Efeitos dos parâmetros no modelo SISa para estados emocionais

Ana Claudia Pereira [1]
Eliza Maria Ferreira[2]
Graziane Sales Teodoro[3]
Ricardo Edem Ferreira[4]

Utilizando um mesmo modelo matemático é possível descrever o comportamento de diversos fenômenos, fazendo pequenas adaptações quando necessárias, já que muitos desses apresentam comportamentos semelhantes. Neste trabalho, o modelo clássico de doença infecciosa suscetível-infectado-suscetível (SIS) foi modificado com o intuito de representar a disseminação de emoções, considerando que as emoções podem ser contraídas tanto espontaneamente quanto por transmissão. O modelo apresentado, conhecido como SISa, difere do modelo SIS tradicional pela coexistência de dois estados emocionais (o equivalente a um modelo com duas doenças sem superinfecção) e também pelo contágio espontâneo. Devido ao contágio espontâneo não faz sentido o cálculo do número de reprodução básico R_0. Esse modelo possui três classes, neutros, N, contentes, C e descontentes, D e foi baseado em [1]. Veja o modelo a seguir:

$$\begin{cases} \dot{N} &= (1-N)\beta - (\beta_c C + \beta_d D)\, N - (a_c + a_d)N + g_c C + g_d D \\ & \quad -((1-N)\delta_n - \delta_c C - \delta_d D)N \\ \dot{C} &= -\beta C + \beta_c CN + a_c N - g_c C - s_{cd} DC + s_{dc} CD \\ & \quad -((1-C)\delta_c - \delta_n N - \delta_d D)C \\ \dot{D} &= -\beta D + \beta_d DN + a_d N - g_d D - s_{dc} CD + s_{cd} DC \\ & \quad -((1-D)\delta_d - \delta_n N - \delta_c C)D. \end{cases} \tag{1}$$

Veja na tabela a descrição dos parâmetros utilizados no modelo.

[1]Universidade Federal de Lavras, anaclaudia@ufla.br
[2]Universidade Federal de Lavras, eliza.ferreira@ufla.br
[3]Universidade Federal de Lavras, graziane.teodoro@ufla.br
[4]Universidade Federal de Lavras, ricardoedem@ufla.br

Parâmetros	Descrição
β	taxa de natalidade da população
β_c, β_d	taxas com que indivíduos neutros passam para classes infectadas
a_c, a_d	taxas de mudança espontânea de neutro para as classes infectadas
g_c, g_d	taxas de retorno à classe neutra
δ_n, δ_c e δ_d	taxas de mortalidade
s_{cd}, s_{dc}	taxas de mudança entre classes de infectados

Tabela 1: Parâmetros do modelo

Neste trabalho analisaremos como a relação entre os parâmetros afeta a dinâmica do modelo abordado.

References

[1] A. L. Hill, D. G. Rand, M. A. Nowak, and N. A. Christakis, "Emotions as infectious diseases in a large social network: the sisa model," *Proceedings of the Royal Society B: Biological Sciences*, vol. 277, no. 1701, pp. 3827–3835, 2010.

Compactificação de Stone-Čech

Ana Cristina Porto Silveira [1]
Orientador: Sérgio Guilherme de Assis Vasconcelos[2]

No decorrer deste trabalho, abordaremos o conceito de compactificação de Stone-Čech. Esta foi construída independentemente por M. Stone e E. Čech em 1937 e possui diversas aplicações na análise moderna. A compactificação por um ponto é, de alguma forma, a compactificação mínima de X. O nosso objeto de estudo, a *Compactificação de Stone-Čech*, é a compactificação máxima de X.

Primeiramente, retomaremos os conceitos de compactificação e de espaços completamente regulares, que nos serão úteis ao decorrer deste trabalho. Uma *compactificação* de um espaço X é um espaço compacto Hausdorff Y contendo X como subespaço tal que $\overline{X} = Y$. Duas compactificações Y_1 e Y_2 de X são ditas *equivalentes* se existe um homeomorfismo $h : Y_1 \to Y_2$ tal que $h(x) = x$ para todo $x \in X$.

Um espaço X é dito *completamente regular* se os conjuntos unitários são fechados em X e se para cada ponto x_0 e cada conjunto fechado A, com $x_0 \notin A$, existe uma função contínua $f : X \to [0, 1]$ tal que

$$f(x_0) = 1 \text{ e } f(A) = \{0\}.$$

Todo espaço compacto Hausdorff é normal, isto é, separa fechados. Logo, pelo Lema de Urysohn, são completamente regulares. Assim, se X possui uma compactificação, sendo subespaço de um compacto, é também completamente regular. Por outro lado, se X é completamente regular, então X tem uma compactificação . Para isso, basta fazermos um mergulho de X no espaço $Y = [0, 1]^J$, que nos dará uma compactificação de X e, então chamaremos Y de *compactificação induzida* pelo mergulho h.

Referências

[1] J. R. Munkres, *Topology*, 2ª ed., Prentice Hall, Upper Saddle River, NJ, 2000.

[1]Universidade Federal de Juiz de Fora, anacristina.silveira@estudante.ufjf.br
[2]Universidade Federal de Juiz de Fora, sergio.guilherme@ufjf.br

Critérios de Divisibilidade

Athos de Azevedo Pereira [1]

Neste trabalho, veremos como construir, para números escritos na base decimal, critérios de divisibilidade por um inteiro qualquer $d > 1$. Para isso, usaremos congruências e a ordem de 10 módulo d para explicar a construção desses critérios. Exibiremos alguns critérios que serão úteis e outros nem tanto, mas que podem ser aplicados computacionalmente.

Referências

[1] A. A. Pereira, "Critérios de divisibilidade," *submetido*, 2025.

[2] F. MARTINEZ, C. MOREIRA, N. SALDANHA, and E. Tengan, "Teoria dos números: um passeio com primos e outros números," *IMPA, Rio de Janeiro, 5ª edição*, 2018.

[3] J. P. d. O. Santos, *Introdução à teoria dos números*. IMPA, 1998.

[1]Universidade Federal de Ouro Preto ,
athos.pereira@aluno.ufop.edu.br

Cocaracteres de uma PI-álgebra via a ação dos grupos S_n e GL_m

Breno Oliveira Souza [1]

Sejam F um corpo algebricamente fechado de característica zero e A uma PI-álgebra. Para cada $n \in \mathbb{N}$, consideramos o espaço P_n dos polinômios multilineares de grau n, sobre o qual o grupo simétrico S_n age naturalmente permutando as variáveis. A partir dessa ação, define-se o n-ésimo cocaracter de A, denotado por $\chi_n(A)$, cuja decomposição em caracteres irredutíveis de S_n fornece informações relevantes sobre a estrutura da álgebra, particularmente de sua sequência de codimensão.

Neste trabalho, buscamos estudar as multiplicidades m_λ na decomposição de $\chi_n(A)$, por meio de idempotentes essenciais associados às tabelas de Young e vetores de altura máxima, construídos a partir da estrutura de GL_m-módulo na álgebra dos polinômios multihomogêneos. Essa estrutura permite que o espaço dos polinômios homogêneos de grau n seja decomposto como soma direta de submódulos irredutíveis $W_m(\lambda)$, associados a partições $\lambda \vdash n$. O estudo dessas representações refina a análise dos cocaracteres, possibilitando identificar quais partições contribuem com multiplicidade não nula, utilizando técnicas combinatórias e a teoria de representações de álgebras simétricas.

Palavras chaves: Cocaracteres, Idempotente essencial, Multiplicidade.

Referências

[1] W. Q. Cota, *Álgebras com estruturas adicionais de crescimento polinomial*. Dissertação de mestrado, Programa de Pós-Graduação em Matemática, ICEx, Universidade Federal de Minas Gerais, 2021.

[2] R. B. dos Santos e A. C. Vieira, *PI-álgebras: Uma introdução à PI-teoria*, Rio de Janeiro: Editora do IMPA, 2021.

[1]Universidade Federal de Minas Gerais, breno55@ufmg.br

Equação de Klein-Gordon com fronteiras móveis: uma abordagem em coordenadas hiperbólicas

Bruno Rabelo Finóchio [1]
Helvécio Geovani Fargnoli Filho[2]

A equação de Klein-Gordon unidimensional é um modelo fundamental para a descrição de partículas escalares relativísticas. No cenário tradicional de um poço de potencial infinito com paredes fixas, as soluções são bem conhecidas e constituem uma base importante para a compreensão de sistemas quânticos confinados. No entanto, quando uma das paredes do poço se move, a situação torna-se significativamente mais complexa, uma vez que as condições de contorno passam a depender explicitamente do tempo, dificultando a separação de variáveis e a obtenção de soluções analíticas. Neste trabalho, abordamos especificamente o caso em que uma das paredes se afasta com velocidade constante. Demonstramos que, por meio de uma transformação para coordenadas hiperbólicas, é possível simplificar drasticamente a formulação do problema. Essa mudança de variáveis permite reescrever a equação de Klein-Gordon original em uma forma matematicamente tratável, na qual as variáveis podem ser separadas. Como resultado, tornou-se viável construir uma família infinita de soluções exatas, tanto para o caso massivo quanto para o caso sem massa. Esse resultado não apenas fornece um conjunto explícito de soluções para um problema com fronteira móvel, mas também evidencia o poder das coordenadas hiperbólicas como ferramenta para transformar problemas de evolução temporal com contornos dinâmicos em problemas equivalentes com contornos estáticos. Em suma, o trabalho ilustra como técnicas geométricas e transformações inteligentes podem ser empregadas para resolver problemas não triviais em física teórica, oferecendo insights valiosos para o estudo de sistemas quântico-relativísticos em contextos dinâmicos e não estacionários.

Referências

[1] M. Koehn. Solutions of the Klein–Gordon equation in an infinite square-well potential with a moving wall. arXiv:1301.0436, 2014.

[1]Universidade Federal de Lavras , bruno.finochio@estudante.ufla.br
[2]Universidade Federal de Lavras , helvecio.fargnoli@ufla.br

O Teorema de Seifert - Van Kampen

Damata, Carlos Eduardo [1]
Benedini Riul, Pedro[2]

Resumo: A topologia enquanto ciência e linguagem, tem sido um dos campos de pesquisa mais influentes e promissores da matemática do século XXI. Embora suas origens possam ser rastreadas por centenas de anos levando a França da Guerra Franco-Prussiana, foi Poincaré quem, "deu asas à topologia" em uma série clássica de artigos publicados na virada do século. [1]

Embora que, alguns conceitos que usamos hoje tenham sido cunhados por ideais matemáticos do século XIX, a topologia algébrica, que é a parte principal deste trabalho, com definições precisas e demonstrações mais coesas e corretas, só começou a ser trabalhada no início do século XX sendo relativamente nova na história.

Neste trabalho, o objetivo é estudar o Teorema de Seifert - Van Kampen, um resultado central na teoria do primeiro grupo de homotopia, mais conhecido como Grupo Fundamental. O Teorema de Seifert-Van Kampen é utilizado para determinar o grupo fundamental de um espaço topológico X que seja reunião de subespaços abertos em X, cuja interseção é conexa por caminhos e com grupos fundamentais conhecidos. Utilizando o Teorema de Seifert-Van Kampen é possível calcular o grupo fundamental de uma classe bastante grande de superfícies fechadas (orientáveis ou não).

Para este trabalho, assume-se conhecimento prévio de topologia geral e de álgebra. Para mais detalhes, consulte [2], [3].

Referências

[1] I. Stewart, *Desbravadores da matemática: Da alavanca de Arquimedes aos fractais de Mandelbrot*. Editora Schwarcz-Companhia das Letras, 2019.

[2] W. S. Massey, *A basic course in algebraic topology*, vol. 127. Springer, 2019.

[3] J. R. Munkres, *Elements of algebraic topology*. CRC press, 2018.

[1]Aluno de Graduação do Bacharelado em Matemática, Universidade Federal de São João del Rei - MG,
carlosdamata.exatas@aluno.ufsj.edu.br

[2]Professor orientador, Universidade Federal de São João del-Rei - MG, Departamento de Matemática e Estatística,
benedini@ufsj.edu.br

Implementações Didáticas de RSA e ECC-ElGamal: Uma Comparação Conceitual de Eficiência

Diego Alves[1] Carolina Cheik[2] Kailainy Silva[3] Neila Oliveira[4] Divane Dantas[5]

A criptografia desempenha papel fundamental na segurança da informação em uma sociedade cada vez mais digital. Entre os métodos assimétricos, destacam-se o RSA, baseado na dificuldade da fatoração de inteiros, e a criptografia de curvas elípticas (ECC), fundamentada no problema do logaritmo discreto em curvas elípticas [1, 2]. Este trabalho apresenta implementações didáticas em *Python* de ambos os algoritmos, utilizando parâmetros simplificados, a fim de ilustrar seu funcionamento e realizar uma comparação conceitual de eficiência em termos de tempo de execução, memória e uso de CPU. Além disso, usamos [3] nas implementações.

A segurança da informação consolidou-se como área essencial frente ao crescimento das comunicações digitais. O RSA, proposto em 1977, constitui-se como o sistema assimétrico mais difundido, enquanto a ECC, introduzida por Koblitz e Miller em meados da década de 1980, representa uma alternativa mais recente, com vantagens documentadas em termos de eficiência para níveis equivalentes de segurança [4, 5]. Diversos trabalhos comparativos evidenciam que, quando se utilizam chaves de tamanho realista, a ECC supera o RSA tanto em custo computacional quanto em memória [6].

A metodologia adotada neste estudo envolveu três etapas: implementação do RSA em *Python*, incluindo geração de chaves, codificação de mensagens e criptografia modular [7]; implementação da ECC com base no esquema de ElGamal sobre uma curva elíptica definida em corpo finito de pequena ordem [5]; e análise computacional, com medições de tempo, memória e CPU, utilizando as bibliotecas `time`, `tracemalloc` e `psutil`, em linha com estudos experimentais na área [6].

As implementações foram executadas em *Python* (versão 3.13.7), em uma máquina com processador Intel Core i7, 8 GB de RAM e sistema Windows 10 Pro, tendo como mensagem de teste a expressão **MATEMÁTICA APLICADA**. Para o RSA, cada bloco M foi criptografado por $C \equiv M^e \pmod{n}$ e decriptado por $M \equiv C^d \pmod{n}$. Já na ECC, aplicou-se o esquema de ElGamal sobre a curva $y^2 \equiv x^3 + 5x - 3 \pmod{29}$, com parâmetros $(a = 5, b = -3, p = 29)$ e ponto gerador $P = (4, 9)$, assegurando a correta recuperação do texto após a decriptação.

Os resultados médios registrados indicaram, para o RSA, tempo de execução de 17,6 s, consumo de memória $\approx$ 38,62 MB e uso de CPU entre 11% e 13%. Já o ElGamal-ECC apresentou tempo de 15,370 s, memória de 38,63 MB e uso de CPU entre 12% e 14%.

[1]dirox03@gmail.com, PUC MG
[2]carolina.cheik@gmail.com, PUC MG
[3]kailainy.aparecida@sga.pucminas.br, PUC MG
[4]neilamaragomes@yahoo.com.br , PUC MG
[5]vanedantas@yahoo.com.br, CEFET MG

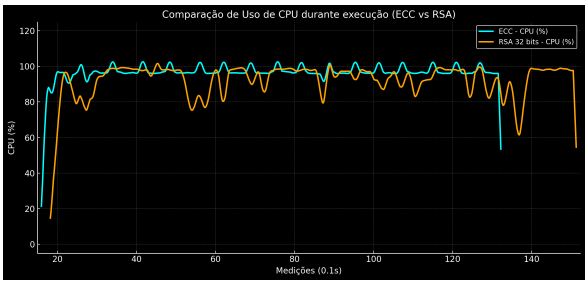


Figura 1: Gráfico Comparativo

Nestas condições simplificadas, o ECC mostrou menor tempo de execução. Além disso, conforme a literatura, quando se considera a equivalência de segurança (e.g. RSA-3072 vs ECC-256), a ECC apresenta desempenho superior, especialmente em dispositivos com recursos limitados [2, 5, 6].

Assim, este estudo cumpre um papel de ilustração conceitual, evidenciando como a escolha dos parâmetros influencia a eficiência computacional dos métodos assimétricos. Os testes realizados confirmam que, mesmo em simulações didáticas, com chaves menores, o ECC se mostra vantajoso em relação ao RSA no que se refere ao tempo de execução.

Palavras-chave: Criptografia, RSA, ECC, Matemática Aplicada, Implementação Computacional.

Referências

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Boston: Pearson, 7 ed., 2017.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Dec. 2018.

[3] S. Nakov, *Practical Cryptography for Developers*. Sofia, Bulgaria: Software University and SoftUni Foundation, 2020. PhD.

[4] N. Koblitz, *A Course in Number Theory and Cryptography*. Springer, 2 ed., 1994.

[5] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[6] Y. Banu, B. K. Rath, and D. Gountia, "Analyzing cryptographic algorithm efficiency with in graph-based encryption models," *Frontiers in Computer Science*, vol. 7, July 2025.

[7] L. S. Cerqueira Júnior, "Criptografia RSA: uma aplicação de teoria dos números," dissertação (mestrado em matemática), Universidade Federal do Recôncavo da Bahia, Cruz das Almas, BA, 2015.

Polinômios primitivos em corpos finitos

Conrado Rigotti de Carvalho [1]
José Alves Oliveira[2]

A Teoria de Corpos Finitos é uma área que vem ganhando grande importância nas últimas décadas, especialmente pela sua vasta aplicabilidade, como teoria de códigos, criptografia e combinatória. O objetivo deste trabalho é explorar os polinômios primitivos, uma classificação especial para polinômios irredutíveis, tópico de grande importância para os estudos da área, tendo como foco o Teorema 1, proposto em [1].

Teorema 1 *Um polinômio $f \in \mathbb{F}_q[x]$ de grau m é um polinômio primitivo em $\mathbb{F}_q$ se, e somente se, f é mônico, $f(0) \neq 0$ e $ord(f) = q^m - 1$.*

Também será usado para a base teórica o manuscrito [2], extraído do livro produzido pelos autores junto da professora Luciane Quoos Conte intitulado Corpos Finitos: Polinômios e Aplicações, disponível em [3], o qual também será usado.

Referências

[1] R. Lidl and H. Niederreiter, *Finite fields*, vol. 20. Cambridge University Press, 2nd. ed., 1997.

[2] F. E. Brochero Martínez, D. A. de Oliveira, and L. G. C. S. de Jesus, *Polinômios Irredutíveis sobre Corpos Finitos*. Rio de Janeiro: Editora Pi, 1a. ed., 2025.

[3] F. E. Brochero Martínez, L. Q. Conte, D. A. de Oliveira, and L. G. C. S. de Jesus, "Corpos finitos: Polinômios e aplicações." Online. Acessado em 14/08/2025, https://corposfinitos.wixsite.com/2024/publica%C3%A7%C3%B5es.

[1]Universidade Federal de Lavras, UFLA
conrado.carvalho@estudante.ufla.br
[2]Universidade Federal de Lavras, UFLA
jose_oliveira@ufla.br

Modelagem Matemática do Código Genético via Espaços Projetivos e Teoria de Designs Combinatórios

Débora Barbosa Souza [1]
Anderson José de Oliveira[2]
Cátia Regina de Oliveira Quilles Queiroz[3]

O código genético pode ser relacionado aos sistemas de comunicação digitais no sentido de armazenar e transmitir informações, estando estas sujeitas a interferências que podem acarretar mutações [1, 2]. Assim como nos sistemas digitais, essas informações precisam ser corretamente interpretadas para garantir o funcionamento adequado do organismo.

No núcleo das células encontram-se os cromossomos, responsáveis por carregar a informação genética em moléculas de DNA (ácido desoxirribonucleico). No processo de transcrição, o DNA é copiado para a formação de RNA (ácido ribonucleico), que é transportado para o citoplasma, onde será lido pelos ribossomos para a produção de proteínas. Durante a tradução, o RNA é lido em grupos de três bases nitrogenadas (adenina, guanina, citosina ou uracila - que substitui a timina presente no DNA), chamadas códons, os quais codificam os aminoácidos necessários à formação das proteínas [3].

A organização dos códons, fundamental para a síntese correta das proteínas, pode ser representada por meio de diagramas de Hasse, que os dispõem de acordo com sua associação algébrica [4]. Nesses diagramas, cada aresta corresponde à distância de Hamming entre dois códons, permitindo explorar propriedades de reticulados booleanos e identificar padrões relacionados a possíveis mutações na estrutura do DNA. Essa representação gráfica revela a ordem estrutural dos códons e sua relação com as propriedades dos aminoácidos.

A estrutura do código genético também pode ser estudada no contexto de espaços projetivos, definidos como o conjunto de todos os subespaços vetoriais de $\mathbb{F}_q^m$ e denotados por $\mathbb{P}(\mathbb{F}_q^m)$. Para a construção de códigos de subespaços, associa-se a esse espaço uma métrica, sendo adotada a distância de subespaço. É possível construir um diagrama de Hasse para $\mathbb{P}(\mathbb{F}_q^m)$ considerando a relação de ordem $\preceq$, onde $S_1 \preceq S_2$ se, e somente se, S_1 é um subespaço de S_2. Dois subespaços S_1 e S_2 estão conectados no diagrama se, e somente se, um é subespaço do outro e suas dimensões (dim) diferem exatamente em uma unidade, isto é, $dimS_2 = dimS_1 + 1 \quad$ ou $\quad dimS_1 = dimS_2 + 1$. Nesse caso, o diagrama de Hasse

[1]Universidade Federal de Alfenas, debora.souza@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, anderson.oliveira@unifal-mg.edu.br
[3]Universidade Federal de Alfenas, catia.quilles@unifal-mg.edu.br

permite interpretar a distância de subespaço entre dois subespaços como o comprimento do caminho mínimo (geodésica) que os conecta [5].

Como os códons são formados por 64 combinações possíveis, eles podem ser associados ao espaço projetivo $\mathbb{P}(\mathbb{F}_2^6)$, construído a partir do espaço vetorial sobre o corpo $\mathbb{F}_2$. Esse espaço vetorial contém todos os vetores com seis coordenadas binárias, totalizando $2^6 = 64$ vetores.

Para organizar e estudar a distribuição desses elementos, recorre-se à teoria de *designs* combinatórios, que descreve como dispor elementos de um conjunto finito em subconjuntos distintos, obedecendo a propriedades específicas [6].

Dessa maneira, o objetivo deste trabalho é estabelecer e apresentar possíveis relações entre os diagramas de Hasse do código genético e dos códigos de subespaço, recorrendo também à teoria dos *designs* combinatórios, para facilitar a análise de fenômenos biológicos e possivelmente identificar mutações genéticas, contribuindo para avanços em áreas da Matemática, Biologia e Engenharia.

Referências

[1] L. C. B. Faria, *Existências de Códigos Corretores de Erros e Protocolos de Comunicação em Sequências de DNA*. PhD thesis, Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, 2011.

[2] A. S. L. Rocha, *Modelo de sistema de comunicações digital para o mecanismo de importação de proteínas mitocondriais através de códigos corretores de erros*. PhD thesis, Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, 2010.

[3] A. Uzunian and E. Birner, *Biologia*. São Paulo: Harbra, 3 ed., 2008.

[4] R. S. Fernandes and A. J. Oliveira, "Caracterização das propriedades dos aminoácidos por meio do Diagrama de Hasse associado ao rotulamento a do código genético," *Brazilian Eletronic Journal of Mathematics*, vol. 2, no. 4, 2021.

[5] L. B. Lima, *Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana*. PhD thesis, Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, 2017.

[6] L. B. Lima and J. R. O. Moreira, "Fundamentos de design combinatórios e aplicações em códigos," *PORANDU - Revista de Divulgação Científica em Ciências Exatas e Tecnológicas*, vol. 3, no. 1, 2019.

Educação Financeira? Uma Análise Praxeológica do Livro Didático do 7^o ano

Débora Perizato [1]
Angela L. Moreno [2]

A Educação Financeira, segundo Destefani [1], é um assunto a ser discutido desde a infância e, independente da classe social em que se encontram, os pais são conscientes da importância deste tópico, sendo poucos os que consideram cedo para introduzir o assunto. Como ponto de partida, a capacitação financeira se torna o primeiro passo da Educação Financeira para desenvolver habilidades de gerenciamento do orçamento pessoal.

Durante a Educação Básica, o LD (livro didático) desempenha um papel crucial nas aulas de Matemática, funcionando como uma ferramenta que auxilia tanto professores quanto alunos na construção do conhecimento. Apesar de sua importância, muitos educadores acabam se restringindo exclusivamente ao material didático fornecido pelas escolas por ser o instrumento mais disponível nas instituições. Vale lembrar que a alta demanda e a sobrecarga dos professores também implicam na inibição de tempo hábil para uma análise minuciosa do LD a ser utilizado durante a regência e, assim como descrito por Macêdo, Brandão e Nunes ([2], p.84) "[...] a escolha do livro deixa a desejar, pois o Estado interfere de forma negativa, oferecendo aos professores poucas opções de escolha, num intervalo de tempo insuficiente para sua análise criteriosa".

Entre as diversas formas de se analisar o LD temos a Análise Praxeológica, baseada na Teoria Antropológica do Didático (TAD) introduzida por Chevallard [3] e deriva das palavras gregas: *praxis*, que significa ações e se refere ao bloco prático do saber-fazer; e *logos*, que significa a parte racional e lógica se referindo ao bloco teórico desse saber-fazer. Tal análise identifica os parâmetros tarefas(T)-técnicas(τ) (bloco prático), em que as tarefas se relacionam ao objeto do saber e exigem o uso de uma ou mais técnicas para sua execução adequada, e teoria(θ)-tecnologia(Θ) (bloco teórico), na qual a teoria fundamenta a tecnologia, que por sua vez, tem o propósito de justificar as técnicas para a execução das tarefas. Consequentemente, para identificar tanto tarefas-técnicas quanto teorias-tecnologias, é necessário analisar as habilidades descritas nos documentos oficiais norteadores, concomitantemente com a revisão dos conteúdos presentes no LD.

Deste modo, foram explorados documentos oficiais como os Parâmetros Curriculares Nacionais (PCNs) [4], Base Nacional Comum Curricular (BNCC) [5] e Currículo Referência Minas Gerais (CRMG) [6] com a finalidade de identificar habilidades que desenvolvam a capacitação financeira no 7^o Ano do Ensino Fundamental. No PCN cita a Matemática Financeira apenas quando se refere ao tema proporcionalidade e expõe um trecho sobre Matemática Comercial e Financeira com cálculo de juros simples e compostos. A revisão da BNCC elenca a habilidade EF07MA02 referente a Matemática Financeira no

[1]Departamento de Matemática, Universidade Federal de Alfenas, perizato.corp@gmail.com
[2]Departamento de Matemática, Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

7^o Ano e o CRMG separa tal habilidade em duas habilidades distintas como EF07MA02A e EF07MA02B, além de inserir as habilidades EF07MA38MG e EF07MA39MG.

Ao fim da inspeção dos documentos oficiais, a coleção escolhida para realizar a análise praxeológica foi o livro do 7^o Ano da coleção Teláris Essencial [7] e, com isso, foi desenvolvida a tabela abaixo que elenca as técnicas e respectivas tarefas.

Tabela 1: Exemplos de tarefas e suas respectivas técnicas apresentadas no LD.

Tarefa	Técnica
T_1 : Representar depósitos e saques	τ_1 : Utilizar números inteiros positivos para depósitos e números inteiros negativos para saques
T_5 : Calcular acréscimos	τ_8 : Calcular porcentagem de acréscimo usando fração na base 100 para então somar com o valor inicial τ_9 : Calcular porcentagem de acréscimo somado com 100% do que já se tinha usando fração na base 100
T_7 : Calcular inversão proporcional monetária	τ_{12} : Comparar duas grandezas analisando o fator de proporcionalidade

O LD analisado apresenta 8 tarefas e 13 técnicas com o tema Matemática Financeira e a maioria das tarefas apresentam apenas uma técnica. Não obstante, é necessário salientar que tal relação um para um de tarefa-técnica é um problema a ser enfrentado pelo professor, uma vez que é crucial ofertar múltiplos caminhos para uma melhor aprendizagem, tendo em vista que cada pessoa detém um processamento cognitivo diferente [8]. Vale considerar que durante toda a revisão, tanto dos documentos oficiais norteadores quanto do LD, não é exposto, apresentado ou debatido o tema Educação Financeira.

Referências

[1] S. M. Destefani, "Educação financeira na infância," *Revista Eventos Pedagógicos*, vol. 6(4), pp. 274–282, 2015.

[2] J. A. Macêdo, D. P. Brandão, and D. M. Nunes, "Limites e possibilidades do uso do livro didático de matemática nos processos de ensino e de aprendizagem," *Educação Matemática Debate*, vol. 3(7), pp. 68–86, 2019.

[3] Y. Chevallard, "Analyse des pratiques enseignantes et didactique des mathématiques: l'approche anthropologique," *Actes de l'UE de la Rochelle*, pp. 91–118, 1998.

[4] B. M. da Educação e do Desporto: Secretaria de Educação Fundamental., *Parâmetros Curriculares Nacionais: Matemática*. Brasília: MEC/SEF, 1998.

[5] B. M. da Educação, *Base Nacional Comum Curricular*. Brasília: MEC, 2018.

[6] SEE/MG and UNDIME-MG, *Currículo Referência de Minas Gerais*. Minas Gerais: Secretaria da Educação, 2024.

[7] L. R. Dante and F. Viana, *Teláris Essencial*. Teláris Essencial Matemática, Ática Didáticos, 2022.

[8] N. R. COUNCIL., *How People Learn: Brain, Mind, Experience, and School*. Washington: National Academies Press, 2000.

Equações Diferenciais Binárias e Geometria Diferencial

Erik Vinicius Amaro Alves [1]
Marco Antônio do Couto Fernandes[2]

Uma Equação Diferencial Binária (EDB) é uma Equação Diferencial Implícita que define até duas direções no plano. Neste trabalho tratamos de EDB's da forma

$$a(x,y)dy^2 + 2b(x,y)dydx + c(x,y)dx^2 = 0 \tag{1}$$

com a, b e c funções suaves em um aberto $U \subset \mathbb{R}^2$.

A equação das linhas de curvatura e curvas assintóticas são exemplos de EDB's da forma (1), logo é possível usar os resultados estudados para conhecer seu comportamento em superfícies [1][2]. De fato, dada uma superfície regular $M \subset \mathbb{R}^3$, tome uma parametrização local $x : U \to M$ com U aberto em $\mathbb{R}^2$. Para essa parametrização, temos que a equação das linhas de curvatura é dada por $(fE - eF)du^2 + (gE - eG)dudv + (gF - fG)dv^2 = 0$ e das linhas assintóticas é dada por $edu^2 + 2fdudv + gdv^2 = 0$, onde E, F e G são os elementos da primeira forma fundamental e e, f e g são os elementos da segunda forma fundamental [3].

Nesse trabalho, também é estudado o comportamento das EDB's das linhas de curvatura de superfícies no Espaço de Minkowski $\mathbb{R}^3_1$ [4].

Referências

[1] J. Sotomayor and C. Gutierrez., "Structurally stable configurations of lines of principal curvature," *Asterisque*, p. 195–215, 1982.

[2] J. W. Bruce and D. Fidal., "On binary differential equations and umbilics," *Proc. Royal Soc. Edinburgh, 111A*, p. 147–168, 1989.

[3] M. P. do Carmo, *Geometria diferencial de curvas e superfcies*. Textos Universitarios, Sociedade Brasileira de Matematica, 2006.

[4] S. Izumiya and F. Tari, "Self-adjoint operators on surfaces with singular," *SIAM Journal on Discrete Mathematics*, 2009.

[1]Universidade Federal de Viçosa - UFV, erik.alves@ufv.br
[2]Universidade Federal de Viçosa - UFV, marco.a.fernandes@ufv.br

NORA: Assistente Virtual

Filipe Augusto da Silva Bem [1]
Mariane Moreira de Souza [2]
Angela Leite Moreno [3]

Assistentes Virtuais Inteligentes (AVIs) têm se consolidado como ferramentas essenciais na automação de atividades cotidianas, proporcionando conveniência e eficiência em diversas tarefas do dia a dia. Com o avanço tecnológico, essas soluções, fundamentadas em inteligência artificial e aprendizado de máquina, possibilitam que os usuários realizem atividades simples, como agendar compromissos e gerenciar dispositivos domésticos, somente por meio de comandos de voz [1].

A popularidade das AVIs é evidenciada por estudos que indicam que uma parte significativa da população já as utiliza regularmente, ressaltando a percepção de que esses assistentes tornam as interações mais ágeis e simples em comparação aos métodos tradicionais. Além disso, a combinação das AVIs com a Internet das Coisas (IoT) permite a construção de residências conectadas, onde ações como acender luzes ou trancar portas podem ser realizadas remotamente. Essa automação não somente melhora a eficiência das tarefas diárias, mas também contribui para um ambiente mais seguro e controlado [2].

A motivação deste trabalho nasce da convicção de que a tecnologia, especialmente a computação, existe para facilitar e melhorar a vida das pessoas. Inspirado pela necessidade de tornar as tarefas diárias mais simples, acessíveis e eficientes, o desenvolvimento da inteligência artificial Nora busca justamente reduzir o esforço físico e mental envolvido em atividades repetitivas ou complexas. Afinal, a verdadeira razão de existir dos computadores é servir como ferramentas que ampliam as capacidades humanas, promovem inclusão e possibilitam que todos possam dedicar seu tempo e energia ao que realmente importa, seja no aspecto profissional ou pessoal.

Nesse contexto, este trabalho visa apresentar o protótipo da Nora, uma assistente virtual desenvolvida para otimizar tarefas cotidianas por meio de comandos de voz, utilizando técnicas de aprendizado de máquina e inteligência artificial. Os objetivos específicos que nortearam o desenvolvimento incluíram: investigar o uso de comandos de voz para a execução de tarefas simples e repetitivas, como buscas na internet; avaliar como a automação pode aumentar a eficiência do usuário ao permitir a realização de múltiplas tarefas simultaneamente; e examinar o potencial dos comandos de voz como ferramenta de auxílio em estudos e pesquisas. Assim, o objetivo deste trabalho é apresentar o protótipo da Nora, uma assistente virtual, desenvolvida utilizando aprendizado de máquina e inteligência artificial para otimizar tarefas cotidianas por comandos de voz.

A arquitetura do protótipo Nora foi desenvolvida em torno de um fluxo de três módulos principais: entrada, processamento e geração de resposta.

[1]Universidade Federal de Alfenas, filipe.bem@sou.unifal-mg.br
[2]Universidade Federal de Alfenas, mariane@souza.unifal-mg.br
[3]Universidade Federal de Alfenas, angela@moreno.unifal-mg.br

O processo inicia-se com o módulo de Processamento de Linguagem Natural (PLN), que lida com a entrada por voz do usuário. Quando o usuário emite um comando, a assistente primeiramente realiza uma limpeza do ruído do áudio captado para garantir maior precisão. Em seguida, o áudio limpo é convertido em texto, e o sistema reconhece a pergunta ou instrução contida nesse texto.

Uma vez que o comando é compreendido, o módulo de processamento e compreensão, focado na análise de conteúdo web, é ativado. A Nora executa uma busca no Google com base na solicitação do usuário. A partir dos resultados, o sistema é programado para extrair o texto contido no primeiro resultado considerado relevante.

Finalmente, no módulo de geração de resposta, a informação textual extraída da internet é processada e passa por uma conversão para áudio. Essa resposta sintética é então apresentada ao usuário, completando o ciclo de interação. Dessa forma, a Nora compõe um sistema que processa linguagem natural falada e retorna informação contextualizada extraída diretamente da internet.

O protótipo da assistente virtual Nora já possui uma gama funcional e diversificada de comandos. Para o controle da própria aplicação, o usuário pode pausar a captação de áudio e encerrar o programa. Na área de produtividade, a assistente pode realizar gravações, gerar relatórios e gerenciar lembretes e alarmes. Uma de suas funcionalidades mais extensas é a capacidade de abrir uma vasta lista de programas e aplicações, que vão desde ferramentas do sistema como Bloco de Notas, Calculadora, Paint e Explorador de Arquivos, até navegadores de internet como Google Chrome, Mozilla Firefox e Microsoft Edge, além de softwares de entretenimento e trabalho como Spotify, Word, PowerPoint, Excel, Discord e Steam. A Nora também pode realizar buscas na web e tocar músicas, gerenciar comunicações via WhatsApp, fazer ligações e apagar contatos, e executar ações como tirar fotos e utilizar o GPS.

O desenvolvimento do protótipo da Nora evidencia o potencial da aplicação de inteligência artificial e aprendizado de máquina para criar ferramentas que facilitam as atividades diárias. A assistente virtual consegue interpretar comandos de voz, buscar informações relevantes na internet e fornecer respostas em forma de áudio, cumprindo o objetivo de otimizar tarefas e reduzir o esforço do usuário. Os resultados atuais são promissores e estabelecem uma base para futuras expansões, como a integração com mais dispositivos e o aprimoramento da capacidade de compreensão contextual.

Referências

[1] A. J. Alencar, E. A. Schmitz, and L. T. Cruz, *Assistentes virtuais inteligentes: conceitos e estratégias*. Brasport, 2013.

[2] L. T. Cruz, A. J. Alencar, and E. A. Schmitz, *Assistentes Virtuais Inteligentes e Chatbots: Um guia prático e teórico sobre como criar experiências e recordações encantadoras para os clientes da sua empresa*. Brasport, 2019.

Caracterização das Matrizes Reais de Ordem 2, Nilpotentes de Índice 2

Francismara Fernandes Guerra [1]
Mariana Garabini Cornelissen Hoyos[2]

Nos últimos anos, o estudo das matrizes vem ganhando destaque nos livros didáticos brasileiros do ensino médio, por sua ampla aplicabilidade em diversas áreas de conhecimento. Neste trabalho, apresentamos a proposta de um recurso educacional voltado ao Ensino Médio [1]: um projeto de Iniciação Científica Júnior (PIBIC-Jr) com foco no estudo de matrizes, que pode ser utilizado por professores de Matemática para participarem dos editais de Iniciação Científica Júnior lançado pelas FAP's, CAPES, CNPq ou outras agências de fomento, estimulando assim os professores de matemática a incorporarem em seu cotidiano a pesquisa com estudantes do ensino médio, desenvolvendo o pensamento científico e o espírito questionador em seus alunos, ampliando o conhecimento deles na área de matemática e preparando-os para um futuro desempenho profissional e acadêmico através do enfrentamento e resolução de problemas. Além disso, a iniciação científica júnior também pode ser uma fonte de descobertas de novos talentos para a matemática! O objetivo do projeto é caracterizar as matrizes reais de ordem 2, nilpotentes de índice 2, com dois tipos de produtos: o produto usual de matrizes e o produto de Jordan dado por:

$$A \circ B = \frac{1}{2}(A.B + B.A)$$

onde $A.B$ e $B.A$ denotam o produto usual de matrizes.

Referências

[1] F. F. Guerra and M. G. Cornelissen, "Caracterização das matrizes reais de ordem 2, nilpotentes de Índice 2.." https://educapes.capes.gov.br/handle/capes/868700, 2024. Acesso em: 23 de junho de 2025.

[1]Intituto Federal de Minas Gerais, francismara.guerra@ifmg.edu.br
[2]Universidade Federal de São João dei-Rei, mariana@ufsj.edu.br

RSA e Phi de Euler

Gabriel Davi da Silva [1]
Osnel Broche Cristo[2]

Um dos métodos de criptografia mais utilizados e conhecidos é a criptografia RSA, que utiliza o método assimétrico, que consiste em duas etapas, ou seja, o par de chaves utilizadas para criptografar e descriptografar são diferentes, conhecidas como chave pública e chave privada respectivamente, sendo que apenas o receptor da mensagem possui a chave privada para descriptografar a mesma. Para a funcionalidade do RSA precisa-se de um número n que é o produto de dois primos distintos, utilizado para codificar e quanto maiores forem os números primos, maior será a dificuldade de se quebrar a mensagem criptografada.

Para conseguir gerar o par de chaves pública e privada no sistema RSA é necessário encontrar o valor da função Phi de Euler

$$\phi(n) = \{k \in \mathbb{Z} \mid 1 \leq k \leq n, (k, n) = 1\},$$

pois a chave pública é formada com o par de números (e, n), tal que e é invertível módulo $\phi(n)$ e a chave privada é formada por (d, n) tal que d é o inverso de e módulo $\phi(n)$[1].

Proposição: Dados dois números m e n primos relativos temos que

$$\phi(mn) = \phi(m)\phi(n).$$

Dado um número p primo e α um inteiro positivo:

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \left(1 - \frac{1}{p}\right).$$

De fato, como a $\phi(p^\alpha)$ é a quantidade de inteiros positivos não superior a p^α e relativamente primos com p^α, os únicos números positivos menores que p^α e relativamente primos com p^α são aqueles que não possuem o fator p. Observe que os números que possuem o fator p são os seguintes múltiplos: $p, 2p, 3p, ..., kp = p^\alpha$. Logo $k = p^{\alpha-1}$. Portanto, existem $p^{\alpha-1}$ inteiros não primos com p^α.

A segurança do sistema RSA [2] é dada pelo fato de que calcular $\phi(n)$ e fatorar o número n possui um custo muito elevado. Um sistema reduzido de resíduos módulo n é um conjunto de $\phi(n)$ inteiros $r_1, r_2, ..., r_{\phi(n)}$ tais que cada elemento deste conjunto é relativamente primo com n, e se $i \neq j$, então $r_i \not\equiv r_j \ (mod\ n)$.

Teorema de Euler: Dados a e n primos relativos temos que

$$a^{\phi(n)} \equiv 1 \ (mod\ n).$$

[1]Universidade Federal de Lavras
gabrielgdsdavi17@gmail.com.br
[2]Universidade Federal de Lavras
osnel@ufla.br

Demostração: Seja $r_1, r_2, ...r_{\phi(n)}$ um sistema reduzido de resíduos módulo n. Verifica-se que: $ar_1, ar_2, ..., ar_{\phi(n)}$ também é um sistema reduzido de resíduos módulo n pois, $(a, n) = 1$. Temos que

$$ar_1 \cdot ar_2 \cdots ar_{\phi(n)} = a^{\phi(n)} r_1 \cdot r_2 \cdots r_{\phi(n)} \equiv r_1 \cdot r_2 \cdots r_{\phi(n)} \ (mod\ n).$$

Como $(r_i, n) = 1$ temos que $a^{\phi(n)} \equiv 1 \ (mod\ n)$.

Com o par de chave definido, sendo a chave pública (e, n), e a chave privada (d, n), temos que dada a função $f_y(x) = x^{y \ mod\ \phi(n)} \ mod\ n$, temos que a função que encripta a mensagem m é definida por $f_e(m) = m^e \ mod\ n = M$. Como a função f_y tem a propriedade $f_y \circ f_z \equiv f_{yz}$ e $ed \equiv 1(mod\ \phi(n))$, temos que $f_d(M) = (f_d \circ f_e)(M) = (m^e)^d \ mod\ n = m^{ed} \ mod\ n = m$, sendo $f_d = M^d \ mod\ n$ a função que desencripta a mensagem encriptada, pois f_d é a função inversa de f_e.

O sistema RSA é utilizado também para assinatura de documentos [3], porém ao invés de ser apenas a utilização de uma unica função para encriptar, utiliza-se duas funções, ou seja, passa por uma dupla criptografia, primeiro com a chave privada do emissor (assinante) logo após com a chave pública do receptor (solicita a assinatura). Considere que Alice vai assinar um documento de forma remota para Bob. Sendo a chave de Alice (e, n) e (d, n) pública e privada respectivamente, e a chave de Bob (e_1, n) e (d_1, n) pública e privada respectivamente. Assim, temos que $f_e(f_{d_1}(a)) = A$, desta forma o que aparece no documento é A. Para conferir a assinatura A é realizado o processo inverso ou seja $f_{e_1}(f_d(A)) = a$. Processo análogo se Bob for assinar um documento para Alice:

$$f_{e_1}(f_d(a)) = A \quad \text{e} \quad f_e(f_{d_1}(A)) = a.$$

A segurança da criptografia RSA está relacionada na dificuldade decompor o número n e calcular o valor da função Phi de Euler. Para gerar o par de chave pública e privada é necessário que $\phi(n)$ seja conhecido. A assinatura de forma remota, facilita as assinaturas de documentos que necessita de uma certa urgencia ou um custo elevado para assinar presencialmente. Passando por duas criptografias seguidas, primerio com a chave privada, logo em seguida com a chave pública, garantindo assim um nivel maior de segurança, pois a assinatura só fara sentido ao descriptografar se for realmente realizada a criptografia pelo real emissor, pois o mesmo é o unico que possui a chave privada.

Referências

[1] A. Hefez, *Aritmética*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016. v. 08.

[2] S. Burnett, *Criptografia e segurança: o guia oficial RSA*. Gulf Professional Publishing, 2002.

[3] S. C. Coutinho, *Números inteiros e criptografia RSA*. IMPA, 1997.

O problema das sete pontes de Königsberg e uma introdução à teoria dos grafos

Gabriela Aparecida Sacramento Castro [1]
Pedro Benedini Riul[2]

Na antiga cidade de Königsberg, onde hoje se localiza Kaliningrado, na Rússia, existiam sete pontes que atrevessavam o Rio Pregel. Uma dúvida que instigava os moradores dessa cidade era se havia alguma maneira de se fazer um percurso que passasse uma só vez por cada uma das sete pontes, retornando ao local de origem. Esse problema foi solucionado pelo matemático suíço Leonhard Euler, em 1736.

Para resolver o problema, Euler simplificou o mapa da cidade da seguinte maneira: As margens do rio e as ilhas foram representadas por pontos, chamados de **vértices**, enquanto as pontes foram associadas a **arestas**. Assim, Euler encontrou uma resposta para o problema das pontes, a partir do desenvolvimento de um teorema.

A representação utilizada por Euler foi considerada o primeiro exemplo de grafo simples, que pode ser definido como um par $G = (V, A)$ em que V é um conjunto não-vazio e finito, denominado conjunto de vértices, e A é um conjunto de subconjuntos de dois elementos de V, nomeado conjunto de arestas. Dessa maneira, o teorema de Euler e os grafos foram a temática desta pesquisa, que tem por finalidade definir os principais conceitos ligados à teoria de grafos, como multigrafos, grafos complementares, caminhos e árvores.

As principais referências utilizadas são [1, 2].

Referências

[1] S. Jurkiewicz, "Grafos–uma introdução," *São Paulo: OBMEP*, 2009.

[2] J. C. V. Sampaio, *Uma introdução à topologia geométrica: passeios de Euler, superfícies, eo teorema das quatro cores*. EdUFSCar, 2008.

[1]Universidade Federal de São João del Rei, gabrielacastro2006@aluno.ufsj.edu.br
[2]Universidade Federal de São João del Rei, benedini@ufsj.edu.br

Criação de uma Base de Dados para Avaliação da Sustentabilidade e Combate ao *Greenwashing* na Moda

Heloisa Pimentel de Souza [1]
Mariane Moreira de Souza [2]
Angela Leite Moreno [3]

A sustentabilidade tem ganhado crescente destaque na indústria da Moda [1], considerada uma das mais poluidoras e consumidoras de recursos naturais no mundo. Desde a produção de matérias-primas até o descarte das peças, o setor gera impactos significativos, como poluição da água, emissão de gases de efeito estufa, uso intensivo de energia e exploração social [2]. Nesse contexto, é pertinente agrupar e consolidar informações confiáveis que permitam não somente compreender os múltiplos impactos socioambientais da Moda, como também diferenciar atividades genuinamente sustentáveis de estratégias enganosas de responsabilidade ambiental, mecanismo conhecido como *greenwashing*.

A prática de *greenwashing* consiste em ações nas quais empresas se apoiam em discursos e estratégias de divulgação que transmitem uma imagem não correspondente à realidade[3]. Na Moda, evidencia-se por meio de coleções e etiquetas ecológicas que não refletem mudanças efetivas na cadeia de produção, dificultando análises críticas e reforçando a necessidade de maior transparência no setor.

Embora existam múltiplas plataformas de código aberto utilizadas em Ciência de Dados, como o *UCI Machine Learning Repository*, *Kaggle* ou conjuntos disponibilizados pela AWS [4], não é possível encontrar bases públicas que contemplem de forma abrangente os indicadores socioambientais da indústria da Moda. Algumas iniciativas relacionadas ao assunto já existem, como o *GreenDB* [5], que expõe dados sobre atributos de sustentabilidade de produtos em geral e o *Fast Fashion Eco Commitment Dataset* [6] que contempla o catálogo da marca Zara e reúne informações de composição, preço e presença de etiquetas ecológicas em suas peças. Apesar de relevantes, esses conjuntos de dados não capturam toda a complexidade socioambiental da indústria da Moda.

Diante dessa lacuna, este trabalho propõe a construção e organização de uma nova base de dados, reunindo informações específicas sobre a indústria da Moda. Os dados coletados são advindos de relatórios de transparência com indicadores diretos, como o *Fashion Transparency Index* [7], documentos e publicações oficiais, assim como outras bases de dados menos consolidadas. As variáveis contempladas englobam indicadores que vão além dos impactos ambientais diretos, incluindo também, transparência de marca, rastreabilidade da cadeia produtiva, direitos trabalhistas e compromissos com metas sustentáveis, conforme descrito em relatórios setoriais [7] e revisões acadêmicas recentes [8].

[1]Universidade Federal de Alfenas, heloisa.pimentel@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, mariane.souza@unifal-mg.edu.br
[3]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

Esse trabalho não somente apresenta a produção de uma fonte inédita de dados a partir do uso de técnicas de ciência de dados com foco no setor da Moda, mas também reforça a importância da transparência e da responsabilização socioambiental, fornecendo subsídios para escolhas mais conscientes e para o avanço de aplicações tecnológicas baseadas em inteligência artificial [8]. Pretende-se ainda, explorar técnicas de aprendizado de máquina e modelos de inteligência artificial voltados à análise de padrões e níveis de sustentabilidade na cadeia produtiva, ampliando o potencial dessa nova base de dados para apoiar análises mais consistentes, promover maior rastreabilidade e contribuir para o combate abrangente às práticas de *greenwashing*.

Referências

[1] J. Ma, L. Huang, Q. Guo, and Y. Zhu, "Sustainability in design: sustainable fashion design practices and environmental impact using mixed-method analysis," *Business Strategy and the Environment*, vol. 33, no. 7, pp. 6889–6910, 2024.

[2] A. G. Ragab *et al.*, "Environmental impact of clothing manufacturing and the fashion industry," *Journal of Textiles, Coloration and Polymer Science*, vol. 22, no. 2, pp. 31–34, 2025.

[3] J. Adamkiewicz *et al.*, "Greenwashing and sustainable fashion industry," *Current opinion in green and sustainable chemistry*, vol. 38, p. 100710, 2022.

[4] A. Géron, *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow*. Sebastopol: "O'Reilly Media, Inc.", 2022.

[5] S. Jäger *et al.*, "Greendb: toward a product-by-product sustainability database," *arXiv preprint arXiv:2205.02908*, 2022.

[6] A. Marrodan Badell and M. Solanich Ventura, "Fast fashion eco commitment dataset," Nov. 2020.

[7] Fashion Revolution Brasil, "Fashion transparency index brazil 2024." Online. Acessado em 12/07/2025, https://www.fashionrevolution.org/fashion-transparency-index/.

[8] L. Ramos *et al.*, "Artificial intelligence and sustainability in the fashion industry: a review from 2010 to 2022," *SN Applied Sciences*, vol. 5, no. 12, p. 387, 2023.

Comparando infinitos: Quando infinitos são maiores que outros?

Iarly Evangelista Araújo [1]
Wilker Thiago Resende Fernandes [2]

Vamos partir da seguinte pergunta: todos os infinitos são iguais ou existem infinitos maiores que outros? Este trabalho tem como objetivo apresentar algumas das principais ideias desenvolvidas pelo matemático alemão Georg Cantor, no âmbito da Teoria dos Conjuntos, com ênfase na comparação entre diferentes tamanhos de infinitos. Apresentaremos também a noção de cardinalidade de conjuntos, ou seja, de quantidade de elementos de um conjunto X, denotada por $card\ X$ e de equipotência entre conjuntos, ou seja, quando dois conjuntos têm a mesma cardinalidade, denotado por $A \sim B$. Essa última diz que $A \sim B$ quando existe uma função bijetora $f : A \to B$. Um exemplo é que podemos concluir que $\mathbb{Z} \sim \mathbb{N}$, pela função bijetora $f : \mathbb{N} \to \mathbb{Z}$ dada por:

$$f(n) = \begin{cases} \dfrac{n}{2}, & \text{se } n \text{ for par,} \\ \dfrac{-(n-1)}{2}, & \text{se } n \text{ for ímpar.} \end{cases}.$$

Outro tópico abordado diz respeito à ordenação dos números cardinais. Dizemos que $card(A) < card(B)$ quando existe uma função injetora $f : A \to B$ e $A \nsim B$. Essa noção nos mostra quando um conjunto tem mais elementos que outro, em especial quando infinitos são maiores que outros, o que nos leva à famosa Hipótese do Contínuo, que afirma que não existe nenhum conjunto cuja cardinalidade esteja estritamente entre a cardinalidade de $\mathbb{N}$ e a de $\mathbb{R}$, esta ultima conhecida como cardinalidade do contínuo. Por fim mostraremos um dos resultados mais importantes da teoria, o Teorema de Cantor, que constrói uma sequência crescente de infinitos, respondendo completamente à pergunta descrita acima.

Referências

[1] E. L. Lima, *Curso de Análise*, vol. 1 of *Projeto Euclides*. Rio de Janeiro: IMPA, 15 ed., 2019.

[2] E. L. Lima, *Análise Real*, vol. 1 of *Coleção Matemática Universitária*. Rio de Janeiro: IMPA, 10 ed., 2009.

[1]Universidade Federal de São João del-Rei, iarly533@gmail.com
[2]Universidade Federal de São João del-Rei, wilker@ufsj.edu.br

[3] I. Dias and S. M. S. Godoy, "SMA0341 e SLC0603 - Elementos de Matemática: Notas de Aulas." https://www.icmc.usp.br/institucional/estrutura-administrativa/departamentos/sma/material-didatico, 2012. Acesso em 02 de agosto de 2025.

[4] T. Jech, *Teoria dos Conjuntos*. Berlim ; Heidelberg: Springer, 1997.

Classificação de Homeomorfismos no Círculo

Autor: João Paulo Cobucci de Oliveira Costa
[1]

Sistemas dinâmicos são sistemas que evoluem com o tempo ou outra variável. A teoria de sistemas dinâmicos busca entender como esse processo ocorre. Dentre os tópicos estudados, este trabalho discutirá homeomorfismos no círculo e como podemos classificar suas dinâmicas a partir de um parâmetro: o número de rotação.

Homeomorfismos são bijeções contínuas com inversa também contínua. No caso específico do círculo, isso ocorre quando seu grau é igual a 1 em módulo. Neste trabalho, iremos discutir apenas os casos nos quais o grau é igual a 1 (positivo), chamamos este último de homeomorfismo que preserva orientação. Já o número de rotação é um invariante dinâmico que pode ser usado, dentre outras coisas, para classificar homeomorfismos no círculo de acordo com a presença ou ausência de pontos periódicos.

A dicotomia mencionada acima ocorre pois, caso o número de rotação seja racional, então a dinâmica terá pontos periódicos e, caso o número de rotação seja irracional, então não teremos pontos periódicos. Ambos os casos possuem dinâmicas bem entendidas. Quando há pontos periódicos, as órbitas não periódicas tendem assintoticamente para a órbita periódica, e quando não há pontos periódicos, temos o Teorema de Classificação de Poincaré.

O Teorema de Classificação de Poincaré nos garante que, caso o homeomorfismo de número de rotação irracional seja transitivo, então a dinâmica será conjugada a uma rotação de ângulo irracional ou será semiconjugada a uma rotação de ângulo irracional, caso o homeomorfismo não seja transitivo. Para o caso não transitivo, irei discutir como podemos construir tal dinâmica e o porquê de a função que conjuga o homeomorfismo à rotação não possuir inversa.

Referências

[1] K. A. Hasselblatt B., *A First Course in Dynamics: with a Panorama of Recent Developmentsr*. Reino Unido: Cambridge University Press, 1a. ed. ed., 2003.

[1]Graduando em Matemática pela Universidade Federal de Minas Gerais - UFMG.
jpaulococ@gmail.com.br.
Orientador: José Antônio Gonçalves Miranda.
jan@mat.ufmg.br.

O Criptossistema de Chave Pública RSA

Júlia Maria dos Santos Ladeira [1]
Gustavo Terra Bastos [2]

A criptografia é um estudo que possui o objetivo de ocultar o significado de alguma mensagem. Por outro lado, a criptoanálise estuda formas de desvendar um sistema criptográfico. A data de origem da criptografia é incerta, mas estudiosos acreditam que ela surgiu logo após o desenvolvimento da linguagem escrita. Encontra-se registros das cifras sendo utilizadas na era romana e da criptoanálise sendo estudada por árabes nos séculos XIV e XV. Depois de muita pesquisa, na década de 1970, surgiu a ideia da criptografia de chave pública, cujo seus objetivos principais são fornecer recursos para que duas pessoas, mesmo sem se conhecerem, troquem informações confidenciais sem que qualquer terceiro descubra o que está sendo compartilhado, e também propocionar segurança nas assinaturas digitais.

O criptossistema RSA, publicado em 1978 e criado por Ron Rivest, Adi Shamir e Leonard Adleman, foi o primeiro criptossistema de chave pública inventado e está sendo utilizado até os dias de hoje. Além disso, seu nome é composto pela inicial do sobrenome de seus criadores. Esse sistema se baseia em teoremas como o Algoritmo Euclidiano Estendido e a Fórmula de Euler para pq, e em proposições da Aritmética Modular.

O criptossistema RSA pode ser resumido da seguinte forma: supondo que Bob e Alice queiram trocar informações, sem que uma terceira pessoa tenha acesso, Bob seleciona dois números primos p e q. Além disso, escolhe o expoente de encriptação e, com $\text{mdc}(e, (p-1)(q-1)) = 1$. Assim, ele torna público os valores $N = pq$ e e. Ao receber tais números de Bob, Alice escolhe a mensagem m e usa a chave pública de Bob (N, e) para calcular $c \equiv m^e \pmod{N}$, com isso, envia a ele o texto cifrado c.

Portanto, esse estudo irá adentrar em alguns conceitos fundamentais da Aritmética Modular, com a finalidade de explicar o funcionamento e a validade do criptossistema RSA. Além disso, será apresentado exemplos que complementarão o entendimento.

Referências

[1] C. Paar and P. Jan, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag, 2010.

[2] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics, Springer, 2a. ed., 2014.

[1]Aluna do curso de Matemática - Licenciatura da Universidade Federal de São João del-Rei, ladeira.julia03@gmail.com

[2]Professor do Departamento de Matemática e Estatística da Universidade Federal de São João del-Rei, gtbastos@yahoo.com.br

Equivalência entre as integrais de Riemann e Darboux-Riemann

Karina Geralda Gervásio [1]
Rafaela Neves Bonfim[2]

Nos cursos de Cálculo, o conceito de *Integral de Riemann* para uma função contínua definida em um intervalo fechado $[a, b]$ é introduzido utilizando a versão que é devida ao matemático francês Augustin-Louis Cauchy. Nessa versão, utiliza-se a ideia de partição do intervalo $[a, b]$. Já nos cursos de Análise Matemática, apresenta-se uma versão mais refinada, a *Integral de Darboux-Riemann*, usando conceitos de soma inferior, soma superior, integral inferior e integral superior. Essas duas definições da Integral de Riemann, embora pareçam distintas, são equivalentes, e é importante conhecer ambas as versões, uma vez que alguns teoremas são mais fáceis de serem provados usando uma ou outra definição. Portanto, este trabalho tem como objetivo central estudar as definições da Integral de Riemann conforme estudado no Cálculo Diferencial e Integral e na Análise Real, mostrando a equivalência entre essas definições.

Palavras-chave: Integral de Riemann, Integral de Darboux-Riemann, Soma inferior, Soma superior.

Referências

[1] H. L. Guidorizzi, *Um Curso de Cálculo: vol. 1.* Rio de Janeiro: LTC, 5 ed., 2013. Reimp.

[2] E. L. Lima, *Análise Real: Funções de uma Variável*, vol. 1. Rio de Janeiro: IMPA, 10 ed., 2009.

[3] G. Strang, E. Herman, *et al.*, *Calculus Volume 2.* 2016. Disponível em: https://openstax.org/books/calculus-volume-2/pages/1-introduction. Acesso em: 31 maio 2025.

[4] J. Stewart, *Cálculo: volume 1.* São Paulo: Cengage Learning, 2013.

[1]Aluna de Graduação em Matemática, Universidade Federal de São João del-Rei, karinagervasiold26@aluno.ufsj.edu.br

[2]Professora orientadora, Universidade Federal de São João del-Rei , rafaelabonfim@ufsj.edu.br

Curvas no Espaço de Lorentz- Minkowski $\mathbb{L}^n$

Laura Gois Vergueiro[1]
Pedro Benedini Riul[2]

A Teoria da relatividade de Einstein revelou as limitações da física clássica, com o surgimento do conceito de *espaço-tempo (spacetime)*, que é formalizado matematicamente por meio do *Espaço de Lorentz-Minkowski* $\mathbb{L}^4$, um espaço quadridimensional, onde a última coordenada, a temporal, é imaginária [1].

Nosso objeto de estudo é o espaço $\mathbb{L}^n = \mathbb{R}^n_1$, um espaço pseudo-euclidiano de índice 1, no qual analisamos a peculiaridade do produto interno associado a ele, que possibilita uma classificação do *tipo causal* dos vetores, sendo os tipos: *espaço (spacelike), tempo (timelike) ou luz (lightlike or null).* Conseguimos visualizar geometricamente tais tipos por meio de uma decomposição no plano $\mathbb{L}^2$, dada pelas retas $y = x$ e $y = -x$, e no espaço $\mathbb{L}^3$, pelo *cone de luz* $x^2 + y^2 = z^2$. Tal classificação também carrega uma interpretação física em relação à velocidade relativa a dois eventos, que são interpretados como pontos em $\mathbb{L}^n$.

Além disso, investigamos as curvas desse espaço. Para tanto, definimos curva parametrizada regular, sua causalidade, comprimento de arco, energia, parametrização por comprimento do arco e parametrização por arco-fóton (que é um similar para curvas de tipo luz, que modelam o movimento de partículas sem massa, como os fótons). Por fim, definimos o Diedro de Frenet, as equações de Frenet-Serret e a função curvatura para curvas em $\mathbb{L}^n$. As referências principais deste trabalho são [2] e [3].

Referências

[1] A. EINSTEIN, *Teoria da Relatividade Especial e Geral.* Contraponto Editora, 2021.

[2] A. COUTO, Ivo Terek; LYMBEROPOULOS, *Introdução à Geometria Lorentziana: Cuvas e Superfícies.* Sociedade Brasileira de Matemática, 2018.

[3] A. P. FRANCISCO, "Deformações geométricas de curvas no plano minkowski.," Master's thesis, Universidade de São Paulo, 2019.

[1]Universidade Federal de São João del Rei,
lauragoisvergueiro@aluno.ufsj.edu.br

[2]Universidade Federal de São João del Rei, Departamento de Matemática e Estatística,
benedini@ufsj.edu.br

Estimativa dos parâmetros do modelo de regresssão linear simples: uma abordagem matricial

Laura Silva [1]
Leandra Egg Campos [2]
Alysson Helton Santos Bueno[3]
Andreia Malacarne[4]
Andréa Cristiane dos Santos Delfino[5]

Resumo: O conceito de "regressão" foi introduzido por Sir Francis Galton (1822–1911) no final do século XIX, a partir de seus estudos sobre hereditariedade, especialmente na relação entre a estatura de pais e filhos. Ao analisar dados de várias famílias, Galton observou que indivíduos muito altos (acima da média populacional) tendiam a ter filhos com altura acima da média mas de estatura mais baixa que seus pais, enquanto que indivíduos muito baixos (abaixo da média populacional) tendiam a ter filhos com altura abaixo da média mas mais altos que seus pais. Dessa forma, Galton observou que pais com estaturas extremas tendem a gerar descendentes mais próximos da média populacional — o fenômeno foi descrito como *regression towards mediocrity* (regressão à média) [1] [2]. Análise de regressão é uma metodologia estatística utilizada para modelar e estabelecer relação funcional entre variáveis [3]. Neste trabalho será apresentado o método de regressão linear simples. O modelo de regressão linear simples é dado por: $Y = \beta_0 + \beta_1 X + \epsilon$, em que Y é a variável dependente; X é a variável independente ou variável regressora; β_0 é o coeficiente linear; β_1 é o coeficiente angular e o ϵ é o erro aleatório. O objetivo na regressão linear simples é definir uma reta que melhor represente a tendência central dos dados. Para tanto, é necessário determinar estimadores β_0 e β_1 de tal forma que as distâncias médias entre a reta de regressão estimada e os valores observados (desvios) em um experimento sejam mínimos. Os desvios são representados pela seguinte expressão: $\epsilon = Y - \beta_0 - \beta_1 X$. O modelo de regressão linear simples representado matricialmente é dado por: $Y = X\beta + \epsilon$ [4]. Considerando-se n observações de Y e X, tem-se o seguinte formato matricial:

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & x_1 \\ \vdots & \vdots \\ 1 & x_n \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} + \begin{bmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{bmatrix}$$

[1]UFSJ, lauraaparerecidasilva@aluno.ufsj.edu.br
[2]UFSJ, leandraegg21@aluno.ufsj.edu.br
[3]DEMEP- UFSJ, alyssonbueno@ufsj.edu.br
[4]DEMAT - UFSJ, andreiam@ufsj.edu.br
[5]DEMAT - UFSJ, andrea@ufsj.edu.br

Sendo o desvio representado por: $\epsilon = Y - X\beta$. Este trabalho tem como objetivo estimar os parâmetros do modelo de regressão linear simples por meio de uma abordagem matricial, utilizando o Método dos Mínimos Quadrados, que consiste em minimizar a soma dos quadrados dos desvios [5].

Referências

[1] S. SENN, *"Francis Galton and regression to the mean,"* Significance, v. 8, n. 3, p. 124–126, 2011. DOI: 10.1111/j.1740-9713.2011.00506.x.

[2] S. M. STIGLER, *"The History of Statistics: The Measurement of Uncertainty before 1900,"* Cambridge, MA: Harvard University Press, 1986.

[3] D. C. MONTGOMERY; E. A. PECK, & G. G. VINING, *"Introduction to Linear Regression Analysis,"* 4ª ed., John Wiley & Sons, 2009.

[4] D. C. MONTGOMERY; G. C. RUNGER, *"Estatística Aplicada e Probabilidade para Engenheiros,"* 4ª ed. Rio de Janeiro: LTC, 2009.

[5] L. G. GUIDORIZZI, *"Um curso de cálculo - volume 2,"* 6ª ed. São Paulo: Editora Ática, 2025.

Matemática e cidadania: contribuições da plataforma *Kahoot* na consolidação da aprendizagem de conteúdos matemáticos

Leonardo Jacon Gonçalves[1] , Janaína Aparecida Rossi de Sá[2] , Maria Luiza Alves Belarmino[3] , Luciana Borges Goecking[4] , Anderson José de Oliveira[5] , Franco Bassi Rocha [6]

O Projeto de Extensão Matemática e Cidadania é uma parceria entre a Universidade Federal de Alfenas (UNIFAL-MG) e o Programa Lar-Escola Zita Engel Ayer (CAZITA) e visa contribuir para a recomposição e consolidação da aprendizagem matemática de estudantes do 6º ao 8º ano do Ensino Fundamental, em situação de vulnerabilidade social, além de desmistificar a Matemática como disciplina inacessível e aproximar o conhecimento matemático de situações cotidianas.

A metodologia adotada visa criar um ambiente investigativo e acolhedor, como preconizado por [1], e as atividades desenvolvidas utilizam materiais manipuláveis, jogos didáticos, laboratório de informática e atividades dialogadas. O trabalho é conduzido por acadêmicos dos cursos de Licenciatura em Matemática e Bacharelado em Ciência da Computação, por meio de encontros semanais.

O projeto é desenvolvido desde o ano de 2016 e, em cada ano de edição, o projeto escolhe um tema central ligado ao cotidiano dos alunos e sobre o qual são explorados conceitos matemáticos com um enfoque lúdico e prático, visando a formação cidadã crítica, a interação respeitosa e inclusiva entre os participantes, além de impactar na formação dos acadêmicos envolvidos no projeto, conforme trabalhos desenvolvidos em [2], [3] e [4].

Para o ano de 2025, o tema escolhido foi sobre a água, onde pretende-se explorar a matemática da conta de água e o seu consumo consciente. E neste sentido, uma das ferramentas utilizadas para auxiliar na aprendizagem de conceitos matemáticos, foi a plataforma *Kahoot*. Tal ferramenta proporciona uma experiência de aprendizagem interativa e digital. Por meio de *quizzes* dinâmicos e desafios em tempo real, os alunos são incentivados a participar ativamente, deixando de lado o modelo tradicional de aulas, centrado apenas na lousa e no caderno. Essa estratégia torna o processo de ensino mais atrativo,

[1]Bacharelado em Ciência da Computação, Universidade Federal de Alfenas, leonardo.goncalves@sou.unifal-mg.edu.br

[2]Licenciatura em Matemática, Universidade Federal de Alfenas, janaina.sa@sou.unifal-mg.edu.br

[3]Bacharelado em Ciência da Computação, Universidade Federal de Alfenas, maria.belarmino@sou.unifal-mg.edu.br

[4]Docente do Departamento de Matemática, Universidade Federal de Alfenas, luciana.goecking@unifal-mg.edu.br

[5]Docente do Departamento de Matemática, Universidade Federal de Alfenas, anderson.oliveira@unifal-mg.edu.br

[6]Docente do Departamento de Matemática, Universidade Federal de Alfenas, franco.rocha@unifal-mg.edu.br

favorece a assimilação de conteúdos, estimula a competição saudável e contribui para o desenvolvimento de habilidades digitais.

O objetivo deste trabalho é apresentar um breve relato de experiência acerca da utilização da plataforma *Kahoot* no processo de ensino e aprendizagem das operações matemáticas fundamentais e os impactos da realização desta atividade, tanto para os alunos atendidos pelo projeto, quanto para os acadêmicos em seu processo de formação.

Ao utilizar o *Kahoot*, foi notória a mudança de comportamento dos alunos, uma vez que a matemática, normalmente vista pelos alunos como algo negativo, ganhou destaque, por meio de uma atividade divertida, despertando a atenção e fomentando um ambiente propício para o aprendizado.

O jogo consistia numa série de perguntas que, quando respondidas corretamente, geravam pontos para o aluno e, ao final, os participantes eram ranqueados com base na pontuação. As perguntas giravam em torno da matéria do sétimo ano do Ensino Fundamental, focando em divisão, multiplicação e frações, utilizando diversas estratégias, como fotos e representações geométricas, todas relacionadas ao tema da água, visando estimular a utilização dos conceitos previamente apresentados durante as aulas.

Desta forma, a utilização do *Kahoot* trouxe contribuições significativas à dinâmica das atividades desenvolvidas, colaborando para aprofundar o aprendizado dos conceitos matemáticos, despertar a curiosidade e engajamento dos alunos, fornecer aos mesmos uma nova forma de aprender matemática além de incentivar os acadêmicos a buscarem novas ideias e novas ferramentas que possam tornar as aulas de Matemática mais criativas e interessantes.

Agradecimentos

À UNIFAL-MG, à PROEC e ao Lar-Escola Zita Engel Ayer - CAZITA.

Referências

[1] O. Skovsmose, *Educação Crítica: incerteza, matemática, responsabilidade*. São Paulo: Cortez, 2007.

[2] A. C. Oliveira, A. M. Melo, L. B. Goecking, L. A. Beijo, and A. J. Oliveira, "Matemática para a cidadania: Calculando perímetro e área em situações do cotidiano," *Revista Extensão e Cidadania*, vol. 8, pp. 211–227, 2020.

[3] N. H. Silva, L. B. Goecking, and A. J. Oliveira, "Matemática e cidadania: Tecnologias da informação e comunicação aplicadas no consumo consciente de combustíveis," *Revista Conexão UEPG*, vol. 17, pp. 1–13, 2021.

[4] C. V. Oliveira, L. B. Goecking, A. J. Oliveira, and F. B. Rocha, "Matemática e cidadania: um estudo comparativo entre a matemática da 'feira' e a matemática da sala de aula," *SIGMAE*, vol. 13, pp. 85–98, 2024.

Fundamentos do Criptossistema de Chave Pública Elíptico Elgamal

Letícia Maria da Silva [1]
Gustavo Terra Bastos[2]

Desde que a humanidade começou a desenvolver a linguagem escrita, a criptografia é usada de uma maneira ou de outra em muitas culturas. Com o tempo, a criptografia, como todas as ciências, foi se desenvolvendo. Até 1970, esta era usada prioritariamente em aplicações diplomáticas, militares e governamentais. A partir de 1980, a criptografia passa a ser amplamente utilizada pelas indústrias financeiras e de telecomunicações. [1, p. vii].

Atualmente, a criptografia está presente em vários objetos e aspectos do cotidiano, por exemplo: no dispositivo de controle remoto de um carro, no cartão de crédito ou débito, ao instalar uma atualização de software, na utilização de navegadores da Web, nos programas de e-mail etc. [1, p. vii-ix], ou seja, existem vários sistemas de criptografia que são utilizados com os mais variados objetivos.

Em 1985, os matemáticos Neal Koblitz e Victor Miller propuseram que o *Problema do Logaritmo Discreto em Curvas Elípticas* poderia ser mais complexo do que o *Problemas do Logaritmo Discreto módulo p*, com a possibilidade de ser mais eficiente do que o RSA (primeiro sistema de criptografia de chave pública inventado). Desse modo, antes de adentrar em sistemas de criptografia de curvas elípticas, precisamos entender alguns conceitos como "Curvas Elípticas", segundo Weierstrass, "Troca de Chaves Elípticas de Diffie–Hellman" e "Problema do Logaritmo Discreto em Curvas Elípticas", para então compreender um "Criptossistema de Chave Pública Elíptico ElGamal".

Assim, nesse contexto, se dois indivíduos desejam estabelecer uma comunicação segura e privada, eles podem optar pelo criptossistema mencionado acima. Neste sistema de criptografia, eles deverão acordar uma curva elíptica; em seguida, após alguns cálculos, os indivíduos trocam pontos desta curva que, na verdade, será o mesmo. A esse ponto chamamos de *chave pública*. Com essa chave, eles poderão encriptar mensagens e se comunicar secretamente, como desejaram. Portanto, nesse projeto, apresentaremos os conceitos básicos de curvas elípticas, troca de chaves de curvas elípticas e criptosistema elíptico Elgamal que levam a segurança e privacidade que os indivíduos buscam.

Referências

[1] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Heidelberg: Springer-Verlag, 2010. Printed on acid-free paper.

[1]Universidade Federal de São João del-Rei, ls3536358@aluno.ufsj.edu.br
[2]Universidade Federal de São João del-Rei, gtbastos@yahoo.com.br

[2] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. Undergraduate Texts in Mathematics, New York: Springer, 2 ed., 2014.

Jogo Pedagógico Agência M^2 (Mentes Matemáticas)[1]

Lucas Cruz [2]
Evandro Monteiro[3]

A transição da aritmética para o pensamento algébrico constitui um dos marcos mais significativos e, frequentemente, um dos maiores desafios no percurso educacional dos estudantes. Dentro deste campo, os sistemas de equações emergem como uma ferramenta de extraordinário poder analítico, mas também como uma fonte recorrente de dificuldades de aprendizagem. A importância de dominar este tópico transcende as fronteiras da disciplina de matemática, pois representa uma competência essencial para a modelagem de problemas complexos e para o desenvolvimento do raciocínio lógico estruturado. Um sistema de equações, definido como um conjunto de duas ou mais equações com múltiplas incógnitas, que devem ser satisfeitas simultaneamente, ensina o aluno a trabalhar com diversas restrições para encontrar uma solução única, espelhando a natureza multifacetada de muitos desafios do mundo real [1].

Apesar de sua relevância, a aprendizagem de sistemas de equações é frequentemente marcada por obstáculos, sendo o principal deles a tradução da linguagem verbal para a linguagem algébrica, um processo de modelagem que exige interpretação e abstração [2]. Diante deste cenário, o presente trabalho detalha a concepção e a estrutura do "Agência M^2 (Mentes Matemáticas)", um Jogo de Interpretação de Papéis (RPG) pedagógico, projetado para atacar diretamente essas dificuldades.

A abordagem de aprendizagem baseada em jogos surge como uma poderosa estratégia para superar a desconexão entre a teoria e a prática. Em vez de apresentar a matemática como um conjunto de regras a serem memorizadas, os jogos criam um ambiente onde o conhecimento é uma ferramenta necessária para atingir um objetivo engajador, transformando a motivação extrínseca em intrínseca [3]. O formato de RPG é particularmente eficaz, pois os alunos são imersos em uma narrativa que dá propósito a cada ação. O jogo "Agência M^2 (Mentes Matemáticas)" utiliza essa estrutura para criar uma necessidade genuína pela matemática, funcionando como um complemento à instrução teórica, onde os conceitos aprendidos são aplicados e consolidados. A estrutura do jogo coloca as equipes para solucionar um crime através da decifração de pistas que são, em essência, problemas matemáticos. A solução numérica encontrada não é um fim em si mesma, mas a chave que revela uma evidência concreta, atacando diretamente as dificuldades de aprendizagem, ao tornar a tradução mecânica em tradução interpretativa da história. A eficácia pedagógica

[1]Agradecemos à UNIFAL-MG, ao PROFMAT, à CAPES e à FAPEMIG.
[2]Universidade Federal de Alfenas ,
lucashenrique.cruz@sou.unifal-mg.edu.br
[3]Universidade Federal de Alfenas,
evandro.monteiro@unifal-mg.edu.br

desta abordagem é profundamente sustentada pela Teoria Sociocultural de Lev Vygotsky, o jogo cria um ambiente que é uma manifestação prática de seus conceitos, onde os enigmas são projetados para se situarem na Zona de Desenvolvimento Proximal (ZDP) dos alunos – desafiadores, mas solucionáveis com a colaboração em equipe e a mediação do professor-mestre. A matemática funciona como uma ferramenta de mediação semiótica, sendo a interação social para resolver os problemas, o motor da aprendizagem [4]. Adicionalmente, o projeto estabelece uma conexão rigorosa com a Base Nacional Comum Curricular (BNCC), desenvolvendo tanto as competências gerais, pensamento crítico e argumentação, quanto as habilidades específicas de matemática, com foco na EF08MA08 (sistemas de equações de 1º grau) e EF09MA09 (equações de 2º grau) [5].

Este trabalho tem como objetivo analisar e apresentar o jogo de investigação "Agência M^2 (Mentes Matemáticas)" como uma ferramenta pedagógica de aprendizagem ativa, com o propósito de promover uma compreensão mais significativa e engajadora da modelagem e resolução de sistemas de equações de equações para alunos do nono ano do Ensino Fundamental.

A construção deste projeto foi embasada por uma revisão bibliográfica sistemática, com buscas em bases de dados acadêmicas, utilizando descritores como "RPG pedagógico", "ensino de álgebra"e "sistemas de equações", cujos artigos foram selecionados por critérios de relevância, qualidade e alinhamento teórico. O sistema de avaliação proposto para o jogo reflete sua natureza pedagógica, sendo um modelo híbrido que combina uma avaliação quantitativa, que equilibra a precisão do desempenho com a agilidade na resolução, e uma avaliação qualitativa, baseada na observação do professor sobre a colaboração e o raciocínio da equipe.

É fundamental ressaltar que este documento apresenta uma proposta de pesquisa em sua fase de concepção, o jogo "Agência M^2 (Mentes Matemáticas)", seus materiais e sua metodologia foram integralmente desenhados e estão prontos para a fase de testes. No entanto, a aplicação prática com os estudantes e a coleta de dados empíricos sobre seu impacto ainda não foram realizadas, pois o projeto aguarda aprovação por um Comitê de Ética em Pesquisa. As conclusões sobre a eficácia do jogo são, portanto, projeções teóricas que aguardam validação empírica.

Referências

[1] L. R. Dante, "Matemática: contexto e aplicações," *São Paulo: Ática*, vol. 2, 2013.

[2] R. C. LINS, "Gimenez, joaquim. perspectivas em aritmética e álgebra para o século xxi," 1997.

[3] M. Prensky, "Digital game-based learning," *Computers in entertainment (CIE)*, vol. 1, no. 1, pp. 21–21, 2003.

[4] L. S. Vygotsky *et al.*, "A formação social da mente," *São Paulo*, vol. 3, 1984.

[5] Brasil, *Base Nacional Comum Curricular*. Brasília: MEC, 2018.

CombineQuests: integrando gamificação ao ensino de Análise Combinatória

Lucas Pessoa Oliveira Alves [1]
Anderson José de Oliveira[2]
Luiz Eduardo da Silva[3]

O ensino de Matemática, especialmente na Educação Básica, ainda é fortemente marcado por metodologias tradicionais que privilegiam a memorização de fórmulas e a resolução mecânica de exercícios, em detrimento da compreensão conceitual e do desenvolvimento do pensamento crítico. Esse cenário contribui para altos índices de desmotivação e baixo desempenho escolar, agravando-se em conteúdos mais abstratos, como a Análise Combinatória, que exige raciocínio lógico e domínio de técnicas específicas. A apresentação descontextualizada desses conceitos frequentemente afasta o estudante, tornando o aprendizado pouco significativo.

Nas últimas décadas, observa-se um crescente interesse por metodologias ativas e recursos tecnológicos que promovam maior engajamento discente. Entre eles, destacam-se os Jogos Educacionais Digitais (JEDs) e a gamificação, que incorporam elementos como desafios, pontuação e *feedback* imediato para tornar o aprendizado mais motivador e interativo [1, 2]. Diversos estudos evidenciam os benefícios dessa abordagem no ensino de Matemática: o jogo "Sofia e suas roupas" aumentou em 40% o engajamento de alunos na Análise Combinatória [3], enquanto iniciativas em probabilidade e contagem também mostraram ganhos em desempenho e motivação [4, 5]. Além disso, revisões sistemáticas [6, 7] apontam que, quando alinhados aos objetivos pedagógicos, os JEDs favorecem a aprendizagem significativa [8] ao integrar novos conceitos às experiências prévias do aluno.

Apesar dessas evidências, ainda há lacunas quanto à aplicação prática de JEDs no ensino da Análise Combinatória e à disponibilidade de materiais interativos voltados para esse conteúdo, especialmente no Ensino Médio. Nesse contexto, este trabalho tem como objetivo investigar o potencial pedagógico dos Jogos Educacionais Digitais no ensino de Análise Combinatória, por meio do desenvolvimento do jogo CombineQuests - um recurso lúdico e interativo voltado tanto para alunos do Ensino Médio quanto do Ensino Superior. O jogo, em estilo *top-down* e desenvolvido na engine *GameMaker Studio 2*, contará com mecânicas que transformam problemas combinatórios em desafios narrativos, incorporando elementos de gamificação como progressão por níveis e *feedback* imediato. Sua fundamentação pedagógica se apoia na teoria da Aprendizagem Significativa [8], buscando contextualizar e tornar tangíveis os conceitos de princípio fundamental da contagem, permutações, combinações e arranjos.

[1]Universidade Federal de Alfenas , lucas.pessoa@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas , anderson.oliveira@unifal-mg.edu.br
[3]Universidade Federal de Alfenas , luiz.silva@unifal-mg.edu.br

A validação será realizada com base na heurística HEDEG [9], avaliando aspectos como usabilidade, engajamento e clareza pedagógica. O projeto encontra-se atualmente em fase de desenvolvimento, com etapas de criação de artes, elaboração dos desafios e implementação das mecânicas centrais já em andamento. Espera-se que o CombineQuests contribua para aumentar a motivação e facilitar a compreensão dos conceitos combinatórios, além de fornecer um estudo de caso para futuras pesquisas sobre o uso de jogos digitais no ensino de Matemática.

Referências

[1] R. B. Japiassu and C. D. A. Rached, "A gamificação no processo de ensino-aprendizagem: uma revisão integrativa," *Revista Educação em Foco*, vol. 12, no. 1, pp. 49–60, 2020.

[2] V. T. Soares, "Jogos digitais e o ensino-aprendizagem: gamificação," *Revista Santa Rita*, no. 34, pp. 20–26, 2020.

[3] R. Rostirolla *et al.*, "Sofia e suas roupas: um jogo para o ensino de análise combinatória," in *Anais do Congresso Brasileiro de Ensino de Matemática*, 2022.

[4] F. Vasconcelos *et al.*, "Jogos digitais no ensino de probabilidade," *Revista Brasileira de Informática na Educação*, 2018.

[5] J. Oliveira and A. Silva, "Jogo digital para o ensino de análise combinatória," *Revista de Ensino de Matemática*, 2019.

[6] S. S. Ferreira and A. C. B. Rocha, "Contribuição de jogos digitais no ensino de matemática: revisão sistemática da literatura," *Revista Foco*, vol. 17, no. 8, p. e2193, 2024.

[7] J. F. S. da Costa, "Jogos digitais e matemática no ensino fundamental: uma revisão sistemática," *Jornal Internacional de Estudos em Educação Matemática*, vol. 17, no. 2, pp. 159–170, 2024.

[8] D. P. Ausubel, *Aquisição e retenção de conhecimentos: uma perspectiva cognitiva*. Lisboa: Plátano, 2003.

[9] P. H. D. Valle *et al.*, "Hedeg: heurística para avaliação de jogos educacionais digitais," in *TISE – Nuevas Ideas en Informática Educativa*, vol. 12, pp. 247–256, 2013.

Evolutóides de curvas planas e função suporte

Luiz Fernando Saldanha Vieira [1]
Ady Cambraia Junior[2]
Alessandro Gaio Chimenton[3]

Resumo: O estudo das propriedades geométricas dos evolutóides de curvas planas e suas singularidades tem aplicações em diferentes áreas como Física, Computação e Engenharia. Nosso trabalho visa explorar conceitos e propriedades sobre o envelope de retas de curvas que fazem ângulo fixado com a reta tangente em cada ponto da curva $\gamma(t) : [0, L] \to \mathbb{R}^2$, que consideramos suaves, fechadas e estritamente convexas.

Inicialmente, estudamos o conceito de evolutas como o lugar geométrico das interseções de retas normais próximas, ou seja, o envelope de curvas perpendiculares a γ, seguindo as definições de Giblin [1]. Em seguida, para cada ângulo fixado, foi deduzida uma parametrização do evolutóide com a qual, usando funções suporte de curvas, deduzimos fórmulas para o comprimento e a área dos evolutóides, inspirados nos trabalhos de Jerónimo-Castro [2]. Esta parametrização pode ser descrita por:

$$\gamma_\alpha(t) = p_\alpha(t)u(t) + \dot{p}_\alpha(t)\dot{u}(t) \tag{1}$$

em que p_α representa a função suporte do evolutóide γ_α.

O trabalho apresenta propriedades dos evolutóides de curvas planas por meio do uso da função suporte, estabelecendo relações entre suas áreas e comprimentos com os da curva original, como visto abaixo nos seguintes teoremas

Teorema 1 *Seja γ uma curva convexa e fechada de classe C^2 no plano e seja $\alpha > 0$ um número suficientemente pequeno para que γ_α seja uma curva convexa. Então*

$$A(\gamma_\alpha) \leq \cos^2 \alpha \cdot A(\gamma)$$

com igualdade se, e somente se γ for uma circunferência euclidiana.

Teorema 2 *Seja γ uma curva convexa, fechada e suave no plano e seja $\alpha \in (0, \pi/2)$. Então*

$$L(\gamma_\alpha) = \cos \alpha \cdot L(\gamma)$$

[1]Universidade Federal de Viçosa , luiz.fernando.viera@ufv.br
[2]Universidade Federal de Viçosa, ady.cambraia@ufv.br
[3]Universidade Federal Fluminense , alessandrogaio@id.uff.br

Um dos principais resultados é a caracterização dos círculos como as únicas curvas cujos evolutóides também são círculos para todo ângulo fixado, conforme o seguinte teorema:

Teorema 3 *Seja γ uma curva convexa, fechada e diferenciável no plano e seja $\alpha \in (0, \pi/2)$. Então γ é círculo se, e somente se, γ_α for um círculo.*

Referências

[1] P. J. Giblin and J. P. Warder., "Evolving evolutoids," *The American mathematical Monthly*, 2014.

[2] J. Jerónimo-Castro, "On evolutoids of planar convex curves," *Springer Bases*, 2013.

Convergência de sequências: da reta real ao conceito de vizinhança

Luiz Gustavo Silva Prata [1]
Daiane Alice Henrique Ament[2]

Ao analisar a convergência de uma sequência X_n que converge para um ponto a na reta real escolhe-se um ε arbitrário que vai ser uma "barreira" que vai de a - ε até $a + \varepsilon$ e de um momento em diante "X_n vai estar ε próxima de a", ou seja, X_n entra no intervalo já citado e não sai mais. Abstraindo-se um pouco mais, ao analisar agora espaços vetoriais normados com a norma euclidiana, pode-se observar que a definição é muito similar, a ideia agora é que o ε escolhido para ser a barreira vai ser o raio de uma bola centrada no ponto a, então vamos ter que a partir de dado momento a sequência X_n entra nessa bola e não sai mais. Usando as definições de distâncias podemos generalizar esse conceito de convergência de sequências para os espaços métricos como sendo " $\mathrm{d}(X_n, a) < \varepsilon$ ", depois generalizando novamente, agora sem usar o conceito de métrica ficaremos com "$X_n \in B_\varepsilon$ (a)", ou seja, uma bola de raio ε com todos os pontos cuja a distância até o ponto a seja menor do que ε. A partir de agora, dada uma família de todas as bolas centradas em a, de um momento em diante se X_n estiver dentro de uma bola para todas as bolas, afirmamos que X_n converge para o ponto a. A última abstração, é que para cada ponto do conjunto das bolas escolhe-se uma família que será chamada de vizinhança e para saber se X_n converge para a deve ser provado que para toda vizinhança de a, temos que a sequência X_n eventualmente esta dentro dessa vizinhança. Logo, se for escolhida uma família que contém não só bolas, inclusive um conjunto que contem mais elementos que a bola, a sequência eventualmente tem que entrar nesse conjunto também e não sair mais.

Referências

[1] E. L. Lima, *Espaços métricos*. Rio de Janeiro: RJ: CNPq, 1977.

[2] H. H. Domingues, *Espaços métricos e introdução à topologia*. São Paulo: Atual, 1982.

[3] E. L. Lima, *Elementos de topologia geral*. Rio de Janeiro: RJ: Ao livro técnico, 1970.

[1]Universidade Federal de Lavras , luiz.prata@estudante.ufla.br
[2]Universidade Federal de Lavras, daiane.ament@ufla.br

Infinitude de números primos via Teorema de Lagrange

Luiz Gustavo Silva Prata [1]
José Alves Oliveira [2]

O Teorema de Lagrange, que é um resultado de grande importância dentro da teoria dos grupos finitos, afirma que a ordem de qualquer elemento de um grupo finito deve dividir a ordem total desse grupo. Essa propriedade, embora de caráter abstrato e teórico, tem aplicações significativas, principalmente no campo da teoria dos números. Por exemplo, é possível utilizar esse teorema para demonstrar, de forma rigorosa, que o conjunto dos números primos é infinito. O raciocínio por trás dessa demonstração faz uso de resultados obtidos a partir da teoria dos grupos e da noção de divisibilidade, e é uma das muitas maneiras pelas quais a álgebra abstrata pode ser utilizada para resolver problemas clássicos da aritmética, uma área da matemática focada no estudo dos números inteiros e suas propriedades. Essa aplicação do Teorema de Lagrange revela, portanto, uma conexão profunda e poderosa entre diferentes ramos da matemática, mostrando como conceitos que surgem em um contexto abstrato e teórico, como os grupos finitos e suas ordens, podem ser usados para resolver problemas aparentemente distantes da álgebra, mas que estão intimamente relacionados ao estudo da aritmética e da estrutura dos números.

Referências

[1] DOMINGUES, HYGINO. H.; IEZZI, GELSON . *Algebra Moderna* . 4. ed. reformul. São Paulo: Atual, 2003. 368 p.

[2] HEFEZ, ABRAMO . *Curso de Álgebra, Volume 1*. Rio de Janeiro: IMPA, 2024. 268p.

[3] GONÇALVES, ADILSON . *Introdução à Álgebra*. 6.ed, Rio de Janeiro: IMPA, 2017, 192p.

[1]Universidade Federal de Lavras , luiz.prata@estudante.ufla.br
[2]Universidade Federal de Lavras , jose_oliveira@ufla.br

Estratégias para Balanceamento de Classes no BRSET: Um Estudo de Caso em Retinopatia Diabética

Maicon Almeida Mian[1]
Angela Leite Moreno[2]

O BRSET (*A Brazilian Multilabel Ophthalmological Dataset*) é um banco de dados brasileiro que reúne mais de dezesseis mil imagens de fundo de olho, com foco em doenças relacionadas ao diabetes [1]. Entretanto, o treinamento de modelos médicos sobre esses dados é desafiador, uma vez que a distribuição das classes costuma ser desbalanceada. No caso específico da retinopatia diabética, somente cerca de 6,58% das imagens do BRSET são rotuladas como positivas para a doença. Dessa forma, esse trabalho busca avaliar o desempenho de estratégias para lidar com esse desbalanceamento entre classes.

Assim, foi escolhida a rede neural convolucional, por se tratar de imagens, a qual foi estruturada em seis blocos, cada um contendo uma camada convolucional, com número de filtros variando de 128 a 16, sendo que alguns incluiram *max pooling* e *batch normalization*, seguido por um bloco contendo uma camada densa final, responsável pela classificação, com 128 neurônios, utilizando Adam como otimizador.

Das 16.266 imagens, 70% foram divididas para treino (das quais 15% foram alocadas para validação) e 30% para testes. As métricas avaliadas foram Acurácia, Sensibilidade, Precisão, F1-*Score*, AUC-ROC (*Area Under the Curve of the Receiver Operating Characteristic*) e Especificidade. Também ajustou-se o *threshold* T com base no F$_\beta$-*Score* ($\beta = 1,5$) em todas as técnicas para avaliar possíveis ganhos de desempenho.

Desse modo, as estratégias adotadas seguiram a abordagem de tratamento de dados proposta por Johnson e Khoshgoftaar [2]. Na primeira fase, utilizaram-se as estratégias de *undersampling* (U), redução de amostras negativas, e *oversampling* (O), aumento de amostras positivas, simples, ambas realizadas de forma aleatória, buscando deixar as classes com o mesmo número de imagens. O treinamento foi limitado a 30 épocas, com parada antecipada (*early stopping*) pelo valor de sensibilidade (paciência de 3 épocas) para evitar o *overfitting* e salvamento do modelo quando a sensibilidade aumentava. Observou-se nesta abordagem, que ao se ter a sensibilidade de 100%, o modelo não conseguia melhorar, fazendo com que o resultado se tornasse enviesado.

Na segunda fase, para resolver este problema, os modelos foram treinados por no máximo 30 épocas, mas com parada antecipada baseada no valor de AUC-ROC (paciência de 3 épocas) e salvamento contínuo, permitindo um melhor equilíbrio entre sensibilidade e especificidade. Também foi introduzido o tratamento dos dados antes de se iniciar o treinamento da rede, utilizando o algoritmo do *K-means*, agrupando as imagens a terem sua quantidade aumentada ou diminuída em grupos de 20 *clusters*, garantindo a preservação dos padrões originais. Assim, as estratégias adotadas nessa fase foram *undersampling*

[1]Universidade Federal de Alfenas, maicon.mian@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

com *clusterização* (UC) e *oversampling* com clusterização (OC). Os resultados obtidos em ambas as fases podem ser vistos na Tabela 1.

Métrica	Fase 1				Fase 2			
	U		O		UC		OC	
	0.5 T	0.51 T	0.5 T	0.93 T	0.5 T	0.51 T	0.5 T	0.63 T
Acurácia (%)	58,30	81,76	77,93	94,12	83,40	84,71	91,31	92,73
Sensibilidade (%)	63,86	34,89	85,67	62,31	45,17	42,68	73,21	67,60
Especificidade (%)	57,91	85,06	77,39	96,36	86,09	87,67	92,59	94,49
Precisão (%)	9,65	14,12	21,06	54,64	18,61	19,60	41,01	46,37
F1-*Score* (%)	16,77	20,11	33,80	58,22	26,36	26,86	52,57	55,01
AUC-ROC	0,6614	0,6614	0,8974	0,8974	0,6999	0,6999	0,9008	0,9008

Tabela 1: Tabela das Métricas de Erro.

A Tabela 1 indica que os métodos ainda podem ser aprimorados, sugerindo que ajustes na arquitetura ou nos parâmetros do modelo podem levar a ganhos de desempenho. Entretanto, mesmo com esse percurso, é possível identificar quais técnicas ajudaram a contornar o problema de classe desbalanceada. Comparando as fases, o *oversampling* (O e OC) apresentou um balanceamento melhor das métricas entre uma fase e outra antes do ajuste do *threshold*, mantendo valores muito próximos após a sua alteração. Já o *undersampling* (U e UC) mostrou uma melhora interessante, com as métricas realmente mais balanceadas, mesmo com a sensibilidade mais baixa. Isso se deve, em grande parte, porque o corte feito no *undersampling* era muito brusco, com muitos dados sendo perdidos, e a *clusterização* provavelmente ajudou a manter o padrão.

Avaliando agora os métodos, no *oversampling*, os resultados foram mais promissores, com AUC-ROC elevado. Na versão simples (O), observou-se sensibilidade alta, embora perda de precisão, e o *threshold* de 0,93 foi o único que manteve todas as métricas acima de 50%. A versão da fase 2 (OC) teve seus valores bem balanceados antes mesmo do ajuste do *threshold*.

Dessa maneira, os resultados evidenciaram fatos interessantes: favorecer a classe minoritária revelou-se mais vantajoso do que reduzir a classe majoritária, e o treino com AUC-ROC e clusterização deixou os valores mais balanceados sem necessitar da alteração do *threshold*. A principal consequência foi o custo computacional: no caso do *oversampling*, o treino com 8.360 imagens negativas e a duplicação da classe minoritária resultou em um conjunto de treino com 16.720 imagens, aumentando o tempo de treinamento.

Para trabalhos futuros, pretende-se avaliar se a arquitetura da rede neural é a mais adequada. Também será investigada a combinação de técnicas, além de modelos pré-treinados.

Referências

[1] L. F. Nakayama, *Criação de um banco de dados Brasileiro de retinografia com objetivo de reduzir vieses em aplicações de inteligência artificial*. PhD thesis, Universidade Federal de São Paulo – Escola Paulista de Medicina, 2024.

[2] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *Journal of Big Data*, vol. 6, no. 27, pp. 1–54, 2019.

Interpolação Numérica: Uma Análise Comparativa entre Newton, Lagrange e *Cubic Spline*

Maicon Almeida Mian[1]
Pedro Henrique Botelho da Silva[2]
Vinicius Henrique Piotto Boiago[3]
Angela Leite Moreno[4]

Este trabalho apresenta uma análise dos métodos de interpolação de Newton, Lagrange e *Cubic Spline* [1], focando em critérios de precisão, desempenho computacional e estabilidade. O objetivo é investigar a adequação de cada algoritmo para diferentes cenários de aplicação.

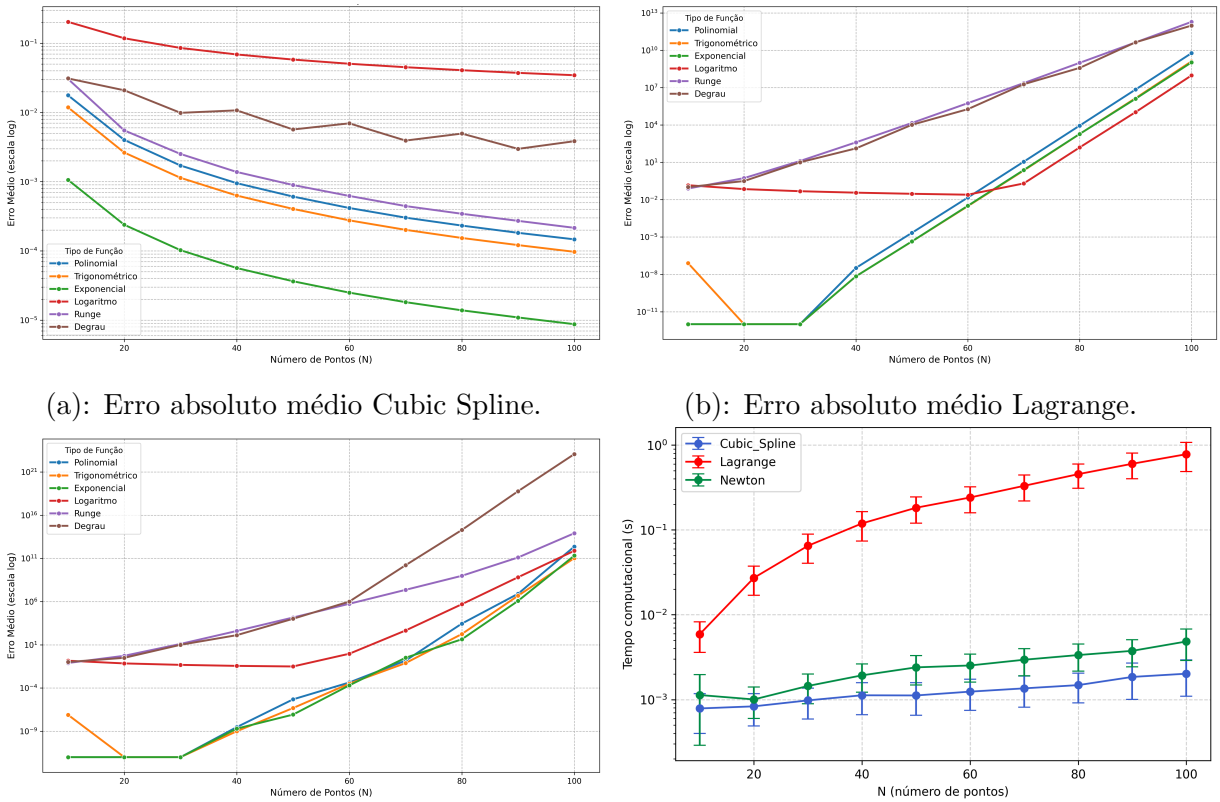
Para esta avaliação, os métodos foram aplicados a um conjunto de funções, incluindo polinomiais, trigonométricas, exponenciais, logarítmicas, a função de Runge e uma função degrau. Utilizando os valores reais das funções no intervalo de $[-1, 1]$, com o número de pontos de amostragem (N) variando de 10 a 100, com incrementos de 10. Para cada configuração, a análise quantificou duas métricas: o tempo de avaliação sobre 10.000 iterações com pontos e a precisão mensurada através do erro absoluto médio. Os testes foram realizados em uma máquina com um AMD Ryzen 5 5500U, 20GB de RAM sob o Fedora 42.

Os resultados revelam comportamentos distintos entre os métodos. O método *Cubic Spline* demonstrou convergência, na qual o erro absoluto médio diminuiu com o aumento do número de pontos (N) para as funções contínuas testadas, como pode ser visto na Figura 1(a).

Em contrapartida, os métodos baseados em um polinômio de grau elevado, Newton e Lagrange, exibiram instabilidade numérica. Para a maioria das funções, observa-se divergência no erro a partir de $N \approx 70$ (Lagrange – Figura 1(b)) e $N \approx 80$ (Newton – Figura 1(c)), nas quais os valores de erro crescem. Esta instabilidade manifestou-se para a função de Runge, na qual a divergência iniciou-se em $N \approx 30$, e para a função degrau, que viola a premissa de continuidade, em $N \approx 40$.

Embora instáveis para N elevado, a interpolação de Newton apresenta um desempenho superior à de Lagrange quando avaliações são necessárias. Seu custo de pré-processamento para a construção da tabela de diferenças divididas é de $O(n^2)$, mas cada avaliação possui um custo de $O(n)$. O método de Lagrange não possui etapa de pré-processamento, mas incorre num custo de $O(n^2)$ para cada ponto. Do ponto de vista computacional, a análise de complexidade corrobora os tempos medidos, conforme ilustrado na Figura 1(d), onde se apresenta a média dos tempos de execução para cada função em diferentes valores de n.

[1]Universidade Federal de Alfenas, maicon.mian@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, pedro.botelho@sou.unifal-mg.edu.br
[3]Universidade Federal de Alfenas, vinicius.boiago@sou.unifal-mg.edu.br
[4]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br



(a): Erro absoluto médio Cubic Spline.

(b): Erro absoluto médio Lagrange.

(c): Erro absoluto médio Newton.

(d): Custo computacional médio.

Figura 1: Comparativo dos métodos em erro e custo computacional. Fonte: Os autores.

A variância dos dados foi incluída para avaliar a representatividade da média. Observa-se que o método de menor custo é aquele com menor complexidade, o *Cubic Spline*.

O método *Cubic Spline*, embora apresente um erro inicial superior para valores baixos de N, demonstrou ser uma abordagem de menor custo computacional. A sua precisão aumenta com o número de pontos, evitando as oscilações presentes nos métodos polinomiais, que geravam *underfitting* ao aproximar polinômios de maior grau para muitos pontos.

Para trabalhos futuros, propõe-se a investigação do impacto da distribuição de nós na estabilidade dos métodos, como os nós de Chebyshev, e a aplicação destes algoritmos em problemas de otimização e controle reais.

Referências

[1] E. M. de Carvalho, "Estudos numéricos dos métodos de interpolação: Lagrange, Newton, Hermite e spline cúbico," dissertação de mestrado, Universidade Federal de São João del-Rei (UFSJ), 2016.

Classificação das variedades de δ-crescimento quase polinomial

Márcio Ribeiro de Oliveira Filho [1]

Em 1979, Kemer caracterizou variedades de crescimento polinomial das codimensões via exclusão de álgebras da variedade, demonstrando que uma variedade de álgebras sobre um corpo F de característica zero tem crescimento polinomial se, e somente se, $UT_2, \mathcal{G} \notin \mathcal{V}$. A existência dessa classificação para álgebras ordinárias motivou a busca de resultados que estendessem a caracterização demonstrada por Kemer no contexto de identidades centrais próprias. É conhecido, por exemplo, que a álgebra $M_k(F)$ admite polinômios centrais próprios, provado por Formanek e Razmyslov. Esses polinômios centrais próprios são fundamentais na produção de identidades polinomiais de $M_{k-1}(F)$. Para o desenvolvimento desse estudo, noções similares de T-ideais, variedades de álgebras, polinômios multilineares e codimensões foram estendidas de maneira natural das álgebras ordinárias. Mediante a extensão desses conceitos, serão apresentados os teoremas de caracterização das variedades de δ-crescimento quase polinomial.

Palavras chaves: Identidades centrais, Variedades, Crescimento quase polinomial.

Referências

[1] A. Giambruno, D. La Mattina e C. Milies, *On almost polynomial growth of proper central polynomials*, Proceedings of the American Mathematical Society, vol. 152, 2024. DOI: 10.1090/proc/16904.

[2] R. B. dos Santos e A. C. Vieira, *PI-álgebras: Uma introdução à PI-teoria*, Rio de Janeiro: Editora do IMPA, 2021.

[1]Universidade Federal de Minas Gerais, marcin74@ufmg.br

Compacidade em Espaços Métricos: o Teorema de Ascoli

Maria Cláudia Sousa Resende [1]
Orientador: Sérgio Guilherme de Assis Vasconcelos[2]

Em espaços métricos, as noções de compacidade, ponto limite compacto e sequencialmente compacto são equivalentes. Este trabalho tem como objetivo apresentar uma formulação de compacidade nesses espaços, baseada na noção de completude.

Segundo 1, todo espaço métrico compacto é completo, mas a recíproca não vale. Desta forma, para fazer tal formulação deveremos acrescentar uma condição chamada totalmente limitado, em que um espaço métrico (X, d) é dito totalmente limitado se, para todo $\varepsilon > 0$, existe uma cobertura finita de X por bolas de raio ε.

Como aplicação, será provado o Teorema de Ascoli que caracteriza quais subespaços de $\mathcal{C}(X, \mathbb{R}^n)$, conjunto formado por todas as funções contínuas de X em $\mathbb{R}^n$, são compactos na topologia uniforme. Tal resultado evidencia o papel central da compacidade em análise funcional e topologia, conectando conceitos métricos abstratos a aplicações concretas.

Referências

[1] J. R. Munkres, *Topology*, 2ª ed., Prentice Hall, Upper Saddle River, NJ, 2000.

[1]Universidade Federal de Juiz de Fora, resende.maria@estudante.ufjf.br
[2]Universidade Federal de Juiz de Fora, sergio.guilherme@ufjf.br

Sistemas Dinâmicos e Caos em Álgebra Não Comutativa

Maurício Reis [1]
Adélcio C. Oliveira[2]

O movimento é objeto de estudo da humanidade desde as observações astronômicas da antiguidade e o pensamento filosófico da Física Aristotélica até os tempos atuais. O cerne desse estudo se faz pela correspondência de posições de objetos ou partículas de acordo com o decorrer do tempo [1]. Desta forma, podemos pensar na forma mais simples de um Sistema Dinâmico de uma partícula como sendo um mapa: $\Phi : \mathbb{R} \to \mathbb{R}^3$ que associa instantes de tempo a posições no espaço tridimensional.

Entre as possíveis formulações da mecânica clássica, destaca-se nesse campo investigativo a Dinâmica de Hamilton [2], dada pelo sistema de equações diferenciais no hyperespaço de posição $\mathbf{q}$ e *momenta* $\mathbf{p}$, as chamadas variáveis canônicas. O gerador da dinâmica é a função hamiltoniana, $\mathcal{H}(\mathbf{q}, \mathbf{p})$. A evolução temporal de qualquer função das variáveis canônicas pode ser obtida pelos parênteses de Poisson, definido como:

$$\{f, g\}_{\mathbf{q},\mathbf{p}} = \sum_i \left(\frac{\partial f}{\partial q_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q_i} \right),$$

onde q_i, p_i são os componentes dos vetores de variáveis canônicas. Em particular, a evolução temporal no espaço de fases de uma distribuição de probabilidades $F(\mathbf{q}, \mathbf{p}, t)$ é dada por:

$$\frac{dF}{dt} = \{F, \mathcal{H}\} + \frac{\partial F}{\partial t}.$$

A mecânica quântica, por sua vez, é normalmente feita com base em operadores de álgebras não comutativas atuando num espaço vetorial denominado Espaço de Hilbert [3]. Os estados físicos de um sistema quântico são operadores positivos-definidos descritos como funções dos N operadores $\{\hat{O}_i\}_{i=1}^N$ que geram a estrutura algébrica do espaço correspondente [4]. Dado um dado estado quântico $\rho(\hat{O}_i, t)$ sua evolução temporal é dada pela relação:

$$\frac{d\hat{\rho}}{dt} = [\hat{\rho}, \hat{H}] + \frac{\partial \hat{\rho}}{\partial t},$$

onde $\hat{H}$ é o operador Hamiltoniano escrito em termos dos geradores da álgebra e $[\hat{A}, \hat{B}]$ é o comutador entre $\hat{A}$ e $\hat{B}$. Verifica-se, portanto, a correspondência entre os parênteses de Poisson da dinâmica clássica, de álgebra comutativa, e o comutador dos operadores

[1]Universidade Federal de São João del Rei - UFSJ, mreis@ufsj.edu.br
[2]Universidade Federal de São João del Rei - UFSJ, adelcio@ufsj.edu.br

da álgebra não comutativa, no caso da dinâmica quântica. Dessa forma, para um dado sistema físico é possível estabelecer correspondências com os dois tipos de dinâmicas: uma clássica, comutativa, e outra quântica, não comutativa [5, 6].

Apesar das características distintas nas duas álgebras que caracterizam as duas dinâmicas, é possível estabelecer interpretações que vinculam resultados nas duas abordagens. Por esse motivo, questões como a representação do sistema físico no espaço de fases [7, 8], o conceito de trajetória e a unicidade no procedimento de obtenção dessas correspondências [9], mesmo em se tratando do mesmo sistema físico, são objeto de interesse investigativo na área de sistemas dinâmicos. Em alguns casos, essa correspondência interpretativa leva a resultados com mesmo significado, mas há casos em que as duas dinâmicas apresentam discrepâncias que a simples correspondência não é capaz de conciliar. Pretende-se, nesse trabalho, explorar essas similaridades e discrepâncias em diferentes modelos de dinâmicas nas duas álgebras.

Referências

[1] I. Newton, *The Principia: Mathematical Principles of Natural Philosophy*. Berkeley: University of California Press, 1999.

[2] H. Goldstein, C. Poole, and J. Safko, *Classical Mechanics*. Addison Wesley, 3rd ed., 2002.

[3] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Quantum Mechanics, Volume 1*, vol. 1. Wiley-VCH, 1991.

[4] L. E. Ballentine, *Quantum Mechanics: A Modern Development*. Singapore: World Scientific Publishing Co. Pte. Ltd., 2nd ed., 2014.

[5] H. Weyl, "Quantenmechanik und gruppentheorie," *Zeitschrift für Physik*, vol. 46, no. 1-2, pp. 1–46, 1927.

[6] B. C. Hall, *Quantum Theory for Mathematicians*, vol. 267 of *Graduate Texts in Mathematics*. Springer, 2013.

[7] E. P. Wigner, "On the quantum correction for thermodynamic equilibrium," *Physical Review*, vol. 40, pp. 749–759, 1932.

[8] G. S. Agarwal and E. Wolf, "Calculus for functions of noncommuting operators and general phase-space methods in quantum mechanics. I. Mapping theorems and ordering of functions of noncommuting operators," *Physical Review D*, vol. 2, no. 10, pp. 2161–2186, 1970.

[9] W. H. Louisell, *Quantum Statistical Properties of Radiation*. Wiley, 1st ed., 1990.

Avaliação Somativa: impactos e contribuições no Ensino Médio a partir de uma intervenção didática em Matemática

Natal Elson Martins [1]
Anderson José de Oliveira[2]
Franco Bassi Rocha[3]

Este trabalho tem como objetivo central analisar a apropriação e o uso pedagógico dos resultados da Avaliação Somativa do SIMAVE em Matemática, aplicada ao 3º ano do Ensino Médio, por parte dos profissionais de uma escola da rede estadual de Minas Gerais. A partir dessa análise, propõe-se uma intervenção didática fundamentada nos dados levantados, buscando potencializar a aprendizagem dos estudantes e contribuir para o enfrentamento das defasagens históricas no ensino da disciplina. A Educação Básica brasileira, especialmente nas últimas décadas, tem sido marcada pela crescente preocupação com a qualidade do ensino e da aprendizagem. Essa preocupação é impulsionada, em grande parte, pela adoção de avaliações externas em larga escala, as quais desempenham papel fundamental no monitoramento do sistema educacional e na definição de políticas públicas. O Sistema Mineiro de Avaliação e Equidade da Educação Pública (SIMAVE) insere-se nesse contexto, oferecendo subsídios para a gestão pedagógica e para a tomada de decisões em diferentes esferas. No entanto, observa-se que, apesar da ampla disponibilidade de dados, a efetiva apropriação dos resultados por professores e gestores ainda representa um desafio. No campo da Matemática, essa lacuna tende a ser ainda mais significativa, dada a persistência de baixos índices de desempenho e o acúmulo de defasagens que se intensificam ao longo da escolarização. De acordo com Ferreira (2019) [1] e Marques (2017) [2], fatores como a falta de formação específica para a análise dos relatórios, a sobrecarga de trabalho docente e a dificuldade em traduzir indicadores em práticas pedagógicas concretas comprometem a utilização estratégica das informações geradas. Assim, faz-se necessário investigar não apenas como esses resultados são compreendidos pelos profissionais da escola, mas também propor caminhos que possibilitem sua integração ao planejamento de ensino e ao processo de aprendizagem.

A presente pesquisa, desenvolvida no âmbito do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT/UNIFAL-MG), adota uma abordagem metodológica de natureza predominantemente qualitativa, com suporte de elementos quantitativos. Caracteriza-se como um estudo de caso e pesquisa-ação/intervenção, conduzida

[1]Discente do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), Universidade Federal de Alfenas,
natal.martins@sou.unifal-mg.edu.br
[2]Docente orientador, Departamento de Matemática, Universidade Federal de Alfenas,
anderson.oliveira@unifal-mg.edu.br
[3]Docente coorientador, Departamento de Matemática, Universidade Federal de Alfenas,
franco.rocha@unifal-mg.edu.br

na Escola Estadual Professor Eduardo Daniel Ferreira Dias, localizada em Campos Gerais (MG). Os participantes do estudo são alunos do 3º ano do Ensino Médio, professores de Matemática e a equipe gestora da escola. Os procedimentos metodológicos envolvem: (i) análise documental dos relatórios do portal SIMAVE referentes ao desempenho em Matemática; (ii) rodas de conversa com professores e gestores, com o intuito de compreender suas percepções e estratégias de uso pedagógico dos resultados; e (iii) desenvolvimento de uma intervenção didática direcionada às principais defasagens identificadas, tomando como referência os descritores com menor índice de acerto e as habilidades previstas na Base Nacional Comum Curricular [3].

A pesquisa está em andamento e encontra-se atualmente em fase de análise quantitativa dos dados e planejamento da intervenção. A etapa documental foi concluída, bem como a obtenção dos termos de anuência da Secretaria de Estado da Educação de Minas Gerais e da escola campo de estudo, além do envio da proposta para o Comitê de Ética em Pesquisa da Universidade Federal de Alfenas (UNIFAL-MG). Os próximos passos consistem na aplicação da intervenção didática em sala de aula e na realização das rodas de conversa, que permitirão verificar a analisar os dados coletados.

Espera-se que este estudo contribua para qualificar o uso das informações do portal SIMAVE, fornecendo subsídios para que a escola possa refletir sobre a gestão pedagógica e a prática docente, promovendo ações mais eficazes para o desenvolvimento de habilidades, conforme a Base Nacional Comum Curricular.

Agradecimentos

À Universidade Federal de Alfenas (UNIFAL-MG), ao Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), à Secretaria de Estado de Educação de Minas Gerais (SEE-MG), à Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) e à Escola Estadual Prof. Eduardo Daniel Ferreira Dias.

Referências

[1] A. S. V. Ferreira, *Interpretação e apropriação dos resultados do SIMAVE: um estudo de caso do uso das informações da avaliação externa de matemática como instrumento de gestão curricular*. PhD thesis, Dissertação de Mestrado, Mestrado Profissional em Gestão e Avaliação da Educação Pública, 2019.

[2] M. V. S. Marques, *Apropriação de resultados da avaliação em larga escala em uma escola mineira de ensino médio: limites e possibilidades de ações gestoras*. PhD thesis, Dissertação de Mestrado, Mestrado Profissional em Gestão e Avaliação da Educação Pública, 2017.

[3] BRASIL, *Base Nacional Comum Curricular*. Brasília, DF: MEC, 2017.

Ensino de Matemática Aplicada por meio da Criptografia com um Site Educacional

Nícolas Francisco Martins Chagas [1]
Divane Aparecida de Moraes Dantas[2] Clístenes Lopes da Cunha [3] Izabela Marques de Oliveira.[4]

Introdução: A Criptografia é um campo dedicado a técnicas para tornar mensagens inacessíveis para interceptadores, por meio de protocolos que as codificam de modo que apenas destinatários autorizados possam decodificá-las. Uma das primeiras ocorrências documentadas remonta ao século XV a.C na Mesopotâmia. Visando proteger sua receita de cerâmica, um ceramista substituiu os símbolos cuneiformes originais por outros [1]. Apesar de rudimentar, essa prática demonstra como as cifras são meios eficazes de implementar confidencialidade.

Desse modo, a Criptografia é essencial em diversos contextos até os dias atuais. Comunicação estratégica militar e política, serviços de e-mail e cartões de crédito, por exemplo, seriam inviáveis sem essa área. Em resposta à evolução dos meios de comunicação e dos ataques de criptoanálise, os métodos criptográficos foram inovados. Foi a aplicação da Matemática que possibilitou os principais avanços da área, pois a eficácia desses métodos é fundamentada em conceitos matemáticos como Funções, Matrizes, Teoria dos Números e Curvas Algébrica.

Desenvolvimento: O trabalho busca mostrar como conteúdos ensinados no Ensino Médio podem ser aplicados em Criptografia. Por isso, foram selecionadas cifras que permitem associação direta com tópicos curriculares, como a Cifra de César (funções bijetivas) e a Cifra de Hill (matrizes).

A Cifra de César, um dos métodos criptográficos mais conhecidos, consiste em deslocar cada letra da mensagem original no alfabeto em um número de casas definido pela chave [2]. Era usada para conferir confidencialidade à comunicação militar, mas pode ser facilmente quebrada por ataques de força bruta.

Enquanto isso, a Cifra de Hill se baseia em realizar transformações reversíveis em matrizes. A chave é uma matriz quadrada K com $det(K) \not\equiv 0\ mod(28)$ e $mdc(det(K), 28) = 1$. As letras da mensagem são convertidas em números e inseridas em uma matriz, que então é dividida em vetores coluna. Cada vetor é multiplicado pela matriz chave e alocado novamente em uma matriz, cujos elementos são extraídos e convertidos em letras novamente, formando o texto cifrado. Para decodificar, o texto cifrado deve ser realocado em uma matriz numérica que será dividida em vetores e multiplicada pela matriz inversa da chave. Ao realizar a montagem e a conversão de volta para letras, obtêm-se o texto original, [3].

[1]nicolaschagas5588@gmail.com , CEFET-MG
[2]divane@cefetmg.br, CEFET-MG
[3]clistenes@cefetmg.br, CEFET-MG
[4]izabelamarques@cefetmg.br, CEFET-MG

Ambos os métodos são cifras simétricas, ou seja, a mesma chave é usada para cifrar e decodificar. Isso cria a necessidade de combinar a chave previamente, que é limitante, especialmente em sistemas computadorizados modernos. Para solucionar esse problema, foi proposto o conceito de criptografia assimétrica. Para cada usuário é criada uma chave privada E e uma pública D, de forma que determinar D a partir de E é computacionalmente inviável. Se Bob quer enviar uma mensagem para Alice, ela é cifrada pública dela. Apenas Alice, com sua chave privada, pode decodificar a mensagem, garantindo confidencialidade. Se Bob quer provar que ele é o remetente, ele cifra a mensagem com sua chave privada. Assim, todos podem usar a chave pública dele para verificar a autenticidade. Isso resolve o problema da distribuição de chaves e permite o uso de assinaturas digitais [4]. Uma das implementações desse conceito é o RSA, cuja segurança é baseada na dificuldade de computadores em fatorar números primos grandes, [5].

Para abordar os princípios matemáticos presentes na criptografia clássica, estamos elaborando um site no qual cada página apresenta uma explicação teórica da matemática por trás de uma cifra, em conjunto com um simulador que realiza a cifragem, decifragem e exibição do passo a passo do procedimento, fundamentando-se nas informações disponibilizadas pelo usuário. Assim, o estudo se torna mais interativo e relacionado a uma aplicação prática. Além dos materiais associados a esses valores, o site possui uma página para testar números primos, a qual será fundamental para os próximos tópicos relacionados à criptografia RSA

Conclusão: Desde a Antiguidade até os dias de hoje, cifras são empregadas para garantir segurança e privacidade durante uma troca de informações. Além disso, a Criptografia aplica conceitos matemáticos que estão incluídos no Ensino Médio, como Matrizes e Funções. Portanto, o ensino de Criptografia é recurso valioso para reforçar o aprendizado desses temas. Conteúdo claro e dinâmico sobre Criptografia pode servir de introdução a estudantes, motivando a curiosidade deles pelo campo. Material desenvolvido disponível em: criptocefet.github.io.

Palavras-chave: Criptografia, Cifra de César, Cifra de Hill.

Referências

[1] A. Mardon, G. Barara, I. Chana, A. Di Martino, I. Falade, R. Harun, A. Hauser, J. Johnson, A. Li, J. Pham, *et al.*, "Cryptography," 2021.

[2] F. O. Loureiro, "Tópicos de criptografia para o ensino médio," dissertação (mestrado em ciências matemáticas), Universidade Estadual do Norte Fluminense Darcy Ribeiro (UENF), Campos dos Goytacazes, RJ, Aug. 2014.

[3] L. D. A. Barbosa and M. G. Cornelissen, "Cifra de hill: Uma aplicação ao estudo de matrizes," *Revista Ciencias Exatas e Naturais*, vol. 19, no. 2, 2017.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] S. C. Coutinho, *Números inteiros e criptografia RSA*. Série de computacão de matemática, Rio de Janeiro: IMPA, 2. ed., 5. impr. ed., 2009.

Modelagem Matemática do Tipo SI Aplicado ao Estudo da Tuberculose no Estado do Rio de Janeiro

Levy dos Santos de Paula[1]
Cristiane de Souza Siqueira[2]
Orlando dos Santos Pereira [3]

O presente trabalho tem como objetivo usar o modelo epidemiológico SI(Suscetível-Infectado) para avaliar a dinâmica da Tuberculose no estado do Rio de Janeiro entre os anos de 2013 e 2023, auxiliando na previsão de sua propagação e no desenvolvimento de estratégias de controle.

A tuberculose é uma doença infectocontagiosa causada pela bactéria Mycobacterium tuberculosis ou Bacilo de Koch. Estima-se que no período de um ano um indivíduo Bacilífico, que pode eliminar bacilos para o exterior, conseguirá infectar de 10 a 15 pessoas. A tuberculose é transmitida de pessoa para pessoa, principalmente através do ar, como em atos de falar, espirrar e principalmente tossir. As principais motivações da pesquisa vêm do fato da tuberculose, segundo a Organização Mundial de Saúde (OMS), ser a décima doença que mais mata no mundo, ultrapassando as mortes causadas pelo HIV e malária[1]. Ainda segundo a OMS, a tuberculose é responsável por mais de 1 milhão de mortes todos os anos desde 2010[2].

Resumidamente, segundo Bassanezi [3], um modelo matemático é uma descrição de um fenômeno do mundo real, frequentemente apresentado por meio de funções ou equações. Dessa forma, os modelos traduzem em linguagem matemática a propagação das doenças.

Primeiramente, essa pesquisa tem como base o trabalho de Falcão[4], que tratou da utilização do modelo SI na modelagem da hanseníase em Codó-MA.

Esse modelo considera a população dividida em duas subpopulações: Suscetíveis (S), que são os indivíduos sadios, podendo contrair a doença ao entrar em contato com os infectados, e Infectados (I), que são indivíduos portadores da doença, que podem transmiti-la. A dinâmica desse modelo é descrita pelo seguintes sistema de equações diferenciais já discretizado:

$$S_{t+1} - S_t = \alpha S_t - \beta S_t I_t, \tag{1}$$

$$I_{t+1} - I_t = \beta S_t I_t - \gamma I_t, \tag{2}$$

em que $S(t)$ é o número de indivíduos suscetíveis no tempo t; $I(t)$ é o número de indivíduos infectados no tempo t; α taxa de variação (crescimento ou decrescimento) dos suscetíveis;β é a taxa de transmissão, que representa a probabilidade de um indivíduo suscetível ser contaminado por um indivíduo infectado; γ taxa de decrescimento da classe

[1]Graduando de Matemática, UFRRJ-ICE , levy979@gmail.com
[2]Professora Adjunta e Pró-Reitora de Pós-Graduação, UNIVASSOURAS , crispereirauss@gmail.com
[3]Professor Titular, UFRRJ-ICE, orlandopereira@ufrrj.br

dos infecciosos(taxa de cura ou mortalidade); Usando que $S_{t+1} + I_{t+1} = 1$ e manipulando as equações (1) e (2), obtém-se que os infectatos I_t stisfazem a uma equação logística

$$I_{t+1} = rI_t(1 - I_t), \tag{3}$$

em que $r = 1 - \gamma + \frac{\beta}{1+\alpha}$.

Neste caso do modelo discreto, o númeror r acima é o número de reprodutividade basal, que representa o número médio de novos infectados gerados por um único infeccioso.

Para a obtenção do valor de $\beta = 0,00000333$, foi realizado uma regressão linear, como mostra a Figura1 (à esquerda) e, de modo análogo, usando os suscetíveis, calculou-se $\alpha = 0,00102$. Com isso, substituindo o valor de β na Equação 2 do sistema, encontrou-se $\gamma = -0,0218706$ e portanto, $r = 1,0218740$.

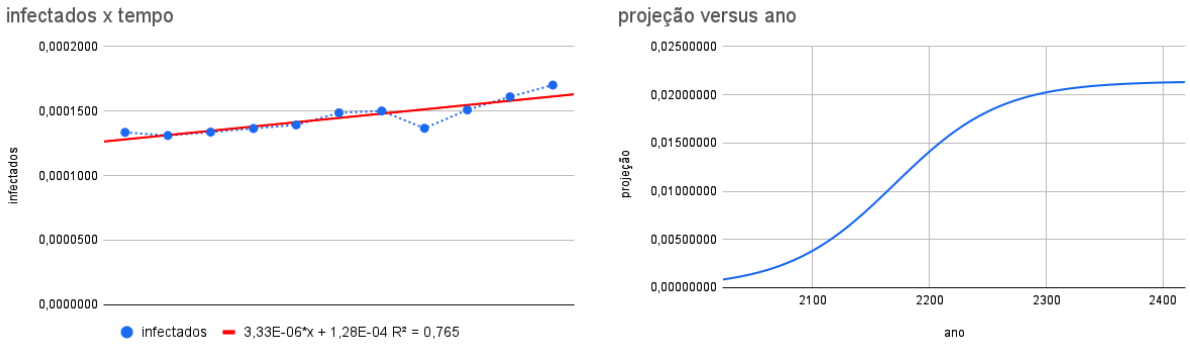


Figura 1: Regressão linear dos infectados (à esquerda) e projeção do Modelo Logístico (à direita).

Os resultados indicam que a doença permanecerá em estado endêmico e tende a se estabilizar a partir do ano de 2350 (Figura 1, à direita). No futuro, será realizado uma simulação no MATLAB usando o método de Euler, afim de verificar aderência do modelo aos dados.

Referências

[1] W. H. ORGANIZATION, "The top 10 causes of death.." Online. Acessado em 25/05/2025, https://www.who.int/news-room/fact-sheets/detail/the-top-10-causes-of-death.

[2] W. H. ORGANIZATION, "Tuberculosis in the world.." Online. Acessado em 25/05/2025, https://worldhealthorg.shinyapps.io/TBrief/?_inputs_&sidebarItemExpanded=null&sidebarCollapsed=true&entity_type=%22group%22&group_code=%22global%22.

[3] R. C. Bassanezi, *Equações Diferenciais Ordinárias:Um Curso Introdutório*. São Paulo: UFABC, 1 ed., 2006.

[4] D. Falcão, J. Leite, and R. Marcolino, "Modelagem matemática para a hanseníase em codó-ma," *Biomatemática*, vol. 27, no. 1, pp. 63–74, 2017.

Grupos de cohomologia de De Rham do espaço projetivo real

Pablo Augusto Santos Nogueira [1]
Prof. Dr. Lonardo Rabelo[2]

Este trabalho apresenta um estudo detalhado e o cálculo explícito dos grupos de cohomologia de De Rham para o espaçovprojetivo real, $\mathbb{RP}^n$. A cohomologia de De Rham, uma ferramenta fundamental da topologia algébrica, permite extrair informações topológicas de uma variedade a partir da análise de suas formas diferenciais. O objetivo principal é demonstrar como a estrutura diferencial desse espaço clássico reflete suas características topológicas. As referências a serem utilizadas são [1], [2] e [3].

Referências

[1] J. M. Lee, *Introduction to Smooth Manifolds. 2a ed.* New York, NY: Springer, 2013.

[2] E. L. Lima, *Homologia Básica. 2a ed.* Rio de Janeiro: IMPA, 2012.

[3] L. W. Tu, *An Introduction to Manifolds. 2a ed.* New York, NY: Springer, 2010.

[1]Universidade Federal de Juiz de Fora, pablo.nogueira@estudante.ufjf.br
[2]Universidade Federal de Juiz de Fora, lonardo.rabelo@ufjf.br

Máximo de Pares Resto-Quociente na Divisão Euclidiana dos Inteiros Gaussianos

Patrick Sodré de Araújo Caldeira [1]
Edney Augusto J. de Oliveira [2]

O conjunto dos inteiros gaussianos, $\mathbb{Z}[i]$, é um subanel do corpo dos números complexos, formado por números da forma $a + bi$, em que a e b são inteiros e i representa a unidade imaginária.

Em $\mathbb{Z}[i]$, é possível definir a função norma do seguinte modo:

$$N : \mathbb{Z}[i] \to \mathbb{N}$$
$$a + bi \mapsto a^2 + b^2$$

Com essa definição, é possível provar que:

Teorema 1 (Divisão Euclidiana) *Dados $D, d \in \mathbb{Z}[i]$ com $d \neq 0 + 0i$, sempre existem $q, r \in \mathbb{Z}[i]$ tais que $D = q \cdot d + r$ e $N(r) < N(d)$.*

Perceba que o Teorema 1 garante que $\mathbb{Z}[i]$ é um domínio euclidiano, ou seja, dados dois inteiros gaussianos, sempre é possível realizar a sua divisão de forma análoga à divisão euclidiana de números inteiros - o que estabelece diversos paralelos entre as aritméticas de $\mathbb{Z}[i]$ e $\mathbb{Z}$, servindo como uma das principais motivações para o estudo dos inteiros gaussianos.

Ademais, é possível acrescentar uma restrição adicional ao resto que pode ser aceito em uma divisão euclidiana de $\mathbb{Z}[i]$, como é mostrado abaixo:

Teorema 2 (Divisão Euclidiana Forte) *Dados $D, d \in \mathbb{Z}[i]$ com $d \neq 0 + 0i$, sempre existem $q, r \in \mathbb{Z}[i]$ tais que $D = q \cdot d + r$ e $N(r) \leq 0,5N(d)$.*

Tomando $D = 4 + 2i$ e $d = 3 + 1i$, por exemplo, a divisão euclidiana forte pode ser realizada da seguinte forma:

$$4 + 2i = (1 + 0i) \cdot (3 + 1i) + (1 + 1i)$$

Entretanto, também poderíamos ter feito:

$$4 + 2i = (2 + 0i) \cdot (3 + 1i) + (-2 + 0i)$$

Com isso, fica evidente que nem sempre a divisão euclidiana forte pode ser realizada de forma única em $\mathbb{Z}[i]$, o que conduz ao seguinte questionamento: qual é o número máximo de pares resto-quociente para uma divisão em $\mathbb{Z}[i]$?

[1]Universidade Federal de Ouro Preto, patrick.caldeira@aluno.ufop.edu.br
[2]Universidade Federal de Ouro Preto, edney@ufop.edu.br

Este trabalho tem como objetivo responder esse questionamento e continuar explorando a divisão euclidiana de inteiros gaussianos por meio da análise das particularidades aritméticas associadas a cada número possível de pares resto-quociente.

Referências

[1] L. C. Alves, R. P. Moura, and E. Strey, "Inteiros gaussianos," *Revista Professor de Matemática Online*, vol. 11, no. 3, 2023.

[2] A. Hefez, *Curso de Álgebra*, vol. 1 of *Coleção Matemática Universitária*. Rio de Janeiro: IMPA, 4 ed., 2010.

[3] J. L. Boldrini, S. I. R. Costa, V. L. Figueiredo, and H. G. Wetzler, *Álgebra Linear*. São Paulo: Harbra, 3a. ed. ed., 1986.

Métodos Numéricos na Resolução de EDOs: Estudo de Caso em Circuito RC

Maicon Almeida Mian[1]
Pedro Henrique Botelho da Silva[2]
Vinicius Henrique Piotto Boiago[3]
Angela Leite Moreno[4]

Este trabalho foca na análise do desempenho e da precisão de diferentes métodos numéricos aplicados à resolução de uma Equação Diferencial Ordinária (EDO) que modela a descarga de um capacitor em um circuito RC com tensão de entrada variável.

A tensão $V_c(t)$ em um capacitor de um circuito RC [1] com resistência $R = 100\,\Omega$ e capacitância $C = 0{,}001\,\mathrm{F}$, submetido à tensão de entrada $V_{in}(t) = 12\cos(2\pi t)$ V, satisfaz a Equação Diferencial (1):

$$\frac{dV_c}{dt} = \frac{V_{in}(t) - V_c}{RC} = 10\left(12\cos(2\pi t) - V_c\right), \tag{1}$$

com condição inicial $V_c(0) = 0$. O objetivo é aproximar $V_c(t)$ para $t \in [0, 5]$ segundos, usando passo $h = 0{,}25$ s.

Para realizar a tarefa foram selecionados os métodos numéricos: Euler Implícito (EI) e Explícito (EE), Adams-Bashforth 2 (AB2), Adams-Moulton 2 (AM2), o Método do Trapézio (TI), *Backward Differentiation 2nd-order* (BDF2), Ponto Médio Explicítio (PME) e Método do Ponto Médio Implícito (PMI) [2]. Todos foram implementados em C e executados em um sistema com processador AMD Ryzen 5 5500 e 32 GB de RAM, sob o Fedora 41. Os resultados relacionados aos erros e tempo foram apresentados na Tabela 1, em que Q1, Q2, Q3 e Q4 correspondem, respectivamente, aos intervalos [0;1,25], [1,25; 2,5], [2,5;3,75] e [3,75; 5,0].

Tabela 1: Tabela das Métricas de Erro

Métricas	Métodos Instáveis			Métodos Estáveis				
	EE	AB2	PME	EI	AM2	TI	BDF2	PMI
Erro (Q1)	4.62	45.36	5.80	0.28	1.40	0.14	1.58	0.31
Erro (Q2)	36.84	1.41×10^4	67.91	0.29	0.14	0.10	0.22	0.29
Erro (Q3)	279.65	4.37×10^6	77.03×10^1	0.24	0.07	0.12	0.23	0.26
Erro (Q4)	2.92×10^3	3.88×10^9	12.98×10^3	0.26	0.08	0.11	0.23	0.27
Erro RMS	1.56×10^3	2.06×10^9	69×10^2	0.27	0.69	0.12	0.79	0.28
Erro	4.6×10^4	7.74×10^{10}	2.16×10^5	0.67	0.05	1.29	2.14	1.74
Tempo (μs)	3.18	3.56	3.86	5.02	5.02	5.49	5.53	6.22

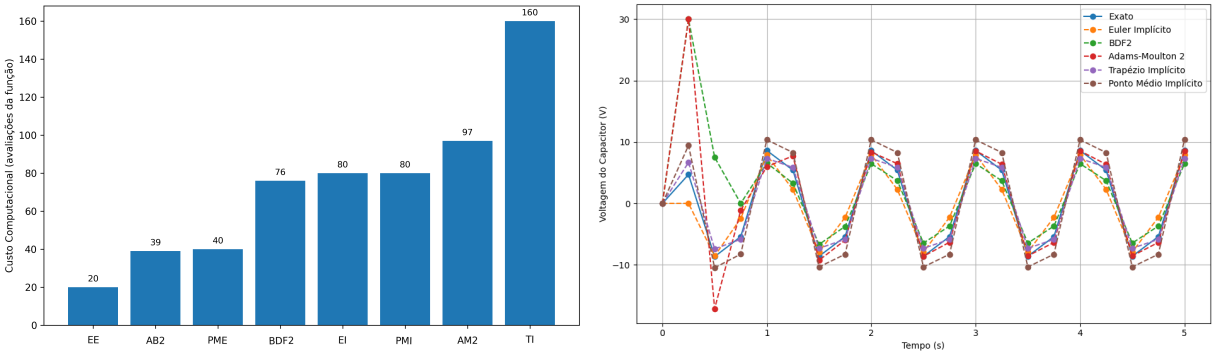
[1]Universidade Federal de Alfenas, maicon.mian@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, pedro.botelho@sou.unifal-mg.edu.br
[3]Universidade Federal de Alfenas, vinicius.boiago@sou.unifal-mg.edu.br
[4]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

Para estimar o custo computacional, contabilizou-se o total de avaliações da função da EDO ao longo da simulação [2], conforme a Equação (2):

$$\text{Custo} \;=\; n_f \cdot \frac{b-a}{h}, \tag{2}$$

em que n_f é o número de avaliações da função $f(t, y)$ por cada passo h e $[a, b]$ é o intervalo.

A partir dos resultados obtidos, notou-se que os métodos explícitos apresentaram tempos médios de execução (Tabela 1) e custo computacional (Figura 1(a)) menores, possivelmente por não exigirem a busca de zeros da função a cada iteração. Contudo, mostraram-se instáveis, explodindo a cada passo. Assim, focou-se em apresentar as soluções em função do tempo de cada um dos métodos estáveis, juntamente com a solução exata, conforme Figura 1(b).



(a). Custo computacional de cada método.

(b). Simulações em relação ao tempo.

Figura 1: Comparativo dos métodos. Fonte: Os autores.

Os métodos Trapézio, Ponto Médio Implícito e Euler Implícito mostraram maior estabilidade por serem autoinicializáveis, ao contrário de Adams-Moulton e BDF2, que dependem de um valor inicial. A partir do 3^o quartil, o método Adams-Moulton se recuperou, apresentando menor erro e alta adaptabilidade. Por outro lado, os métodos mais estáveis implicam maior custo computacional, ao contrário dos menos estáveis.

Para pesquisas futuras, espera-se investigar as razões dos métodos explícitos terem apresentado resultados insatisfatórios nesse problema.

Referências

[1] B. N. Biswas *et al.*, "A discussion on Euler method: A review," *Electronic Journal of Mathematical Analysis and Applications*, vol. 1, pp. 294–317, July 2013. Submitted April 30, 2013.

[2] A. A. Wendimu *et al.*, "A comparative study of one-step and multi-step numerical methods for solving ordinary differential equations in water tank drainage systems," *Engineering Reports*, vol. 7, no. 3, p. e70080, 2025.

Dinâmica caótica no toro $\mathbb{T}^2$

Pedro Lucas Ribeiro da Silva [1]
Wilker Thiago Resende Fernandes[2]

Resumo

Os sistemas dinâmicos constituem uma área da Matemática responsável por modelar e ajudar a compreender o comportamento de fenômenos naturais conforme o tempo passa. Estes podem ser classificados em contínuos e discretos, dependendo da natureza do tempo considerado. Os sistemas dinâmicos contínuos tratam o tempo como uma variável contínua, enquanto os sistemas dinâmicos discretos tratam o tempo em etapas discretas, ou seja, descrevem o comportamento em momentos específicos. Neste trabalho, estudaremos a função $f_A : \mathbb{T}^2 \to \mathbb{T}^2$ dada por

$$f_A(x_1, x_2) = \pi(A(x_1, x_2)) = (x_1 + x_2 \mod 1, x_1 \mod 1)$$

onde $\pi : \mathbb{R}^2 \to \mathbb{T}^2$ é a projeção dada por $\pi(x_1, x_2) = (x_1 \mod 1, x_2 \mod 1)$ e A é a matriz

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

em um exemplo muito conhecido de um *automorfismo hiperbólico* do toro. Apresentaremos alguns resultados importantes sobre o comportamento da dinâmica no toro $\mathbb{T}^2$, como a existência de conjuntos estáveis e instáveis, pontos periódicos, órbitas densas, transitividade, e por fim, o caos. Este estudo foi baseado em [1] e [2].

Palavras-chave: Sistemas dinâmicos discretos, toro, conjuntos estáveis, conjuntos instáveis, caos.

Referências

[1] BACKES, L.; BARAVIERA, A. T.; BRANCO, F. M. **Uma introdução aos sistemas dinâmicos via exemplos**. Rio de Janeiro: IMPA, 2023.

[2] DEVANEY, R. L. **An Introduction to Chaotic Dynamical Systems**. Westview Press, 2003.

[1]Universidade Federal de São João del Rei , pe.lucas.silva35@gmail.com
[2]Universidade Federal de São João del Rei , wilker@ufsj.edu.br

Códigos Corretores de Erros

Priscilla Nádia Aparecida Ferreira [1]
José Alves Oliveira[2]

Os Códigos Corretores de Erros fazem parte da vida de várias pessoas, como uma ferramenta. Está presente em inúmeras funções do nosso dia a dia, como o Wi-Fi, CDs, DVDs, QRCode, ou até mesmo em uma simples compra no mercado, ou em recepção de imagens de um planeta a quilômetros de distância da Terra, que é enviada através de dados via satélite. Uma teoria fundada pelo matemático Claude Elwood Shannon (1916-2001), por volta dos anos de 1950 e, posteriormente com uma grande contribuição das pesquisas do também matemático Richard Wesley Hamming (1915-1998) [1] [2] [3]. Estudos na área de Teoria dos Números são primordiais para um melhor entendimento deste tema [4]. O esquema de um código é apresentado pela Figura 1:

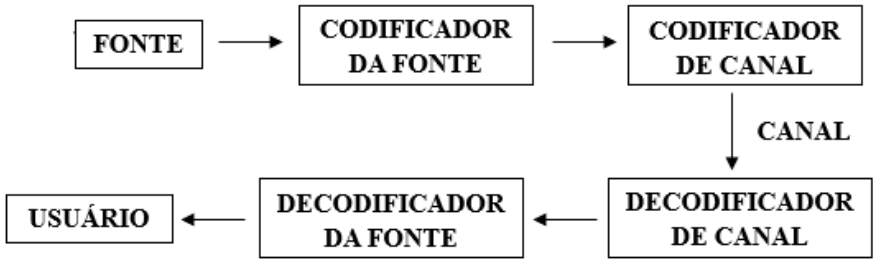


Figura 1: Esquema de um Código.
Fonte: Elaborado pela autora (2025).

Uma importante contribuição de Hamming, a chamada "Distância de Hamming", pode ser definida como:

Definição 1 *Dados dois elementos* $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{A}^n$, *a distância de Hamming entre* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *é definida como:*

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

Nosso objetivo é estudar esse e outros conceitos básicos relacionados aos Códigos Corretores de Erros, com o intuito de explorar estratégias para tornar a apresentação do tema mais inclusiva e acessível.

[1]Universidade Federal de Lavras, UFLA
priscilla.ferreira1@estudante.ufla.br
[2]Universidade Federal de Lavras, UFLA
jose_oliveira@ufla.br

Referências

[1] A. HEFEZ and M. L. T. VILLELA, "*Códigos corretores de erros,*" Rio de Janeiro: IMPA, 2a. ed., 2008.

[2] G. A. P. SABADIN, "*Códigos corretores de erros,*" Master's thesis, Universidade Federal de Santa Catarina, 2019.

[3] J. V. BALAN and R. PEIXOTO, "*Códigos corretores de erros,*" Universidade Federal de São Carlos, 2024. Online. Acessado em 29/04/2025, https://sbm.org.br/xi-bienal/wp-content/uploads/sites/31/2024/07/XI_BM_Poster_Joao_Victor_Balan.pdf.

[4] C. P MILIES and S. P. COELHO, "*Números: uma Introdução à Matemática,*" São Paulo: Editora da Universidade de São Paulo, 3a. ed., 2000.

A parábola de curvatura para superfícies de coposto 1 em $\mathbb{R}^3$

Rafael de Castro Andretto[1]
Pedro Benedini Riul[2]

Considerando M uma superfície de coposto 1 em $p \in \mathbb{R}^3$, nosso objetivo é estudar a sua geometria de segunda ordem, ou seja, as características de M herdadas de sua segunda forma fundamental. Para isso, definimos a primeira e segunda formas fundamentais e a parábola de curvatura Δ_p: uma curva plana contida no plano normal que desempenha um papel similar à elipse de curvatura para superfícies regulares, definida em [1].

Em [2], o autor prova que existem quatro $\mathcal{A}^2$-órbitas no conjunto de germes de aplicações de coposto 1: $f : (\mathbb{R}^2, 0) \to (\mathbb{R}^3, 0)$. Mostramos que a parábola de curvatura é um invariante completo desta classificação. Além disso, provamos que, dadas duas superfícies localmente parametrizadas por dois germes de aplicação de coposto 1, $f, g : (\mathbb{R}^2, 0) \to (\mathbb{R}^3, 0)$, tais germes são $\mathcal{R}^2 \times \mathcal{O}(3)$-equivalentes se, e somente se, existe uma isometria linear entre os dois planos normais das superfícies que mapeia a parábola de curvatura de uma superfície na da outra. Portanto, fica evidente que a parábola de curvatura Δ_p codifica toda a geometria de segunda ordem de M em p. Este estudo é baseado em [3].

Referências

[1] J. A. Little, "On singularities of submanifolds of higher dimensional euclidean spaces," *Annali di Matematica Pura ed Applicata*, vol. 83, no. 1, pp. 261–335, 1969.

[2] D. Mond, "On the classification of germs of maps from $\mathbb{R}^2$ to $\mathbb{R}^3$," *Proceedings of the London Mathematical Society*, vol. 3, no. 2, pp. 333–369, 1985.

[3] L. F. Martins and J. J. Nuno-Ballesteros, "Contact properties of surfaces in $\mathbb{R}^3$ with corank 1 singularities," *Tohoku Mathematical Journal, Second Series*, vol. 67, no. 1, pp. 105–124, 2015.

[1]Universidade Federal de São João del-Rei, rafaelvilaandretto2003@aluno.ufsj.edu.br
[2]Universidade Federal de São João del-Rei, benedini@ufsj.edu.br

Identificação Exata de Grupos Fuchsianos por Meio de Curvas Algébricas de Grau Par

Rafael Ferreira Cardoso[1]
Anderson José de Oliveira[2]
Cátia Regina de Oliveira Quilles Queiroz[3]

Este trabalho contribui para o desenvolvimento da teoria de sistemas de comunicação, área essencial na transmissão de dados, composta por fontes, codificadores, canais e decodificadores, até o usuário final. Nas últimas décadas, especialmente a partir dos trabalhos de Valery Goppa, na década de 1970, e de Mark Goresky, na década de 1980, a análise de curvas algébricas e de espaços com curvatura negativa consolidou-se como uma das principais abordagens matemáticas para o aprimoramento desses sistemas.

Propomos um novo tratamento para obter e interpretar grupos fuchsianos associados a curvas definidas por $y^2 = z^n \pm 1$, com $n \in \mathbb{N}$ par, e analisar suas propriedades geométricas. Os geradores são obtidos pelo Algoritmo de Whittaker [1], modificado para representar as raízes em radicais, eliminando aproximações comuns na literatura [1, 2]. Identificações aproximadas são usadas em aplicações específicas, mas limitam generalizações.

Buscamos fornecer ferramentas algébricas para estudos em tesselações hiperbólicas. Pelo procedimento de Whittaker, partimos das raízes da curva algébrica, determinamos o polígono fundamental via transformações elípticas S_i de cada aresta, normalizadas quando necessário. Fixada uma transformação, calculamos os produtos S_iS_j, $j \neq i$, e, constatando que são transformações hiperbólicas, identificamos os geradores do grupo fuchsiano.

Definição 1 *Denote por* $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ *o disco de Poincaré. As isometrias de* $\mathbb{D}$ *são exatamente as transformações de Möbius*

$$\gamma(z) = \frac{\alpha z + \beta}{\overline{\beta} z + \overline{\alpha}}, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 - |\beta|^2 = 1. \tag{1}$$

Um grupo fuchsiano é um subgrupo discreto do grupo dessas isometrias.

Resultados para valores específicos de n (como $2, 4, 6, 8$) revelam padrões nos traços das matrizes dos geradores, sugerindo regularidades passíveis de formulação conjectural. Esses padrões podem subsidiar a classificação de famílias de grupos fuchsianos oriundos de curvas de grau par e estabelecer relações com invariantes do polígono fundamental. Essa classificação, apoiada por representações exatas, abre possibilidades para aplicações em teoria de codificação, especialmente em cenários com simetrias hiperbólicas centrais.

[1]Mestrando em Estatística Aplicada e Biometria, Universidade Federal de Alfenas, rafael.cardoso@sou.unifal-mg.edu.br
[2]Docente orientador, Departamento de Matemática, Universidade Federal de Alfenas, anderson.oliveira@unifal-mg.edu.br
[3]Docente coorientadora, Departamento de Matemática, Universidade Federal de Alfenas, catia.quilles@unifal-mg.edu.br
Agradecemos à UNIFAL-MG e ao PPGEAB. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Exemplo 1 *Seja a curva* $y^2 = z^6 - 1$*, após obter as seis raízes na forma de radicais, aplica-se o procedimento de Whittaker, gerando transformações com coeficientes exatos, como:*

$$S_1S_2 = \frac{\frac{-5-3\sqrt{3}i}{2}z + (-3+\sqrt{3}i)}{(-3-\sqrt{3}i)z + \frac{-5+3\sqrt{3}i}{2}}.$$

Trata-se de uma transformação hiperbólica, pois $|\mathrm{tr}(S_1S_2)| = 5 > 2$*, análoga para os demais produtos* S_iS_j*. Os geradores do grupo são denotados por* $\Gamma = \langle S_1S_2, S_1S_3, S_1S_4, S_1S_5, S_1S_6\rangle$*.*

A Figura 1 apresenta um decágono hiperbólico, após as transformações aplicadas ao hexágono hiperbólico, além da superfície bitoro, associados à curva $y^2 = z^6 - 1$.

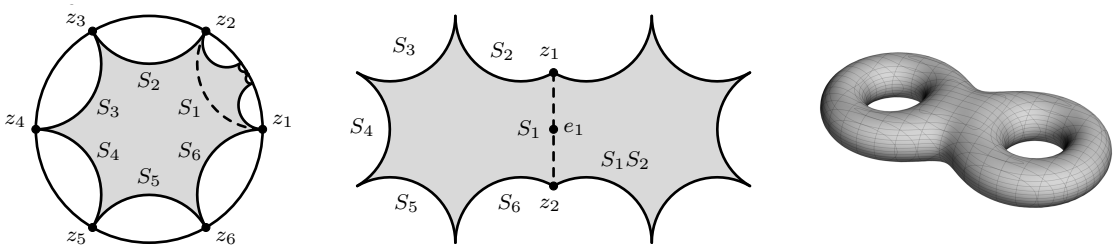


Figura 1: Decágono hiperbólico e bitoro associados à curva $y^2 = z^6 - 1$.

Fonte: os autores.

Concluímos que a identificação exata de grupos fuchsianos associados a curvas algébricas permite construir tesselações hiperbólicas com propriedades de uniformidade e simetria aplicáveis à modelagem de grafos altamente estruturados [3]. Essas estruturas fundamentam o desenvolvimento de códigos geometricamente uniformes, com aplicações diretas em sistemas de comunicação, oferecendo eficiência na correção de erros e robustez a ruídos. Além disso, a abordagem algébrica favorece algoritmos computacionais precisos para manipulação desses grupos, ampliando seu uso em cenários práticos, como canais com topologias complexas e ambientes onde a geometria influencia a transmissão de dados.

Referências

[1] E. P. D. O. Guazzi and R. Palazzo Jr., "Influência da alocação de pólos associados a curvas algébricas com g= 1 na determinação de grupos fuchsianos," *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, vol. 6, no. 1,, 2018.

[2] A. J. Oliveira, *Uniformização de curvas algébricas associadas a sequências de Farey através de equações diferenciais fuchsianas na proposta de novos sistemas de comunicação.* PhD thesis, Tese de Doutorado, FEECUNICAMP, 2017.

[3] C. R. O. Q. Queiroz, *Códigos Geometricamente Uniformes Derivados de Grafos sobre Anéis Quocientes de Inteiros e de Ordens dos Quatérnio.* PhD thesis, Tese de Doutorado, FEECUNICAMP, 2011.

O Impacto da Métrica de Distância na Classificação de Arritmias com o Algoritmo KNN

Renan Catini Amaral[1]
Reginaldo José da Silva[2]
Angela Leite Moreno[3]

As arritmias cardíacas representam um risco significativo para a saúde, sendo fundamental um diagnóstico preciso para um acompanhamento clínico adequado. Entretanto, a análise de eletrocardiogramas (ECG) baseada na interpretação visual é uma tarefa complexa, que pode ser subjetiva e gerar divergência entre profissionais [1]. Assim, ao se utilizar algoritmos de Aprendizado de Máquina (*Machine Learning*-ML) e padrões do ECG, consegue-se prever o diagnóstico com maior precisão e confiabilidade.

É nesse cenário que este trabalho está inserido, separando os diagnósticos em normais e anormais, buscando analisar qual configuração do modelo é mais sensível para identificar corretamente cada tipo de batimento. O conjunto de dados utilizado para tal tarefa foi o tratado por [2], obtido diretamente do "*MIT-BIH Arrhythmia Database*" [3]. Este conjunto contém registros de ECG com cerca de 30 minutos de duração. No pré-processamento, cada exame foi separado batimento por batimento, visando treinar o modelo para reconhecer os diferentes tipos de batimentos. Cada batimento foi rotulado seguindo o padrão AAMI, sendo eles: batimentos normais (N), supraventriculares (S), ventriculares (V), fusão (F) e não classificáveis (Q). Ao se analisar a quantidade de dados em cada classe, verificou-se que ele é altamente desbalanceado, com cerca de 93% de casos classificados como normais. Portanto, tais rótulos foram separados em dois grupos: os normais (N), compostos somente por batimentos rotulados como N, e os anormais (AN), composto por todos os outros rótulos, visando reduzir o desbalanceamento e possibilitar a formulação de um problema binário, para uma primeira investigação.

Para realizar a classificação, o algoritmo de aprendizado de máquina escolhido foi o K-*Nearest Neighbors* (KNN). A base de dados foi dividida em 70% para treinamento e 30% para teste. A busca por hiperparâmetros foi realizada no conjunto de treinamento utilizando a técnica 5-*fold* comparando-se o desempenho do modelo sob diferentes métricas de distância (*Minkowski*), controladas pelo hiperparâmetro p. O resultado indicou que, dentre os valores testados para o número de vizinhos ($\texttt{n\_neighbors} \in \{5, 7, 9, 11, 15\}$, o valor ideal foi 5 e que o uso de pesos ponderados pela distância ($\texttt{weights} = \texttt{distance}$) apresentou os melhores resultados consistentemente. Para os casos $p = 1$ e $p = 2$, esses valores foram encontrados por meio de uma busca em grade (*Grid Search*). No entanto, para os testes com $p = 4$ e $p = 8$, a busca completa se mostrou inviável devido ao alto

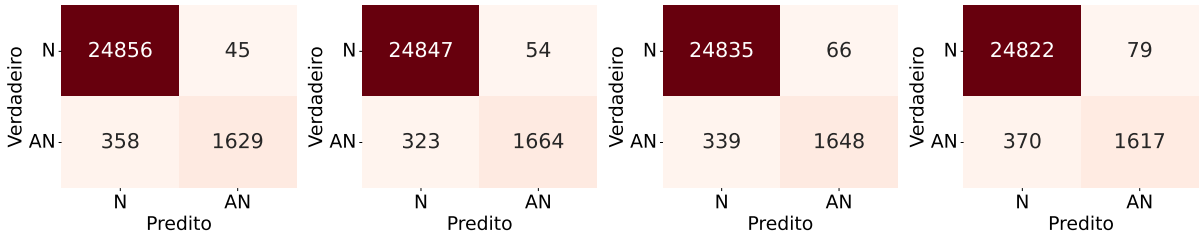
[1]Departamento de Ciência da Computação, Universidade Federal de Alfenas, renan.amaral@sou.unifal-mg.edu.br
[2]Faculdade de Engenharia de Ilha Solteira, Universidade Estadual Paulista, reginaldo.silva@unesp.br
[3]Departamento de Matemática, Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

custo computacional. Nesses casos, o valor de `n_neighbors` foi fixado em 5 (com base no resultado anterior) e a otimização focou no hiperparâmetro `weights`. Todo o processo de otimização foi focado em maximizar a Sensibilidade.

Os resultados dos testes, reunidos na Tabela 1, apontam a distância Euclidiana ($p = 2$) como a de melhor desempenho. Esta configuração se destacou por alcançar a maior Sensibilidade, com 83,74%. A prioridade foi dada a esta métrica, pois em um diagnóstico clínico, a importância de um Falso Negativo (não detectar uma arritmia real) é muito maior do que o de um Falso Positivo. A superioridade do modelo com $p = 2$ é confirmada em sua matriz de confusão (Figura 1), que mostra o menor número de Falsos Negativos entre os testes: 323, ou seja, 323 batimentos anormais foram classificados como normais, ao custo de somente 9 batimentos normais classificados como anormais em relação ao melhor modelo apresentado. Portanto, esta configuração provou ser a mais eficaz para a tarefa. Os próximos passos da pesquisa são verificar se isso se mantém para o problema multiclasse e também utilizar outros classificadores para tratar o problema.

Métrica	Accuracy	Recall	ROC	F1	Precision	Specificity
1	98,50	81,98	0,9090	0,8899	97,31	99,82
2	98,60	83,74	0,9176	0,8982	96,86	99,78
4	98,49	82,94	0,9134	0,8906	96,15	99,73
8	98,33	81,38	0,9053	0,8781	95,34	99,68

Tabela 1: Resultados do treinamento do modelo KNN.



(a) $p = 1$. (b) $p = 2$. (c) $p = 4$. (d) $p = 8$.

Figura 1: Matrizes de confusão do modelo KNN para cada métrica. Fonte: Os autores.

Referências

[1] A. A. Ahmed, W. Ali, T. A. Abdullah, and S. J. Malebary, "Classifying cardiac arrhythmia from ecg signal using 1d cnn deep learning model," *Mathematics*, vol. 11, no. 3, p. 562, 2023.

[2] R. J. Silva *et al.*, "Classificação de arritmias no tempo e tempo-frequência: uma abordagem baseada em subproblemas," in *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, vol. 11, pp. 010360–1–7, 2025.

[3] G. B. Moody and R. G. Mark, "The impact of the mit-bih arrhythmia database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45–50, 2001.

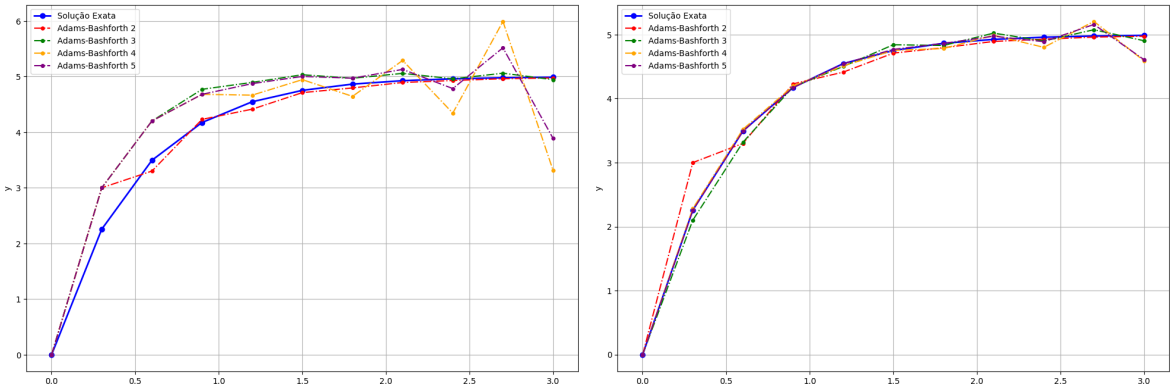
Avaliação do Desempenho do Método Adams-Bashforth: Um Estudo sobre Ordem e Inicialização

Leonardo Bonardi Marques Silva[1]
Rodrigo Luís Gasparino Lucatelli[2]
Angela Leite Moreno[3]

O trabalho analisa e compara a convergência de um mesmo método numérico, com diferentes ordens, na resolução de uma Equação Diferencial Ordinária (EDO). Para isto, considere o seguinte problema: um farmacologista estuda a absorção e eliminação de um medicamento injetado na corrente sanguínea. A concentração do medicamento, $I(t)$, diminui com o tempo devido ao metabolismo do corpo. A taxa de variação da concentração é proporcional à própria concentração, um processo de decaimento de primeira ordem. A taxa de variação da concentração de medicamento $I(t)$ é modelada pela EDO $\frac{dI}{dt} = -kI + D$, em que k é a constante de eliminação do medicamento e D é a taxa de absorção constante. Para isto, considerou-se a constante de eliminação $k = 2\,\mathrm{h}^{-1}$, a taxa de absorção $D = 10\,\mathrm{mg/L/h}$ e a concentração do medicamento é zero no início do processo. Assim, temos o Problema de Valor Inicial (PVI):

$$\begin{cases} \dfrac{dI}{dt} = \dfrac{50 - 10I}{5} = 10 - 2I \\ I(0) = 0 \end{cases}$$

O PVI foi resolvido utilizando o Método Adams-Bashforth de segunda, terceira, quarta e quinta ordem [1]. Os resultados obtidos são apresentados na Figura 1.



(a) Inicialização Degradada. (b) Inicialização Aprimorada.

Figura 1: Comparação entre os Métodos de Adams-Bashforth de diferentes ordens.

[1]Universidade Federal de Alfenas, leonardo.bonardi@sou.unifal-mg.edu.br
[2]Universidade Federal de Alfenas, rodrigo.lucatelli@sou.unifal-mg.edu.br
[3]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

Ao analisar a Figura 1a, a inicialização degradada dos pontos foi realizada pelo método de Euler explícito de primeira ordem, introduzindo um erro significativo nos primeiros pontos calculados. Como o método de Adams-Bashforth depende dos dados já calculados, o erro se propagou e se acumulou em cada iteração, afetando desproporcionalmente os métodos de ordem mais alta. Isso ocorre porque os métodos de ordem mais alta utilizam mais pontos iniciais (com "má" precisão) em seus cálculos, amplificando o erro total. Em contrapartida, a Figura 1b mostra os resultados da inicialização apropriada, na qual foi realizada separadamente para cada ordem, sendo Euler explícito de primeira ordem para Adams de segunda ordem, Runge-Kutta de segunda ordem para Adam de terceira, Runge-Kutta de terceira para Adam de quarta e Runge-Kutta de quarta para Adams de quinta. Como a precisão dos pontos de partida foi melhorada, permitiu-se que os métodos de ordem maior operassem de forma mais próxima de seu potencial teórico. Observa-se a convergência para todas as ordens de Adams-Bashforth é muito mais consistente com a solução exata. Mas o que acontece se o intervalo for ampliado? Será que seu comportamento se mantém?

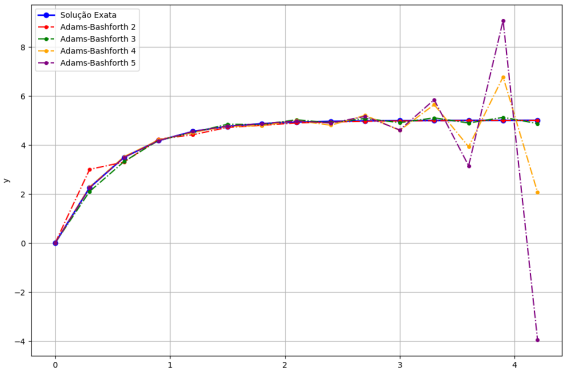


Figura 2: Métodos de Adams-Bashforth com mais iterações.

Infelizmente não, como pode ser observado na Figura 2. Novamente, mesmo com a melhoria inicial, o método de Bashforth acumula os erros de convergência a cada iteração. Portanto, quanto mais pontos com "má" precisão são utilizados, maior será o erro por ordem, afetando consequentemente os métodos de ordem maiores, como visto nos gráficos.

Com isso, pode-se observar comportamento inesperado do método de Adams-Bashforth. Contrariando a premissa de que métodos de ordem superior proporcionam maior precisão, os dois métodos de ordens menores (segunda e terceira) obtiveram uma melhor convergência em relação aos dois métodos de ordens maiores (quarta e quinta). Esse fenômeno é uma consequência direta do problema de inicialização, que impacta a acumulação de erros ao longo das iterações.

Ainda é possível investigar como o tamanho do passo afeta a convergência e a eficácia do método de Adams-Bashforth.

Referências

[1] G. P. Silveira and R. O. Garcia, "Análise do comportamento das soluções numéricas de um sistema que modela interações entre três espécies," *Biomatemática*, vol. 30, pp. 287–305, 2020.

Análise das orientações didáticas nos documentos curriculares oficiais de Grandezas e Medidas[1]

Roselene Aparecida da Silva Lino [2]
Angela leite Moreno[3]

A Matemática é uma ferramenta crucial para a compreensão do mundo e a formação de cidadãos críticos. Longe de se limitar a quantificar e calcular, a disciplina é responsável por criar sistemas abstratos que organizam fenômenos como espaço, movimento, formas e números, os quais são fundamentais para a compreensão, representação e construção de argumentos consistentes. Deste modo, ajuda a compreender o mundo e é resultado da iteração humana com o ambiente [1]. Assim, a Matemática se torna uma ferramenta fundamental para a compreensão do mundo e a formação de cidadãos críticos.

Segundo os Parâmetros Curriculares Nacionais (PCN) [2] a falta de conhecimento matemático pode limitar a compreensão e a participação em questões sociais. Por sua vez, a Base Nacional Comum Curricular (BNCC) [1] destaca que a Matemática contribui para a cidadania ao desenvolver o raciocínio lógico, a capacidade de investigação e a resolução de problemas sociais, além de estimular a avaliação crítica e ética de informações. Enquanto o Currículo Referência de Minas Gerais (CRMG) [3] foca no papel do currículo como materializador do direito de aprender, definindo o que, por que e quando ensinar, alinhando o conteúdo às expectativas da sociedade.

Nesse contexto, o eixo Grandezas e Medidas é fundamental para a compreensão da realidade e para a quantificação de fenômenos do mundo físico. Sua relevância na formação do indivíduo foi evidenciada ao ser incorporada como um eixo temático nos PCN em 1997, que reconheceu Grandezas e Medidas como um campo matemático autônomo e não mais como um ramo da Geometria. O documento ressalta a relevância social e o caráter prático e utilitário do tema. A BNCC e o CRMG reforçam essa ideia, afirmando que a unidade temática contribui para a consolidação da noção de número, a aplicação da geometria e o desenvolvimento do pensamento algébrico. O CRMG ainda adiciona que essa unidade propicia o desenvolvimento de atitudes éticas, responsáveis e sustentáveis do consumo.

A abordagem de "Grandezas e Medidas" também se alinha profundamente com os quatro pilares da educação da UNESCO [4]. O "aprender a conhecer" é atendido quando o aluno compreende conceitos matemáticos abstratos, resolve problemas históricos e integra a Matemática a outras disciplinas como Ciências e Geografia. Enquanto o "aprender a fazer" é promovido pela aplicação prática da Matemática em situações cotidianas e pelo uso de instrumentos de medição. Além disso, estimula o desenvolvimento de habilidades de investigação e raciocínio ágil. Já o "aprender a viver juntos" é promovido ao se utilizar o tema para debater questões sociais e ambientais, como movimentos migratórios e

[1]Agradecemos à UNIFAL-MG, ao PROFMAT, à CAPES e à FAPEMIG.
[2]Universidade Federal de Alfenas, roseleneaslino@gmail.com
[3]Universidade Federal de Alfenas, angela.moreno@unifal-mg.edu.br

distribuição de renda, e ao se trabalhar de forma cooperativa. Por fim, "aprender a ser" é contemplado quando o aluno desenvolve senso crítico e autonomia, compreendendo a imprecisão das medidas e atuando de forma ética e responsável em relação ao consumo. Essa abordagem contribui para a formação de um cidadão autônomo e consciente.

No que diz respeito aos objetivos, os documentos apresentam similaridades e diferenças. O PCN, nos 3º e 4º ciclos, visa à competência métrica, levando o aluno a ampliar e construir noções de medida, e a resolver problemas que envolvam diferentes grandezas. O documento também sugere o estudo de grandezas determinadas pela razão ou produto de outras, como velocidade e densidade demográfica. A BNCC, nos anos finais, espera que os alunos reconheçam grandezas como comprimento, área, volume e abertura de ângulo, e que consigam resolver problemas utilizando unidades de medida padronizadas. O CRMG também enfatiza o desenvolvimento de atitudes éticas e sustentáveis em relação ao consumo.

A análise detalhada das habilidades nos documentos para os anos finais do Ensino Fundamental (6º ao 9º ano) revela um aprofundamento progressivo do tema:

- 6º Ano: O foco é em problemas envolvendo grandezas como comprimento, massa, tempo, temperatura, área e volume, sem o uso de fórmulas.
- 7º Ano: As habilidades incluem o cálculo de volume de blocos retangulares, o estabelecimento de expressões de cálculo de área de triângulos e quadriláteros, e a compreensão da medida do comprimento da circunferência.
- 8º Ano: O estudo se aprofunda na área de figuras planas e do círculo, e no cálculo de volume de cilindro reto, além de medidas de capacidade.
- 9º Ano: Os alunos devem reconhecer e empregar unidades de medida para distâncias muito grandes ou pequenas, além de trabalhar com volume de prismas e cilindros.

A análise revela que os documentos curriculares brasileiros, através do eixo Grandezas e Medidas, buscam superar um ensino meramente técnico. Eles se complementam na formação de cidadãos capazes de aplicar conhecimentos matemáticos de forma crítica e contextualizada, respondendo às demandas sociais contemporâneas. Essa convergência transforma o tema em ponte entre teoria matemática e prática cotidiana, além de eixo integrador com outras áreas do conhecimento. Assim, fica uma reflexão: se os relacionam uma abordagem contextualizada, alinhada para a formação cidadã, como nossos alunos continuam com dificuldades nesses conceitos?

Referências

[1] Brasil, *Base Nacional Comum Curricular*. Brasília: MEC, 2018.

[2] Brasil, *Parâmetros Curriculares Nacionais: Matemática*. Brasília: MEC/SEF, 1998.

[3] SEE/MG and UNDIME-MG, *Currículo Referência de Minas Gerais*. Minas Gerais: Secretaria da Educação, 2024.

[4] L. R. Silva, "Unesco: Os quatro pilares da "educação pós-moderna"," *Revista Inter-Ação*, vol. 33, p. 359–378, dez. 2008.

Compacidade na Topologia Fraca*: o Teorema Alaoglu-Bourbaki

Vanessa Coelho dos Santos [1]
Eduard Toon [2]

O Teorema de Tychonoff é um resultado com aspecto topológico que possui equivalência a dois importantes resultados da Teoria de Conjuntos: o Axioma da Escolha e o Lema de Zorn. A equivalência existente entre esses três resultados possibilita que seja feita a prova de um importante resultado da Análise Funcional: o Teorema Alaoglu-Bourbaki.

Em espaços normados de dimensão finita, bolas fechadas unitárias são sempre compactas. No entanto, em dimensão infinita, essa propriedade falha na topologia da norma, o que motiva o estudo da topologia fraca e o uso do Teorema de Alaoglu-Bourbaki para contornar a falta dessa compacidade. Neste trabalho, exploramos o Teorema de Alaoglu-Bourbaki para garantir compacidade na topologia fraca* em espaços de dimensão infinita.

Referências

[1] Erwin Kreyszig, *Introductory Functional Analysis with Applications*, John Wiley & Sons, New York, 1978.

[2] J. R. Munkres, *Topology*, 2ª ed., Prentice Hall, Upper Saddle River, NJ, 2000.

[1]Universidade Federal de Juiz de Fora, coelho.vanessa@estudante.ufjf.br

[2]Universidade Federal de Juiz de Fora, eduard.toon@ufjf.br

Análise da aplicação de uma proposta didática para o ensino de Matemática Financeira no ensino médio

Edilamar Rodrigues de Melo Maciel Campos [1]
Viviane Pardini Valério[2]
Wilker Thiago Resende Fernandes[3]

A Matemática Financeira desempenha um papel crucial na formação educacional dos estudantes, especialmente na educação básica. Sua importância transcende a simples habilidade de realizar cálculos financeiros, abrangendo competências essenciais para a vida cotidiana, como o planejamento e a gestão de recursos. A Base Nacional Comum Curricular (BNCC) [1], destaca a relevância da Matemática Financeira ao estabelecer, por exemplo, que os estudantes do ensino médio desenvolvam habilidades como: interpretação de taxas e de índices de natureza socioeconômica, elaboração e resolução problemas envolvendo porcentagens, criação e a utilização de planilhas para o controle do orçamento familiar e para o cálculo de juros compostos. Alinhado a essas habilidades, o Currículo Referência de Minas Gerais [2] fornece uma orientação pedagógica para que nós, professores, possamos trabalhá-las de forma integrada, utilizando exemplos práticos do cotidiano (reais ou hipotéticos), como os investimentos financeiros, e incentivando a interdisciplinaridade, com o uso de ferramentas como calculadoras gráficas, planilhas eletrônicas e softwares de matemática para a realização de cálculos. O ensino de Matemática Financeira, e também de Educação Financeira, tem sido o foco de diversas dissertações do PROFMAT. Alguns desses trabalhos se baseiam na BNCC e fornecem novas ideias ou análises sobre como aperfeiçoar o ensino desses tópicos, como é o caso dos trabalhos [3] e [4].

Visando contribuir com os estudos voltados ao ensino de Matemática Financeira no ensino médio, desenvolvemos uma pesquisa delineada através de uma proposta didática e dois questionários. A proposta didática, elaborada com base nos documentos norteadores da BNCC e do Currículo Referência de Minas Gerais, pautou-se no uso de diferentes metodologias e recursos tecnológicos, colocando sempre o estudante como foco e protagonista do seu aprendizado. Nela, foram abordados tópicos de Matemática Financeira como: fluxo de caixa, juros simples e compostos, taxas de juros, acréscimos e descontos, lucro e prejuízo, sistemas de amortização, investimentos de renda fixa e uma introdução sobre como utilizar planilhas eletrônicas para fazer os cálculos relacionados aos conteúdos descritos acima. A abordagem metodológica desses conteúdos pautou-se, principalmente, através da resolução de problemas que se inserem na realidade dos discentes de forma

[1]Discente do PROFMAT Universidade Federal de São João del-Rei
edilamar.campos@educacao.mg.gov.br
[2]Professora Coorientadora Universidade Federal de São João del-Rei,
vivipardini@ufsj.edu.br
[3]Professor Orientador Universidade Federal de São João del-Rei,
wilker@ufsj.edu.br

a instigá-los a buscar as soluções para situações do seu cotidiano, como defendem, por exemplo, [5] e [6]. Os questionários, sendo um deles aplicado antes da execução da proposta didática e o outro após, foram elaborados com dez questões de múltipla escolha acerca do tema trabalhado. Cada questão foi pensada para que extraísse o conhecimento dos discentes sobre pontos específicos do conteúdo. No questionário inicial a pergunta foi feita de forma mais simples e direta e no questionário final mais elaborada e aplicada. Dessa forma esperávamos não apenas verificar um ganho de conhecimento teórico, mas também desenvoltura na aplicação desse conhecimento.

Nesta apresentação, faremos uma análise tanto quantitativa (a partir das respostas dos questionários) quanto qualitativa (com base nas observações realizadas em sala de aula durante a aplicação da proposta) dos resultados da pesquisa. Os resultados evidenciam uma melhora significativa na compreensão dos discentes em relação aos conceitos de Matemática Financeira e, além do desenvolvimento/consolidação das habilidades de realizar cálculos, observamos o desenvolvimento da capacidade crítica de análise e aplicação desses conceitos em contextos variados, o que nos leva a concluir que a proposta foi eficaz. Faremos também uma discussão sobre pontos onde a proposta pode ser aprimorada e sobre a percepção das dificuldades e estratégias para o ensino de Matemática Financeira no ensino médio.

Referências

[1] Brasil, *Base nacional comum curricular*. Brasília: Ministério da Educação, 2018.

[2] M. Gerais, *Currículo Referência de Minas Gerais*. Belo Horizonte: Secretaria de Estado de Educação de Minas Gerais, 2025. https://curriculoreferencia.educacao.mg.gov.br/.

[3] M. N. Silva, "Análise e aplicação do estudo da educação financeira para jovens do ensino médio, com ênfase na comparação entre financiamento e investimento, no âmbito em uma escola estadual do rio de janeiro.," Master's thesis, UFRRJ, 2024.

[4] A. A. Couto, "Educação financeira: uma proposta didática em sala de aula com o uso de planilhas eletrônicas.," Master's thesis, UFG, 2024.

[5] G. Polya, *A arte de resolver problemas. Tradução e adaptação de Heitor Lisboa de Araújo*. Rio de Janeiro: Interciências, 1986.

[6] J. Dewey, *Como pensamos : como se relaciona o pensamento reflexivo com o processo educativo; uma reexposicao*. São Paulo: Nacional, 1959.

Caracterização das variedades de δ-Expoente 2

Yngrid Barbosa da Costa [1]

Neste trabalho, iremos estudar o conceito de δ-Expoente de uma variedade $\mathcal{V} = var(A)$, onde A é uma álgebra associativa que gera $\mathcal{V}$, sobre um corpo F algebricamente fechado e de característica zero. O δ-Expoente é utilizado para estudar o crescimento dos polinômios centrais próprios da variedade $\mathcal{V}$, ou seja, os polinômios centrais de $\mathcal{V}$ que não são identidades. A fim de estudar esse crescimento, Regev introduziu em [1] a sequência numérica $\{c_n^\delta(A)\}_{n\geq 1}$, de modo que

$$c_n^\delta(A) = \dim_F \left(\frac{P_n \cap Id^z(A)}{P_n \cap Id(A)} \right),$$

onde $P_n = span_F\{x_{\sigma(1)} \dots x_{\sigma(n)}; \sigma \in S_n\}$, $Id(A)$ é o conjunto das identidades de A e $Id^z(A)$ é o conjunto do polinômios centrais de A. Em [2], Giambruno e Zaicev demonstraram que essa sequência tem crescimento exponencial ou é limitada polinomialmente, o que gerou o interesse em estudar a sequência $\{\sqrt[n]{c_n^\delta(A)}\}_{n\geq 1}$ e definir o δ-Expoente de A como

$$exp^\delta(A) = \lim_{n\to\infty} \sqrt[n]{c_n^\delta(A)}.$$

Giambruno e Zaicev demonstraram também, no trabalho [3], que esse limite existe e é um inteiro não-negativo.

Dada uma variedade $\mathcal{V} = var(A)$, definimos $exp^\delta(\mathcal{V}) := exp^\delta(A)$. Então, vamos estudar a caracterização das variedades que possuem δ-Expoente maior que 2, vista em [4], e juntamente com o resultado trabalhado em [5], será possível concluir uma caracterização das variedades que possuem δ-Expoente exatamente 2.

Referências

[1] Amitai Regev. Growth for the central polynomials. *Communications in Algebra*, 44(10):4411–4421, 2016.

[2] Antonio Giambruno and Mikhail Zaicev. Central polynomials and growth functions. *Israel Journal of Mathematics*, 226:15–28, 2018.

[3] Antonio Giambruno and Mikhail Zaicev. Central polynomials of associative algebras and their growth. *Proceedings of the American Mathematical Society*, 147(3):909–919, 2019.

[1]Universidade Federal de Minas Gerais,
yngridbc@ufmg.br

[4] Francesca S. Benanti and Angela Valenti. A characterization of varieties of algebras of proper central exponent greater than two. *Journal of Algebra*, 679:96–116, 2025.

[5] Antonio Giambruno, Daniela La Mattina, and Cesar Milies. On almost polynomial growth of proper central polynomials. *Proceedings of the American Mathematical Society*, 152(11):4569–4584, 2024.