed-Muller de Primeira Ordem, ou seja, o comprimento de $R(1,m)$ é:

$$n = 2^m.$$

Agora, observe que a cardinalidade de $R(1,0)$ que será denotada aqui por $|R(1,0)|$, é igual a 2,

$$|R(1,1)| = 4 = 2^2, \quad |R(1,2)| = 8 = 2^3, \quad |R(1,3)| = 16 = 2^4$$

obtendo por indução que

$$|R(1,m)| = 2^{m+1}$$

Assim, o número de palavras de $R(1,m)$ é

$$M = 2^{m+1}$$

Segue pela observação 2.1 que a dimensão do espaço vetorial $R(1,m)$ sobre $\mathbb{F}_2$ é $k = m+1$.

Vamos mostrar, agora, que a distância mínima do código Reed-Muller de 1ª ordem é $d = 2^{m-1}$.

Para isso, temos que mostrar que o peso de qualquer palavra de $R(1,m)$, exceto as palavras $\bar{0} = \underbrace{000\ldots0}_{2^m}$ e $\bar{1} = \underbrace{111\ldots1}_{2^m}$ é igual a 2^{m-1}, que tem $w(\bar{0}) = 0$ e $w(\bar{1}) = 2^m$. Com isso, segue pela Proposição 2.1 que $d = w(R(1,m)) = 2^{m-1}$.

Teorema 3.1 *Seja* $c \in R(1,m)$, $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ *e* $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$. *Então,* $w(c) = 2^{m-1}$.

Demonstração: (Vamos verificar a afirmação por indução em m)

Para $m = 1$, temos que $R(1,1) = \{00, 01, 10, 11\}$, donde qualquer palavra, $c \neq \bar{0} = 00$ e $c \neq \bar{1} = 11$, tem peso $2^{1-1} = 1$. Observe que, 01 e 10, ambas tem peso 1. Logo, o resultado é verdadeiro para $m = 1$.

Hipótese de Indução: Em $R(1,m-1)$ qualquer palavra, $c \neq \bar{0} = \underbrace{000\ldots0}_{2^{m-1}}$ e $c \neq \bar{1} = \underbrace{111\ldots1}_{2^{m-1}}$, tem peso $2^{(m-1)-1} = 2^{m-2}$.

Observe que, em $R(1,m)$ dizer que qualquer palavra, $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ e $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$, tem peso 2^{m-1} equivale a dizer que ela é composta por metade $0's$ e metade $1's$ já que seu comprimento é 2^m e $2^{m-1} = \frac{2^m}{2}$.

Seja c uma palavra de $R(1,m)$, $c \neq \bar{0} = \underbrace{000\ldots0}_{2^m}$ e $c \neq \bar{1} = \underbrace{111\ldots1}_{2^m}$.

Temos duas possibilidades:

(1) $c = u\ u, u \in R(1,m-1)$.

Como $c \neq \underbrace{000\ldots0}_{2^m}$ e $c \neq \underbrace{111\ldots1}_{2^m}$, então, $u \neq \underbrace{000\ldots0}_{2^{m-1}}$ e $u \neq \underbrace{111\ldots1}_{2^{m-1}}$. Por hipótese de indução, $w(u) = 2^{m-2}$, ou seja, u tem 2^{m-2} posições iguais a 1. Logo, $c = u\ u$ terá

$2.2^{m-2} = 2^{m-1}$ posições iguais a 1. Portanto, $w(c) = 2^{m-1}$.

(2) $c = u\ (u + \bar{1}), u \in R(1, m-1)$.

(2.1) Se $u = \underbrace{000\ldots0}_{2^{m-1}}$, então, $u + 1 = \underbrace{111\ldots1}_{2^{m-1}}$. Logo,

$$c = \underbrace{000\ldots0}_{2^{m-1}}\underbrace{111\ldots1}_{2^{m-1}} \Longrightarrow w(c) = 2^{m-1}$$

.

(2.2) Se $u = \underbrace{111\ldots1}_{2^{m-1}}$, então, $u + 1 = \underbrace{000\ldots0}_{2^{m-1}}$. Logo,

$$c = \underbrace{111\ldots1}_{2^{m-1}}\underbrace{000\ldots0}_{2^{m-1}} \Longrightarrow w(c) = 2^{m-1}$$

.

(2.3) Caso $u \neq \underbrace{000\ldots0}_{2^{m-1}}$ e $u \neq \underbrace{111\ldots1}_{2^{m-1}}$ temos que, $c = u\ (u + \bar{1})$, onde $u \in R(1, m-1)$.

Pela hipótese de indução, $w(u) = 2^{m-2} = \frac{2^{m-1}}{2}$, ou seja, metade das coordenadas de u são iguais a zero e metade das coordenadas de u são iguais a 1. Observe que, 0 em u, vira 1 em $u + 1$ e, 1 em u, vira 0 em $u + 1$. Logo, a palavra $u\ (u + 1)$ terá 2.2^{m-2} posições iguais a 1. Portanto,

$$w(c) = 2^{m-1}$$

■

3.2 Codificação do Código Reed-Muller de 1ª Ordem

A seguir, vai ser apresentada uma construção recorrente para a matriz geradora do código $R(1, m)$, que será denotada por $G(1, m)$.

Considere a matriz geradora de $R(1, 1)$ por

$$G(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Se $G(1, m-1)$ é a matriz geradora para $R(1, m-1)$, então, a matriz geradora para $R(1, m)$ é

$$G(1,m) = \begin{bmatrix} G(1,m-1) & G(1,m-1) \\ \underbrace{0\ldots0}_{2^{m-1}} & \underbrace{1\ldots1}_{2^{m-1}} \end{bmatrix}_{(m+1)\times 2^m}$$

Conforme visto anteriormente, a dimensão de $R(1, m)$ sobre $\mathbb{F}_2$ é igual a $m + 1$, o que implica que a matriz $G(1, m)$ possui $m + 1$ linhas. E como o comprimento de $R(1, m)$ é 2^m, a matriz $G(1, m)$ possui 2^m colunas.

Desta forma, temos, por exemplo:

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0\ldots0 & 1\ldots1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0\ldots0 & 1\ldots1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

e assim sucessivamente.

Para codificar uma mensagem b utilizando o código Reed-Muller de 1ª ordem, basta efetuar a operação:

$$b.G(1,m)$$

Como a matriz $G(1,m)$ é uma matriz de tamanho $(m+1) \times 2^m$, a mensagem b, ou o código da fonte, deverá ter comprimento $m+1$, ou seja, $b = (b_0, b_1, \ldots, b_m)$ e o código de canal ou a mensagem codificada terá comprimento 2^m.

Exemplo 3.1 *Para codificar uma mensagem usando a matriz geradora do código $R(1,3)$ de tamanho 4×8, a mensagem, código da fonte, deverá ter tamanho 1×4. A mensagem é codificada para a palavra do código do seguinte modo,*

$$(b_0, b_1, b_2, b_3).\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{4\times8} =$$

$$= (b_0, b_0+b_1, b_0+b_2, b_0+b_1+b_2, b_0+b_3, b_0+b_1+b_3, b_0+b_2+b_3, b_0+b_1+b_2+b_3)$$

3.3 Decodificação dos Códigos Reed-Muller - Reed Decoding

A decodificação dos códigos Reed-Muller, denominada "Reed Decoding", é relativamente simples e será explicada neste trabalho através de um exemplo. Vamos considerar inicialmente o caso $m = 3$. Já sabemos que o código $R(1,3) \subset \mathbb{F}_2^8$ possui 16 palavras, tem dimensão 4 e distância mínima também igual a 4. Por isso, esse código detecta até 3 erros e corrige até 1 erro. Considere a matriz geradora do código $R(1,3)$ dada abaixo:

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

As linhas desta matriz são os vetores de uma base do código $R(1,3)$ identificadas como $\{v_0, v_1, v_2, v_3\}$, nesta sequência, da primeira até a quarta linha. Qualquer palavra c deste código é uma combinação linear destes vetores, isto é,

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3, \text{ onde } a_i \in \mathbb{F}_2.$$

Assim qualquer vetor c do código $R(1,3)$ é da forma:

$c = (c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7) = (a_0, a_0+a_1, a_0+a_2, a_0+a_1+a_2, a_0+a_3, a_0+a_1+a_3, a_0+a_2+a_3,$
$a_0 + a_1 + a_2 + a_3)$.

Agora, note que: (lembre-se que em $\mathbb{F}_2$ a soma de dois elementos iguais é zero)

$$a_1 = c_0 + c_1 = c_2 + c_3 = c_4 + c_5 = c_6 + c_7$$
$$a_2 = c_0 + c_2 = c_1 + c_3 = c_4 + c_6 = c_5 + c_7$$
$$a_3 = c_0 + c_4 = c_1 + c_5 = c_2 + c_6 = c_3 + c_7$$

Se não ocorrer nenhum erro na transmissão da palavra c, cada uma das 4 equações em cada linha acima resultará no valor de a_i, $i = 1, 2, 3$ correspondente. Caso ocorra erro na transmissão da palavra c, a palavra recebida será $r = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7)$ e, neste caso, os valores dos $a_i's$ serão dados por:

$$a_1 = r_0 + r_1 = r_2 + r_3 = r_4 + r_5 = r_6 + r_7$$
$$a_2 = r_0 + r_2 = r_1 + r_3 = r_4 + r_6 = r_5 + r_7$$
$$a_3 = r_0 + r_4 = r_1 + r_5 = r_2 + r_6 = r_3 + r_7$$

Observe, agora, que nem todas as 4 equações em cada linha vão coincidir (pois houve erro) e, neste caso, o valor de a_i será igual ao dígito que mais aparece nas 4 equações acima que determinam o respectivo a_i.

Já para encontrar o valor de a_0, vamos lembrar que

$$r = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3$$

$$a_0v_0 = r - (a_1v_1 + a_2v_2 + a_3v_3)\,.$$

$$\text{Como } v_0 = \bar{1} = 11111111, \text{ então } \; a_0v_0 = a_0,$$

logo o valor de a_0 será determinado pela maioria dos elementos que aparecem em

$$r - (a_1v_1 + a_2v_2 + a_3v_3)\,.$$

Assim a palavra transmitida será recuperada por:

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3.$$

Exemplo 3.2 *Suponha que seja transmitida a palavra* $c = 01010101 = v_1$ *e recebida a palavra* $r = 01010100$ *(observe que houve* 1 *erro no último dígito). Lembre-se que o código* $R(1,3)$ *detecta até* 3 *erros e corrige até* 1 *erro. Portanto, neste caso, o erro será detectado e corrigido. Utilizando a decodificação Reed, temos que:*

$$a_1 = r_0 + r_1 = r_2 + r_3 = r_4 + r_5 = r_6 + r_7$$
$$a_2 = r_0 + r_2 = r_1 + r_3 = r_4 + r_6 = r_5 + r_7$$
$$a_3 = r_0 + r_4 = r_1 + r_5 = r_2 + r_6 = r_3 + r_7$$

Os valores de a_1, a_2 e a_3 são obtidos da seguinte forma:

$$a_1 = 0 + 1 = 0 + 1 = 0 + 1 = 0 + 0$$
$$a_1 = 1 = 1 = 1 = 0 \Longrightarrow a_1 = 1$$

Observe que, conforme explicado anteriormente, como houve erro na transmissão, nem todas as equações foram iguais. Neste caso, consideramos como o valor de a_1, o dígito que mais aparece como resultado das 4 equações que, neste caso, foi $a_1 = 1$. Temos, a seguir, o mesmo raciocínio para a_2 e a_3.

$$a_2 = 0 + 0 = 1 + 1 = 0 + 0 = 1 + 0$$
$$a_2 = 0 = 0 = 0 = 1 \Longrightarrow a_2 = 0$$

$$a_3 = 0 + 0 = 1 + 1 = 0 + 0 = 1 + 0$$
$$a_3 = 0 = 0 = 0 = 1 \Longrightarrow a_3 = 0$$

Para encontrar o valor de a_0, calculamos:

$$\begin{aligned} r - (a_1v_1 + a_2v_2 + a_3v_3) &= r - (1.v_1 + 0.v_2 + 0.v_3) \\ &= 01010100 - 01010101 \\ &= 00000001 \end{aligned}$$

Como a maioria dos dígitos da palavra encontrada são iguais a zero, então, $a_0 = 0$. Deste modo, encontramos a palavra transmitida calculando:

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3$$
$$c = 0.v_0 + 1.v_1 + 0.v_2 + 0.v_3$$

$c = v_1 = 01010101$*, que é a palavra transmitida corrigida de um erro.*

4 O Código da Mariner 9

A nave espacial Mariner 9 ([11]) transmitiu para a Terra 7.329 fotografias, em preto e branco, que cobriram mais de 80% da superfície do planeta Marte. Estas fotografias revelaram leitos de rios, crateras, vulcões extintos, e um sistema de canyons com mais de 4.000 km de extensão, denominados “Valles Mariners", em homenagem a nave espacial Mariner 9. Foram encontradas evidências de erosão eólica e hídrica, frentes meteorológicas, nevoeiros, e ainda, registradas as primeiras imagens das luas de Marte; Phobos e Deimos. Também foi obtida uma revelação surpreendente, a grande cratera encontrada em Marte, era um vulcão extinto, hoje chamado de “Monte Olimpo"(Figura 1), que possui mais de 20 km de altitude.

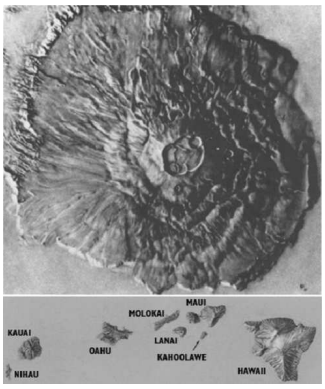


Figura 1. Monte Olimpo em comparação com o arquipélago do Havai. Fonte NASA

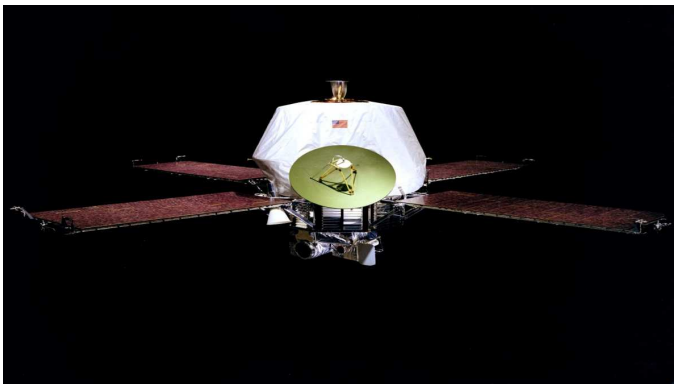


Figura 2. Nave Espacial Mariner 9. Fonte NASA

O código utilizado para a detecção e correção de erros dos dados enviados pela nave espacial Mariner 9 (Figura 2), à Terra, pertence à família de Códigos de Reed-Muller de Primeira Ordem, $R(1, m)$, para $m = 5$, ou seja, o código da Mariner 9 é o $R(1, 5)$.

Conforme visto, os parâmetros desse código são:

$$n = 32$$

$$M = 64$$

$$d = 16$$

Portanto,

- cada palavra deste código contém um comprimento igual a 32, ou seja, é uma sequência de 32 dígitos $0's$ e $1's$: isto significa que a codificação de canal, dada pelo $R(1, 5)$, transformou sequências binárias de 6 dígitos em sequências binárias de 32 dígitos, acrescentando 26 dígitos à codificação da fonte, através da multiplicação do código da fonte pela matriz geradora do código $R(1, 5)$.

- o código utilizado pela Mariner 9 possui 64 palavras: isto consiste em atribuir, pela codificação da fonte, a 64 tons de cinza pré-estabelecidos, sequências binárias de comprimento 6, sendo o branco denotado por 000000 e o preto por 111111. Já pela

codificação de canal do $R(1,5)$ essas sequências binárias de comprimento 6 são transformadas em sequências binárias de comprimento 32, as quais representam os mesmos 64 tons de cinza, sendo o branco denotado por $\underbrace{000\ldots0}_{32}$ e o preto por $\underbrace{111\ldots1}_{32}$.

- esse código detecta até 15 erros e corrige até 7 erros.

Exemplo 4.1 *Como exemplo, se* $b = 000011$ *representa uma determinada tonalidade de cinza, ao multiplicarmos* b *pela matriz* $G(1,5)$ *geradora do código* $R(1,5)$*,*

$$\begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{bmatrix}_{6\times32}$$

obtemos

$c = 00000000111111111111111100000000$ *que é a mesma tonalidade de cinza, porém, representada agora com* 32 *dígitos, para possibilitar a detecção e correção de possíveis erros que podem ocorrer durante a transmissão.*

4.1 Decodificação da Mariner 9

Um dos motivos da utilização do código Reed-Muller $R(1,5)$ pela nave Mariner 9, é por causa do seu algoritmo de decodificação, visto na seção 3.4. Seja a matriz $G(1,5)$

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

As linhas dessa matriz formam uma base para o código $R(1,5)$ que identificaremos como $\{v_0, v_1, v_2, v_3, v_4, v_5\}$, nesta sequência, da primeira até a sexta linha. Qualquer vetor c do código é uma combinação linear destes vetores, isto é,

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5, \text{ onde } a_i \in \mathbb{F}_2.$$

Assim, se nenhum erro ocorrer, qualquer vetor c do código $R(1,5)$ é da forma:

$c = (c_0, c_1, \ldots, c_{31}) = (a_0, a_1, a_2, a_3, a_4, a_5).G(1,5) = (a_0, a_0+a_1, a_0+a_2, a_0+a_1+a_2, a_0+a_3,$
$a_0+a_1+a_3, a_0+a_2+a_3, a_0+a_1+a_2+a_3, a_0+a_4, a_0+a_1+a_4, a_0+a_2+a_4, a_0+a_1+a_2+a_4,$
$a_0+a_3+a_4, a_0+a_1+a_3+a_4, a_0+a_2+a_3+a_4, a_0+a_1+a_2+a_3+a_4, a_0+a_5, a_0+a_1+a_5,$
$a_0+a_2+a_5, a_0+a_1+a_2+a_5, a_0+a_3+a_5, a_0+a_1+a_3+a_5, a_0+a_2+a_3+a_5, a_0+a_1+a_2+a_3+a_5,$
$a_0+a_4+a_5, a_0+a_1+a_4+a_5, a_0+a_2+a_4+a_5, a_0+a_1+a_2+a_4+a_5, a_0+a_3+a_4+a_5,$

$a_0 + a_1 + a_3 + a_4 + a_5, a_0 + a_2 + a_3 + a_4 + a_5, a_0 + a_1 + a_2 + a_3 + a_4 + a_5$).

Logo, temos:

$a_1 = c_0 + c_1 = c_2 + c_3 = c_4 + c_5 = c_6 + c_7 = c_8 + c_9 = c_{10} + c_{11} = c_{12} + c_{13} = c_{14} + c_{15} = c_{16} + c_{17} = c_{18} + c_{19} = c_{20} + c_{21} = c_{22} + c_{23} = c_{24} + c_{25} = c_{26} + c_{27} = c_{28} + c_{29} = c_{30} + c_{31}$

$a_2 = c_0 + c_2 = c_1 + c_3 = c_4 + c_6 = c_5 + c_7 = c_8 + c_{10} = c_9 + c_{11} = c_{12} + c_{14} = c_{13} + c_{15} = c_{16} + c_{18} = c_{17} + c_{19} = c_{20} + c_{22} = c_{21} + c_{23} = c_{24} + c_{26} = c_{25} + c_{27} = c_{28} + c_{30} = c_{29} + c_{31}$

$a_3 = c_0 + c_4 = c_1 + c_5 = c_2 + c_6 = c_3 + c_7 = c_8 + c_{12} = c_9 + c_{13} = c_{10} + c_{14} = c_{11} + c_{15} = c_{16} + c_{20} = c_{17} + c_{21} = c_{18} + c_{22} = c_{19} + c_{23} = c_{24} + c_{28} = c_{25} + c_{29} = c_{26} + c_{30} = c_{27} + c_{31}$
$a_4 = c_0 + c_8 = c_1 + c_9 = c_2 + c_{10} = c_3 + c_{11} = c_4 + c_{12} = c_5 + c_{13} = c_6 + c_{14} = c_7 + c_{15} = c_{16} + c_{24} = c_{17} + c_{25} = c_{18} + c_{26} = c_{19} + c_{27} = c_{20} + c_{28} = c_{21} + c_{29} = c_{22} + c_{30} = c_{23} + c_{31}$

$a_5 = c_0 + c_{16} = c_1 + c_{17} = c_2 + c_{18} = c_3 + c_{19} = c_4 + c_{20} = c_5 + c_{21} = c_6 + c_{22} = c_7 + c_{23} = c_8 + c_{24} = c_9 + c_{25} = c_{10} + c_{26} = c_{11} + c_{27} = c_{12} + c_{28} = c_{13} + c_{29} = c_{14} + c_{30} = c_{15} + c_{31}$

Se não ocorrer nenhum erro na transmissão da mensagem c, cada uma das 16 equações em cada linha acima resultará no valor de $a_i = 1, 2, 3, 4, 5$ correspondente. Caso ocorra erro na transmissão da palavra c, a palavra recebida será $r = (r_0, r_1, \cdots, r_{31})$ e, neste caso, os valores dos $a_i's$ serão dados por:

$a_1 = r_0 + r_1 = r_2 + r_3 = r_4 + r_5 = r_6 + r_7 = r_8 + r_9 = r_{10} + r_{11} = r_{12} + r_{13} = r_{14} + r_{15} = r_{16} + r_{17} = r_{18} + r_{19} = r_{20} + r_{21} = r_{22} + r_{23} = r_{24} + r_{25} = r_{26} + r_{27} = r_{28} + r_{29} = r_{30} + r_{31}$

$a_2 = r_0 + r_2 = r_1 + r_3 = r_4 + r_6 = r_5 + r_7 = r_8 + r_{10} = r_9 + r_{11} = r_{12} + r_{14} = r_{13} + r_{15} = r_{16} + r_{18} = r_{17} + r_{19} = r_{20} + r_{22} = r_{21} + r_{23} = r_{24} + r_{26} = r_{25} + r_{27} = r_{28} + r_{30} = r_{29} + r_{31}$

$a_3 = r_0 + r_4 = r_1 + r_5 = r_2 + r_6 = r_3 + r_7 = r_8 + r_{12} = r_9 + r_{13} = r_{10} + r_{14} = r_{11} + r_{15} = r_{16} + r_{20} = r_{17} + r_{21} = r_{18} + r_{22} = r_{19} + r_{23} = r_{24} + r_{28} = r_{25} + r_{29} = r_{26} + r_{30} = r_{27} + r_{31}$

$a_4 = r_0 + r_8 = r_1 + r_9 = r_2 + r_{10} = r_3 + r_{11} = r_4 + r_{12} = r_5 + r_{13} = r_6 + r_{14} = r_7 + r_{15} = r_{16} + r_{24} = r_{17} + r_{25} = r_{18} + r_{26} = r_{19} + r_{27} = r_{20} + r_{28} = r_{21} + r_{29} = r_{22} + r_{30} = r_{23} + r_{31}$

$a_5 = r_0 + r_{16} = r_1 + r_{17} = r_2 + r_{18} = r_3 + r_{19} = r_4 + r_{20} = r_5 + r_{21} = r_6 + r_{22} = r_7 + r_{23} = r_8 + r_{24} = r_9 + r_{25} = r_{10} + r_{26} = r_{11} + r_{27} = r_{12} + r_{28} = r_{13} + r_{29} = r_{14} + r_{30} = r_{15} + r_{31}$

Depois de serem feitos todos estes cálculos, vamos obter pelo menos 9 dos 16 valores correspondentes para cada a_i, sendo assim, o valor correto será obtido pela maioria dos dígitos de cada a_i, isto é, o dígito que mais aparece na igualdade é o que será tomado como a_i. Finalmente, a_0 pode ser determinado pela maioria dos dígitos de:

$$r - (a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5).$$

Assim, a mensagem transmitida corrigida de até 7 erros pode ser recuperada fazendo:

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5$$

Vamos mostrar como funciona o algoritmo com o exemplo a seguir.

Exemplo 4.2 *Seja a mensagem transmitida* $c = 0101\mathbf{01}0101010\mathbf{1}0101010\mathbf{01}0101010\mathbf{01}$ *e, recebida a mensagem* $r = 0101\mathbf{10}0101011101010\mathbf{10}0101010\mathbf{10}$ *com* 7 *erros. Usando o algoritmo de Decodificação Reed desenvolvido por Irving Stoy Reed para decodificar os códigos Reed-Muller e, em especial, para decodificar o código* $R(1,5)$*, temos:*

$a_1 = 1 = 1 = 1 = 1 = 1 = 1 = 0 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1$, *assim* $a_1 = 1$.
$a_2 = 0 = 0 = 1 = 1 = 0 = 0 = 1 = 0 = 0 = 0 = 1 = 1 = 0 = 0 = 1 = 1$, *assim* $a_2 = 0$.
$a_3 = 1 = 1 = 0 = 0 = 1 = 0 = 0 = 0 = 1 = 1 = 0 = 0 = 0 = 0 = 1 = 1$, *assim* $a_3 = 0$.
$a_4 = 0 = 0 = 0 = 0 = 0 = 1 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 1 = 1 = 1 = 1$, *assim* $a_4 = 0$.
$a_5 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 0 = 1 = 0 = 1 = 1$, *assim* $a_5 = 0$.
Segue, então que, para encontrar o valor de a_0*, fazemos:*

$r - (a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5) = 0101100101011101010110010101011 0 -$
$[1.(01010101010101010101010101010101) + 0.(00110011001100110011001100110011) +$
$0.(00001111000011110000111100001111) + 0.(00000000111111110000000011111111) +$
$0.(00000000000000001111111111111111)] = 00001100000010000000110000000011.$

Como a maioria dos dígitos do resultado é zero, então, este é o valor de a_0*, ou seja,* $a_0 = 0$.

Desta forma, a mensagem transmitida c, corrigida dos 7 *erros, é obtida por:*

$$c = a_0v_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5 = 0.v_0 + 1.v_1 + 0.v_2 + 0.v_3 + 0.v_4 + 0.v_5$$

Portanto, $c = v_1 = 01010101010101010101010101010101$*, é a mensagem transmitida do código* $R(1,5)$*, código de canal, corrigida dos* 7 *erros, que representa a tonalidade de cinza* $b = 010000$*, código da fonte.*

Referências

[1] LABORATORY, J. P. California Institute of Technology. Disponível em http://www.jpl.nasa.gov. Acesso em 12/01/2016.

[2] HEFEZ, A.; VILLELA, M. L. Códigos corretores de erros. 1ª ed. Rio de Janeiro: IMPA, 2002.

[3] POLCINO, C. M. Breve introdução à teoria dos códigos corretores de erros. São Paulo: IME-USP, 2009.

[4] MENEGHESSO, C. Códigos Corretores de Erros. Disponível em https://www.dm.ufscar.br/dm/index.php/component/attachments/download/40 Acesso em 17/10/2017.

[5] KOCH, H. C. R. Códigos Corretores de Erros e Teoria de Galois. Disponível em http://www.mtm.ufsc.br/ ebatista/2016-1/Helena.pdf Acesso em 17/10/2017.

[6] VICENTE, A. G. Um estudo dos Códigos de Reed Muller. Disponível em https://repositorio.ufsc.br/bitstream/handle/123456789/157503/201961.pdf Acesso em 17/10/2017.

[7] RAAPHORST, S. Reed-Muller Codes. Disponível em http://citeseerx.ist.psu.edu /viewdoc/download?doi=10.1.1.115.3214&rep=rep1&type=pdf. Acesso em 17/10/2017.

[8] MALEK, M. Coding Theory. Disponível em http://www.mcs.csueastbay.edu/∼malek /Class/Reed-Muller.pdf. Acesso em 17/10/2017.

[9] CHEROWITZO, B. Reed-Muller Codes. Disponível em http://www-math.ucdenver.edu/ wcherowi/courses/m7823/reedmuller.pdf. Acesso em 17/10/2017.

[10] HOUAISS, A. Dicionário Houaiss da Língua Portuguesa. 1.ed. Rio de Janeiro: Objetiva, 2009.

[11] NASA JPL. Mariner 9 Mars Exploration. Disponível em http://www.youltube.com/watch?v=JTNyoUj4mBI. Acesso em 20/01/2016.

Uma Apresentação do Teorema de Mamikon

Mamikon's Theorem Revisited

Eloy Nicotera Junior
Universidade Federal do ABC - UFABC, Santo André, SP
eloynjunior@gmail.com

Sinuê Dayan Barbero Lodovici
Universidade Federal do ABC - UFABC, Santo André, SP
sinue@ufabc.edu.br

Resumo: O Teorema de Mamikon apresenta caminhos geométricos alternativos ao Cálculo para determinação de áreas. Este método tem uma abordagem dinâmica e requer poucos conhecimentos de Matemática Superior, o que nos permite a apresentação do assunto para alunos ainda nos anos iniciais do ensino básico. Por ser um trabalho recente, quase todos os trabalhos e artigos sobre o teorema são publicações do próprio Mamikon e de seus colaboradores. Acreditamos, porém, que esta seja a primeira apresentação desse em português. Neste artigo apresentamos o desenvolvimento do teorema, contando com uma abordagem intuitiva e visual de fácil entendimento, principalmente se apresentadas com softwares de visualização como o Geogebra[1]. Apresentamos, então, aplicações para o cálculo da área sob a curva de algumas das principais funções estudadas tanto pelos alunos do ensino básico como superior. Finalizamos o artigo com uma apresentação da demonstração formal do teorema fundamentada em Geometria Diferencial.

Palavras-chave: teorema de Mamikon; cálculo visual; geometria; geometria dinâmica; geometria diferencial.

Abstract: Mamikon's Theorem brings us an alternative geometric approach on evaluating some areas to Differential Calculus. The theorem offers a dynamic appeal which enables someone to teach this subject even to high school students with little mathematical background. Due to the fact that such a result is recent, almost every paper and article about the subject was written by Mamikon himself and his collaborators. As so, we believe that this is the first work on the subject written in Portuguese. Here, we try to present this theorem with a simple, visual and intuitive approach that could be easily grasped by anyone, mainly if supported by a software such as Geogebra. Some applications with well-known functions were also presented. We conclude this article by presenting a formal proof of theorem with Differential Geometry.

Key words: Mamikon's theorem; visual calculus; geometry; dynamic geometry; differential geometry.

[1] http://www.geogebra.org

Recebido em 07/09/2017 - Aceito em 28/11/2017

1 Introdução

Este trabalho tem como base o livro *New Horizons in Geometry* [1], de Tom Apostol e Mamikon Mnatsakanian, que traz uma abordagem visual e inovadora, com métodos geométricos que requerem pouco ou nenhuma fórmula, para resolver muitos problemas clássicos do Cálculo. Como tal, grande parte dos resultados e aplicações aqui presentes são uma releitura e um detalhamento daquilo ali apresentado.

Nos próximos parágrafos desta introdução, por exemplo, apresentamos uma tradução livre de parte do prefácio que Tom. M. Apostol escreveu para seu livro com Mamikon Mnatsakanian.

Mamikon concebeu as ideias principais de seu trabalho em 1959, quando estudante de graduação na *Yerevan University* na Armênia. Ainda jovem, apresentou seu método para matemáticos soviéticos, porém estes o desincentivaram dizendo *"Não pode estar certo. Você não pode resolver problemas de Cálculo tão facilmente"*.

Posteriormente, Mamikon obteve o título de Ph.D. em Física e tornou-se professor de astrofísica da *Yerevan University*. Mamikon publicou seu trabalho em 1981, mas não conseguiu com ele grande repercussão, provavelmente, por ter publicado em russo em um jornal armênio de circulação limitada [8].

Em 1990, Mamikon viajou para a Califórnia com o objetivo de estudar terremotos. Quando a União Soviética colapsou, Mamikon ficou extraditado nos Estados Unidos e com o auxílio de alguns matemáticos começou a trabalhar na *UC Davis* e para o Departamento de Educação da Califórnia, onde desenvolveu seu método como uma ferramenta de ensino universal onde alunos podiam realizar experimentos com a ajuda de computadores e diagramas. Ele ensinou seu método em diversas escolas, desde o Ensino Fundamental até o Ensino Médio e demonstrava-o para professores em conferências. Tanto os professores quanto os alunos ficaram entusiasmados, pois este método dinâmico não requer um grande formalismo da Álgebra, Trigonometria ou Cálculo.

Alguns anos mais tarde, em visita à *Caltech*, Mamikon conheceu Tom Apostol[2] e mostrou a ele os potenciais que seu método poderia trazer para o ensino de Matemática, especialmente quando combinado com as ferramentas modernas de visualização que a tecnologia trouxe. Desde então, Mamikon e Apostol publicaram 30 trabalhos em conjunto, a maioria na área da Geometria. Juntos conquistaram três *Lester R. Ford Awards*[3] por cinco trabalhos publicado na *American Mathematical Monthly*, em 2004, 2007 e 2009.

O método de Mamikon requer simples conceitos matemáticos e sempre que possível apela para o toque intuito dos alunos para chegar a resultados e conclusões surpreendentes. De maneira geral, Mamikon e Apostol abordam a geometria clássica com uma visão moderna bem como a geometria moderna utilizando-se de um toque clássico. Os resultados discutidos pelos autores são inovadores e, quando não, apresentam abordagens não usuais para obter generalizações inesperadas.

O trabalho destes autores pode trazer para os alunos do ensino básico um primeiro contato com problemas normalmente resolvidos com o uso do Cálculo e de Equações Diferenciais. Com seu teorema, muitos destes problemas podem ser resolvidos apelando para noções da Geometria e um toque de imaginação para abordar as figuras de uma forma dinâmica.

Nossa contribuição pessoal para o problema encontra-se principalmente no maior detalhamento das aplicações e na demonstração apresentada na Seção 4. Nossa demonstração

[2]Tom Apostol é membro da *Caltech* desde 1950. Apostol atua na área de Teoria dos Números e é autor de mais de 100 trabalhos e 61 livros, dentre os quais estão os dois volumes de Cálculo publicados e traduzidos para diversos idiomas há mais de 50 anos.

[3]Prêmio concedido aos melhores artigos publicados no periódico *American Mathematical Monthly*.

difere ligeiramente da demonstração apresentada por Mamikon e Apostol no apêndice de [1], pois naquela o uso de uma mudança de variáveis numa integral torna, a nosso ver, sua apresentação não muito clara para o caso de curvas não planas. Tentamos também adicionar alguns comentários no intuito de tornar os teoremas expostos matematicamente mais precisos que nas referências originais. Por fim, disponibilizamos em goo.gl/xKkMXj uma apresentação dinâmica, utilizando o software Geogebra, de alguns dos resultados aqui tratados.

2 Formulação do Teorema de Mamikon

Nesta seção trazemos as ideias iniciais do teorema partindo de sua forma mais simples, calcular a área de uma coroa circular, até sua forma completa que pode ser usada para o cálculo da área de algumas superfícies geradas à partir de curvas no espaço.

2.1 Evolução do Teorema

O método de Mamikon teve início com um simples problema de geometria, muitas vezes apresentado aos alunos do final do Ensino Fundamental. Determinar a área de uma coroa circular dado uma corda, de comprimento a, da circunferência maior que seja tangente à circunferência interior.

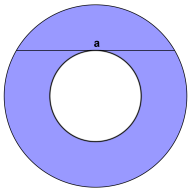


Figura 1. Coroa circular.

Este problema é facilmente resolvido observando que a circunferência menor de raio r tem área πr^2 e a circunferência maior de raio R tem área πR^2, então a área da coroa circular será dada por $\pi R^2 - \pi r^2 = \pi(R^2 - r^2)$. Mas os raios e o segmento de comprimento a formam um triângulo retângulo de catetos $a/2$ e r e hipotenusa R, então pelo Teorema de Pitágoras temos que $R^2 - r^2 = (a/2)^2$. Logo, a área procurada será $\pi a^2/4$. Ou seja, a resposta depende apenas do comprimento de a e não dos raios das circunferências.

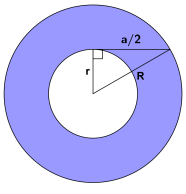


Figura 2. Coroa circular e o triângulo retângulo.

Mamikon notou que se soubéssemos que a resposta dependia apenas de a poderia haver outra forma de abordar o problema. Como os comprimentos dos raios, mantida a corda de comprimento a, não influenciam na resposta poderíamos imaginar em diminuir linearmente

o raio das circunferências até que o raio r da circunferência menor ficasse nulo (e a circunferência menor degenerasse para um ponto apenas). Nesse ponto nossa figura se tornaria apenas um disco de diâmetro a e, logo, sua área seria $\pi a^2/4$. Mamikon perguntou-se ainda se haveria outra forma de mostrar que a resposta dependia apenas de a. Trouxe, então, uma ideia dinâmica ao problema.

Interpretando a metade da corda como um vetor de comprimento $L = a/2$ tangente à circunferência interior, observamos que, movendo este vetor sobre a circunferência de modo a manter sua tangência a mesma, ele varre toda a região da coroa circular. Intuitivamente, a área da coroa poderia ser então determinada "somando" o comprimento dos vetores criados durante esse movimento de rotação.

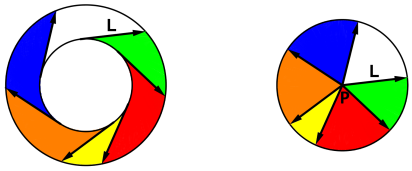


Figura 3. Coroa varrida pelo vetor de comprimento fixo e a região composta pela translação dos vetores .

Observe, porém, que transladando estes vetores paralelamente de modo que a origem destes coincida (esteja sobre um único ponto) criamos um círculo de raio L (veja Figura(3)). Assim, uma maneira de analisarmos a área, é verificar que a medida que o vetor de comprimento L se move pela coroa, ele descreve em sua imagem com origem fixa uma rotação ao redor de um ponto P, desenhando, dessa forma, um círculo de raio L. Portanto, as duas regiões teriam áreas equivalentes, o que de fato ocorre.

Também foi percebido que esta dinâmica poderia ser aplicada quando trocamos a circunferência interior por uma curva simples, fechada e convexa qualquer, a qual nos referiremos no artigo simplesmente como *forma oval*. Na Figura 4 mostramos a mesma ideia usando duas elipses.

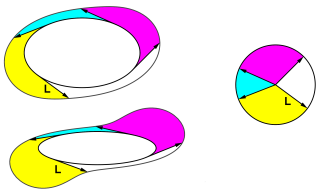


Figura 4. Tangente às elipses varrendo a coroa oval.

Enquanto o segmento tangente de tamanho fixo move-se ao longo das elipses ela descreve uma região que chamaremos de *coroa oval*[4].

Novamente transladando cada segmento para o vértice comum P enquanto a tangente desliza pelas elipses, sua imagem gera um círculo de raio L. Então a área da coroa oval deve ser igual à área do círculo de raio L.

Veja que neste caso não podemos utilizar o Teorema de Pitágoras e, para determinar a área, provavelmente teríamos que recorrer ao Cálculo, caindo em uma tarefa não muito

[4]No original, *Oval Ring*.

trivial. Inicialmente deveríamos determinar uma equação para a curva interior, em seguida usar sua derivada para descrever a área varrida por um vetor tangente.

Ao longo deste artigo usaremos a expressão *"área da região definida por uma tangente"* para nos referir a áreas, como as coroas ovais acima descritas, delimitadas por uma curva base e pela curva descrita pela extremidade de um vetor que se desloca mantendo sua tangência à tal curva base. A expressão *"feixe de tangentes"* será usada, então, para descrever a região varrida por esses mesmos vetores quando tomados todos com origem num ponto comum. No caso das coroas ovais, o feixe de tangentes seria o círculo de raio L.

2.2 "Demonstração" por polígonos

Ao invés de uma circunferência ou elipse como base da nossa figura, poderíamos considerar um polígono convexo? A resposta é sim. A propósito é muito mais fácil observar a relação entre a área da região definida por uma tangente e do feixe de tangentes quando consideramos polígonos. Abaixo mostramos um triângulo e a região descrita por seus segmentos tangentes.

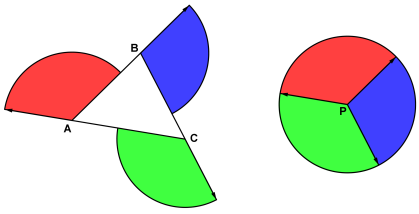


Figura 5. Tangente de comprimento constante movendo-se pelo triângulo.

Como os lados do triângulo são suportados por retas, durante seu deslocamento entre os vértices, a tangente não muda de direção, logo não descreve nenhuma área ao se mover. A área da região definida por uma tangente, nesse caso, surge durante a mudança de direção que ocorre quando a tangente passa por um dos vértices em direção ao lado consecutivo do triângulo, onde irá descrever um setor circular com raio igual ao comprimento do segmento.

Ao percorrer o perímetro do triângulo a tangente irá descrever três setores circulares de mesmo raio e que juntos completarão um círculo de raio igual ao comprimento dessa tangente.

O mesmo vale para um polígono convexo qualquer. Em um polígono com n lados a tangente irá descrever n setores circulares. Se lembrarmos que a soma de todos os ângulos externos de um polígono convexo é sempre 360^o e observarmos que os setores circulares varridos pela tangente descrevem exatamente esses ângulos, é fácil verificar que o feixe de tangentes, nesse caso, formará também um círculo.

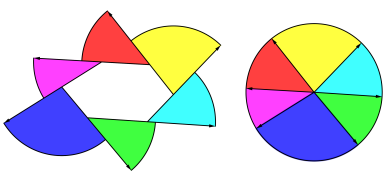


Figura 6. Tangente de comprimento constante movendo-se pelo hexágono.

Assim, a área da região varrida pela tangente ao caminhar pelos lados do polígono será igual à área do círculo cujo raio é o comprimento do segmento tangente.

Considerando agora a área da região definida por uma tangente de uma forma oval qualquer como o limite das áreas descritas por polígonos convexos inscritos cujo número de lados tende ao infinito e cujos comprimentos tendem a zero, concluímos:

Teorema 12 (Teorema de Mamikon para coroas ovais) *A área de uma coroa oval obtida por uma tangente de comprimento L de uma forma oval qualquer é sempre igual a πL^2.*

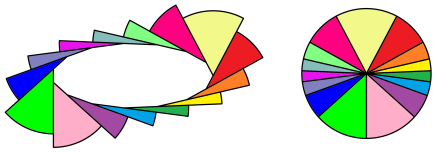


Figura 7. Tangente de comprimento constante movendo-se por um polígono convexo de muitos lados.

2.3 Área da região definida por uma tangente de comprimento constante sobre uma curva sem inflexões

Imaginando uma curva plana como o caminho percorrido por um ente móvel, chamamos de *ponto de inflexão* um ponto onde a concavidade da curva se inverte, ou seja, um ponto onde o sentido de rotação descrito pelo ente móvel se inverte.

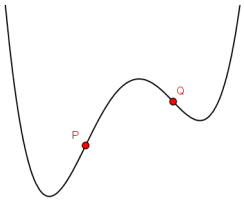


Figura 8. Curva com inflexão nos pontos P e Q.

Considere uma curva plana suave sem inflexões[5], que chamaremos de *curva de tangência* τ. A reunião de todos os segmentos tangentes de comprimento constante define uma região que é cercada por τ e por uma curva superior σ definida pela outra extremidade dos segmentos. A forma desta região depende da curva τ e do comprimento do segmento tangente que vai de τ até σ. Nos referiremos a esta região novamente como a *região definida pela tangente*.

[5]Curvas suaves são curvas descritas por uma função $f : I \subset \mathbb{R} \to \mathbb{R}^2$ que têm todas as derivadas f', f'', f''' ... contínuas.

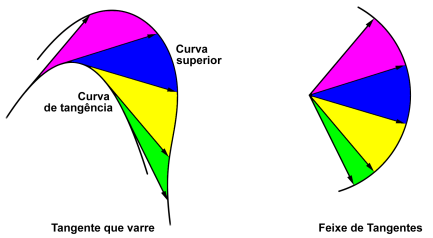


Figura 9. O feixe de tangentes correspondente à região definida pela tangente de comprimento constante é um setor circular.

Quando cada segmento é transladado paralelo de modo que o ponto de tangência de todos seja trazido a um ponto comum teremos a região definida como feixe de tangentes. Notamos que poderíamos ter trazido a outra extremidade de cada segmento a um ponto comum, gerando um feixe de tangentes simétrico ao anterior.

Como cada segmento tem comprimento constante o feixe de tangentes é um setor circular cujo raio é o comprimento do segmento.

Visto que área descrita pela tangente sobre uma curva suave simples sem inflexões pode ser vista como uma parte de uma coroa oval segue imediatamente do Teorema 12 o resultado:

Teorema 13 (Teorema de Mamikon para tangentes de comprimento constante) *A área descrita pela tangente sobre uma curva suave simples sem inflexões τ é igual à área do setor circular que forma o feixe de tangentes correspondente. Tal setor independe da forma da curva, dependendo apenas da variação angular total descrita pela tangente durante o percurso ao longo da curva. Ou seja, se as tangentes de comprimento L nos pontos inicial e final descrevem ângulo θ, então a área da região definida por uma tangente é $\frac{\theta L^2}{2}$.*

Podemos ver esta aplicação no mundo real observando uma bicicleta fazendo uma mudança de trajetória. A roda da frente da bicicleta traça uma curva enquanto a roda traseira traça uma outra.

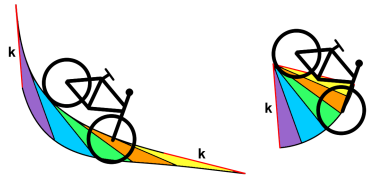


Figura 10. Determinar a área da região entre as marcas das duas rodas da bicicleta.

A área descrita pela tangente, desde que o percurso da roda traseira não cruze com o percurso da roda dianteira, tem área igual a um setor circular dependendo apenas do comprimento da bicicleta e da mudança de ângulo entre a posição inicial e a posição final conforme mostramos acima[6].

[6]Situações mais gerais da bicicleta podem sem vistas em [1].

2.4 Tangente com comprimento variável.

Trazemos agora uma ideia um pouco mais abrangente, onde os segmentos tangentes que partem de τ até a curva σ não precisam ter um comprimento constante. Considere a região definida por uma tangente com comprimento variável e o feixe de tangentes correspondente quando trazemos todos os pontos de tangência para o ponto comum O, como ilustrado na Figura 11.

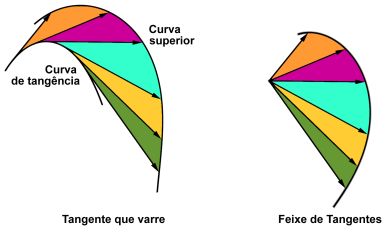


Figura 11. Tangente e feixe de tangentes com comprimento variável.

O Teorema de Mamikon sugere que ambas as figuras têm a mesma área. Essa verificação pode ser feita considerando o Teorema de Mamikon para segmentos tangentes de comprimento constante e ao fazer um recorte contínuo em uma região definida pela tangente de comprimento constante cada segmento cortado ao ser transladado para o feixe de tangentes trará uma perda de área equivalente à primeira figura. Logo, o Teorema pode ser aplicado também a uma tangente de comprimento variável. Ou seja:

Teorema 14 (Teorema de Mamikon para tangentes de comprimento variável) *A área descrita pela tangente a uma curva suave simples sem inflexões τ é igual à área do feixe de tangentes correspondente, mesmo que o comprimento da tangente varie ao longo do seu percurso em τ.*

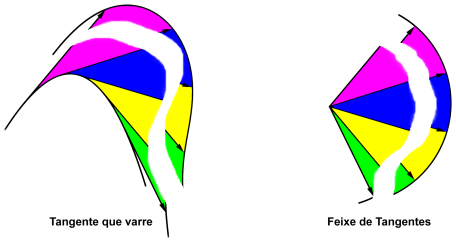


Figura 12. Os cortes retirados têm área equivalente.

2.5 Forma Geral do Teorema de Mamikon.

No caso mais geral do Teorema de Mamikon a curva inicial nem mesmo precisa ser plana. Podemos considerar qualquer curva suave no espaço com os segmentos tangentes variando seu tamanho.

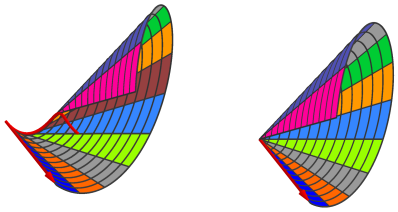


Figura 13. Tangentes e feixe de tangentes de uma curva espacial.

A área da região formada pelas tangentes ao percorrer uma curva espacial suave é igual à área de seu feixe de tangentes, que é descrito sobre uma "superfície cônica".

A região da tangente está sobre uma superfície desenvolvível[7] que pode ser desenrolada em um plano sem distorção de área. Novamente a forma descrita pela tangente depende apenas da curva inicial e de como os comprimentos e direção dos segmentos tangentes variam pela curva. Aqui, o feixe de tangentes de uma curva no espaço será uma superfície cônica cujo vértice é o ponto comum a que transladamos os segmentos tangentes (uma superfície que também pode ser desenrolada em um plano).

Ressaltamos que as ideias aqui apresentadas foram apresentadas de maneira visual e intuitiva. Uma demonstração formal dos resultados descritos será apresentada no final do artigo.

3 Aplicações

Nos anos iniciais dos cursos superiores na área de exatas somos apresentados ao Cálculo Diferencial e suas aplicações para determinar a área sob curvas. Estas ideias requerem uma base não tão modesta quanto aos conhecimentos matemáticos. Porém, com o Teorema de Mamikon, podemos apresentar algumas destas ideias e problemas a alunos do Ensino Médio, bastando que estes tenham conhecimentos básicos de Geometria e alguma noção sobre funções.

Para o uso do Teorema de Mamikon necessitamos de algum conhecimento o sobre retas tangentes e subtangentes. *Subtangente* é a projeção sobre um eixo, e especialmente sobre um eixo de coordenadas, do segmento da tangente compreendido entre o ponto de contato de uma curva e o ponto onde a tangente encontra o eixo considerado[8].

Nesta seção trazemos a discussão e aplicações do teorema a algumas funções e equações clássicas presentes nos ensinos fundamental e médio e em cursos de cálculo diferencial.

3.1 Pitágoras a partir de Mamikon

Assumindo verdadeiro o Teorema de Mamikon, podemos, usando a recíproca da ideia que originou o teorema, encontrar mais uma prova do Teorema de Pitágoras.

Considerando uma coroa circular onde a circunferência interior tem raio r e a circunferência exterior raio R, sabemos que sua área será dada pela diferença $\pi R^2 - \pi r^2$.

[7] Mais sobre este assunto pode ser visto em [6] e [9].
[8] Apresentamos tais conceitos mais detalhadamente em [9]

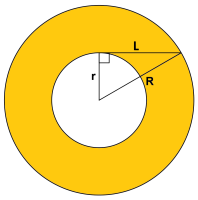


Figura 14. O Teorema de Mamikon implica o Teorema de Pitágoras.

Mas pelo Teorema de Mamikon vimos que sua área também é igual a πL^2, onde L é um segmento tangente à circunferência interior. Igualando as equações temos:

$$\begin{aligned} \pi R^2 - \pi r^2 &= \pi L^2 \\ R^2 - r^2 &= L^2 \\ r^2 + L^2 &= R^2 \end{aligned}$$

ou seja, o Teorema de Pitágoras.

3.2 Área sob o gráfico de funções Exponenciais

As funções exponenciais estão em toda parte nas aplicações da Matemática. Elas ocorrem em problemas relacionados ao crescimento populacional, decaimento radioativo, transmissão do fluxo de calor e outras situações físicas onde a taxa de crescimento/decrescimento de uma quantidade é proporcional à quantidade presente.

A curva exponencial é o gráfico de uma função que apresenta subtangente constante[9], fato este, que nos ajuda a calcular a área da região sobre o gráfico de uma função da forma $f(x) = e^{\frac{x}{b}}$ usando o *Teorema da tangente* de Mamikon.

Observando a Figura 15, notamos que ao traçar a reta tangente no ponto $(x, e^{\frac{x}{b}})$ dividimos a área sob a curva em duas partes. Um triângulo retângulo de área T, com catetos b e $e^{\frac{x}{b}}$, e a região sombreada à esquerda que vai de $-\infty$ até $x - b$ com área S. Esta região de área S pode ser, no entanto, descrita ao deslocarmos a tangente no sentido negativo sobre a curva, ou seja, esta é a *região definida pela tangente* da curva.

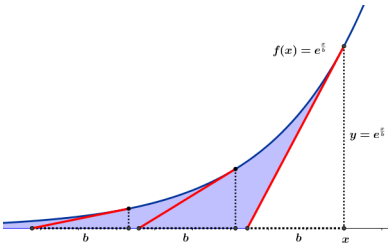


Figura 15. Região sombreada de área S e o triângulo de área T.

Deslocando cada segmento tangente para uma origem comum, o ponto $(x - b, 0)$, estaremos descrevendo o triângulo de área T.

[9]Sugerimos ao leitor interessado verificar tal propriedade com o axílio do livro [7].

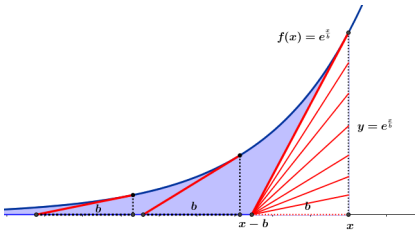


Figura 16. Segmentos tangentes transladados para o ponto $x - b$.

Essa equivalência se dá pelo fato das subtangentes serem constantes. Cada triângulo formado pelo segmento tangente tem base b e altura decrescendo de $e^{\frac{x}{b}}$ conforme x vai para $-\infty$.

Portanto, ao transladar os segmentos tangentes para $x - b$ estamos montando o *feixe de tangentes* da área S e pelo *Teorema de Mamikon* ambos possuem mesma área, $S = T$. Temos então, que a área sobre f de $-\infty$ à x será dada por duas vezes a área T.

$$2T = 2\frac{be^{\frac{x}{b}}}{2} = be^{\frac{x}{b}} \tag{1}$$

Na linguagem do cálculo, mostramos que:

$$\int_{-\infty}^{x} e^{\frac{t}{b}}\, dt = be^{\frac{x}{b}} \tag{2}$$

3.3 Área sob uma parábola

Uma outra função muito conhecida pelos alunos é a função quadrática, cuja curva é uma parábola. Esta função é vista desde o 9^o ano do Ensino Fundamental II, onde se trabalha com pontos de máximo/mínimo e raízes. Esse estudo estende-se, no Ensino Superior, com o cálculo da área sob a parábola em cursos de cálculo diferencial.

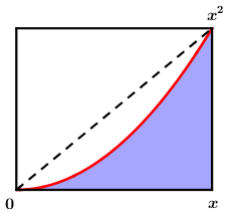


Figura 17. Segmento parabólico: região compreendida entre a curva e o eixo x.

Para a utilização do Teorema de Mamikon no cálculo da área sob uma curva de equação $y = x^2$ no intervalo $[0, x]$ consideramos o retângulo de base x e altura x^2 no qual o segmento parabólico está inscrito. Precisamos também de uma curva auxiliar $y = 2x^2$, a qual chamaremos de parábola bissetora.

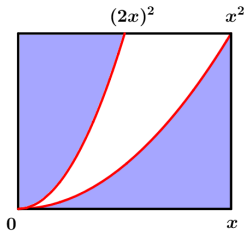


Figura 18. Parábola bissetora $y = (2x)^2$ e a parábola $y = x^2$ inscritas no retângulos.

As duas regiões à esquerda delimitadas pela parábola bissetora possuem mesma área. Este fato é melhor entendido tomando os segmentos de comprimento x_i paralelos ao eixo x na altura x_i^2. A parábola $y = (2x)^2$ divide estes segmentos ao meio e como as áreas podem ser obtidas com a "soma" destes segmentos (Princípio de Cavalieri) ambas serão iguais[10].

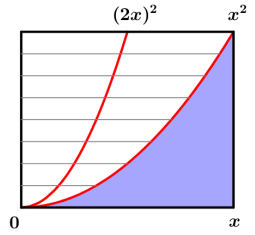


Figura 19. Segmentos de comprimento x_i divididos ao meio pela parábola bissetora.

Mostraremos agora que a região sob a parábola $y = x^2$ também é igual as duas outras partes.

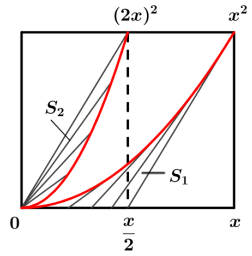


Figura 20. *Região definida pela tangente* S_1 e seu *feixe de tangentes* S_2.

Na Figura 20 o triângulo à esquerda e acima da parábola $(2x)^2$ e o triângulo abaixo de x^2 tem mesma área. Logo, reduzimos nosso trabalho a mostrar que as regiões sombreadas S_1, abaixo de x^2, e S_2, acima de $(2x)^2$, têm mesma área.

S_1 é a *região definida pela tangente* da parábola x^2. Tomando um segmento tangente à x^2 no ponto (t, t^2) sua outra extremidade no eixo x será $(\frac{t}{2}, 0)$. Transladando cada um

[10]O mesmo princípio é usado na soma de Riemann e também no Princípio de Cavalieri se aplicado ao plano (http://eaulas.usp.br/portal/video.action?idItem=2861).

destes segmentos em $\frac{t}{2}$ à esquerda os pontos $\left(\frac{t}{2},0\right)$ serão levados à origem e o ponto (t,t^2) será levado para $\left(\frac{t}{2},t^2\right)$, ou seja, sobre a parábola $(2x)^2$. Logo, a região S_2 é o *feixe de tangentes* relacionado à região definida pela tangente S_1 e pelo Teorema de Mamikon têm mesma área.

Concluímos então, que cada região apresentada na Figura 18 têm área equivalente a um terço da área do retângulo, mostrando que a área sob a parábola $y = x^2$ é $\frac{x^3}{3}$.

De maneira análoga, utilizando o Teorema de Mamikon, podemos mostrar que a área compreendida entre o eixo x e uma curva $y = x^r$, com $r > 0$ é dada por:[11].

$$\int_0^x t^r \, dt = \frac{x^{r+1}}{r+1} \tag{3}$$

3.4 Área sob o gráfico de potências com expoente negativo

Podemos também para determinar a área sob o gráfico de $f(x) = x^{-r}$, com $r > 1$ usando o Teorema da Tangente de Mamikon. A área abaixo de f é composta pelo triângulo de área T e a *região definida pela tangente* de área S.

Na Figura 21, o *feixe de tangentes* de S obtido ao transladar cada segmento tangente para a origem. A curva do *feixe de tangentes* tem sua equação paramétrica em função do vetor tangente à f, ou seja $v(t) = (-s(t), -f(t))$, onde $s(t) = -\frac{t}{r}$. Pelo Teorema de Mamikon estas regiões têm mesma área S. Note que adjacente ao *feixe de tangentes* temos também um triângulo de área T.

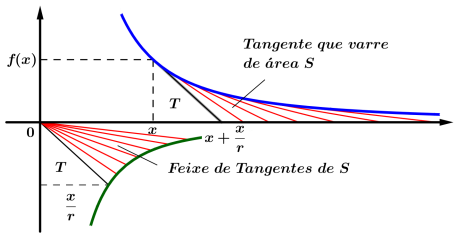


Figura 21. *Região definida pela tangente* e seu *feixe de tangentes*.

Refletindo o *feixe de tangentes* e o triângulo pelo eixo x teremos uma região congruente com área $S + T$. Agora, estendendo esta região por um fator r, isto é, multiplicando cada coordenada x por um fator r, teremos uma nova região cuja área será $r(S + T)$.

[11] Estes casos podem ser melhor analisados em [9]

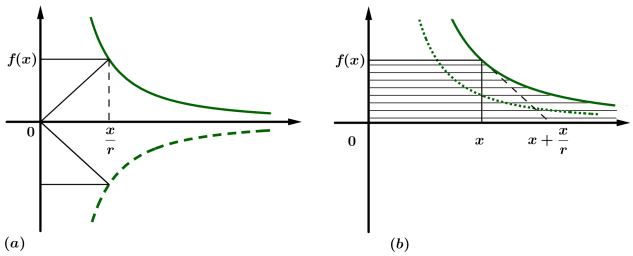


Figura 22. (a) Reflexão da área do *feixe de tangentes* e do triângulo (b) Região de (a) com cada coordenada x multiplicada por r.

Note que como a curva do *feixe de tangentes* é dada por $s(t) = (-s(t), -f(t)) = \left(\frac{t}{r}, -t^{-r}\right)$, ao refleti-la pelo eixo y e multiplicando a primeira coordenada por r, obteremos a curva original (t, t^{-r}).

Portanto, esta área redimensionada é composta por um retângulo de área R e a região original de área $S + T$ da figura 21. Logo, $r(S + T) = R + (S + T)$, e novamente:

$$S + T = \frac{R}{r - 1} = -\frac{x^{-r+1}}{(-r + 1)} \tag{4}$$

3.5 Uma aplicação reversa do teorema de Mamikon: área da região delimitada por $f(\theta) = \tan\theta$.

Em algumas das aplicações apresentadas conseguimos calcular a área da *região definida pela tangente* a partir da área do seu *feixe de tangentes*, que era mais fácil de ser determinado. Em alguns casos, porém, podemos usar o Teorema de Mamikon na direção inversa se a área da *região definida pela tangente* for mais simples de ser calculada do que a área do seu *feixe de tangentes*.

Mostraremos aqui uma prova geométrica para a fórmula:

$$\int_0^x \tan^2\theta \; d\theta = \tan x - x \tag{5}$$

Na Figura 23 (a) vemos o gráfico polar da equação $r(\theta) = \tan\theta$ enquanto θ varia de 0 à x. A área sombreada $A(x)$, formada por cada segmento com uma das extremidades na origem e a outra na curva r, é dada por:

$$A(x) = \frac{1}{2}\int_0^x r(\theta)^2 \; d\theta = \frac{1}{2}\int_0^x \tan^2\theta \; d\theta \tag{6}$$

Considere uma circunferência de raio unitário onde cada segmento tangente é cortado pela reta que passa em seu centro, mostrado na figura (b).

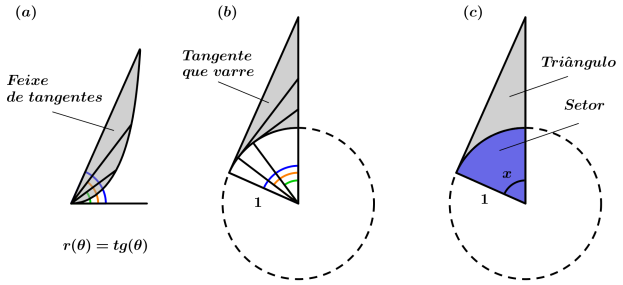


Figura 23. (a) A região à esquerda é o *feixe de tangentes* da *região definida pela tangente* em (b),ou seja, têm a mesma área. Em (c),o triângulo é composto pela *região definida pela tangente* e um setor circular.

Seja θ o ângulo formado pelo raio ligado ao ponto tangente e a reta que passa pelo centro, então cada segmento tangente terá comprimento $\tan\theta$. Logo, esta região sombreada na figura (b) é a *região definida pela tangente* correspondente ao *feixe de tangentes* na figura (a) e pelo Teorema de Mamikon têm mesma área $A(x)$.

Mas, área da *região definida pela tangente* pode ser calculada como a área do triângulo retângulo onde os catetos são o raio da circunferência de comprimento 1 e o segmento tangente de comprimento $\tan x$ menos a área do setor circular de ângulo x. Logo:

$$A(x) = \frac{1}{2}\int_0^x \tan^2\theta \; d\theta = \frac{1}{2}\tan x - \frac{x}{2} \tag{7}$$

4 Teorema de Mamikon: Demonstração Formal

Nesta seção trazemos a demonstração formal do teorema utilizando a Geometria Diferencial. Para mais detalhamento das ferramentas aqui utilizadas sugerimos consultar [6], [10], [11] e [9].

Teorema 15 *A área da região definida pela tangente de uma curva suave, onde o vetor aceleração não se anula, é igual à área do seu feixe de tangentes correspondente.*

Demonstração: *Considere uma curva α suave no espaço descrita dada por $X : [a, b] \subset \mathbb{R} \to \mathbb{R}^3$, com $X"(s) \neq 0$ para todo s, parametrizada pelo comprimento de arco no intervalo $0 \leq a \leq s \leq b$. Denotamos por $T(s)$ o vetor unitário tangente a α, ou seja,*

$$T(s) = \frac{X'(s)}{|X'(s)|} = X'(s) \tag{8}$$

Considere agora a equação paramétrica:

$$Y(s,u) = X(s) + uT(s), \text{ com } 0 \leq u \leq f(s), \text{ onde } f \text{ é uma função qualquer.} \tag{9}$$

Então Y descreve uma superfície S.

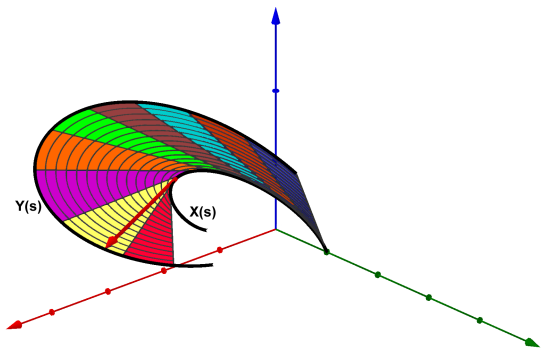


Figura 24. Área gerada sobre a curva X

Note que como Y varia em função de s e u no intervalo $[0, f(s)]$, S é gerada estendendo-se o vetor tangente T de X até a posição do vetor Y em $(s, f(s))$.

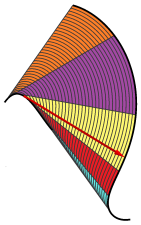


Figura 25. Planificação da superfície parametrizada Y.

Geometricamente, S é uma superfície desenvolvível, isto é, ela pode ser desenrolada em um plano sem distorção. Ou seja, a superfície S é a região definida pela tangente.
A área de S é dada por:

$$a(S) = \int_a^b \int_0^{f(s)} \left\| \frac{\partial Y}{\partial u} \times \frac{\partial Y}{\partial s} \right\| duds \tag{10}$$

Para resolver a integral calculamos as derivadas parciais:

$$\frac{\partial Y}{\partial s} = \frac{\partial X}{\partial s} + u\frac{dT}{ds} = T(s) + uT'(s) \tag{11}$$

e

$$\frac{\partial Y}{\partial u} = T(s) \tag{12}$$

logo,

$$\frac{\partial Y}{\partial u} \times \frac{\partial Y}{\partial s} = (T(s) + uT'(s)) \times T(s) = T(s) \times T(s) + uT'(s) \times T(s) \tag{13}$$

Como $T(s) \times T(s) = 0$, temos então que:

$$a(S) = \int_a^b \int_0^{f(s)} \|uT'(s) \times T(s)\| duds \tag{14}$$

O feixe de tangentes S_1 correspondente à superfície S é obtido ao transladar paralelamente os vetores tangentes a X para um ponto P de origem comum.

Uma parametrização da superfície S_1 é dada por:

$$Y_1(s,u) = P + uT(s), \text{ com } 0 \leq u \leq f(s) \tag{15}$$

A superfície S_1 é um cone generalizado[12] *onde sua geratriz é dada pelo vetor $uT(s)$ e P o seu vértice.*

Sua área também pode ser obtida por:

$$a(S_1) = \int_a^b \int_0^{f(s)} \left\| \frac{\partial Y_1}{\partial u} \times \frac{\partial Y_1}{\partial s} \right\| duds \tag{16}$$

onde as derivadas parciais são:

$$\frac{\partial Y_1}{\partial s} = u\frac{dT}{ds} = uT'(s) \tag{17}$$

e

$$\frac{\partial Y_1}{\partial u} = T(s), \tag{18}$$

logo,

$$\frac{\partial Y_1}{\partial u} \times \frac{\partial Y_1}{\partial s} = uT'(s) \times T(s) \tag{19}$$

Portanto, a área de S_1 é:

$$a(S_1) = \int_a^b \int_0^{f(s)} \|uT'(s) \times T(s)\| \, duds = a(S) \tag{20}$$

■

Concluímos então que a área de S descrita pela *região definida pela tangente* é igual a área S_1 do *feixe de tangente* correspondente à S.

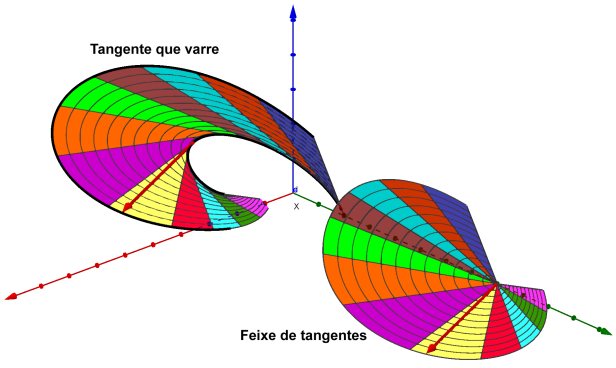


Figura 26. Superfície descrita pela *região definida pela tangente* e seu *feixe de tangentes* correspondente.

[12] Um cone generalizado é uma união de retas passando por um ponto P (chamado de vértice do cone) e pelos pontos de uma dada curva δ.

Esta demonstração também cobre as curvas no plano, bastando considerar uma das coordenadas do vetor X como uma constante. E neste caso o feixe de tangentes será um setor circular generalizado.

O teorema também é válido para as superfícies cujas curvas inicias podem ser decompostas em uma soma ou diferença de um número finito de curvas que atendam as características descritas na hipótese. Isto deve dar conta das curvas não suaves, como por exemplo as curvas poligonais. E também aquelas que apresentam pontos de inflexão, onde a tangente muda de direção podendo causar sobreposição da região gerada, conforme mostrado abaixo. Nestes casos, podemos dividir a curva em intervalos onde não tenhamos $X'' = 0$. Isso cuidaria também de curvas planas com inflexões, sob a ressalva de que áreas "sobrepostas" seriam contadas segundo o número de vezes que foram sobrepostas (ver Figuras 27 e 28).

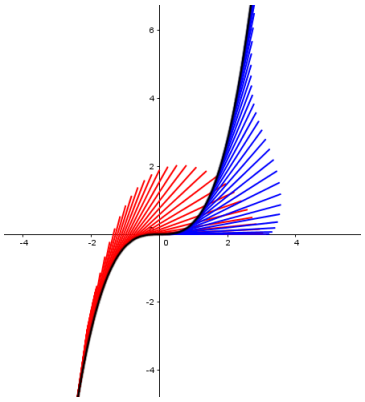


Figura 27. $f(x) = x^3$ com inflexão em $x = 0$.

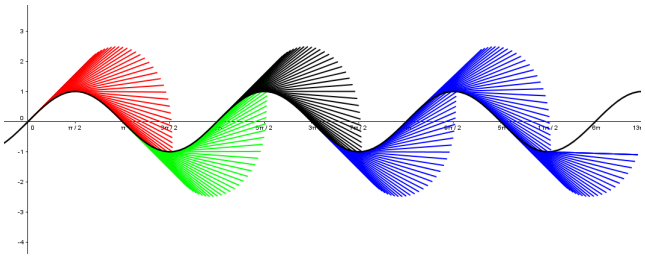


Figura 28. $f(x) =$ sen$x$ com inflexão em $x = k\pi$, com $k \in \mathbb{Z}$.

5 Conclusões

Esperamos que este artigo possa ajudar professores e alunos a terem uma visão mais ampla e curiosa da Matemática; servir, também, como uma possibilidade de apresentação do Cálculo aos alunos do Ensino Médio e motivá-los para prosseguir seus caminhos na área de exatas; ou ainda, motivar estudos futuros do trabalho de Mamikon e Apostol apresentados no livro *A visual approach to calculus problems* que explora a possibilidade de aplicações para diversos problemas envolvendo as cônicas, cicloides, cálculos de volume entre outros.

Referências

[1] APOSTOL, T. M.; MNATSAKANIAN, M. A. New Horizons in Geometry. Washington D.C.: The Mathematical Association of America, ISBN 978-0883853542, 2012.

[2] APOSTOL, T. M. A visual approach to calculus problems. *Engineering & Science*, Califórnia, n. 3, p.22-31, 2000. Disponível em: http://calteches.library.caltech.edu/712/2/Calculus.pdf. Acesso em 06 de jun. 2016.

[3] APOSTOL, T. M. *Calculus - Volume I.* Rio de Janeiro: Reverté , ISBN 978-8429150155, 2007.

[4] APOSTOL, T. M.; MNATSAKANIAN, M. A. Tangents and Subtangents Used to Calculate Areas. *The American Mathematical Monthly*, Washington D.C., v. 109, n. 10, p.900-908, 2002. Disponível em: https://www.jstor.org/stable/3072457. Acesso em 14 de mar. 2016.

[5] APOSTOL, T. M.; MNATSAKANIAN, M. A. Differential Geometry of Curves and Surfaces. Nova Jersey: Dover Publication, ISBN 978-0486806990, 2016.

[6] DO CARMO, M. P. Differential Geometry of Curves and Surfaces: Revised and Updated Second Edition. Courier Dover Publications, ISBN 978-0486806990, 2016.

[7] LIMA, E. L. Números e Funções Reais. Sociedade Brasileira de Matemática, ISBN 978-8585818814, 2013.

[8] MNATSAKANIAN, M. A. On the Area of a Region on a Developable Surface. *Communicated by the Armenian Academy of Sciences*, Armênia, v. 8, n. 2, p.97-102, 1981. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.474.6699. Acesso em 08 de out. 2016.

[9] NICOTERA JUNIOR, E. Cálculo Visual: Uma apresentação do Teorema de Mamikon. 2017. Dissertacão de Mestrado em Matemática - Universidade Federal do ABC. Santo André, SP. 2017. Disponível em: http://www.profmat-sbm.org.br/dissertacoes/?polo=ufabc&titulo=&aluno=eloy. Acesso em 07 de nov. 2017.

[10] STEWART, J. Single Variable Calculus: Early Transcendentals. São Paulo: Cengage Learning, ISBN 978-8522114610, 2013.

[11] STEWART, J. Single Variable Calculus: Vol. 2. São Paulo: Cengage Learning, ISBN 978-8522114634, 2013.

Uma Introdução à Teoria dos Jogos

A Introduction to the Game Theory

David Jonnes Francez
Universidade Federal de Santa Catarina, Floriánopolis, SC
davidfrancez@gmail.com

Resumo: A Teoria dos Jogos é um ramo da matemática aplicada que estuda situações estratégicas onde jogadores escolhem diferentes ações na tentativa de melhorar seu ganho. Inicialmente desenvolvida como ferramenta para compreender comportamento econômico, a teoria dos jogos é hoje usada em diversos campos acadêmicos. O objetivo do trabalho é mostrar, a partir de jogos simples, os conceitos de soma-zero, estratégias, matriz de ganhos, jogos estritamente e não estritamente determinados.

Palavras-chave: Teoria dos Jogos; Maximin; Minimax; matriz de ganhos; Soma-zero.

Abstract: The Game Theory is a branch of applied mathematics whose main concern is the study strategic situations where players choose different actions in an attempt to improve their payoffs. Initially developed as a tool to understand economic behavior, game theory is now used in many academic fields. The objective of this work is to show, from simple games, the concepts of zero-sum, strategies, matrix of payoffs, games strictly and nonstrictly determined.

Key words: Game Theory; Maximin; Minimax; payoffs; Sum-zero.

1 Introdução

A teoria dos jogos foi inicialmente desenvolvida como um modelo para analisar situações de conflito, na busca da racionalidade para embasar as decisões entre os agentes envolvidos.

Alguns matemáticos já fizeram estudos de jogos. Porém, nenhum deles deu continuidade às suas pesquisas para melhor fundamentá-las. Assim, esta teoria começou a se tornar realmente um foco de estudo na Matemática na década de 30 , ganhando um enfoque maior no ano de 1944.

Em 1944 a teoria dos jogos foi voltada, principalmente, a aplicações na área da Economia, porém, a complexidade de suas contribuições conseguem abranger muitas áreas pela diversidade de sua aplicabilidade.

Os jogos a serem considerados nestes estudos não são aqueles em que o resultado está sujeito exclusivamente ao fator sorte, no qual a atuação do jogador independe do resultado, como o jogo de dados, por exemplo. Tratam-se daqueles que são denominados jogos de estratégia, nos quais os sujeitos envolvidos criam uma sequência de tomadas de decisões e portanto passam a ter responsabilidade no resultado do jogo.

Partimos do pressuposto que os jogadores envolvidos sempre estarão em busca de vencer, ou seja, eles criarão estratégias que possam maximizar suas possibilidades, sempre tendo como objetivo a vitória. Salientamos que há a possibilidade de empate, mas quando um

Recebido em 08/10/2017 - Aceito em 30/10/2017

jogador vence, essa ação implica automaticamente na derrota de seu adversário, excluindo a possibilidade de ambos serem vencedores.

2 Ideia de Jogo

Nesta teoria, qualquer situação de conflito ou interação a ser considerada é denominada de "jogo", e os sujeitos envolvidos de "jogadores". Nesta pesquisa, por se tratar de uma introdução a esta complexa teoria, iremos limitar a utilização de situações em que constam apenas dois jogadores.

O exemplo a seguir serve para ilustrar a teoria dos jogos antes de introduzir a formalização matemática.

Exemplo 2.1 (Cobrança de Pênalti) *Vamos supor agora que João e Pedro estejam fazendo uma disputa de pênaltis, no caso João é o goleiro e Pedro o cobrador, suponha ainda que Pedro possua apenas duas estratégias: chutar a bola no lado direito do gol ou chutar a bola no lado esquerdo do gol. Como a distância entre o gol e a marca do pênalti é muito curta, isto impossibilita o goleiro João de determinar de que lado Pedro chutará a bola. Assim, ele deve escolher para que lado pular sem saber qual será a direção do chute. Suponha também que, sempre que o goleiro adivinhar corretamente o lado do chute, ele é capaz de fazer a defesa em 80% das vezes caso o chute seja à direita e 60% à esquerda. O batedor possui um tiro certeiro quando chuta no lado direito, mas não é tão bom quando chuta do lado esquerdo. Se Pedro chutar do lado direito do gol e o goleiro pular para o lado esquerdo, a bola entrará com 100% de certeza. Se o batedor chutar do lado esquerdo do gol e o goleiro pular para o lado direito, a bola entrará no gol com uma probabilidade de 50%.*

Este jogo não é um jogo simétrico, ou seja, existem grupos de estratégias diferentes para cada jogador. Se forem realizadas muitas cobranças, os jogadores não devem manter uma única estratégia (Estratégia Pura), pois colocaria seu oponente em vantagem. Nessas situações a melhor escolha é trocar constantemente de estratégia (Estratégia Mista). A vantagem da estratégia mista é que se coloca a dúvida na cabeça do oponente, pois ao alterar sistematicamente os lados para quais chuta, o cobrador não dá ao goleiro a certeza para qual lado chutará a bola. Da mesma forma, o chutador também não saberá exatamente qual canto escolher, se não tem certeza do que o goleiro fará.

Perceba que caso o goleiro pule para o mesmo lado que a bola, então terá 80% ou 60% de chance de fazer a defesa, dependendo do lado que Pedro chutar, gerando assim dois eventos favoráveis a João considerando os quatro possíveis (direita-direita e esquerda-esquerda). Enquanto Pedro estará certo do gol, caso faça a cobrança à direita e João pule para a esquerda. Por outro lado, caso Pedro cobre à esquerda e João pule à direita, isto não implica na certeza de gol, uma vez que o jogador não apresenta muita habilidade ao chutar para a esquerda, acertando assim, apenas a metade dos pênaltis. A matriz de ganhos da situação descrita fica assim:

Tabela 1. Cobrança de Pênalti

		João	
		Direita	Esquerda
Pedro	Direita	20%	100%
	Esquerda	50%	40%

Pedro sabe que se chutar constantemente no lado esquerdo do gol, ele terá uma expectativa de converter no mínimo 40% das cobranças. Por outro lado, João percebe também tal informação e com o objetivo de minimizar as conversões de Pedro, escolhe sempre fazer defesas à esquerda, mantendo assim, suas chances em 60%. Porém, como Pedro gosta muito de "blefar", decide trocar o lado da cobrança ocasionalmente. Sendo assim, vamos supor que ele faça a troca em 25% das vezes, João enfrentará o dilema de qual seria a melhor frequência para maximizar suas defesas.

Nesse exemplo, é extremamente importante não confundir taxa de sucesso com estratégia. Definiremos formalmente o que é estratégia mais a frente. Porém, para diferenciar essas ideias, entenda que estratégia é a frequência com que se escolhe uma opção em um jogo qualquer e taxa de sucesso é a probabilidade de ocorrência quando ambos os jogadores fazem suas respectivas escolhas.

Supondo que João queira minimizar as conversões de Pedro, e por isso decide trocar de lado metade das cobranças, a situação descrita pode ser resumida pela Tabela 2:

Tabela 2. Frequência Pênaltis I

			Frequência Defesa	
			50% Direita	50% Esquerda
Frequência Cobrança	25%	Direita	20%	100%
	75%	Esquerda	50%	40%

Analisando a Tabela 2 de frequências, podemos agora definir a probabilidade de cada um dos quatro eventos possíveis de ocorrerem. As respectivas chances de cada evento se encontram na Tabela 3.

Tabela 3. Pênaltis I

Evento Composto	**Probabilidade Evento**	**Sucesso Cobrança**
Cobrar à direita e defender à direita	0,25 . 0,50=0,125	20%
Cobrar à direita e defender à esquerda	0,25. 0,50= 0,125	100%
Cobrar à esquerda e defender à direita	0,75.0,50=0,375	50%
Cobrar à esquerda e defender à esquerda	0,75.0,50=0,375	40%

Assim, podemos calcular a probabilidade de sucesso da cobrança de pênaltis em relação a Pedro:

$$0,125.20\%+0,125.100\%+0,375.50\%+0,375.40\% =$$
$$2,5\%+12,5\%+18,75\%+15\% = 48,75\%.$$

Note que devido ao blefe de Pedro, este conseguiu criar uma situação de sucesso de

48,75%, o que gera um aumento de aproximadamente 22% em relação a manter as cobranças na esquerda, no qual garantiria em exatamente 40% suas chances de êxito.

Essa análise traz vários questionamentos que serão respondidos nos próximos capítulos: Pedro pode aumentar suas chances para além de 48,5% com uma estratégia diferente? Qual é a maior probabilidade de sucesso que Pedro pode fazer? Qual a melhor resposta de João para qualquer estratégia de Pedro? João consegue definir uma melhor estratégia independente das decisões de Pedro? As respostas serão respondidas mais adiante.

3 Estratégia

A teoria dos jogos pode ser definida como a teoria dos modelos matemáticos que estuda a escolha de decisões ótimas sob condições de conflitos. O elemento básico em um jogo é o conjunto de jogadores que dele participam e suas estratégias. Neste trabalho definiremos estratégia como o conjunto das frequências com que um jogador escolhe as opções de um determinado jogo. Assim, diante de suas escolhas, cria-se uma situação ou perfil no espaço de todas as situações (perfis) possíveis.

Os detalhes específicos de cada jogo serão ignorados no exemplo subsequente e simplesmente trataremos de uma matriz de números, sem unidade de medida. Portanto, podemos tratar um jogo de soma-zero 2×2 com a forma:

Tabela 4. Soma-Zero: Genérico

		João	
Pedro		a_{11}	a_{12}
		a_{21}	a_{22}

no qual a_{11}, a_{12}, a_{21} e a_{22} são números quaisquer. Essa abstração matemática tem o intuito de simplificar cada jogo estudado, facilitando a compreensão dos mesmos. Entretanto, faremos discussões de alguns casos concretos para que os exemplos se tornem palpáveis e de fácil entendimento.

Cada jogo de soma-zero 2×2 tem dois jogadores, que continuaremos chamando de Pedro e João. Quando os jogadores tomam alguma decisão, consequentemente, escolhem uma linha ou uma coluna da matriz. Especificamente nos exemplos anteriores, Pedro escolhe uma linha e João uma coluna. Por exemplo, suponha que no jogo *Cobrança de Pênalti* Pedro chute à direita e João pule à esquerda, a situação descrita seria assim:

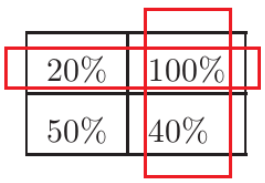


Figura 1. Tomada de Decisão

Cada jogador faz sua escolha simultânea e independentemente do oponente. Assim, a seleção da linha e coluna representa o resultado da jogada, e a entrada da matriz, cujo elemento está contido na intersecção da linha e coluna selecionada, é o ganho do jogador

(*payoff*). No caso acima o ganho de Pedro é 100%. Por outro lado, se Pedro tivesse chutado à esquerda e João mantido sua escolha, o ganho do batedor seria de 40%. Note que o ganho é em relação ao cobrador, conforme comentado no capítulo anterior, e obviamente o ganho de Pedro implica diretamente a perda de João.

Como o objetivo de Pedro é maximizar suas chances de gol e João de minimizar o sucesso das cobranças, cada jogador aplica uma estratégia, ou seja, toma uma decisão entre as opções possíveis.

Definição 3.1 *Uma estratégia em um jogo de soma-zero* 2×2 *é um par de números* p_1, p_2*, denotaremos* $[p_1; p_2]$*, em que:*

$$0 \leqslant p_1 \leqslant 1, \quad 0 \leqslant p_2 \leqslant 1 \quad onde \quad p_1 + p_2 = 1$$

no qual p_1 *representa a frequência com que a primeira linha (ou coluna) é escolhida, e* p_2 *a frequência com que a segunda linha (ou coluna) é escolhida.*

No Exemplo *Cobrança de Pênalti* Pedro faz a escolha de chutar 25% das vezes para o lado direito, ou seja, o par de números que representa sua estratégia é $[0,25; 0,75]$, enquanto a estratégia inicial de João é manter metade de suas defesas para cada lado, ou seja, sua estratégia é $[0,5; 0,5]$. Quando se faz a discussão de estratégias de um modo geral, pode-se definir a estratégia de Pedro como $[1-p; p]$ e a de João como $[1-q; q]$.

Conforme visto anteriormente no jogo *Cobrança de Pênalti*, cada jogador aplicou uma estratégia e com isso foi possível estabelecer a probabilidade de ganho para cada oponente. Agora será feito o cálculo de maneira genérica em termos de um jogo de soma-zero 2×2, tomando as estratégias $[1-p; p]$ $[q; 1-q]$ obteremos a seguinte matriz:

Tabela 5. Soma-Zero:Genérico II

	1-q	**q**
1-p	a_{11}	a_{12}
p	a_{21}	a_{22}

Vamos supor que Pedro tenha escolhido uma linha e João uma coluna. Desde que ambos os jogadores tenham feito suas escolhas de maneiras independentes, podemos concluir que:

- A probabilidade de Pedro receber o ganho a_{11} é $(1-p) \times (1-q)$
- A probabilidade de Pedro receber o ganho a_{12} $(1-p) \times q$
- A probabilidade de Pedro receber o ganho a_{21} $p \times (1-q)$
- A probabilidade de Pedro receber o ganho a_{22} $p \times q$

E como os quatro eventos são mutuamente exclusivos e cobrem todas as possibilidades, segue que o ganho esperado de Pedro ($G_{\mathcal{P}}$) é uma função de variáveis p e q definida por:

$$G_{\mathcal{P}}(p,q) = (1-p).(1-q).a_{11} + (1-p).q.a_{12} + p.(1-q).a_{21} + p.q.a_{22}.$$

O diagrama representado pela Tabela 14 serve de auxílio para o cálculo dos ganhos de cada jogador. Tais diagramas são chamados de *diagramas auxiliares*, com eles pode-se computar de forma rápida e precisa o resultado do jogo, principalmente quando aplicado em uma rotina repetidas vezes.

Exemplo 3.1 *No jogo Cobrança de Pênalti, supondo que Pedro tenha uma estratégia* $[0,3;0,7]$ *e João* $[0,6;0,4]$*, então o diagrama auxiliar seria :*

Tabela 6. Exemplo 3.1

	60%	40%
30%	20%	100%
70%	50%	40%

Tomando os cálculos dos ganhos de Pedro, temos

$$0,3.0,6.20\%+0,3.0,4.100\% + 0,7.0,6.50\% + 0,7.0,4.40\%$$
$$3,6\%+12\% + 21\% + 11,2\% = 47,8\%.$$

Portanto, quando Pedro e João aplicarem, respectivamente, as estratégias $[0,3;0,7]$ e $[0,6;0,4]$ então, Pedro deve esperar um sucesso em 47,8% de suas cobranças.

□

As estratégias de um jogador podem ser classificadas de duas maneiras: Estratégias Puras e Estratégias Mistas. Uma estratégia é dita pura quando o jogador escolhe apenas uma das opções do jogo, ou seja, a frequência de uma determinada opção é 1, enquanto todas as outras é nula.

Definição 3.2 *Dada uma estratégia* $p_1, p_2, p_3, ...p_m$ *em um jogo de soma-zero* $m \times n$*, tal estratégia é dita pura quando existir* $p_k = 1$ *para algum* $k \in (1, 2, 3, ...m)$*.*

Por outro lado, uma estratégia é dita mista quando não for pura, ou seja, o jogador não escolhe constantemente uma única opção do jogo.

Definição 3.3 *Dada uma estratégia* $p_1, p_2, p_3, ...p_m$ *em um jogo de soma-zero* $m \times n$*, tal estratégia é dita mista quando* $p_k \neq 1$ *para todo* $k \in (1, 2, 3, ...m)$*.*

No jogo *Cobrança de Pênalti*, Pedro possui duas estratégias puras: $[1,0]$ e $[0,1]$ que representariam, respectivamente, cobranças de pênaltis apenas à direita e apenas à esquerda. Estratégias que não são puras são chamadas de mistas. Portanto, $[0,1;0,9]$ e $[1-p;p]$ são estratégias mistas, contanto é claro, que p não seja 0 ou 1.

Ao final desse capítulo, seria natural nos perguntarmos: qual a melhor estratégia possível para maximizar os ganhos de um jogador? E como poríamos encontrá-la? A resposta será discutida a seguir.

4 Respostas Ideais para Estratégias Específicas

Nesse capítulo procuraremos encontrar as melhores táticas quando sabe-se a estratégia do oponente. Antes de fazermos essa análise, devemos ter precaução, pois deduzir a estratégia do adversário a partir de movimentos anteriores não é uma tarefa simples, e por mais que encontremos tal estratégia, isto não significa que saberemos a próxima jogada do oponente.

Uma estratégia é uma lista de números que representa a frequência com que cada opção é escolhida no jogo.

Voltemos ao jogo *Cobranças de Pênalti*. Em dado momento Pedro definiu a estratégia $[0,25; 0,75]$, ou seja, cobrar 25% das vezes à direita e 75% à esquerda. Suponha que João perceba a estratégia de seu adversário e procure a melhor resposta para minimizar o sucesso de Pedro. Seja $[1-q; q]$ a melhor estratégia para João, portanto o diagrama auxiliar seria dado por:

Tabela 7. Resposta Ideal Pênalti I

	1-q	q
25%	20%	100%
75%	50%	40%

e a expectativa de Pedro é

$$\begin{aligned} &0,25.(1-q).0,2 + 0,25.q.1 + 0,75.(1-q).0,5 + 0,75.q.0,4 \\ &= 0,05(1-q) + 0,25q + 0,375(1-q) + 0,3q \\ &= 0,05 - 0,05q + 0,25q + 0,375 - 0,375q + 0,3q \\ &= 0,425 - 0,125q. \end{aligned}$$

Perceba então, que o ganho de Pedro depende da estratégia a ser aplicada por João, ou seja, o *payoff* do cobrador está em função da frequência q do goleiro. Note que o menor valor do ganho de Pedro acontece quando João decide defender exclusivamente à esquerda, ou seja, tomando $q = 1$ entre todos os valores possíveis de q, assim o ganho seria dado por:

$$0,425 - 0,125q = 0,425 - 0,125.1 = 0,3$$

Portanto, o ganho esperado de Pedro é 30%, consequentemente, João tem em média 70% de sucesso.

Suponha agora que Pedro diversificará seus chutes à direita e à esquerda igualmente, ou seja, aplicará a estratégia $[0,5; 0,5]$. Qual seria a resposta ideal de João para minimizar o sucesso de Pedro? Vejamos o diagrama auxiliar

Tabela 8. Resposta Ideal Pênalti II

	1-q	q
50%	20%	100%
50%	50%	40%

e portanto o ganho esperado é

$$\begin{aligned} &0,5.(1-q).0,2 + 0,5.q.1 + 0,5.(1-q).0,5 + 0,5.q.0,4 \\ &= 0,1(1-q) + 0,5q + 0,25(1-q) + 0,2q \\ &= 0,1 - 0,1q + 0,5q + 0,25 - 0,25q + 0,2q \\ &= 0,35 + 0,35q. \end{aligned}$$

Analisando a expressão com o intuito de minimizá-la, basta João tomar a contra-estratégia $[1; 0]$ para que o sucesso do cobrador seja reduzido a 35%. Entre outras palavras, caso Pedro

chute metade dos pênaltis à direita e a outra metade à esquerda, a melhor escolha para o goleiro seria apostar constantemente no lado direito.

Quando um jogador aplica uma estratégia qualquer, seu oponente procura uma tática que resulte no ganho mínimo de seu adversário, tal tática chamaremos de *contra-estratégia ideal*. Note que nos exemplos anteriores, as duas contra-estratégias de João são puras, isto de certa forma não é mera coincidência. Podemos formular esse princípio de maneira mais geral, como um teorema.

Teorema 4.1 *Se um dos dos jogadores aplicar uma estratégia fixa, então seu oponente tem uma contra-estratégia ideal e ela é pura.*

Demonstração: Suponha que João aplique uma estratégia fixa $[1-q_0; q_0]$ e Pedro deseja encontrar a contra-estratégia ideal, ou seja, procura maximizar seus ganhos. Vejamos a situação descrita em um jogo genérico abaixo:

Tabela 9. Demonstração 4.1

		João	
		1-q_0	q_0
Pedro	1-p	a_{11}	a_{12}
	p	a_{21}	a_{22}

Note então que a função ganho de Pedro é dada por:

$$G_{\mathcal{P}}(p) = (1-p).(1-q_0).a_{11} + (1-p).q_0.a_{12} + p.(1-q_0).a_{21} + p.q_0.a_{22}$$

fazendo as operações de multiplicação e colocando p em evidência temos:

$$G_{\mathcal{P}}(p) = p\big(q_0(a_{11} - a_{12} - a_{21} + a_{22}) - a_{11} + a_{21}\big) + a_{11} + q_0.(a_{12} - a_{11})$$

Observe que $G_{\mathcal{P}}$ é uma função do tipo afim com variável independente p, logo seu gráfico é representado por um segmento de reta,uma vez que a função está definida apenas para $0 \leqslant p \leqslant 1$. Assim, o ponto de máximo é dado pela extremidade do segmento, ou seja, para $p = 0$ ou $p = 1$, portanto a contra-estratégia ideal para Pedro é dada por $[0; 1]$ ou $[1; 0]$ e ambas são puras como queríamos mostrar.

■

5 A estratégia Maximin

Neste capítulo buscaremos uma estratégia ideal, ou seja, procurar a melhor tática possível para Pedro em qualquer jogo de soma-zero 2×2, justificando-a matematicamente. Seja o jogo:

Tabela 10. Estratégia Ideal I

	João	
Pedro	a_{11}	a_{12}
	a_{21}	a_{22}

Devido ao Teorema 3.1, sabemos que para qualquer estratégia $[1-p, p]$ imposta por Pedro, existe uma contra-estratégia pura que João pode aplicar para minimizar o ganho de seu adversário. Sejam $g_1(p)$ e $g_2(p)$ os respectivos ganhos de Pedro quando o mesmo aplica as estratégias puras $[1, 0]$ e $[0, 1]$. Segue abaixo os diagramas auxiliares da situação descrita:

Tabela 11. Estratégia Ideal II

	1	0
1-p	a_{11}	a_{12}
p	a_{21}	a_{22}

Tabela 12. Estratégia Ideal III

	0	1
1-p	a_{11}	a_{12}
p	a_{21}	a_{22}

portanto o ganho é dado por

$$g_1(p) = (1-p).1.a_{11} + p.1.a_{21} = a_{11}(1-p) + a_{21}p = (a_{21} - a_{11})p + a_{11}.$$
$$g_2(p) = (1-p).1.a_{12} + p.1.a_{22} = a_{12}(1-p) + a_{22}p = (a_{22} - a_{12})p + a_{12}.$$

Se denotarmos como $G_P(p)$ a expectativa do ganho de Pedro aplicando as estratégias descritas acima, mesmo sabendo que João pode minimizá-las, então o ganho de Pedro é dado por

$$G_P(p) = min\,(g_1(p), g_2(p))$$

Acabamos de determinar o ganho de Pedro $G_{\mathcal{P}}(p)$ em função de p, ou seja, temos uma relação direta entre a estratégia $[1-p; p]$ aplicada e o ganho esperado.

Perceba que a variável independente p aparece nas expressões $g_1(p)$ e $g_2(p)$ como uma função afim, portanto, o respectivo gráfico é dado por uma reta. Perceba, é claro, que o valor de p é um número real entre 0 e 1, uma vez que p representa uma probabilidade, assim, o gráfico da função descrita é formado por segmentos de reta no intervalo $[0, 1]$. Note que as extremidades dessa função são dadas por:

$$g_1(0) = (a_{21} - a_{11}).0 + a_{11} = a_{11}.$$
$$g_1(1) = (a_{21} - a_{11}).1 + a_{11} = a_{21}.$$

Isso mostra que o gráfico de $g_1(p)$ é um segmento de reta que contém as extremidades $(0, a_{11})$ e $(1, a_{21})$. Analogamente:

$$g_2(0) = (a_{22} - a_{12}).0 + a_{12} = a_{12}.$$
$$g_2(1) = (a_{22} - a_{12}).1 + a_{12} = a_{22}.$$

e o gráfico de $g_2(p)$ é um segmento de reta que contém as extremidades $(0, a_{12})$ e $(1, a_{22})$. Com essas informações de $g_1(p)$ e $g_2(p)$, podemos notar que ao aplicar a estratégia $[1-p; p]$ ou $[p; 1-p]$, consequentemente, as funções teriam seus gráficos trocados, ou seja, o gráfico de $g_1(p)$ seria de $g_2(p)$ e vice-versa. O gráfico de $G_{\mathcal{P}}(p)$ é feito a partir da observação seguinte:

O gráfico de $G_{\mathcal{P}}(p)$ consiste em uma linha que, para qualquer valor possível de p, contém o menor valor entre $g_1(p)$ e $g_2(p)$.

O exemplo a seguir mostram uma variedade de informações importantes para a escolha de uma estratégia, apenas observando o gráfico da função.

Exemplo 5.1 *Para o jogo do Cobranças de Pênalti tínhamos a seguinte matriz de ganhos:*

Tabela 13. Exemplo 2.1 - Cobrança de Pênalti

20%	100%
50%	40%

Temos $a_{11} = 0,2$,$a_{12} = 1$,$a_{21} = 0,5$ e $a_{22} = 0,4$. Determinando n $g_1(p)$ e $g_2(p)$, temos:

$$g_1(p) = (a_{21} - a_{11})p + a_{11} = (0,5 - 0,2)p + 0,2 = 0,3p + 0,2.$$
$$g_2(p) = (a_{22} - a_{12})p + a_{12} = (0,4 - 1)p + 1 = -0,6p + 1.$$

e o gráfico da função é dada pela Figura 5 abaixo:

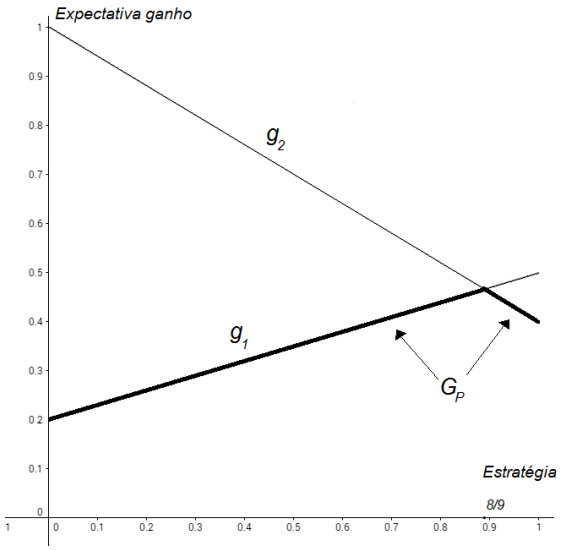


Figura 2. Exemplo 5.1 - Gráfico Expectativa

Perceba que o gráfico de $G_{\mathcal{P}}$ é dado grande parte por $g_1(p)$, onde João aplicaria a contra-estratégia pura $[1; 0]$ até o determinado momento em que João trocaria de estratégia e passaria a aplicar $[0; 1]$. Note que o momento de troca de estratégia é exatamente a intersecção de $g_1(p)$ e $g_2(p)$. Esse ponto é de extrema importância para a análise do jogo, podemos encontrá-lo facilmente resolvendo a equação:

$$g_1(p) = g_2(p)$$

isto é,

$$0,3p + 0,2 = -0,6p + 1$$
$$0,9p = 0,8$$
$$p = \frac{8}{9}.$$

Consequentemente,

$[1;0]$ é uma contra-estratégia ideal para João quando $0 \leqslant p \leqslant \frac{8}{9}$.

$[0;1]$ é uma contra-estratégia ideal para João quando $\frac{8}{9} \leqslant p \leqslant 1$.

Fazendo uma análise informal, podemos concluir que caso Pedro chute à esquerda com uma frequência menor que $\frac{8}{9}$, então João irá persistir em defender à direita. Porém, quando Pedro faz as cobranças com probabilidade superior a $\frac{8}{9}$ à esquerda, então o goleiro fará suas defesas constantemente à esquerda. Finalmente, quando $p = \frac{8}{9}$ temos o mesmo valor da função independente da estratégia pura aplicada por João, ou seja, o ganho será o mesmo para $g_1(p)$ ou $g_2(p)$.

Uma vez que a intersecção dos gráficos de $g_1(p)$ e $g_2(p)$ é o ponto de máximo da função G_P temos que esse ponto representa a escolha ideal para Pedro, assim temos que a estratégia é dada por:

$$\left[1 - \frac{8}{9}; \frac{8}{9}\right] = \left[\frac{1}{9}; \frac{8}{9}\right]$$

Portanto, a maior expectativa de ganho que Pedro, levando em conta que João quer minimizá-la, pode garantir é calculada abaixo:

$$g_1\left(\frac{8}{9}\right) = 0,3.\frac{8}{9} + 0,2 = \frac{8}{30} + 0,2 = 0,26... + 0,2 = 0,26... = 46,6...\%$$

ou

$$g_2\left(\frac{8}{9}\right) = -0,6.\frac{8}{9} + 1 = -\frac{8}{15} + 1 = -0,53... + 1 = 0.46... = 46,66...\%$$

□

Está claro nos exemplos vistos anteriormente, que o ponto de máximo da função G_P é uma estratégia especial. Infelizmente, há situações nas quais há mais de um ponto máximo e devemos ter cautela. Porém podemos formular a seguinte definição/teorema:

Teorema 5.1 *Se (x, y) é o ponto de máximo do gráfico de $G_{\mathcal{P}}$ então:*

$[1 - x; x]$ é uma estratégia Maximin para Pedro, e y é o ganho Maximin esperado.

Se Pedro aplicar a estratégia Maximin $[1 - x; x]$ então ele pode esperar vencer no mínimo y em cada jogada.

Essa nomenclatura é dada porque cada ponto do gráfico é o mínimo de duas possíveis escolhas de João, e por outro lado, Pedro está escolhendo o ponto mais alto do gráfico, ou seja, está maximizando o mínimo. Entre outras palavras, Pedro está escolhendo o valor mais alto abaixo da curva de mínimo.

Para concluir esse capítulo, percebemos que a estratégia Maximin é boa no sentido de garantir o ganho mínimo por jogada, além disso, é o melhor valor que pode ser assegurado. No entanto, é natural nos questionarmos se a estratégia Maximin é realmente a melhor tática para aumentarmos o ganho esperado. A resposta dessa questão, é claro, depende das circunstâncias de cada jogo.

6 A Estratégia Minimax

Vamos, agora, em busca de uma boa estratégia para João. O gráfico da expectativa de ganho de João em um jogo de soma-zero 2×2, pode ser encontrado de maneira análoga a de Pedro, porém, com algumas pequenas diferenças e similaridades que serão descritas abaixo.

Devido ao Teorema 4.1, sabemos que para qualquer estratégia $[1-q, q]$ aplicada por João em um jogo qualquer de soma-zero 2×2

Tabela 14. Estratégia Ideal IV

		João	
Pedro			
	a_{11}	a_{12}	
	a_{21}	a_{22}	

existe uma contra-estratégia pura que Pedro pode aplicar para maximizar seu ganho. Sejam $h_1(q)$ e $h_2(q)$ os respectivos ganhos de Pedro quando o mesmo aplica as estratégias puras $[1;0]$ e $[0;1]$. Seguem abaixo os diagramas auxiliares da situação descrita:

Tabela 15. Estratégia Ideal VI

	1-q	q
1	a_{11}	a_{12}
0	a_{21}	a_{22}

Tabela 16. Estratégia Ideal VII

	1-q	q
0	a_{11}	a_{12}
1	a_{21}	a_{22}

portanto o ganho de Pedro é dado por

$$h_1(q) = (1-q).1.a_{11} + q.1.a_{12} = a_{11}(1-q) + a_{12}q = (a_{12} - a_{11})q + a_{11}.$$
$$h_2(q) = (1-q).1.a_{21} + q.1.a_{22} = a_{21}(1-q) + a_{22}q = (a_{22} - a_{21})q + a_{21}.$$

Se denotarmos como $G_{\mathcal{J}}(q)$ a expectativa do ganho de Pedro aplicando as estratégias descritas acima, mesmo sabendo que ele pode maximizá-las, então o ganho de Pedro é dado por:

$$G_{\mathcal{J}}(q) = max\,(h_1(q), h_2(q))$$

Acabamos de determinar o ganho de Pedro $G_J(q)$ em função de q, ou seja, temos uma relação direta entre a estratégia $[1-q; q]$ aplicada e o ganho esperado.

Perceba que a variável independente q aparece nas expressões $h_1(q)$ e $h_2(q)$ como uma função afim, portanto o respectivo gráfico é dado por uma reta. Perceba é claro, que o valor de q é um número real entre 0 e 1, uma vez que q representa uma probabilidade, assim o gráfico da função descrita é formado por segmentos de reta no intervalo $[0;1]$. Note que as extremidades dessa função são dadas por:

$$h_1(0) = (a_{12} - a_{11}).0 + a_{11} = a_{11}.$$
$$h_1(1) = (a_{12} - a_{11}).1 + a_{11} = a_{12}.$$

Isso mostra que o gráfico de $h_1(q)$ é um segmento de reta que contém as extremidades $(0, a_{11})$ e $(1, a_{12})$. Analogamente,

$$h_2(0) = (a_{22} - a_{21}).0 + a_{21} = a_{21}.$$
$$h_2(1) = (a_{22} - a_{21}).1 + a_{21} = a_{22}.$$

e o gráfico de $h_2(q)$ é um segmento de reta que contém as extremidades $(0, a_{11})$ e $(1, a_{12})$. Com essas informações de $h_1(q)$ e $h_2(q)$ podemos notar que aplicar a estratégia $[1-q; q]$ ou $[q; 1-q]$ não mudaria o ganho esperado de João, pois essa escolha de estratégia implicaria em apenas uma troca de gráficos, ou seja, o gráfico de $h_1(q)$ seria de $h_2(q)$ e vice-versa. O gráfico de $G_{\mathcal{J}}(q)$ é feito a partir da observação seguinte:

O gráfico de $G_{\mathcal{J}}(q)$ consiste em uma linha que, para qualquer valor possível de q, contém o maior valor entre $h_1(q)$ e $h_2(q)$.

Agora reexaminaremos os exemplos anteriores visto sob a perspectiva de João.

Exemplo 6.1 *No jogo Cobranças de Pênalti temos a seguinte matriz de ganhos:*

Tabela 17. Exemplo 2.1 - Cobrança de Pênalti

20%	100%
50%	40%

temos então $a_{11} = 0,2$, $a_{12} = 1$, $a_{21} = 0,5$ e $a_{22} = 0,4$. Calculando as expressões de $h_1(q)$ e $h_2(q)$, temos:

$$h_1(q) = (a_{12} - a_{11})q + a_{11} = (1 - 0,2)q + 0,2 = 0,8q + 0,2.$$
$$h_2(q) = (a_{22} - a_{21})q + a_{21} = (0,4 - 0,5)q + 0,5 = -0,1q + 0,5.$$

e o gráfico da função é dada pela Figura 10 abaixo.

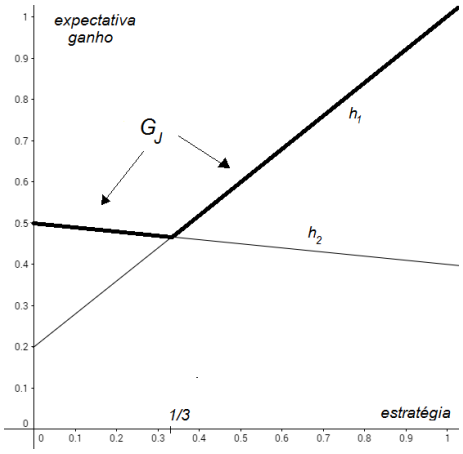


Figura 3. Exemplo 6.1 - Gráfico Expectativa

O gráfico de $G_{\mathcal{J}}$ coincide inicialmente com h_2 para pequenos valores de q. Portanto, quando João aplicar a estratégia $[1-q; q]$ para valores próximos de zero, Pedro deve responder com a estratégia pura $[0; 1]$; quando q está próximo de 1, então Pedro emprega $[1; 0]$. De maneira mais informal, se João raramente defender à esquerda, Pedro irá cobrar exatamente nesse lado; se João pular à esquerda, então Pedro sempre chutará à direita. O ponto mais interessante para minimizar a expectativa de ganho de Pedro é a intersecção de $h_1(q)$ e $h_2(q)$. Para encontrar tal ponto basta resolvermos a equação abaixo:

$$\begin{aligned} h_1(q) &= h_2(q) \\ 0,8q + 0,2 &= -0,1q + 0,5 \\ 0,9q &= 0,3 \\ q &= \frac{1}{3}. \end{aligned}$$

Consequentemente,

$$[0; 1] \text{ é uma contra-estratégia ideal para Pedro quando } 0 \leqslant q \leqslant \tfrac{1}{3},$$
$$[1; 0] \text{ é uma contra-estratégia ideal para Pedro quando } \tfrac{1}{3} \leqslant q \leqslant 1.$$

Em outras palavras, caso João não defenda mais que $\frac{1}{3}$ das vezes à esquerda, Pedro deve persistir com cobranças à esquerda. Uma vez que João pule mais que $\frac{1}{3}$ à esquerda, então, Pedro chutará sempre à direita. Finalmente, quando $q = \frac{1}{3}$ independente da estratégia de Pedro, o ganho será o mesmo.

Como a intersecção dos gráficos de $h_1(q)$ e $h_2(q)$ também representa o ponto mais baixo de $G_{\mathcal{J}}$, isto quer dizer, que para esse valor de q temos a escolha ideal para João. Impondo a estratégia a seguir:

$$\left[1 - \frac{1}{3}; \frac{1}{3}\right] = \left[\frac{2}{3}; \frac{1}{3}\right],$$

o valor mínimo esperado por João é dado por

$$h_1\left(\frac{1}{3}\right) = 0,8.\frac{1}{3} + 0,2 = \frac{8}{30} + 0,2 = 0,26... + 0,2 = 0,46... = 46,6...\%.$$

ou

$$h_2\left(\frac{1}{3}\right) = -0,1.\frac{1}{3} + 0,5 = -\frac{1}{30} + 0,5 = -0,03... + 0,5 = 0,46... = 46,6...\%.$$

□

Está claro que o ponto de mínimo da função representa uma estratégia significativa. Assim, como o ponto de máximo da função $G_{\mathcal{P}}$, o gráfico de $G_{\mathcal{J}}$ pode ter mais de um ponto de mínimo. Analogamente ao capítulo anterior podemos enunciar a definição/teorema

Teorema 6.1 *Se (x, y) é o ponto de mínimo do gráfico de $G_{\mathcal{J}}$, então,*

$[1 - x; x]$ é uma estratégia Minimax para João, e y é o ganho Minimax esperado.

Se João aplicar a estratégia Minimax $[1 - x; x]$,então, ele pode impedir, em média, que Pedro ganhe nada mais que y em cada jogada.

Assim como no Teorema 5.1, o nome Minimax faz referência à escolha mínima de João entre as maiores escolhas de Pedro, ou seja, representa o ponto mais baixo da curva de máximo.

7 Soluções de Jogos Soma zero

Nas seções 5 e 6 encontramos uma coincidência nos exemplos. As expectativas de ganho eram iguais quando as estratégias de Maximin e Minimax eram impostas. Tal coincidência acontece devido ao valor das expectativas não mudarem conforme as partidas são disputadas. Porém, as estratégias Minimax e Maximin possuem definições diferentes. Informalmente falando, a estratégia Maximin é um "base"para Pedro, enquanto a estratégia Minimax é um "teto"nos ganhos de Pedro, imposto por João.

A certeza da coincidência para jogos repetitivos de soma-zero é o teorema central da Teoria dos Jogos. Esse teorema será inicialmente discutido em um contexto de jogos 2×2 e reformulado para um caso mais geral, o qual será demonstrado no final desse capítulo.

Teorema 7.1 *Para qualquer jogo de soma-zero 2×2 há um único número v em que*

i) a estratégia Maximin de Pedro garante uma expectativa de ganho de mínimo v;

ii) a estratégia Minimax de João garante uma expectativa de ganho a Pedro que não exceda v.

Os dois capítulos anteriores tiveram como objetivo encontrar métodos e soluções de jogos de soma-zero 2×2. Faremos agora algumas simplificações para agilizar as análises feitas anteriormente. Inicialmente, vamos classificar os jogos de soma-zero 2×2 em dois tipos.

• **Jogos 2×2 Estritamente Determinados** - Dizemos que um jogo é estrtitamente determinado se as estratégias Minimax e Maximin são puras. Essa classificação recebe este

nome, uma vez que, cada jogador já sabe o que esperar de seu adversário, ou seja, uma estratégia pura.

• **Jogos 2×2 Não Estritamente Determinados** - são todos os outros jogos que possuem estratégias de Maximin e Minimax não puras, ou seja, são estratégias mistas.

Para entendermos melhor os jogos estritamente determinados precisamos do conceito Ponto de Sela de um jogo de soma-zero $m \times n$.

Definição 7.1 *Dizemos que um elemento a_{ij} de uma matriz A $m \times n$ é um ponto de sela da matriz A, se ele for simultaneamente um mínimo em sua linha e um máximo em sua coluna, isto é, se*

$$a_{ij} \leqslant a_{il} \quad \textit{para todo} \quad l = 1, ..., n \quad e$$

$$a_{ij} \geqslant a_{kj} \quad \textit{para todo} \quad k = 1, ..., m.$$

Exemplo 7.1 *A entrada de número 3 representa o ponto de sela do jogo*

Tabela 18. Exemplo 7.1

1	0
3	4

□

Vamos demonstrar dois lemas, para jogos estritamente determinados, necessários para a demonstração do Teorema Minimax que enunciaremos mais tarde.

Lema 7.1 *Pedro tem uma estratégia Maximin pura se, e somente se, a matriz do jogo G tem um ponto de sela, e nesse caso o ganho do ponto de sela é igual valor Maximin.*

Demonstração: Dado um jogo qualquer

Tabela 19. Lema 7.1

G=

a_{11}	a_{12}
a_{21}	a_{22}

vamos assumir sem perda de generalidade que $a_{11} \leqslant a_{12}$. Suponha inicialmente que Pedro tem uma estratégia Maximin pura. Lembremos que os segmentos $g_1(p) = (1-p)a_{11} + pa_{21}$ e $g_2(p) = (1-p)a_{12} + pa_{22}$ com $0 \leqslant p \leqslant 1$ estão entre nos pontos $(0, a_{11})$ e $(1, a_{21})$ para $g_1(p)$ e $(0, a_{12})$ e $(1, a_{22})$ para $g_2(p)$. Como a estratégia Maximin é dada pelo ponto de máximo do gráfico de $G_P(p)$ então podemos afirmar, de acordo com a suposição acima, que os segmentos não se interceptam em um ponto interior (Fig. 13.1 e 13.2), os segmentos possuem coeficientes angulares positivos (Fig. 13.3) ou ambos negativos (Fig. 13.4). Mantendo em mente ainda que $a_{11} \leqslant a_{12}$, podemos notar que, nos quatro casos possíveis, os pontos de sela que ocorrem em cada uma das figuras são dados por a_{11}, a_{21}, a_{22} e a_{11}, respectivamente, e esses valores são iguais ao Maximin de cada jogo.

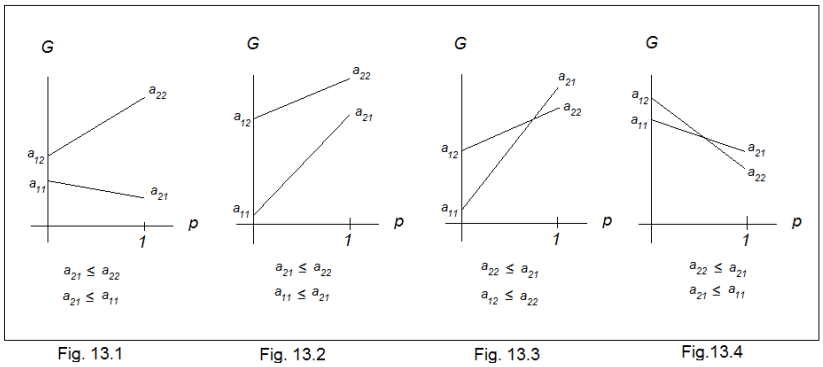


Figura 4. Demonstração - Lema 7.1

Suponha, agora, que o jogo G admita um ponto de sela. Esse ponto de sela implica algumas desigualdades para o gráfico de $G_P(p)$ gerando assim quatro possibilidades para a função ganho de Pedro, considerando ainda a suposição que $a_{11} \leqslant a_{12}$, os casos são dados pelas figuras 14.1 a 14.4. Perceba facilmente, que em todos os casos, existe uma estratégia Maximin pura e o valor do ganho coincide com o ponto de sela.

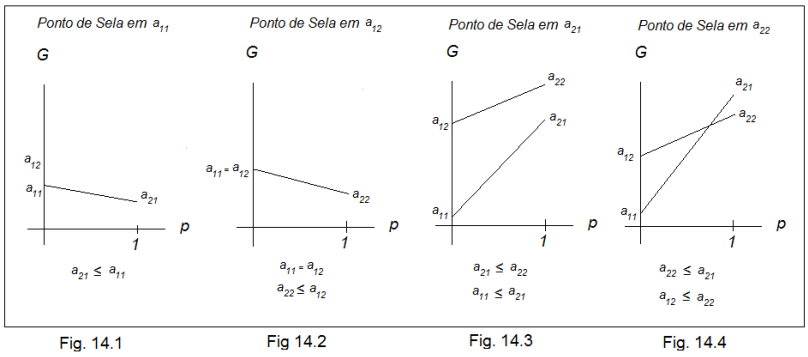


Figura 5. Demonstração - Lema 7.1

■

Lema 7.2 *João tem uma estratégia Minimax pura se, e somente se, o jogo G tem um ponto de sela, e nesse caso o ganho do ponto de sela é igual valor Minimax.*

A demonstração é análoga ao Lema 7.1

Os jogos não estritamente determinados são sujeitos a um procedimento de solução diferentes, porém tão simples quanto os estritamente determinados. Seja o jogo

Tabela 20. Jogo não determinado

		João	
		1-q	q
Pedro	1-p	a_{11}	a_{12}
	p	a_{21}	a_{22}

Retomando as funções $g_1(p)$ e $g_2(p)$ deduzidas quando João aplica uma contra-estratégia ideal pura temos:

$$g_1(p) = (1-p).1.a_{11} + p.1.a_{21} = a_{11}(1-p) + a_{21}p = (a_{21} - a_{11})p + a_{11}$$
$$g_2(p) = (1-p).1.a_{12} + p.1.a_{22} = a_{12}(1-p) + a_{22}p = (a_{22} - a_{12})p + a_{12}$$

Já sabemos que um jogo não estritamente determinado tem uma estratégia mista que representa o Maximin para Pedro e o Minimax para João. Assim, o valor de p é intersecção dos segmentos $g_1(p)$ e $g_2(p)$. Para encontramos tal valor, basta resolvermos a equação abaixo:

$$\begin{aligned} g_1(p) &= g_2(p) \\ (a_{21} - a_{11})p + a_{11} &= (a_{22} - a_{12})p + a_{12} \\ (a_{21} - a_{11} - a_{22} + a_{12})p &= a_{12} - a_{11} \\ p = \frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}} \quad &\text{com} \quad a_{11} - a_{12} - a_{21} + a_{22} \neq 0 \end{aligned}$$

Consequetemente, a estratégia Maximin mista $[1-p, p]$ para Pedro é dada por

$$\left[\frac{a_{22} - a_{21}}{a_{11} - a_{12} - a_{21} + a_{22}}, \frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}}\right]$$

Portanto, temos um método simples de encontrar a estratégia Maximin para Pedro.

Teorema 7.2 (Minimax) *Para qualquer jogo de soma-zero 2×2 há um único número v em que:*

i) a estratégia Maximin de Pedro garante uma expectativa de ganho de mínimo v;

ii) a estratégia Minimax de João garante uma expectativa de ganho a Pedro que não exceda v.

Demonstração: Caso o jogo venha a ter um ponto de sela, então o Teorema se resume no Lemas 7.1 e 7.2 . Caso o jogo não tenha um ponto de sela, ou seja, um jogo não estritamente determinado, podemos utilizar a teoria do Cálculo para demonstra-lo.

Suponha que em um jogo qualquer Pedro aplique a estratégia $[1-x; x]$ e João $[1-y; y]$. A situação se resume no quadro abaixo:

Tabela 21. Demonstração Teorema Minimax

		João	
		1-y	y
Pedro	1-x	a_{11}	a_{12}
	x	a_{21}	a_{22}

Note então que a função ganho de Pedro é dada por:

$$G_{\mathcal{P}}(x,y) = (1-x).(1-y).a_{11} + (1-x).y.a_{12} + x.(1-y).a_{21} + x.y.a_{22}$$

Simplificando a função em termos de x e y, obtemos:

$$G_{\mathcal{P}}(x,y) = xy(a_{11} - a_{12} - a_{21} + a_{22}) + x(a_{21} - a_{11}) + y(a_{12} - a_{11}) + a_{11}$$

Eventualmente definida para $0 \leqslant x, y \leqslant 1$ uma vez que $[1-x, x]$ e $[1-y, y]$, são as respectivas estratégias aplicadas por Pedro e João.

Vamos agora encontrar um valor da função $G_{\mathcal{P}}(x,y)$ que seja máximo na direção x e mínimo na direção y, ou seja,um ponto de sela de acordo com a teoria do Cálculo. É importante não confundir ponto de sela do cálculo, com o ponto de sela da teoria dos jogos, ambos são diferentes em suas definições. A figura abaixo mostra um ponto de sela do cálculo em uma curva dada.

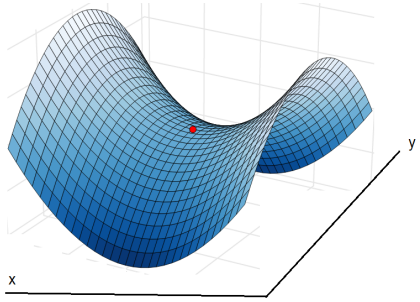


Figura 6. Ponto Sela Cálculo

Sabemos que o ponto de sela se dá em um dos seus pontos críticos, ou seja, nos pontos em que as derivadas parciais são nulas, isto é:

$$\frac{\partial G_{\mathcal{P}}}{\partial x} = 0 \qquad \text{e} \qquad \frac{\partial G_{\mathcal{P}}}{\partial y} = 0.$$

Calculando as derivadas parciais temos:

$$\frac{\partial G_{\mathcal{P}}}{\partial x} = y(a_{11} - a_{12} - a_{21} + a_{22}) + (a_{21} - a_{11}) = 0,$$

$$\frac{\partial G_{\mathcal{P}}}{\partial y} = x(a_{11} - a_{12} - a_{21} + a_{22}) + (a_{12} - a_{11}) = 0.$$

Com isso concluímos que:

$$y = \frac{a_{11} - a_{21}}{a_{11} - a_{12} - a_{21} + a_{22}} \qquad \text{e} \qquad x = \frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}}$$

Tendo em mente que um jogo não estritamente determinado admite $a_{11} - a_{12} - a_{21} + a_{22} \neq 0$, pois caso contrário, o gráfico de $G_{\mathcal{P}}$ seria um plano e consequentemente teria a estratégia Maximin e Minimax em um de seus vértices, conforme visto anteriormente.

Portanto o ponto $\left(\frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}}; \frac{a_{11} - a_{21}}{a_{11} - a_{12} - a_{21} + a_{22}}\right)$ é um ponto crítico de $G_{\mathcal{P}}$, classifiquemos agora o ponto crítico usando o teste da derivada segunda e a matriz Hessiana.

$$\Delta(x_0, y_0) = det \begin{pmatrix} \dfrac{\partial^2}{\partial x^2} & \dfrac{\partial^2}{\partial x \partial y} \\ \dfrac{\partial^2}{\partial y \partial x} & \dfrac{\partial^2}{\partial y^2} \end{pmatrix}$$

Calculando as derivadas segundas de $G_{\mathcal{P}}$ obtemos:

$$\frac{\partial^2}{\partial x^2} = 0, \qquad \frac{\partial^2}{\partial x \partial y} = a_{11} - a_{12} - a_{21} + a_{22},$$
$$\frac{\partial^2}{\partial y^2} = 0, \qquad \frac{\partial^2}{\partial y \partial x} = a_{11} - a_{12} - a_{21} + a_{22}.$$

Substituindo os valores acima na matriz Hessiana e calculando o determinante temos:

$$\Delta(x_0, y_0) = det \begin{pmatrix} 0 & a_{11} - a_{12} - a_{21} + a_{22} \\ a_{11} - a_{12} - a_{21} + a_{22} & 0 \end{pmatrix}$$
$$\Delta(x_0, y_0) = -(a_{11} - a_{12} - a_{21} + a_{22})^2$$

Com isso, mostramos que o determinante da matriz Hessiana é negativo para todo valor de x e y. Assim o ponto de sela

$$\left(\frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}}; \frac{a_{11} - a_{21}}{a_{11} - a_{12} - a_{21} + a_{22}} \right)$$

representa o máximo na direção x e mínimo na direção y, ou vice-versa, portanto

$$v = G_{\mathcal{P}} \left(\frac{a_{11} - a_{12}}{a_{11} - a_{12} - a_{21} + a_{22}}; \frac{a_{11} - a_{21}}{a_{11} - a_{12} - a_{21} + a_{22}} \right)$$

representa o Maximin para Pedro e o para João Minimax.

■

Ao analisar o Teorema Minimax, observamos que a função $G_{\mathcal{P}}(p, q)$ sempre possuirá um ponto de sela do cálculo, desde que a condição $a_{11} - a_{12} - a_{21} + a_{22} \neq 0$ seja satisfeita. Contudo, o ponto de sela pode estar dentro do domínio da função ou não. Caso esteja dentro, o jogo será não estritamente determinado e consequentemente o ponto de sela representa a estratégia Maximin, Minimax e o valor esperado do ganho. Por outro lado, se o ponto o ponto de sela estiver fora do domínio, ou $a_{11} - a_{12} - a_{21} + a_{22} = 0$, o que representaria um plano, então, o jogo será estritamente determinado. Assim, a estratégia Minimax e Maximin será dada por um dos vértices do gráfico de $G_{\mathcal{P}}(p, q)$.

Em resumo, a função $G_{\mathcal{P}}(p, q)$:

• Representa um jogo estritamente determinado se:

i) Se a função representa um plano, ou seja, $a_{11} - a_{12} - a_{21} + a_{22} = 0$;

ii) Se o ponto de sela não pertencer ao domínio da função;

• Representa um jogo não estritamente determinado se:

i) Se o ponto de sela pertencer ao quadrado $[0, 1] \times [0, 1]$, ou seja, pertencer ao domínio da função.

8 Resultados e discussão

Ao propor utilizar jogos de estratégia para analisar quaisquer situações de conflito, muitos matemáticos retornaram a uma prática milenar para entender e estudar o mundo. Ao fazer isso, criaram uma ciência com uma grande capacidade de generalização e precisão matemática.

Em uma breve discussão sobre alguns jogos, percebemos que um jogador pode obter alguma vantagem sobre seu oponente, dependendo de suas escolhas. Com isso, definimos o importante conceito de estratégia, bem como sua classificação em: estratégia pura e estratégia mista. Concluímos que a melhor contra estratégia, ou seja, a estratégia que gera um maior ganho é necessariamente a pura.

Nas seções quatro e cinco mostramos que cada jogador tem uma estratégia ideal, pelo menos do ponto de vista defensivo. Tais estratégias são denominadas: Maximin e Minimax. Ao aplicar a estratégia Maximin obtém-se o ganho máximo, quando o oponente tenta minimizá-lo, ou seja, um valor 'base'. Por outro lado, a estratégia Minimax gera o ganho mínimo do oponente, quando o mesmo tenta maximizá-lo, ou seja, um 'teto'.

Ao fim do trabalho, mostramos que os jogos de soma-zero 2×2 podem ser classificados em jogos estritamente determinados e não estritamente determinados. Definimos nesse momento, o importante conceito de ponto de sela e mostramos, formalmente, que todo jogo estritamente determinado o possui, e que as estratégias que representam o Maximin e Minimax são puras. Já em jogos não estritamente determinados, mostramos que as estratégias ideais são mistas. Tal afirmação é demonstrada pelo Teorema Minimax.

Referências

[1] CONWAY, J. H. All games bright and beautiful. *American Mathematical Monthly*, p. 417-434, 1977.

[2] DUTTA, P. K. Strategies and games: theory and practice. MIT press, 1999.

[3] FIANI, R. Teoria dos jogos. Elsevier Brasil, 2006.

[4] FUDENBERG, D.; TIROLE, J. Game theory, 1991. Cambridge, Massachusetts, v. 393, p. 12, 1991.

[5] GUIDORIZZI, H. L. Um curso de Cálculo, vol. 2. Grupo Gen-LTC, 2000.

[6] OSBORNE, M. J.; RUBINSTEIN, A. A course in game theory. MIT press, 1994.

[7] RASMUSEN, E.; BLACKWELL, B. Games and information. Cambridge, MA, v. 15, 1994

[8] SCHELLING, Thomas C. The strategy of conflict. Harvard university press, 1980.

[9] SARTINI, B. A. *et al.* Uma introdução à teoria dos jogos. II Bienal da SBM?Universidade Federal da Bahia, p. 1-61, 2004.

[10] VON NEUMANN, J.; MORGENSTERN, O. Theory of games and economic behavior. Princeton university press, 2007.

A Equação de Condução de Calor Uni e Bidimensional: Solução Usando Transformada Integral e o Método da Separação de Variáveis

The Uni and Bidimensional Heat Conduction Equation: Solution Using Integral Transform and the Method of Variable Separation

Reynaldo D'Alessandro Neto
Universidade Federal de São Carlos, Sorocaba, SP
reynaldo.dalessandro@gmail.com

Antonio Luís Venezuela
Universidade Federal de São Carlos, Sorocaba, SP
alvenez@ufscar.br

Resumo: As propriedades térmicas dos materiais são de grande importância para os projetos mecânicos, principalmente os que envolvem sistemas térmicos. A simulação e determinação do campo da temperatura pelo modelo matemático conhecido como equação do calor, auxilia na representação do comportamento térmico, isto é, nos fornece informações prévias de como a temperatura varia com a posição e o tempo em um sólido, e assim, poder caracterizar o material termicamente e saber as condições apropriadas a se impor ao objeto em estudo. O objetivo deste trabalho, é resolver a EDP que modela os processos de transporte de calor unidimensional e bidimensional em geometria retangular por meio da técnica da transformada integral clássica e separação de variáveis, respectivamente. Por fim, faz-se a análise dos modelos encontrados a partir da utilização de gráficos e tabelas de convergência.

Palavras-chave: transformada integral; método de Fourier; equação do calor.

Abstract: The thermal properties of materials are of great importance for mechanical projects, especially those involving thermal systems. The simulation and determining the mathematical model for the temperature field known as heat equation, assists in the representation of the thermal behavior, that is , it gives us prior information on how the temperature varies with the position and time in a solid, and so power thermally characterize the material and know the appropriate conditions to impose on the object under study. The objective of this work is to solve the EDP modeling the one-dimensional and two-dimensional heat transfer processes in rectangular geometry through the Classical Integral Transformation Technique and the Separation of Variables, respectively. Finally, we analyze the models found from the use of graphs and convergence tables

Key words: integral transformation; Fourier method; heat equation.

1 Introdução

Com o avanço tecnológico, os estudos que envolvem a transferência de calor ganham um grande destaque, já que a maioria dos processos industriais e de projetos de usinas nucleares e térmicas utilizam equipamentos de troca de calor como geradores de vapor, fornos, motores

Recebido em 29/08/2017 - Aceito em 28/11/2017

de calor, condensadores e outros. O mesmo acontece na área de produção de energia, que está em processo de expansão com projetos no controle do meio ambiente.

Existem outros processos em nosso dia-a-dia onde ocorre a transferência de calor, como os conversores catalíticos presentes nos motores de combustão interna dos automóveis, as unidades de refrigeração e ar-condicionado, os equipamentos eletrônicos, a refrigeração de motores elétricos, os transformadores e geradores elétricos, aquecimento e refrigeração de processos químicos, a minimização de perdas de calor em construções e aprimoramento de técnicas de isolamento térmico.

Com essa vasta gama de aplicações, vemos que os problemas relativos a transferência de calor aparecem como enormes desafios a se resolver. Assim, matemáticos, físicos e engenheiros estão constantemente confrontando com a necessidade de se maximizar e/ou minimizar taxas de transferência de calor, impulsionando um avanço rápido em várias tecnologias de aprimoramento, incluindo o uso de superfícies estendidas, agitadores e campos elétricos ou magnéticos externos [1] e [2]

A transferência de calor ocorre por condução, convecção e radiação, mas na maioria das vezes, por combinação das mesmas [3]. A maioria destes problemas são tratados a partir das Equações de Conservação de Energia Térmica, as quais são resolvidas utilizando técnicas numéricas, analíticas ou híbridas (analíticas-numéricas). A partir da década de 80, as técnicas analíticas e/ou híbridas têm sido desenvolvidas e utilizadas na solução destas equações, devido a sua versatilidade no tratamento matemático/computacional.

No trabalho de [4] examina-se analiticamente a transferência de calor convectivo laminar forçado de um fluido newtoniano em um microcanal entre duas placas paralelas e para isso é utilizada a Técnica da Transformada Integral Generalizada. A teoria dos estresses térmicos com base na equação de condução de calor relacionada a uma derivada temporal de ordem maior que 2 é usada para investigar os estresses térmicos em um corpo cilíndrico infinito, cuja solução é obtida aplicando transformação integral de Laplace e Weber [5].

O objetivo deste trabalho, oriundo da dissertação de mestrado do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT [6], é resolver a EDP que modela os processos de transporte de calor unidimensional e bidimensional em geometria retangular, as quais estão acopladas às condições de contornos de Dirichlet. O primeiro problema de valor de contorno está relacionado a uma barra feita de material condutor térmico e o segundo problema vinculado a uma placa também feita de um material condutor. Inicialmente resolveremos o problema unidimensional utilizando a Técnica de Transformada Integral Clássica e, finalmente, o problema bidimensional será resolvido via Técnica de Separação de Variáveis. Para cada uma das soluções analíticas obtidas serão comparadas com resultados analíticos provindos da literatura, além disso serão analisados os perfis de temperatura relativos à variável tempo, t, e às variáveis espaciais, x e y.

Este trabalho procura mostrar uma técnica analítica, que abrange a utilização de procedimentos matemáticos para a resolução de conceitos físicos para a modelagem do problema em questão. Com isso, temos uma avaliação com maior precisão das propriedades térmicas dos materiais que se trabalham. O resultado analítico de Equações Diferenciais Parciais, fornece melhor subsídio para análises térmicas de materiais em problemas de condução de calor, dessa forma esse trabalho ratifica a importância de se propor uma solução analítica a um problema físico, deixando assim a resolução mais próxima da realidade do fenômeno físico em questão.

2 Modelagem Matemática

A modelagem da equação do calor é desenvolvida, por um lado, a partir da Lei de Fourier e das equações do fluxo de calor e balanço de energia e, por outro lado, pelas equações da capacidade térmica e da massa específica [3] e [6]. Neste contexto, há a ocorrência da difusividade térmica $\alpha = k/c\rho$, que possui as dimensões m^2/s, sendo k (W/mK) a condutividade térmica, c (J/K) a capacidade térmica e ρ (kg/m^3) a densidade.

Sejam $\Omega \subseteq \mathbb{R}^r$, $r \geqslant 1$, um aberto limitado de fronteira Γ, $\overline{\Omega} = \Omega \cup \Gamma$, $Q = \Omega \times (0, +\infty)$ e $\Sigma = \Gamma \times (0, +\infty)$. Procuramos uma função u, tal que $u \in C^2(\Omega \times (0, +\infty)) \cap C(\overline{\Omega} \times [0, +\infty))$, relativa ao problema de valor de contorno [7]:

$$\frac{\partial u}{\partial t} = \alpha \Delta u, \text{ em Q}, \tag{1}$$

$$u = \tilde{T}, \text{ sobre } \Sigma, \tag{2}$$

$$u(v, 0) = f(v), \text{ em } \overline{\Omega}, \tag{3}$$

sendo $\Delta = \sum_{i=1}^{r} \frac{\partial^2}{\partial x_i^2}$ o laplaciano relativo às variáveis espaciais e t à variável tempo (s). Como u deve ser uma função diferenciável de classe $C^2(\Omega \times (0, +\infty))$, no mínimo, e também contínua, $C(\overline{\Omega} \times [0, +\infty))$, logo a função f também deve ser continua, $C(\overline{\Omega})$.

A Equação (1) é a *equação do calor*, pois modela a distribuição da temperatura u no domínio Ω e no instante t. A Equação (2) é a *condição de contorno de Dirichlet*, a qual pode ser substituída pela *condição de Neumann*, $\frac{\partial u}{\partial \widehat{n}} = \tilde{T}$ sobre Σ, sendo $\widehat{n}$ o vetor unitário da normal exterior a Γ. A condição de Dirichlet expressa que o bordo Γ de Ω se mantém a temperatura $\tilde{T}$. A condição de Neumann expressa que o fluxo de calor através do bordo Γ é $\tilde{T}$. A Equação (3) é a *condição inicial* ou *condição de Cauchy*.

Para que exista solução do referido problema de valor de contorno, a função f deve satisfazer a *condição de compatibilidade*: $f(v) = \tilde{T}$, $v \in \overline{\Omega}$.

Na sequência, expomos três problemas de valor de contorno, respectivamente, uni, bi e tridimensional, juntamente com o desenvolvimento matemático para se obter as soluções, isto é, a determinação do perfil de temperatura.

2.1 Equação do calor unidimensional

Problema de valor de contorno unidimensional

Considerando as Equações (1), (2) e (3), sejam $\Omega = (0, L_x) \subset \mathbb{R}$, $\Gamma = \{0, L_x\}$, $L_x > 0$, assim temos uma barra de seção uniforme, $\overline{\Omega}$, com área muito pequena em relação ao comprimento L_x. Neste caso, não há troca de calor com o exterior através da superfície lateral da barra, sendo que os extremos correspondem ao bordo Γ e estão mantidos à temperatura $\tilde{T}(^\circ C)$, conforme a condição de contorno (2). Procuramos uma função u, tal que $u \in C^2(\Omega \times (0, +\infty)) \cap C(\overline{\Omega} \times [0, +\infty))$, relativa ao problema de valor de contorno unidimensional [8]:

$$\frac{\partial u}{\partial t} = \alpha \frac{\partial^2 u}{\partial x^2}, \quad \text{em } (0, L_x) \times (0, \infty) \tag{4}$$

$$u(0, t) = \tilde{T}, \quad t \in [0, \infty), \tag{5}$$

$$u(L_x, t) = \tilde{T}, \quad t \in [0, \infty), \tag{6}$$

$$u(x, 0) = f(x), \quad x \in [0, L_x]. \tag{7}$$

Para resolver este problema, na sequência, utilizaremos a Técnica da Tranformada Integral Clássica-TTIC.

Técnica da Tranformada Integral Clássica-TTIC

A TTIC exige que as condições de contorno sejam homogêneas, mas isto não ocorre nas Equações (5) e (6). Com o objetivo de homogeneizá-las, aplicamos o seguinte filtro matemático:

$$u(x,t) = u_h(x,t) + M(x), \tag{8}$$

sendo que $M(x)$ é obtida a partir do seguinte problema de valor inicial:

$$\begin{aligned} \frac{d^2}{dx^2}M(x) &= 0, \quad \text{em } (0, L_x) && (9)\\ M(0) &= \tilde{T}, && (10)\\ M(L_x) &= \tilde{T}. && (11) \end{aligned}$$

Resolvendo a Equação (9) temos: $M(x) = c_1 x + c_2$. As constantes c_1 e c_2 são determinadas usando as Equações (10) e (11), daí $c_1 = 0$ e $c_2 = \tilde{T}$. Com isto, o filtro M é dado por:

$$M(x) = \tilde{T}. \tag{12}$$

Substituindo a Equação (8) no problema inicial, Equações (4) - (7), e considerando a Equação (12), obtemos o problema de valor de contorno (com condições de contorno homogêneas):

$$\begin{aligned} \frac{\partial u_h}{\partial t} &= \alpha \frac{\partial^2 u_h}{\partial x^2}, \quad \text{em } (0, L_x) \times (0, \infty) && (13)\\ u_h(0,t) &= 0, \quad t \in [0, \infty) && (14)\\ u_h(L_x,t) &= 0, \quad t \in [0, \infty) && (15)\\ u_h(x,0) &= f(x) - \tilde{T}, \quad x \in [0, L_x] && (16) \end{aligned}$$

Problema Auxiliar

Seguindo a TTIC, o problema auxiliar (ou problema de autovalor) apropriado é dado por:

$$\begin{aligned} \frac{d^2\Psi_n(x)}{dx^2} + \lambda_n^2 \Psi_n(x) &= 0, && (17)\\ \Psi_n(0) &= 0, && (18)\\ \Psi_n(L_x) &= 0, && (19) \end{aligned}$$

sendo Ψ_n as autofunções associadas aos autovalores λ_n, sendo $n = 0, 1, \ldots$.

A solução deste problema auxiliar é dada por [9], a saber:

$$\Psi_n(x) = \operatorname{sen}(\lambda_n x).$$

Considerando a condição inicial, Equação (19), obtemos os autovalores:

$$\lambda_n = \frac{n\pi}{L_x}.$$

A partir da propriedade de ortogonalização das autofunções Ψ_n:

$$\left\langle \Psi_m, \Psi_n \right\rangle = \int_0^{L_x} \operatorname{sen}(\lambda_m x)\operatorname{sen}(\lambda_n x)dx = \begin{cases} N_n, & m = n, \\ 0, & m \neq n, \end{cases}$$

sendo N_n dado por [9]:

$$N_n = \int_0^{L_x} \Psi_n^2 dx = \int_0^{L_x} \operatorname{sen}^2(\lambda_n x)dx = \frac{2}{L_x}.$$

As autofunções normalizadas (ou núcleo) são dadas por, para $n = 0, 1, 2, ...$:

$$\tilde{\Psi}_n(x) = \frac{\Psi_n(x)}{N_n^{1/2}} \quad \Longrightarrow \quad \tilde{\Psi_n}(x) = \sqrt{\frac{2}{L_x}}\operatorname{sen}(\lambda_n x). \tag{20}$$

Logo, temos que:

$$\left\langle \tilde{\Psi}_m, \tilde{\Psi}_n \right\rangle = \int_0^{L_x} \tilde{\Psi}_m \tilde{\Psi}_n dx = \delta_{mn} = \begin{cases} 1, & m = n, \\ 0, & m \neq n. \end{cases} \tag{21}$$

sendo δ_{mn} o delta de Kronecker.

Par Transformada-Inversa

O próximo passo da TTIC é determinar o par transformada-fórmula de inversão:

$$\overline{u}_n(t) = \int_0^{L_x} \tilde{\Psi}_n(x) u_h(x,t)dx : \text{Transformada}, \tag{22}$$

$$u_h(x,t) = \sum_{n=0}^{\infty} \tilde{\Psi}_n(x)\overline{u}_n(t) : \text{Fórmula de inversão}. \tag{23}$$

A partir da fórmula de inversão, temos:

$$\frac{\partial u_h}{\partial t} = \sum_{m=0}^{\infty} \tilde{\Psi}_m(x)\overline{u}'_m(t), \tag{24}$$

e

$$\frac{\partial^2 u_h}{\partial x^2} = \sum_{m=0}^{\infty} \tilde{\Psi}''_m(x)\overline{u}_m(t). \tag{25}$$

Na Equação (13) multiplicamos ambos os membros por $\tilde{\Psi}_n(x)$ e aplicamos a integral definida no intervalo $[0, L_x]$ e nesta substituimos as Equações (24), (25) e (21), com isso obtemos:

$$\sum_{m=0}^{\infty} \overline{u}'_m(t) \int_0^{L_x} \tilde{\Psi}_n(x)\tilde{\Psi}_m(x)dx = \sum_{m=0}^{\infty} (-\lambda_m^2 \alpha)\overline{u}_m(t) \int_0^{L_x} \tilde{\Psi}_n(x)\tilde{\Psi}_m(x)dx.$$

Logo, para $m, n = 0, 1, 2, ...$, obtemos:

$$\sum_{m=0}^{\infty} \delta_{mn} \overline{u}'_m(t) = \sum_{m=0}^{\infty} (-\alpha \lambda_m \lambda_n \delta_{mn}) \overline{u}_m(t). \tag{26}$$

As Equações (26) podem ser escritas na forma matricial e referem-se a um sistema infinito de Equações Diferenciais Ordinárias lineares homogêneas, ou seja:

$$\begin{pmatrix} \overline{u}'_0(t) \\ \overline{u}'_1(t) \\ \vdots \\ \overline{u}'_n(t) \\ \vdots \end{pmatrix} = \begin{pmatrix} -\lambda_0^2\alpha & 0 & \dots & 0 & 0 & \dots \\ 0 & -\lambda_1^2\alpha & \dots & 0 & 0 & \dots \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots \\ 0 & 0 & \dots & 0 & -\lambda_n^2\alpha & \dots \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots \end{pmatrix} \begin{pmatrix} \overline{u}_0(t) \\ \overline{u}_1(t) \\ \vdots \\ \overline{u}_n(t) \\ \vdots \end{pmatrix}.$$

Assim, para cada $n = 0, 1, 2, ...$, o sistema acima reduz-se ao problema de valor inicial:

$$\overline{u}'_n(t) = -\alpha \lambda_n^2 \overline{u}_n(t), \tag{27}$$

cuja condição inicial é dada pela Transformada, Equação (22), no ponto $t = 0$, isto é:

$$\overline{u}_n(0) = \int_0^{L_x} \tilde{\Psi}_n(x)(f(x) - \tilde{T}) dx. \tag{28}$$

A solução do problema dado pelas Equações (27) e (28) é:

$$\overline{u}_n(t) = \overline{u}_n(0) e^{-\alpha \lambda_n^2 t}. \tag{29}$$

Substituindo a Equação (20) e a Equação (29) na fórmula de inversão, Equação (23), obtemos:

$$u_h(x,t) = \sum_{n=0}^{\infty} \sqrt{\frac{2}{L_x}} \operatorname{sen}(\lambda_n x) \overline{u}_n(0) e^{-\alpha \lambda_n^2 t}. \tag{30}$$

Substituindo as Equações (12) e (30) na Equação (8), temos:

$$u(x,t) = \sum_{n=0}^{\infty} \sqrt{\frac{2}{L_x}} \operatorname{sen}(\lambda_n x) \overline{u}_n(0) e^{-\alpha \lambda_n^2 t} + \tilde{T}, \tag{31}$$

sendo:

$$\overline{u}_n(0) = \sqrt{\frac{2}{L_x}} \int_0^{L_x} \operatorname{sen}(\lambda_n x)(f(x) - \tilde{T}) dx.$$

Portanto, a solução da equação do calor unidimensional, via TTIC, é dada por:

$$u(x,t) = \frac{2}{L_x} \sum_{n=0}^{\infty} \operatorname{sen}(\lambda_n x) e^{-\alpha \lambda_n^2 t} \int_0^{L_x} \operatorname{sen}(\lambda_n x)(f(x) - \tilde{T}) dx + \tilde{T}. \tag{32}$$

2.2 Equação do calor bidimensional

Problema de valor de contorno bidimensional

Considerando as Equações (1), (2) e (3), sejam $\Omega = (0, L_x) \times (0, L_y) \subset \mathbb{R}^2$, $L_x > 0$ e $L_y > 0$, e o bordo Γ formado pelas arestas do retângulo $[0, L_x] \times [(0, L_y]$. Com isto, temos uma placa plana retangular de material homogêneo, $\overline{\Omega}$, onde não há troca de calor com o exterior através da superfície lateral da placa, sendo que os extremos correspondem ao bordo, Γ, e estão mantidos à temperatura constante igual a zero, $\tilde{T} = 0$ $(^\circ C)$, conforme a condição de contorno (2).

Procuramos uma função u, tal que $u \in C^2(\Omega \times (0, +\infty)) \cap C(\overline{\Omega} \times [0, +\infty))$, relativa ao problema de valor de contorno bidimensional [8]:

$$\frac{\partial u}{\partial t} = \alpha \left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} \right), \quad \text{em } \Omega \times (0, \infty) \tag{33}$$

$$u(0, y, t) = 0, \quad y \in [0, L_y], \ \ t \in [0, \infty), \tag{34}$$

$$u(L_x, y, t) = 0, \quad y \in [0, L_y], \ \ t \in [0, \infty), \tag{35}$$

$$u(x, 0, t) = 0, \quad x \in [0, L_x], \ \ t \in [0, \infty), \tag{36}$$

$$u(x, L_y, t) = 0, \quad x \in [0, L_x], \ \ t \in [0, \infty), \tag{37}$$

$$u(x, y, 0) = f(x, y), \quad (x, y) \in \overline{\Omega}, \tag{38}$$

Separação de Variáveis

Para a resolução do problema de condução de calor bidimensional com condições de contornos homogêneos, será utilizado o método da separação de variáveis. Para isso, tomamos a função u definida da seguinte forma:

$$u(x, y, t) = F(x)G(y)H(t), \tag{39}$$

sendo F, G, funções diferenciáveis de classe $C^2(\Omega \times (0, +\infty))$, no mínimo, relativas às variáveis x e y, respectivamente, e H uma função diferenciável de classe $C^1(\Omega \times (0, +\infty))$, no mínimo, relativa a variável t. Logo, temos que $\frac{\partial u}{\partial t} = F(x)G(y)\frac{dH(t)}{dt}$, $\frac{\partial^2 u}{\partial^2 x} = \frac{d^2F(x)}{d^2x}G(y)H(t)$ e $\frac{\partial^2 u}{\partial^2 y} = F(x)\frac{d^2G(y)}{d^2y}H(t)$. Substituindo estas expressões na Equação (33), obtemos:

$$F(x)G(y)H_t(t) = \alpha(\ F_{xx}(x)G(y)H(t) + F(x)G_{yy}H(t)\ ),$$

onde considerando $H_t(t) = \frac{dH(t)}{dt}$, $F_{xx}(x) = \frac{d^2F(x)}{d^2x}$ e $G_{yy}(y) = \frac{d^2G(y)}{d^2y}$.

Na expressão acima, dividimos ambos lados por $\alpha F(x)G(y)H(t) \neq 0$, para $x \in [0, L_x], y \in [0, L_y]$ e $t \in [0, +\infty]$, daí obtemos:

$$\frac{1}{\alpha}\frac{H_t(t)}{H(t)} = \frac{F_{xx}(x)}{F(x)} + \frac{G_{yy}(y)}{G(y)}. \tag{40}$$

O lado esquerdo da Equação (40) depende somente de t e, o lado direito, depende das variáveis x e y. Desta forma, podemos representar cada lado desta expressão pela constante, $-\sigma^2$, assim temos que:

$$\frac{1}{\alpha}\frac{H_t(t)}{H(t)} = -\sigma^2, \quad \text{e} \tag{41}$$

$$\frac{F_{xx}(x)}{F(x)} + \frac{G_{yy}(y)}{G(y)} = -\sigma^2. \tag{42}$$

Na Equação (42) fazemos:

$$\frac{F_{xx}(x)}{F(x)} = -\frac{G_{yy}(y)}{G(y)} - \sigma^2, \tag{43}$$

e analogamente ao que fizemos acima, cada lado da Equação (43) pode ser igualado à constante "$-\xi^2$", já que o lado esquerdo depende somente da variável x e o lado direito depende da variável y. Desta forma, temos:

$$\begin{aligned} \frac{F_{xx}(x)}{F(x)} &= -\xi^2, \quad \text{e} \\ -\frac{G_{yy}(y)}{G(y)} - \sigma^2 &= -\xi^2. \end{aligned} \tag{44}$$

Considerando $\eta^2 = \sigma^2 - \xi^2$, temos a seguinte expressão:

$$\frac{G_{yy}(y)}{G(y)} = -\eta^2. \tag{45}$$

Aplicamos as condições de contorno, Equações (34) até (38), na Equação (39), daí, a partir das Equações (44) e (45), temos os seguintes problemas de valor inicial:

$$\begin{cases} F_{xx}(x) + \xi^2 F(x) = 0 \\ F(0) = F(L_x) = 0 \end{cases} \tag{46}$$

$$\begin{cases} G_{yy}(y) + \eta^2 G(y) = 0 \\ G(0) = G(L_y) = 0 \end{cases} \tag{47}$$

As autofunções F_m relativas aos autovalores ξ_m do problema de valor inicial (46) e as autofunções G_n relativas aos autovalores η_n do problema de valor inicial (47), conforme [9], respectivamente, são dadas, para $m, n = 0, 1, 2, ...$:

$$\begin{cases} F_m(x) = \operatorname{sen}(\xi_m x) \\ \xi_m = \frac{m\pi}{L_x} \end{cases} \tag{48}$$

$$\begin{cases} G_n(y) = \operatorname{sen}(\eta_n y) \\ \eta_n = \frac{n\pi}{L_y} \end{cases} \tag{49}$$

A partir da Equação (41) temos a equação diferencial ordinária homogênea $H_t(t) + \sigma^2 \alpha H(t) = 0$, cuja solução geral é dada por $H_{mn}(t) = c_0 e^{-\sigma_{mn}^2 \alpha t}$, sendo $\sigma_{mn}^2 = \xi_m^2 + \eta_n^2$, e sem perda da generalidade, tomamos $c_0 = 1$, logo:

$$H_{mn}(t) = e^{-\sigma_{mn}^2 \alpha t}. \tag{50}$$

Pelo princípio da superposição, temos que:

$$u(x, y, t) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} A_{mn} u_{mn}(x, y, t), \tag{51}$$

sendo $u_{mn}(x, y, t) = F_m(x) G_n(y) H_{mn}(t)$.

A seguir determinaremos os coeficientes A_{mn} e o perfil de temperatura u.

(a) Condição inicial para $t = 0$

Pela condição inicial, Equação (34), e considerando a Equação (50), tem-se $H_{mn}(0) = 1$, logo, a Equação (51) é dada por:

$$f(x,y) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} A_{mn}F_m(x)G_n(y). \tag{52}$$

(b) Coeficientes A_{mn}

Sendo $u_1 \in C(\overline{\Omega} \times \{0\})$ e $u_2 \in C^2(\Omega \times \{0\})$, definimos o produto interno:

$$\Big\langle u_1, u_2 \Big\rangle = \int_0^{L_x}\int_0^{L_y} u_1 u_2 dydx.$$

Tomando $u_1 = u_1(x,y,0) = f(x,y)$ e $u_2 = u_2(x,y,0) = F_p(x)G_q(y)$, $p,q = 0,1,2,...$, e pela Equação (52), juntamente com as propriedades do produto interno, temos:

$$\Big\langle f(x,y), F_p(x)G_q(y) \Big\rangle = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} A_{mn}\Big\langle F_m(x)G_n(y), F_p(x)G_q(y) \Big\rangle.$$

Pela propriedade de ortogonalidade [10], temos que:

$$\Big\langle F_m(x)G_n(y), F_p(x)G_q(y) \Big\rangle = \begin{cases} N_{mn}, & m = p \ \text{ e } n = q, \\ 0, & m \neq p \ \text{ e } n \neq q, \end{cases}$$

sendo $N_{mn} = \int_0^{L_x}\int_0^{L_y} F_m^2 G_n^2 dydx$ e considerando as autofunções, Equações (48) e (49), obtemos:

$$\Big\langle f(x,y), F_m(x)G_n(y) \Big\rangle = A_{mn}\frac{L_x L_y}{4}.$$

Logo, para $m,n = 0,1,2,...$:

$$A_{mn} = \frac{4}{L_x L_y}\int_0^{Lx}\int_0^{Ly} f(x,y)F_m(x)G_n(y)dydx.$$

(c) Perfil de temperatura $u = u(x,y,t)$

Na Equação (51) substituímos as Equações (48), (49) e (50) e, com isso, determinamos a solução da equação do calor bidimensional, ou seja:

$$u(x,y,t) = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} A_{mn}e^{-\alpha\pi^2\left(\left(\frac{m}{L_x}\right)^2+\left(\frac{n}{L_y}\right)^2\right)t}\,\text{sen}\left(\frac{mx\pi}{L_x}\right)\,\text{sen}\left(\frac{ny\pi}{L_y}\right). \tag{53}$$

2.3 Equação do calor tridimensional

Problema de valor de contorno tridimensional

No objetivo deste trabalho propomos determinar as soluções dos problemas de condição de valor de contorno uni e bidimensional, contudo, estendemos o problema de condução de calor da placa plana para um sólido e para este não será realizado a análise dos resultados.

Considerando as Equações (1), (2) e (3), sejam $\Omega = (0, L_x) \times (0, L_y) \times (0, L_z) \subset \mathbb{R}^3$, $L_x > 0$, $L_y > 0$ e $L_z > 0$, e o bordo Γ formado pelas faces do paralelogramo regular $[0, L_x] \times [0, L_y] \times [0, L_z]$. Desta forma, temos um sólido de material homogêneo, $\overline{\Omega}$, onde não há troca de calor com o exterior através da superfície lateral deste sólido, sendo que os extremos correspondem ao bordo, Γ, e estão mantidos à temperatura constante igual a zero, $\tilde{T} = 0\ (^\circ C)$, conforme a condição de contorno (2).

Procuramos uma função u, tal que $u \in C^2(\Omega \times (0, +\infty)) \cap C(\overline{\Omega} \times [0, +\infty))$, relativa ao problema de valor de contorno tridimensional [8]:

$$\begin{aligned}
\frac{\partial u}{\partial t} &= \alpha\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}\right), \quad \text{em } \Omega \times (0, \infty), \\
u(0, y, z, t) &= 0, \quad y \in [0, L_y], \ z \in [0, L_z] \ \text{ e } \ t \in [0, \infty), \\
u(L_x, y, z, t) &= 0, \quad y \in [0, L_y], \ z \in [0, L_z] \ \text{ e } \ t \in [0, \infty), \\
u(x, 0, z, t) &= 0, \quad x \in [0, L_x], \ z \in [0, L_z] \ \text{ e } \ t \in [0, \infty), \\
u(x, L_y, z, t) &= 0, \quad x \in [0, L_x], \ z \in [0, L_z] \ \text{ e } \ t \in [0, \infty), \\
u(x, y, 0, t) &= 0, \quad x \in [0, L_x], \ y \in [0, L_y] \ \text{ e } \ t \in [0, \infty), \\
u(x, y, L_z, t) &= 0, \quad x \in [0, L_x], \ y \in [0, L_y] \ \text{ e } \ t \in [0, \infty), \\
u(x, y, z, 0) &= f(x, y, z), \quad (x, y, z) \in \overline{\Omega}.
\end{aligned}$$

A solução do problema de valor de contorno relativo à equação do calor tridimensional é obtida de forma análoga ao procedimento realizado para a equação do calor bidimensional, ou seja, utilizando a separação de variáveis, $u(x, y, z, t) = F(x)G(y)H(z)V(t)$, temos:

$$\begin{aligned}
u(x, y, z, t) &= \sum_{m,n,k=0}^{\infty} A_{mnk} e^{-\alpha\pi^2\left(\left(\frac{m}{L_x}\right)^2 + \left(\frac{n}{L_y}\right)^2 + \left(\frac{k}{L_z}\right)^2\right)t} \operatorname{sen}\left(\frac{mx\pi}{L_x}\right) \operatorname{sen}\left(\frac{ny\pi}{L_y}\right) \operatorname{sen}\left(\frac{kz\pi}{L_z}\right), \\
A_{mnk} &= \frac{4}{L_x L_y L_z} \int_0^{Lx} \int_0^{Ly} \int_0^{Lz} f(x, y, z) F_m(x) G_n(y) H_k(z) dz dy dx,
\end{aligned}$$

sendo $F_m(x) = \operatorname{sen}(\frac{mx\pi}{L_x})$, $G_n(y) = \operatorname{sen}(\frac{ny\pi}{L_y})$ e $H_k(z) = \operatorname{sen}(\frac{kz\pi}{L_z})$.

3 Análise dos resultados

Nesta seção serão analisados a solução, via TTIC, da equação do calor unidimensional, Equação (32), e a solução, via separação de variáveis, da equação do calor bidimensional, Equação (53). Para cada caso, será determinada a ordem de truncamento, N, com erro relativo global previamente definido, bem como a análise qualitativa (ou coerência dos resultados provindos da solução exata relativamente ao modelo físico) por intermédio de gráficos gerados pelo *software* SciDaVis [11]. Os resultados do perfil de temperatura relativos à equação do calor unidimensional e bidimensional foram gerados utilizando o sistema algébrico computacional SAGe [12, 13].

Na Tabela (1) temos os resultados do perfil de temperatura relacionados à equação do calor unidimensional e na Tabela (2) representamos os resultados do perfil de temperatura relacionados à equação do calor bidimensional, onde, em ambos os casos, estabelecemos a ordem de truncamento.

Relativamente à equação de calor unidimensional, nas Figuras (1) e (2) são apresentados os resultados do perfil de temperatura, respectivamente, em função da coordenada tempo t e x. Na Figura (3) temos a temperatura representada no espaço tridimensional.

Nas Figuras (4) e (5) temos os perfis de temperatura, respectivamente, em função da coordenada tempo t e x, referentes à equação do calor bidimensional. Na Figura (7) temos a temperatura representada no espaço tridimensional, onde fixamos uma das variáveis espaciais.

3.1 Equação do Calor Unidimensional – Solução via TTIC

Para esta análise, estabelecemos os seguintes parâmetros iniciais: $L_x = 0,06m$, $\alpha = 1,1410^{-4}m^2/s$ (cobre), $f(x) = 100°C$, $x \in [0; L_x]$, $\tilde{T} = 0°C$ e $t(s) \in [0; 16]$. O tempo máximo foi considerado $16s$, pois, para $t > 16s$, o perfil de temperatura u tende assintoticamente a zero. Os valores da temperatura foram tomados com 3 casas decimais, onde consideramos esta a precisão do instrumento de medição de temperatura.

Tabela 1. (Equação do calor unidimensional) Análise da convergência da temperatura u, na posição $x = 0,01m$ em função da coordenada t.

$\boldsymbol{u}(°C)$				
	$\boldsymbol{N}$			
$\boldsymbol{t}$**(s)**	**1**	**2**	**3**	**4**
2,4	18,624	18,584	18,624	18,624
3,2	14,477	14,473	14,477	14,477
4,0	11,271	11,271	11,271	11,271
4,8	8,778	8,778	8,778	8,778
5,6	6,836	6,836	6,836	6,836
6,4	5,324	5,324	5,324	5,324
7,2	4,146	4,146	4,146	4,146
8,0	3,229	3,229	3,229	3,229
8,8	2,514	2,514	2,514	2,514
9,6	1,958	1,958	1,958	1,958
10,4	1,525	1,525	1,525	1,525
11,2	1,188	1,188	1,188	1,188
12,0	0,925	0,925	0,925	0,925
12,8	0,720	0,720	0,720	0,720
13,6	0,561	0,561	0,561	0,561
14,4	0,437	0,437	0,437	0,437
15,2	0,340	0,340	0,340	0,340
16,0	0,265	0,265	0,265	0,265

A Tabela (1) apresenta resultados para a temperatura, em função da variável t, para vários truncamentos N, relacionados à equação do calor unidimensional, onde fixamos $x = 0,01m$. Para esta análise, podemos tomar qualquer valor de x, $x \in [0,00; 0,06]$, que teremos

as mesmas ordens de truncamento. Para verificar a ordem de truncamento, fixamos uma linha, por exemplo, em $t = 2,4s$, e verificamos que, para $N = 1$ temos $u = 18,624$, para $N = 2$ temos $u = 18,584$, para $N = 3$ temos $u = 18,624$ e para $N \geq 4$ os valores $u = 18,624$ se repetem. Para $t \geq 4,0s$, a convergência de u ocorre para $N = 1$. Desta forma, consideramos a maior ordem de truncamento, assim $N = 3$.

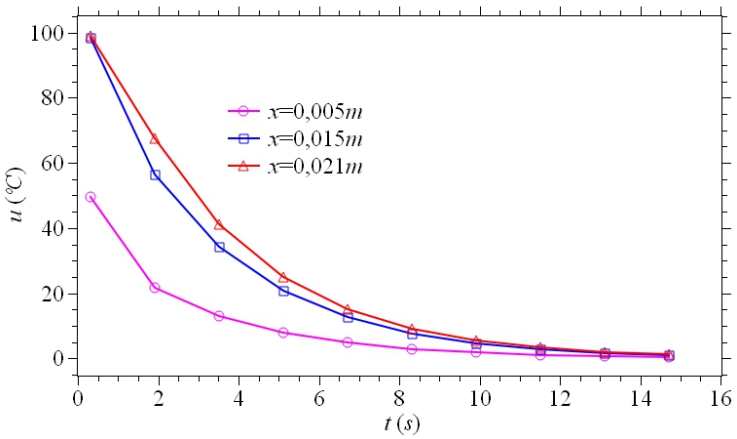


Figura 1. (Equação do calor unidimensional) Perfil de temperatura em função do tempo t, para as posições $x = 0,005m$, $x = 0,015m$ e $x = 0,021m$. Fonte: Próprio autor.

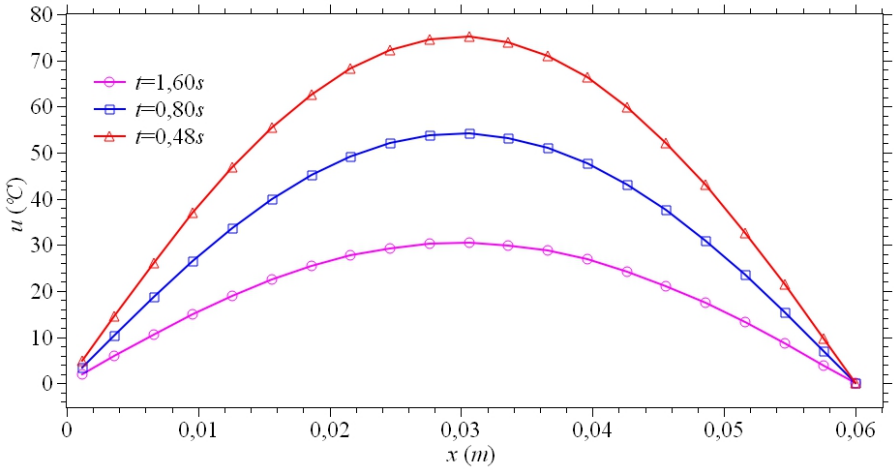


Figura 2. (Equação do calor unidimensional) Perfil de temperatura em função da posição x, para os tempos $t = 0,48s$, $t = 0,80s$ e $t = 1,60s$. Fonte: Próprio autor.

Na Figura (1) são apresentados os perfis da temperatura u em função do tempo t, fixando $x = 0,005m$, $x = 0,015m$ e $x = 0,021m$. Vemos que, conforme o tempo aumenta a temperatura decresce, até atingir o valor mínimo igual a $\tilde{T} = 0°C$. Aumentando a posição x, a temperatura u também aumenta e isto ocorre até a posição $x = 0,03m$, e daí, a partir

deste ponto, a temperatura começa à diminuir (ver Figura (2)). Essa evolução está de acordo com a teoria física apresentada, ou seja, quando o material condutor cede calor, ocorre a diminuição da temperatura.

Temos na Figura (2) os perfis da temperatura u em função da posição x, fixando $t = 0,48s$, $t = 0,80s$ e $t = 1,60s$. Nas posição $x = 0,00m$ e $x = 0,06m$ a temperatura inicial é $\tilde{T} = 0°C$ e, quando $t = 0s$ tem-se uma temperatura uniforme de $100°C$ em toda extensão da barra. Fixando o tempo, para $t > 0$, observamos que, conforme se aumenta x até a posição $x = 0,03m$ a temperatura cresce até $100°C$ e, a partir deste ponto até $x = 0,06m$, ocorre a diminuição da temperatura voltando para $\tilde{T} = 0°C$. Fixando uma posição x vemos que, se aumentamos o tempo t, a temperatura diminui. Este processo está de acordo como fenômeno físico que envolve transporte de calor em uma barra.

Os efeitos físicos observados nas Figuras (1) e (2) podem ser vistos na Figura (3), que refere-se a representação gráfica do perfil de temperatura $u = u(x,t)$. A solução da equação do calor unidimensional, provinda do trabalho de [14], é equivalente a Equação (32).

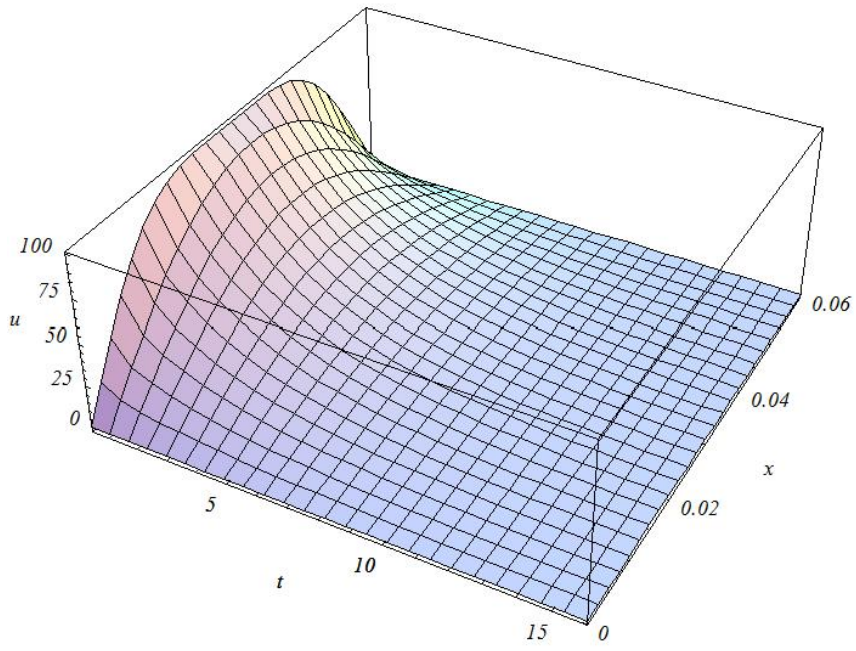


Figura 3. (Equação do calor unidimensional) Representação gráfica tridimensional do perfil de temperatura $u = u(x,t)$, considerando o domínio $(x,t) \in [0,00; 0,06] \times [0; 16]$. Fonte: Próprio autor.

3.2 Equação do Calor Bidimensional – Solução via Separação de Variáveis

Para esta análise, estabelecemos os seguintes parâmetros iniciais: $L_x = 0,06m$, $L_y = 0.10m$, $\alpha = 1,1410^{-4}m^2/s$ (cobre), $f(x,y) = 100°C$, $x \in [0; L_x]$, $y \in [0; L_y]$ e $t \in [0; 16]$. O tempo máximo foi considerado $16s$ e os valores da temperatura foram tomados com 3 casas decimais, conforme justificativa feita na seção anterior.

Tabela 2. (Equação do calor bidimensional) Análise da convergência da temperatura u, na posição $x = 0,01m$ e $y = 0,01m$ em função da coordenada t.

$\boldsymbol{u}(^\circ C)$						
	$\boldsymbol{N}$					
$\boldsymbol{t}$ (s)	**1**	**2**	**3**	**4**	**5**	**6**
1.6	7.842	7.842	9.614	9.614	9.683	9.683
2,4	5,582	5,582	6,156	6,156	6,162	6,162
3,2	3,973	3,973	4,168	4,168	4,169	4,169
4,0	2,827	2,827	2,895	2,895	2,895	2,895
4,8	2,012	2,012	2,036	2,036	2,036	2,036
5,6	1,432	1,432	1,440	1,440	1,440	1,440
6,4	1,019	1,019	1,022	1,022	1,022	1,022
7,2	0,726	0,726	0,727	0,727	0,727	0,727
8,0	0,516	0,516	0,517	0,517	0,517	0,517
8,8	0,368	0,368	0,368	0,368	0,368	0,368
9,6	0,262	0,262	0,262	0,262	0,262	0,262
10,4	0,186	0,186	0,186	0,186	0,186	0,186
11,2	0,133	0,133	0,133	0,133	0,133	0,133
12,0	0,094	0,094	0,094	0,094	0,094	0,094
12,8	0,067	0,067	0,067	0,067	0,067	0,067
13,6	0,048	0,048	0,048	0,048	0,048	0,048
14,4	0,034	0,034	0,034	0,034	0,034	0,034
15,2	0,024	0,024	0,024	0,024	0,024	0,024
16,0	0,017	0,017	0,017	0,017	0,017	0,017

A Tabela (2) apresenta resultados para a temperatura u, em função da variável t, para vários truncamentos N, relacionados à equação do calor bidimensional, onde fixamos $x = 0,01m$ e $y = 0,01m$. Para esta análise, podemos tomar qualquer valor de x e y, $x \in [0,00; 0,06]$ e $y \in [0,00; 0,10]$, que teremos as mesmas ordens de truncamento. Para verificar a ordem de truncamento, fixamos uma linha, por exemplo, em $t = 1,6s$, e verificamos que, para $N = 1$ temos $u = 7,842$, para $N = 2$ temos $u = 7,842$, para $N = 3$ temos $u = 9,614$, para $N = 4$ temos $u = 9,614$, para $N = 5$ temos $u = 9,683$ e para $N \geq 6$ os valores $u = 9,683$ se repetem. Para $t \geq 8,8s$, a convergência de u ocorre para $N = 1$. Desta forma, consideramos a maior ordem de truncamento, assim $N = 5$.

Na Figura (4) são apresentados os perfis da temperatura u em função do tempo t, $t \in [0; 16]$, para $y = 0,01m$, $y = 0,04m$ e $y = 0,08m$, fixando $x = 0,01m$. Vemos que, conforme o tempo cresce, a temperatura decresce, até atingir o valor mínimo igual a $\tilde{T} = 0^\circ C$. Aumentando a posição y, fixando x, a temperatura u também aumenta. Essa evolução está de acordo com a teoria física apresentada, ou seja, quando o material condutor cede calor, ocorre a diminuição da temperatura.

Temos na Figura (5) os perfis da temperatura u em função da posição x, $x \in [0,00; 0,06]$, para $y = 0,01m$, $y = 0,04m$ e $y = 0,08m$, fixando $t = 1,6s$. Nas posição $x = 0,00m$ e $x = 0,06m$ a temperatura inicial é $\tilde{T} = 0^\circ C$ e, quando $t = 0s$ tem-se uma temperatura uniforme de $100^\circ C$ em toda extensão da barra. Fixando a posição x, observamos que, conforme se aumenta x até a posição $x = 0,03m$ a temperatura cresce até $100^\circ C$ e, a partir deste ponto até $x = 0,06m$, ocorre a diminuição da temperatura voltando para $\tilde{T} = 0^\circ C$. Fixando uma posição x vemos que, se aumentamos o tempo t, a temperatura diminui. Este processo está de acordo como fenômeno fisico que envolve transporte de calor em uma barra.

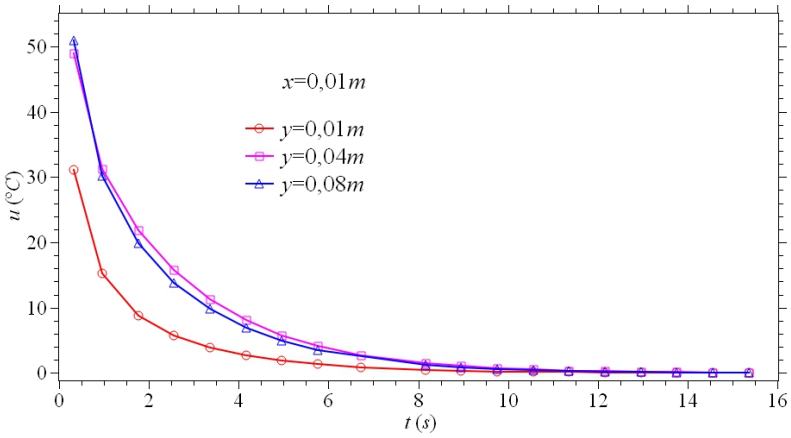


Figura 4. (Equação do calor bidimensional) Perfil de temperatura em função do tempo t, para as posições $y = 0,01m$, $y = 0,04m$ e $y = 0,08m$, fixando $x = 0,01m$. Fonte: Próprio autor.

Na Figura (6) mostramos os perfis da temperatura u em função da posição y, $y \in [0,00; 0,10]$, para $t = 0,1,6s$, $t = 3,2s$ e $t = 4,8s$, fixando $x = 0,012m$. Nas posições $y = 0,00m$ e $y = 0,1m$ a temperatura inicial é $\tilde{T} = 0°C$ e, quando $t = 0s$ tem-se uma temperatura uniforme de $100°C$ em toda extensão da placa. Variando a posição y, observamos que, conforme se aumenta t até a posição $y = 0,05m$ a temperatura cresce até $100°C$ e, a partir deste ponto até $y = 0,1m$, ocorre a diminuição da temperatura voltando para $\tilde{T} = 0°C$. A oscilação térmica também é facilmente observada, como por exemplo, escolhendo arbitrariamente $x = 0,012$ (poderia ser qualquer outro valor de x, pois o comportamento oscilatório é por toda placa, havendo apenas a variação da amplitude da temperatura), e com a variação de y, o perfil ondulatório é visto no gráfico. Por fim, o decaimento da temperatura ao longo de y é esperado devido ao resfriamento que ocorreu nas extremidades da placa e que estão contempladas nas condições de contorno da Equação do Calor Bidimensional.

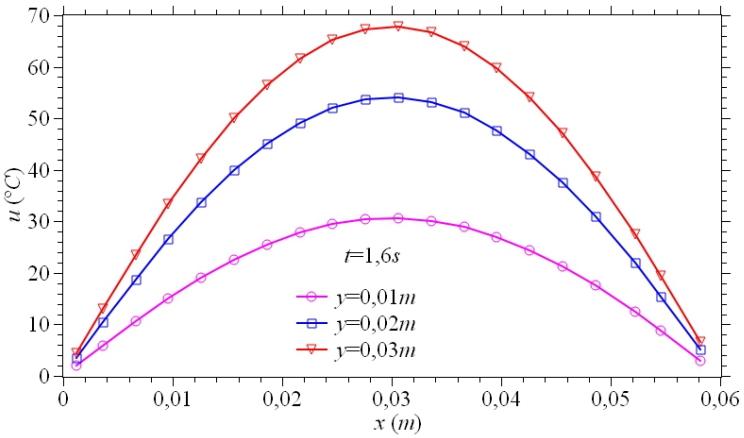


Figura 5. (Equação do calor bidimensional) Perfil de temperatura em função da coordenada x, para as posições $y = 0,01m$, $y = 0,02m$ e $y = 0,03m$, fixando $t = 1,6s$. Fonte: Próprio autor.

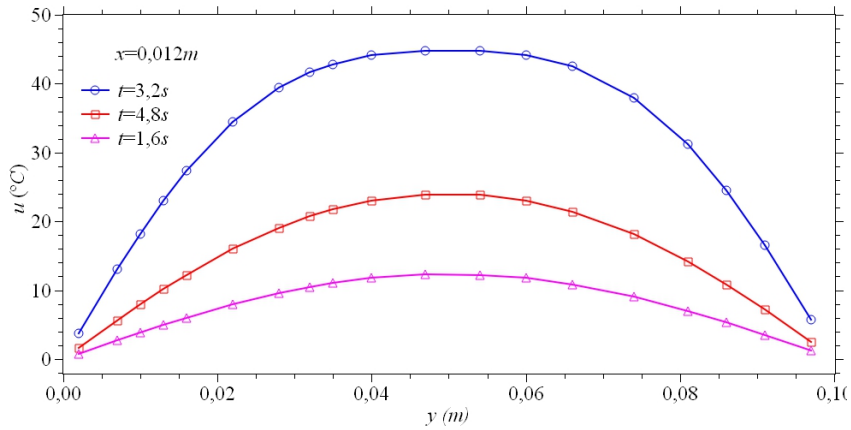


Figura 6. (Equação do calor bidimensional) Perfil de temperatura em função da coordenada y, para os tempos $t = 1,6s$, $t = 3,2s$ e $t = 4,8s$, fixando $x = 0,012m$. Fonte: Próprio autor.

Os efeitos físicos observados nas Figuras (4) e (5) podem ser vistos na Figura (7), que refere-se a representação gráfica do perfil de temperatura $u = u(x, y, t)$. A solução da equação do calor bidimensional, provinda do trabalho de [15], é equivalente a Equação (53).

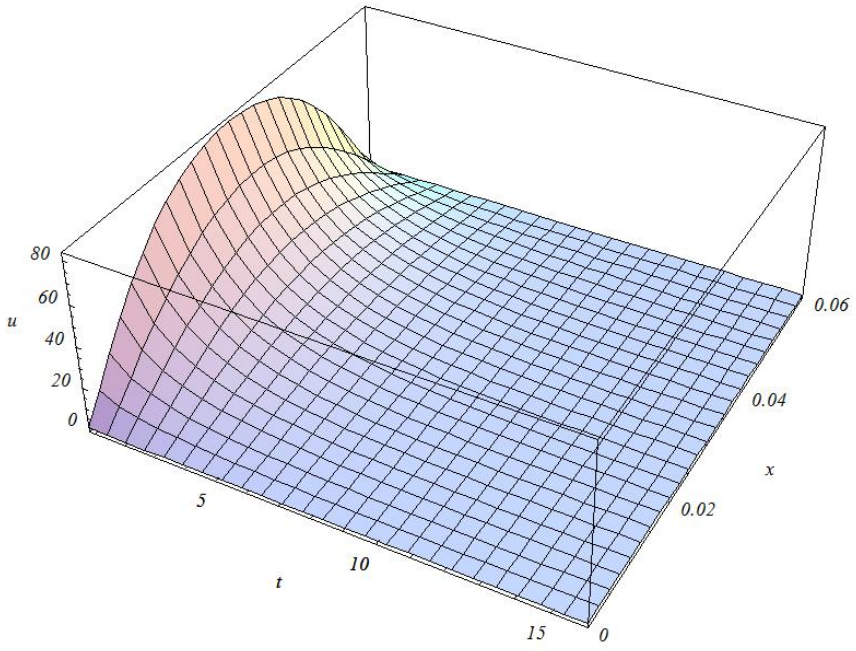


Figura 7. (Equação do calor bidimensional) Representação gráfica tridimensional do perfil de temperatura $u = u(x, y, t)$, considerando o domínio $(x, t) \in [0,00; 0,06] \times [0; 16]$, para $y = 0,02m$. Fonte: Próprio autor.

4 Conclusões

Este trabalho teve como objetivo principal analisar a equação diferencial parcial do calor unidimensional e bidimensional, para determinar seu perfil através da resolução por meio da (TTIC) Técnica da Transformada Integral Clássica e Separação de Variáveis. Assim, com os resultados obtidos, pode-se verificar as temperaturas de acordo com o tempo em um condutor.

A aplicação da Técnica da Transformada Integral para a obtenção do campo de temperatura unidimensional e da Separação de Variáveis para o modelo bidimensional se mostraram ferramentas eficazes, pois, a partir dos resultados obtidos, vimos que o perfil de temperatura foi desenvolvido com grande êxito, em todas as condições de contorno impostas, isso pode ser comprovado após a análise dos gráficos e tabelas obtidos computacionalmente.

Como sugestão para futuros trabalhos, para dar continuidade a mesma linha de pesquisa, seria o desenvolvimento de um modelo bidimensional, para se observar como a temperatura se comporta e se haveria semelhança com os resultados obtidos a partir da construção de um experimento, que consiste no aquecimento das bordas em uma placa condutora. Dessa forma, pode-se comparar a solução analítica com resultados experimentais, isso seria um ponto importante a ser estudado.

Referências

[1] KARCZ, J; CUDAK, M; SZOPLIK, J. Stirring of a liquid in a stirred tank with an eccentrically located impeller. *Chemical Engengineering Science*, v.60, p. 2369-2380, 2005.

[2] SCHÄFER, M; KARASÖZEN, B; ULUDAG, Y; YAPICI, K; UGUR, Ö. Numerical method for optimizing stirrer configurations. *Computational Chemical Engineering*, v.30, p. 183-190, 2005.

[3] INCROPERA, F.P; DEWITT, D.P. Fundamentos de Transferência de Calor e de Massa. LTC, 3a Edição, Rio de Janeiro, 1990.

[4] AYDIN, O; AVCI, M. Analysis of laminar heat transfer in micro-Poiseuille flow. International *Journal of Thermal Sciences*, v. 46, p. 30-37, 2007.

[5] POVSTENKO, Y. Z. Fractional radial heat conduction in an infinite medium with a cylindrical cavity and associated thermal stresses. *Mechanics Research Communications*, v. 37, p. 436-440, 2010.

[6] D'ALESSANDRO, N. R. Estudo das Soluções Analíticas da Equação do Calor Unidimensional e Bidimensional. Dissertação de Mestrado - Universidade Federal de São Carlos, 2016.

[7] BRÉZIS, H. Análisis Funcional: Teoría y Aplicaciones. Alianza Editorial. Madrid, 1984.

[8] IÓRIO, V. EDP: Um Curso de Graduação. IMPA, Rio de Janeiro, 2016

[9] ÖZISIK, M.N. Heat Conduction. John Wiley, New York., 1980.

[10] CALLIOLI, C. A; DOMINGUES, H.H; COSTA, R.C.F. Álgebra Linear e Aplicações. 4a. edição, São Paulo, Atual, 1983.

[11] QTIPLOT, SciDavis v. 1.D8. http://www.scidavis.sourceforge.net, 2014.

[12] DEVELOPERS, T. S: SageMath, the SageMathematics Software System (Version 7.2), http://www.sagemath.org, 2016.

[13] PÉRES, F, GRANGER, B. E. IPython: A System for Interactive Scientific Computing, Computing in Science and Engineering. Disponível em: http://ipython.org. Acessado em 27/04/2017. 2007.

[14] ZILL, D.G; CULLEN, M.R. Equações Diferenciais - Vol. 2. Pearson Makron Books, São Paulo, 2001.

[15] BIEZUNER, R.J. Equações Diferenciais Parciais Lineares. Disponível em: http://www.mat.ufmg.br/rodney. Acessado em 27/04/2017. 2010.

Sistemas de Identificação Modular: Uma Aplicação no Ensino Fundamental

Modular Identification Systems: An Application in Elementary Education

Fernanda Rodrigues Alves Costa
Instituto Federal de Educação Ciências e Tecnologia de Minas Gerais - Belo Horizonte, MG
fernandaracosta@gmail.com

Marcelo Oliveira Veloso
Universidade Federal de São João del-Rei - UFSJ, Ouro Branco, MG
veloso@ufsj.edu.br

Resumo: Neste trabalho realizamos um breve estudo sobre os sistemas de identificação modular que detectam erros cometidos durante a transmissão, digitação ou leitura de dados. Listamos os erros mais frequentes cometidos por um operador ao digitar um número. Em particular, descrevemos três exemplos de sistemas de identificação modular, o CPF, o ISBN e o cartão de crédito, analisando-os em relação à capacidade de detectarem erros. Por fim, recomendamos uma aplicação direta em sala de aula utilizando o recurso dos blocos lógicos.

Palavras-chave: sistemas de identificação de erros; aritmética modular; blocos lógicos.

Abstract: In this paper we perform a brief study on modular identification systems that detects errors committed during transmission, typing or data reading. We list the most frequent mistakes made by an operator when entering a number. In particular, we describe three examples of modular identification systems, the CPF, the ISBN and the credit card, analyzing them for the ability to detect errors. Finally, we recommend a direct application in the classroom using the logic blocks.

Key words: error identification systems; modular arithmetic; logic blocks.

1 Introdução

"Os erros são quase sempre de uma natureza sagrada. Nunca tente corrigi-los. Pelo contrário: racionalize-os, compreenda-os a fundo. Depois disso, lhe será possível sublimá-los."
(Salvador Dalí)

Imagine se em uma transferência bancária o operador cometesse um erro ao digitar o número da conta e o valor fosse depositado para um desconhecido. Seria uma situação realmente desagradável, mas as chances desta falha ocorrer são raras.

O número que identifica uma conta bancária é gerado por um sistema capaz de detectar a maioria dos erros cometidos durante a sua leitura, digitação e transmissão. Estes sistemas utilizam um ou mais algarismos acrescentados ao número original que permitem alertar o operador da ocorrência de um erro. Este dígito adicional é conhecido como dígito verificador.

Recebido em 15/09/2017 - Aceito em 24/11/2017

O dígito verificador é determinado por algoritmos que utilizam conceitos simples da Teoria dos Números, mais especificamente Aritmética Modular. Por isto, estes sistemas são conhecidos como sistemas de identificação modular.

Os sistemas de identificação modular têm grande importância no comércio, na identificação civil, na arrecadação de tributos e em muitas outras áreas. Eles são amplamente utilizados em códigos de barra, documentos de identificação, passaportes, notas fiscais, boletos de cobrança bancária, etc.

Neste artigo apresentamos um breve estudo dos sistemas de identificação modular e exemplos que são avaliados quanto à capacidade de detectar erros. Além disso, propomos uma sequência didática para o desenvolvimento do tema com alunos do Ensino Fundamental.

O principal objetivo deste trabalho é servir como material de apoio para os professores de matemática, principalmente os que lecionam no Ensino Fundamental, em aulas sobre aritmética e suas aplicações. Proporcionado aos alunos uma oportunidade para refletirem, investigarem e construírem o próprio conhecimento. E exemplificar como ideias e conceitos abstratos levam ao desenvolvimento de tecnologias que estão presentes no nosso cotidiano e que visam o bem estar de toda a sociedade.

O texto foi organizado da seguinte maneira: na seção 2, apresentamos as conceitos básicos que fundamentam o trabalho. Na seção 3, discutimos sobre os tipos de erros cometidos ao digitar um número de identificação, definimos os sistemas de identificação modular e estabelecemos as condições para que os sistemas possam detectar determinados tipos de erros. Nas seções 4, 5 e 6 descrevemos, respectivamente, três exemplos concretos de sistema de identificação em utilização no Brasil: o CPF, o ISBN e o cartão de crédito. Para uma melhor compreensão da estrutura de cada um destes modelos analisamos situações concretas. Estes sistemas também são avaliados em relação a capacidade de detecção de erros. Na seção 7 apresentamos uma possibilidade de trabalho deste tema com alunos a partir do 6^o ano do Ensino Fundamental. Uma sequência didática baseada na metodologia de resolução de problemas e investigação matemática é cuidadosamente descrita para orientar o trabalho do professor. A proposta utiliza o recurso dos blocos lógicos para oportunizar a vivência de experiências de codificação e transmissão de dados. Por fim, na seção 8, apresentamos as considerações finais.

2 Conceitos iniciais

Nesta seção, apresentamos algumas definições e propriedades referentes à Teoria dos Números, mais especificamente à Aritmética Modular. Um estudo mais detalhado desse tema pode ser encontrado em [1, 2, 3].

Neste texto, $\mathbb{Z}$ representa o conjunto dos números inteiros com suas operações usuais de adição ($+$) e multiplicação ($\cdot$) e sua relação de ordem ($\leq$), "menor ou igual".

Definição 2.1 *Sejam a e b números inteiros com $a \neq 0$. Dizemos que a divide b e denotamos por $a \mid b$, se existir um inteiro c tal que $b = ac$. Se a não divide b, escrevemos $a \nmid b$.*

É usual dizer que a é um **divisor** de b, ou b é **divisível** por a, ou ainda b é um **múltiplo** de a quando $a \mid b$.

Exemplo 2.1 *Como $6 = 2.3$, então 2 divide 6 e denotamos por $2 \mid 6$. Segue que 2 é um divisor de 6, ou 6 é divisível por 2, ou ainda 6 é um múltiplo de 2.*

Definição 2.2 *Um número inteiro $n > 1$ é **primo** se possui apenas dois divisores positivos: n e 1. Se $n > 1$ não é primo, dizemos que n é **composto**.*

Proposição 2.1 *Se a, b, c, m e n são inteiros, $c \mid a$ e $c \mid b$, então $c \mid (ma + nb)$.*

Demonstração: Se $c \mid a$ e $c \mid b$ então existem inteiros k_1 e k_2 com $a = ck_1$ e $b = ck_2$. Multiplicando essas duas igualdades por m e n, respectivamente, temos $ma = mck_1$ e $nb = nck_2$. Somando membro a membro, obtemos $ma + nb = c(mk_1 + nk_2)$. Assim, segue da Definição 2.1 que $c \mid (ma + nb)$. ■

Definição 2.3 *Para cada inteiro x, define-se o inteiro módulo ou valor absoluto de x, denotado por $|x|$, pela igualdade:*

$$|x| = \begin{cases} x & se\ x \geq 0, \\ -x & se\ x < 0. \end{cases}$$

Segue da definição que $|x| \geq 0$ para todo x e que $|x| = 0$ se, e somente se, $x = 0$.

Teorema 2.1 *Sejam a, d e n números inteiros. Então:*

1. $1 \mid n$, $n \mid n$ e $n \mid 0$;
2. $d \mid n \Rightarrow ad \mid an$;
3. $ad \mid an$ e $a \neq 0 \Rightarrow d \mid n$;
4. $d \mid n$ e $n \neq 0 \Rightarrow |d| \leq |n|$;
5. $d \mid n$ e $n \mid d \Rightarrow |d| = |n|$;
6. $d \mid n$ e $m \in \mathbb{Z} \Rightarrow d \mid nm$.

Demonstração: As afirmações são verificadas individualmente.

1. Observe que $n = 1.n$, $n = n.1$ e $0 = n.0$.
2. Se $d \mid n$, então existe $c \in \mathbb{Z}$ tal que $n = dc$. Logo, $an = (ad)c$, isto é, $ad \mid an$.
3. Se $ad \mid an$, então $an = adc$, para algum inteiro c. Logo $an - adc = 0$ e $a(n - dc) = 0$. Como $a \neq 0$, segue que $(n - dc) = 0$ e, portanto, $n = dc$.
4. Se $d \mid n$, temos que $n = dc$, $n \neq 0$ implica que $c \neq 0$. Portanto, $|c| \geq 1$ e $|n| = |dc| = |d||c| \geq |d|$.
5. Se $d \mid n$ e $n \mid d$, temos que $n = dk_1$ e $d = nk_2$, k_1, $k_2 \in \mathbb{Z}$. Então, $n = dk_1 = nk_2k_1$. Assim, $k_2k_1 = 1$, $k_1 = k_2 = \pm 1$ e, portanto, $|d| = |n|$.
6. Se $d \mid n$, então $n = dc$. Multiplicando ambos os lados desta igualdade por $m \in \mathbb{Z}$, temos $nm = dcm = d(cm)$. Assim, segue pela Definição 2.1 que $d \mid nm$.

■

O próximo resultado é conhecido como Algoritmo da Divisão ou Algoritmo de Euclides.

Teorema 2.2 *Sejam a e b dois números inteiros com $a > 0$. Então existem inteiros q e r tais que*

$$b = a.q + r, \text{ onde } 0 \leq r < a.$$

Os inteiros q e r são únicos e são designados, respectivamente, por quociente e resto da divisão de b por a.

Demonstrado em Teorema 1.2 de [3].

Definição 2.4 *Se a e b são inteiros, dizemos que a é congruente a b módulo $m\,(m > 0)$ se $m \mid (a - b)$ e denotamos $a \equiv b \pmod{m}$. O caso em que a não é congruente ao inteiro b módulo m denotamos por $a \not\equiv b \pmod{m}$.*

Exemplo 2.2 *Temos que $11 \equiv 3 \pmod{2}$ pois $2 \mid (11 - 3)$.*

Proposição 2.2 *Sejam a e b inteiros. Então $a \equiv b \pmod{m}$ se, e somente se, a e b possuem o mesmo resto na divisão por m.*

Demonstração: Pelo Algoritmo da Divisão, Teorema 2.2, existem q_1, q_2, r_1, r_2, inteiros com $0 \leq r_1, r_2 < m$, tais que $a = q_1 m + r_1$ e $b = q_2 m + r_2$. Logo, $a - b = m(q_1 - q_2) + (r_1 - r_2)$ e $(a - b) - m(q_1 - q_2) = (r_1 - r_2)$.

Se $a \equiv b \pmod{m}$, temos que $m \mid (a - b)$ e $m \mid m(q_1 - q_2)$. Portanto, pela Proposição 2.1, $m \mid (a - b) - m(q_1 - q_2)$, ou seja, $m \mid (r_1 - r_2)$. Agora note que $|r_1 - r_2| < m$. Contudo isso só é possível se $r_1 = r_2$.

Reciprocamente, se a e b possuem o mesmo resto na divisão por m, pelo Teorema 2.2 existem inteiros r, q_1, q_2 tais que $a = mq_1 + r$ e $b = mq_2 + r$. Logo, $a - b = m(q_1 - q_2)$. Como $m \mid m(q_1 - q_2)$, segue que $m \mid (a - b)$ e, pela Definição 2.4, que $a \equiv b \pmod{m}$. ■

Exemplo 2.3 *Como $21 = 2.10 + 1$ e $13 = 2.6 + 1$, temos que $21 \equiv 13 \pmod{2}$ pois o resto da divisão de 21 e de 13 por 2 são iguais a 1.*

A relação $\pmod{m}$ é uma relação de equivalência, ou seja, é reflexiva, simétrica e transitiva (veja a Proposição 2.3).

Proposição 2.3 *Sejam a, b, c e m números inteiros com $m > 0$. Então:*

1. *$a \equiv a \pmod{m}$;*
2. *Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;*
3. *Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.*

Demonstração:

1. Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \pmod{m}$.
2. Como $a \equiv b \pmod{m}$, pela Definição 2.4 temos que $m \mid a - b$. Segue pelo Teorema 2.1 que $m \mid -(a - b) = b - a$. Logo, $m \mid b - a$ e, portanto, $b \equiv a \pmod{m}$.
3. Como $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m \mid a - b$ e $m \mid b - c$. Segue da Proposição 2.1 que $m \mid [(a - b) + (b - c)]$. Logo $m \mid a - c$, o que implica $a \equiv c \pmod{m}$.

■

O teorema a seguir estabelece que a relação de equivalência é compatível com as operações de adição e multiplicação no conjunto dos números inteiros.

Teorema 2.3 *Se a, b, c, r, s e m são inteiros tais que $a \equiv b \pmod{m}$ e $r \equiv s \pmod{m}$, então:*

1. $a + c \equiv b + c \pmod{m}$;
2. $a - c \equiv b - c \pmod{m}$;
3. $ac \equiv bc \pmod{m}$;
4. $a + r \equiv b + s \pmod{m}$;
5. $ar \equiv bs \pmod{m}$.

Demonstração: Aplicando o Teorema 2.1 e a Definição 2.4, obtemos:

1. $a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid a - c + c - b \Rightarrow m \mid (a + c) - (b + c) \Rightarrow a + c \equiv b + c \pmod{m}$;
2. $a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - c) - (b - c) \Rightarrow a - c \equiv b - c \pmod{m}$;
3. $a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - b)c \Rightarrow m \mid ac - bc \Rightarrow ac \equiv bc \pmod{m}$;
4. $a \equiv b \pmod{m}$ e $r \equiv s \pmod{m} \Rightarrow m \mid a - b$ e $m \mid r - s \Rightarrow m \mid (a - b) + (r - s) \Rightarrow m \mid (a + r) - (b + s) \Rightarrow a + r \equiv b + s \pmod{m}$;
5. $a \equiv b \pmod{m}$ e $r \equiv s \pmod{m} \Rightarrow m \mid a - b$ e $m \mid r - s \Rightarrow m \mid r(a - b) + b(r - s) \Rightarrow m \mid ar - bs \Rightarrow ar \equiv bs \pmod{m}$.

■

Definição 2.5 *Sejam a e b inteiros, com $a \neq 0$ ou $b \neq 0$. O máximo divisor comum de a e b, denotado por $mdc(a, b)$, é o inteiro positivo d que satisfaz:*

1. *$d \mid a$ e $d \mid b$;*
2. *Se existe um inteiro c tal que $c \mid a$ e $c \mid b$, então $c \leq d$.*

Exemplo 2.4 *Observe que $mdc(4, 14) = 2$ pois os divisores de 4 são $\{\pm 1, \pm 2, \pm 4\}$ e 4 não divide 14.*

Proposição 2.4 *Sejam a, b e c números inteiros não nulos. Se $c \mid ab$ e $mdc(b, c) = 1$ então $c \mid a$.*

Demonstração: Sejam $m, n \in \mathbb{Z}$ tais que $mb + nc = 1$. Multiplicando ambos os membros dessa igualdade por a, obtemos $(ab)m + c(an) = a$. Como $c \mid (ab)$, segue da Proposição 2.1 que $c \mid a$. ■

3 Sistemas de identificação modular

Frequentemente utilizamos um número para identificar rapidamente um artigo, uma propriedade, um livro ou uma pessoa. Estes números de identificação podem armazenar uma grande quantidade de dados e informações. Sua utilização é observada no Registro de Identidade (RG), no Cadastro de Pessoa Física (CPF), no Código de Endereçamento Postal (CEP), na identificação de livros (ISBN), no código de barras, na conta bancária e em várias outras situações. Estes números de identificação são, em geral, formados de algarismos (códigos numéricos) ou de letras e algarismos (códigos alfanuméricos).

Para se detectar e evitar fraudes e possíveis erros de transmissão, digitação ou leitura, a maioria dos sistemas de identificação utiliza alguma informação redundante transmitida em simultâneo com o código que se pretende comunicar. Esta informação adicional ou redundância é chamada de dígito verificador, algarismo de controle ou ainda algarismo de teste. Na maioria dos sistemas de identificação o dígito verificador é o ultimo dígito da sequência e seu valor é calculado utilizando Aritmética Modular. Por esse motivo, estes sistemas são conhecidos como sistemas de identificação modular.

A utilização de dígitos verificadores não permite a correção automática do erro. Contudo, permite que o sistema alerte o operador sobre a ocorrência do mesmo. E, consequentemente, da necessidade de reescrever o número.

Os erros cometidos ao digitar um número foram sistematicamente investigados por autores como Beckley e Verhoeff, citados em [4, 5, 6]. Estas pesquisas revelam que cerca de 79% dos erros ocorrem com a digitação equivocada de um único dígito, como, por exemplo, digitar 1.573, quando o correto seria 1.673. Este tipo de erro recebe o nome de erro singular. Os chamados erros de transposição, cerca de 11% dos erros de digitação, são divididos em dois casos: os erros de transposição adjacente e os erros de transposição intercalada. O primeiro tipo corresponde à troca de posição de dois dígitos diferentes situados lado a lado, enquanto o segundo corresponde à troca de posição de dois dígitos diferentes intercalada por um terceiro dígito. Por exemplo, escrever 3.876, quando o correto seria 3.786 configura um erro de transposição adjacente, enquanto escrever o número 3.687 representa um erro de transposição intercalada. Os demais 9,9% dos erros estão distribuídos em diversas categorias, nenhuma delas representando mais de 1% do total. Estes estudos também nos dizem que a incidência de mais de um erro ao digitar um número é muito pouco provável.

Assim, os erros que serão considerados neste texto, singular e de transposição, cobrem mais de 90% dos erros possivelmente cometidos pelo homem, como observamos na Tabela 1, que citamos abreviando tabela publicada em [4, 5, 6].

Tabela 1. *Tipos de erros*

Tipo de erro		**Frequêcia relativa**
erro singular	$\cdots a \cdots \to \cdots b \cdots$	79,1%
erro de transposição adjacente	$\cdots ab \cdots \to \cdots ba \cdots$	10,2%
erro de transposição intercalada	$\cdots acb \cdots \to \cdots bca \cdots$	0,8%
outros erros	–	9,9%
Total		100%

É necessário esclarecermos que existem especificidades em cada sistema de códigos ou até mesmo em cada idioma que podem mudar significativamente a distribuição de probabilidades da Tabela 1.

Nos sistemas que utilizam a aritmética modular um número de identificação é da forma

$$x_1x_2x_3\ldots x_nC,$$

onde C é o algarismo de controle ou dígito verificador. O valor de C é determinado pela congruência

$$p_1x_1 + p_2x_2 + \cdots + p_nx_n + C \equiv 0 \pmod{k},$$

onde os elementos $\{p_1, p_2, \cdots, p_n\}$ são previamente escolhidos e denominados pesos.

Os sistemas deste tipo são chamados de *sistema módulo k* e a soma $p_1x_1 + p_2x_2 + \cdots + p_nx_n + C$, por soma controle ou soma teste, que iremos designar por S.

Usualmente é utilizado o zero nesta congruência, embora qualquer outro valor inteiro entre 0 e $k-1$ possa ser empregado. Essa escolha se deve à vantagem de que, se $S \equiv 0 \pmod{k}$, temos que $k \mid S$, ou seja, a soma teste é um múltiplo de k.

Analisemos a situação a seguir para melhor compreensão da estrutura de um sistema modular.

Exemplo 3.1 *Uma empresa utiliza três dígitos, $x_1x_2x_3$, para identificar cada produto que vende. Para ter certeza de que estes números serão corretamente transmitidos, ela acrescenta um quarto dígito (o algarismo de controle) em cada número, criando o código de identificação $x_1x_2x_3C$. O dígito de controle C é a solução da equação $3x_1 + x_2 + 3x_3 + C \equiv 0 \pmod{10}$, ou seja, a empresa utiliza um sistema módulo 10 com pesos $\{3, 1, 3\}$.*

Assim, para o produto identificado pelo número 854, $C = 9$, pois C é escolhido para satisfazer a seguinte congruência:

$$\begin{aligned} 3 \cdot 8 + 1 \cdot 5 + 3 \cdot 4 + C &\equiv 0 \pmod{10}; \\ 24 + 5 + 12 + C &\equiv 0 \pmod{10}; \\ 41 + C &\equiv 0 \pmod{10}. \end{aligned}$$

O dígito 9 foi escolhido como dígito de controle porque $41 + 9 = 50$ e $50 \equiv 0 \pmod{10}$. Portanto, o código de identificação desse produto é 8549. Já o número 7632 é um código inválido, uma vez que $3 \cdot 7 + 1 \cdot 6 + 3 \cdot 3 + 2 = 38$ e $38 \not\equiv 0 \pmod{10}$.

Os teoremas a seguir estabelecem as condições para que sistemas de identificação modular detectem os erros singulares e de transposição.

Teorema 3.1 *Um sistema de identificação módulo k, com pesos $\{p_1, p_2, \ldots, p_n\}$, detecta todo erro singular $a_i \to a_i'$, na $i-$ésima posição, se, e somente se, $mdc\,(p_i, k) = 1$.*

Demonstração: Considere um número $a_1a_2a_3\cdots a_n$ de um sistema de identificação módulo k, cujo dígito de verificação é a_n e a soma teste é S. Sabe-se que $S \equiv 0 \pmod{k}$. Designaremos por S' a soma teste com a troca $a_i \to a_i'$ na $i-$ésima posição. Neste caso, $a_i \neq a_i'$. Apesar do erro cometido é possível termos $S' \equiv 0 \pmod{k}$ e assim não podemos detectar o erro. Caso contrário, $S' \not\equiv 0 \pmod{k}$, podemos detectar o erro.

Contudo se considerarmos a diferença

$$\begin{aligned} S' - S &= (p_1a_1 + p_2a_2 + \cdots + p_ia_i' + \cdots + p_na_n) - (p_1a_1 + p_2a_2 + \cdots + p_ia_i + \cdots + p_na_n) \\ &= p_ia_i' - p_ia_i \\ &= p_i(a_i' - a_i), \end{aligned}$$

observamos que um erro singular $a_i \to a_i'$, na $i-$ésima posição, é detectável se, e somente se, $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$. É fácil ver que $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$ se, e somente se, $mdc\,(p_i, k) = 1$. De fato, suponha que $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$ e $mdc\,(p_i, k) = d > 1$. Então $p_i = dd_1$ e $k = dd_2$, com $d_2 \in \{0, 1, 2, \cdots, k-1\}$. Agora observe que para $a_i' = d_2$ e $a_i = 0$ obtemos

$$p_i a_i' = pd_2 = dd_1 d_2 = d_1 dd_2 = d_1 k \equiv 0 \pmod{k}$$

e assim $p(a_i' - a_i) \equiv 0 \pmod{k}$. Absurdo! Portanto, $d = 1$. Por outro lado, suponha que $mdc\,(p_i, k) = 1$ e $p(a_i' - a_i) \equiv 0 \pmod{k}$. Então $k \mid p_i(a_i' - a_i)$ e segue da Proposição 2.4 que $k \mid (a_i' - a_i)$. Temos novamente um absurdo, pois $(a_i' - a_i) \in \{0, 1, 2, \cdots, k-1\}$. Verificando nossa afirmação. Portanto, um erro singular $a_i \to a_i'$, na $i-$ésima posição, é detectável se, e somente se, $mdc\,(p_i, k) = 1$. ■

Teorema 3.2 *Um sistema de identificação módulo k, com pesos $\{p_1, p_2, ..., p_n\}$, detecta todos os erros de transposição dos algarismos a_i e a_j nas posições i e j se, e somente se, $mdc\,(p_i - p_j, k) = 1$.*

Demonstração: Neste caso, a diferença entre a soma teste do número errado e a soma teste correta é

$$\begin{aligned} S' - S &= (p_1a_1 + \cdots + p_ia_j + \cdots + p_ja_i + \cdots + p_na_n) - (p_1a_1 + \cdots + p_ia_i + \cdots + p_ja_j + \cdots + p_na_n) \\ &= p_ia_j + p_ja_i - p_ia_i - p_ja_j \\ &= p_i(a_j - a_i) + p_j(a_j - a_i) \\ &= (p_i - p_j)(a_j - a_i). \end{aligned}$$

Portanto, o sistema detecta todas as transposições de algarismos nas posições i e j se para quaisquer $a_i, a_j \in \{0, 1, 2, ..., k-1\}$ com $a_i \neq a_j$, temos $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$. De modo análogo à demonstração do teorema anterior, esta condição é equivalente a $mdc\,(p_i - p_j, k) = 1$. ■

Estes resultados justificam uma maior utilização de sistemas módulo 11, pela facilidade de encontrar pesos primos com 11, usando apenas um carácter para o algarismo de controle. Este método, porém, tem uma pequena desvantagem, no conjunto dos dígitos de 0 a 9, não há nenhum que represente o número 10, sendo necessário incluir mais um símbolo para representar este número. Em geral, utilizamos o algarismo romano X, sendo este método denominado módulo 11 completo. Outra possibilidade é o esquema módulo 11 restrito, que utiliza o dígito 0 para representar o algarismo 10.

No caso $k = 10$, as condições dos Teoremas 3.1 e 3.2 são incompatíveis: é impossível satisfazer o segundo se o primeiro for verificado pois, nesse caso, os pesos são necessariamente ímpares e temos que a diferença entre dois números ímpares é um número par. Portanto, qualquer sistema módulo 10 que tenha 100% de eficiência na detecção dos erros singulares não detectará todos os erros de transposição.

É necessário destacarmos a importância dos Teoremas 3.1 e 3.2 como mecanismos para a construção de novos sistemas modulares.

4 Número do CPF

O Cadastro de Pessoas Físicas, mais conhecido como CPF, é o registro de um cidadão na Receita Federal brasileira. Neste registro devem estar todos os contribuintes (pessoas

físicas brasileiras ou estrangeiras com negócios no Brasil). O CPF armazena informações fornecidas pelo próprio contribuinte e por outros sistemas da Receita Federal. Sua posse não é obrigatória, mas é necessária em várias situações, como abertura de contas em bancos e emissão de passaporte, por exemplo.

O número de um CPF tem nove dígitos de identificação e mais dois dígitos verificadores que são indicados por último. Portanto, um CPF tem onze algarismos.

O dígito anterior aos dígitos verificadores (isto é, o terceiro dígito da direita para a esquerda) identifica a unidade federativa em que a pessoa registrou-se pela primeira vez. Por exemplo, a origem do CPF 043.658.306-27 é Minas Gerais, cujo código é "6". Segue a lista com o número que identifica cada um dos estados brasileiros:

0. Rio Grande do Sul.
1. Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul e Tocantins;
2. Amazonas, Pará, Roraima, Amapá Acre e Rondônia;
3. Ceará, Maranhão e Piauí;
4. Paraíba, Pernambuco, Alagoas e Rio Grande do Norte;
5. Bahia e Sergipe;
6. Minas Gerais;
7. Rio de Janeiro e Espírito Santo;
8. São Paulo;
9. Paraná e Santa Catarina.

Seja $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}$ um número de CPF, onde x_i representa um dígito de identificação para $1 \leq i \leq 9$ e x_{10} e x_{11} são os dígitos de controle. O algoritmo abaixo, adaptado de [7], permite calcular os dígitos de controle.

$$x_{10} = \left(\sum_{i=1}^{9} ix_i \pmod{11} \right) \pmod{10};$$
$$x_{11} = \left(\sum_{i=2}^{10} (i-1)x_i \pmod{11} \right) \pmod{10}.$$

Com a finalidade de ilustrar a aplicação do algoritmo, vamos verificar a autenticidade do CPF $043.658.306 - 27$ calculando os dígitos de controle x_{10} e x_{11}.

Fazendo as devidas substituições obtemos a seguinte expressão para x_{10}:

$x_{10} = ((1.\mathbf{0} + 2.\mathbf{4} + 3.\mathbf{3} + 4.\mathbf{6} + 5.\mathbf{5} + 6.\mathbf{8} + 7.\mathbf{3} + 8.\mathbf{0} + 9.\mathbf{6}) \pmod{11}) \pmod{10};$
$x_{10} = ((0 + 8 + 9 + 24 + 25 + 48 + 21 + 0 + 54) \pmod{11}) \pmod{10};$
$x_{10} = ((189 \pmod{11})) \pmod{10};$
$x_{10} = 2 \pmod{10};$
$x_{10} = 2.$

O resultado confirma o valor do primeiro dígito verificador. Calculemos agora o segundo dígito, x_{11}:

$x_{11} = ((1.\mathbf{4} + 2.\mathbf{3} + 3.\mathbf{6} + 4.\mathbf{5} + 5.\mathbf{8} + 6.\mathbf{3} + 7.\mathbf{0} + 8.\mathbf{6} + 9.\mathbf{2}) \pmod{11}) \pmod{10};$
$x_{11} = ((4 + 6 + 18 + 20 + 40 + 18 + 0 + 48 + 18) \pmod{11}) \pmod{10};$
$x_{11} = ((172 \pmod{11})) \pmod{10};$
$x_{11} = 7 \pmod{10};$

$x_{11} = 7$.

Os cálculos confirmam o valor do segundo dígito de controle. Assim, concluímos que o CPF $043.658.306 - 27$ é autêntico.

É importante ressaltar que o fato de um número de CPF ser autenticado pelos seus dígitos verificadores não o torna um CPF válido. Para isso, é necessário que ele esteja cadastrado no banco de dados da Receita Federal. Assim, um número correto de CPF nem sempre será um documento já emitido. É o que acontece, por exemplo, com números de CPF que têm todos os dígitos iguais: apesar de serem autenticados pelos seus dígitos verificadores, eles não são válidos.

O sistema que utiliza dois dígitos verificadores melhora o método módulo 11 restrito. Porém, poderia ter uma maior capacidade de detecção de erros caso a escolha dos pesos fosse feita de forma mais criteriosa. Mesmo assim, a falha na detecção de erros é de apenas 0,22% nos casos de erro singular e de 0,17% nos erros de transposição. A demonstração destes resultados pode ser encontrada em [7], ANEXO A.

Um fato interessante é a implementação no Brasil do Registro de Identidade Civil (RIC). Ele será um cartão com chip que conterá os números de RG, CPF, Título de Eleitor, PIS (Programa de Integração Social), PASEP (Programa de Formação do Patrimônio do Servidor Público), Carteira de Trabalho e Carteira Nacional de Habilitação. Nele constará ainda um campo com informações como o tipo sanguíneo e se a pessoa é ou não doadora de órgãos. O identificador será um número de onze dígitos, sendo o último um dígito verificador que é calculado empregando o sistema módulo 11 restrito e os seguintes pesos $\{9, 8, 7, 6, 5, 4, 3, 2, 9, 8\}$.

5 Código ISBN

O ISBN - International Standard Book Number - é um dos sistemas de identificação mais antigos, criado em 1967 e oficializado como norma internacional em 1972. Ele identifica numericamente os livros segundo o título, o autor, o país e a editora, individualizando inclusive edições diferentes.

O sistema é controlado pela Agência Internacional do ISBN, que orienta e delega poderes às agências nacionais. No Brasil, a Fundação Biblioteca Nacional representa a Agência Brasileira desde 1978, com a função de atribuir o número de identificação aos livros editados no país.

Inicialmente o ISBN era composto por dez dígitos, $x_1x_2x_3x_4x_5x_6x_7x_8x_9C$, onde os nove primeiros identificavam o livro e o décimo era o dígito verificador. Segundo [6], este sistema, que indicaremos por ISBN-10, utiliza os pesos $\{10, 9, 8, 7, 6, 5, 4, 3, 2, 1\}$ e uma congruência módulo 11.

Assim, o cálculo do dígito verificador do ISBN-10 era efetuado da seguinte forma:

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + C \equiv 0 \pmod{11}.$$

Se o valor C necessário para satisfazer esta condição fosse 10, este seria substituído por um "X". Como no último romance de Eça de Queirós, *A Cidade e As Serras*, cujo ISBN-10 é o número 85-87328-14-X.

A partir de 1º de janeiro de 2007, o ISBN passou de dez para treze dígitos, sendo conhecido por ISBN-13, o que tornou possível o uso do código de barras denominado EAN

(European Article Number)[1]. O objetivo foi aumentar a capacidade do sistema, devido ao crescente número de publicações. A nova numeração foi precedida pelo número 978, que identifica o produto livro e o número de controle foi recalculado. Quando o "prefixo 978"se esgotar, será adotado o "prefixo 979".

O dígito de verificação de um ISBN-13 é de 1 dígito com valores entre 0 e 9, mostrado como um caractere final no término da sequência. Veja o exemplo de ISBN-13: $978-85-85818-25-8$, referente ao livro *Elementos de Aritmética* de Abramo Hefez. O primeiro elemento, 978, é especificado pela Agência Internacional do ISBN, em conformidade com o sistema global de numeração de produtos e indica a indústria, neste caso, publicação de livros. O segundo elemento identifica os grupos nacionais geográficos, sendo o número 85 o identificador do Brasil. O terceiro elemento refere-se ao editor, nesse caso a Sociedade Brasileira de Matemática (SBM). O quarto elemento é um elemento de publicação, destinado para o editor da publicação, que etiquetou o livro com o número 25. Por fim, o quinto elemento corresponde ao dígito verificador.

Os diferentes componentes do ISBN-13 (indústria, país, editor e título) possuem quantidade variada de dígitos. Esta variação permite que os idiomas mais utilizados e que as grandes editoras tenham um número de identificação menor, possibilitando catalogar um maior número de livros.

O ISBN-13 utiliza os pesos $\{1,3,1,3,1,3,1,3,1,3,1,3,1\}$ e $k=10$. Logo, determinaremos o dígito verificador deste sistema resolvendo a equação abaixo, adaptada de [8]:

$$x_1+3x_2+x_3+3x_4+x_5+3x_6+x_7+3x_8+x_9+3x_{10}+x_{11}+3x_{12}+C\equiv 0 \pmod{10},$$

onde x_i são os algarismos do código ISBN-13 na posição i e C o dígito de controle.

Por exemplo, o livro *O homem que calculava*, de Malba Tahan, tem como ISBN-13 o número 978-85-0106-196-6. O dígito de verificação é 6 porque

$$S=\mathbf{9}+3.\mathbf{7}+\mathbf{8}+3.\mathbf{8}+\mathbf{5}+3.\mathbf{0}+\mathbf{1}+3.\mathbf{0}+\mathbf{6}+3.\mathbf{1}+\mathbf{9}+3.\mathbf{6}+\mathbf{6},$$
$$S=9+21+8+24+5+0+1+0+6+3+9+18+6=110\equiv 0 \pmod{10}.$$

Teorema 5.1 *O sistema ISBN-13 detecta todo erro singular.*

Demonstração: Como os pesos do sistema $ISBN-13$ são $\{1,3,1,3,1,3,1,3,1,3,1,3,1\}$, $mdc\,(1,10)=1$ e $mdc\,(3,10)=1$, segue do Teorema 3.1 que esse sistema detecta todo erro singular. ■

Portanto, este sistema tem uma eficiência de 100% na detecção de erros singulares.

Teorema 5.2 *O sistema ISBN-13 não detecta todos os erros de transposição adjacente.*

Demonstração: Segue do Teorema 3.2, uma vez que $mdc\,(2,10)=2>1$. ■

Exemplo 5.1 *Se $a_9=6$ e $a_8=1$ forem trocados teríamos $S'-S=2(a_9-a_8)=2.5=10$ e o erro não seria detectado.*

[1]O sistema EAN (European Article Number) adotado na Europa em 1976 é análogo ao sistema UPC (Universal Product Code), o primeiro código de barras, criado nos E.U.A. em 1973. Esse código de 13 dígitos é atualmente utilizado no mundo inteiro principalmente para a identificação de itens do varejo.

Verificamos que as trocas de algarismos adjacentes $\ldots a_i a_{i+1} \ldots \rightarrow \ldots a_{i+1} a_i \ldots$ que este sistema não detecta são aquelas em que $\mid a_{i+1} - a_i \mid = 5$. Com efeito, supondo i par, temos que a diferença entre a soma teste do número errado e a soma teste correta é dada por:

$$S' - S = (a_1 + \cdots + 3a_{i+1} + a_i + \cdots + C) - (a_1 + \cdots + 3a_i + a_{i+1} + \cdots + C) = 2(a_{i+1} - a_i).$$

No caso em que i é ímpar, tem-se a diferença com o sinal trocado, $2(-a_{i+1} + a_i)$. Segue que

$$10 \mid S' \Leftrightarrow 10 \mid (S' - S) \Leftrightarrow 10 \mid 2(a_{i+1} - a_i) \Leftrightarrow \mid a_{i+1} - a_i \mid = 5.$$

Logo, o sitema ISBN-13 não detecta os seguintes casos de transposição adjacente: “05", “50"; “16", “61"; “27", “72"; “38", “83"; “49"e “94", o que corresponde a 10 dos 90 casos possíveis. Este sistema tem assim uma eficiência de 88,9% na detecção deste tipo de erro. Mas esse é um problema sem relevância prática, uma vez que leitores ópticos são muito precisos e, quando muito, cometem erros singulares.

6 Número do cartão de crédito

Os principais números de cartões de crédito no Brasil possuem uma sequência de 16 dígitos: os 6 primeiros dígitos definem a instituição emissora, sendo que o primeiro desses seis dígitos caracteriza a bandeira do cartão, por exemplo, 4 - Visa e 5 - Mastercard; os nove dígitos que seguem identificam o cliente; o último dígito, na extremidade direita, representa o dígito verificador.

Esse dígito é utilizado para decidir se um cartão de crédito é válido e pode ser calculado por uma fórmula chamada *Algoritmo de Luhn*. Segundo [9], esta fórmula foi assim nomeada em homenagem ao cientista Hans Peter Luhn (1896-1964), um engenheiro da IBM (International Business Machines), que recebeu em 1960 a patente dos Estados Unidos por inventar a técnica. Atualmente, o algoritmo é de domínio público, conhecido como Módulo 10 IBM, sendo largamente utilizado por bancos e demais entidades financeiras para validar o número dos cartões de crédito e de débito.

Constatamos a autenticidade de um cartão resolvendo a equação que segue, adaptada de [7, 9]: $\overline{2x_1}+x_2+\overline{2x_3}+x_4+\overline{2x_5}+x_6+\overline{2x_7}+x_8+\overline{2x_9}+x_{10}+\overline{2x_{11}}+x_{12}+\overline{2x_{13}}+x_{14}+\overline{2x_{15}}+C \equiv 0 \pmod{10}$, onde x_i é o algarismos do número do cartão na posição i e C o algarismo de controle. Temos ainda que:

$$\overline{2x_i} = \begin{cases} 2x_i, & \text{se} \quad 2x_i < 10, \\ 2x_i - 9, & \text{se} \quad 2x_i \geq 10. \end{cases}$$

Portanto, após os algarismos do identificador serem multiplicados pelos pesos 2 e 1 alternadamente, em cada produto, subtrai-se 9 quando este é maior ou igual a 10 e escolhe-se o algarismo de controle C de forma a que a soma teste seja um múltiplo de 10.

Esse sistema, com um único dígito de verificação, detecta erros típicos que as pessoas cometem quando transcrevem números de cartão, por exemplo, em compras via internet.

Para ilustrar esta situação, suponha que ao digitar o número 4073038870480971 de um cartão de crédito, tenha se cometido um erro, e que o número de fato digitado fosse 4072038870480971. Ao fazer a verificação de leitura, o computador que recebeu a infor-

mação faz as seguintes operações:

$$\begin{aligned} S &= 2.\mathbf{4} + \mathbf{0} + 2.\mathbf{7} + \mathbf{2} + 2.\mathbf{0} + \mathbf{3} + 2.\mathbf{8} + \mathbf{8} + 2.\mathbf{7} + \mathbf{0} + 2.\mathbf{4} + \mathbf{8} + 2.\mathbf{0} + \mathbf{9} + 2.\mathbf{7} + \mathbf{1} \\ &= 8 + 0 + 14 + 2 + 0 + 3 + 16 + 8 + 14 + 0 + 8 + 8 + 0 + 9 + 14 + 1 \\ &= 8 + 0 + (14 - 9) + 2 + 0 + 3 + (16 - 9) + 8 + (14 - 9) + 0 + 8 + 8 + 0 + 9 + (14 - 9) + 1 \\ &= 8 + 0 + 5 + 2 + 0 + 3 + 7 + 8 + 5 + 0 + 8 + 8 + 0 + 9 + 5 + 1 \\ &= 69. \end{aligned}$$

Como o resultado obtido não é um múltiplo de 10, o computador avisa que foi cometido algum erro e o número deve ser novamente digitado.

Teorema 6.1 *O Algoritmo de Luhn ou Módulo 10 IBM detecta todo erro singular.*

Demonstração: Considere separadamente dois casos: o erro ocorre em um algarismo com índice par ou o erro ocorre em um algarismo de índice ímpar.

Nas posições de índice par, o peso é 1 e sendo $mdc\,(1, 10) = 1$, pelo Teorema 3.1, todos os erros singulares são detectados.

No caso de erro em um algarismo de índice ímpar, temos que $S' - S = \overline{2a_i'} - \overline{2a_i}$, onde S' é a soma teste de um número com um erro singular e S é a soma teste de um número correto. Mas observe que $\overline{2a_i'}$ e $\overline{2a_i}$ são o resultado de uma das transformações a seguir.

$0 \to 0$	$5 \to 10 \to 1$
$1 \to 2$	$6 \to 12 \to 3$
$2 \to 4$	$7 \to 14 \to 5$
$3 \to 6$	$8 \to 16 \to 7$
$4 \to 8$	$9 \to 18 \to 9$

Se S' fosse múltiplo de 10, teríamos que $10 \mid (S' - S)$. Logo, 10 dividiria $(\overline{2a_i'} - \overline{2a_i})$, o que é um absurdo, pois $(\overline{2a_i'} - \overline{2a_i})$ é um número inteiro não nulo entre -9 e 9. ■

Portanto, o Algoritmo de Luhn detecta todo erro singular. Ele também detecta todas as transposições de algarismos adjacentes, com exceção dos casos "09"e "90", ou seja, detecta 88 casos em 90. Dessa forma, o Algoritmo de Luhn possui uma taxa de detecção de transposições adjacentes de 97,8%, melhor do que os 88,9% observado no sistema ISBN. Uma exposição mais detalhada sobre os erros de transposição pode ser encontrada em [7].

Mas o dígito verificador não é o bastante para garantir a segurança no uso de cartões de crédito, por isso ainda há um código de três dígitos que fica atrás do cartão. Esse código é gerado pela própria instituição e calculado ao criptografar o número do cartão e sua data de validade. Cada empresa decide qual algoritmo usar nessa criptografia e a chave de decodificação não é pública.

7 Proposta didática

Nesta seção, propomos uma sequência didática para trabalhar com os estudantes do Ensino Fundamental o tema identificadores de erros, utilizando os blocos lógicos como recurso didático. Esperamos com o desenvolvimento desta proposta que os alunos, realizando apenas operações aritméticas, compreendam a tecnologia dos códigos identificadores de erros.

Os blocos lógicos foram criados na década de 50 pelo matemático húngaro Zoltan Paul Dienes. Segundo [10], o modelo mais utilizado nas escolas brasileiras tem 48 peças geométricas, divididas em:

1. Quatro formas: círculos, quadrados, triângulos e retângulos;
2. Três cores: amarelo, azul e vermelho;
3. Dois tamanhos: grande e pequeno;
4. Duas espessuras: fino e grosso.

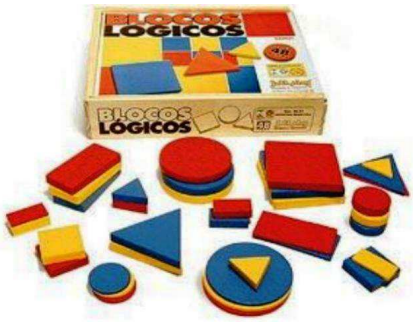


Figura 1. Blocos Lógicos

Assim, cada peça possui quatro atributos. Por exemplo, podemos ter um círculo, vermelho, grande e fino. O objetivo da sequência é propor atividades que estimulem os estudantes a determinar um código que identifique cada peça e a transmitir uma lista de peças utilizando o código construído por eles. Esta atividade permitirá que os alunos percebam como identificar um artigo por uma sequência numérica agiliza a transmissão de informações e a importância do dígito verificador para identificação de possíveis erros durante a transmissão, digitação ou leitura de dados.

Para o desenvolvimento dessa proposta, sugerimos a organização da turma em grupos de trabalho heterogêneos, compostos de 4 a 5 alunos em diferentes níveis de aprendizagem. Orientamos iniciar a discussão com uma conversa informal sobre códigos e números de identificação. É interessante preparar uma pequena exposição de embalagens com códigos de barras, documentos pessoais, cartões bancários, folhas de cheque, livros, entre outros objetos que possuam número de identificação.

Após esse primeiro momento, os grupos deverão iniciar a exploração livre dos blocos lógicos. É importante que o professor faça perguntas que oportunize aos alunos discutir sobre as características das peças e agrupar as peças considerando diferentes critérios. Nesta etapa, não se espera que os estudantes demonstrem dificuldades, embora seja interessante que o professor represente no quadro alguns dos esquemas, tabelas ou desenhos utilizados pelos grupos como forma de registro.

Logo após a exploração do material, o professor deverá apresentar a proposta de atividade para a turma. A tarefa será estabelecer um código que identificará cada uma das peças e transmitir para outro grupo uma mensagem contendo uma lista com o código de pelo menos 10 peças. Esperamos que o professor incentive a turma a discutir sobre as diferentes possibilidades de solucionar a situação proposta e a perceber a importância de estabelecer um código padrão.

A seguir, apresentamos na Figura 2 uma possibilidade de associação entre um algarismo e uma característica das peças.

Ressaltamos que diferentes códigos podem ser elaborados pelo professor, ou pelos alunos, para identificação dos blocos lógicos nessa proposta de trabalho. Sugerimos uma sequência

FORMA	ALGARISMO
Círculo	1
Quadrado	2
Triângulo	3
Retângulo	4

COR	ALGARISMO
Amarelo	1
Azul	2
Vermelho	3

TAMANHO	ALGARISMO
Grande	1
Pequeno	2

ESPESSURA	ALGARISMO
Fino	1
Grosso	2

Figura 2. Sugestão de algarismo por característica da peça

de 5 algarismos, onde o 1º algarismo identifica a forma, o 2º a cor, o 3º o tamanho, o 4º a espessura e o 5º é o dígito verificador calculado a partir dos anteriores. Para determinar o algarismo de controle C, do código $x_1x_2x_3x_4 - C$, basta calcular o resto da divisão por 5 da soma $x_1 + 2x_2 + 3x_3 + 4x_4$. Este é um sistema módulo 5 com pesos $\{1, 2, 3, 4\}$. Assim, por exemplo, um círculo, vermelho, grande e fino será identificado pelo código $1311 - 4$. Oserve que $mdc\,(p_i, 5) = 1$ para $i = \{1, 2, 3, 4\}$, verificando a condição do Teorema 3.1 para detecção de erro singular. Como $mdc\,(p_i - p_j, 5) = 1$ para $i, j \in \{1, 2, 3, 4\}$, a condição do Teorema 3.2 para detecção de erros de transposição é verificada. Portanto, a escolha por este modelo não é aleatória uma vez que ele detecta todos os casos de erro singular e de transposição.

Retomando a atividade, é possível que mesmo o professor apresentando a relação estabelecida na Figura 2, os grupos respondam a questão com diferentes códigos, pois podem estabelecer ordens distintas para os atributos das peças. Por exemplo, um grupo pode estabelecer que o 1º algarismo identifique a forma, o 2º a cor, o 3º o tamanho, o 4º a espessura e um outro grupo pode identificar as peças segundo o critério espessura, cor, forma e tamanho. O professor deverá explorar essa situação, pedindo aos grupos que digam alguns códigos e que os outros grupos tentem descobrir qual é a peça associada a esse código. É importante que os alunos percebam a necessidade de se estabelecer um padrão e elaborem um código único para identificação das peças. Por exemplo:

$$1^o\ algarismo \to forma;$$
$$2^o\ algarismo \to cor;$$
$$3^o\ algarismo \to tamanho;$$
$$4^o\ algarismo \to espessura.$$

Antes dos alunos iniciarem o processo de etiquetar as peças dos blocos lógicos, o professor verificará se todos os grupos compreenderam o padrão estabelecido pela turma. Neste momento é interessante fixar um cartaz ou anotar no quadro o código definido pela turma e que deverá ser utilizado por todos os grupos. Esperamos que os alunos percebam que identificar numericamente as peças simplifica e agiliza a transmissão de informações.

Após cada grupo etiquetar, transmitir e receber uma lista com pelo menos dez códigos, iniciasse a etapa de decodificar e conferir os dados recebidos com os emissores. O professor deverá motivar o debate sobre segurança na transmissão de informações e erros na leitura, escrita e transmissão de dados, sendo propício novas questões para discussão, tais como: Quais foram os erros cometidos na transmissão das listas? Há erros comuns aos grupos? Há formas de evitar ou minimizar essas falhas?

É importante ressaltar que os alunos, individualmente ou em grupo, devem ser orientados a sistematizar e registrar as observações, os questionamentos e as conclusões que forem surgindo durante o trabalho.

Após a discussão sobre os erros cometidos na transmissão e recepção de dados, o professor apresentará a teoria dos dígitos verificadores. Conceitos como erro singular e de transposição devem ser formalizados. Em sua exposição, o professor ressaltará a simplicidade dessa teoria, suas inúmeras aplicações no dia a dia e a eficiência na detecção de erros. A situação proposta no Exemplo 3.1 ou o Código de Barras (Sistema EAN-13) pode ser utilizado para ilustrar o uso do dígito verificador e seu cálculo.

Retomando o trabalho com os blocos lógicos e o código de identificação elaborado pela turma, chegamos ao momento em que surge o grande desafio da proposta: elaborar uma fórmula para determinar o dígito verificador do código criado para identificação dos blocos lógicos. O professor deve levantar algumas questões: A fórmula elaborada pela turma estabelece uma relação com os primeiros algarismos? É eficiente na detecção de erros? Quais as limitações do sistema elaborado pelo seu grupo?

Neste ponto, pressupomos que os alunos se apropriaram do sentido do problema, estejam motivados a buscar uma solução para essas questões e a fazer novas perguntas. Assim, várias estratégias e ideias informais podem surgir durante a discussão e precisam ser valorizadas pelo professor. A realização de simulações para verificar a eficiência do dígito verificador construído pelos grupos deve ser reconhecida e estimulada.

Recomendamos que o professor solicite o registro dos processos gerais utilizados na elaboração da fórmula para o cálculo do dígito verificador. E também, estimule as justificativas, pedindo aos alunos que mostrem se os códigos criados são adequados do ponto de vista da detecção de erros. Neste ponto, os estudantes devem perceber que a utilização de números primos torna o sistema mais eficiente.

Em seguida o professor pode apresentar, ou construir coletivamente, uma fórmula única para o cálculo do dígito verificador para a turma. Uma sugestão de sistema módulo 5 com pesos $\{1, 2, 3, 4\}$ foi apresentada no início desta seção.

Neste momento é importante que o professor faça uma síntese dos conceitos trabalhados: algoritmo da divisão, resto da divisão, números primos, divisores e múltiplos de números naturais.

Para verificar se os estudantes compreenderam o algoritmo elaborado para o cálculo do 5^{o} algarismo, o professor pode escolher algumas peças e pedir que os alunos calculem o dígito verificador. Outra estratégia é escrever alguns códigos inválidos, ou faltando um dos dígitos, e solicitar que os alunos tentem encontrar o erro e em seguida corrigi-lo.

Para finalizar, indicamos a produção de um relatório descrevendo a prática, as conclusões e os conceitos matemáticos envolvidos. Pode ocorrer que os relatórios produzidos pelos estudantes sejam inicialmente pouco desenvolvidos, com respostas curtas e justificativas insuficientes ou não fundamentadas. Uma alternativa para sanar essa dificuldade é fornecer roteiros e indicar, durante a discussão nos grupos, pontos importantes a serem mencionados nos relatos.

8 Considerações finais

Neste trabalho abordamos as noções básicas de Teoria dos Números e sua aplicação no cálculo do dígito verificador de sistemas de identificação modular. Discutimos sobre a utilização dos números de identificação no cotidiano e os erros cometidos na leitura, escrita e transmissão destes números. Recorremos à Aritmética Modular para generalizar os siste-

mas de identificação estudados e destacamos a importância dos Teoremas 3.1 e 3.2 para a construção de novos sistemas modulares. Apresentamos três exemplos concretos de sistema de identificação em utilização no país: o CPF, o ISBN e o cartão de crédito. Situações concretas foram utilizadas para ilustrar a aplicação destes modelos e para uma melhor compreensão da estrutura de cada sistema. Uma proposta de aplicação da teoria dos códigos foi descrita para o trabalho com estudantes do Ensino Fundamental. A sequência didática recorreu à exploração dos blocos lógicos para criar um ambiente motivador e estimulador à aprendizagem.

Problemas relativos a correção de erros não foram discutidos neste texto. Acreditamos ser necessário a realização de estudos posteriores para melhor compreensão de métodos que possam além de detectar os erros, fazer sua correção automática: os chamados sistemas corretores de erros.

Professores de matemática, que atuam principalmente no Ensino Fundamental, poderão utilizar este trabalho como um instrumento para o desenvolvimento de aulas de aritmética. Para tanto, buscamos utilizar uma linguagem simples e objetiva, apresentando ao longo do texto exemplos e situações concretas que auxiliam o professor no planejamento de aulas.

Além disso, esperamos que a realização da prática em sala de aula contribua para o desenvolvimento dos alunos e fomente o interesse por projetos e atividades de investigação e exploração. Desejamos, também, ter cumprido o objetivo de motivar um estudo mais aprofundado sobre Aritmética Modular, mostrando como ideias e conceitos matemáticos levam ao desenvolvimento de tecnologias que visam o avanço e o bem estar social.

Enfim, acreditamos que este trabalho possa contribuir para que alunos e professores construam uma visão mais completa da verdadeira natureza da atividade matemática e percebam que o estudo de temas aparentemente abstratos como sistemas de identificação modular é uma oportunidade ímpar de aprendizagem, possibilitando momentos de reflexão, investigação e construção de conhecimento que, em geral, não observamos no dia-a-dia da sala de aula. Confiamos também, que, motivados por este, outros trabalhos possam ser elaborados apresentando aplicações da matemática afim de serem desenvolvidos na Educação Básica.

9 Agradecimentos

Agradecemos à Coordenação de Aperfeiçoamento Pessoal de Nível Superior (CAPES) pela concessão de bolsa de estudo durante todo o período de realização do curso, Mestrado Profissional em Matemática (PROFMAT), e pela histórica contribuição no desenvolvimento da educação e da ciência brasileira.

Referências

[1] HEFEZ, A. Elementos de Aritmética. 2. ed., SBM, Rio de Janeiro, 2011.

[2] NETO, A. C. M. Tópicos de Matemática Elementar: Teoria dos Números. Coleção do Professor de Matemática, v. 5, SBM, Rio de Janeiro, 2012.

[3] SANTOS, J. P. O. Introdução à Teoria dos Números. IMPA, Rio de Janeiro, 2012.

[4] MILIES, F. C. P. A matemática dos códigos de barras. *Revista do Professor de Matemática*, v. 65, p. 46-53, 2008.

[5] MILIES, F. C. P. A matemática dos códigos de barras: detectando erros. *Revista do Professor de Matemática*, v. 68, p. 38-42, 2009.

[6] PICADO, J. A álgebra dos sistemas de identificação: da artmética modular aos grupos diedrais. *Boletim da Sociedade Portuguesa de Matemática*, nº 44, 2011.

[7] SOUZA, N. P. Uma análise dos esquemas de dígitos verificadores usados no Brasil. Dissertação (Mestrado), UERJ, 2013.

[8] LOURENÇO, P. J. P. Aritmética Modular: aplicações nos sistemas de identificação. Faculdade de Ciências e Tecnologia da Universidade de Coimbra, Coimbra, 2011.

[9] KIRTLAND, J. Indefication Numbers and Check Digit Schemes. USA: The Mathematical Association of America, 2001.

[10] SIMONS, U. M. Blocos Lógicos. Vozes, Petrópolis, 2007.

Funções Exponenciais: Uma Contextualização Através de Aplicações Cotidianas

Exponential Functions: a Contextualization Through Everyday Applications

Igor Alvarenga da Silva Nascimento
Universidade Federal do Estado do Rio de Janeiro -UNIRIO
igor.ime@gmail.com

Mário César Martins de Lima
Universidade Federal do Estado do Rio de Janeiro -UNIRIO
marinholc1@gmail.com

Resumo: A didática que envolve o ensino de modelos exponenciais se reveste de um caráter muito puro, sem conexão com a realidade do discente. O artigo apresenta algumas aplicações que podem ser utilizadas no ensino de funções exponenciais no Ensino Médio, tornando a assimilação dos conteúdos por parte do aluno uma atividade prazerosa e relacionada ao seu cotidiano. Ainda, pretende-se deixar uma sugestão de abordagem do conteúdo por meio de uma sequência didática simples de aulas, otimizando e buscando a correta compreensão dos tópicos pelos jovens, bem como despertando o interesse pelo assunto.

Palavras-chave: funções exponenciais; aplicações; curiosidades; modelos.

Abstract: The didacticism that involves the teaching of exponential models is of a very pure character, without connection with the reality of the student. The article presents some applications that can be used in the teaching of exponential functions in High School, making the assimilation of contents by the student a pleasant activity and related to their daily life. Still, it is intended to leave a suggestion to approach the content through a simple didactic sequence of classes, optimizing and seeking the correct understanding of the topics by young people, as well as arousing interest in the subject.

Key words: exponential functions; applications; curiosities; models.

1 Introdução

A motivação para o estudo dos modelos exponenciais reside na aplicabilidade de inúmeros fenômenos que se pode observar. Diante da observação, percebeu-se que a forma como a matéria é ministrada nas escolas de Ensino Médio não apresenta uma recepção adequada pelos discentes. É tida como bastante abstrata e pura, fazendo com que o aluno, de forma geral, não perceba a importância do assunto para a sua formação como cidadão e para o seu futuro profissional.

Apesar da constatação dos métodos de ensino, os documentos educacionais já previam um ensino mais contextualizado, adequado às realidades do público-alvo. Corroborando, cita-se os Parâmetros Curriculares Nacionais (PCN) para o Ensino Médio [1], na área de Matemática:

Recebido em 30/09/2017 - Aceito em 30/10/2017

"A Matemática no Ensino Médio tem um valor formativo, que ajuda a estruturar o pensamento e o raciocínio dedutivo, porém também desempenha um papel instrumental, pois é uma ferramenta que serve para a vida cotidiana e para muitas tarefas específicas em quase todas as atividades humanas."

Assim, fica claro que é necessário abordar os conteúdos matemáticos de forma mais aplicada possível à realidade do discente. Caso contrário, corre-se o risco de que o aluno se desinteresse cada vez mais pelos assuntos ensinados, resultando em reprovações e ojeriza aos conteúdos.

Ainda, conforme os PCN [1]:

"De fato, não basta revermos a forma ou metodologia de ensino, se mantivermos o conhecimento matemático restrito à informação, com as definições e os exemplos, assim como a exercitação, ou seja, exercícios de aplicação ou fixação. Pois, se os conceitos são apresentados de forma fragmentada, mesmo que de forma completa e aprofundada, nada garante que o aluno estabeleça alguma significação para as ideias isoladas e desconectadas umas das outras. Acredita-se que o aluno sozinho seja capaz de construir as múltiplas relações entre os conceitos e formas de raciocínio envolvidas nos diversos conteúdos; no entanto, o fracasso escolar e as dificuldades dos alunos frente à Matemática mostram claramente que isso não é verdade."

Assim, combate-se o ensino puramente pragmático e totalmente desconexo da realidade que cerca o aluno. Deve-se buscar, incessantemente, as aplicações atinentes ao conteúdo ministrado, sempre que possível. Desta forma, possivelmente haverá uma recepção melhor do aluno aos ensinamentos transmitidos.

No ensino brasileiro, já está consagrada a preocupação com a contextualização e a interdisciplinaridade. Novamente, nos PCN [1], em sua página 43, tem-se:

"O critério central é o da contextualização e da interdisciplinaridade, ou seja, é o potencial de um tema permitir conexões entre diversos conceitos matemáticos e entre diferentes formas de pensamento matemático, ou, ainda, a relevância cultural do tema, tanto no que diz respeito às suas aplicações dentro ou fora da Matemática, como à sua importância histórica no desenvolvimento da própria ciência."

Tratando-se de funções exponenciais, é importante contextualizar o seu ensino. A modelagem deste tipo de função surgiu ante a necessidade de solucionar um problema ainda sem resposta. A modelagem da função afim já era conhecida, porém com o surgimento de uma nova demanda, houve a procura de um novo modelo teórico. Conforme Bassanezi [2], ressalta-se a importância:

"O objetivo fundamental da aplicação da matemática é de fato extrair a parte essencial da situação-problema e formalizá-la em um contexto abstrato onde o pensamento possa ser absorvido com uma extraordinária economia de linguagem. Desta forma, a matemática pode ser vista como um instrumento intelectual capaz de sintetizar ideias concebidas em situações empíricas que estão quase sempre camufladas num emaranhado de variáveis de menor importância."

Portanto, acredita-se que, através de uma adequada contextualização, se consiga atingir melhores resultados quanto à assimilação dos conteúdos. É importante ressaltar que, em nenhuma hipótese, se deseja deixar o formalismo matemático em detrimento da realidade do assunto. Ambos são importantes para a construção do saber do nosso aluno. O que se pretende evitar é o exagero de qualquer uma das ferramentas. Caberá ao docente, no momento adequado, formalizar os conceitos, fornecendo o embasamento necessário e oportuno, tendo em vista que é um dos objetivos do ensino da Matemática.

Explicar a origem do assunto e o seu motivo de surgimento, através de exemplos, também podem ser ótimos caminhos para motivar o estudo da Matemática e, especificamente, de funções exponenciais. Um ótimo exemplo é a famosa história (porém pouco conhecida, infelizmente) de um rei persa que, ao perceber que o seu reino se encontrava entendiado com a rotina diária, recompensaria quem criasse algum jogo para entretenimento da corte.

A notícia, rapidamente, se espalhou por todo o domínio real, até que um dos súditos apresentou uma espécie de jogo de xadrez. Vale ressaltar que não se sabe ao certo se o jogo era inédito. Relatos afirmam que foi uma adaptação de um jogo de tabuleiro já experimentado pelos gregos.

O jogo de 32 peças e 64 casas quadradas com um dinâmica bem interessante. O rei ficou maravilhado e o passatempo foi um sucesso. Diante disso, mandou que chamassem o súdito imediatamente para uma conversa. Perguntou-lhe o que queria como recompensa, já que o objetivo havia sido atingido em sua plenitude. Ofereceu-lhe ouro, joias, posses e até um casamento com uma de suas filhas.

Porém, para a surpresa do governante, a resposta do súdito foi que queria grãos de arroz, distribuídos da seguinte forma: 1 grão na primeira casa, 2 na segunda, 4 na terceira, 8 na quarta e assim sucessivamente, sempre duplicando a quantidade de grãos da casa anterior, até que as 64 casas estivessem completas.

O rei, maravilhado e boquiaberto com a humildade do súdito, mandou que trouxessem imediatamente os grãos de arroz. Ao iniciar a empreitada, percebeu que todo o seu reino não possuía quantidade de grãos suficiente para arcar com o compromisso. Desesperado, mandou chamar um matemático da corte. Este falou-lhe que nem todos os grãos do mundo seriam suficientes para cumprir o trato realizado.

Este é o primeiro relato de noções exponenciais que se conhece. É sabido que havia outros povos que já conheciam o modelo, mas o conto é o registro antigo mais conhecido.

Trata-se de uma simples história que poderia ser abordada para motivar o ensino do assunto. Decerto, o aluno ficaria muito mais curioso e atento às explicações, já que estaria ouvindo uma narrativa ocorrida no passado, englobando o assunto que será estudado logo a seguir.

Por meio deste simples exemplo, tenta-se mostrar que é possível realizar uma abordagem de conteúdos exponenciais com uma natureza aplicada e voltada para os problemas diários e de outras áreas do conhecimento.

A intenção deste trabalho é retratar a importância do conteúdo matemático exposto através de aplicações cotidianas e curiosidades rotineiras. Portanto, serão mostradas algumas das principais aplicações e curiosidades que envolvem o assunto de funções exponenciais. Existem diversas aplicações bem interessantes da teoria de funções exponenciais que podem ser aplicadas no Ensino Médio, inclusive referenciando outras disciplinas além da Matemática.

2 Aplicações cotidianas de funções exponenciais

Este artigo é baseado em dois trabalhos de conclusão do PROFMAT, cujos temas serão inicialmente omitidos nesta versão do artigo para evitar identificação dos autores. Essas dissertações possuem um grande viés pedagógico, e objetivam impactar o ensino nas escolas, mostrando aos docentes como a contextualização pode ajudar o docente em sala de aula. Nelas são propostas sequências didáticas com a exibição de aplicações de funções exponenciais em sala de aula se antecipando ao conteúdo propriamente dito, despertando interesse no discente e mostrando que antes do modelo matemático vem a situação real, cotidiana. Para

subsidiar os professores, foram apresentadas nestes trabalhos diversas aplicações de funções exponenciais. Foi feita uma seleção das mais interessantes para serem aqui expostas.

2.1 Desintegração radioativa

Os átomos de uma substância radioativa (como o rádio e o urânio, por exemplo) tendem a se desintegrar, emitindo partículas e transformando-se noutra substância. As partículas emitidas não alteram consideravelmente a massa total do corpo mas, com o passar do tempo, a quantidade da substância original diminui (aumentando, consequentemente, a massa da nova substância transformada). Isto ocorre de tal modo que, em cada instante, a quantidade de matéria que se está desintegrando naquele momento é proporcional à massa da substância que ainda resta.

Assim sendo, se denominarmos de *meia-vida de uma substância radioativa* o tempo necessário para que se desintegre a metade da massa de um corpo formado por aquela substância, constatamos que a meia-vida é um número intrinsecamente associado a cada substância radioativa: o tempo necessário para reduzir à metade a radioatividade de uma tonelada de urânio é igual ao tempo que leva um grama da mesma substância para ter sua metade desintegrada. A propósito, como exemplo, os vários isótopos do urânio têm meia-vida da ordem de 10^9 anos. Enquanto isso, a meia-vida do rádio 224 é de 3 dias e 15 horas.

De um modo geral, se designarmos por $m = m(t)$ a massa da substância radioativa presente no corpo no instante t, verifica-se que m é uma função decrescente de t e, além disso, a perda relativa $\dfrac{m(t+h)-m(t)}{m(t)}$, ocorrida após o decurso do tempo h, depende apenas de h e não do instante inicial t, ou seja, da massa $m(t)$ existente naquela ocasião.

Outra vez, constatamos a necessidade de uma função real de variável $m : \mathbb{R} \to \mathbb{R}$, que seja monótona injetiva (desta vez, decrescente) e tal que a variação relativa $\dfrac{m(t+h)-m(t)}{m(t)}$ dependa apenas de h. Ou, equivalentemente, que a razão $\dfrac{m(t+h)-m(t)}{m(t)}$ não dependa de t mas somente de h.

Se aplicarmos o Teorema de Caracterização de Funções do tipo Exponencial, concluiremos que a função que representa a massa da substância é deste tipo, ou seja, $m(t) = m_0.a^t$, onde m_0 é a massa inicial da substância e a é o fator de decaimento, sendo $0 < a < 1$.

Vamos dar um exemplo genérico de como encontrar esta função exponencial que representa a massa de uma substância X no instante t, dado que o tempo de meia-vida dessa substância é $t_{1/2}$, ou seja, a massa desta substância se reduz à metade após $t_{1/2}$ unidades de tempo. Logo, se a massa inicial da substância é m_0, após decorridos $t_{1/2}$ unidades de tempo, a massa será igual a $\dfrac{m_0}{2}$. Analisando a fórmula genérica e utilizando estes valores, temos:

$$m(t) = m_0.a^t \Rightarrow \frac{m_0}{2} = m_0.a^{t_{1/2}} \Rightarrow \frac{1}{2} = a^{t_{1/2}} \Rightarrow a = \left(\frac{1}{2}\right)^{\frac{1}{t_{1/2}}}$$

Portanto, a função exponencial encontrada é: $m(t) = m_0.a^t = m_0.\left(\dfrac{1}{2}\right)^{\frac{t}{t_{1/2}}}$

2.2 Aplicação de capital a juros fixos

Como já foi citado no início deste capítulo, a função que expressa a variação do capital, quando aplicado por um período do tempo é do tipo exponencial, isto é, é da forma $c(t) =$

$c_0.a^t$, onde $c(t)$ expressa o capital no instante t e c_0 é considerado o fator de aumento do capital. Neste caso, o fator de aumento a é igual a $(1+i)$, onde i é chamado de taxa de juros. Para exemplificar, considere um capital inicial de R$2000,00 aplicado a uma taxa fixa de juros de 2% ao mês. Portanto, a função que representa o capital no instante t, em meses, é dada por:

$$c_0.(1+i)^t = 2000.(1+0,02)^t = 2000.(1,02)^t$$

Para um quadrimestre, isto é, para um $t = 4$, a título de exemplo, temos:

$$c_0.(1+i)^4 = 2000.(1+0,02)^4 = 2000.(1,02)^4 \approx 2164,86$$

Antes de passarmos à próxima aplicação, tentaremos realizar uma distinção entre juros simples e juros compostos. Em vez de procurarmos definições rígidas e financeiras, vamos à citação do livro de Eli Maor: [3]

"Juro é a remuneração que se paga por tomar dinheiro emprestado, ou que se recebe por emprestá-lo. Usualmente é um percentual do dinheiro que se tomou ou emprestou. Juro simples é o dinheiro pago ou recebido pela quantia original, e que permanece o mesmo em cada prestação, ou seja, se um banco cobra 20% ao ano de juros simples sobre um empréstimo de cem libras, então, um ano depois, a dívida é de 120 libras, depois de dois anos é de 140 libras, depois de três anos é de 160 libras e assim por diante. Com juro composto, no entanto, cada pagamento é uma proporção do total composto, ou acumulado. O dinheiro que se deve dos juros vai alimentar o "pote". Assim, se um banco cobra 20% de juros compostos, um dívida de 100 libras será de 120 libras após um ano, de 144 libras depois de dois, de 172,80 libras depois de três."

Como o trabalho destina-se a motivar o estudo das funções exponenciais e, em sentido mais *strictu*, a funções exponencial natural, deixa-se uma citação bem interessante de Maor [3], que explica muito sobre o mundo que vivemos:

"Quem empresta dinheiro tem preferido os juros compostos aos simples ao longo de toda a história conhecida. Inclusive, num dos primeiros problemas da literatura matemática, numa tabuleta de barro mesopotâmica de 1700 a.C., a pergunta é quanto tempo levaria para que uma quantia dobrasse de valor a um juro composto de 20% ao ano. Um dos motivos que fazem a atividade bancária ser tão lucrativa é que o juro composto faz crescer a dívida, ou o empréstimo, exponencialmente, o que vale dizer que você pode acabar pagando, ou ganhando, quantias exorbitantes em pouco tempo. Os romanos condenaram o juro composto como a pior forma de usura. No Alcorão, é declarado um pecado. Não obstante, o sistema financeiro moderno baseia-se nessa prática. É como os nossos saldos devedores, faturas de cartão de crédito e pagamentos de hipotecas são calculados. O juro composto tem sido o principal catalisador do crescimento econômico desde o início da civilização."

Infelizmente, no nosso Ensino Básico, não se tem a devida preocupação com Educação Financeira. O assunto está intimamente ligado aos modelos exponenciais abordados no presente trabalho. Conforme citado acima, instituições financeiras praticam o emprego de composições exponenciais, por serem mais lucrativas ao sistema. Ensina-se porcentagem, função afim, função logarítmica, função exponencial e outros assuntos sem relacioná-los com a realidade financeira que nos cerca. Atualmente, falar-se em ser educado financeiramente resume-se apenas a ter um consumo responsável, controlar gastos e caderneta de poupança. A matéria é muito mais abrangente que isso.

Assim, novamente com o intuito de despertar a completa atenção do discente, vamos a um exemplo, o qual é imperioso que seja tratado em sala de aula. Refere-se como o sistema financeiro britânico se comporta ao oferecer serviços aos seus consumidores. Certamente,

muitos consumidores ficam bastante confusos quando observam determinados financiamentos com as mais variadas modalidade de capitalização. Vejamos como a Inglaterra tenta ser um pouco mais clara, neste ponto:

> *"Isso porque as instituições financeiras britânicas são obrigadas por lei a declarar a taxa de juro composto contínua em cada produto que vendem, qualquer que seja a sua opção de creditar mensalmente, bisanualmente, anualmente ou o que for. Digamos que um banco ofereça uma conta de depósito que remunera 15% ao ano, composto em um crédito anual, o que significa que depois de um ano um depósito de cem libras terá aumentado para 115 libras. Se esses 15% forem compostos continuamente, após mais um ano aumentará para* $£100.e^{\frac{15}{100}}$*, o que resulta em 116,18 libras, revelando uma taxa de juros de 16,18%. O banco é obrigado por lei a declarar que essa conta de depósito rende 16,18%. Embora pareça estranho que um banco declare um valor não usado na prática, isso foi introduzido para que os clientes possam comparar coisa com coisa. Uma conta que credita mensalmente e uma que credita anualmente serão avaliadas por sua taxa composta contínua. Como quase todo produto financeiro envolve juros compostos, e cada cálculo de composição contínua vai dar num e, a constante exponencial é o número do qual depende todo o sistema financeiro."*
>
> *(Bellos [3])*

2.3 O caso do paraquedas

Esta aplicação deve ser abordada com bastante cuidado pelo professor, pois apesar de interdisciplinar (envolve Matemática e Física), ela também engloba conhecimentos que fogem ao conteúdo do Ensino Médio. Todavia, se usada adequadamente, agregará ao aluno algumas noções de força, de resistência do ar e de como ocorre a redução de velocidade do paraquedista.

Analisemos, então, o caso de um homem que salta de paraquedas. As forças que atuam sobre ele são: a força peso, na direção vertical com sentido para baixo e a força de resistência do ar, que é proporcional à velocidade do corpo, também vertical e com sentido contrário ao da força peso. De acordo com a Segunda Lei de Newton, o somatório das forças é igual ao produto da massa pela aceleração. Logo, sendo m a massa do paraquedista, a sua aceleração, v a sua velocidade, k a constante de proporcionalidade da força de resistência do ar ($F_{ar} = kv$) e g a aceleração da gravidade, temos:

$$ma = mg - kv$$

Como a função aceleração é a função derivada da função velocidade em relação ao tempo, podemos resolver essa equação diferencial ordinária e encontrar uma expressão para a velocidade. Obviamente, este assunto foge ao escopo do Ensino Médio e, por isso, o professor deve se ater a analisar a equação do balanço de forças e, em seguida, exibir o resultado final, a fim de mostrar aos alunos que a velocidade cai exponencialmente quando o corpo sofre a resistência do ar. A expressão final da velocidade em função do tempo é:

$$v(t) = \frac{mg}{k} + C.e^{-\frac{kt}{m}}$$

onde C é uma constante e e é a constante neperiana. Ainda, com uma manipulação algébrica para não ter a massa do saltador na expressão, vale dizer:

$$v = \frac{g}{a}(1 - e^{-at}) + v_0 e^{-at} \tag{1}$$

com $a = \frac{k}{m}$. [1]

Observando a equação 1, pode-se ter conclusões interessantes e importantes: se o paraquedista comandar (termo utilizado para o acionamento do paraquedas, quando isso é possível, já que existem paraquedas que são acionados pela ação da gravidade quando a pessoa salta do aerotransporte) o seu equipamento assim que sair do avião, pode-se dizer que $v_0 = 0$, fazendo com que o último termo da equação 1 seja eliminado.

Ainda, se ele cair livremente, ou em linguagem técnica, entrar em queda-livre, antes de comandar o seu paraquedas, sua velocidade v_0 aumentará bastante, porém o seu efeito diminui exponencialmente conforme o avançar do tempo. Isso é fato pois, se $t \to \infty$, a expressão e^{-at} tende a zero e a velocidade limite, chamada, por exemplo, de v_∞ será igual a $\frac{g}{a}$ ou ainda, $v_\infty = \frac{mg}{k}$ será atingida.

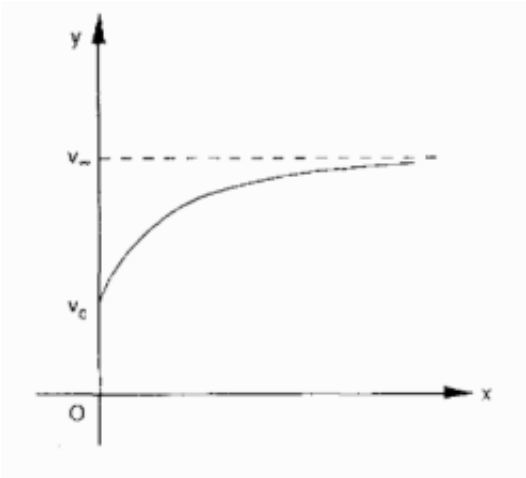


Figura 1. Atingimento da velocidade limite v_∞ do salto de paraquedas
Fonte: Maor, 2003. [4]

E isso é o mais interessante: se a velocidade limite é atingida independente do v_0 inicial do acionamento do paraquedas, dependendo apenas do peso do saltador e do coeficiente de resistência, podemos concluir que tal fato é o que permite que o pouso seja seguro, chegando ao solo com uma velocidade compatível. Mas é claro: deve-se acionar o paraquedas!

2.4 Percepções a estímulos físicos - Experiência sonora

Assim como a anterior, a aplicação deve ser usada com muito cuidado. Alguns conceitos mais avançados podem confundir a construção do raciocínio e do conhecimento do estudante do Ensino Médio. Todavia, trata-se de algo muito interessante de ser levado ao conhecimento.

O fisiologista alemão Ernst Heinrich Weber (1975-1878) [2] desenvolveu um teste, obtido por intermédio de vários experimentos, que seria capaz de quantificar a resposta humana a diversos estímulos físicos recebidos ou aplicados. A generalização deste teste para todos os sentidos foi recepcionada pelo médico alemão Gustav Theodor Fechner (1801-1887) e ficou

[1] A demonstração detalhada poderá ser obtida na obra *e: a história de um número*, de Eli Maor.

[2] Ernst Heinrich Weber (Wittenberg, 24 de junho de 1795 — 26 de janeiro de 1878) foi um médico alemão e é considerado fundador da psicologia experimental.

conhecida como a lei de Weber-Fechner. Para ilustrar melhor, um dos experimentos foi aplicado em um homem totalmente vendado que segurava um determinado peso. Assim, outros pesos menores eram acrescentados gradativamente e a cobaia humana deveria responder quando percebia uma alteração de peso pela primeira vez [4].

Após inúmeros experimentos desta natureza e em todos os sentidos sensoriais, Weber pode concluir que a resposta ao estímulo era proporcional ao aumento relativo, e não ao aumento absoluto. Explicando melhor: se um homem estivesse segurando um peso de 20 quilogramas e pudesse sentir um aumento de peso quando fosse introduzido um peso de 2 quilogramas, quando ele estivesse com um peso de 40 quilogramas, só sentiria o aumento a partir de 4 quilogramas, que corresponde a 10% de aumento do peso em ambos os casos.

Conforme Maor [4], em modo matemático, se pode escrever:

$$ds = k\frac{dW}{W}, \tag{2}$$

onde ds é o aumento perceptível (seria a condição limite, o menor aumento de peso que pudesse ser percebido), dW é o aumento de peso correspondente, W o peso já usado com a cobaia e k uma constante de proporcionalidade.

A lei de Weber-Fechner, como está em 2, é uma equação diferencial. Devemos ter muito cuidado ao apresentar tal conteúdo no Ensino Médio: aqui, não se deve adentrar em explicações detalhadas sobre como obter a função derivada ou a antiderivada, bastando apenas informar o que foi feito. Isso não prejudicará o aprendizado, tampouco o exemplo trazido.

Então, integrando 2, tem-se:

$$s = k\ln W + C, \tag{3}$$

com C sendo uma constante de integração. Conforme [4], fazendo W_0 o mais baixo nível de estímulo físico, isto é, o nível limite, teremos, $s = 0$ quando $W = W_0$, obtendo $C = -k\ln W_0$. Colocando na equação 3 e usando as propriedades de logaritmos, tem-se:

$$s = k\ln\frac{W}{W_0}, \tag{4}$$

mostrando que a resposta segue um padrão logarítmico (função inversa da exponencial). Trocando em miúdos: se o estímulo aumentar em taxa constante, isto é, em progressão geométrica, a resposta ao estímulo aumentará em proporções iguais.

Apesar da contestação dos experimentos, já que a receptividade humana é uma questão subjetiva, os testes se aplicam muito bem à sensação de volume, dada a capacidade de percepção da audição humana.

> *"Quando a lei de Weber-Fechner é aplicada à tonalidade, ela diz que intervalos musicais iguais (aumentos de tonalidade) correspondem a aumentos fracionais iguais na frequência. Daí os intervalos musicais corresponderem a relações de frequência. Por exemplo, uma oitava corresponde à proporção 2:1 na frequência, uma quinta à proporção 3:2, uma quarta a 4:3 e assim por diante. Quando ouvimos uma série de notas separadas por oitavas, sua frequência na verdade aumenta em uma progressão 1, 2, 4, 8, e assim por diante."*
>
> *(Maior [4])*

Figura 2. Notas musicais separadas em intervalos iguais correspondem a frequências em uma progressão geométrica

Fonte: Maor, 2003 [4].

Isso nos permite concluir que as pautas onde as notas musicais são escritas é, na verdade, uma escala logarítmica, na qual a distância vertical, chamada de tom, é proporcional ao logaritmo da frequência. [4]

2.5 A corrente suspensa

O problema da corrente suspensa envolve o número e e a função $f(x) = e^x$. Trata-se da seguinte indagação: *qual é a curva formada por um fio pendente, livremente suspenso por dois pontos fixos, assumindo que o fio é flexível em toda a sua extensão e possui uma espessura constante?* (entende-se como densidade linear uniforme). Tal problemática foi exposta por Jakob Bernoulli em maio de 1690 na *Acta eruditorum*, revista esta que o próprio havia fundado oito anos antes.

Acerca das respostas a este questionamento, citamos [4]:

> *"A história desse famoso problema é bem semelhante à da braquistócrona e quase os mesmos personagens tomaram parte nela. Galileu já tinha demonstrado interesse e imaginara que a curva era uma parábola. Aos olhos, a corrente suspensa certamente se parece com uma parábola. Mas Christian Huygens, o prolífico cientista holandês, cujo papel na história tem sido um tanto subestimado (sem dúvidas porque viveu entre as eras de Kepler e Galileu antes dele, e Newton e Leibniz depois), provou que a catenária não podia ser uma parábola."*

Houve outras respostas para o problema evidenciado. Em 1691, a publicação *Acta* expôs três soluções corretas para a questão: uma por Leibniz; outra por Huygens; e por Johann Bernoulli.

Fazendo uma nota histórica, na verdade, uma curiosidade acerca da família Bernoulli. Jakob e Johann eram rivais acirrados. Mesmo sendo irmãos, a competição pelas descobertas matemáticas eram muito maiores que a afeição familiar. Rivalizaram por toda a vida pelas respostas e soluções dos principais desafios matemáticos da época, a ponto de ficarem sem se falar durante um longo período de tempo. Comprovando o exposto, ainda em [4]:

> *"Johann acrescentou que, das duas curvas, a parábola é algébrica enquanto a catenária é transcendental. Impetuoso como sempre, concluiu: "O senhor conhece a disposição do meu irmão. Ele não hesitaria, se pudesse fazê-lo honestamente, em tirar-me a honra de ser o primeiro a resolvê-lo, em vez de me deixar tomar parte - e muito menos me cederia o lugar, se já fosse meu". A notoriedade dos Bernoullis de brigarem entre si - e com os outros - não diminuíra nada com a passagem do tempo."*

A catenária é a curva cuja equação é dada por:

$$y = \frac{e^{ax} + e^{-ax}}{2a} \tag{5}$$

para a uma constante cujo valor é relacionado aos parâmetros físicos da corrente, como densidade linear e tensão com a qual ela é segura.

Quanto à equação acima vale expressar:

> *" Devemos mencionar que a equação da catenária não foi apresentada originalmente na forma acima. O número e ainda não tinha um símbolo especial, e a função exponencial não era considerada função independente e sim um inverso da função logarítmica."*

Para $a = 1$, podemos construir o gráfico por intermédio dos gráficos de e^x e de e^{-x} no mesmo sistema de coordenadas: trata-se de realizar, para cada ponto x do domínio, a soma $e^x + e^{-x}$ e, na sequência, dividir o resultado por 2. Esse será a ordenada de cada ponto x do domínio.

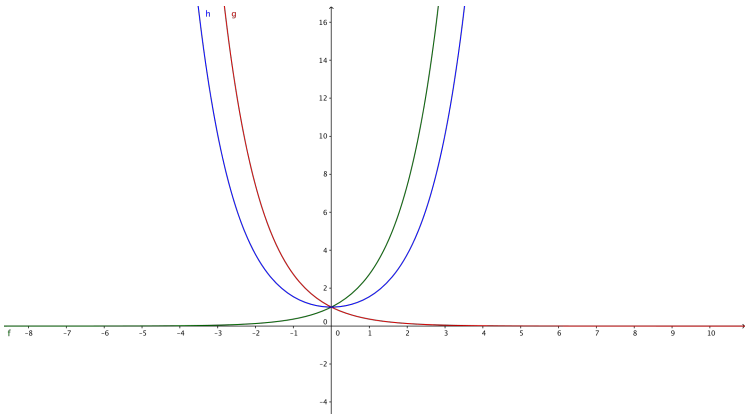


Figura 3. Gráfico de e^x, e^{-x}, e da catenária para $a = 1$

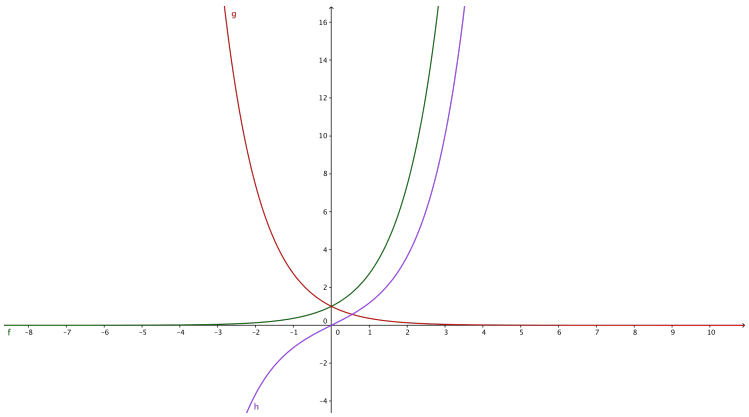


Figura 4. Gráfico de $\frac{e^x - e^{-x}}{2}$

Considerando as equações dos dois gráficos plotados acima, quando em função de x, são muito semelhantes às equações das funções circulares cosseno e seno (sen e cos). Essas similaridades foram notadas por Vincenzo Ricatti (1707-1775) [3] que introduziu as notações de seno e cosseno hiperbólicos (sinh e cosh), a saber:

$$\sinh\phi = \frac{e^x + e^{-x}}{2} \; ; \cosh\phi = \frac{e^x + e^{-x}}{2} \tag{6}$$

O italiano demonstrou que é válida a igualdade

$$\cosh^2\phi - \sinh^2\phi = 1 \tag{7}$$

que, excetuando-se pelo sinal negativo, é igual à identidade trigonométrica consagrada no Ensino Médio:

$$\cos^2\phi + \text{ sen}^2\phi = 1 \tag{8}$$

Vale aqui uma analogia importante a ser trabalhada com os alunos do Ensino Médio: comparar a identidade trigonométrica consagrada, representada pela equação 8 e a igualdade hiperbólica da equação 7 com as equações de um círculo de raio unitário centrado na origem e de uma hipérbole equilátera de equação $x^2 - y^2 = 1$, respectivamente.

A notação de Rivatto ficou consagrada para $\cosh\phi$ como cosseno hiperbólico de ϕ e seno hiperbólico de ϕ como $\sinh\phi$. Através das propriedades especiais das funções e^x e e^{-x}, a identidade da equação 7 pode ser demonstrada elevando-se ao quadrado ambos os lados das equações 6 e usando as identidades $e^x.e^y = e^{x+y}$ e $e^0 = 1$.

3 Uma conversa com os professores do Ensino Médio

Na época da elaboração dos já citados trabalhos de conclusão de curso, com o objetivo de verificar como estava o ensino de funções exponenciais nas escolas de Ensino Médio, foi feita uma pesquisa entre diversos docentes, tanto pela Internet quanto presencialmente. Uma das perguntas feitas, cuja temática está sendo abordada neste artigo, é a seguinte: **Você apresenta em sala possíveis aplicações para funções exponenciais? Caso positivo, cite alguns exemplos.**

Nesta pergunta, todos os professores citaram os casos clássicos como: matemática financeira (juros compostos), crescimento populacional, decaimento radioativo, ingestão de medicações. Casos menos convencionais também foram citados: distribuição de Poisson (aplicações em teoria das filas; filas de banco; filas de *buffer* de um roteador; filas de paginação de um sistema operacional, entre outros), ruído gaussiano branco, curvas PV^α do gás ideal.

Seguem algumas respostas interessantes a esta pergunta:

1. Sim, mostro que elas representam uma progressão geométrica e cito os juros compostos em matemática financeira. São conteúdos que possuem diversas aplicações na literatura

[3] Vincenzo Riccati (Castelfranco Veneto, 11 de janeiro de 1707 — Treviso, 17 de janeiro de 1775) foi um matemático e físico italiano. Irmão de Giordano Riccati, foi o segundo filho de Jacopo Francesco Riccati. Riccati continuou a obra de seu pai em análise matemática, especialmente no campo das equações diferenciais e física. A equação de Riccati é denominada em memória de seu pai.

2. Sim. Como exemplos cito o sistema de juros compostos, a decomposição de determinadas substâncias e o crescimento de determinados seres vivos microscópicos, como as bactérias.

3. Sim, falo sobre o decaimento radioativo e a escala Richter para intensidade de terremotos.

4. Sim, sempre é bom mostrar exemplos. Costumo falar de crescimento de populações na ausência de predadores naturais (como em algumas bactérias). Também menciono o crescimento da população mundial. Se der tempo falo de poupança também.

5. Sim, falo de diversas aplicações: Ruído gaussiano branco, através da função exponencial de Gauss; probabilidade, através da distribuição de Poisson (aplicações em teoria das filas: filas de banco, filas de *buffer* de um roteador, filas de paginação de um sistema operacional).

Essas respostas demonstram a preocupação desses professores em conectar a realidade à teoria, o que é fundamental para auxiliar num melhor processo de aprendizagem por parte do discente. É bastante motivador perceber que já existe essa preocupação em sala de aula, e este trabalho intenta municiar os professores de mais possibilidades de aplicações práticas para exibir em sala.

4 Conclusões

Procurou-se com este trabalho, sob um enfoque mais amplo, mostrar que o ensino através de uma perspectiva aplicada pode obter melhores resultados quanto ao processo de ensino-aprendizagem do aluno. Através de uma minuciosa revisão de literatura, tentou-se corroborar o que foi defendido ao longo desta jornada. Os Parâmetros Curriculares Nacionais foram os norteadores deste estudo, confirmando que já há um preocupação antiga em se ensinar Matemática de forma mais natural e aplicada, sem abandonar o formalismo necessário à ciência. Buscou-se trazer exemplos interessantes, como por exemplo a abertura de paraquedas modelada por uma função tipo exponencial natural, permitindo concluir que o saltador sempre chegará com uma velocidade de pouso compatível, impedindo acidentes. A pequena contribuição que este artigo almeja é fazer com que o aluno do Ensino Médio se interesse mais pela Matemática ao aprender o conteúdo de funções exponenciais, já que este possui uma enorme gama de aplicações que conseguem despertar um maior interesse do discente. A Matemática tem sido há muito tempo vista como vilã pelos estudantes, repleta de conteúdos teóricos intermináveis e exercícios repetitivos e sem correspondência com a realidade. Portanto, algo precisa ser mudado na forma como a mesma é ministrada nas milhares de salas de aula espalhadas pelo nosso país.

Referências

[1] BRASIL; Parâmetros Curriculares Nacionais - Ensino Médio, 1998

[2] BASSANEZI; Ensino-aprendizagem com modelagem matemática: uma nova estratégia, Contexto, 2002

[3] BELLOS, A; Alex através do espelho: como a vida reflete os números e como os números refletem a vida, Companhia das Letras, 2015.

[4] MAOR, E. e: a história de um Número. Record, 2003.