13° conpeex

congresso de pesquisa, ensino e extensão

Ciência **alimentando** o Brasil

ANAIS DO XIII CONPEEX

Congresso de Pesquisa, Ensino e Extensão
Universidade Federal de Goiás

De 17 a 19 de outubro de 2016

PICME

Apoio:

Realização:

Aluno	Trabalho
GEANNE OLIVEIRA RODRIGUES	Análise Fatorial e Psicologia
GUSTAVO RODRIGUES DOS REIS	AES (Advanced Encryption Standard) e corpos finitos.
HEITOR DE SOUSA NAVES	COMBINAÇÕES NÃO LINEARES DE REGISTROS DE DESLOCAMENTO APLICADAS A ¿STREAM CIPHERS¿
LUCAS GOMES DE MELLO	Galois e raízes de um polinômio
LUIZ GUSTAVO BARROS DOS SANTOS	Grupos Simples com ordem menor que 60
MARCOS LUCAS VELOSO JUNQUEIRA	Grafo de Ciclos - Aproximação para o problema de ordenação por reversões
MURILO RODRIGUES DE FREITAS	Funções Absolutamente Contínuas
ORIAL LINO DO NASCIMENTO JÚNIOR	ANÁLISE DA ASSISTÊNCIA ÀS GESTANTES NAS CAPITAIS BRASILEIRAS: UM AGRUPAMENTO BASEADO EM INDICADORES DE SAÚDE
VICTOR GONÇALVES NETTO	A CURVATURA DE GAUSS DE UMA SUPERFÍCIE REGULAR E SUA RELAÇÃO COM A CONSTRUÇÃO DE MAPAS DA TERRA
VINÍCIUS LOTI DE LIMA	ATIVIDADES DO PICME: Estudo de disciplinas básicas em preparação para o mestrado em matemática

Análise Fatorial e Psicologia

Geanne Oliveira Rodrigues [1], Eduardo Arbieto Alarcon [2]

1: Faculdade de Educação

Universidade Federal de Goiás - FE

e-mail: ge.anne.r@hotmail.com

2: Instituto de Matemática e Estatística

Universidade Federal de Goiás - IME

e-mail: arbietoalarcon@ufg.br

Palavras chaves: Psicologia; Análise Fatorial.

Em geral, a Psicologia trabalha com fenômenos não diretamente observáveis, sendo um de seus maiores desa os a operacionalização de conceitos abstratos em variáveis empirica- mente observáveis. Tal desa o justi ca a elaboração do presente trabalho, que pretendeelucidar o fato de que esses problemas podem ser superados por meio da análise fatorial, apresentando os elementos centrais desta. Para alcançar os objetivos propostos, realizou- se uma pesquisa bibliográ ca.

Durante a execução do projeto de pesquisa, entre agosto/2015 e julho/2016, foi realizado um encontro semanal com a orientador, em que eram discutidos os resultados de estudoacerca dos métodos matemáticos e da estatística aplicados a Psicologia , bem como te- oremas, resultados, e exemplos propostos pela orientador na semana anterior. Após a discussão, elaboramos trabalhos (listas de exercícios) com intuito de apresentar o conhe- cimento adquirido pela leitura dos livros escolhidos que melhor abordavam o tema.

Ao início do período de vigência da bolsa, pesquisamos a teoria fundamental dos méto- dos matemáticos, começando pela de nição de número real , funções, diferenciabilidade, integrabilidade de funções e exemplos. Esta etapa do cronograma serviu para introduzir, o conceito de probabilidade e variável aleatória . Estudo-se os fundamentos do Análise Fatorial e algumas aplicações, especi camente a Psicologia.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG

2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

Para o desenvolvimento do trabalho foi necessário os conhecimentos preliminares que podem ser encontrados mais detalhados em [1, 2, 4, 3].

Obteve-se uma compreensão e sedimentação dos conhecimentos adquiridos durante o programa de iniciação cientí ca, especialmente em relação a Análise Factorial, uma area de pesquisa da Estatística Matemática aplicado a Psicologia onde, a análise fatorial pode ser utilizada para reduzir um conjunto de variáveis a poucas dimensões. Em Psicologia, a análise fatorial desempenha um relevante papel na validação de instrumentos psico- lógicos. É importante salientar que tal método de análise, é um antigo conhecido da Psicologia e teve como um de seus pioneiros o Psicólogo Charles Spearman, que ainda em 1904 testou a hipótese de que diferentes testes de habilidade mental- habilidades emmatemática, verbais, raciocínio lógico, entre outras - poderiam ser explicadas por um fator

comum de inteligência que ele denominou g. (FIGUEIREDO; SILVA, 2010, p.4 [4]) Para realizar um psicodiagnóstico, a Psicologia se utiliza de diversos testes, regularizados no Brasil pelo CFP (Conselho Federal de Psicologia). De acordo com Alves, Souza e Bap- tista (2011)- [1], para que um desses instrumentos seja aprovado para uso pro ssional e comercialização, ele precisa possuir evidências empíricas de validade e precisão. Validade diz respeito, basicamente, a comprovação de que o instrumento mede exatamente aquilo que se propõe a medir, sendo que em um teste, são avaliadas a validade de conteúdo, de critério, e de constructo. A última, conta com uma relevância particular da análise fatorial. (DANCEY; REIDY, 2006- [2]) Os questionários de avaliação psicológica, geralmente apresentam diversas questões relacionadas a um constructo, de forma que certas questões se relacionam entre si por mencionarem o mesmo constructo. Tais constructos, são utilizados para descrever as escalas de um teste. Assim, a análise de fatores permite

que o pesquisador descubra a validade fatorial das questões que compõem cada escala ou

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

constructo (DANCEY; REIDY, 2006, p; 423- [2])

A análise fatorial é um importante método de análise na construção e validação de testes psicológicos, sendo utilizada há anos pelos pro ssionais dessa área e permitindo a redução de um conjunto de variáveis a poucas dimensões.

[1] ALVES, G.; SOUZA, M.; BAPTISTA, M. , Validade e precisão de testes psicológicos.AMBIEL, R. et al. (Org). Avaliação Psicológica: Guia de consulta para estudantes e pro ssionais da psicologia. São Paulo: Casa do Psicólogo, 2011. p. 109-128.

[2] DANCEY, C. D.; REIDY, J. Introdução à análise de fatores, Estatística sem matemática para psicologia: Usando SPSS para Windows. Porto Alegre: Artmed, 2006. p. 420-455.

[3] LIMA E. L., Análise Real , Rio de Janeiro: IMPA, Terceira Edição, (1997).

[4] FIGUEIREDO, B. D.; SILVA J. A. Visão além do alcance: Uma introdução à análisefatorial, Opinião Pública, Campinas, v. 14, n. 1, p. 160-185, 2010.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

AES (ADVANCED ENCRYPTION STANDARD) E CORPOS FINITOS

9 de Setembro de 2016

Serconek, Shirlei[1]

Reis, Gustavo Rodrigues dos[2]

Palavras Chave: AES, Block Ciphers, Corpos Finitos, Galois

Introdução

A Teoria de Galois teve início com os trabalhos escritos pelo matemático francês Évariste Galois (1811-1832), que estabelecendo a conexão do conceito de grupos com o de corpos, possibilitou um grande avanço na área de Álgebra, colaborando para o surgimento de inúmeros estudos e aplicações posteriores e que são bastante investigados e usados atualmente.

O Advanced Encryptation Standard (AES), novo padrão de criptografia em blocos utilizado nos Estados Unidos, anunciado em 2001 pelo Instituto Nacional de Padrões e Tecnologia (NIST), que substituiu o Data Encryption Standard (DES), é o sistema denominado Rijndael, elaborado por dois criptógrafos belgas, Joan Daemen e Vincent Rijmen. Utilizando conceitos de Teoria de Galois aplicada à computação foi possível desenvolver um sistema criptográfico com alto grau de confiabilidade e segurança.

Justificativa

A Teoria de Galois possibilita a compreensão e a elaboração de métodos matemáticos para outras áreas correlatas, como engenharia e computação. Seu estudo vem sendo ainda mais estimulado pelas crescentes pesquisas e aplicações nestes campos.

A construção de Corpos de Galois que usa polinômios irredutíveis sobre o corpo base disponibiliza um novo conjunto de operações com seus elementos, que aliadas ao conceito de blocos de bits e sua representação em polinômios com coeficientes

1-Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG

2 Orientando – gleitor@gmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

em $\mathbb{Z}_2$, produz unicidade à mensagem criptografada, proporcionando mais segurança a mesma, nas comunicações digitais atuais.

Metodologia

Foram promovidos encontros semanais de orientação, além de pesquisa e estudo individual.

Resultados

No estudo de sistemas criptográficos em blocos conseguimos perceber a influência e a importância da Álgebra para a criação dos sistemas computacionais atuais. O algoritmo AES usa o Corpo de Galois: $\mathbb{F}_{2^8} = \frac{\mathbb{Z}_2[x]}{x^8+x^4+x^3+x+1}$. A estrutura de corpo destaca-se como uma ferramentas para maior segurança, confiabilidade do sistema criptográfico, bem como facilidade de implementação para a proteção de dados.

O estudo de estruturas algébricas foi fundamental para alcançar a compreensão dos sistemas AES e DES.

Conclusão

A matemática continua a desenvolver estruturas do conhecimento e evolução da tecnologia no mundo atual.

Conseguimos perceber a sua grande importância para a sociedade. Sem ela não conseguiríamos manter em funcionamento a movimentação segura de dados, por exemplo, e estaríamos desprotegidos, vulneráveis a ataques na transmissão de informações, e na manutenção da privacidade.

Referências

[1] Stinson, D.R. *Cryptography: Theory and Practice*, CRC, 2005

[2] Christoforus, J.B. *Galois Field in Cryptography*, Washington University, May 31,2012.

[3] Nover, H. Algebraic Cryptanalysis of AES, 1-6.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

National Institute of Standards and Technology, Advanced Encryption Standard, FIPS 197 (2011).

[4] Hernstein, I.N *Topics in Algebra*, John Wiley and Sons, 1975.

[5] McEliece, R.J. *Finite Fields for Computer Scientists and Engineers,* Kruwer Academic Publishers, 1987.

[6] *Federal Information Processing Data Encryption Standard*, Federal Register, August 1, 1975.

[7] Artigo Enciclopédico Finite Fields
< https://en.wikipedia.org/wiki/Finite_field >. Acesso em: 4 de setembro de 2016.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

COMBINAÇÕES NÃO LINEARES DE REGISTROS DE DESLOCAMENTO APLICADAS A "STREAM CIPHERS"

Heitor de Sousa NAVES[1]

Shirlei SERCONEK[2]

29 de agosto de 2016

Palavras-chave: Stream-Ciphers, Criptografia, Combinações, Segurança

INTRODUÇÃO

A criptografia é a ciência que estuda, entre outros, métodos para codificar uma mensagem de modo que apenas seu destinatário consiga interpretá-la.

Os sistemas de criptografia são classificados em: sistemas simétricos e sistemas assimétricos (ou de chave pública). Na criptografia assimétrica existem duas chaves, uma conhecida por chave pública e a outra por chave privada. Já a criptografia simétrica define uma única chave para cifrar e decifrar uma mensagem. Os algoritmos simétricos, por sua vez, podem ser subdivididos em algoritmos de bloco e algoritmos "stream ciphers". Um algoritmo é tanto mais poderoso (e eficiente) quanto mais resistente for à criptanálise, isto é, teoricamente o único método de descoberta da chave for o método da exaustão.

JUSTIFICATIVA

No mundo em que vivemos, totalmente baseado nas telecomunicações, a segurança da informação que é transmitida é primordial e a cada dia os modos de criptografar as mensagens são atualizados e aperfeiçoados.

OBJETIVOS

O objetivo de nosso estudo é um sistema que na sua concepção usa sequências com boas características estatísticas e que possua uma chave com tamanho adequado, atingindo um razoável nível de segurança computacional.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

METODOLOGIA

Foram realizados encontros semanais de orientação, além de pesquisas e estudos individuais.

RESULTADOS

Nossos estudos de "stream ciphers" nos levaram ao aprofundamento em registros de deslocamento com realimentação linear. Denotaremos um tal registro por LFSR (linear feedback shift register). Um algoritmo criptográfico do tipo "stream ciphers" fornece às mensagens cifradas boas propriedades aleatórias e assim um alto valor de complexidade linear. Mas estas propriedades somente não são suficientes para assegurar uma boa proteção. Visando melhorar ainda mais tais propriedades, passamos à análise de combinações de diferentes LFSR's.

Verificamos que algumas formas de combinar os LFSR's possuem um funcionamento prático bastante simples, como é o caso do Gerador de Geffe, mas que possuem propriedades algébricas bastante interessantes, que elevam bastante a complexidade linear da sequencia gerada em relação às sequencias originais que os LFSR's geram individualmente.

CONCLUSÃO

O estudo de criptografia e aplicações mostra que a matemática é primordial no desenvolvimento de nossa sociedade. Na era em que a Internet se torna um pilar, a segurança dos dados deve estar em constante desenvolvimento e a matemática, mais especificamente a álgebra mostram, então, sua força ao garantir, por meio da criptografia, a segurança das informações de cada indivíduo da sociedade e sua privacidade.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] GOLOMB, Solomon W., **Shift Register Sequences**, Rev Laguna Hills, Calif.: Aegan Park Press, 1982.

[2] SILVA, Elida A., **Produtos de Sequencias com Complexidade Linear Máxima**, IME-UFG, Goiânia, dissertação de mestrado, 1998.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

[3] SOUZA, Carmen L. S., **Complexidade Linear Aplicada à Teoria de Códigos**, IME-UFG, Goiânia, dissertação de mestrado, 2000.

[4] LEMOS, Glen C., **Uma Análise da Estrutura e Complexidade Linear de Sequencias Binarias Produzidas por Geradores não Lineares**, IME-UFG, Goiânia, dissertação de mestrado, 1999.

[5] LUCHETTI, Cinthya M. P., **O Algoritmo de Berlekamp-Massey e a Decodificação de Códigos BCH,** IME-UFG, Goiânia, dissertação de mestrado, 2000.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

GALOIS E RAÍZES DE UM POLINÔMIO

SERCONEK, Shirlei[1] **MELLO**,

Lucas Gomes de[2] 14 de setembro de

2016

Palavras-chave: Grupo de Galois, Lagrange, Equações Polinomiais.

INTRODUÇÃO

As equações polinomiais têm uma grande relevância na história da Matemática. Desde a antiguidade notamos o interesse de diversos povos em resolver determinados tipos de equações. Vários matemáticos, dentre eles Lagrange (1736-1813), estudaram o problema de encontrar uma solução para determinar as raízes de equações polinomiais em termos dos coeficientes da equação e radicais. Para as equações de segundo grau a solução foi dada pela fórmula de Bhaskara, para equações de terceiro grau a solução foi dada por Cardano (1501-1576) e Tartaglia (1500-1557). Algumas equações de quarto grau, as equações biquadradas, também tem solução. Porém para o problema de grau maior ou igual a 5, a resposta negativa foi dada por Evariste Galois (1811-1832) que para isto criou a teoria de grupos.

JUSTIFICATIVA

Ao resolver o problema acima citado Galois criou a teoria de grupos, uma das mais belas subáreas da Álgebra.

OBJETIVO

Buscamos neste trabalho, destacar a importância da contribuição e a genialidade do trabalho de Galois e claro seus antecessores, entre eles, Lagrange.

METODOLOGIA

Foram realizados encontros semanais de orientação, além de pesquisas e estudos individuais.

RESULTADOS

As fórmulas de Cardano possibilitam encontrar as raízes de um polinômio de 3º grau, solução também obtida por Lagrange. Entretanto o método de Lagrange só funcionava até polinômios de 4º grau, o que o fez suspeitar da impossibilidade de resolver equações de grau maior ou igual a

5. Então Abel provou em 1824 que a equação geral de grau 5 não é resolúvel por meio de radicais. Mas foi apenas no trabalho de Galois, publicado por Liouville em 1843, que encontramos uma solução que respondia precisamente quando um polinômio de grau maior ou igual a 5 é ou não resolúvel por meio de radicais.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

CONCLUSÃO

Certamente Galois foi um gênio e mostrou para o mundo uma bela teoria e também resultados que levam seu nome (Teoria de Galois).

REFERÊNCIAS

[1]___________. Das simetrias à Teoria de Galois. Disponível em: < http://www.ime.unicamp.br/~engler/notas1ma673.pdf>.

[2]___________. Equações do quinto grau: portais para outra dimensão. Disponível em<https://epxx.co/artigos/quinticas.html>.

[3] GONÇALVES, Adilson. Introdução à Álgebra. Editora Projeto Euclides, IMPA, 1979.

[4] GALLIAN, Joseph A. Contemporary Abstract Algebra. Editora BROOKS/COLE CENGAGE Learning, 8ª edição, 2012.

[5] STEWART, Ian. Galois Theory. Editora CHAPMAN & HALL/CRC, 3ª edição, 2000.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

GRUPOS SIMPLES COM ORDEM MENOR DO QUE 60

Luiz Gustavo Barros dos SANTOS[1]
Thaynara Arielly de LIMA[2]
Escola de Engenharia Civil[1]
Instituto de Matemática e Estatística[2]
luizgustavobarros@outlook.com[1]; thaynaradelima@gmail.com[2]

Palavras-chaves: Grupos, Grupos simples, Teorema de Sylow, Grupos solúveis.

1 Justificativa

O estudo de Teoria de Grupos é intrigante e atrativo, pois possibilita o contato com elementos teóricos e demonstrações matemáticas; isto desenvolve o raciocínio lógico e escrita matemática, o que contribui significamente para a formação de um estudante de Ciências Exatas.

2 Objetivo

Seja G um grupo e denote por $|G|$ a ordem de G. O objetivo é discutir o seguinte resultado:

Teorema 2.1. *Se* $|G| < 60$, *G é simples se, e somente se, $|G| = p$, onde p é um número primo.*

3 Metodologia

A demonstração do Teorema 2.1, será tratada de duas maneiras:

Primeiro método: utilizando basicamente os Teoremas de Sylow e Lagrange, e fazendo uma análise sobre a fatoração da ordem dos grupos de cardinalidade menor que 60;

Segundo método: utilizandooconceitode Grupos solúveise aplicandoos Teoremasde Burnside e Hall.

4 Resultados eDiscussão

Neste trabalho, por falta de espaço, analisaremos somente um caso de cada um dos métodos mencionados anteriormente. Para tais análises, precisaremos de definições e resultados preliminares. Algumas definições acerca de Teoria de Grupos serão admitidas e podem ser consultadas em (HERSTEIN, 1996).

Teorema 4.1 (Cauchy)**.** *Seja G um grupo finito e p um primo tal que p divide $|G|$. Então, existe um elemento $g \in G$ com ordem p.*

Teorema 4.2 (Sylow-1872)**.** *Seja G um grupo finito, tal que $|G| = p^{\alpha} \cdot m$ onde p é primo,* *M.D.C*$(p, m) = 1$ *e* $\alpha \geq 1$. *Então:*

a) *Quaisquer dois subgrupos* H_1 *e* H_2 *de G de ordem igual a* p^{α} *são conjugados em* G;

b) *O número* n_p *de subgrupos de G de ordem* p^{α} *é do tipo* $n_p = kp + 1$ *onde* $k \in$◆, *e* n_p *divide*$|G|$.

Definição 4.3. *Um grupoGéditosimplesseseusúnicossubgruposnormaissãootrivial e ele próprio.*

Lema 4.4. *Todogrupo de ordem prima é cíclico e simples.*

Definição 4.5. *Um grupo G é dito solúvel se contém uma cadeia de subgrupos* $\{id\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$, *tal que cada* G_{i-1} *é normal em* G_i *e o grupo quociente* $\frac{G_i}{G_{i-1}}$ *é abeliano para*$1 \leq i \leq n$.

Teorema 4.6 (Hall). *Seja G um grupo finito e q, r e p números primos distintos. Se* $|G| = pqr$, *então G é solúvel.*

4.1 PrimeiroMétodo

Por falta de espaço, analisaremos somente o caso em que $|G| = mp^{\alpha}$, em que p é um número primo.

Proposicão 4.7. *Se G é um grupo tal que* $|G| = mp^{\alpha}$ *onde p é primo e* $1 < m < p$, *então G não é simples.*

Demonstração. Pelo teorema de Sylow, $Syl_p f = \emptyset$, $n_p | m$ e $n_p \equiv 1 (\mathrm{mod}\, p)$. Como $m < p$ só podemos ter $n_p = 1$. Consequentemente, o único p-Sylow subgrupo é normal, e G não é simples.

□

4.2 Segundo Método

Por motivo de espaço, analisaremos apenas o caso em que $|G| = pqr$. Tal análise baseia-se no Teorema de Hall.

Demonstração. Da definição temos que se G é solúvel e não abeliano G possui um subgrupo normal. Logo, G não é simples. Se $|G| < 60$ e G é abeliano, temos apenas as seguintes possibilidades para ordem de G, ou $|G| = p^a q^b$ ou $|G| = pqr$, onde p,q e r são números primos distintos. Caso, $|G| = pqr$, G não é simples, pois o teorema de Cauchy garante que exista $g \in G$ tal que $|g| = p$ se tomarmos o subgrupo normal em G, mostrando que ele não é simples.

□

5 CONCLUSÃO

Neste trabalho, discutiu-se a não simplicidade de grupos de ordem menores do que 60 não prima. Usou-se duas abordagens para argumentar tal resultado: uma baseada principalmente nos Teorema de Sylow e Langrange e outra utilizando os Teoremas de Burnside e Hall.

REFERÊNCIAS

DUMMIT, D. S.; FOOTE, R. M. *Abstract algebra*. [S.l.]: Wiley Hoboken, 2004. v. 3. Nenhuma citação no texto.

GARCIA, A.; LEQUAIN, Y. *Algebra: um curso de introduçao*. [S.l.]: IMPA, 1988. Nenhuma citação no texto.

HERSTEIN, I. N. *Abstract algebra*. Third. [S.l.]: Prentice Hall, Inc., Upper Saddle River, NJ, 1996. xviii+249 p. With a preface by Barbara Cortzen and David J. Winter. ISBN 0-13-374562-7. Citado na página 2.

MARTIN, P. A. *Introdução a teoria dos grupos e a teoria de Galois*. [S.l.]: IME-USP, 1998. Nenhuma citação no texto.

Grafo de Ciclos - Aproximação para o problema de ordenação por reversões

Marcos Lucas Veloso JUNQUEIRA, **Thaynara Arielly de LIMA**, **Kélem Gomes LOURENÇO** UFG - *marcosjunqueira@inf.ufg.br*, UFG - *thaynaradelima@gmail.com*, UFG - *kelem.gomes@ufg.br* **Palavras-chave:** Ordenação, Reversões,1.5-Aproximativo

Encontrar a distância entre genomas de dois organismos é um problema de relevância, pois nos permite avaliar o grau de parentesco entre dois seres e possibilita a construção de árvores filogenéticas. A distância entre dois genomas pode ser medida através do número mínimo de mutações necessárias para se transformar um organismo em outro. Neste trabalho considera- mos a operação de reversão representando tais mutações. Um genoma será representado por uma permutação $\pi = [\pi(1)\ldots\pi(i)\ldots\pi(j)\ldots\pi(n)]$ tal que $\pi(i) \in \{1,\ldots,n\}$, $1 \leq i \leq n$. Uma reversão $\rho(i,j)$ aplicada em π gera a permutação $\pi\rho = [\pi(1)\ldots\pi(j)\ \pi(j-1)\ldots\pi(i)\ldots\pi(n)]$. O problema da distância de reversões consiste em encontrar o número mínimo de reversões ne- cessárias para se transformar uma permutação π na identidade $[1\ 2\ldots n]$. Caprara[1] mostrou que o problema da distância de reversões é NP-Difícil. Neste sentido, estão presentes na litera- tura heurísticas que fornecem soluções aproximadas para o cálculo da distância de reversões entre duas permutações. Em [2], Christie apresenta um algoritmo aproximativo com raio 1.5 para o problema da distância de reversões. Tomando por base uma implementação já existente de tal algoritmo [3], implementamos uma variante e comparamos os resultados obtidos com oalgoritmo genético proposto em[3].

É necessário, para o entendimento do algoritmo, o conceito de Grafos de Ciclos. Dada uma permutação $\pi = [\pi(1)\ldots\pi(n)]$ de comprimento n, estenda tal permutação transformando-a em $[0\ \ \pi(1)\ldots\pi(n)\ \ n+1]$. O Grafo de Ciclos $G(\pi)$ é um grafo de arestas coloridas, com $n+2$ vértices, em que cada vértice está associado a um elemento $\pi(i)$ de π. Neste, dois vértices são conectados por uma aresta preta caso representem um ponto de quebra em π e são conectados por uma aresta cinza caso representem um ponto de quebra em π^{-1}. Se uma reversão ρ é tal que $G(\pi\rho)$ possui k arestas cinzas (e, consequentemente, pretas) a menos que $G(\pi)$, ρ é dita uma k-reversão.

Preservando a abstração dada no artigo[2], o algoritmo se baseia na construção e manipulação do grafo de reversões tido sobre o Grafo de Ciclos da permutação dada. Em nosso trabalho, foi utilizada a linguagem C++ na implementação do algoritmo 3/2-Aproximativo apresentadoabaixo.

Algoritmo 3/2-Aproximativo para ordenação por reversões:

Entrada: Uma permutação π com tamanho n.

1. Construir o Grafo de Ciclos $G(\pi)$ sobre π;
2. Estabelecer uma decomposição cíclica C sobre $G(\pi)$;
3. Determinar o Grafo de Reversões $R(C)$ inicial sobre C;
4. Encontrar uma sequência de eliminação para $R(C)$.

Tomando como exemplo a permutação $[1\ 7\ 6\ 4\ 2\ 5\ 3]$, podemos acompanhar o proces- samento do algoritmo na figura 1. No grafo de ciclos resultante, figura 1-(a), podemos destacar o ciclo alternante (1, 2, 4, 3, 8, 7, 1). Note que é possível decompor o grafo de ciclos em ci- clos alternantes de arestas disjuntas; essa decomposição não é única. Descrita no artigo [2], temos uma relação denotando que, em maior quantidade de ciclos na decomposição cíclica, temos uma menor quantidade de reversões necessárias. Assim, através do denominado Grafo de Acoplamento, figura 1-(b), que relaciona os 2-ciclos existentes no grafo, procuramos obter o acomplamento máximo, escolhendo, portanto, a decomposição cíclica com maior número de 2-ciclos possíveis; para nosso exemplo, obtemos a decomposição cíclica na figura1-(c).

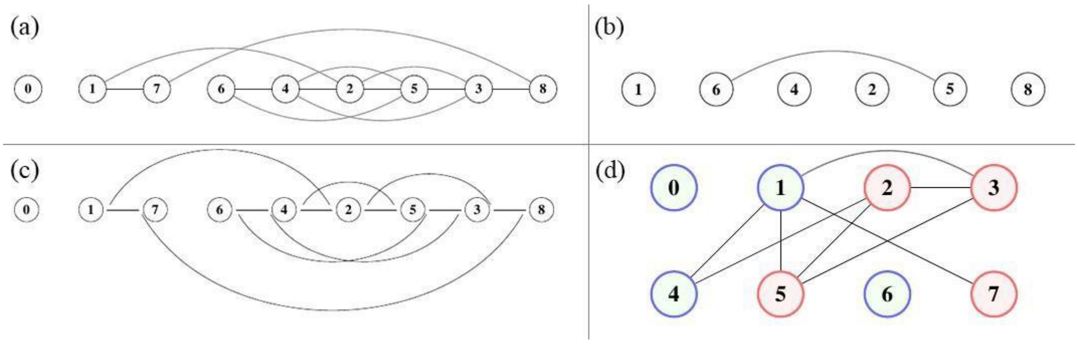

Figura 1: Grafos montados para o exemplo $[1\ \ 7\ \ 6\ \ 4\ \ 2\ \ 5\ 3]$

Para o próximo passo do algoritmo, é utilizada a estrutura do Grafo de Reversões:

(**Grafo de Reversões**) Dada uma decomposição cíclica C de π, o grafo de reversões $R(C)$ atende às propriedades: para cada par adjacentes de elementos em π que não são conectados por uma aresta preta em $G(\pi)$ existe um vértice azul isolado e, para cada aresta cinza em $G(\pi)$ existe um vértice colorido da seguinte forma: é colorido azul caso pertença a um ciclo em C em que a aresta cinza correspondente conecta a cabeça da aresta preta à cauda de outra aresta preta; caso contrário é colorido vermelho; dois vértices são conectados por uma aresta caso suas arestas cinzas se entrelacem em C; cada vértice corresponde a uma reversão aplicada sobre as arestas pretas adjacentes à cinza no ciclo C que a aresta cinza associada ao vértice pertence.

Segundo a definição dada, encontramos o grafo de reversões apresentado na figura 1-(d). Na abstração de componentes dada em [2], é seguido o seguinte algoritmo para encontrar a sequência de reversões.

Algoritmo para Sequência de Eliminação:

Entrada: Um Grafo de Reversão $R(\pi)$.

1. Enquanto $R(C)$ não for constituído apenas de vértices azuis isolados repita os passos de 2 e 3;
2. Para cada componente conexa B não-orientada em $R(C)$ aplique uma reversão sobre um vértice v para que todos os componentes de B_v sejam orientados;
3. Para cada componente conexa A orientada em $R(C)$, aplique uma reversão em um vértice vermelho v tal que todos os componentes de A_v sejam orientados. Repita esse processo até que A seja totalmente eliminada.

Garantido pelos lemas apresentados em [2], o algoritmo encontra uma sequência de reversões que ordena π. Concluímos então os passos de execução do algoritmo encontrando a sequência sobre os índices de π: $[6,7],[5,7],[2,7],[4,5]$. Após a implementação do algoritmo proposto em [2] e corrigido em [3], obtemos os seguintes resultados.

Tam	Qt	1.5 Approx	Total Rev.	Genetic Approx	Total Rev.
10	33	5.78	191	5.85	193
30	147	22	3234	22.04	3240
50	282	39.52	11144	39.8688	11243
70	429	57.60	24712	58.3636	25038
90	584	76.03	44401	77.0873	45019
110	745	94.61	70481	95.7517	71335
130	912	113.57	103575	115.001	104881
150	1084	132.65	143794	134.044	145304

Referências

[1] Alberto Caprara, *Sorting by reversals is difficult*, RECOMB, 1997, pp. 75–83.

[2] David A. Christie, *A 3/2-approximation algorithm for sorting by reversals*, Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 1998), ACM, New York, 1998, pp. 244–252. MR 1642934

[3] José Luis Soncco-Álvarez and Mauricio Ayala-Rincón, *A genetic approach with a simple fitness function for sorting unsigned permutations by reversals*, Computing Congress (CCC),2012 7th Colombian, IEEE, 2012, pp. 1–6.

FUNÇÕES ABSOLUTAMENTE CONTÍNUAS*

Abiel, C. Macedo & Murilo R. de Freitas

Resumo

Neste trabalho apresentamos uma introdução básica ao estudo de funções de variaçãoo limitada e absolutamente continuas visando estabelecer alguns os pré-requisitos básicos para para o estudo do problema de estabilidade bidimensional de um fluido viscoso entre cilindros rotativos[1]. Os estudos aqui apresentados estão em sua maioria baseados em Royden [2].

1 Introdução

Os espaços de funções consistem no ambiente principal para busca de soluções de problemas oriundos da Física, Química, Biologia, Engenharia e etc. Buscamos a introdução às funções absolutamente contínuas para o estudo da estabilidade bidimensional de um fluido viscoso entre cilindros rotativos[1]. Este espaço consiste no ambiente onde o problema, sobre certas hipóteses, pode ser resolvido.

Os espaços de funções são de extrema importância na solução de problemas reais. Neste contexto fica evidente a necessidade do estudo e compreensão dos mesmo.

2 Resultados Principais

Definição 2.1. *Seja* f *integrável sobre o intervalo fechado e limitado* $[a, b]$*. Estenda* f *para pegar o valor* $f(b)$ *em* $(b, b+1]$*. Para* $0 < h \leq 1$*, definimos a função de diferença dividida* $\mathrm{Diff}_h f$ *e a função do valor médio* $\mathrm{Av}_h f$ *de* $[a,b]$ *por*

$$\mathrm{Diff}_h f(x) := \frac{f(x+h)-f(x)}{h} \quad \text{e} \quad \mathrm{Av}_h f(x) = \frac{1}{h}\int_x^{x+h} f \quad \text{para todo } x \in [a,b].$$

*Artigo submetido ao 13° CONPEEX

†Instituto de Matemática e Estatística, UFG, GO, Brasil, abielcosta@gmail.com

‡Instituto de Matemática e Estatística, UFG, GO, Brasil,

Definição 2.2. *Se c pertence a (a, b), P é uma partição de $[a.b]$, e P^r é o refinamento de P obtido adicionando c*

a P, ent˜ao, pela desigualdade triangular, $V(f, P) \leq V(f, P^r)$. Assim, na defini¸c˜ao da varia¸c˜ao total de uma func¸˜ao

em $[a, b]$, o supremo pode ser tomado sobre partições de $[a, b]$ que contém o ponto c. Agora uma partição P de $[a, b]$ que contém o ponto c induz, e é induzida por, partições de $P1$ e $P2$ de $[a, c]$ e $[c, b]$, respectivamente, e para tais parti¸c˜oes,

$$V(f[a,b], P) = V(f[a,b], P1) + V(f[a,b], P2).$$

Pegue o supremo ao longo de tais parti¸c˜oes para concluir que

$$TV(f[a,b]) = TV(f[a,c]) + TV(f[c,b]).$$

Inferimos a partir disso que se f ´e de varia¸c˜ao limitada em $[a, b]$, ent˜ao

$$TV(f[a,v]) - TV(f[a,u]) = TV(f[u,v]) \geq 0 \text{ para todo } a \leq u < v \leq b. \tag{2.1}$$

Portanto a função $x \to TV(f[a,x])$, que nós chamamos função de variação total para f, é uma função crescente de valores reais em $[a, b]$. Além disso, para $a \leq u < v \leq b$, se tomarmos a partição mais crua $P = \{u, v\}$ de $[u, v]$, temos

$$\begin{aligned} f(u) - f(v) &\leq |f(v) - f(u)| \\ &= V(f[u,v], P) \\ &\leq TV(f[u,v]) \\ &= TV(f[a,v]) - TV(f[a,u]) \end{aligned}$$

Assim,

$$f(v) + TV(f[a,v]) \geq f(u) + TV(f[a,u])$$

para todo $a \leq u < v \leq b$.

Lema 2.1. *Seja que a função f seja de variação limitada no intervalo fechado e limitado $[a, b]$. Então f tem a seguinte express˜ao impl´ıcita como a diferen¸ca de duas func¸˜oes crescentes em $[a, b]$:*

$$f(x) = [f(x) + TV(f[a,x])] - TV(f[a,x]) \tag{2.2}$$

para todo $x \in [a,b]$.

Definição 2.3. *Uma função de valor real f em um intervalo fechado e limitado $[a, b]$ é dita absolutamente contínua em $[a, b]$ se para todo $\varepsilon > 0$, existe um $\delta > 0$ tal que para toda coleção finita disjunta $\{(a_k, b_k)\}_{k=1}^{n}$ de intervalos abertos em (a, b),*

$$\text{se } \sum_{k=1}^{n} [b_k - a_k] < \delta, \text{ então } \sum_{k=1}^{n} |f(b_k) - f(a_k)| < \varepsilon.$$

O critério para continuidade absoluta no caso de coleção finita de intervalos consistem de um intervalo único é o critério para continuidade uniforme de f em $[a,b]$. Assim, funções absolutamente contínuas são contínuas. O contrário é falso, mesmo com funções crescentes.

Proposição 2.1. *Se a função f é Lipschitz em um intervalo fechado e limitado $[a,b]$, então ela é absolutamente contínua em $[a,b]$.*

Demonstração. Seja que $c > 0$ seja uma constante de Lipschitz para f em $[a,b]$, tal que,

$$|f(u) - f(v)| \leq c \cdot |u - v| \text{ para todo } u, v \in [a,b].$$

Então, em relação ao critério para continuidade absoluta de f, é claro que $\delta = \frac{s}{c}$ □

Teorema 2.1. *Seja f uma função absolutamente contínua no intervalo fechado e limitado $[a,b]$. Então f é a diferença entre funções absolutamente contínuas e, em particular, de variação limitada.*

Teorema 2.2. *Seja f uma função contínua no intervalo fechado e limitado $[a,b]$. Então f é absolutamente contínua em $[a,b]$ se, é somente se, a família de funções de diferença dividida $\{\mathrm{Diff}_h f\}_{0<h\leq 1}$ é uniformemente integrável sobre $[a,b]$.*

Prova do Teorema 2.1: Primeiro provamos que f é de variação limitada. De fato, defina δ que responda ao desafio $s = 1$ com relação ao critério de continuidade absoluta de f. Faça P uma partição do intervalo $[a,b]$ em N intervalos fechados $\{[c_k, d_k]\}_{k=1}^N$ cada um de um tamanho menor que δ. Então, pela definição de δ em relação à continuidade absoluta de f, está claro que $TV(f_{[c_k,d_k]}) \leq 1$, para $1 \leq k \leq n$. A fórmula de aditividade estende para somas finitas.

Consequentemente

$$TV(f) = \sum_{k=1}^{N} TV(f_{[c_k,d_k]}) \leq N.$$

Portanto f é de variação limitada.

Tendo em vista (2.2) e a continuidade absoluta de somas de funções absolutamente contínuas, para mostrar que f é a diferença de funções absolutamente contínuas crescentes basta mostrar que a função da variação total para f é absolutamente contínua. Seja $s > 0$. Escolha δ que corresponda a $\frac{s}{2}$ em relação ao critério de continuidade absoluta de f em $[a,b]$. Seja $\{(c_k, d_k)\}$ uma coleção disjunta de subintervalos abertos de (a,b) tal que $\sum_{k=1}^{n} [d_k - c_k] < \delta$.

Para $1 \leq k \leq n$, deixe que P_n seja uma partição de $[c_k, d_k]$. Pela escolha de δ em relação à continuidade absoluta de f em $[a,b]$.

$$\sum_{k=1}^{n} TV(f_{[c_k,d_k]}, P_n) < \frac{s}{2}$$

Pegue o supremo como, para $1 \leq k \leq n$, P_k varia ao longo das partições de $[c_k, d_k]$, para obter

$$\sum_{k=1}^{n} TV(f_{[c_k,d_k]}, P_k) \leq \frac{s}{2} < s$$

Inferimos de (2.1) que, para $1 \leq k \leq n$, $TV(f_{[c_k,d_k]}) = TV(f_{[a,d_k]}) - TV(f_{[a,c_k]})$. Consequentemente, se

$$\sum_{k=1}^{n} [d_k - c_k] < \delta, \text{ entao } \sum_{k=1}^{n} |TV(f_{[a,d_k]}) - TV(f_{[a,c_k]})| < s$$

Portanto, a função de variação total para f é absolutamente contínua em $[a,b]$.

Refer^encias

[1] Ali, Halima N.; Herron, Isom H.: *The two-dimensional stability of a viscous fluid between rotating cylinders* Journal of Mathematical Analysis and Applications **203** (1996), no. 2, 481–489.

[2] Royden, H. L. *Realanalysis*. Third edition. Macmillan Publishing Company, New York, 1988.

[3] Rudin, W.: *Principlesofmathematicalanalysis* Thirdedition. International Seriesin Pureand Applied Mathe- matics. McGraw-Hill Book Co., New York-Auckland-Du¨sseldorf, 1976.

ANÁLISE DA ASSISTÊNCIA ÀS GESTANTES NAS CAPITAIS BRASILEIRAS: UM AGRUPAMENTO BASEADO EM INDICADORES DE SAÚDE*

Orial Lino do Nascimento JÚNIOR

Orientando – orial.lino@gmail.com – Faculdade de Medicina, UFG

Everton Batista da ROCHA

Orientador – evertonbatista@ufg.br – Instituto de Matemática e Estatística, UFG

Palavras-Chave: Assistência às Gestantes, Capitais, Álgebra de Matrizes.

Introdução

A falta ou assistência inadequada durante o pré-natal podem trazer graves consequências para a saúde da mãe e do feto. Segurança na assistência obstétrica se reveste de grande importância ao se considerar o elevado número de pacientes envolvidos, uma vez que são aproximadamente 3 milhões de nascimentos acontecendo a cada ano no Brasil, resultando em mais de 6 milhões de pacientes, entre parturientes e recém-nascidos [2].

Justificativa

Abordar por meio de indicadores pré-estabelecidos as dificuldades e carências da assistência pré-natal e obstétrica nas capitais brasileiras, onde vivem mais de 47 milhões de pessoas, ou seja, cerca de um quarto da população do país [1] tornará possível saber como se assemelham e diferem tais localidades e quais as dificuldades comuns que elas enfrentam no fornecimento deste tipo de cuidado que é tão essencial, justificando este estudo.

Objetivos

Por meio de conceitos de Estatística Multivariada, em particular Análise de Agrupamentos, objetiva-se neste trabalho analisar um conjunto de dados com indicadores de atenção gestacional para as 27 capitais brasileiras e agrupar esses municípios de acordo com suas similaridades no que se refere às variáveis propostas, buscando interpretar os resultados obtidos após oagrupamento.

**Revisado pelo Orientador*

Metodologia

O conjunto de dados foi construído por meio de informações na plataforma virtual do Departamento de Informática do SUS – DATASUS, sendo todos os indicadores colhidos entre 2008 e 2010, nas datas mais recentes encontradas nesta fonte oficial [4].

Os indicadores (variáveis) considerados neste estudo são: número de gineco- obstetras disponíveis por mil habitantes, totais e pelo SUS, número de aparelhos de ultrassonografia disponíveis por dez mil habitantes, totais e pelo SUS, valor médio (custo médio), período médio e mortalidade hospitalar média por internações obstétricas, percentual de partos cesáreos, percentual de mães com idade entre 10 e 19 anos, mortalidade infantil por mil nascidos vivos e percentuais de cobertura pré- natal.

O método utilizado foi o Agrupamento Hierárquico (*cluster)*, que é uma técnica baseada em álgebra de matrizes, que procura formar grupos entre os elementos de um conjunto de dados por meio de uma matriz de dissimilaridades. Vale destacar que quanto mais próxima de 1 é a Correlação Cofenética de um agrupamento, melhor será este [3]. As análises estatísticas foram realizadas no programa R [5].

Resultado e Discussão

O agrupamento que apresentou a melhor Correlação Cofenética, foi o método de ligação por média, aplicado sob uma matriz de dissimilaridades constituída sob o Método de Manhattan, cujo coeficiente foi de 0,8155. Por meio de análise visual do dendograma decidiu-se por um corte que formou cinco grupos.

O grupo 1 foi formado pelas cidades de Palmas e Recife e apresentou os maiores valores para custo médio de internações obstétricas entre as capitais, mas também foi o grupo com menores resultados de mortalidade infantil. No grupo 2, em que estão as capitais Aracajú, Boa Vista, Florianópolis e Porto Velho, o destaque é que estas cidades apresentam os melhores indicadores de gineco-obstetras e custo médio de internações obstétricas. A capital do Amapá destaca-se negativamente entre as cidades estudadas, com indicadores abaixo da média geral, como quantidade de aparelhos de ultrassom, além do percentual de mães com menos de 19 anos e a mortalidade infantil, bem acima do que se encontrou nas outrascapitais.

No grupo 4, as capitais Belém, Belo Horizonte, Curitiba e Rio Branco se agruparam por mesclarem baixos indicadores de recursos humanos e tecnológicos (gineco-obstetras e aparelhos de ultrassom) associados a altos custos relativos de internações obstétricas. Por fim, no grupo 5, as demais capitais brasileiras provavelmente ficaram agrupadas ao se assemelharem no que tange o período médio de internações obstétricas, além de custos por internações obstétricas medianos, em relação ao conjunto de dados.

Conclusão

O estudo realizado tornou possível observar as deficiências e méritos das capitais brasileiras no que se refere à assistência às suas gestantes. Uma das variáveis escolhidas que mais interferiu na configuração final do agrupamento foi a de Custo Médio de Interações Obstétricas, que oscilou muito de um conjunto para outro, embora nem sempre altos custos tenham ocasionado em melhores indicadores dos serviços, como mortalidade hospitalar. Ademais todos os indicadores foram importantes na interpretação dos resultados para a análise realizada.

Referências Bibliográficas

[1] IBGE – Instituto Brasileiro de Geografia e Estatística. **IBGE cidades**. [online]. Disponível em: <http://www.cidades.ibge.gov.br/xtras/home. php/> Acesso em 20- 08-2016.

[2] MARCOLIN, A.C. **Qualidade e segurança: caminhos para o sucesso do redesenho do modelo de cuidado obstétrico.** Ver. Bras. Ginecol. Obstet. [online]. 2015, vol.37, n.10, PP 441-445. ISSN 0100-7203

[3] MINGOTI, Sueli Aparecida. **Análise de Dados Através de Métodos de Estatística Multivariada.** Minas Gerais: Editora da UFMG, 2005.

[4] Ministério da Saúde. **DATASUS**. [online] Disponível em < http:// DATASUS.saude.gov.br/> Acesso em 12-08-2016.

[5] R Core Team et al. **R: A language and environment for statistical computing,** (2016)

A CURVATURA DE GAUSS DE UMA SUPERFÍCIE REGULAR ESUA RELAÇÃO COM A CONSTRUÇÃO DE MAPAS DA TERRA

Victor Gonçalves NETTO IF-
UFG, vigonetto@gmail.com

Rosângela Maria da SILVA
IME-UFG, rosangelamath@gmail.com

Palavras Chaves: Curvatura de Gauss, Teorema Egregium de Gauss, Geometria Diferencial, Mapas da Terra.

Justificativa: Um dos temas abordado entre agosto/2015 até julho/2016 foi o das superfícies regulares. A teoria de superfícies é muito rica, e um de seus resultados mais conhecidos, devido a Gauss, é o *Teorema Egregium de Gauss*. O intuito desse trabalho é relacionar esse importante teorema a uma questão cotidiana: a criação de mapas fiéis do planeta Terra.

Objetivos: Com os conceitos apresentados, pretendemos verificar a possibilidade da construção de um mapa de toda a Terra que possa, ao mesmo tempo, ser desenhado numa folha de papel e que seja fiel. A palavra fiel significa que não há nenhuma distorção de áreas, comprimentos ou ângulos.

Metodologia: A metodologia usada para o estudo das superfícies foi a leitura e a resolução de exercícios dos livros que estão nas referências bibliográficas.

Durante o *XXIV Seminário de Iniciação Científica* será feita a exposição de um pôster.

Resultado e Discussão: A teoria da geometria diferencial nos mostra que a curvatura de Gauss é uma propriedade intrínseca das superfícies regulares. Portanto duas superfícies isométricas têm a mesma curvatura de Gauss.

Visto de outra maneira, se existe uma isometria entre duas superfícies regulares, então a curvatura de Gauss é a mesma para as duas superfícies.

Conclusão: Se existir uma isometria entre o plano e uma esfera (um mapa plano e um mapa esférico), então essas duas superfícies têm a mesma curvatura de Gauss. Isso não está de acordo com a teoria, que diz que a curvatura de Gauss de um plano é identicamente nulo, enquanto a curvatura de Gauss de uma esfera é estritamente positivo. Portanto não existe nenhuma projeção plana fiel de um mapa da Terra.

Referências Bibliográficas:

(1) - TENENBLAT, Keti, Introdução à geometria diferencial. 2.ed. São Paulo: Blucher, 2008.

(2) - CARMO, Manfredo Perdigão do, Geometria Diferencial de Curvas e Superfícies. 6.ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 20014.

ATIVIDADES DO PICME: ESTUDO DE DISCIPLINAS BÁSICAS EM PREPARAÇÃO PARAO MESTRADO EM MATEMÁTICA

Vinícius Loti de LIMA*, Porfírio Azevedo dos Santos JÚNIOR IMTec/Regional Catalão/UFG

O PICME é um programa de capacitação de recursos humanos em matemática que propicia aos alunos medalhistas da OBMEP ou OBM uma oportunidade de complementar a sua graduação com estudos avançados, além de oferecer a oportunidade de ingressar no Mestrado em Matemática, buscando elevar o nível de conhecimento em matemática como ciência básica para o fortalecimento das áreas tecnológicas e científicas. Na busca destes objetivos, o aluno do PICME desenvolve atividades com intuito de preparar-se para o Mestrado. Neste sentido, o bolsista desenvolveu estudos dirigidos em diferentes disciplinas de formação básica, a saber: Álgebra Linear, Álgebra (teoria de grupos), Equações diferenciais, Análise na Reta, Geometria Diferencial, finalizando com um trabalho de iniciação científica vinculado ao estudo de teoria de grupos.

Nestes estudos dirigidos, foram realizadas reuniões semanais com o orientador para esclarecimento de dúvidas, entrega de resolução de exercícios e seminários sobre alguns tópicos de relevância em cada disciplina. Os conteúdos estudados propiciaram uma formação complementar e solidifica o conhecimento básico em Matemática, visando a preparação para o mestrado. Na disciplina, Álgebra Linear, vários tópicos escolhidos para estudo constavam na grade curricular do curso de Matemática Industrial. Portanto, foram acrescentados tópicos como “forma canônica de Jordan” e “Operadores Autoadjuntos”, proporcionando uma ótima oportunidade para o aluno estudar assuntos que poderiam não ser vistos em sua graduação, complementando assim a sua formação. Durante a primeira etapa também foram desenvolvidos estudos complementares de Equações diferenciais, uma vez que a ementa desta disciplina no Curso de Matemática Industrial é bem ampla. Desta forma, foi acrescentado apenas um direcionamento no estudo voltado para a parte mais teórica, pois no curso é trabalhada com bastanteaplicações.

Na parte de Álgebra Moderna, foi dada ênfase aos tópicos de homomorfismos e isomorfismos de grupos, automorfismos de grupos, Teorema de Cayley, grupos de permutações, Teorema de Cauchy e Teoremas de Sylow. Além disso, estudou anéis,

Vinícius Loti de Lima*, aluno do Curso de Matemática Industrial / Regional Catalão/ UFG e bolsista do Programa de Iniciação Científica e Mestrado - PICME nos períodos de Março de 2013 até Junho de 2014 e de Setembro de 2015 até Julho de 2016, sob a orientação do Professor Porfírio Azevedo dos Santos Júnior.

homomorfismo de anéis e ideais, complementando com definição de corpos e exemplos. Em seguida, iniciou o estudo de Análise na Reta, mas foi interrompido pela contemplação de uma bolsa de intercâmbio pelo programa Ciência sem Fronteiras na University of California - Davis, onde o aluno cursou as disciplinas “Advanced Calculus”, “Real Analysis A” e “Real Analysis B” que correspondem a um curso de Análise Real em um curso de Bacharelado em Matemática. Após o término da bolsa de Intercâmbio, durante o período de setembro de 2015 até fevereiro de 2016, foram feitos estudos em Geometria Diferencial, seguindo os mesmos procedimentos, com exercícios e apresentações de exercícios e resultados importantes da disciplina sobre os tópicos de curvas regulares planas, curvas regulares no espaço e superfícies regulares.

Durante o último período e prologando os estudo até julho de 2016, foi desenvolvido uma iniciação à pesquisa, na área de teoria de grupos, onde foi elaborada uma apostila que mostra como a Teoria dos Grupos está relacionada a estrutura do cubo de Rubik 5x5x5, e ao final da apostila é proposto um algoritmo para a montagem deste cubo. Este trabalho será apresentado em forma de um minicurso na semana do IME (Instituto de Matemática e Estatística/UFG), um evento que ocorrerá em Goiânia no período de 18 a 21 de Outubro de 2016.

O objetivo do minicurso é apresentar definição de grupos, especialmente, um grupo que permuta certos elementos. Além de apresentar uma solução do cubo mágico 5x5x5, deixando claro que, o cubo mágico nada mais é do que uma estrutura que permuta certos elementos de seis maneiras distintas. Seguindo esta linha, são abordadas algumas observações sobre grupos de permutações e, por meio do G.A.P (Group Algorithms and Programming), é feita a construção de um grupo de permutações e análise de sua estrutura, abordando a pesquisa de seus subgrupos, determinação de ordem, índices e, principalmente, a cadeia de estabilizadores do grupo. Inicialmente serão abordados de forma teórica os conceitos de teoria de grupos, apresentando exemplos. Posteriormente, utilizaremos o programa GAP para definir o grupo que gera o cubo mágico, seu índice, pesquisar as órbitas dos pontos do cubo, além de permitir a pesquisa da possibilidade de um cubinho de uma aresta poder ser girado ou não sozinho através do estudo das órbitas dos pontos do cubo. O programa também será utilizado para verificar alguns passos da solução do cubo, os quais fazem parte do algoritmo que apresentado como solução do cubo mágico. Por fim, concluímos os procedimentos com a solução do cubo 5x5x5 por meio de um algoritmo que estabelece uma sequência de passos para a montagem do cubo. Neste parte da pesquisa foi utilizado o material do professor Helder Carvalho de Matos do Departamento de Matemática/ UnB sobre “Teoria de Grupos e Uma Solução para o Cubo Mágico”, no qual trata do cubo 3x3x3.

Nesta perspectiva, conclui-se que o estudo de teoria de grupos pode ser motivado por um desafio e os conceitos podem ser estudados usando como motivação material concreto e um programa como material didático.