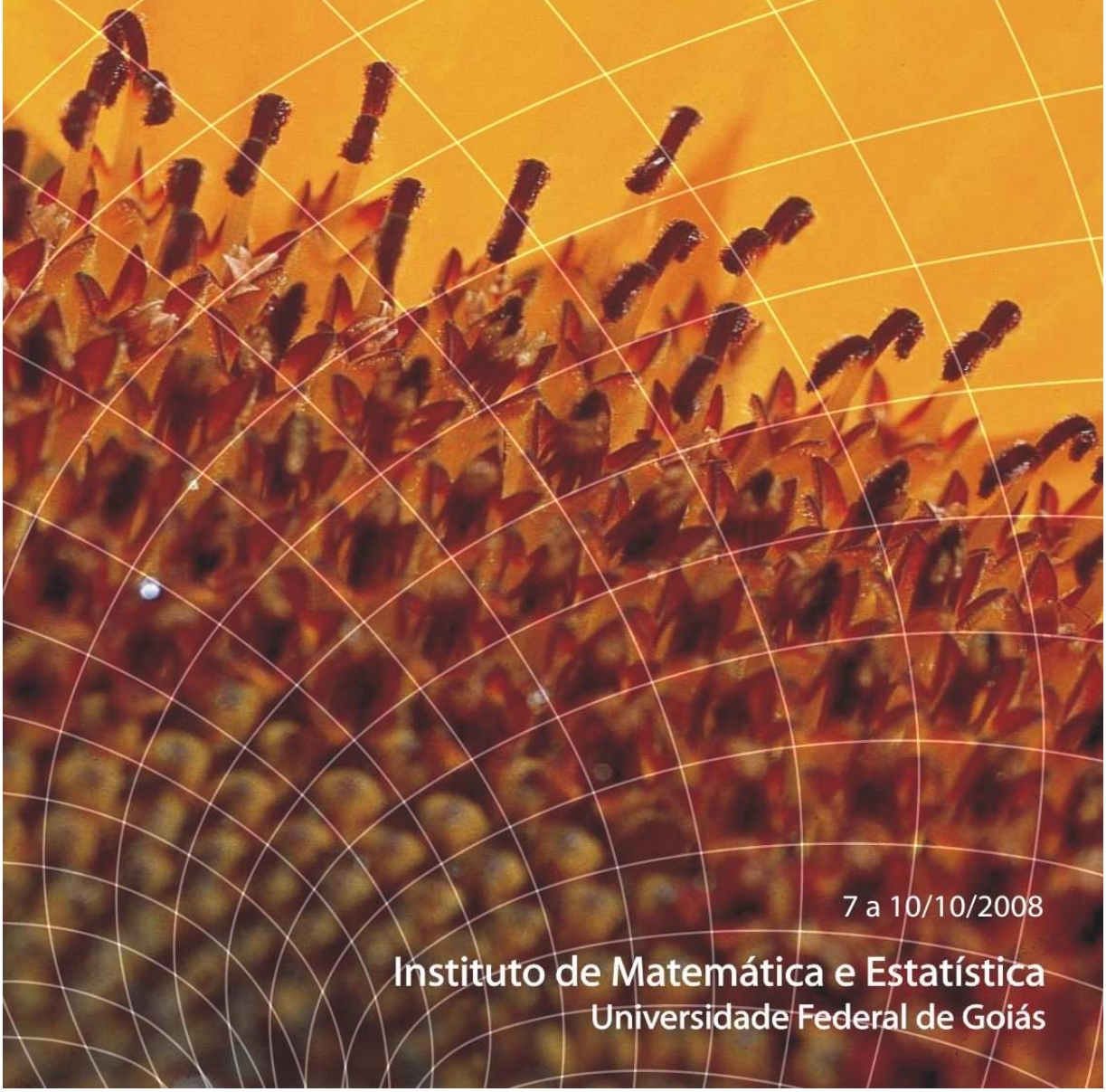
Anais da

XXIII Semana do IME

em homenagem aos 60 anos do professor **Jesus Carlos da Mota**



7 a 10/10/2008

Instituto de Matemática e Estatística
Universidade Federal de Goiás

Proceedings do XXIII Semana do IME/UFG

Goiânia-GO, 07 a 10 de outubro de 2008.

No período de 1986 à 1996, o Instituto de Matemática e Física (IMF) da UFG realizou anualmente o evento científico denominado Semana do IMF (Semana do Instituto de Matemática e Física). No ano 1997, com a criação do Instituto de Matemática e Estatística (IME), o IME passou a realizar a Semana do IME/UFG.

Neste ano de 2008, estaremos realizando a XXIII Semana do Instituto de Matemática e Estatística da UFG, no período de 07 a 10 de outubro.

Salientamos que ações como esta que realizamos anualmente desde 1997 são de fundamental importância para o aprimoramento e formação de profissionais que atuam nas áreas de Matemática e Estatística.

Paralelamente a XXIII Semana do IME/UFG, estará sendo realizado o V Congresso de Pesquisa, Ensino e Extensão (V CONPEEX) da UFG, com a participação de alunos de graduação da UFG e de outras Instituições. O CONPEEX visa a divulgação dos trabalhos de alunos da graduação com bolsa PIBIC e de todas as outras atividades compreendendo Ensino, Pesquisa e Extensão, as quais são desenvolvidos através de recursos captados pela UFG.

As atividades da XXIII Semana do IME/UFG estará aberta para os participantes do V CONPEEX. A simultaneidade dos eventos permitirá que pesquisadores de destaque que estiverem participando do V CONPEEX possam tanto proferir palestras destinadas aos pesquisadores participantes do evento, bem como para as atividades direcionadas ao público da XXIII Semana do IME/UFG.

Proceedings XXIII Semana do IME/UFG

07 à 10 de outubro de 2008

Editoração

Profa. Dra. Marina Tuyako Mizukoshi

Arte

Prof. Dr. Rogério Queiróz Chaves

Universidade Federal de Goiás

Instituto de Matemática e Estatística

Campus Samambaia

Caixa Postal 131

74.001-970 - Goiânia - Goiás

Tel.: (62) 521 1208, Fax: (62) 521 1180

URL: www.mat.ufg.br

PROGRAMAÇÃO DIÁRIA da XXIII Semana do IME/UFG

Terça-Feira, 07	
8:00 - 12:00	veja programação CONPEEX
8:00 -9:30	veja programação CONPEEX
9:30 -10:30	*Palestra de Abertura do XVI Seminário de Iniciação Científica
9:30 -10:30	veja programação CONPEEX
12:00- 14:00	Almoço/Cinema(Faculdade de Letras)
14:00 -18:00	*Apresentação Oral PIBIC/PIVIC(V CONPEEX)
16:00- 17:30	veja programação CONPEEX
17:30 -19:00	Intervalo
19:00- 19:50	Professor Vanderlei Horita (IBILCE/UNESP/SJRP)
19:50- 20:10	Coquetel
20:10-21:30	Minicurso MC1, MC3 e MC14

Quarta-Feira, 08	
8:30 - 10:00	*Mesa-Redonda:Formação de Formadores - Faculdade de Letras
8:30 - 10:00	Minicurso MC4
10:00 -10:20	Intervalo
10:20 -11:40	Minicursos MC2, MC6, MC7, MC8
11:40- 14:00	Almoço
14:00 -15:30	Minicursos MC9 ao MC13
15:30- 16:00	Intervalo
16:00- 16:50	George Freitas von Borries (UnB/Estatística)
17:00- 17:50	Marcelo Almeida Bairral (UFRRJ)
18:00 -19:00	Intervalo
19:00- 19:50	Walter Batista dos Santos (Doutorando UnB)
19:50- 20:10	Intervalo
20:10-21:40	Minicurso MC1, MC3 e MC14

Quinta-Feira, 09	
8:30 - 10:00	Minicursos MC4 e MC5
10:00 -10:20	Intervalo
10:20 -11:40	Minicursos MC2, MC6, MC7, MC8
11:40- 14:00	Almoço
14:00 -15:30	Minicursos MC9 ao MC13
15:30- 16:00	Intervalo
16:00- 16:50	Evander P. de Rezende (UFG/Catalão)
16:00- 16:50	Bryon Richard Hall (IME/UFG)
17:00 -18:00	Sessão de Poster
18:00 -19:00	Intervalo
19:00- 19:50	Venício Veloso Borge (UCG)
19:50- 20:10	Intervalo
20:10-21:30	Minicursos MC1 e MC14

Sexta-Feira, 10	
8:30 - 10:00	Minicursos MC4 e MC5
10:00 -10:20	Intervalo
10:20 -11:40	Minicursos MC2, MC6, MC7, MC8
10:20 -11:10	Sessão Técnica de EDP - P1
11:10 -12:00	Sessão Técnica de EDP - P2
12:00- 14:00	Almoço
14:00 -15:30	Minicursos MC9 ao MC13
14:00 -14:50	Sessão Técnica de EDP P3
14:50 -15:40	Sessão Técnica de EDP P4
15:30- 16:00	Intervalo
16:00- 17:00	Rodney Carlos Bassanezi(UFABC)

Observações:1) As atividades do CONPEEX com * são recomendados à todos os participantes da XXIII Semana do IME/UFG.

Minicursos

MC1 - **Números: dos Naturais aos Reais**

Ministrantes: Eudes Antonio da Costa (UFT/Campus Arraias)
Ronaldo Antonio dos Santos (IME/UFG)

MC2 - **Alguns Problemas Interessantes em Probabilidade**

Ministrante: Fabiano Fortunato Teixeira dos Santos (CAJ/UFG/Doutorando UnB).

MC3 - **A Modelagem Matemática como Metodologia de Ensino-Aprendizagem da Matemática na Educação Básica.**

Ministrantes: Crhistiane da Fonseca Souza (CAC/UFG)
Mariane Cardoso (Bolsista Prolicen/ CAC/UFG)

MC4 - **Matemática Algumas Vezes Aplicada.**

Ministrante: Luciana Aparecida Elias (CAJ/UFG)

MC5 - **Análise dos parâmetros de controle em pesquisas de intenção de votos/ Controle Estatístico de Qualidade - Controle on-line de processos: uma abordagem econômica para contagem do número de não-conformidades na amostra via modelagem probabilística.**

Renata Mendonça Rodrigues (Mestranda - PPGMAE / CCET - UFRN)

MC6 - **Classificação de Pontos Singulares No Plano.**

Ministrantes : Alysson Tobias Ribeiro da Cunha (CAJ/UFG)
Marcos Leandro Mendes Carvalho (CAJ/UFG).

MC7 - **Teoria local das curvas planas.**

Ministrante: Luciana Maria Dias de Ávila Rodrigues (UnB)

MC8 - **Sistemas Criptográficos em Blocos.**

Ministrantes: Shirlei Serconek (IME/UFG)
Celso Júnior (Especialização IME/UFG)
Nilo Célio (Especialização IME/UFG)

MC9 - **Testes de Primalidade e Aplicações.**

Ministrantes: Maria Aparecida de Faria(Especialização IME/UFG)
Shirlei Serconek (IME/UFG)

MC10 - **Tópicos em passeios aleatórios.**

Ministrante: Valdivino Vargas Júnior (Doutorando IME/USP)

MC11 - **O Lema de Lax-Milgram e Aplicações.**

Ministrante: Maurilio Marcio Melo (IME/UFG)

MC12 - **Mapas Mentais como Ferramenta de Apoio a Aprendizagem.**

Ministrante: Edinaldo Augusto Lemes Garcia (IME/EEEC-UFG)

MC13 - **O Produto Wreath e o Grupo de Automorfismos de Árvores.**

Ministrante: Márcio Roberto Rocha Ribeiro (CAC/UFG)

MC14 - **Códigos Corretores de Erros.**

Ministrante: Mário José de Souza (IME/UFG)

Conferências

Palestra de Abertura: **Funções Simples x Dinâmicas Interessantes.**

Palestrante: Vanderlei Horita (IBILCE/UNESP/SJRP)

Local: Auditório do Instituto de Química (IQ)

C1 - **"Uma Discussão sobre o Uso de Técnicas de Agrupamento para Dados Superdimensionados com Amostras Pequenas".**

Conferencista: George Freitas von Borries (UnB/Estatística)

Local: Auditório do Instituto de Química (IQ)

C2 - **Pesquisas e inovação com ambientes virtuais em educação matemática.**

Conferencista: Marcelo Almeida Bairral (UFRRJ)

Local: Auditório do Instituto de Química (IQ)

C3 - **Aproximação do valor de π via simulação Monte Carlo.**

Conferencista: Walter Batista dos Santos (Doutorando UnB)

Local: Auditório do Instituto de Química (IQ)

C4 - **O Teorema da Base de Hilbert e o método dos conjuntos parcialmente bem-ordenados.**

Conferencista: Evander Pereira de Rezende (Doutorando UnB)

Local: sala 112 do IME/UFG.

C5 - **Números surreais e análise não-standard.**
Conferencista: Bryon Richard Hall (IME/UFG)
Local: Auditório do Instituto de Química (IQ)

C6 - **Sofismas na Matemática**
Palestrante: Venício Veloso Borge (UCG)
Local: Auditório do Instituto de Química (IQ)

Palestra de Encerramento - **Modelagem Matemática no Ensino Aprendizagem.**
Palestrante: Rodney Carlos Bassanezi (CMCC - UFABC/ Santo André)
Local: Auditório do Instituto de Química (IQ)

Sessão Técnica de Equações Diferenciais Parciais

P1 - **Existência de Atratores para Equações de Evolução Não-Lineares.**
Ministrante: Eduardo Arbieto Alarcon(UFG)
Local: Sala 112

P2 - **Estabilidade de Ondas de Combustão.**
Ministrante: Aparecido Jesuíno de Souza (UFCG)
Local: Sala 112

P3 - **Problema de Riemann para um Modelo Quadrático.**
Ministrante: Arthur Vicentini de Azevedo(UnB)
Local: Sala 112

P4 - **Uma aplicação do método iterativo monótono a um problema de combustão em meios porosos.**
Ministrante: Marcelo Martins dos Santos (UNICAMP)
Local: Sala 112

Sessão de Poster

*Painel 1:***Estágio I - Acompanhamento Pedagógico de Reforço Matemático para Alunos da 2^a Fase do Ensino Fundamental no CEPAE.**

Fábio Moreira Araújo (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof. Msc. Marcos Vinicius Lopes (CEPAE/UFG)
José Anthony Novak Faria (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof. Msc. Marcos Vinicius Lopes (CEPAE/UFG)
José Francisco Arruda Silva (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Profa. Tatiana Marla da Costa (CEPAE/UFG)
Marciene Alves da Silva (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Msc. Marcos Antônio Gonçalves Jr
Wérica Pricylla de Oliveira Valeriano (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Profa. Msc. Gene Maria Vieira Lyra Silva (CEPAE/UFG)

Painel 2: **Estágio I - Didática da Matemática à Luz de uma Abordagem a distância.**

Diego Rodrigues da Silva (Graduando Lic. em Matemática - IME/UFG)
Douglas Nascimento Ribeiro (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. José Pedro Machado Ribeiro(IME/UFG)

Painel 3: **Estágio I - Etnomatemática.**

Patrícia Ferreira Berchol (Graduanda Lic. em Matemática - IME/UFG)
Raniere Elias Tavares (Graduando Lic. em Matemática - IME/UFG)
Wivian Sena Moraes (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. José Pedro Machado Ribeiro (IME/UFG)

Painel 4: **Estágio I - Jogos matemáticos estratégicos no processo de ensino e aprendizagem da matemática na escola do Ensino Básico**

Lorena L. da Costa (Graduanda Lic. em Matemática - IME/UFG)
Ludimila C. C. de Andrade (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. José Pedro Machado Ribeiro (IME/UFG)

Painel 5: **Estágio I - Jogos no Ensino de Matematica.**

Fernando Goncalves Pinto (Graduando Lic. em Matemática - IME/UFG)
Julio Cesar Prado Souza Rodrigues (Graduando Lic. em Matemática - IME/UFG)
Julyan do Vale Ferreira (Graduando Lic. em Matemática - IME/UFG)
Thais Naves Melo (Graduanda Lic. em Matemática - IME/UFG)
Willian do Amaral Barra (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Profa. Msc. Maria Bethania Sardeiro dos Santos (IME/UFG)

Painel 6: **Estágio I - Monitoria no Waldemar Mundin**

Denise Ramos Galvão (Graduanda Lic. em Matemática - IME/UFG)
Orientadora: Profa. Msc. Susane Fernandes de Abreu Teixeira (Subs. IME/UFG)
Giovanna Marques Inácio (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. Paulo Henrique de Azevedo
Ronivon de Morais Leonel (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Profa. Msc. Susane Fernandes de Abreu Teixeira (Subs. IME/UFG)

Painel 7: **Estágio I - Monitoria no Castelo Branco**

Aguiobey de Souza Roque (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. Ricardo Nunes de Oliveira (IME/UFG)
Carla de Faima Souza (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. Maurílio Márcio Melo (IME/UFG)
Fernando e Silva Luciano (Graduando Lic. em Matemática - IME/UFG)
Orientador: Profa. Dra. Marina Tuyako Mizukoshi (IME/UFG)
Oscar Joaquim da Siva Neto (Graduando Lic. em Matemática - IME/UFG)

Orientador: Prof. Dr. Ricardo Nunes de Oliveira (IME/UFG)
Reinaldo Resende Tadeu (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Profa. Dra. Edméia Fernandes da Silva (IME/UFG)

Painel 8: **Estágio I - Monitoria no CEFET.**

Renata Rodrigues Ramos (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. Maurílio Márcio Melo (IME/UFG)
Sheila Ferreira dos Santos (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. Maurílio Márcio Melo (IME/UFG)

Painel 9: **Estágio I - Resolução de Problemas e Investigação Matemática.**

Daniel Antônio Mendonça da Silva (Graduando Lic. em Matemática - IME/UFG)
Liliane de Souza Gomes (Graduanda Lic. em Matemática - IME/UFG)
Wesley Carvalho (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof Msc. Marcos Antônio Gonçalves Junior (CEPAE/UFG)

Painel 10: **Projeto Re-vivenciando o Colméia.**

Lucimar de Lima Canêdo (Graduanda Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. José Pedro Machado Ribeiro (IME/UFG)

Painel 11: **Software - Prática e Educação Matemática**

Douglas Santos Oliveira (Graduando Lic. em Matemática - IME/UFG.)
Humberto Irineu Chaves Ribeiro (Graduando Lic. em Matemática - IME/UFG)
Orientadora: Elisabeth Cristina de Faria (IME/UFG)

Painel 12: **PET - Vivenciando o Cálculo no Curso de Matemática.**

Daniella Porto (Graduanda Lic. em Matemática - IME/UFG)
José Henrique de Salazar Amaral (Graduando Lic. em Matemática - IME/UFG)
Orientador: Prof. Dr. José Pedro Machado Ribeiro (IME/UFG).

Painel 13: **O Ensino de Geometria Analítica Utilizando os Softwares WINPLOT, RÉGUA E COMPASSO, VRUM VRUM E MATHGV.**

Carlos Roberto da Silva (Bolsista/Graduando em Ciência da Computação - UniEvangélica)
Pedro Henrique de Oliveira Caetano (Bolsista/ Sistemas de Informação - UniEvangélica)
Eliana Carla Rodrigues (voluntária/ Graduanda em Lic. em Matemática - UEG)
Juliano José Gomes (voluntário / Graduando Lic. em Matemática - UEG)
Ronyérisson dos Santos e Silva (voluntário/ Graduando Lic. em Matemática)
Orientadora: Profa. Msc. Eliane de Fátima Rodrigues Martins (UniEvangélica)

Painel 14: **Problema de Valores de Contorno e Teoria de Sturm-Liouville aplicados ao**

escoamento de fluido em uma rocha porosa.

Adriane Sardinha Macêdo (Graduanda em Matemática - UEG/Iporá)
Thársis Sousa Silva. (Graduanda em Matemática - UEG/Iporá)
Orientador: Prof.Rodrigo Miyasaki (UEG/Iporá)

Painel 15: **A complementaridade entre a linguagem corrente e a linguagem matemática.**

Tatiana Marla da Costa (CEPAE/UFG)

Painel 16: **Teste da razão de verossimilhanças sinalizada em modelo com erros nas variáveis.**
Tatiane Ferreira do Nascimento Melo (Doutoranda IME/USP)

Sumário

Funções Simples × Dinâmicas Interessantes

Vanderlei Horita

Instituto de Biociências, Letras e Ciências Exatas

Departamento de Matemática, IBILCE, UNESP

15.054-000, São José do Rio Preto, SP

E-mail: vander@ibilce.unesp.br

Às vezes somos tentados a pensar que para termos um sistema dinâmicos interessante ("complicado") precisamos ter uma função com expressão algébrica difícil de entender. Discutiremos, usando exemplos simples porém com dinâmicas ricas, algumas noções centrais da teoria de sistemas dinâmicos como hiperbolicidade, estabilidade, transitividade e outras. Veremos que mesmo funções lineares, desde que em ambientes apropriados, possuem dinâmicas extremamente ricas.

C1 - Uma Discussão sobre o Uso de Técnicas de Agrupamento para Dados Superdimensionados com Amostras Pequenas

George Freitas von Borries

Departamento de Estatística, IE, UnB,
Campus Universitário Darcy Ribeiro,
Asa Norte, 70910-900, Brasília, DF
E-mail: gborries@unb.br

The advent of new technologies for collecting and storing data has motivated the research of inference methods applied to high dimensional low sample size data in areas such as microarray experimentation (Pomeroy et al. [9]), spectrometry studies (Thiele [14]), pattern recognition (Reese [10]) and agriculture screening trials (Brownie and Boos [2]). For example, scientists have been able to study complex disorders through the monitoring of expression of thousands of genes from a single DNA chip, known as DNA microarray (see for example [5], [1], [11], [4]) and one of the most important statistical learning technologies used to identify groups of differentially expressed genes has been cluster analysis (as in [7], [6], [3]). According to McLachlan [8], reasons for clustering of genes are: to discover genes with difference in expression in different tissues; to discover genes belonging to a particular pathway; to find common characteristics in genes declared similar through a comparison of expression patterns. Clustering can also be used as an exploratory tool to compare different experimental conditions (as a batch of reagents, technicians), to support visual methods in generating hypotheses about the existence of possible groups, to identify subgroups in complex data, to identify gene expression patterns in time or space and to reduce redundancy in prediction. More about the subject is available in Segal et al. [12, 13].

A medium-size microarray study often contains information from thousands of genes with no more than a hundred samples for each gene. The dimensionality of the study will impose many restrictions to traditional statistical analysis. Drawbacks of available clustering algorithms are the difficulty in specifying the number of clusters in advance, their sensitiveness to outliers, the long processing time, their lack of robustness in the presence of small perturbations, their non-uniqueness, problems with inversion, distributional assumptions, and their failure to computate covariance matrices when one or more components is singular or nearly singular.

The purpose of this presentation is to review some of the terminology related to cluster analysis with the objective to clarify and differentiate common terms from different scientific areas that are frequently used without a precise meaning in the literature about clustering of high dimensional low sample size (HDLSS) data. The terms covered are: (1) data mining; (2) statistical learning; (3) supervised/unsupervised learning; (4) clustering; (5) gene-based clustering; (6) class discovery; and (7) classification. It is also reviewed some benchmark algorithms used in the clustering of high dimensional data and discussed advantages and disadvantages of some proximity measures and algorithms used in studies with HDLSS data.

In recent bioinformatics literature there are many new algorithms working with HDLSS data. Difficulties in using those algorithms are also explored. Finally, the ideas of a new algorithm specifically designed to clustering of HDLSS data are introduced.

Referências

[1] D. B. Allison, G. P. Page, T. M. Beasley, and J. W. Edwards, editors. DNA mi- croarrays and related genomics techniques: design, analysis, and interpretation of experiments. Chapman and Hall/CRC, 2006.

[2] D. D. Boos and C. Brownie. ANOVA and rank tests when the number of treatment is large. Statistics & Probability Letters, 23:183?191, 1995.

[3] L. Fu and E. Medico. Flame, a novel fuzzy clustering method for the analysis of DNA microarray data. BMC Bioinformatics, 8, 2007.

[4] E. Geraque. Pequenos grandes arranjos. Scientific American Brazil, 16:56?57, 2006.

[5] J. Hardin. Microarray data from a statistician?s point of view. Stats: the magazine for students of statistics, 42:4?13, 2005.

[6] C. Huttenhower, A. I. Flamholz, J. N. Landis, S. Sahi, C. L. Myers, K. L. Olszewski, M. A. Hibbs, N. O. Siemens, O. G. Troyanskaya, and H. A. Coller. Nearest neighbor networks: clustering expression data based on gene neighborhoods. BMC Bioinfor- matics, 8, 2007.

[7] D. Jiang, C. Tang, and A. Zhang. Cluster analysis for gene expression data: a survey. IEEE Transactions on Knowledge and Data Engineering, 16:1370?1386, 2004.

[8] G. J. McLachlan, K. A. Do, and C. Ambroise. Analyzing microarray gene expression data. Wiley-Interscience, 2004.

[9] S. Pomeroy, P. Tamayo, M. Gaasenbeek, L. Sturla, M. Angelo, M. McLaughlin, J. Kim, L. Goumnerova, P. Black, C. Lau, and et al. Prediction of central nervous system ebryonal tumor outcome based on gene expression. Nature, 415:436?442,2002.

[10] S. Reese, G. Sukthankar, and R. Sukthankar. An efficient recognition technique for minelike objects using nearest-neighbor classification. Technical report, Intel Corportation, 2003.

[11] H. Schwender, S. Rabstein, and K. Ickstadt. Do you speak genomish? Chance, 19:3?10, 2006.

[12] E. Segal, H. Wang, and D. Koller. Discovering molecular pathways from protein interaction and gene expression data. Bioinformatics, 19:264?272, 2003.

[13] E. Segal, R. Yelensky, and D. Koller. Genome-wide discovery of transcriptional modules from DNA sequence and gene expression. Bioinformatics, 19:273?282, 2003.

[14] H. Thiele. Mass spectometry and bioinformatics in proteomics. Chance, 16:29?36, 2003.

C2 - Pesquisas e Inovação com Ambientes Virtuais em Educação Matemática

Marcelo Almeida Bairral

Instituto de Educação, Departamento de Teoria e Planejamento de Ensino

Universidade Federal Rural do Rio de Janeiro,

BR 865 km 7 Sala 21, Campus Universitário, 23851970, Seropedica, RJ

E-mail: marcelo.bairral@pq.cnpq.br

Nesta palestra ilustrarei duas vertentes da educação matemática a distância que tenho atuado. A primeira, na construção e implementação de ambientes virtuais para a formação (inicial e continuada) de professores em geometria. Na segunda estou atuando em colaboração com a Rutgers e com a Drexel University (EUA) no ambiente Virtual Math Team (VMT-Chat) com estudantes brasileiros e americanos - do Ensino Médio. Neste estudo estamos analisando o desenvolvimento colaborativo de estratégias heurísticas pelos discentes.

C3 - Aproximação do Valor de π Via Simulação Monte Carlo

Walter Batista dos Santos

Departamento de Matemática, MAT–UnB,

Campus Universitário Darcy Ribeiro,

70910-900, Brasília, DF

Asa Norte, 70910-900, Brasília, DF

E-mail: batista216@gmail.com

1.1 Introdução

É conhecido que $\pi = 3,1415926...$ e que existem algorítmos determinísticos eficientes para determinar seu bilionésimo dígito. Também, métodos não determinísticos podem ser usados para aproximar (ou estimar) o valor de π e o Teorema do Limite Central é a ferramenta fundamental para determinar o quão "boa" é esta aproximação. Esta palestra visa divulgar um método Monte Carlo que consiste em usar números aleatórios para obter uma aproximação de π.

1.2 Conceitos Básicos

Nesta seção são introduzidos os conceitos da teoria de probabilidade que serão utilizados. Usaremos ao longo do texto "v.a." para indicar "variável aleatória".

1.2.1 Variável Aleatória Discreta

Definição 1.1. *Uma v.a. $X : \Omega \to \mathbb{R}$ é dita discreta se existem $a_1, a_2, \ldots, a_n, \ldots$ em $\mathbb{R}$ tais que $P(X \in \{a_1, a_2, \ldots, a_n, \ldots\}) = 1$.*

Definição 1.2. *A esperança ou valor esperado da v.a. discreta X é definido como $E[X] = \sum_{j=1}^{\infty} a_j P(X = a_j)$.*

Observação 1.3. *Seja X uma v.a. discreta e $g(X)$ uma função de X. Então o valor esperado da nova v.a. é dado por*

$$E[g(X)] = \sum_{j=1}^{\infty} g(a_j) P(X = a_j).$$

Definição 1.4. *A variância de uma v.a. X é definida como*

$$var[X] = E[X^2] - (E[X])^2.$$

Observação 1.5. *Se X é uma v.a. com distribuição Binomial de parâmetros n e p então*

$$P(X = k) = \left(\begin{array}{c} n \\ k \end{array} \right) p^k (1-p)^{n-k}, \;\; k = 0, 1, \ldots, n.$$

Neste caso, é conhecido que $E[X] = np$

1.2.2 Teorema do Limite Central

O Teorema do Limite Central (TLC) pode ser encontrado em [2]. Enuniaremos o teorema sem entrar em detalhes das hipóteses, pois, somente nos interessará seu resultado para aplicação.

Teorema 1.6. *Seja $X_1, X_2, \ldots, X_n, \ldots$ uma seqüência de variáveis aleatórias independentes e identicamente distribuídas com média comum μ e variância σ^2. Então,*

$$\frac{S_n - n\mu}{\sigma\sqrt{n}} \xrightarrow{D} N(0,1), \text{ quando } n \to \infty,$$

onde, $S_n = X_1 + X_2 + \ldots + X_n$ e, $\xrightarrow{D}$ significa convergência em distribuição.

Método Monte Carlo

No que segue, suporemos que π é um número na vizinhança de 3 e usaremos um método Monte Carlo para estimar seu valor. Para tal, consideremos o círculo C, de diâmetro 2, inscrito no quadrado Q, de lado 2, de acordo com a figura abaixo.

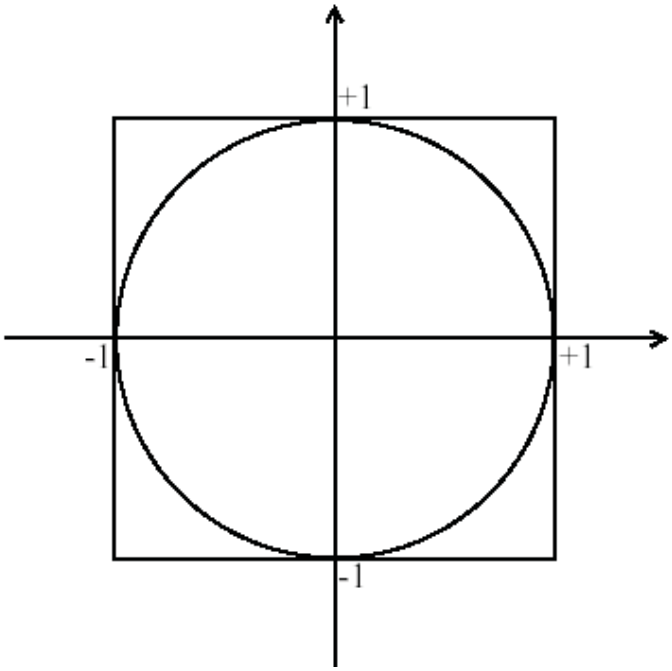


Figura 1.1.

A área de C é π e a área de Q é 4. Vamos retirar um ponto v aleatoriamente (uniformemente) de dentro do quadrado Q. A probabilidade que v situe dentro do círculo C (isto é, $v \in C$) é $\frac{\pi}{4}$, ou seja,

$$P(v \in C) = \frac{\text{área}(C)}{\text{área}(Q)} = \frac{\pi}{4}.$$

Este exprimento pode ser repetido n vezes, isto é, podemos selecionar pontos $v_1, v_2, \ldots, v_n$ independentemente, cada um uniformemente distribuído no quadrado Q. Seja Z a quantidade de v_i's que situam-se dentro do círculo C. Então Z tem distribuição binomial de parâmetros n e $\frac{\pi}{4}$, e em particular, $E[Z] = \frac{n\pi}{4}$. Por isso, $E\left[\frac{4Z}{n}\right] = \pi$; ou seja, $\frac{4Z}{n}$ é um estimador "não-viesado" de π.

Exemplo 1.7. *Suponhamos que $n = 10000$ e que observamos $Z = 7932$ (cf. [1]). Então, a estimativa de π deve ser*

$$\frac{4(7932)}{10000} = 3,1728.$$

1.3 Precisão do Método Monte Carlo

Usando $n = 10000$ e $Z = 7932$, podemos verificar o quão "boa" é a estimativa encontrada. Antes porém, vamos reescrever o estimador $\frac{4Z}{n}$ como soma de uma sequência de n váriaveis aleatórias independentes e

identicamente distribuídas, para usarmos o TLC. Para cada $i = 1, 2, \ldots, n$ vamos definir X_i da seguinte forma:

$$X_i = \begin{cases} 4 & \text{se } v_i \in C \\ 0 & \text{caso contrário} \end{cases}$$

ou seja, X_i assume o valor 4 se v_i está no interior de C e, o valor 0, se v_i está no interior de Q e não está no interior de C. Dessa forma o estimador $\dfrac{4Z}{n}$ é o mesmo que $\overline{S_n}$, onde

$$\overline{S_n} = \frac{X_1 + X_2 + \ldots + X_n}{n}.$$

Pelo TLC, um intervalo de confiança de 95% para π é dado por

$$\left[\overline{S_n} - 1,96\frac{\sigma}{\sqrt{n}}\ ,\ \overline{S_n} + 1,96\frac{\sigma}{\sqrt{n}}\right]$$

onde σ é o desvio padrão de X_i. Segue de um cálculo simples que $\sigma = \sqrt{\pi(4-\pi)}$. Agora, usando a estimativa de π na fórmula $\sigma = \sqrt{\pi(4-\pi)}$ obtemos $\sqrt{3,1728(4-3,1728)} \approx 1,62$. Logo, o intervalo de confiança aproximando torna-se

$$[3,1410\ ,\ 3,2046].$$

Com isso concluímos que a estimativa $3,1728$ é precisa para uma casa decimal. Uma pergunta natural é: quantas observações são necessárias para se ter uma precisão de duas casas decimais? Como a precisão é medida pela largura do intervalo de confiança, que é proporcional a $\dfrac{\sigma}{\sqrt{n}}$, para melhorar a precisão por um fator de 10 precisamos aumentar n por um fator de 100. Assim, seria necessário em torno de $n = 10^6$ para obtermos precisão de duas casas decimais e, em torno de $n = 10^8$ para três casas decimais.

1.4 Conclusão

A palaestra divulga o uso de métodos Monte Carlo na resolução de problemas. Apesar desta modesta aplicação existem aplicações bastante sofisticadas desta teoria como por exemplo em problemas de filtragem não linear.

Referências

[1] N.N. Madras, *Lectures on Monte Carlo Methods*, American Mathematical Society, 2002.

[2] D.P. Bertsekas and J.N. Tsitsiklis, *Introduction to Probability*, 2nd edition, Athena Scientific, 2008.

C4 - O Teorema da Base de Hilbert e o Método dos o Método dos Conjuntos Parcialmente Bem-Ordenados

Evander P. Rezende

Departamento de Matemática, MAT–UnB,

Campus Universitário Darcy Ribeiro,

70910-900, Brasília, DF

Asa Norte, 70910-900, Brasília, DF

E-mail: evander.rezende@gmail.com

É fato conhecido que sobre um corpo K, todo ideal do anel de polinômios $K[x]$ é principal, ou seja, todo ideal de $K[x]$ é gerado por um único elemento. Podemos enfraquecer um pouco esta hipótese e exigir apenas que o anel K seja comutativo com unidade e todo ideal de K seja finitamente gerado (i.é., K é um anel *Noetheriano*). Assim, obteremos que, sobre um anel K Noetheriano o anel $K[x_1, x_2, \ldots, x_n]$ também é Noetheriano (este fato é conhecido com o Teorema da Base de Hilbert. Na demonstração proposta para este teorema utilizaremos o método dos conjuntos parcialmente bem-ordenados. Finalmente, apresentaremos outros resultados que usam o mesmo método na demonstração, como o Teorema de Cohen [1] (uma variação do Teorema da Base, mas em infinitas variáveis) e avanços recentes em teoria de álgebras associativas.

Referências

[1] D.E. Cohen, *On the laws of a metabelian variety*, J. Algebra **5** (1967), 267-273.

[2] A. Garcia, Y. Lequain, Elementos de álgebra. Rio de Janeiro: Projeto Euclides-IMPA, 2002. 327 p.

[3] G. Higman, *Ordering by divisibility in abstract algebras,* Proc. London Math. Soc.(3) **2**, (1952), 326–336.

[4] S.M. Vovsi, Topics in varieties of group representations. London Mathematical Society Lecture Note Series, 163. Cambridge University Press, Cambridge, 1991. xiv+200 pp.

C5 - Números Surreais e Análise Não-Standard

Bryon Richard Hall

Instituto de Matemática e Estatística, IME/UFG,

Campus II - Samambaia,

74001-970, Goiânia, GO

E-mail: bryon@mat.ufg.br

É possível estender o conjunto R de modo a incluir números transfinitos e infinitesimais, como foi feito por Abraham Robinson em 1960. A álgebra do conjunto $\mathbb{R}*$, chamado de números surreais por John Conway, é uma simples extensão de $\mathbb{R}$, mas com várias aplicações interessantes para as quais $\mathbb{R}$ não basta. O melhor exemplo disso é a teoria dos jogos matemáticos desenvolvida por John Conway, Richard Guy e Martin Berlekamp desde a década de 1970 até hoje.

MC1 - Números: dos Naturais aos Reais

Eudes Antonio da Costa, Ronaldo Antonio Santos

UFT/Campus de Arraias | IME/UFG

77330-000 ,Arraias - TO| 74001-970, Goiânia - GO

| E-mail:rasantos@mat.ufg.br

2.5 APRESENTAÇÃO

A invenção dos números é sem dúvida uma grande evolução do pensamento humano. Porém esta evolução deu-se fortemente apoiada a conceitos intuitivos deixando vários fatos sem explicação satisfatória. Um exemplo foi o problema enfrentado pela escola Pitagórica ao descobrir grandezas incomensuráveis (números irracionais). Um outro problema foi o de mostrar que todo conjunto de números reais limitado superiormente possui supremo, resultado de grande necessidade em análise.

Foi por volta de 1858 que Richard Dedekind(1831-1916) fez a construção formal dos números reais a partir dos números racionais. Posteriormente percebeu-se a necessidade da construção dos números naturais, inteiros e racionais. Em 1891 Giuseppe Peano (1858-1932) construiu de maneira formal o conjunto dos números naturais. E a partir deste conjunto podemos construir os números inteiros, racionais e reais.

Neste trabalho faremos uma apresentação histórica da construção (Fundamentação) dos Números Naturais seguindo o método axiomático. Aceitando os **Conceitos Primitivos** de **o zero, número natural** e **sucessor de** e os **Axiomas** de Peano:

A_1 - Zero é um número natural.

A_2 - Todo número natural tem um único sucessor que também é um número natural.

A_3 - Zero não é sucessor de nenhum natural.

A_4 - Dois números naturais que tem sucessores iguais são, eles próprios, iguais.

A_5 - Se uma coleção S de números naturais contém o zero e também contém o sucessor de todos os seus elementos, então S é o conjunto de todos os naturais.

Seguiremos mostrando algumas propriedades acerca dos números (Naturais, Inteiros, Racionais e Reais), destacando a necessidade (prática) de tais números e sua fundamentação.

2.6 Discussões Preliminares

O conjunto mais simples de números são os inteiros positivos: 1, 2, 3, 4, ... usados para contar (quantidade de objetos) e chamados de séries dos números naturais e cujo conjunto é representado por $\mathbb{N}$. Estes números são tão antigos que Kronecker supostamente disse "Deus criou os números naturais; todo o resto é obra do homem".

Em muitos textos o 0 (**zero**) é também considerado um número natural. Mais adiante quando formalizarmos (Axiomas de Peano) esse conjunto também o consideraremos. Houve uma certa demora na invenção de um símbolo para representar o **nada**. Tal demora é justificada com o fato de que não sentimos necessidade em contar o que não temos. E a falta desse elemento causou inúmeros problemas

de interpretação, já que no sistema de numeração posicional decimal, a ausência do zero causa confusão; por exemplo, como distinguir o número 32 do número 302 ou do 320; pois não sabemos se são 3 centenas ou 3 dezenas, ou ainda, se são 2 dezenas ou 2 unidades. Com o zero podemos colocar o algarismo na posição correta. Esses problemas se sucederam até que os hindus, no final do século VI, inventaram o zero.

O princípio posicional consiste em dar ao algarismo um valor que depende não apenas do valor que ele representa na seqüência natural; como também da posição que ocupa, com respeito aos outros algarismos. No ábaco, a "coluna vazia"representava o nada(zero), por isso, não havia a necessidade de um símbolo, somente quando houve necessidade de fazer um registro permanente de uma operação realizado no ábaco, que enfrentamos esta dificuldade. Assim um progresso só foi possível após a criação de um símbolo para a classe "vazia", um símbolo para o "nada", o nosso "zero"moderno.

O conjunto dos números naturais é, como sabemos, fechado com relação a adição e multiplicação, isto é,

$$a, b \in \mathbb{N} \Rightarrow a + b \in \mathbb{N}$$

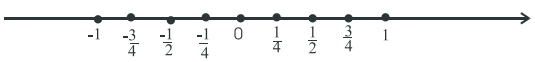
, e

$$a, b \in \mathbb{N} \Rightarrow a \cdot b \in \mathbb{N}.$$

Porém não é fechado com relação a subtração, pois, $a, b \in \mathbb{N}$ nem sempre implica em $a - b \in \mathbb{N}$. Portanto, além dos números naturais, são necessários outros símbolos para representar números como $3-5$ de modo a tornar o conjunto fechado com relação a subtração. Esses novos símbolos são os números negativos e o conjunto formado pela união desses aos naturais é chamado de conjuntos dos números inteiros e representado por $\mathbb{Z}$.

Dessa forma $\mathbb{Z}$ é fechado com relação a adição, multiplicação e subtração. No entanto não é fechado com relação a divisão, pois, $a \in \mathbb{Z}, b \in \mathbb{Z}^*$ a divisão de a por b pode não ser um número inteiro. O conjunto dos números inteiros é então acrescido dos símbolos $\frac{a}{b}$ para representar o resultado de tais divisões, obtendo um conjunto fechado com relação a divisão. Esse novo conjunto é chamado de conjunto de números racionais e denotado por $\mathbb{Q}$.

Todos esses números racionais podem ser representados como pontos em uma reta e estão relacionados ao "problema da medida", isto é, dados os segmentos AB e CD será que existe um segmento $OU = u$ chamada unidade, tal que $AB = m\dot{u}$ e $CD = n\dot{u}$? No caso afirmativo, os segmentos AB e CD são comensuráveis.



Os Pitagóricos acreditavam que os números racionais eram suficientes para medir qualquer segmento de reta. No entanto se surpreenderam ao constatar que não havia um número racional para medir a diagonal de um quadrado de lado 1. Portanto $\sqrt{2}$ não é racional, assim como π, $\sqrt{5}$, $\sqrt{1+\sqrt{3}}$,$sen(45^0)$, $2^{\sqrt{2}}$ e muitos outros.

O conjunto formado por todos os números racionais e irracionais é chamado de conjuntos de números reais e é denotado por $\mathbb{R}$.

O problema enfrentado pelos pitagóricos sugere a seguinte questão: Será que todo segmento de reta tem seu comprimento expresso por um número real? A resposta à essa questão é afirmativa e está ligada a completude dos números reais.

2.7 Fundamentação dos Números Naturais

Desde os primeiros anos do ensino fundamental estamos acostumados a trabalhar com *números naturais*, associando-os sempre à idéia de quantidade e utilizando-os para realizar contagens. Aprendemos a adicionar e multiplicar tais números, mas não estabelecemos exatamente o que eles são. Faremos isto nesta seção.

Tomemos como ponto de partida a série

$0, 1, 2, 3, ..., n, n+1, ...$

é esta série que teremos em mente quando falarmos da "série dos números naturais". Sabemos que foi necessário muito tempo para aceitar que um par "cadeiras"e um casal de humanos são ambos manifestações da quantidade (número) 2. O grau de abstração envolvido está longe de ser fácil.

O método axiomático, introduzido por Euclides na geometria grega (clássica) no século III a.C. é na álgebra utilizado por Peano (somente no séc. XIX) para fundamentar de forma lógica a aritmética.

No método axiomático deve-se, em primeiro lugar, aceitar certos termos da teoria sem uma explicação formal. Estes termos são chamados de **Conceitos Primitivos** e em nosso caso são: **o zero, número natural** e **sucessor de**. Em segundo lugar aceitar certas sentenças (ou asserções) como verdadeiras (independente de demonstração), tais sentenças são chamadas de **Axiomas**.

A partir dos termos primitivos acima, Peano formulou cinco axiomas, são eles:

A_1 - Zero é um número natural.

A_2 - Todo número natural tem um único sucessor que também é um número natural.

A_3 - Zero não é sucessor de nenhum natural.

A_4 - Dois números naturais que tem sucessores iguais são, eles próprios, iguais.

A_5 - Se uma coleção S de números naturais contém o zero e também contém o sucessor de todos os seus elementos, então S é o conjunto de todos os naturais.

A teoria se completa com Proposições (Teoremas) que, a partir dos axiomas, podem ser demonstrados por raciocínio lógico e correto. Formularemos e demonstraremos algumas dessas proposições.

Proposição 2.8. *Existe um número natural diferente de zero.*

Demonstração. Suponha que não exista um número natural diferente de zero. Pelo axioma A_2, zero tem um sucessor, que é portanto o próprio zero. Mas isso contraria o axioma A_3, pois zero seria o sucessor de zero. Portanto existe um natural diferente de zero. □

Usaremos o símbolo 0 para representar o número zero e o símbolo a^+ para indicar o sucessor de um número natural a. Além disso denotaremos o conjunto formado por todos os números naturais de $\mathbb{N}$.

Proposição 2.9. *Se $a \in \mathbb{N}$, então $a^+ \neq a$.*

Demonstração. Seja $S = \{a \in \mathbb{N}; a^+ \neq a\}$. Como vimos, o axioma A_3 garante que $0 \in S$. Se $a \in S$, então $a^+ \neq a$. Pelo axioma A_4 temos que $(a^+)^+ \neq a^+$, portanto $a^+ \in S$ sempre que $a \in S$. O axioma A_5 conclui que $S = \mathbb{N}$. □

Proposição 2.10. *Se $b \in \mathbb{N}$ e $b \neq 0$. Então existe $a \in \mathbb{N}$ tal que $a^+ = b$.*

Demonstração. Seja
$S = \{0\} \cup \{y \in \mathbb{N}; y \neq 0 \quad \text{e} \quad x^+ = y \quad \text{para algum} \quad x \in \mathbb{N}\}$. Por construção $0 \in S$. Se $a \in S$ e $a \neq 0$, então $b^+ = a$ para algum $b \in \mathbb{N}$. Decorre que $(b^+)^+ = a^+$ e portanto $a^+ \in S$. Novamente por A_5 temos que $S = \mathbb{N}$. □

Proposição 2.11. *Seja $S \subset \mathbb{N}$, não vazio, tal que $0 \notin S$. Então existe $a \in \mathbb{N}$ tal que $a \notin S$ e $a^+ \in S$.*

Demonstração. Suponha falsa a proposição. Tome $K = \{x \in \mathbb{N}; x^+ \notin S\}$, então $0 \in K$. Se $a \in K$ temos que $a^+ \notin S$, como estamos supondo falsa a afirmação, temos que $(a^+)^+ \notin S$ e portanto $a^+ \in K$. Concluímos por A_5 que $K = \mathbb{N}$, implicando $S = \emptyset$. Mas isso contradiz a hipótese. Logo a proposição está demonstrada. □

Proposição 2.12. *O conjunto dos números naturais não pode ser finito.*

Demonstração. O axioma A_2 garante que todo número natural tem sucessor. O Axioma A_3 diz que zero não é sucessor de nenhum número natural. Dessa forma, caso o conjunto dos numeros naturais seja finito, com n elementos, teremos que os n sucessores devem estar entre $n-1$ elementos o que obriga um elemento a ser sucessor de pelo menos dois elementos distintos, contrariando o axioma A_4. Concluímos que $\mathbb{N}$ não pode ser finito. □

Proposição 2.13. *(Princípio da indução completa) Suponha que a todo natural n esteja associada uma afirmação $P(n)$ tal que:*
i) $P(0)$ é verdadeira.
ii) $P(r^+)$ é verdadeira sempre que $P(r)$ for verdadeira.
Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração. Decorre diretamente de A_5. □

Outras proposições podem ser formuladas e sendo provadas, a partir dos axiomas e das proposições precedentes, passam a fazer parte da teoria.
A nossa próxima etapa é definir as operações de adição e multiplicação e uma relação de ordem no conjunto dos números naturais.

2.7.1 Adição em $\mathbb{N}$

Definição 2.14. *Dados $a, b \in \mathbb{N}$, o elemento $a + b \in \mathbb{N}$ é dito soma de a com b e é definido da seguinte forma:*

1. $a + 0 = a$

2. $a + b^+ = (a + b)^+$.

Observe que tal definição é uma lei de recorrência.

Até o momento não adotamos símbolos para representar os números naturais. Uma primeira representação pode se dar da forma,
$\mathbb{N} = \{0, 0^+, 0^{++}, 0^{+++}, 0^{++++}, ...\}$, sendo $0^{++} = (0^+)^+$ e assim por diante.

Exemplo 2.15.

- $0^+ + 0 = 0^+$
- $0^+ + 0^+ = (0^+ + 0)^+ = (0^+)^+ = 0^{++}$
- $0^{++} + 0^{++} = (0^{++} + 0^+)^+ = ((0^{++} + 0)^+)^+ = ((0^{++})^+)^+ = 0^{++++}$

Veja que as idéias primitivas de Peano - zero, número e sucessor - são passíveis de infinitas interpretações diferentes, todas as quais satisfarão as cinco proposições primitivas. Por exemplo:

Exemplo 2.16. *Suponha que "0"significa 100 e que "número"seja tomado como significando os números de 100 em diante na série dos números naturais. Nesse caso, todas as proposições primitivas ficam atendidas, e por conseqüência 99 não é um "número"no sentido que estamos usando.*

Exemplo 2.17. *Na notação usual, denotamos* $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, ...\}$*, sendo o sucessor de* 0 *é* 1*, o sucessor de* 1 *é* 2*, o sucessor de* 2 *é* 3 *e assim por diante. O exemplo anterior teria a forma:*

- $1 + 0 = 1$
- $1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2$
- $2 + 2 = 2 + 1^+ = (2 + 1)^+ = (2 + 0^+)^+ = ((2 + 0)^+)^+ = (2^+)^+ = 3^+ = 4$

2.7.2 Propriedades da Adição

1. Associativa: $a + (b + c) = (a + b) + c$, para todo $a, b, c \in \mathbb{N}$.
   Prova por indução sobre c.
   Se $c = 0$, então $a + (b + 0) = a + b = (a + b) + 0$. Suponha que $a + (b + r) = (a + b) + r$, então
   $(a + b) + r^+ = [(a + b) + r]^+ = [a + (b + r)]^+ = a + (b + r)^+ = a + (b + r^+)$,
   portanto pela indução completa temos que $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{N}$.

2. Elemento Neutro: $a + 0 = 0 + a = a$, para todo $a \in \mathbb{N}$.
   Para mostrar que 0 é o elemento neutro da adição basta provar que $0 + a = a$, pois a outra igualdade é a definição. Provaremos por indução sobre a. Observe que $0 + 0 = 0$. Suponha que $0 + a = a$. Temos que, $0 + a^+ = (0 + a)^+ = a^+$. O que prova a afirmação.

3. Comutatividade: $a + b = b + a$, para todo $a, b \in \mathbb{N}$.
   A prova deste fato é feita por indução sobre b.
   Para $b = 0$, temos pelo item anterior que $a + 0 = 0 + a$.
   Suponha que $a + b = b + a$, observe que $a + b^+ = (a + b)^+ = (b + a)^+ = b + a^+ = b^+ + a$(prove por indução que $b + a^+ = b^+ + a$) . Concluindo a prova.

4. Lei do Cancelamento: $b + a = c + a \Rightarrow b = c$.
   Faremos a prova por indução sobre a. Para $a = 0$ a afirmação é verdadeira, pois se $b + 0 = c + 0$ então $b = c$.
   Suponha que, $b + a = c + a \Rightarrow b = c$. Então,
   $b+a^+ = c+a^+$ implica pela definição $(b+a)^+ = (c+a)^+$ implicando pelo axioma A_4 que $b+a = c+a$ implicando pela hipótese de indução que $b = c$.
   A indução completa conclui que tal afirmação é verdadeira para todo $a \in \mathbb{N}$.

2.7.3 Multiplicação em $\mathbb{N}$

Definição 2.18. *Dados $a, b \in \mathbb{N}$, o elemento $a \cdot b = ab \in \mathbb{N}$ é dito de produto de a com b, e é definido da seguinte forma:*

1. $a \cdot 0 = 0$
2. $a \cdot b^+ = a \cdot b + a$

Propriedades da Multiplicação

1. Associativa: $a(bc) = (ab)c$
   Prova: (por indução sobre c)
   Vemos que se $c = 0$, então $a(b.0) = a.0 = 0 = (ab).0$.
   Suponha verdadeira para $c \in \mathbb{N}$, isto é, $a(bc) = (ab)c$.
   Temos que $a(bc^+) = a(bc+b) = a(bc)+ab = (ab)c+ab = a(bc)+ab = a(bc+b) = a(cb^+)$. Mostrando que é também verdadeira para c^+. Pela indução completa a afirmação é verdadeira para todo $c \in \mathbb{N}$.

2. Comutativa: $ab = ba$
   Prova: Exercício

3. Para todo $b \in \mathbb{N}$, $0.b = 0$.
   Prova: Indução sobre b. Se $b = 0$ então $0 \cdot 0 = 0$ (definição). Suponha verdadeiro para $b \in \mathbb{N}^*$, isto é, $0 \cdot b = 0$. Assim $0 \cdot b^+ = 0 \cdot b + 0 = 0 + 0 = 0$. O que prova a afirmação para todo natural.

4. Elemento Neutro: $a.1 = 1.a = a$
   Prova: Veja que por definição $a \cdot 1 = a \cdot 0^+ = a \cdot 0 + a = 0 + a = a$. E $1 \cdot a = a$ basta usar a comutatividade da multiplicação.

5. Distributiva: $(b + c)a = ba + ca$
   Prova: Indução sobre a. Se $a = 0$, temos $(b+c) \cdot a = 0 = b \cdot 0+c \cdot 0$. Supondo verdadeira para algum $a \in \mathbb{N}^*$, Assim $(b+c) \cdot a^+ = (b+c) \cdot a+(b+c) = (ba+ca)+(b+c) = (ba+b)+(ca+c) = ba^+ + ca^+$.
   Portanto vale para qualquer inteiro a.

6. Anulamento:$ab = 0 \quad \Rightarrow \quad a = 0 \quad \text{ou} \quad b = 0$
   Prova: Exercício

2.7.4 Relação de Ordem em $\mathbb{N}$

Definição 2.19. *Dados $a, b \in \mathbb{N}$ diremos que a é menor ou igual a b e denotaremos por $a \leq b$, se existir $c \in \mathbb{N}$ tal que $a + c = b$.*

Exemplo 2.20. $5 \leq 7$ *pois tomando* $c = 2$ *temos que* $5 + 2 = 7$.

Proposição 2.21. *Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.*

Demonstração. Seja S um subconjunto não vazio de $\mathbb{N}$ e admita que S não possua um menor elemento. Vamos mostrar que S é vazio (uma contradição).

Considere o conjunto T, suplementar de S em $\mathbb{N}$. Defina o conjunto $I_n = \{k \in \mathbb{N} : k \leq n\}$ e considere a sentença

$$p(n) : I_n \subset T.$$

Como $0 \leq n$ para todo n, segue que $0 \in T$, pois, caso contrário, 0 seria um menor elemento de S. Logo, $p(0)$ é verdade.

Admita que $p(k)$ seja verdade, para algum $k \geq 0$. Se $k+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $k+1$ é o menor elemento de S, o que não é permitido. Logo $k+1 \in T$, seguindo daí que

$$I_{k+1} = I_k \cup \{k+1\} \cup T,$$

o que garante que, para todo $n, I_n \cup T$; portanto, $\mathbb{N} \cup T \cup N$ e, conseqüentemente, $T = N$ e $S = \emptyset$ (um absurdo).

Portanto S possui um menor elemento. □

2.8 Exercícios

Exercício 1. *Não existe nenhum número natural n tal que $0 < n < 1$.*

Exercício 2. *Para todo $a \in \mathbb{N}$ temos que $0 \cdot a = 0$.*

Exercício 3. *Dado um número natural n qualquer, não existe nenhum número natural m tal que $n < m < n + 1$.*

Exercício 4. *Sejam $a, b \in \mathbb{N}$ se $a + b = 0$ então $a = b = 0$. Se $a + b = 1$ então $a = 1$ ou $b = 1$. Se $a + b = 2$ então $a = b = 1$.*

Exercício 5. *Sejam $a, b \in \mathbb{N}$ se $a \cdot b = 1$ então $a = b = 1$. Se $a + b = 1$ então $a = 1$ ou $b = 1$. Se $a + b = 2$ então $a = b = 1$.*

Exercício 6. *A relação "menor ou igual"($\leq$) é uma relação de ordem (Reflexiva, anti-Simétrica e Transitiva) em $\mathbb{N}$.*

Exercício 7. *Sejam $a, b, c \in \mathbb{N}$. $a \leq b$ se e só se $a + c \leq b + c$. $a \leq b$ se e só se $a \cdot c \leq b \cdot c$.*

Dados dois números naturais a e b com $a \leq b$, sabemos que existe um número natural c tal que $b = a + c$. Neste caso, definimos o número **b menos a**, denotado por $b - a$, como sendo o número c.

Exercício 8. *Sejam $a, b, c \in \mathbb{N}$. Se $a \leq b$, então $c \cdot (b - a) = c \cdot b - c \cdot a$.*

Exercício 9. *Sejam $a, b, c \in \mathbb{N}$ tais que $a-(b-c)$ esteja bem definido. Mostre que $a-(b-c) = (a+c)-b$.*

Exercício 10. *Sejam $a, b \in \mathbb{N}$ com $0 < a < b$. Mostre que existe n tal que $na > b$. Se $a > 1$ então existe n tal que $a^n > b$*

2.9 Construção dos Números Inteiros

Considerando a equação $a + x = c$, para a, c números naturais e m uma incógnita, temos que no conjunto dos naturais existe solução se e só se, $c \geq a$. No entanto existem situações na prática em que necessitamos investigar a equação $a + x = c$ com $c < a$. Por exemplo, você tem em sua conta bancária 100 reais e sabe-se que amanhã será apresentado um cheque no valor de 120 reais, o resultado disso sabemos, fica-se devendo 20 reais ao banco, ou seja, fica-se com um saldo "negativo". Uma questão é, como expressar essa situação, sabendo que os números naturais não abarca tal situação. Assim precisamos de um novo conjunto numérico.

A construção dos números inteiros não será feita como a dos naturais onde foram introduzidos conceitos primitivos e axiomas. Faremos essa construção a partir dos números naturais obtidos anteriormente.

Os números inteiros devem ser construídos de tal forma a dar sentido a expressão $a - b$ para todo $a, b \in \mathbb{N}$. Para tanto associaremos a expressão $a - b$ ao par $(a, b) \in \mathbb{N} \times \mathbb{N}$ e nesse conjunto definiremos a seguinte relação,

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

Proposição 2.22. *A relação $\sim$ é uma relação de equivalência,isto é,*

1. *Reflexiva:* $(a, b) \sim (a, b)$

2. *Simétrica:* $(a, b) \sim (c, d) \Leftrightarrow (c, d) \sim (a, b)$

3. *Transitiva:* $(a, b) \sim (c, d) \quad e \quad (c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$

Demonstração. 1. $(a, b) \sim (a, b) \Leftrightarrow a + b = b + a$ Comutativa da adição.

2. $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow c + b = d + a \Leftrightarrow (c, d) \sim (a, b)$

3. De $(a, b) \sim (c, d)$ temos $a + d = b + c \Leftrightarrow a + d + f = b + c + f$ (1). De $(c, d) \sim (e, f)$ temos $c + f = d + e$. Assim fazendo (2) em (1) temos:

$$a + d + f = b + (c + f) = b + (d + e) = b + d + e$$

o que acarreta que $a + f = b + e \Leftrightarrow (a, b) \sim (e, f)$.

□

Portanto essa relação define uma partição no conjunto $\mathbb{N} \times \mathbb{N}$ em classes de equivalência. Uma classe de equivalência determinada por um elemento (a, b) é denotada por $\overline{(a, b)}$ e é o conjunto,

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N}; (x, y) \sim (a, b)\}.$$

O conjunto de todas as classes de equivalência de $\mathbb{N} \times \mathbb{N}$ é denotado por $\mathbb{N} \times \mathbb{N}/\sim$ e chamado de quociente de $\mathbb{N} \times \mathbb{N}$ pela relação $\sim$. Tal conjunto será entendido como conjunto dos números inteiros e denotado por $\mathbb{Z}$.

Exemplo 2.23.

1. $\overline{(4, 2)} = \{(2, 0), (3, 1), (4, 2), ...\}$
2. $\overline{(3, 5)} = \{(0, 2), (1, 3), (3, 4), ...\}$
3. $\overline{(0, 0)} = \{(0, 0), (1, 1), (2, 2), ...\}$
4. $\overline{(1, 5)} = \{(0, 4), (1, 5), (2, 6), ...\}$

Algumas dessas classes estão representadas na Figura(2.9), onde cada classe tem uma parte no primeiro quadrante e a outra no segundo. Lembramos que no terceiro e quarto quadrante encontram-se outras classes de equivalência da relação.

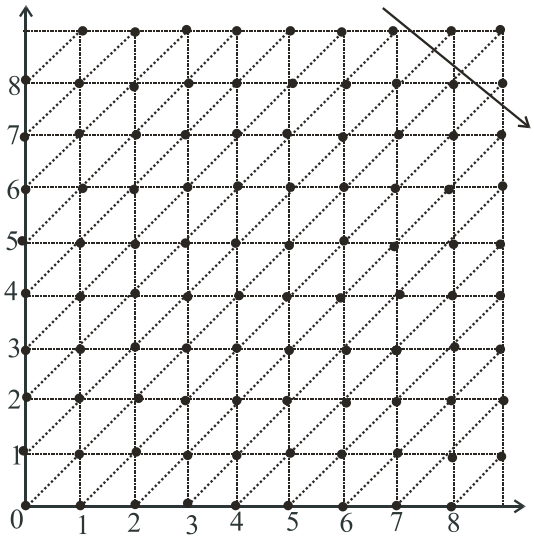


Figura 1: Classes de equivalência da relação $\sim$

Observando a figura associamos algumas classes aos números naturais (positivos) e outras aos números negativos, da seguinte forma:

$\overline{(1, 0)} = 0$	$\overline{(0, 1)} = -1$
$\overline{(2, 0)} = 2$	$\overline{(0, 2)} = -2$
$\overline{(3, 0)} = 3$	$\overline{(0, 3)} = -3$
$\overline{(4, 0)} = 4$	$\overline{(0, 4)} = -4$
$\vdots$	$\vdots$
$\overline{(k, 0)} = k$	$\overline{(0, k)} = -k$
$\vdots$	$\vdots$

Além disso a seta na figura acima já nos da uma possível ordenação dos inteiros a qual mantém a ordenação dos naturais. Para que tais idéias se consolidem, devemos agora definir as operações (adição e multiplicação) e a relação "menor ou igual"(ordem) em $\mathbb{Z}$.

Observando que gostaríamos de ter $2 + (-3) = -1$, isto é,

$$\overline{(2,0)} + \overline{(0,3)} = \overline{(0,1)};$$

e também que $(-2).(-3) = 6$, isto é,

$$\overline{(0,2)}.\overline{(0,3)} = \overline{(6,0)};$$

e ainda $-1 \leq 1$, ou seja,

$$\overline{(0,1)} \leq \overline{(1,0)}.$$

Começamos definindo a adição em $\mathbb{Z}$.

2.9.1 Adição em $\mathbb{Z}$

Lembrando que o par (a,b) está associado a diferença $a-b$ é razoável pensar que $(a,b)+(c,d)$ é $(a-b)+(c-d)$ que pode se escrito da forma $(a+c)-(b+d)$, que por sua vez está associado ao par $(a+c, b+d)$. Isso nos motiva a seguinte definição.

Definição 2.24. *Dados os elementos $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$ chama-se soma o elemento definido por,*

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, c+d)}.$$

Como se trata de soma de classes de equivalência e uma mesma classe pode ser representada por diferentes elementos. Devemos mostrar que tal definição não depende dos representantes escolhidos para cada uma das classes, isto é,
se

$$\overline{(a,b)} = \overline{(a_1,b_1)} \quad \text{e} \quad \overline{(c,d)} = \overline{(c_1,d_1)}$$

então,

$$\overline{(a+c, b+d)} = \overline{(a_1+c_1, b_1+d_1)}.$$

Vejamos, temos que $(a,b) = (a_1,b_1) \Leftrightarrow a + b_1 = b + a_1 (1)$ e $(c,d) = (c_1,d_1) \Leftrightarrow c + d_1 = d + c_1 (2)$. Usando (1) e (2) em

$$(a+c) + (b_1+d_1) = (a+b_1) + (c+d_1) = (b+a_1) + (d+c_1) = (b+d) + (a_1+c_1),$$

ou $(a,b) + (c,d) = (a_1,b_1) + (c_1+d_1)$, assim demonstramos que a adição de inteiros independe do representante da classe.

2.9.2 Propriedades da Adição em $\mathbb{Z}$

Seja $x \in \mathbb{Z}$, então existe um par de naturais $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, sendo x uma classe de equivalência e (a, b) um representante da classe.

1. Associativa: $x + (y + z) = (x + y) + z$, para todo $x, y, z \in \mathbb{Z}$.
   Prova: Considere $x = (a, b)$, $y = (c, d)$ e $z = (e, f)$. Assim,

   $$x + (y + z) = (a, b) + [(c, d) + (e, f)] = (a, b) + (c + f, d + e) = (a + (d + e), b + (c + f)),$$

   usando a associatividade nos naturais, temos,

   $(a+(d+e), b+(c+f)) = ((a+d)+e, (b+c)+f) = (a+d, b+c)+(e, f) = [(a, b)+(c, d)]+(e, f) = (x + y) + z$.

2. Comutativa: $x + y = y + x$, para todo $x, y \in \mathbb{Z}$.
   Prova: Exercício.

3. Elemento neutro: $x + 0 = 0 + x = x$, para todo $x \in \mathbb{Z}$, sendo $0 = \overline{(0, 0)}$.
   Prova: Segue diretamente da definição.

4. Elemento simétrico (oposto): Para todo $x \in \mathbb{Z}$ existe $y \in \mathbb{Z}$ tal que $x + y = 0$.
   Prova: Veja que dado $x = (a, b)$ então $y = (-a, -b$, pois $x + y = (a, b) + (-a, -b) = (0, 0) = 0$.

2.9.3 Subtração em $\mathbb{Z}$

A subtração pode ser definida a partir da adição utilizando o elemento simétrico (oposto), isto é, dados $x, y \in Z$ então $x - y = x + (-y)$.

2.9.4 Multiplicação em $\mathbb{Z}$

Lembrando novamente que (a, b) está associado a $a - b$, temos que $(a, b).(c, d)$ pode ser associado a $(a - b).(c - d)$ que é igual a $(ac + bd) - (bc + ad)$ que pode ser associado ao par $(ac + bd, bc + ad)$. Dessa forma somos levados a seguinte definição para o produto:

Definição 2.25. *Dados $x = \overline{(a, b)}$ e $y = \overline{(c, d)}$ números inteiros, chamaremos de produto de x por y o elemento $x \cdot y$ definido da forma,*

$$x \cdot y = \overline{(ac + bd, ad + bc)}$$

Novamente devemos mostrar que tal definição independe do representante escolhido para a classe.

Propriedades da Multiplicação em $\mathbb{Z}$

Sejam $x = (a, b)$, $y = (c, d)$ e $z = (e, f)$ números inteiros então vale as seguintes propriedades em relação à multiplicação de inteiros:

1. Associativa: $x.(y.z) = (x.y).z$
2. Comutativa: $x.y = y.x$
3. Elemento Neutro: $x.1 = 1.x = x$, sendo $1 = \overline{(1, 0)}$.
4. Lei do Anulamento do produto: $x.y = 0 \Rightarrow x = 0 \quad$ ou $\quad y = 0$.

   E ainda, uma propriedade que relaciona a multiplicação e a adição, a propriedade

5. Distributiva da multiplicação em relação a adição: $x.(y+z) = x.y + x.z$

2.9.5 Relação de Ordem em $\mathbb{Z}$

A ordem definida em $\mathbb{Z}$ é semelhante a ordem definida em $\mathbb{N}$ e tem o sentido mostrado na Figura (2.9).

Definição 2.26. *Sejam $m, n \in \mathbb{Z}$, dizemos que m é menor ou igual a n, denotamos $m \leq n$, se $n = m + r$ para algum $r \in \mathbb{Z}_+$,*
onde $\mathbb{Z}_+ = \{0, 1, 2, 3, ...\} = \{\overline{(0,0)}, \overline{(0,1)}, \overline{(0,2)}, \overline{(0,3)}, ...\}$.

Neste caso dizemos que n é maior ou igual a m e denotamos por $n \geq m$.

Daremos mais algumas definições que serão necessária adiante.

Definição 2.27. *Um subconjunto de números inteiros $S \neq \emptyset$ é dito limitado superiormente se existir um número inteiro a tal que $x \leq a$ para todo $x \in S$. Se existir $a \in S$ satisfazendo a condição anterior, então a é dito máximo de S.*

Definição 2.28. *Um subconjunto de números inteiros $S \neq \emptyset$ é dito limitado inferiormente se existir um número inteiro a tal que $x \geq a$ para todo $x \in S$. Se existir $a \in S$ satisfazendo a condição anterior, então a é dito mínimo de S.*

Definição 2.29. *Um subconjunto de números inteiros é dito limitado quando é limitado superiormente e inferiormente.*

Podemos formular o seguinte teorema.

Proposição 2.30. *Todo subconjunto limitado e não vazio de números inteiros possui máximo e mínimo.*

Demonstração. Vamos mostrar que tal conjunto $S \cup \mathbb{Z}$ possui mínimo.

Seja $S' = \{x - k : x \in S\}$, sendo k uma cota inferior de S, que, por hipótese, existe. Notemos que $S' \neq \emptyset$, pois $S \neq \emptyset$ e que, como $k \leq x$ então $x - k \geq 0$ para todo $x \in S$, ou seja, $S' \cup N$. Logo, pelo princípio do menor número natural, S' possui mínimo, digamos $min(S') = m_0 = m - k$ para algum $m \in S$.

Mostremos que $m = min(S)$. Se $x \in S$, então $x - k \in S'$ disto temos $m - k \leq x - k$. Donde $m \leq x$, e como $m \in S$ temos que $m = min(S)$. □

O procedimento da demonstração pode ser visto no seguinte situação. Seja $S = \{-1, 0, 1, 2, 3\}$. Neste caso, considere $k = -2$, por exemplo, então $S' = \{k - x : x \in S\} = \{1, 2, 3, 4, 5\}$ cujo mínimo é $1 = min(S') = m - (-2)$, disto temos que $m = -1 = min(S)$. (Evidente!)

2.10 Exercícios

Exercício 11. *Dado $a \in \mathbb{Z}$ com $a > 0$. Mostre que $a \cdot (-1) = -a$ e que $-a < 0$.*

Exercício 12. *Dados $a, b \in \mathbb{Z}$. Mostre que $a \cdot (-b) = -ab$ e que $(-a) \cdot (-b) = ab$.*

Exercício 13. *Dados $a, b, c, d \in \mathbb{Z}$. Mostre que $(a-b)\cdot(c-d) = (ac+bd)-(ad+bc)$ e que $(a+b)\cdot(c-d) = (ac + bc) - (ad + bd)$.*

Exercício 14. *Dados $a, b \in \mathbb{Z}$ com $a \cdot b = 1$. Mostre que $a = b = 1$ ou $a = b = -1$.*

Exercício 15. *Para todo $a \in \mathbb{Z}$. Se $a^2 = a$ então $a = 0$ ou $a = 1$.*

Exercício 16. *Mostre que todo subconjunto limitado e não vazio de números inteiros possui máximo.*

Exercício 17. *Mostre que, Para todo $n \in \mathbb{Z}$, o conjunto $V = \{x \in \mathbb{Z} : n < x < n + 1\}$ é vazio.*

2.11 Construção dos Números Racionais

Nesse momento faremos a construção do conjunto dos números racionais a partir dos números inteiros. A idéia é dar sentido a expressão $\frac{p}{q}$ para todo $p \in \mathbb{Z}$ e $q \in \mathbb{Z}^*$. Seguindo a mesma idéia na construção dos inteiros, associaremos a expressão $\frac{p}{q}$ ao par $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$, onde $\mathbb{Z}^* = \{x \in \mathbb{Z}; x \neq 0\}$. Definiremos nesse conjunto a seguinte relação,

$$(a, b) \sim (c, d) \Leftrightarrow a.d = b.c$$

Proposição 2.31. *A relação " $\sim$ ", definida acima, é uma relação de equivalência.*

Demonstração. Devemos mostrar que valem as propriedades: Reflexiva, Simétrica e Transitiva.

a) Reflexiva: $(a, b) \sim (a, b)$ pois $a.b = b.a$.

b) Simétrica: $(a, b) \sim (c, d) \Leftrightarrow a.d = b.c \Leftrightarrow c.b = d.a \Leftrightarrow (c, d) \sim (a, b)$.

c) Transitiva: Temos que

$$(a, b) \sim (c, d) \Leftrightarrow a.d = b.c \Leftrightarrow a.d.f = b.c.f \quad (1)$$

$$(c, d) \sim (e, f) \Leftrightarrow c.f = d.e \Leftrightarrow b.c.f = b.d.e \quad (2)$$

De (1) e (2) temos

$$a.d.f = b.d.e \Leftrightarrow a.f = b.e \Leftrightarrow (a, b) \sim (e, f).$$

□

A relação $\sim$ determina no conjunto $\mathbb{Z} \times \mathbb{Z}^*$ uma partição em classes de equivalência. Cada par $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ determina uma classe de equivalência indicada por $\frac{p}{q} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^*; (x, y) \sim (p, q)\}$.

Exemplo 2.32.

- $\frac{1}{1} = \{(1, 1), (2, 2), (3, 3), ...\}$
- $\frac{1}{2} = \{(1, 2), (2, 4), (3, 6), ...\}$
- $\frac{3}{1} = \{(3, 1), (6, 2), (9, 3), ...\}$

O conjunto de todas essas classes é chamado de quociente de $\mathbb{Z} \times \mathbb{Z}^*$ pela relação $\sim$, denotado por $\mathbb{Z} \times \mathbb{Z}^* / \sim$. Tal conjunto será designado por conjunto dos números racionais e denotado por $\mathbb{Q}$.

Graficamente essas classes são dadas por:

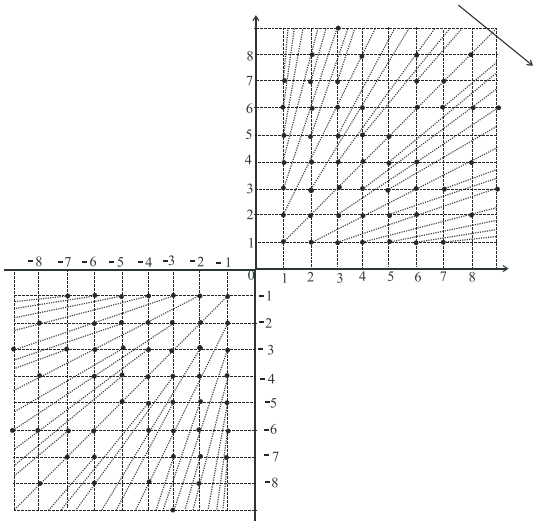


Figura 2: Classe de equivalência

Novamente temos uma possível ordenação para essas classes. Observe também que as classes de equivalência que formaram os números inteiros se mantinham a uma "distância"fixa. Enquanto que essas tem classes muito "próximas"umas das outras. Vamos, nesse momento, definir as operações e a relação de ordem de $\mathbb{Q}$

2.11.1 Adição em $\mathbb{Q}$.

Definição 2.33. *Sejam* $a = \frac{m}{n}, b = \frac{p}{q} \in \mathbb{Q}$. *Chama-se soma de* a *com* b *e indica-se por* $a+b$ *o elemento de* $\mathbb{Q}$ *definido por:*

$$a + b = \frac{mq}{nq} + \frac{np}{nq} = \frac{mq + np}{nq}$$

Devemos mostrar que tal definição independe dos representantes escolhidos para as classes a e b. O que é verdade, pois se $a = \frac{m}{n} = \frac{m'}{n'}$ e $b = \frac{p}{q} = \frac{p'}{q'}$, então

$$m.n' = n.m' \quad \text{e} \quad p.q' = q.p'$$

Multiplicando a primeira igualdade por $q.q'$ e a segunda por $n.n'$, somando membro a membro e agrupando obtemos,

$$(mq + pn)n'q' = nq(m'q' + p'n')$$

portanto,

$$\frac{mq + pn}{nq} = \frac{m'q' + p'n'}{n'q'}.$$

Propriedades da Adição

1. Associativa: $(a + b) + c = a + (b + c), \forall a, b, c \in \mathbb{Q}$
2. Comutativa: $a + b = b + a, \forall a, b \in \mathbb{Q}$
3. Elemento Neutro: $a + 0 = 0 + a, \forall a \in \mathbb{Q}$ onde $0 = \frac{0}{n}, n \in \mathbb{Z}^*$
4. Elemento Simétrico(oposto): $\forall a \in \mathbb{Q}, \exists -a \in \mathbb{Q}; \quad a + (-a) = 0$

Exercício 18. *Provar as propriedades acima.*

2.11.2 Multiplicação em $\mathbb{Q}$

Definição 2.34. *Sejam* $a = \frac{m}{n}, b = \frac{p}{q} \in \mathbb{Q}$. *Chama-se produto de* a *com* b *e indica-se por* $a.b = ab$ *o elemento de* $\mathbb{Q}$ *definido por:*

$$ab = \frac{mp}{nq}$$

Novamente devemos mostrar que tal definição independe dos representantes escolhidos para a e b.

Sejam

$$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow m.n' = n.m' \tag{3}$$

e

$$\frac{p}{q} = \frac{p'}{q'} \Leftrightarrow p.q' = q.p' \tag{4}$$

Multiplicando (3) por (4), temos

$$(m.n').(p.q') = (n.m').(q.p') \Leftrightarrow (m.p).(n'.q') = (n.q).(m'.p') \Leftrightarrow \frac{m.p}{n.q} = \frac{m'.p'}{n'.q'}$$

Ou seja, a multiplicação de dois números racionais independe dos representantes de classe.

2.11.3 Propriedades da Multiplicação

1. Associativa: $(ab)c = a(bc), \forall a, b, c \in \mathbb{Q}$
2. Comutativa: $ab = ba, \forall a, b \in \mathbb{Q}$
3. Elemento Neutro: $a.1 = 1.a, \forall a \in \mathbb{Q}$ onde $1 = \frac{n}{n}, n \in \mathbb{Z}^*$
4. Elemento Simétrico(inverso): $\forall a \in \mathbb{Q}^*, \exists a^{-1} \in \mathbb{Q}; \quad aa^{-1} = 1$
5. Distributiva: $a(b + c) = ab + ac, \forall a, b, c \in \mathbb{Q}$

Exercício 19. *Provar as propriedades acima.*

2.11.4 Relação de Ordem em $\mathbb{Q}$

Observe que $\forall a \in \mathbb{Q}$ podemos escolher um representante $a = \frac{p}{q}$ de tal forma que $q > 0$.

Exemplo 2.35.

- $\frac{-2}{-3} = \frac{2}{3}$
- $\frac{2}{-3} = \frac{-2}{3}$

Definição 2.36. *Sejam* $a = \frac{m}{n}, b = \frac{p}{q} \in \mathbb{Q}$ *onde* n *e* q *são estritamente positivos. Nessas condições diz-se que* a *é menor ou igual a* b *se* $mq \leq np$ *(Relação de ordem em* $\mathbb{Z}$*).*

Exemplo 2.37.

- $\frac{-2}{3} \leq \frac{2}{3}$, *pois* $-2.3 \leq 3.2$
- $\frac{-5}{7} \leq \frac{-2}{3}$, *pois* $-5.3 \leq 7.(-2)$

Veja na Figura (2) como as classes ficam ordenadas.

2.12 Existem números não Racionais

Os pitagóricos entediam que o sagrado mistério da ciência tinham o seu centro na matemática, isto é, no estudo dos números (racionais). Como relacionavam números às grandezas geométricas (segmentos) pensavam que estes se reduziam as coisas (res:realidade) à unidade e ao ponto. Assim consideravam os números como elementos de todas as coisas.

A tese pitagórica de que as coisas (res) são números, isto é, todas as coisas(res) têm um número (formado por unidades) e que sem os números nada se pode conceber ou compreender; resumidamente diziam eles, os números são a essência de todas as coisas.

O nome de Pitágoras permanece associado a uma importante relação numérica que demonstrou haver no triâgulo retâgulo: área do quadrado sobre a hipotenusa é igual a soma das áreas dos quadrados sobre cada cateto.

No entanto, usando dois conhecimentos pitagóricos: 1) de que todas as coisas(res) podem ser expressas por um número (racional); 2) o teorema de Pitágoras. Leva-nos a uma incompatibilidade, vejamos: Considere o quadrado de lado 1(uma) unidade e aplicando o teorema de Pitágoras encontramos que sua diagonal(d) pode ser expressa pela relação $d^2 = 1^2 + 1^2$, ou seja, $d^2 = 2$.

Surge então no interior da comunidade pitagórica a pergunta: qual número (racional) cujo quadrado é 2? Este problema, aparentemente, foi resolvido pelos pitagóricos, para o desespero da comunidade.

Para resolvermos o problema: existe um número racional $\frac{p}{q}$ cujo quadrado é 2? Utilizaremos o método "redução ao absurdo"que consiste em admitir que tal solução exista e analisar as conseqüências de tal afirmação.

Admita que exista um número racional $\frac{p}{q}$, irredutível cujo quadrado é 2, isto é, $(\frac{p}{q})^2 = 2$ assim $p^2 = 2q^2$ o que podemos concluir que p^2 é par e equivalentemente p é par, assim podemos escrever $p = 2k$, para algum inteiro k. Substituindo p por $2k$ obtemos $4k^2 = 2q^2$, simplificando a equação obtemos $2k^2 = q^2$. Assim obtemos, novamente, que q^2 é par e por conseqüência q é par. Contrariando nossa hipótese de que o número racional $\frac{p}{q}$ seja irredutível, assim somos obrigados a concluir que não existe um número racional cujo quadrado seja 2. Esta foi uma das primeiras crises(fraqueza) da comunidade pitagórica.

Outro fato que revelou mais uma crise(fraqueza) na comunidade pitagórica foi a teoria da existência da menor grandeza geométrica (mônada) e que toda grandeza geométrica era formada por uma quantidade ilimitada de mônodas. A aceitação de tal fato leva-nos à um absurdo, a não explicação racional do movimento, fato observado por Zenão de Eléia.

Exercício 20.

1. *Mostre que* $\sqrt{3}$ *não é racional.*
2. *Mostre que* $\sqrt{p}$ *não é racional, sendo p primo.*
3. *Mostre que* $\log 2$ *não é racional.*

2.12.1 Como obter exemplos de números não-racionais

Apresentaremos uma maneira de se obter números irracionais (não-racionais) a partir do seguinte teorema:

Teorema 2.38. *Considere a equação polinomial com coeficientes inteiros*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0 \tag{5}$$

Se esta equação possuir uma raiz racional irredutível $\frac{p}{q}$. Então p é divisor de a_0 e q divisor de a_n.

Demonstração. Seja $\frac{p}{q}$ irredutível e raiz de (5), então,

$$a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + ... + a_1(\frac{p}{q}) + a_0 = 0. \tag{6}$$

Multiplicando ambos os membros dessa equação por q^n, obtemos,

$$a_n p^n + a_{n-1} q p^{n-1} + ... + a_1 p q^{n-1} + a_0 q^n = 0, \tag{7}$$

que pode ser escrita da forma

$$a_0 q^n = -p(a_n p^{n-1} + a_{n-1} p^{n-2} q + ... + a_1 q^{n-1}). \tag{8}$$

Portanto p é divisor de $a_0 q^n$. Mas p não é um divisor de q^n. Então p é divisor de a_0.

De maneira análoga, podemos escrever a equação (7) da forma

$$a_n p^n = -q(a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q + ... + a_1 p q^{n-2} + a_0 q^{n-1}). \tag{9}$$

Portanto q é divisor de $a_n p^n$. Como q não é divisor de p^n. Concluímos que q é divisor de a_n. Completando a demonstração.

Com esse teorema podemos demonstrar a irracionalidade de vários números.

Exemplo 2.39. *O número $\sqrt{2}$ é irracional.*
Solução: *$\sqrt{2}$ é raiz da equação*

$$x^2 - 2 = 0. \tag{10}$$

Observe que se tal equação polinomial tiver uma raiz racional irredutível $\frac{p}{q}$, teremos que p é divisor de 2 e q é divisor de 1. Portanto as possibilidades são $p = 1, -1, 2, -2$ e $q = 1, -1$. Concluímos que as possíveis raízes são $1, -1, 2$ e -2. Mas essas não são raízes da equação (10), como se pode verificar diretamente; as igualdades

$$1^2 - 2 = 0, \quad (-1)^2 - 2 = 0, \quad 2^2 - 2 = 0, \quad (-2)^2 - 2 = 0$$

são todas falsas.
Portanto a equação 10 não possui raiz racional, de modo que $\sqrt{2}$ é um número irracional.

Exemplo 2.40. *O número $\sqrt{2} + \sqrt{3}$ é irracional.*
Solução: *Construiremos um polinômio que tem tal número como raiz e mostraremos que tal polinômio não tem raiz racional usando o Teorema (2.38). Fazendo*

$$x = \sqrt{2} + \sqrt{3}.$$

Elevando ambos os membros ao quadrado, obtemos

$$x^2 = 2 + 2\sqrt{2}\sqrt{3} + 3,$$

reorganizando os termos, temos

$$x^2 - 5 = 2\sqrt{6}.$$

Elevando novamente ao quadrado, obtemos

$$x^4 - 10x^2 + 25 = 24,$$

ou

$$x^4 - 10x^2 + 1 = 0. \tag{11}$$

A equação 11 foi construída de tal forma que $\sqrt{2}+\sqrt{3}$ *é uma de suas raízes. Aplicando o Teorema 2.38, concluímos que a equação* (11) *não tem raízes racionais, portanto* $\sqrt{2}+\sqrt{3}$ *é irracional.*

Exercício 21.

1. *Provar que se p é primo então* $\sqrt{p}$ *é irracional.*
2. *Verifique se* $\sqrt[3]{\sqrt{3}+\sqrt{2}}$ *é ou não irracional.*

Exemplo 2.41. *Surpreendentemente o número* $\sqrt[3]{2-\sqrt{5}}+\sqrt[3]{2+\sqrt{5}}$ *é racional.*
Solução *Fazendo* $x = \sqrt[3]{2-\sqrt{5}}+\sqrt[3]{2+\sqrt{5}}$. *Elevando ao cubo ambos os membros e fazendo as algumas simplificações teremos,*

$$-3(\sqrt[3]{2-\sqrt{5}}+\sqrt[3]{2+\sqrt{5}}) = x^3 - 4$$

isto é,

$$x^3 + 3x - 4 = 0$$

portanto o número $\sqrt[3]{2-\sqrt{5}}+\sqrt[3]{2+\sqrt{5}}$ *é uma raiz real da equação polinomial acima. Mas tal equação polinomial pode ser escrita da forma*
$(x-1)(x^2+x+4) = 0$ *cuja única raiz real é* $x = 1$. *Concluímos que,*

$$\sqrt[3]{2-\sqrt{5}}+\sqrt[3]{2+\sqrt{5}} = 1$$

e portanto racional.

Exercício 22.

1. *Mostre que se a e b são números racionais, então o número* $\frac{1}{2}(a+b)$ *é racional e está entre a e b.*
2. *Prove que entre dois números racionais existem infinitos números racionais.*
3. *Prove que não existe número racional q cujo quadrado seja igual a p, sendo p primo.*
4. *(Vestibular UFG/2003) Demonstre que* $\sqrt[3]{20+14\sqrt{2}}+\sqrt[3]{20-14\sqrt{2}}$ *é um inteiro múltiplo de 4.*

Os números que são raízes de equações polinomiais com coeficientes inteiros são chamado de números algébricos. Portanto os números irracionais obtidos anteriormente são algébricos. Liouville, em 1851, estabeleceu a existência de números irracionais não algébricos. Tais números são chamados de transcendentes. Exemplos desse números são $2^{\sqrt{2}}$, π, $\log 2$ e $\Sigma_{n=0}^{\infty} 10^{n!}$. O último é conhecido como número de Liouville e a demonstração de que se trata de um número transcendente pode ser encontrada em [2].

Podemos dividir os reais em:

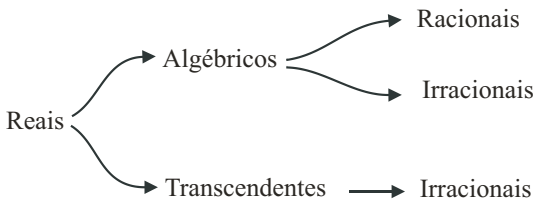


Figura 3:

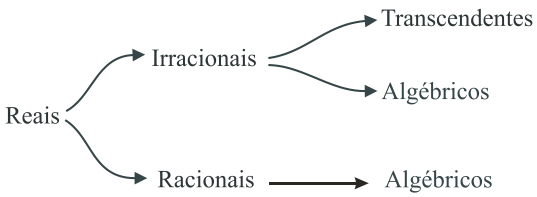


Figura 4:

2.12.2 Representação decimal dos racionais

Outro modo de obtermos exemplos de números não-racionais é observar a representação decimal de um número racional. Provando que a representação decimal de um número racional é finita ou é uma dízima periódica (veja [4]) e admitindo que toda dízima representa um número. Temos uma fábrica de exemplos de números não-racionais. Vejamos alguns;

1) 0,01001000100001...

2) 0,12345678910111213 14...

3) 0,10110111011110...

2.13 Conjuntos Limitados

No conjunto dos números racionais subconjuntos limitados podem não ter máximo e ou mínimo, veja os exemplos.

Exemplo 2.42.

1. $S_1 = \{\frac{1}{n}; n \in \mathbb{N}^*\}$ *não possui mínimo.*
2. $S_2 = \{\frac{(-1)^n}{n+1}n; n \in \mathbb{N}\}$ *não possui máximo nem mínimo.*
3. $S_3 = \{(1-\frac{1}{n})^n; n \in \mathbb{N}^*\}$ *não possui máximo.*
4. $S_4 = \{a_0 = 2, a_n = \frac{1}{2}(a_{n-1} + \frac{3}{a_{n-1}}); n \in \mathbb{N}\}$ *não possui mínimo.*

Definiremos o que vem a ser ínfimo e supremo de um conjunto.

Definição 2.43. *Seja $S \subset \mathbb{Q}$ com $S \neq \emptyset$. Dizemos que λ é uma cota superior de S se $\lambda \geq x, \forall x \in S$ e nesse caso S é limitado superiormente. A menor das cotas superiores, caso exista, é dita supremo do conjunto S.*

Definição 2.44. *Seja $S \subset \mathbb{Q}$ com $S \neq \emptyset$. Dizemos que λ é uma cota inferior de S se $\lambda \leq x, \forall x \in S$ e nesse caso S é limitado inferiormente. A maior das cotas inferiores, caso exista, é dita ínfimo do conjunto S.*

Surge então as seguintes questões. Todo conjunto limitado inferiormente possui ínfimo? Todo conjunto limitado superiormente possui supremo? No conjunto dos números racionais a resposta para tais perguntas é não. Pois para certos conjuntos como S_4 acima o ínfimo é um número que tem o quadrado igual a 3, e já vimos que esse número não é racional. Tal problema é resolvido quando se constrói o conjunto dos números reais, que faremos agora.

2.14 Números Reais

Na construção dos números Reais, seguiremos o processo de Dedekind. A preocupação de Dedekind com o problema dos números irracionais, e por conseqüência com a continuidade, começou em 1858 quando ministrava aulas de cálculo. Até então no conceito de limite usava como guia apenas a geometria, Dedekind achava que tal estudo deveria ser desenvolvido através do uso da aritmética, desejava que fosse rigoroso. O que há na grandeza geométrica contínua que a distingue dos números racionais? Sua preocupação era com a obtenção de uma definição para a "essência da continuidade".

Leibniz achava que a "continuidade"de pontos sobre uma reta era consequência da sua densidade, isto é, do fato que entre dois pontos quaisquer sempre existe um terceiro. Porém os números racionais têm esta propriedade, no entanto não formam um "continuum".

Dedekind buscou inspiração para sua definição de continuidade na reta, melhor exemplo de contínuo para ele. Observou que cada ponto da reta determina uma decomposição da mesma em duas partes de tal natureza que todo ponto de uma delas está a esquerda (precede) de todo o ponto da outra. A correspondência entre decomposição em duas partes com tais propriedades e o ponto de separação levou Dedekind a dar a seguinte definição para números reais:

Definição 2.45. *Sejam A e B subconjuntos não vazios de $\mathbb{Q}$, com $A \cup B = \mathbb{Q}$ e tais que todo elemento de A é menor (precede) que todo elemento de B. Nessas condições o par (A, B) é denominado número real.*

Assim como os números inteiros foram definidos como pares de naturais, os racionais como pares de inteiros, teremos os reais como pares de conjuntos. Vejamos alguns exemplos;

Exercício 23.

1. $A = \{x \in \mathbb{Q}; x \leq 3\}$ *e* $B = \{x \in \mathbb{Q}; x > 3\}$.
2. $A = \{x \in \mathbb{Q}; x \leq \frac{1}{3}\}$ *e* $B = \{x \in \mathbb{Q}; x > \frac{1}{3}\}$
3. $A = \{x \in \mathbb{Q}_+; x^2 < 2\} \cup \mathbb{Q}_-$ *e* $B = \{x \in \mathbb{Q}; x^2 > 2\}$

Os primeiros dois exemplos mostram que temos uma cópia dos racionais contida nos reais, pois cada racional determinar um corte, isto é, um número real. Porém temos corte que não são determinados por racionais, como é o caso do terceiro exemplo. Esses novos números são os irracionais.

2.14.1 Cortes: Propriedades

Após a definição, levada pela intuição de continuidade, faz-se necessário um estudo desse novo conjunto, nos mesmo termos que foram estudados os conjuntos anteriores.

Teorema 2.46. *Em um corte (A, B) não podemos ter, simultaneamente, um maior elemento em A e um menor elemento em B.*

Demonstração. Suponha que isso ocorra. Seja a o maior elemento de A, e b o menor elemento de B. Então, pela definição de corte $a < b$. Nesse caso o número racional $\frac{1}{2}(a+b)$ é maior que qualquer elemento de A e menor que qualquer elemento de B, e $\frac{1}{2}(a+b)$ não pertence a A e nem a B contrariando a definição de corte. Concluindo que o máximo de A e o mínimo de B não podem ocorrer simultaneamente. □

Por outro lado podemos ter máximo ou mínimo em um dos conjuntos. Como, num corte (A, B), o máximo de A, caso exista, é o elemento que colocado em B será seu mínimo. Identificaremos os corte em que apenas esse elemento tenha sido transferido de um conjunto para o outro. Desta forma o corte $A = \{x \in \mathbb{Q}; x \leq 3\}$ e $B = \{x \in \mathbb{Q}; x > 3\}$ determina o mesmo número que o corte $C = \{x \in \mathbb{Q}; x < 3\}$ e $D = \{x \in \mathbb{Q}; x \geq 3\}$. Nesse texto, para evitar delongas com casos particulares, sempre que o elemento de separação de (A, B) for um número racional o incluiremos em A.

Definição 2.47. *Diremos que o número real (A, B) é menor ou igual ao número real (C, D) se, e somente se, $A \subset C$. Denotaremos por $(A, B) \leq (C, D)$*

Exemplo 2.48. *Seja (A, B) dado por $A = \{x \in \mathbb{Q}; x \leq \frac{2}{3}\}$ e $B = \{x \in \mathbb{Q}; x > \frac{2}{3}\}$ e (C, D) dado por $C = \{x \in \mathbb{Q}; x \leq \frac{5}{2}\}$ e $D = \{x \in \mathbb{Q}; x > \frac{5}{2}\}$. Neste, como $A \subset C$, temos que $(A, B) \leq (C, D)$.*

Definiremos a soma e o produto de dois conjuntos da seguinte forma;

$A + B = \{x + y; x \in A \quad e \quad y \in B\}$

$A.B = \{x.y; x \in A \quad e \quad y \in B\}$

$-A = \{-x; x \in A\}$

O objetivo agora é definir as operações no conjunto dos números reais. Iniciaremos pela soma.

Definição 2.49. *Sejam (A, B) e (C, D) números reais, sua soma é o número real $(A + C, B + D)$ que é denotado por $(A, B) + (C, D)$.*

O par $(A + C, B + D)$ é um número real, pois todo elemento de $A + C$ precede todos os elementos de $B + D$. Além disso $A + C$ e $B + D$ são conjuntos não vazios com a propriedade $(A + C) \cap (B + D) = \emptyset$ e $(A + C) \cup (B + D) = \mathbb{Q}$. Prove essas afirmações (Use o fato $A \subset C$ ou $C \subset A$).

Exercício 24.

1. *Mostre que o número real $(\mathbb{Q}_-, \mathbb{Q}_+^*)$ é o elemento neutro da adição.*
2. *Mostre que o número $-(A, B) = (-B, -A)$ é o oposto de (A, B).*
3. *Prove que a adição é comutativa e associativa.*

Diremos que um número real (A, B) é positivo se $(\mathbb{Q}_-, \mathbb{Q}_+^*) < (A, B)$. Será chamado de número negativo se $(A, B) < (\mathbb{Q}_-, \mathbb{Q}_+^*)$.

Definição 2.50. *Dados (A, B) e (C, D) números reais positivos. Seu produto é o número real $((B.D)^c, B.D)$ denotado por $(A, B).(C, D)$.*

Exercício 25.

1. *Defina, a partir do caso anterior, como deve ser o produto de números reais em que pelo menos um não é positivo.*
2. *Mostre que o número real (A, B), dado por $A = \{x \in \mathbb{Q}; x \leq 1\}$ e $B = A^c$ é o elemento neutro da multiplicação. example*
3. *Prove que a multiplicação é comutativa e associativa.*

A principal questão que a formalização dos números reais pretende responder é a de que todo conjunto não vazio e limitado de números reais possui ínfimo e supremo. O teorema a seguir garante esse resultado.

Teorema 2.51. *Todo subconjunto não vazio e limitado de números reais possui supremo e ínfimo.*

Demonstração. Seja $\{(A_i, B_i)\}$, $i \in I$, um conjunto limitado e não vazio de números reais. Então os números reais $(\cup A_i, (\cup A_i)^c)$ e $((\cup B_i)^c, \cup B_i)$ são supremo e ínfimo respectivamente. Inicialmente devemos provar que se trata de números reais. Temos que $\cup A_i \neq \emptyset$, pois é a união de conjuntos não vazios. Sendo o conjunto $\{(A_i, B_i)\}$ limitado, existe (C, D) tal que $(A_i, B_i) \leq (C, D)$ para todo $i \in I$, isso mostra que $\cup A_i \neq \mathbb{Q}$. Além disso a união de $\cup A_i$ com $(\cup A_i)^c$ é o conjunto de todos os racionais. Dado $x \in \cup A_i$ e $y \in (\cup A_i)^c = \cap A_i^c = \cap B_i$. Temos que $x \in A_j$ para algum j e $y \in B_j$, o que mostra que x precede y. Concluímos que $(\cup A_i, (\cup A_i)^c)$ é um corte. É uma cota superior do conjunto $\{(A_i, B_i)\}$ pois $A_n \subset \cup A_i$. E, sendo (C, D) outra cota superior, temos que $A_i \subset C$ para todo $i \in I$, logo $\cup A_i \subset C$, ou $(\cup A_i, (\cup A_i)^c) \leq (C, D)$. Isso mostra que $(\cup A_i, (\cup A_i)^c)$ é o supremo do conjunto. De forma análoga podemos mostrar que $((\cup B_i)^c, \cup B_i)$ é o ínfimo do conjunto. □

O conjunto A^c é o complementar de A em Q.

Esse resultado nos permite provar que se uma seqüencia de números reais é monótona e limitada então converge para um número real. Isso é o que da sentido a qualquer dízima, como aquelas que comentamos quando falamos da representação decimal de um número racional.

Referências

[1] Domingues, Hygino H. *Fundamentos de Aritimética*. Atual, São Paulo, 1991.

[2] Nivem, Ivan. *Números: Racionais e Irracionais*. Coleção Fundamentos da Matemática Elementar, SBM-IMPA.

[3] Pieterzack, Maurício D. *Números Reais*. In: Revista da Olimpíada do Estado de Goiás. no. 1, 2000.

[4] Ávila, Geraldo S. *Análise Matemática para licenciatura*. Edgard Blücher Ltda, 3a. edição,SP, 2006.

[5] Barker, Stepher F. *Filosofia da Matemática*. Tradução de Leonidas Hegenberg e Octanny Silveira da Mota, Zahar, 1964.

[6] Dantzig, Tobias. *Número: A Linguagem da Ciência*. Tradução de Sérgio Goes de Paula. Zahar Editores. Rio de Janeiro. 1970.

[7] Ifrah, Georges. *Os Números: A história de uma grande invenção*. Ed. Globo.

[8] Russell, Bertrand. *Introdução à Filosofia Matemática*. Tradução de Maria L. X. de A. Borges. Rio de Janeiro, Jorge Zahar Editora, 2007.

[9] Silva, Valdir Vilmar. *Números: Construções e Propriedades*. Cegraf- UFG. Goiânia-Go. 2003.

[10] Caraça, Bento Jesus. *Conceitos Fundamentais de Matemática*. Lisboa-Portugal. 1958

MC2 - Alguns Problemas Interessantes em Probabilidade

Fabiano F. T. dos Santos

UFG - Campus Avançado de Jataí

75803-005, Jataí - GO

E-mail: fabianoftds@yahoo.com.br

Pretendo apresentar neste mini-curso alguns problemas envolvendo teoria das probabilidades. Apresentarei problemas que podem ser resolvidos através de técnicas da probabilidade geométrica, como o famoso ***problema da agulha de Buffon***; serão apresentados também, problemas que envolvem o uso de permutações caóticas, como o ***problema do amigo oculto***, por exemplo.

Referências

[1] J. P. Q. Carneiro, O Problema do Amigo Oculto, *Revista do Professor de Matemática*, 28 (1995) 21-26.

[2] C. G. T. A. Moreira , Amigo Oculto, *Revista do Professor de Matemática*, 15 (1989) 37-39.

[3] A. C. O. Morgado et al, "Análise Combinatória e Probabilidade", Coleção Professor de Matemática, 6ª edição, SBM, 2004.

[4] R. R. Paterlini, O Problema do Jogo dos Discos, *Revista do Professor de Matemática*, 48 (2002) 13-20.

[5] J. P. O. Santos et al, "Introdução à Análise Combinatória", 3ª edição, Editora da Unicamp, 2002.

[6] N. Tunala, Determinação de Probabilidades por Métodos Geométricos, *Revista do Professor de Matemática*, 20 (1992) 16-22.

[7] E. Wagner, Probabilidade Geométrica, *Revista do Professor de Matemática*, 34 (1997) 28-35.

MC3 - A Modelagem Matemática como Metodologia de Ensino-Aprendizagem da Matemática na Educação Básica

Crhistiane da Fonseca Souza, Mariane Cardoso

UFG - Campus de Catalão - Departamento de Matemática

75704-020, Catalão - GO

E-mail: crhisfsouza@gmail.com

A sociedade está passando por diversas transformações, desenvolvimento de novas tecnologias e a escola não pode ficar fora destas mudanças. Entretanto, aplicar e acompanhar estas transformações na sala de aula tem sido um desafio para o professor, em especial, para o professor de Matemática. O ensino essencialmente conteudista, distante das aplicações e do contexto social, apesar de extensas críticas recebidas por diversos autores da área, ainda tem presença significativa nas salas de aula. Esse modelo foi e está sendo contestado por propostas que tentam modificar essa situação e relacionar o cotidiano do aluno aos conteúdos abordados em sala.

Neste contexto, a Modelagem Matemática tem sido apresentada como uma tendência em Educação Matemática que sugere a interdisciplinaridade, a resolução de problemas do cotidiano e a contextualização como focos no processo de ensino-aprendizagem. Segundo BARBOSA em [2], a Modelagem vem sendo vista como um dos ambientes de aprendizagem para o ensino de matemática que, de um modo geral, consegue utilizar de idéias ou métodos matemáticos para a compreensão e resolução de situações-problema de diversas áreas. Neste ambiente, o aluno é estimulado a pensar, investigar e compreender fenômenos relacionados ao seu cotidiano. Assim, esta tendência é uma forma de explicitar tais fenômenos por meio da linguagem matemática, ou seja, através da modelagem é possível abstrair a essência matemática de problemas do dia a dia com criatividade e interesse por parte do aluno. Portanto, através da modelagem é possível desenvolver no aluno a capacidade de elaborar estratégias para enfrentar uma situação-problema e, além disso, desenvolver competências no que tange à comunicação, às relações interpessoais, o trabalho em equipe, que muitas vezes são deixadas de lado nas aulas de matemática.

BIEMBENGUT em [3], BURAK em [5] e CALDEIRA em [6] propõem a modelagem como um método de ensino que parte dos interesses dos alunos, buscando com isso o gosto pela aprendizagem, tornando-a prazerosa, significativa e contextualizada. Para [4], "a modelagem matemática pode tornar-se caminho para despertar no aluno interesse por assuntos de matemática". Portanto ao modelar um problema, o aluno deverá usar o conhecimento matemático adquirido, investigar o fenômeno, fazer novas perguntas e tentar respondê-las, estimular sua imaginação e pesquisar referências apropriadas à situação.

A Modelagem Matemática, além de ser vista como um agente facilitador da aprendizagem em Matemática, é uma excelente ferramenta para se trabalhar a interdisciplinaridade das áreas. Além disso, as atividades podem ser direcionadas para proporcionar uma aprendizagem voltada para a cidadania, buscando formar um cidadão crítico, reflexivo e participante da sociedade em que vive.

Temos como objetivo apresentar esta tendência de pesquisa em Educação Matemática neste minicurso, mostrando aos participantes como esta pode ser articulada entre as disciplinas. Além disso, desenvolveremos exemplos que serão representados por modelos matemáticos para o ensino de matemática

da educação básica, buscando temas que promovam o desenvolvimento de competências que qualificam o aluno da educação básica ao exercício da cidadania e contribui para que ele possa superar as dificuldades encontradas ao aprender matemática e tenha, com isso, uma aprendizagem mais significativa.

Referências

[1] R.C. BASSANEZI, "Ensino-aprendizagem com Modelagem Matemática", Contexto, São Paulo, 2004.

[2] J.C. BARBOSA, Modelagem matemática e os futuros professores, em "REUNIÃO ANUAL DA ANPED", 25. Caxambu: ANPED, 2002. 1 CD-ROM.

[3] M.S. BIEMBENGUT, "Modelagem Matemática E Implicações no ensino-aprendizagem", Editora da FURB, Blumenau, 1999.

[4] M.S. BIEMBENGUT, N. HEIN, "Modelagem Matemática no Ensino", Contexto, São Paulo, 2005.

[5] D. BURAK, "Modelagem Matemática: ações e interações no processo de ensino aprendizagem", 329 f. Tese (Doutorado) - Faculdade de Educação, Universidade de Campinas, Campinas, 1992.

[6] A.D. CALDEIRA, Modelagem Matemática e suas implicações na prática docente, em "III Conferência Nacional de Modelagem e Educação Matemática", Piracicaba. Anais do II CNMEM, 2003.

[7] U. D'AMBRÓSIO, A matemática nas escolas, *Educação Matemática em Revista*, ano 9 no 11A, edição especial Campinas, (2002) 29-33.

Anais

[8] W. Gautschi, A survey of Gauss-Christoffel quadrature formulae, em "E.B. Christoffel - The influence of his work in mathematics and physical sciences" (P.L. Butzer e F. Fehér, eds.) pp. 72-147, Birkhäuser Verlag, Basel, 1981.

revista

[9] R. Courant, Variational methods for the solution of problems of equilibrium and vibrations, *Bull. Amer. Math. Soc.*, 49 (1943) 1-23.

MC4 - Matemática Algumas Vezes Aplicada

Luciana Aparecida Elias

UFG - Campus Avançado de Jataí

75803-005, Jataí - GO

E-mail: lucianaeliasmat@gmail.com

Uma pergunta que sempre acompanha um professor de graduação no curso de Matem ática e principalmente em outroscursos que utilizam a Matemática como ferramenta : "Para que serve isto?". Em contrapartida, encontrar respostas criativas sempre foi um momento de descontração em muitos currículos de pesquisadores, professores e/ou estudantes. Para os alunos de Matemática, muitas vezes, são imbuídos pensamentos de que tal pergunta é um paradigma inquebrantável. Muitos estudos ainda são, mas alguns não são e não deixam de ter Matemática e não deixam de ter os seus mistérios e dialéticas próprias.

Este minicurso objetiva obter algumas respostas concretas para tal questão. Através de exemplos, às vezes canônicos, de aplicações divididos em três áreas: ciências agrárias, ciências humanas e ciências exatas, esta última dando enfoque à Física e a própria Matemática esperamos que o participante deste minicurso satisfaça alguns anseios de aplicações de Cálculo (derivada, funções), Álgebra Linear, e alguns ramos da Geometria Euclidiana, utilizando o plano cartesiano e n ão Euclidiana, culminando no avanço da Cosmologia posterior ao entendimento deste tipo de geometria.

MC5 - Análise dos parâmetros de controle em pesquisas de intenção de votos/ Controle Estatístico de Qualidade - Controle on-line de processos: uma abordagem econômica para contagem do número de não-conformidades na amostra via modelagem probabilística

Renata Mendonça Rodrigues

UFRN - PPGMAE / CCET Campus Universitário - Lagoa Nova

CEP 59.072-970, Natal - RGN

E-mail: renata_mat@hotmail.com

(a) É objetivo neste trabalho apresentar uma abordagem geral sobre o conceito de Pesquisas e os procedimentos utilizados para a realização das mesmas bem como uma abordagem sobre o controle estatístico na divulgação dessas pesquisas de modo a facilitar a compreensão dos parâmetros de controle apresentados pelos institutos de pesquisa. Adicionalmente, é apresentada uma análise crítica dos resultados obtidos nas análises dos dados dos parâmetros divulgados por três institutos. A análise desses dados foi feita a partir de algumas pesquisas de intenções de votos para a eleição para prefeito do município de Goiânia em 2004.

(b)O procedimento usual de controle on-line de processo por atributos consiste em inspecionar um item a cada m itens produzidos. A idéia é a de utilizar um sistema de controle baseado no número de não-conformidades do item inspecionado. Através das propriedades de uma cadeia de Markov ergótica, obtém-se uma expressão analítica do custo médio do sistema de controle, que pode ser minimizada por dois parâmetros: o intervalo entre inspeções e o limite superior de controle do gráfico do número de não-conformidades no item inspecionado.

MC6 - Classificação dos Pontos Singulares no Plano

Alysson Tobias Ribeiro da Cunha, Marcos Leandro Mendes Carvalho

UFG - Campus Avançado de Jataí

75803-005, Jataí - GO

E-mail:

3.15 Introdução

As Equações Diferenciais Ordinárias têm sido objeto de estudo em diversas áreas do conhecimento, entre elas a física, com a lei de resfriamento de Newton, e a Lei de Torricelli. Na Biologia temos como aplicação o crescimento populacional e eliminação de drogas. Na Química temos o decaimento radioativo. Na matemática financeira temos os Juros compostos.

Para tal estudo faz-se necessário o conhecimento sistemas de equações diferenciais ordinárias, em particular os pontos singulares destes sistemas, base fundamental para o estudo de campos vetoriais não-lineares.

Neste trabalho classificaremos os pontos singulares no Plano de sistemas de Equações Diferenciais Lineares, para tal, faz-se necessário o conhecimento de Cálculo Diferencial e Integral de uma Variável e Álgebra Linear[1].

3.16 Definições e Notações

A seguir estabeleceremos algumas notações. Ao longo do texto $\dot{x} = \dfrac{dx}{dt}$ denotará a derivada de $x \in \mathbb{R}^n$, em relação ao tempo t. Os vetores de $I\!R^n$ serão escritos na forma de matriz coluna

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Assim temos

$$\dot{x} = \frac{dx}{dt} = \begin{bmatrix} \frac{dx_1}{dt} \\ \frac{dx_2}{dt} \\ \vdots \\ \frac{dx_n}{dt} \end{bmatrix} = \begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \vdots \\ \dot{x_n} \end{bmatrix},$$

e o sistema

$$\begin{cases} \dot{x}_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ \dot{x}_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \qquad\qquad \ldots \\ \dot{x}_n = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{cases}$$

pode ser escrito na forma matricial

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \vdots \\ \dot{x_n} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

[1]Trabalho financiado pelo PROAPI/CAJ/UFG

ou ainda

$$\dot{x} = Ax,$$

onde $x \in \mathbb{R}^n$ e A é a matrix $n \times n$ acima. Suponha que A é uma matriz diagonal, isto é $A = (a_{ij})_{n\times n}$ onde $a_{ij} = 0$, se $i \neq j$. Então por notação

$$A = \text{diag}[a_{11}, ..., a_{nn}].$$

Definição 3.52. *Chamamos de retrato de fase do sistema anterior ao conjunto de todas as suas soluções em $\mathbb{R}^n$.*

Exercício 26. *Considere o sistema*

$$\begin{cases} \dot{x_1} = x_1 \\ \dot{x_2} = -x_2 \end{cases}$$

Este sistema pode ser escrito na forma

$$\dot{x} = Ax,$$

onde

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Note que $A = \text{diag}[1, -1]$. Assim o sistema anterior é um sistema não-acoplado. A solução geral deste sistema é dado por $x_1(t) = c_1e^t$ e $x_2(t) = c_2e^{-t}$. Podemos escrever também como

$$x(t) = \begin{bmatrix} e^t & 0 \\ 0 & e^{-t} \end{bmatrix} c,$$

onde $c = x(0) = (x_1(0), x_2(0))$.

O retratos de fase do deste sistema encontram-se representado na Figura 5.

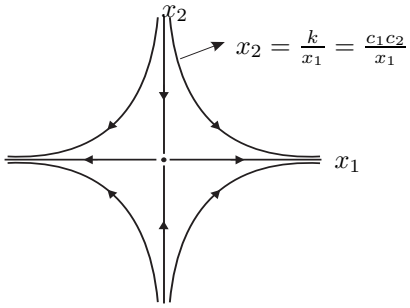


Figura 5: Retrato de Fase no Plano.

Exercício 27. *Um exemplo de sistema linear no espaço é dado por*

$$\begin{cases} \dot{x_1} = x_1 \\ \dot{x_2} = -2x_2 \\ \dot{x_3} = x_3 \end{cases}$$

Sua solução é dada por $x_1(t) = c_1e^t, x_2(t) = c_2e^{-2t}$ e $x_3(t) = c_3e^t$. Note que esta solução pode ser escrita na forma

$$x = \begin{bmatrix} e^t & 0 & 0 \\ 0 & e^{-2t} & 0 \\ 0 & 0 & e^t \end{bmatrix} c,$$

onde $c = x(0) = (x_1(0), x_2(0), x_3(0))$. Na Figura **??** *construímos o retrato de fase do sistema acima*

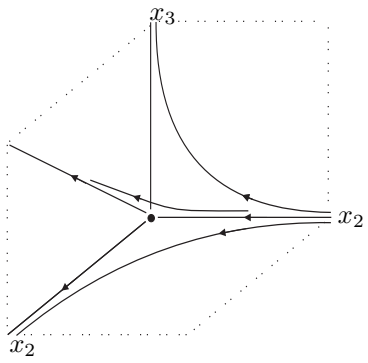


Figura 6: Retrato de Fase no Espaço.

Exercício 28. *Encontre a solução geral para os seguintes sistemas e descreva os seus retratos de fase.*

a) $\begin{cases} \dot{x_1} = -3x_1 \\ \dot{x_2} = x_2 \end{cases}$

b) $\begin{cases} \dot{x_1} = 4x_2 \\ \dot{x_2} = x_1 \end{cases}$

c) $\begin{cases} \dot{x_1} = x_1 \\ \dot{x_2} = x_2 \\ \dot{x_3} = x_3 \end{cases}$

d) $\begin{cases} \dot{x_1} = -\pi x_1 \\ \dot{x_2} = -x_2 \\ \dot{x_3} = x_3 \end{cases}$

Sugestão para o item b): derive uma das equações e transforme o sistema numa equação diferencial linear de segunda ordem, daí resolva pelo método do fator integrante (Veja 2)

Exercício 29. *Determine a solução geral para o sistema linear*

$$\begin{cases} \dot{x_1} = \alpha x_1 \\ \dot{x_2} = x_2. \end{cases}$$

Esboce seu retrato de fase para $\alpha > 0$, $\alpha < 0$ *e* $\alpha = 0$. *Note que quando* $\alpha > 0$ *o sistema tem uma certa estrutura qualitativa e quando* $\alpha < 0$ *tem outra estrutura diferente, dessa forma* $\alpha = 0$, *representa o "divisor de águas"entre dois comportamentos do sistema.*

Exercício 30. *Encontre a solução geral do sistema*

$$\dot{x} = Ax,$$

onde $A = diag[\lambda_1, \lambda_2, ..., \lambda_n]$. *Quais são as condições sobre os autovalores* $\lambda_1, ..., \lambda_n$ *para que* $\lim_{t\to\infty} x(t) = 0$, *para toda solução do sistema?*

3.17 Diagonalização da Matriz A

Utilizando técnicas de diagonalização da matriz A podemos transformar o sistema linear acoplado

$$\dot{x} = Ax,$$

noutro sistema linear não-acoplado.

Teorema 3.53. *Suponha que a matriz $n \times n$ A tenha os autovalores reais e distintos $\lambda_1, ..., \lambda_n$. Então qualquer conjunto de autovetores correspondentes $\{v_1, ..., v_n\}$ forma uma base para $\mathbb{R}^n$, a matriz $P = [v_1, ..., v_n]$ é invertível e*

$$P^{-1}AP = \text{diag}[\lambda_1, ..., \lambda_n].$$

A demonstração deste teorema pode ser encontrada por exemplo em [6] ou [7]. A seguir, vamos reduzir o sistema (1) para um sistema não-acoplado, utilizando o último teorema. Seja P, a matriz do teorema e considere a mudança de coordenadas

$$y = P^{-1}x.$$

Logo

$$\dot{y} = P^{-1}\dot{x} = P^{-1}Ax = P^{-1}APy.$$

Daí pelo teorema anterior temos

$$\dot{y} = \text{diag}[\lambda_1, ..., \lambda_n]y.$$

Este sistema tem a solução

$$y(t) = \text{diag}[e^{\lambda_1 t}, ..., e^{\lambda_n t}]y(0).$$

Como $y(0) = P^{-1}x(0)$, temos

$$x(t) = P\text{diag}[\lambda_1, ..., \lambda_n]P^{-1}x(0).$$

Exercício 31. *A seguir, resolveremos o sistema*

$$\begin{cases} \dot{x_1} = -x_1 \\ \dot{x_2} = x_1 + x_2, \end{cases}$$

diagonalizando a matriz A. Neste caso temos

$$A = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix},$$

sendo que $\lambda_1 = 1$ e $\lambda_2 = -1$ são os autovalores e $v_1 = (0, 1)$, $v_2 = (1, -\frac{1}{2})$, os correspondentes autovetores. Assim

$$P = \begin{bmatrix} 0 & 1 \\ 1 & -1/2 \end{bmatrix} \text{ e } P^{-1} = \begin{bmatrix} 1/2 & 1 \\ 1 & 0 \end{bmatrix}.$$

Temos ainda

$$P^{-1}AP = \begin{bmatrix} 1/2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & -1/2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \text{diag}[\lambda_1, \lambda_2].$$

Portanto, fazendo a mudança de coordenadas $y = P^{-1}x$ temos

$$\dot{y} = \text{diag}[\lambda_1, \lambda_2]y, \quad \therefore \quad y(t) = \text{diag}[e^t, e^{-t}]y(0).$$

Pondo $x(0) = (c_1, c_2)$ obtemos

$$x(t) = P\text{diag}[e^t, e^{-t}]P^{-1}x(0) = \begin{bmatrix} e^{-t} & 0 \\ e^t - \frac{e^{-t}}{2} & e^t \end{bmatrix}x(0).$$

Isto é

$$x_1(t) = c_1e^{-t} \text{ e } x_2(t) = (c_1 + c_2)e^t - \frac{c_1}{2}e^{-t}.$$

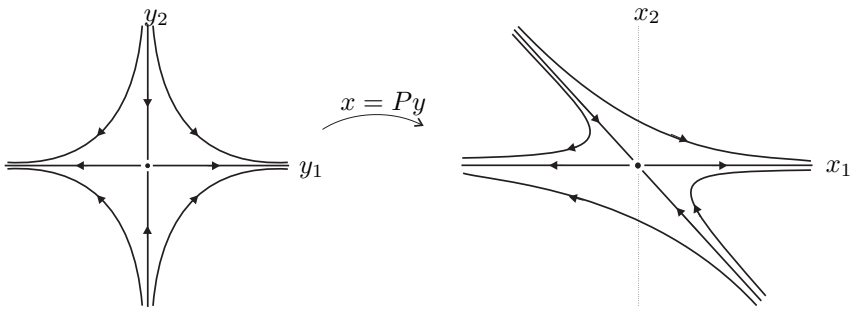


Figura 7: Retrato de Fase pela mudança de coordenadas.

Definição 3.54. *Seja A uma matriz $n \times n$ com k distintos autovalores negativos $\lambda_1, ..., \lambda_k$ e $n-k$ distintos autovalores positivos $\lambda_{k+1}, ..., \lambda_n$. Se $\{v_1, ..., v_n\}$ são os correspondentes autovetores, então os subespaços*

$$E^s = \text{Span}\{v_1, ..., v_n\}$$

$$E^u = \text{Span}\{v_{k+1}, ..., v_n\},$$

são chamados subespaços estável e instável, respectivamente.

Exercício 32. *Resolva o sistema*

$$\begin{cases} \dot{x_1} = 2x_1 + x_2 \\ \dot{x_2} = x_1 + 2x_2 \end{cases}$$

e faça seu retrato de fase nos sistemas x e $y = P^{-1}x$, onde P é a matriz dada pelo teorema anterior e

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Exercício 33. *Seja A uma matriz $n \times n$, com autovalores reais e distintos. Encontre condições necessárias, e suficientes, para que $\lim_{t\to\infty} x(t) = 0$, onde $x(t)$ é solução de $\dot{x} = Ax$.*

3.18 Exponencial de Operadores

Seja $L(\mathbb{R}^n)$ o espaço de todos os operadores lineares $T : \mathbb{R}^n \to \mathbb{R}^n$.

Definição 3.55. *Seja $T \in L(\mathbb{R}^n)$, então a norma de T é definida por*

$$\|T\| = \max_{|x|\leq 1} |T(x)|.$$

Aqui estamos denotando $|x| = \sqrt{x_1^2 + ... + x_n^2}$, se $x \in \mathbb{R}^n$.

Exemplo 3.56. *Sejam $T, S \in \mathbb{R}^n$ então*

a) $\|T\| \geq 0$ *e* $\|T\| = 0 \Leftrightarrow T = 0$.

b) $\|kT\| = |k|\|T\|, \forall\ k \in \mathbb{R}$.

c) $\|T + S\| \leq \|T\| + \|S\|$.

Definição 3.57. *Dizemos que a seqüência de operadores $T_k \in L(\mathbb{R}^n)$ converge para um operador $T \in L(\mathbb{R}^n)$, com $k \to \infty$, se*

$$\lim_{k\to\infty} \|T_k - T\| = 0.$$

Escreveremos $\lim_{k\to\infty} T_k = T$.

Proposição 3.58. *Sejam $T, S \in L(\mathbb{R}^n$ e $x \in \mathbb{R}^n$, então*

a) $|Tx| \leq \|T\||x|$.

b) $\|TS\| \leq \|T\|\|S\|$.

c) $\|T^k\| \leq \|T\|^k$, $\forall\ k = 0, 1, 2, ...$

Prova: a) A desigualdade é verdadeira se $x = 0$. Se $x \neq 0$, defina $u = x/|x|$. Então pela definição de $\|T\|$, obtemos

$$\|T\| \geq |Tu| = \frac{|Tx|}{|x|} \Rightarrow |Tx| \leq \|T\||x|.$$

b) Seja $|x| \leq 1$, então da parte a) temos

$$|T(Sx)| \leq \|T\||Sx| \leq \|T\|\|S\||x| \leq \|T\|\|S\|.$$

Logo

$$\|TS\| = \max_{|x|\leq 1}|TS(x)| \leq \|T\|\|S\|.$$

∎

Um resultato fundamental para a definição de exponencial de um operador é dado pela

Teorema 3.59. *(Teste M de Weierstrass) Seja f_k uma sequência de funções reais com o mesmo domínio D, tal que $|f_k(t)| \leq M_k$, para todo $t \in D$ e $\sum_{k=1}^{\infty} M_k$ é uma série numérica convergente. Então $\sum_{k=1}^{\infty} f_k(t)$, converge absoluta e uniformemente em D.*

Para a demonstração deste teorema veja [5].

Proposição 3.60. *Sejam $T \in L(\mathbb{R}^n)$ e $t_0 > 0$, então a série*

$$\sum_{k=0}^{\infty} \frac{T^k t^k}{k!}$$

converge absolutamente e uniformemente para $|t| \leq t_0$.

Prova: Pelo item c) da proposição anterior temos para $|t| \leq t_0$

$$\left\|\frac{T^k t^k}{k!}\right\| \leq \frac{\|T\|^k|t|^k}{k!} \leq \frac{\|T\|^k t_0^k}{k!}.$$

Como

$$\sum_{k=0}^{\infty} \frac{\|T\|^k t_0^k}{k!} = e^{\|T\|t_0},$$

temos pelo teste M de Weierstrass que

$$\sum_{k=0}^{\infty} \frac{T^k t^k}{k!},$$

converge absolutamente e uniformemente em $|t| \leq t_0$ ∎

Com base na proposição anterior temos o seguinte resultado

Definição 3.61. *Seja $T \in L(\mathbb{R}^n)$, então*

$$e^T = \sum_{k=0}^{\infty} \frac{T^k}{k!}$$

Note que $e^T \in L(\mathbb{R}^n)$ e $\|e^T\| \leq e^{\|T\|}$. Considere o sistema (24), então pondo $Tx = Ax$, a transformação $T \in L(\mathbb{R}^n)$ é dada por uma matriz $n \times n$ com respeito à base canônica de $I\!R^n$ (reciprocamente, todo elemento de $L(\mathbb{R}^n)$ é representado por uma matriz $n \times n$, veja [7]). Assim podemos definir e^{At}

Definição 3.62. *Seja A uma matriz $n \times n$, então*

$$e^{At} = \sum_{k=0}^{\infty} \frac{A^k t^k}{k!}, \ \forall\ t \in I\!R$$

Exercício 34. *Mostre que $\|e^{At}\| \leq e^{\|A\||t|}$, para todo $t \in \mathbb{R}$.*

Exercício 35. *Seja $T \in L(\mathbb{R}^n)$ tal que $\|T\| < 1$. Então $(I - T)$ é inversível e*

$$(I - T)^{-1} = \sum_{n=0}^{\infty} T^n \qquad (\textit{série de Neumann}).$$

Além disso

$$\|(I - T)^{-1}\| \leq (I - \|T\|)^{-1}.$$

Exercício 36. *Calcule, por definição, e^A onde* $A = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$.

Proposição 3.63. *Se P e T são transformações lineares em $\boldsymbol{R}^n$ e $S = PTP^{-1}$, então $e^S = Pe^TP^{-1}$.*

Prova: De fato, segue diretamente da definição de e^S que

$$e^S = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{(PTP^{-1})^k}{k!} = P \lim_{n\to\infty} \sum_{k=0}^{n} \frac{T^k}{k!} P^{-1} = Pe^TP^{-1}.$$

∎

Corolário 3.64. *Se $P^{-1}AP = \operatorname{diag}[\lambda_j]$, então $e^{At} = P \operatorname{diag}[e^{\lambda_j t}]P^{-1}$.*

Prova: De fato, segue da Proposição 3.63 que $e^{P^{-1}AP} = Pe^AP^{-1}$. Por outro lado, $e^{\operatorname{diag}[\lambda_j t]} = \operatorname{diag}[e^{\lambda_j t}]$, donde $e^{At} = P \operatorname{diag}[e^{\lambda_j t}]P^{-1}$.

∎

Exercício 37. *Dada uma transformação linear diagonalizável A, isto é, existe uma transformação linear inversível P tal que $P^{-1}AP = \operatorname{diag}[\lambda_j]$. Mostre que*

$$\det e^A = e^{\mathit{trace}A}.$$

Exercício 38. *Mostre que se v é autovetor da transformação linear A relacionado com autovalor λ, então v também é autovetor de e^A relacionado com o autovalor e^λ.*

Proposição 3.65. *Se S e T são transformações lineares em $\mathbf{R}^n$ tais que $ST = TS$, então $e^{S+T} = e^Se^T$.*

Prova: A saber, temos por hipótese que $ST = TS$, donde

$$(S + T)^n = n! \sum_{j+k=n} \frac{S^jT^k}{j!k!}.$$

Assim,

$$e^{S+T} = \sum_{n=0}^{\infty} \sum_{j+k=n} \frac{S^jT^k}{j!k!} = \sum_{j=0}^{\infty} \frac{S^j}{j!} \sum_{k=0}^{\infty} \frac{T^k}{k!} = e^Se^T.$$

Na penúltima igualdade usamos o fato de que o produto de duas séries absolutamente convergentes é absolutamente convergente.

∎

Exercício 39. *Encontre duas matrizes A e B tais que $e^{A+B} \neq e^A e^B$.*

Se na Proposição 3.65 considerarmos $S = -T$, obtemos:

Corolário 3.66. *Se T é uma transformação linear em $\mathbf{R}^n$, então e^T é inversível e sua inversa é dada por $(e^T)^{-1} = e^{-T}$.*

Corolário 3.67. *Se $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, então $e^A = e^a \begin{bmatrix} \cos b & -\operatorname{sen} b \\ \operatorname{sen} b & \cos b \end{bmatrix}$.*

Prova: Com efeito, se $\lambda = a \pm ib$ segue por indução que

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}^k = \begin{bmatrix} \operatorname{Re}(\lambda^k) & -\operatorname{Im}(\lambda^k) \\ \operatorname{Im}(\lambda^k) & \operatorname{Re}(\lambda^k) \end{bmatrix},$$

onde Re e Im denotam as partes real e imaginária do número complexo λ, respectivamente. Assim,

$$\begin{aligned} e^A &= \sum_{k=0}^{\infty} \begin{bmatrix} \operatorname{Re}(\frac{\lambda^k}{k!}) & -\operatorname{Im}(\frac{\lambda^k}{k!}) \\ \operatorname{Im}(\frac{\lambda^k}{k!}) & \operatorname{Re}(\frac{\lambda^k}{k!}) \end{bmatrix} \\ &= \begin{bmatrix} \operatorname{Re}(e^\lambda) & -\operatorname{Im}(e^\lambda) \\ \operatorname{Im}(e^\lambda) & \operatorname{Re}(e^\lambda) \end{bmatrix} \\ &= e^a \begin{bmatrix} \cos b & -\operatorname{sen} b \\ \operatorname{sen} b & \cos b \end{bmatrix}. \end{aligned}$$

∎

Corolário 3.68. *Se $A = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$, então $e^A = e^a \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$.*

Prova: Inicialmente, observemos que $A = aI + B$, onde $B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$. Observemos também que aI comuta com B. Logo, da Proposição 3.65,

$$e^A = e^{aI} e^B = e^a e^B.$$

Além disso, segue diretamente da definição da exponencial de um matriz que

$$e^B = I + B + \frac{B^2}{2!} + \frac{B^3}{3!} + ... = I + B,$$

pois, $B^2 = B^3 = ... = 0$.

∎

Como no caso real, vale a seguinte fórmula:

Teorema 3.69. ***(Fórmula Alternativa para e^A)*** *Para qualquer transformação linear A em $\mathbb{R}^n$, vale que*

$$e^A = \lim_{k \to \infty} \left(I + \frac{A}{k} \right)^k. \tag{12}$$

Prova: Com efeito, observemos que

$$e^A - \left(I + \frac{A}{k} \right)^k = \sum_{0 \leq j \leq k} \left(\frac{1}{j!} - \frac{C_k^j}{k^j} \right) A^j + \sum_{j > k} \frac{A^j}{j!},$$

observando que

$$\frac{1}{j!} \geq \frac{k(k-1)...(k-j+1)}{m.m...m} \frac{1}{j!}$$

temos que os coeficientes $\left(\frac{1}{j!} - \frac{C_k^j}{k^j}\right) \geq 0$. E para $\|A\| = a$, segue que

$$\left\| e^A - \left(I + \frac{A}{k}\right)^k \right\| \leq \sum_{0 \leq j \leq k} \left(\frac{1}{j!} - \frac{C_k^j}{k^j}\right) a^j + \sum_{j>k} \frac{a^j}{j!} = e^a - \left(I + \frac{a}{k}\right)^k,$$

e como a expressão à direita tende a zero com $m \to \infty$, temos o desejado.

∎

Definição 3.70. *Duas transformações lineares A e B são ditas equivalentes se existe um transformação linear inversível P tal que $A = PBP^{-1}$.*

Exercício 40. *Mostre que a equivalência entre transformações lineares é uma relação de equivalência.*

Lembremos que dada uma matriz A de ordem 2, existe uma matriz inversível P de ordem 2 (cujas colunas são os autovetores generalizados de A) tal que a matriz

$$B = P^{-1}AP,$$

tem uma das seguintes formas

$$B = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}, \; B = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \text{ ou } B = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Segue da definição da exponencial de uma matriz e de suas propriedades que

$$e^{Bt} = \begin{bmatrix} e^{\lambda t} & 0 \\ 0 & e^{\mu t} \end{bmatrix}, \; e^{Bt} = e^{\lambda t} \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \text{ ou } e^{Bt} = e^{at} \begin{bmatrix} \cos bt & -\operatorname{sen} bt \\ \operatorname{sen} bt & \cos bt \end{bmatrix},$$

respectivamente. Logo, da Proposição 3.63

$$e^{At} = Pe^{Bt}P^{-1}.$$

3.19 O Teorema Fundamental para Sistemas Lineares

Seja A uma matriz quadrada de ordem n. E seja $x_0 \in \mathbf{R}^n$, e considere o problema de valor inicial

$$\begin{cases} \dot{x} = Ax \\ x(0) = x_0 \end{cases}. \tag{13}$$

Nesta seção mostraremos que problemas como em (13), tem única solução e é dada por

$$x(t) = e^{At}x_0. \tag{14}$$

Para tal, começaremos mostrando que, como no caso real, a derivada da função exponencial e^{At} é Ae^{At}.

Lema 3.71. *Seja A uma matriz quadrada, então*

$$\frac{d}{dx}e^{At} = Ae^{At}.$$

Prova: Sabemos que A comuta com sigo mesmo, então da Proposição 3.65 que

$$\begin{aligned} \frac{d}{dt}e^{At} &= \lim_{h \to 0} \frac{e^{A(t+h)} - e^{At}}{h} \\ &= \lim_{h \to 0} e^{At} \frac{(e^{Ah} - I)}{h} \\ &= e^{At} \lim_{h \to 0} \lim_{k \to \infty} \left(A + \frac{A^2 h}{2!} + ... + \frac{A^k h^{k-1}}{k!}\right) \\ &= Ae^{At}, \end{aligned}$$

onde a última igualdade é possível dada a convergência uniforme de e^{At} para $|h| \leq 1$, daí a mudança dos limites.

∎

Teorema 3.72. ***(O Teorema Fundamental para Sistemas Lineares)*** *Seja A uma matriz quadrada de ordem n. Então dado $x_0 \in \mathbb{R}^n$, o problema de valor inicial*

$$\begin{cases} \dot{x} = Ax \\ x(0) = x_0 \end{cases}, \tag{15}$$

tem uma única solução dada por

$$x(t) = e^{At}x_0. \tag{16}$$

Prova: Inicialmente, mostraremos que $x(t) = e^{At}x_0$ é solução do Sistema (15). De fato, $x(0) = x_0$ e, como no Lema 3.71

$$x'(t) = \frac{d}{dt}e^{At}x_0 = Ae^{At}x_0 = Ax(t),$$

para todo $t \in \mathbb{R}$. Portanto, $x(t) = e^{At}x_0$ é solução. Para mostrarmos a unicidade, defina

$$y(t) = e^{-At}x(t),$$

onde $x(t)$ é uma solução de (15). Segue do Lema 3.71 e que $x(t)$ é uma solução de (15) que

$$\begin{aligned} \frac{d}{dt}y(t) &= -Ae^{-At}x(t) + e^{-At}\frac{d}{dt}x(t) \\ &= -Ae^{At}x(t) + Ae^{At}x(t) \\ &= 0, \end{aligned}$$

para todo $t \in \mathbb{R}$ e sabendo que e^{-At} e A comutam. Logo, $y(t)$ é constante, e como $y(0) = x_0$, temos que $y(t) = x_0$. Portanto, $x(t) = e^{At}y(t) = e^{At}x_0$, como queríamos demonstrar.

∎

Exercício 41. *Resolva o problema de valor inicial*

$$\begin{cases} \dot{x} = Ax \\ x(0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{cases}, \tag{17}$$

onde $A = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}$.

Solução: Inicialmente, observemos que os autovalores de A são $\lambda_1 = 2$ e $\lambda_1 = 4$ com autovetores associados $v_1 = (1, -1)$ e $v_2 = (1, 1)$, respectivamente. Daí, temos que

$$B = \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} = P^{-1}AP,$$

onde

$$P = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \text{ e } P^{-1} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

Segue da Corolário 3.64 e do *Teorema Fundamental para Sistema Lineares* que

$$x(t) = P\,\mathrm{diag}\left[e^{2t}, e^{4t}\right]P^{-1}x_0 = \frac{1}{2}(e^{2t} + e^{4t}, e^{4t} - e^{2t})^T.$$

∎

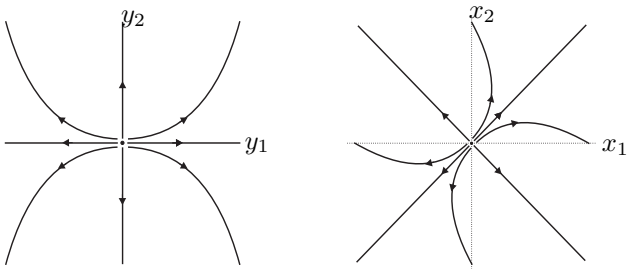


Figura 8: Retratos de fase dos campos vetoriais Y e X.

Exercício 42. *Seja A uma matriz de ordem n e denote por $\mathcal{S} \in \mathcal{F}(R, \mathbb{R}^n)$ o espaço de todas as soluções da equação vetorial $\dot{x} = Ax$. Defina $T : \mathcal{S} \to I\!R^n$ por $T(x) = x(0)$ e, usando a linearidade da equação e o teorema fundamental para sistemas lineares, mostre que T é uma transformação linear, sobrejetora e injetora, respectivamente, ou seja, um isomorfismo linear. Conclua que* $\dim\mathcal{S} = n$.

Exercício 43. *Sejam A uma matriz quadrada, $v_1, v_2, ..., v_n$ uma base de $I\!R^n$ e $x_1, x_2, ..., x_n : I\!R \to I\!R^n$ as soluções de $\dot{x} = Ax$ tais que $x_i(0) = v_i$, $1 \leq i \leq n$. Mostre que $x_1, x_2, ..., x_n$ são linearmente independentes no espaço vetorial das funções e que qualquer solução de $\dot{x} = Ax$ é uma combinação linear de $x_1, x_2, ..., x_n$.*

3.20 Classificação dos pontos Singulares no Plano

Nesta seção discutiremos sobre os vários retratos de fase dos sistemas lineares da forma

$$\dot{x} = Ax, \tag{18}$$

onde A é uma matriz de ordem 2 e $x \in I\!R^n$. Para tal, descreveremos os retratos de fase dos sistemas lineares

$$\dot{y} = By, \tag{19}$$

onde $B = P^{-1}AP$ tem uma das formas dadas no final da seção anterior. Discutiremos os seguintes casos

Caso I $B = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$, onde $\lambda < 0 < \mu$.

Neste caso, a origem é referida como uma sela. Se o Sistema 19 tiver condição inicial $y(0) = (l_1, l_2) \in I\!R^2$, este tem solução

$$y(t) = (l_1 e^{\lambda t}, l_2 e^{\mu t}).$$

Se $l_2 = 0$, solução tende ao infinito quando $t \to -\infty$ e a 0 quando $t \to \infty$. Se $l_1 = 0$ a solução tende a 0 quando $t \to -\infty$ e ao infinito quando $t \to \infty$. Se $l_1 l_2 \neq 0$ a solução tem um comportamento que combina o comportamento dos dois eixos em que uma coordenada tende ao infinito enquanto a outra tende a zero. Por exemplo, se $\lambda = -\mu$ temos que $x_1 x_2 = k$, de modo que a solução descreve uma hipérbole. O comportamento desses campos pode ser visto na Figura 9.

Caso II $B = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$, onde $\lambda \leq \mu < 0$, ou $B = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$, onde $\lambda < 0$.

Neste caso, a origem é dita nó. Se $B = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$ a solução do Sistema 19 provida das condições iniciais $y_0 = (l_1, l_2)$, como no caso anterior, é

$$y(t) = (l_1 e^{\lambda t}, l_2 e^{\mu t}).$$

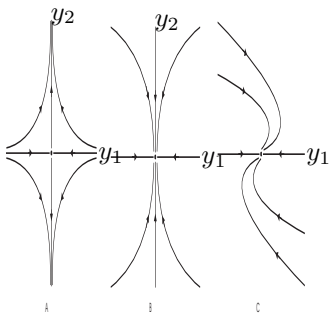


Figura 9: Sela na origem.

Com análise análoga ao caso acima, se $l_1 = 0$ as soluções tendem a zero quando $t \to +\infty$ e tendem ao infinito quando $t \to -\infty$, o comportamento é análogo se considerarmos $l_2 = 0$. Se $l_1 l_2 \neq 0$ as soluções também tendem a zero quando $t \to +\infty$ e tendem ao infinito quando $t \to -\infty$. Se $\lambda = \mu$ o retrato de fase é perfeitamente radial. Porém, se $\lambda < \mu$ as soluções satisfazem a equação $x_1 = kx_2^{\lambda/\mu}$ e $1 < \lambda/\mu$.
Por fim, se $B = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$, onde $\lambda < 0$, o Sistema 19 provido das condições iniciais $y_0 = (l_1, l_2)$ tem solução

$$y(t) = (l_1 e^{\lambda t}, [tl_1 + l_2]e^{\lambda t})$$

e, via *Regra de L'hospital*, os limites quando $t \to \pm\infty$ são idênticos aos limites das soluções da primeira parte deste caso e as curvas soluções não triviais são assintoticamente tangentes à mesma invariante horizontal quando $t \to +\infty$. A discussão do caso caso $0 < \mu \leq \lambda$ é análoga e fica a cargo do leitor e os retratos de fase são ilustrados na Figura 11.

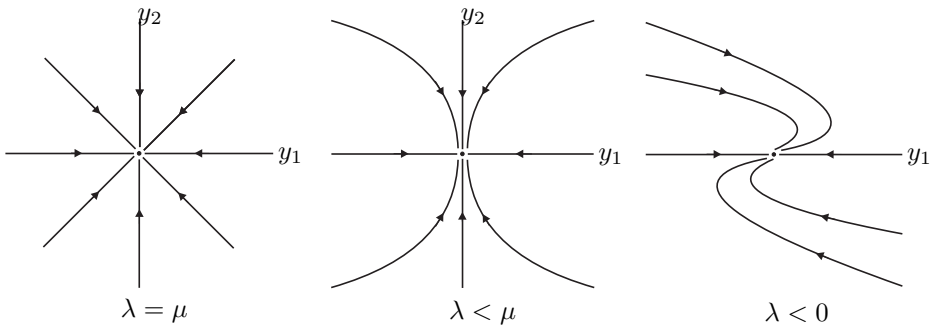


Figura 10: Nó estável na origem.

Para determinar os retratos de fase dos demais casos, discutiremos antes sobre coordenadas polares. Para tal, derivando implicitamente as equações $r^2 = x_1^2 + x_2^2$ e $\theta = \text{tg}^{-1}\frac{x_2}{x_1}$ com respeito a t, obtemos

$$\dot{r} = \frac{x_1\dot{x}_1 + x_2\dot{x}_2}{r} \text{ e } \dot{\theta} = \frac{x_1\dot{x}_2 - x_2\dot{x}_1}{r^2}, \tag{20}$$

para todo $r \neq 0$. Se considerarmos, em particular, o Sistema 19 onde $B = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, obtemos

$$\dot{r} = ar \text{ e } \dot{\theta} = b. \tag{21}$$

Este tem uma única solução se provido das condições iniciais

$$r(0) = r_0 \text{ e } \theta(0) = \theta_0. \tag{22}$$

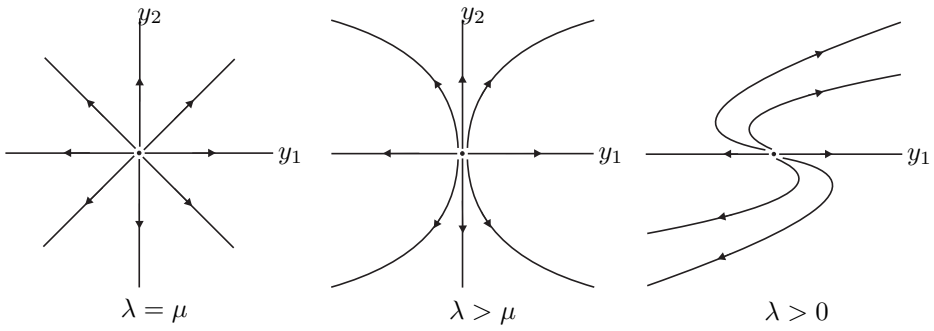


Figura 11: Nó instável na origem.

Caso III $B = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, onde $a < 0$.

Neste caso, B tem uma par de autovalores complexos com parte real não nula $\lambda = a \pm ib$ e a origem é dita *foco estável*. Pelas Equações Polares (21), as trajetórias se aproximam da origem a media que t aumenta, haja vista que r decresce (pois $\dot{r} = ar < 0$). Essas trajetórias se aproximam espiralando (pois $\dot{\theta} = b$), no sentido horário se $b < 0$ e no sentido anti-horário $b > 0$, como pode ser visto na Figura 12.

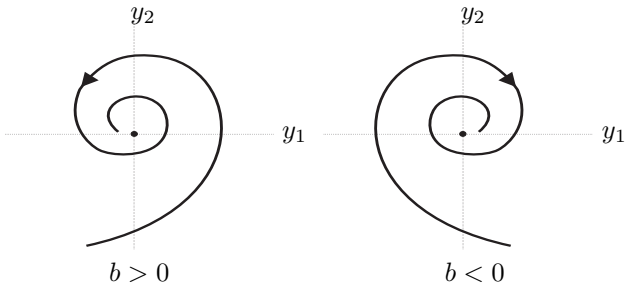


Figura 12: Foco Estável na origem.

Caso IV $B = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, onde $a > 0$.

Neste caso, B tem uma par de autovalores complexos com parte real não nula $\lambda = a \pm ib$ e a origem é dita *foco instável*. Pelas Equações Polares (21), as trajetórias se afastam da origem a media que t aumenta, haja vista que r cresce (pois $\dot{r} = ar > 0$). Essas trajetórias se afastam espiralando (pois $\dot{\theta} = b$), no sentido horário se $b < 0$ e no sentido anti-horário $b > 0$, como pode ser visto na Figura 13.

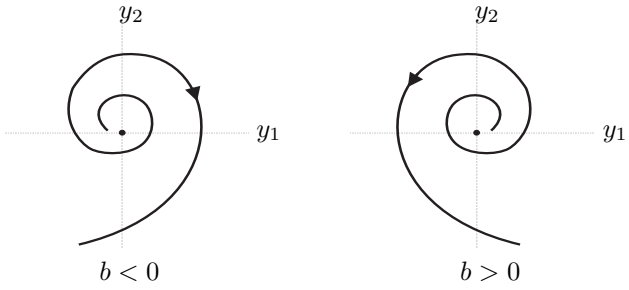


Figura 13: Foco Instável na origem.

Caso V $B = \begin{bmatrix} 0 & -b \\ b & 0 \end{bmatrix}$.

Neste caso, B tem auto-valores complexos $\lambda = \pm ib$ e a origem é dita *centro*. Note que as trajetórias são todas periódicas, haja vista que $\dot{r} = 0$, rodando no sentido no sentido anti-horário se $b > 0$ e no sentido horário se $b < 0$, como pode ser visto no retrato de fase a seguir.

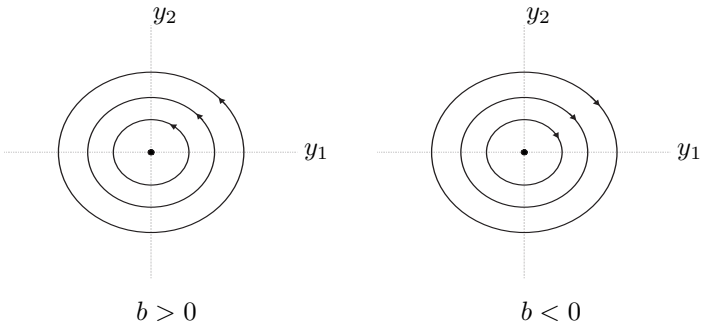


Figura 14: Centro na origem.

Definição 3.73. *O sistema linear 18 é dito ter uma sela na origem se a matriz A for equivalente a matriz B do Caso I, um nó se a matriz A for equivalente a matriz B do Caso II, um foco se a matriz A for equivalente a matriz B dos Casos III e IV. E é dito ser um centro se a matriz A for equivalente a matriz B do Casos V.*

Teorema 3.74. *Seja $\delta = \det A$ e $\tau = traceA$ e considere o sistema linear*

$$\dot{x} = Ax. \tag{23}$$

1. *Se $\delta < 0$, então (23) tem uma sela na origem.*
2. *Se $\delta > 0$ e $\tau^2 - 4\delta \geq 0$, então (23) tem um nó na origem. Esse é estável se $\tau < 0$ e instável se $\tau > 0$.*
3. *Se $\delta > 0$ e $\tau^2 - 4\delta < 0$, então (23) tem um foco na origem. Esse é estável se $\tau < 0$ e instável se $\tau > 0$.*
4. *Se $\delta > 0$ e $\tau = 0$, então (23) tem um centro na origem.*

Prova: Notemos que os autovalores da matriz A são dados pela equação

$$\begin{vmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{vmatrix} = 0,$$

implicando que $\lambda^2 - (a_{11} + a_{22})\lambda + (a_{11}a_{22} - a_{12}a_{21}) = \lambda^2 - \tau\lambda + \delta = 0$, donde

$$\lambda = \frac{\tau \pm \sqrt{\tau^2 - 4\delta}}{2}.$$

Assim,

1. Se $\delta < 0$, segue que $\tau^2 - 4\delta > 0$ e portanto, a transformação linear A tem dois autovalores reais de sinais opostos;
2. Se $\delta > 0$ e $\tau^2 - 4\delta < 0$, então a transformação linear A tem dois autovalores reais com o mesmo sinal de τ;

3. Se $\delta > 0$, $\tau^2 - 4\delta < 0$ e $\tau \neq 0$, então a transformação linear A possui dois autovalores conjugados $\lambda = a \pm ib$ e A é equivalente a matriz B dos Casos III e IV, onde $a = \tau/2$;

4. Se $\delta > 0$ e $\tau = 0$, então a transformação linear A possui dois autovalores complexos imaginários puros conjugados $\lambda = \pm ia$.

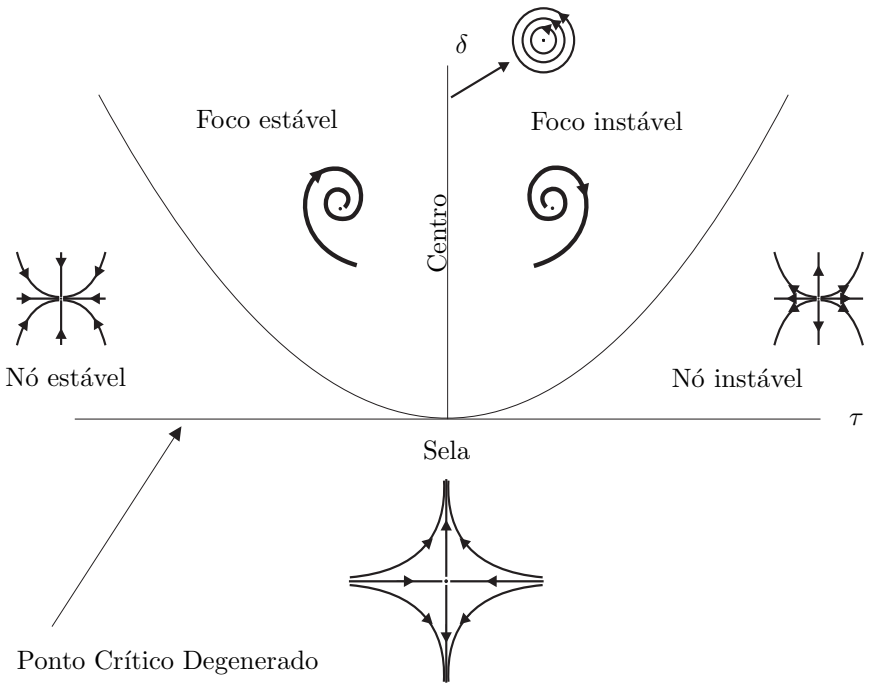


Figura 15: Diagrama de Classificação dos Pontos Críticos no Plano.

Referências

[1] Perko, L., *Differential Equations and Dynamical Systems*. Springer-Verlag, New york, 1991.

[2] Arnold, V.I.,*Equações Diferenciais Ordinárias*. Ed. Mir Moscovo,1985.

[3] Doering, C.I., Lopes, A.O., *Equações Diferenciais Ordinárias*.IMPA, Rio de Janeiro, 2005.

[4] Sotomayor J., *Lições de Equações Diferenciais Ordinárias*. IMPA, Rio de Janeiro, 1979.

[5] Ávila, G., *Introdução à Análise Matemática*. 2° Ed., Ed. Edgard Blucher, São Paulo, 1999.

[6] Lowental, F. *Linear Algebra with Linear Differential Equations*, John Wiley and Sons, New York, 1975.

[7] Lima, E.L., *Álgebra Linear*. 3ªEd, IMPA, Rio de Janeiro, 1998.

[8] Edwards, J. C. H., Penney, D.E. *Equações Diferenciais Elementares, com problemas de contorno*, 3ªEd, Prentice-Hall do Brasil, Rio de Janeiro, 1995.

.

Estas notas são dedicadas a todos aqueles (alunos, docentes, técnicos...) que tive o prazer de conviver durante os 10 anos que trabalhei no IME/UFG. E também à minha filha Bruna Ávila Rodrigues, minha fonte de vida.

MC7 - Teoria local das curvas planas

Luciana Maria Dias de Ávila Rodrigues

UnB - Departamento de Matemática

70910-900, Brasília - DF

E-mail: luavila@mat.unb.br

4.21 Introdução

Neste mini-curso, abordamos o estudo local da teoria das curvas planas. Escolhemos trabalhar com curvas planas pois muitos resultados podem ser apresentados de forma elementar. Elementar no sentido de que os pré-requisitos necessários para o entendimento do mini-curso são os cursos de Cálculo 1 e Geometria Analítica. Por teoria local, entendemos como sendo o estudo do comportamento da curva em uma vizinhança de um de seus pontos. Procuramos ilustrar os conceitos apresentados na teoria por meio de exemplos. Uma ótima referência para um estudo mais aprofundado deste assunto é o livro "Introdução às curvas planas"de Hilário e Walcy, ver [2].

Na seção 2 definimos uma curva parametrizada diferenciável do plano como sendo uma aplicação $\alpha : I \to R^2$ tal que $\forall t \in I$ associa $\alpha(t) = (x(t), y(t))$ onde as funções $x, y : I \to R$ são funções diferenciáveis. Na seção 3 introduzimos o conceito de curva regular. Na seção 4 mostramos que uma curva α está parametrizada pelo comprimento de arco se, e somente se, $|\alpha^{'}(t)| = 1, \forall t \in I$. Mostramos, também, que toda curva regular pode ser reparametrizada pelo comprimento de arco. Na seção 5 deduzimos as chamadas Fórmulas de Frenet. Consideramos curvas parametrizadas pelo comprimento de arco $\alpha(s) = (x(s), y(s))$, onde s é chamado o parâmetro comprimento de arco. O vetor $t(s) = (x^{'}(s), y^{'}(s))$ é chamado vetor tangente à curva α em $\alpha(s)$. O vetor $n(s)$, tal que $\{t(s), n(s)\}$ forma uma base para R^2, é chamado o vetor normal à curva. A partir daí, definimos a curvatura da curva e as Fórmulas de Frenet. Observamos que o sinal da curvatura depende da orientação da curva e damos uma interpretação geométrica para a curvatura na seção 6. Além disso, na seção 7, exploramos o conceito de evoluta e involuta de uma curva e consideramos alguns exemplos. Terminamos, na seção 8, com o Teorema Fundamental das Curvas Planas, que mostra que a curvatura determina uma curva plana a menos de sua posição no plano.

Observamos que todo este estudo, feito para curvas planas, pode ser feito para curvas no espaço R^3. O leitor interessado neste assunto poderá consultar [12] e [5].

Gostaríamos de agradecer a comissão organizadora da XXIII Semana do IME que nos possibilitou lecionar este mini-curso. Aproveitando a ocasião, gostaria de deixar registrado, os meus sinceros agradecimentos a todo o corpo discente, corpo docente e técnicos administrativos do IME/UFG, pelo doce convívio durante os 10 anos que trabalhamos juntos neste Instituto. Foram anos de muita aprendizagem (tanto de matemática quanto de vida...) que ficarão para sempre na minha memória... A vocês meu forte abraço de agradecimento e de muitas saudades...

4.22 Curvas parametrizadas

Nesta seção vamos estudar localmente uma curva α no plano, isto é, fixado t_0, estudaremos como a curva $\alpha(t)$ se comporta para valores de t próximos de t_0.

Definição 4.75. *Uma curva parametrizada diferenciável do plano é uma aplicação $\alpha : I \to R^2$ tal que $\forall t \in I$ associa $\alpha(t) = (x(t), y(t))$ onde as funções $x, y : I \to R$ são funções diferenciáveis de classe C^∞. A variável $t \in I$ é dita parâmetro da curva e o subconjunto de R^2 dos pontos $\alpha(t), t \in I$ é chamado o traço da curva.*

Vejamos alguns exemplos.

Exemplo 4.76. (Curva constante)
A aplicação $\alpha : R \to R^2$ dada por $\alpha(t) = (a, b)$ é uma curva parametrizada diferenciável cujo traço se reduz ao ponto (a, b).

Exemplo 4.77. (Reta)
A aplicação $\alpha : R \to R^2$ dada por $\alpha(t) = (x_0 + at, y_0 + bt)$ onde $a^2 + b^2 \neq 0$ é uma curva parametrizada diferenciável cujo traço é uma linha reta passando pelo ponto (x_0, y_0) e paralela ao vetor de coordenadas (a, b).

Exemplo 4.78. (Circunferência)
A aplicação $\alpha : R \to R^2$ dada por $\alpha(t) = (\cos t, \text{ sen } t)$ é uma curva parametrizada diferenciável cujo traço é uma circunferência de centro na origem e raio igual a 1.

Exemplo 4.79. A aplicação $\alpha : R \to R^2$ dada por $\alpha(t) = (\cos t(2\cos t - 1), \text{ sen } t(2\cos t - 1))$ é uma curva parametrizada diferenciável cujo traço é um cardióide.

Exemplo 4.80. A aplicação $\alpha : R \to R^2$ dada por $\alpha(t) = (t, |t|)$ não é uma curva parametrizada diferenciável, já que $|t|$ não é diferenciável em $t = 0$. Porém a restrição de α, a qualquer intervalo que não contém o ponto $t = 0$, é uma curva parametrizada diferenciável.

Duas curvas parametrizadas podem ter o mesmo traço.

Exemplo 4.81. *Considere $\alpha(t) = (t, 2t), t \in R$ e $\beta(t) = (2r + 1, 4r + 2), r \in R$. Estas curvas têm o mesmo traço que é uma reta passando pela origem na direção do vetor $(1, 2)$.*

4.23 Curva Regular

Para definirmos curva regular, precisamos definir o que é seu vetor tangente em cada ponto.

Definição 4.82. *Seja $\alpha : I \subset R \to R^2$ uma curva parametrizada diferenciável, que para cada $t \in I$ associa $\alpha(t) = (x(t), y(t))$. O vetor*

$$\alpha'(t) = (x'(t), y'(t))$$

é chamado o vetor tangente a α em t.

A seguir vamos definir reta tangente.

Definição 4.83. *Seja $\alpha : I \to R^2$ uma curva regular. A reta tangente a α em $t_0 \in I$ é a reta que passa por $\alpha(t_0)$ na direção de $\alpha'(t_0)$, isto é dada pela função $g(r) = \alpha(t_0) + r\alpha'(t_0), r \in R$.*

Exemplo 4.84. Considere $\alpha : R \to R^2$ dada por $\alpha(t) = (\cos t(2\cos t - 1), \text{ sen } t(2\cos t - 1))$ uma curva parametrizada diferenciável. O vetor tangente a α em t é igual a

$$\alpha'(t) = (\text{ sen } t - 2 \text{ sen } 2t, 2\cos 2t - \cos t).$$

Para o desenvolvimento da teoria local das curvas é necessário que exista reta tangente à curva α para cada valor do parâmetro t. Para isto, é suficiente que o vetor tangente a α não seja nulo para todo t. Portanto restringiremos o nosso estudo apenas às curvas que satisfazem esta condição. Estas curvas são definidas a seguir.

Definição 4.85. *Uma curva parametrizada diferenciável $\alpha : I \to R^2$ é dita regular se $\forall t \in I$, $\alpha^{'}(t) \neq 0$.*

As curvas dos exemplos citados anteriormente são exemplos de curvas regulares. Intuitivamente o traço de uma curva regular é suave, sem bicos, exceto por possíveis pontos de auto-interseção. Localmente, porém, α não tem auto-interseção.

Exemplo 4.86. Um exemplo interessante de uma curva parametrizada diferenciável regular, é dado por $\alpha : I \to R^2$ definida por $\alpha(t) = (t, f(t))$, onde $f : I \to R$ é uma função diferenciável. O traço de α é igual ao gráfico de f. Como $\alpha^{'}(t) = (1, f^{'}(t)) \neq (0, 0), \forall t \in I$, α é uma curva regular. Pode-se mostrar que toda curva regular é dessa forma. Ver [2].

4.24 Reparametrização, Comprimento de arco

Vamos descrever a seguir, como obter várias curvas regulares tendo o mesmo traço.

Definição 4.87. *Sejam I e J intervalos abertos de R, $\alpha : I \to R^2$ uma curva regular e $h : J \to I$ uma função diferenciável (C^∞), cuja derivada de primeira ordem é não nula em todos os pontos de J e tal que $h(J) = I$. Podemos então considerar uma nova curva $\beta : J \to R^2$, definida por*

$$\beta(t) = (\alpha o h)(t) = \alpha(h(t)).$$

A curva β é uma curva regular, que tem o mesmo traço que α, chamada a reparametrização de α por h. A função h é dita mudança de parâmetro.

Vamos considerar apenas reparametrizações onde a função mudança de parâmetro é estritamente crescente ou descrescente. Neste caso $h^{'}(t) \neq 0$ e, portanto se α é uma curva regular em I, sua reparametrização $\beta = \alpha o h$ também será curva regular em J.

Definição 4.88. *A orientação de uma curva regular plana α é o sentido de percurso do traço de α.*

Se h é estritamente crescente, dizemos que a reparametrização $\beta = \alpha o h$ é positiva, ou que preserva a orientação de α. No caso em que h é estritamente decrescente, a reparametrização é dita negativa, ou que reverte a orientação de α.

Exemplo 4.89. Consideremos a circunferência de raio a dada por

$$\alpha(t) = (a\cos t, asent), t \in [0, 2\pi].$$

Seja $h(s) = \dfrac{s}{a}, s \in [0, 2\pi]$. A reparametrização da curva α por h é a curva

$$\beta(s) = \alpha o h(s) = (a\cos\frac{s}{a}, asen\frac{s}{a}).$$

Neste caso as curvas α e β têm a mesma orientação.

Exemplo 4.90. A curva regular

$$\beta(r) = (-2r + 1, -4r + 2), r \in R,$$

é uma reparametrização da curva

$$\alpha(t) = (t, 2t), t \in R.$$

Basta considerar a mudança de parâmetro $h(r) = -2r + 1, r \in R$. Neste caso as curvas α e β têm orientação opostas.

A seguir vamos definir comprimento de arco para uma curva regular.

Definição 4.91. *Seja $\alpha : I \to R^2$ uma curva regular e fixemos t_0 e t_1 pontos do intervalo I. A aplicação*

$$s(t) = \int_{t_0}^{t_1} |\alpha^{'}(t)|dt$$

é denominada a função comprimento de arco da curva α a partir de t_0.

Esta função é diferenciável de classe C^{∞}, pois α é uma curva regular.

Definição 4.92. *Uma curva regular $\alpha : I \to R^2$ é dita uma parametrização pelo comprimento de arco, se para cada $t_0, t_1 \in I$, $t_0 \leq t_1$, o comprimento de arco da curva α de t_0 a t_1 é igual a $t_1 - t_0$. Isto é*

$$\int_{t_0}^{t_1} |\alpha^{'}(t)|dt = t_1 - t_0.$$

Proposição 4.93. *Uma curva $\alpha : I \to R^2$ está parametrizada pelo comprimento de arco, se e somente se, $\forall t \in I, |\alpha^{'}(t)| = 1$.*

Demonstração: Suponhamos α parametrizada pelo comprimento de arco e fixemos $t_0 \in I$. Consideremos a função $s : I \to R$ que para cada $t \in I$ associa $s(t) = \int_{t_0}^{t_1} |\alpha^{'}(t)|dt$. Se $t_0 \leq t$ então por hipótese $\int_{t_0}^{t} |\alpha^{'}(t)|dt = t - t_0$; se $t \leq t_0$ então $-s(t) = \int_{t}^{t_0} |\alpha^{'}(t)|dt = t_0 - t$. Portanto, para todo $t \in I$, $s(t) = t - t_0$, donde $s^{'}(t) = 1$. Como $s^{'}(t) = |\alpha^{'}(t)|$, concluímos que $|\alpha^{'}(t)| = 1, \forall t \in I$. A recípropositionca é imediata. •

Exemplo 4.94. A aplicação

$$\alpha(t) = (a\cos t, asent), t \in R,$$

onde $a \neq 0$, é uma curva regular parametrizada pelo comprimento de arco, já que $|\alpha^{'}(t)| = 1, \forall t \in R$.

Vejamos que, mesmo que o intervalo de definição de uma curva tenha comprimento infinito, seu comprimento pode ser finito.

Exemplo 4.95. A espiral $\alpha(t) = (e^{-t}\cos t, e^{-t}\text{sen}t)$, definida em R é tal que

$$s(t) = \int_{0}^{t} |\alpha^{'}(t)|dt = \sqrt{2}(1 - e^{-t}).$$

Em particular, $s(\alpha_{|[0,+\infty]}) = lim_{t\to\infty} s(t) = \sqrt{2}$, e $s(\alpha_{|[0,-\infty]})$ é infinito.

O próximo resultado mostra que toda curva regular admite uma reparametrização pelo comprimento de arco.

Proposição 4.96. *Seja $\alpha : I \to R^2$ uma curva regular e $s : I \to s(I) \subset R$ a função comprimento de arco de α a partir de t_0. Então existe a função inversa h de s, definida no intervalo aberto $J = s(I)$ e $\beta = \alpha oh$ é uma reparametrização de α, onde β está parametrizada pelo comprimento de arco.*

Demonstração: Se α é uma curva regular, então

$$s^{'}(t) = |\alpha^{'}(t)| > 0,$$

isto é, s é uma função estritamente crescente. Segue-se que existe a função inversa de s, $h : J \to I$. Como $\forall t \in I, h(s(t)) = t$, temos que $\frac{dh}{ds}\frac{ds}{dt} = 1$, portanto

$$\frac{dh}{ds} = \frac{1}{s'(t)} = \frac{1}{|\alpha'(t)|} > 0.$$

Concluímos que $\beta(s) = \alpha oh(s), s \in J$, é uma reparametrização de α e $|\frac{d\beta}{ds}| = |\frac{d\alpha}{dt}\frac{dh}{ds}| = |\frac{\alpha^{'}(t)}{|\alpha'(t)|}| = 1$. Portanto pela proposição 1, β está parametrizada pelo comprimento de arco. •

Definição 4.97. *A aplicação β da proposição acima é chamada uma reparametrização de α pelo comprimento de arco.*

Observamos que esta parametrização não é única, pois depende da função comprimento de arco, que por sua vez depende de t_0 fixado.

Exemplo 4.98. Consideremos $\alpha(t) = (at+c, bt+d), t \in R$ e $a^2+b^2 \neq 0$. Seja $s(t)$ a função comprimento de arco de α a partir de $t_0 = 0$, isto é,

$$s(t) = \int_0^t \sqrt{a^2+b^2}dt = \sqrt{a^2+b^2}t.$$

A função inversa se s é dada por $h(s) = \frac{s}{\sqrt{a^2+b^2}}, s \in R$. Portanto $\beta = \alpha oh$, que a cada s associa

$$\beta(s) = (a\frac{s}{\sqrt{a^2+b^2}} + c, b\frac{s}{\sqrt{a^2+b^2}} + d),$$

é uma reparametrização de α pelo comprimento de arco.

Exemplo 4.99. Consideremos a espiral logarítimica $\alpha(t) = (e^t \cos t, e^t \text{sen}t), t \in R$. Temos que $|\alpha^{'}(t)| = \sqrt{2}e^t$ e portanto a função comprimento de arco de α, a partir de $t_0 = 0$, é $s(t) = \sqrt{2}e^t - \sqrt{2}$. A função inversa é dada por $h(s) = \log(\frac{s}{\sqrt{2}} + 1)$. Portanto,

$$\beta(s) = ((\frac{s}{\sqrt{2}} + 1)\cos(\log(\frac{s}{\sqrt{2}} + 1)), (\frac{s}{\sqrt{2}} + 1)sen(\log(\frac{s}{\sqrt{2}} + 1)))$$

é uma reparametrização de α pelo comprimento de arco.

4.25 Fórmulas de Frenet

Vamos considerar nesta seção curvas $\alpha : I \to R^2$ parametrizadas pelo comprimento de arco,

$$\alpha(s) = (x(s), y(s)), s \in I.$$

Para cada $s \in I$, $\alpha^{'}(s)$ é um vetor unitário, que denotamos por $t(s)$, isto é,

$$t(s) = \alpha^{'}(s) = (x^{'}(s), y^{'}(s)).$$

Definição 4.100. *O vetor $t(s)$ é chamado o vetor tangente à curva α em $\alpha(s)$.*

Seja $n(s)$ um vetor unitário ortogonal a $t(s)$, tal que a base ortonormal de R^2 formada por $t(s)$ e $n(s)$ têm a mesma orientação que a base $e_1 = (1,0)$, $e_2 = (0,1)$ de R^2, isto é,

$$n(s) = (-y^{'}(s), x^{'}(s)).$$

Definição 4.101. *O conjunto de vetores $t(s)$ e $n(s)$ é chamado referencial de Frenet da curva α em s.*

Definição 4.102. *A reta normal a α em s_0 é a reta que passa por $\alpha(s_0)$ na direção de $n(s_0)$.*

Observamos que $t(s)$ e $n(s)$ são funções de I em R^2, diferenciáveis de classe C^∞ e para cada $s \in I$, os vetores de R^2, $t^{'}(s)$ e $n^{'}(s)$, podem ser escritos como combinação linear de $t(s)$ e $n(s)$. Como $t(s)$ é unitário, segue que $t^{'}(s)$ é ortogonal a $t(s)$ e portanto $t^{'}(s)$ é proporcional a $n(s)$.

Definição 4.103. *Este fator de proporcionalidade, denotado por $k(s)$, é chamado curvatura de α em s, isto é,*

$$t^{'}(s) = k(s)n(s).$$

Considerando a curva $\alpha(s) = (x(s), y(s)), s \in I$, segue da definição que

$$k(s) =< t^{'}(s), n(s) >=< \alpha^{''}(s), n(s) >,$$

donde

$$k(s) = -x^{''}(s)y^{'}(s) + y^{''}(s)x^{'}(s).$$

Analogamente como $n(s)$ é unitário, segue que $n^{'}(s)$ é ortogonal a $n(s)$ e portanto $n^{'}(s)$ é proporcional a $t(s)$. Como

$$< n^{'}(s), t(s) >= -x^{'}y^{''}(s) + x^{''}(s)y^{'}(s),$$

concluímos que

$$n^{'}(s) = -k(s)t(s).$$

Definição 4.104. *As equações*

$$t^{'}(s) = k(s)n(s),$$

$$n^{'}(s) = -k(s)t(s)$$

são chamadas as fórmulas de Frenet de uma curva plana.

A função $|k(s)| = |\alpha^{''}(s)|$ indica a velocidade com que as retas tangentes mudam de direção.

De fato, fixemos $s_0 \in I$ e consideremos os vetores tangentes $\alpha^{'}(s_0)$ e $\alpha^{'}(s_0 + h)$, onde $s_0 + h \in I$. Seja $\phi(h)$ o ângulo formado por $\alpha^{'}(s_0)$ e $\alpha^{'}(s_0 + h)$, isto é, $0 \leq \phi(h) \leq \pi$, tal que

$$\cos\phi(h) =< \alpha^{'}(s_0), \alpha^{'}(s_0 + h) > .$$

Então $\lim_{h\to 0} \dfrac{\phi(h)}{h}$ indica a velocidade com que as retas tangentes mudam de direção. Como para todo h

$$|\alpha^{'}(s_0 + h) - \alpha^{'}(s_0)| = 2sen\frac{\phi(h)}{2},$$

concluímos que

$$|k(s_0)| = |\alpha^{''}(s_0)| = \lim_{h\to 0} \frac{\phi(h)}{h}.$$

Exemplo 4.105. Seja $\alpha(s)$ uma curva regular parametrizada pelo comprimento de arco cujo traço é uma reta. Então a curvatura é identicamente nula.

De fato, seja

$$\alpha(s) = (as + x_0, bs + y_0), s \in I,$$

onde a e b são constantes e $a^2 + b^2 = 1$. Como $t(s) = \alpha^{'}(s)$ é constante, segue que $t^{'}(s) = 0$ e portanto $k(s) = 0, \forall s \in I$.

Exemplo 4.106. Consideremos a curva

$$\alpha(s) = (a + b\cos\frac{s}{b}, c + bsen\frac{s}{b}), s \in R, b > 0,$$

cujo traço é uma circunferência de centro (a, c) e raio b. Neste caso

$$t(s) = (-sen\frac{s}{b}, \cos\frac{s}{b}),$$

$$n(s) = (-\cos\frac{s}{b}, -sen\frac{s}{b}).$$

Segue que

$$k(s) =< t'(s), n(s) >= \frac{1}{b}.$$

Consideremos uma reparametrização de α, dada por

$$\beta(s) = (a + b\cos\frac{s}{b}, c - bsen\frac{s}{b}).$$

Então a curvatura será igual a $-\frac{1}{b}$.

Observamos que o sinal da curvatura depende da orientação da curva. Mais adiante veremos a interpretação geométrica do sinal da curvatura.

O próximo resultado expressa a curvatura de uma curva regular e não necessariamente parametrizada pelo comprimento de arco.

Proposição 4.107. *Seja $\alpha(r) = (x(r), y(r)), r \in I$, uma curva regular. Então:*

$$t(r) = \frac{(x^{'}, y^{'})}{\sqrt{(x')^2 + (y')^2}},$$

$$n(r) = \frac{(-y^{'}, x^{'})}{\sqrt{(x^{'})^2 + (y^{'})^2}},$$

$$k(r) = \frac{-x^{''}y^{'} + x^{'}y^{''}}{((x')^2 + (y')^2)^{\frac{3}{2}}}.$$

Demonstração: Seja $\beta(s)$ uma reparametrização de α por comprimento de arco. Derivando $\beta(s(r)) = \alpha(r)$ temos

$$\frac{d\beta}{ds}\frac{ds}{dr} = \alpha^{'}(r) \tag{24}$$

e

$$\frac{d^2\beta}{ds^2}(\frac{ds}{dr})^2 + \frac{d\beta}{ds}\frac{d^2s}{dr^2} = \alpha^{''}(r) \tag{25}$$

daí

$$\frac{ds}{dr} = |\alpha^{'}(r)|. \tag{26}$$

Portanto

$$\frac{d^2s}{dr^2} = \frac{<\alpha^{'}(r), \alpha^{''}(r)>}{|\alpha^{'}(r)|}. \tag{27}$$

Considerando $\alpha(r) = (x(r), y(r))$ segue de (24) e (26) que

$$t(r) = \frac{(x^{'}, y^{'})}{\sqrt{(x^{'})^2 + (y^{'})^2}}.$$

Pela definição de vetor normal temos

$$n(r) = \frac{(-y^{'}, x^{'})}{\sqrt{(x^{'})^2 + (y^{'})^2}}.$$

Como

$$k(s(r)) =< \frac{d^2\beta}{ds^2}(s(r)), n(r) >$$

concluímos usando (24) a (27) que

$$k(r) = \frac{-x^{''}y^{'} + x^{'}y^{''}}{((x^{'})^2 + (y^{'})^2)^{\frac{3}{2}}}.\bullet$$

Vejamos um exemplo.

Exemplo 4.108. Consideremos a espiral logarítimica

$$\alpha(r) = (e^r \cos r, e^r senr), r \in R.$$

Então

$$\alpha(r)^{'} = e^r(\cos r - senr, senr + \cos r),$$

$$\alpha(r)^{''} = e^r(-2senr, 2\cos r),$$

e portanto $k(r) = \dfrac{1}{\sqrt{2}e^r}$.

4.26 Interpretação geométrica do sinal da curvatura

A seguir veremos a interpretação geométrica do sinal da curvatura. Seja $\alpha(s) = (x(s), y(s))$, $s \in I$ uma curva regular parametrizada pelo comprimento de arco. Como o vetor tangente $t(s) = \alpha^{'}(s)$ é unitário temos que $\alpha^{''}(s)$ é ortogonal a $\alpha^{'}(s)$. Fixemos $s_0 \in I$ e suponhamos que $k(s_0) \neq 0$. Observamos que a reta tangente a α em s_0,

$$T(s) = \alpha(s_0) + (s - s_0)\alpha^{'}(s_0),$$

divide o plano em dois semiplanos.

Considerando a expansão de $\alpha(s)$ em séries de Taylor, em torno de s_0 temos

$$\alpha(s) = \alpha(s_0) + (s - s_0)\alpha^{'}(s_0) + \frac{(s - s_0)^2}{2}\alpha^{''}(s_0) + R(s),$$

onde $R(s)$ é uma função vetorial, tal que $\lim\limits_{s \to s_0} \dfrac{R(s)}{(s - s_0)^2} = 0$. Portanto

$$\alpha(s) - T(s) = \frac{(s - s_0)^2}{2}\alpha^{''}(s_0) + R(s).$$

Como $\alpha(s) - T(s)$ é um vetor no sentido do semi-plano que contém $\alpha(s)$, segue da última relação que para todo s, suficientemente próximo de s_0, $\alpha^{''}(s_0)$ tem o sentido do semiplano que contém os pontos $\alpha(s)$.

Como $k(s_0) =< \alpha^{''}(s_0), n(s_0) >$, concluímos que se $k(s_0) > 0$, então $n(s_0)$ tem o mesmo sinal de $\alpha^{''}(s_0)$, se $k(s_0) < 0$ então $\alpha^{''}(s_0)$ e $n(s_0)$ têm sentidos opostos.

4.27 Involutas e Evolutas

Nos exemplos anteriores vimos que, a menos de sinal, a curvatura de uma circunferência de raio r é igual a $\frac{1}{r}$, o que comprova a nossa intuição pois no caso da circunferência pensamos, naturalmente, na recíproca do raio como medida da curvatura.

Definição 4.109. *Se $\alpha(s)$ é uma curva regular com curvatura $k(s) \neq 0$, a quantidade $\rho(s) = \frac{1}{|k(s)|}$ é denominada raio de curvatura de α em s. O círculo de raio $\rho(s)$ e centro $c(s) = \alpha(s) + \frac{1}{k(s)}n(s)$ é denominado círculo osculador e $c(s)$ é dito centro de curvatura. A medida que varia o parâmetro s, o centro de curvatura descreve uma curva β chamada a evoluta de α, cujas retas tangentes são ortogonais à curva α.*

Usando as equações de Frenet, vemos que

$$\beta^{'}(t) = \alpha^{'}(t) + \frac{1}{k(t)}n^{'}(t) - \frac{k^{'}(t)}{k^2(t)}n(t) = -\frac{k^{'}(t)}{k^2(t)}n(t).$$

Portanto temos que β é regular se, e somente se, $k^{'}(t) \neq 0$. Os pontos singulares da evoluta de uma curva α são aqueles para os quais a curvatura de α possui um ponto crítico.

Definição 4.110. *A expressão da evoluta de α é dada por*

$$\beta(t) = \alpha(t) + \frac{1}{k(t)}n(t) = \alpha(t) + \frac{|\alpha^{'}(t)|^2}{< \alpha^{''}(t), n(t) >}n(t). \tag{28}$$

Vejamos alguns exemplos.

Exemplo 4.111. Se o traço de uma curva α descreve um círculo de raio r e centro C, sua evoluta é a curva constante dada por $\beta(s) = C$.

De fato, parametrizando a curva α por

$$\alpha(s) = C + (r\cos\frac{s}{r}, rsen\frac{s}{R}), s \in [0, 2\pi],$$

temos que $k(s) = \frac{1}{r}$ e, portanto,

$$\beta(s) = \alpha(s) + r(-\cos\frac{s}{r}, -sen\frac{s}{r}) = C.$$

Exemplo 4.112. Considere a elipse $\alpha : [0, 2\pi] \to R^2$, definida por

$$\alpha(t) = (a\cos t, bsent).$$

A curvatura de α é dada por

$$k(t) = \frac{ab}{(a^2sen^2t + b^2\cos^2 t)^{\frac{3}{2}}} \neq 0.$$

A evoluta de α, pela equação (28) é dada por

$$\begin{aligned}\beta(t) &= (a\cos t, bsent) + \frac{a^2+\sin^2 t + b^2\cos^2 t}{ab}(-b\cos t, -asent)\\ &= (\frac{a^2-b^2}{a}\cos^3 t, \frac{b^2-a^2}{b}sen^3 t).\end{aligned}$$

O traço da evoluta da elipse é descrito pelo astróide $(ax)^{\frac{2}{3}} + (by)^{\frac{2}{3}} = (a^2-b^2)^{\frac{2}{3}}$, que não é regular nos pontos $\beta(t)$, com $t = 0, \frac{\pi}{2}$ e $\frac{3\pi}{2}$.

Exemplo 4.113. Considere a ciclóide dada pelo traço da curva α, definida por

$$\alpha(t) = (t - sent, 1-\cos t), t \in (0, 2\pi).$$

Sua curvatura é dada por

$$k(t) = \frac{\cos t - 1}{(2-2\cos t)^{\frac{3}{2}}} \neq 0.$$

A evoluta de α é a curva definida por

$$\beta(t) = (t - sent, 1-\cos t) + \frac{2-2\cos t}{\cos t - 1}(-sent, 1-\cos t) = (t + sent, \cos t - 1).$$

Observe que $\alpha(t+\pi) = \beta(t) + (\pi, 2)$. Logo, a menos de uma translação, a evoluta de α é a própria ciclóide.

Definição 4.114. *Uma involuta de uma curva regular β é uma curva que é ortogonal às retas tangentes de β.*

Portanto se β é a evoluta de α, então α é uma involuta de β.

4.28 Teorema Fundamental das Curvas Planas

Nosso objetivo é mostrar o teorema que garante que a função curvatura determina uma curva plana a menos de sua posição no plano.

Teorema 4.115. *a) Dada uma função diferenciável $k(s)$, $s \in I \subset R$, existe uma curva regular $\alpha(s)$, parametrizada pelo comprimento de arco s, cuja curvatura é $k(s)$.*
b)A curva $\alpha(s)$ acima é única quando fixamos $\alpha(s_0) = p_0$ e $\alpha'(s_0) = v_0$, onde v_0 é um vetor unitário de R^2.
c) Se duas curvas $\alpha(s)$ e $\beta(s)$ têm a mesma curvatura, então elas diferem por sua posição no plano, isto é, existe uma rotação L e uma translação T em R^2, tal que $\alpha(s) = (LoT)(\beta(s))$.

Demonstração: a) Consideremos $\theta(s) = \int_{s_0}^{s} k(s)ds$, onde $s_0 \in I$ é fixo. Fixemos um ponto $p_0 = (x_0, y_0)$ de R^2 e $\lambda \in R$. Definimos uma curva $\alpha(s) = (x(s), y(s))$ por

$$x(s) = x_0 + \int_{s_0}^{s} \cos(\theta(s) + \lambda)ds,$$

$$y(s) = y_0 + \int_{s_0}^{s} sen(\theta(s) + \lambda)ds.$$

Vamos verificar que a curva assim definida está parametrizada pelo comprimento de arco s e sua curvatura é $k(s)$.

De fato, o referencial de Frenet é:

$$t(s) = \alpha'(s) = (\cos(\theta(s) + \lambda), sen(\theta(s) + \lambda)),$$

$$n(s) = (-sen(\theta(s) + \lambda), \cos(\theta(s) + \lambda)),$$

e, portanto, temos que $|\alpha^{'}(s)| = 1$ e a curvatura de α é dada por

$$< t^{'}(s), n(s) >= \theta^{'}(s) = k(s).$$

b) Seja $\alpha(s) = (x(s), y(s))$ uma curva regular parametrizada pelo comprimento de arco s, cuja curvatura é $k(s)$. Das equações de Frenet temos que

$$(x^{''}, y^{''}) = k(-y^{'}, x^{'}),$$

isto é, $x(s)$ e $y(s)$ satisfazem as equações

$$x^{''} = -ky^{'},$$
$$y^{''} = kx^{'}.$$

Portanto, segue do teorema de unicidade de solução do sistema de equações diferenciais que fixados $\alpha(s_0) = p_0$ e $\alpha^{'}(s_0) = v_0$ a curva α é única. (Ver [1]).

c) Sejam α e β duas curvas que têm a mesma curvatura. Fixado s_0, existe uma rotação L e uma translação T de R^2 tal que a curva $\overline{\alpha} = LoTo\beta$ satisfaz $\overline{\alpha}(s_0) = \alpha(s_0)$ e $\overline{\alpha}^{'}(s_0) = \alpha^{'}(s_0)$. Do item b) segue que $\overline{\alpha} \equiv \alpha$. Portanto, $\alpha = LoTo\beta$. •

4.29 Exercícios

1) Sejam a e b constantes não nulas. Verifique que a aplicação $\alpha(t) = (a\cos t, b \text{ sen } t), t \in R$ e uma curva parametrizada diferenciável. Descreva o traço de α. O que representa geometricamente o parâmetro t?

2) Obtenha uma curva regular $\alpha : R \to R^2$ tal que $\alpha(0) = (2, 0)$ e $\alpha^{'}(t) = (t^2, e^t)$.

3)Seja $\alpha : I \to R^2$ curva regular. Prove que $|\alpha^{'}(t)|$ é constante se, e somente se para cada $t \in I$, o vetor $\alpha^{''}(t)$ é ortogonal a $\alpha^{'}(t)$.

4) Considere a aplicação

$$\alpha(t) = (sent, \cos t + \log(\tan \frac{t}{2})), t \in (0, \pi).$$

Prove que:

a) α é curva parametrizada diferenciável.

b) $\alpha^{'}(t) \neq 0$ para todo $t \neq \frac{\pi}{2}$.

c) o comprimento da reta tangente, compreendido entre $\alpha(t)$ e o eixo y, é constante igual a 1.

O traço desta curva é chamado Tractriz.

5) Verifique que as curvas regulares $\alpha(t) = (t, e^t), t \in R$ e $\beta(r) = (\log r, r), r \in (0, \infty)$ têm o mesmo traço.

6)Obtenha uma reparametrização da ciclóide

$$\alpha(t) = (a(t - sent), a(1 - \cos t)), 0 < t < 2\pi,$$

pelo comprimento de arco.

7)Obtenha a curvatura das seguintes curvas regulares:
a) $\alpha(t) = (t, t^4), t \in R$.
b) $\alpha(t0 = (\cos(2\cos t - 1), sen(2\cos t - 1)), t \in R$, (cardióide).
c) $\alpha(t) = (t, \cosh t), t \in R$, (catenária).

8) Seja $\alpha(s)$ uma curva regular parametrizada pelo comprimento de arco s e tal que $k(s) > 0, \forall s$. Verifique que o comprimento de arco da evoluta de α entre s_0 e s_1 é igual à diferença entre os raios de curvatura em s_0 e s_1.

9)Caracterize todas as curvas regulares planas que têm curvatura constante.

10) Determine as curvas planas de curvatura $k(s) = \dfrac{1}{\cosh s}$.

11) Determine as curvas regulares do plano cujas retas tangentes se interceptam em um ponto fixo.

12) Determine as curvas regulares do plano cujas retas normais se interceptam em um ponto fixo.

Referências

[1] Figueiredo, D. G. de, "Equações Diferenciais Aplicadas,"12^o Colóquio Brasileiro de Matemática, IMPA, 1979.

[2] H. Alencar e W. Santos, "Introdução às curvas planas", XV Escola de Geometria Diferencial, IMPA, 2008.

[3] P. V. Araújo, "Geometria Diferencial", Matemática Universitária, IMPA, 1998.

[4] G. Ávila, "Cálculo das funções de uma variável", L.T.C., 2003.

[5] M. P. Do Carmo, "Geometria Diferencial das Curvas e Superfícies", Coleção Textos Universitários, S.B.M., 2005.

[6] G. Reis e V. Silva, "Geometria Analítica", L.T.C., 1995.

[7] K. Tenenblat, "Introdução à Geometria Diferencial", Editora Universidade de Brasília, 1990.

MC8 - Sistemas Criptográficos em Blocos

Shirlei Serconek, Celso Júnior, Nilo Célio

IME/UFG | Especialização IME/UFG | Especialização IME/UFG

74901-970, Goiânia - GO

E-mail: shirlei@mat.ufg.br

Este minicurso pretende mostrar a alunos de graduação em Matemática, bem como a professores de Matemática do ensino médio, algumas aplicações de álgebra em criptografia. O curso não possui pré-requisitos pois abordaremos os tópicos de álgebra de corpos finitos necessários para uma boa compreensão da estrutura dos sistemas criptográficos em blocos: Data Encryption Standard (DES) e Advanced Encryption Standard (AES).

MC9 - Números Primos:Testes de Primalidade e Aplicações

Maria Aparecida de Faria, Shirlei Serconek

Especialização IME/UFG | IME/UFG

74001-970, Goiânia - GO

E-mail: shirlei@mat.unb.br

5.30 Introdução

Durante muitas gerações, tentou-se sem muito êxito, aperfeiçoar o entendimento de Euclides sobre os números primos. G.H. Hardy (1877- 1947), matemático inglês, gostava de dizer que: *" Qualquer tolo pode fazer perguntas sobre os números primos que o mais sábio dos homens não consegue responder."* A corrida em busca de fórmulas geradoras de pelo menos uma lista de números primos envolveu mentes muito brilhantes, grandes matemáticos, que não obtiveram sucesso em suas pesquisas. Ainda hoje, muitos matemáticos buscam entender os mistérios que envolvem os números primos com uma vantagem: contam com auxílio de computadores super modernos nessa difícil missão.

Atualmente os números primos deixaram de ser um assunto relevante apenas em Teoria dos Números, devido ao desenvolvimento Criptografia de Chave Pública. Neste artigo, pretendemos mostrar, além de fatos importantes sobre números primos como *O Pequeno Teorema de Fermat* e o *Teorema de Euler*, a Matemática que se utiliza no Criptosistema RSA.

5.31 Conceitos Básicos

Nesta seção, apresentaremos os conceitos necessários ao entendimento deste trabalho.

5.31.1 Divisibilidade

Definição 5.116. *Dados a e $b \in Z$, com $a \neq 0$, dizemos que a divide b, quando existir $c \in Z$ tal que $b = ac$.*

Nota 5.1. *Se a divide b escrevemos $a \mid b$. Se a não divide b escrevemos $a \nmid b$.*

Exemplo 5.117. *Temos que* $2 \mid 4$ *pois* $4 = 2.2$ *e*
$3 \mid 12$ *pois* $12 = 3.4$.

Proposição 5.118. *Se a,b e $c \in Z$ com $a \neq 0$ e x e $y \in Z$ são tais que $a \mid b$ e $a \mid c$ então $a \mid (xb \pm yc)$.*

Demonstração. Se $a \mid b$ e $a \mid c$ então existem f,g $\in Z$ tais que $b = af$ e $c = ag$,logo temos que $xb = xaf$ e $yc = yag$, consequentemente $xb \pm yc = a(xf \pm yg)$ com $xf \pm yg \in Z$. Portanto, $a \mid (xb \pm yc)$. □

Proposição 5.119. ***(Divisão Euclidiana)*** *Sejam a e b números inteiros com a>0. Existem dois únicos números inteiros q e r tais que b=aq+r, com 0≤r<a.*

Demonstração. Suponha que b>a e considere os números b, b-a, b-2a,..., b-na,... Pelo Axioma da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemeto $r = b - aq$. Vamos provar que r<a. Se a|b, então r=0 e nada mais temos a provar. Se a não divide b , então $r \neq a$, e portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c < r$

tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - aq$, teríamos $c = b - (q + 1)a \in$S, com c<r, contradição com o fato de r ser o menor elemento de S.

Unicidade: Dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é, pelo menos a. Logo, se $r = b - aq$ e $r' = b - aq'$ com r<r'<a teríamos r'-r $\geq$a $\Rightarrow$ r'$\geq$ r+a $\geq$a. □

5.31.2 Máximo Divisor Comum

Definição 5.120. *Dados dois números inteiros positivos a e b, não simultaneamente nulos, dizemos que o número inteiro positivo d é um divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Definição 5.121. *Dizemos que d é o máximo divisor comum de a e b se:*

i) d é um divisor comum de a e b;

ii) se d_1 é um divisor comum de a e b então $d_1 \mid d$.

Nota 5.2. *Se d é o máximo divisor comum de a e b escrevemos $d = (a, b)$.*

Exemplo 5.122. *Temos que* $4 = (4, 8)$.

5.31.3 Mínimo Múltiplo Comum

Definição 5.123. *Um número c é um múltiplo comum de dois inteiros a e b se $a \mid c$ e $b \mid c$.*

Definição 5.124. *Sejam a e b dois inteiros tais que $a \neq 0$ ou $b \neq 0$. Dizemos que $m > 0$ é um mínimo múltiplo comum de a e b se:*

i) m é um múltiplo comum de a e b,

ii) se c é um múltiplo comum de a e b, então $m \mid c$.

Nota 5.3. *Se m é o mínimo múltiplo comum de a e b escrevemos $m = [a, b]$.*

Exemplo 5.125. *Temos que* $6 = [2, 3]$.

5.31.4 Congruências

Definição 5.126. *Seja m um número inteiro positivo. Dizemos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais.*

Nota 5.4. *Se a é congruente a b módulo m escrevemos $a \equiv b \bmod m$.*

Proposição 5.127. *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo. Diz-se que a é congruente a b módulo m se e somente se $m \mid a - b$.*

Demonstração. Se $a \equiv b \bmod m$ então $m \mid a - b$. Por hipótese, $a = mq + r$ e $b = mq_1 + r$ onde q e $q_1 \in Z$. Logo $a - b = mq - mq_1 = m(q - q_1)$ onde $q - q_1 \in Z$, portanto, $m \mid a - b$. Se $m \mid a - b$ então $a \equiv b \bmod m$. Por hipótese, $m \mid a - b$, isto é, $a - b = mx$ onde $x \in Z$. Desta forma $a = mx + b$. Seja r o resto da divisão de b por m, logo temos que $b = mx_1 + r$ onde $x_1 \in Z$. Substituindo o valor de b na equação $a = mx + b$ temos: $a = mx + mx_1 + r$, logo $a = mx_2 + r$ onde $x_2 \in Z$, e concluimos que a deixa o mesmo resto r quando dividido por m. Portanto, $a \equiv b \bmod m$. □

Exemplo 5.128. *Temos que* $21 \equiv 13 \bmod 2$ *, pois 21 e 13 deixam o mesmo resto quando divididos por 2.*

5.32 Números Primos

Definição 5.129. *Um número inteiro p>1 é um número primo se ele for divisível somente por 1 e por si mesmo.*

Definição 5.130. *Um número inteiro positivo maior que 1 é um número composto se ele não é um número primo.*

5.32.1 Fatoração Prima

Teorema 5.131. *Todo inteiro positivo é igual a 1, é um número primo, ou pode ser escrito como um produto de números primos.*

Demonstração. Provaremos o teorema usando o segundo princípio de indução. Para n=1 o teorema é válido.

Vamos supor que ele é válido para todo inteiro positivo n<k. Se k é primo então o teorema é válido para k.

Se k não é primo, então k é divisível por algum inteiro p e k=pq onde nem p, nem q é k ou 1. Como p|k e q|k temos que p e q são menores que k. Logo, pela hipótese de indução p e q podem ser escritos como um produto de números primos. Consequentemente, k=pq pode ser escrito como um produto de números primos. □

Exemplo 5.132. *Temos que 37 é primo e 15=3.5 é um produto de números primos.*

Teorema 5.133. *Se p é um número primo e p|ab, onde a e b são inteiros positivos, então p|a ou p|b.*

Demonstração. Se p|a então a conclusão é válida. Por outro lado, se p não divide a então $(a, p) = 1$. Logo, existem x e y, inteiros positivos tais que $ax + py = 1$. Multiplicando a igualdade anterior por b temos: $abx + pby = b$. Por hipótese p|ab, logo $ab = pk$, para algum k inteiro positivo. Desta forma, $pkx + pby = b \Rightarrow$ p(kx+by)=b. Portanto, p|b. □

Lema 5.134. *Se um número primo p divide um produto de inteiros positivos $q_1q_2...q_n$, então p|q_i, para algum i, 1≤i≤n.*

Demonstração. Vamos mostrar o Lema usando indução sobre n, o núme-ro de fatores do produto $q_1q_2...q_n$.

Se $n = 1$, o Lema é válido. Suponhamos que o Lema seja verdadeiro para $n = k$, isto é, se p divide algum produto de k inteiros, então p divide um dos k fatores.

Suponhamos que p divide a produto de k+1 inteiros, isto é,
p|$q_1q_2...q_kq_{k+1}$, logo p| $(q_1q_2...q_k)q_{k+1}$. Se p|q_{k+1} então o Lema está demonstrado.

Se p não divide q_{k+1} então p|$q_1q_2...q_k$. Mas $q_1q_2...q_k$ é o produto de k inteiros , pela hipótese de indução p|q_i, para algum i, 1≤i≤n. □

Lema 5.135. *Se um número primo p divide o produto de primos $q_1q_2...q_n$, então p=q_i para algum i, 1≤i≤n.*

Demonstração. Temos que p|q_i para algum i,onde 1≤i≤n. Consequentemente p e q_i são ambos primos, logo p=q_i para algum i,1≤i≤n. □

Teorema 5.136. *(**Teorema Fundamental da Aritmética**) Qualquer inteiro po-sitivo m>1 é um número primo ou pode ser escrito como um produto de números primos, onde o produto é único exceto pela ordem dos fatores.*

Demonstração. Uma vez que m pode ser escrito como um produto de números primos, vamos assumir que $q_1q_2...q_n$ e $p_1p_2...p_s$ são duas maneiras de escrever m como o produto de números primos.

Faremos a demonstração do teorema usando indução sobre n, o número de fatores primos de $q_1q_2...q_n$.

Se $n = 1$ o teorema é verdadeiro. Suponhamos que o teorema seja válido para $q_1q_2...q_k = p_1p_2...p_s$,isto é, se m= $q_1q_2...q_k = p_1p_2...p_s$ então $k = s$ e o produto é único.

Suponha que m=$q_1q_2...q_{k+1}$=$p_1p_2...p_{s'}$.

Temos que q_{k+1} divide $p_1p_2...p_{s'}$ então $q_{k+1} = p_i$ para algum 1≤i≤s'. Dividindo m=$q_1q_2...q_{k+1} = p_1p_2...p_{s'}$ por q_{k+1} temos
$q_1q_2...q_k$ =$p_1p_2...p_{i-1}p_{i+1}...p_{s'}$. Mas $k = s' - 1$ e o produto é único pela hipótese de indução. Consequentemente $k + 1 = s'$. Portanto, a fatoração de m é única. □

Teorema 5.137. *Existem infinitos números primos.*

Demonstração. Suponha que existe somente um número finito de núme-ros primos, isto é, p_1,p_2,...,p_k. Considere o inteiro $(p_1p_2...p_k) + 1$. Seja p_r um número primo e suponha que $p_r|((p_1p_2...p_k) + 1)$. Mas $p_r|p_1p_2...p_k$, logo $p_r|1$. (Contradição). Portanto, existem infinitos núme-ros primos.

□

Teorema 5.138. *(**Pequeno Teorema de Fermat**) Se p é um número primo e se a é um número inteiro, então $a^p \equiv a$ mod p.*

Demonstração. Faremos a demonstração por indução sobre a. Claramente o resultado vale para $a = 1$, pois $p \mid 0$. Suponhamos que o resultado seja válido para a, provaremos a validade para $a + 1$. Temos, pela fórmula do binômio de Newton, $(a + 1)^p - (a + 1) = a^p - a + \binom{p}{1}a^{p-1} + .. + \binom{p}{p-1}a$. Como $a^p - a$ é divisível por p, pela hipótese de indução, e os números $\binom{p}{i}$, onde $0 < i < p$ são todos divisíveis por p, então $(a + 1)^p - (a + 1)$ é divisível por p. □

5.32.2 Função Φ de Euler

Definição 5.139. *Se n=1, então Φ(n)=1; se n>1, então Φ(n) é o número de inteiros k tais que 1≤k<n e $(k, n) = 1$.*

Exemplo 5.140. *Φ(5)=4.*

Teorema 5.141. *Sejam r e s números inteiros positivos com $r > 1$ e $s > 1$ e $(r, s) = 1$. Então $\phi(r.s) = \phi(r).\phi(s)$.*

Veja demonstração em [12].

5.32.3 Cálculo de $\Phi(n)$

Teorema 5.142. *Se o inteiro $n > 1$, então $\phi(n) = n - 1$ se e somente se n é primo.*

Demonstração. Se $n > 1$ é primo, então cada um dos inteiros positivos menores que n é primo com n e, portanto, $\phi(n) = n - 1$. Se, por outro lado $\phi(n) = n - 1$, com $n > 1$, então n é primo, pois, se n fosse composto, teria pelo menos um divisor d tal que $1 < d < n$, de modo que pelo menos dois dos inteiros 1,2,3,...,n não seriam primos com n, isto é, $\phi(n) = n - 2$. Logo,n é primo. □

Teorema 5.143. *Se p é primo e se k é um inteiro positivo, então: $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$.*

Demonstração. De 1 até p^k, temos p^k números naturais. Precisamos excluir desses números os que não são primos com p^k, ou seja, todos os múltiplos de p, que são $p, 2p, ..., p^{k-1}p$, cujo número é p^{k-1}. Portanto, $\phi(p^k) = p^k - p^{k-1}$. □

Conhecendo os resultados anteriores sobre a função Φ de Euler, podemos obter a expressão $\phi(n)$ para qualquer n pertencente aos inteiros positivos.

Teorema 5.144. *Se $n = p_1^{k_1}....p_r^{k_r}$ é a decomposição de n em fatores primos, então $\phi(n) = p_1^{k_1}....p_r^{k_r}.(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$.*

Demonstração. Como os $p_{r's}$ são números primos temos que
$\phi(n) = \phi(p_1^{k_1}....p_r^{k_r}) = \phi(p_1^{k_1})....\phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})...(p_r^{k_r} - p_r^{k_r-1}) = p_1^{k_1}.(1 - \frac{1}{p_1}).p_2^{k_2}.(1 - \frac{1}{p_2})...p^{k_r}.(1 - \frac{1}{p_r}) = p_1^{k_1}....p_r^{k_r}.(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$.

□

Lema 5.145. *Seja a e $n > 1$ inteiros tais que o $(a, n) = 1$. Se $a_1, a_2, ..., a_{\phi(n)}$ são os inteiros positivos menores que n e que são primos com n, então cada um dos inteiros: $a.a_1, a.a_2, ..., a.a_{\phi(n)}$ é congruente módulo n a um dos inteiros $a_1, a_2, ..., a_{\phi(n)}$ (não necessariamente nesta ordem).*

Veja demonstração em [12].

Teorema 5.146. *(***Teorema de Euler***) Se n é um inteiro positivo e se $(a, n) = 1$ então $a^{\phi(n)} \equiv 1$ mod n.*

Demonstração. Para $n = 1$ o teorema é válido, pois, temos
$a^{\phi(1)} \equiv 1$ *mod* n. Suponhamos, pois, $n > 1$. Sejam $a_1, a_2, ..., a_{\phi(n)}$ os inteiros positivos menores que n e que são primos com n. Como $(a, n) = 1$ então pelo Lema anterior, os inteiros $a.a_1, a.a_2, ..., a.a_{\phi(n)}$ são congruentes módulo n, não necessariamente nesta ordem, aos inteiros $a_1, a_2, ..., a_{\phi(n)}$, isto é,

$$a.a_1 \equiv a'_1 \ mod \ n$$
$$a.a_2 \equiv a'_2 \ mod \ n$$
$$.....$$
$$a.a_{\phi(n)} \equiv a'_{\phi(n)} \ mod \ n$$

onde $a'_1, a'_2, ..., a'_{\phi(n)}$ são os inteiros $a_1, a_2, ..., a_{\phi(n)}$ numa certa ordem. Multiplicando essas $\phi(n)$ congruências obtemos:

$a.a_1, a.a_2, ..., a.a_{\phi(n)} \equiv a'_1.a'_2.....a'_{\phi(n)}$ *mod* n. Daí, temos

$a^{\phi(n)}.(a_1.a_2.....a_{\phi(n)}) \equiv a'_1.a'_2.....a'_{\phi(n)}$ *mod* n. Como $(a_i, n) = 1$ podemos cancelar o fator comum e portanto, $a^{\phi(n)} \equiv 1$ *mod* n.

□

Observe que, se p é um número primo, então $\phi(p) = p - 1$, e se $(a, p) = 1$ temos que $a^{\phi(p)} \equiv 1 \; mod \; p$, logo $a^{(p-1)} \equiv 1 \; mod \; p$ que é o pequeno teorema de Fermat. Desta forma, o teorema de Euler é uma generalização do pequeno teorema Fermat.

5.33 A Busca pelos Números Primos

O Renascimento da Aritmética se deu, com o jurista francês Pierre de Fermat (1601-1665). Os resultados de Fermat foram divulgados, principalmente, por Marin Mersenne (1588-1648) outro curioso que se dedicou ao estudo dos números primos.

Leonhard Euler (1707-1783), a *"Águia Matemática"*, foi sem dúvida um dos maiores e mais férteis matemáticos de todos os tempos. A paixão de Euler pela teoria dos números foi motivada pela correspondência com Christian Goldbach, um matemático amador alemão que vivia em Moscou. Foi a Euler que Goldbach fez sua famosa conjectura de que *" todo número par maior ou igual a 4 pode ser escrito como a soma de dois números primos".*

Euler mostrou que o polinômio $p(n) = n^2 + n + 41$ gera números primos para $0 \leq n < 40$.

Carl Friedrich Gauss (1777-1855), o Príncipe dos Matemáticos, vendo que após séculos de pesquisa ainda não havia sido possível descobrir uma fórmula que gerasse números primos pensava em adotar uma estratégia diferente.

O grande avanço de Gauss, na busca pelos números primos, foi tentar descobrir como se distribuiam os números primos entre os 100 primeiros números inteiros, entre os primeiros 1000 e assim por diante.

Bernhard Riemann (1826-1866) também se dedicou à busca pelos números primos apesar da teoria dos números não ser sua área de interesse.

Riemann teve a idéia de definir a função zeta para todos os números complexos s, tendo parte real maior que 1,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

A Função Zeta de Riemann deu origem à Hípótese de Riemann. Uma hipótese matemática publicada em 1859 por Bernhard Riemann que declara que os *os zeros não triviais da Função Zeta de Riemann pertencem todos à " linha crítica".*

A Hipótese de Riemann é de tal importância que tem intrigado os matemáticos há mais de 150 anos e é hoje um dos poucos problemas apresentados por David Hilbert (1862-1943), em 1900, no Congresso Internacional de Matemática em Paris, não resolvidos.

A busca pelos números primos continua. Atualmente a aplicação mais notável dos números primos é na *Criptografia de Chave Pública.* Um grande avanço foi conseguido na *Criptografia* com o aparecimento dos cripto-sistemas de *chave pública* em 1976. A idéia é a seguinte: no lugar de uma chave secreta, de posse tanto do emissor quanto do receptor, temos duas chaves. Uma delas é pública, disponível para qualquer pessoa, e uma segunda, privada, de posse apenas de receptor, que serve para decodificar a mensagem. O emissor codifica a mensagem com a chave pública e a transmite. O receptor decodifica a mensagem com a chave privada. Caso alguém intercepte a mensagem, não saberá qual é a chave privada, pois ela não é transmitida a ninguém. Essa idéia se concretizou em 1977, através de Rivest, Shamir e

Adleman do Instituto Tecnológico de Massachusetts que criaram o algoritmo *RSA.* Para implementar o mais conhecido dos algoritmos de chave pública o *RSA*, precisamos escolher dois números primos muito grandes p e q. Para codificar a mensagem usamos $n = p.q$ e para decodificar precisamos conhecer p e q. A segurança do método vem da dificuldade de fatorar n para descobrir p e q.

5.34 Criptosistemas de Chave Pública

Recorde que um Criptosistema de Chave Pública é caracterizado pela existência de um *arquivo privado* e um *arquivo público.* Deste modo, para cada usuário U, o arquivo público de U está disponível para todos os usuários, e isto inclui a função codificação E_U. Porém o arquivo privado de U é conhecido somente por U e consiste da função decodificação D_U. Além disso, as funções codificação e decodificação são baseadas na noção de uma "função armadilha"ou trapdoor. Uma função armadilha é uma função f tal que as seguintes propriedades são válidas:

i) f é fácil de calcular;

ii) f^{-1} é difícil de calcular;

iii)f^{-1} é fácil de calcular quando uma função armadilha torna-se disponível.

Desta forma temos que o Criptosistema de Chave Pública consiste de duas famílias E_U e D_U (onde U é o conjunto formado por todos os usuários potenciais) de funções codificação e decodificação, respectivamente, tais que:

i) Para todo U, $D_U(E_U(M) = M$, onde M é um bloco da mensagem pré-codificada;

ii) Para todo U, E_U está no arquivo público, mas D_U é conhecida somente por U;

iii) Para todo U, E_U é a função armadilha ;

iv) Para todo U $E_U(D_U(M) = M$(assinatura digital).

5.34.1 *A Matemática do Criptosistema RSA*

No Criptosistema RSA, dois números primos distintos p e q são escolhidos e mantidos secretos, o produto $N = p.q$ é conhecido. Como N é o produto de dois números primos p e q temos que $\Phi(N) = (p-1).(q-1)$. Desta forma, cada usuário escolhe inteiros e, d menores que $\Phi(N)$ tais que $(e, \Phi(N)) = 1$ e $e.d = 1$ mod $(\phi(N))$ onde e é conhecido, mas d é mantido secreto. As funções *codificação* e *decodificação*, são respectivamente:

$E(x) = x^e mod N$ e $D(x) = x^d mod N$, onde $1 \leq x < N$, representa um bloco da mensagem pré-codificada, isto é, uma mensagem onde houve uma mudança de alfabeto. Suponhamos que a mensagem a ser transmitida seja "VIVA HOJE". Podemos fazer a seguinte mudança: V=31; I=18; A=10; H=17; O=24; j=19; e E=14. Desta forma obtemos uma pré-codificação em blocos da mensagem a ser transmitida:

31-18-31-10-99-17-24-19-14, onde 99 é o espaço entre as duas palavras.

Usando o Algoritmo Euclideano podemos determinar o inteiro d tal que $e.d = 1 \mod (\phi(N))$. Mostraremos agora que $E(D(x)) = x$ e $D(E(x)) = x$, ou seja, as funções E e D são a inversa uma da outra e é por isso que o método funciona. Note que $D(E(x)) = D(x^e mod N) = x^{e.d} mod\ N$ e $E(D(x)) = E(x^d mod\ N) = x^{e.d} mod\ N$. Queremos mostrar que $x^{e.d} \equiv x\ mod\ N$. Como $N = p.q$, onde p e q são primos distintos calculemos $x^{e.d} mod\ p$ e $x^{e.d} mod\ q$. Temos que, $e.d \equiv 1\ mod\ (\phi(N)$. Consequentemente existe um inteiro k tal que $e.d = 1 + k\phi(N) = 1 + K(p-1).(q-1)$ logo $x^{e.d} = x.(x^{p-1})^{k(q-1)} mod\ p$. Para todo x tal

que p não divide x e p primo, aplicando o *Pequeno Teorema de Fermat* temos $x^{p-1} \equiv 1 \; mod \; p$. Logo, $x^{e.d} \equiv x \; mod \; p$. Se p divide x então $x \equiv 0 \; mod \; p$. Assim $x^{e.d} \equiv x \; mod \; p$ vale para qualquer p. Analogamente $x^{e.d} \equiv x \; mod \; q$ vale para qualquer q. Observe que não podemos usar um argumento diretamente para N , pois o fato $(N, x) \neq 1$ não significa que $x \equiv 0 \; mod \; N$, pois N é composto.

Exemplo 5.147. *Seja 31-18-31-10-99-17-24-19-14 a mensagem pré-codi-ficada em blocos vista anteriormente. Queremos codificar o bloco*
$x = 14$. *Vamos determinar os parâmetros para fazermos a codificação. Sejam* $p = 11$ *e* $q = 13$, *daí* $N = 11.13 = 143$. *Temos que*
$\phi(N) = (p-1).(q-1) = (11-1).(13-1) = 10.12 = 120$. *Sabemos que* $(e, \phi(N)) \neq 1$, *desta forma vamos considerar* $e = 7$. *Considerando* $e = 7$ *podemos determinar o valor de d. Sabemos que* $e.d \equiv 1 \; mod \; (\phi(N)) \Rightarrow 7.d \equiv 1 \; mod \; 120 \Rightarrow 120 \mid 7.d - 1 \Rightarrow 7.d - 1 = 120.k \Rightarrow 7.d - 120.k = 1$.

Aplicando o Algoritmo Euclideano para e e $\phi(N)$ *obtemos:* $120 = 17.7 + 1 \Rightarrow 1 = 120 + (-17).7$, *logo o inverso de 7 módulo 120 é -17, mas precisamos que d seja positivo. Portanto,* $d = 120 - 17 = 103$ *que é o menor inteiro positivo congruente a -17 módulo 120.*

Assim o bloco $x = 14$ *é codificado como* $E(14) = 14^7 \; mod \; 143$, *isto é,* $E(14)$= *o resto da divisão de* 14^7 *por* 143. *Fazendo os cálculos encontramos que* $14^7 \equiv 53 \; mod \; 143 \Rightarrow E(14) = 53$. *Para decodificarmos* $E(14) = 53$ *vamos usar a função decodificação D, ou seja,* $D(E(14)) = E(14)^d \; mod \; N = 53^{103} \; mod \; 143$, *isto é,* $D(E(14))$ = *o resto da divisão de* 53^{103} *por 143. Fazendo os cálculos encontramos* $53^{103} \equiv 14 \; mod \; 143$. *Portanto,* $D(53) = 14$.

Como vimos anteriormente, a segurança do RSA está na dificuldade de se fatorar N. Se a escolha dos parâmetros p e q não for feita com cuidado, pode ser fácil quebrar o sistema RSA.

5.35 Tipos de Números Primos

Existem números primos que possuem nomes especiais. A maioria deles leva o nome de seus descobridores e seguem um modelo para obtê-los.

5.35.1 Primos de Fermat

Em 1640, Fermat mostrou que os números F_n=$2^{2^n} + 1$ são primos para
$n = 0, 1, 2, 3, 4$, e conjecturou que todo número desta forma é primo, ficando assim conhecidos como Números Primos de Fermat.

Em 1739, cerca de 100 anos mais tarde, Euler demonstrou que a conjectura de Fermat era falsa ao provar que F_5= 2^{32}+1 é divisível por 641. Ainda não se conhece nenhum outro número primo de Fermat além dos cinco primeiros (3,5,17,257,65537) como também não se sabe se existe uma infinidade de números primos de Fermat ou não.

5.35.2 Primos de Mersenne

Os números primos de Mersenne tem relação com os *números perfeitos*. Um número se diz *perfeito*, se a soma dos seus divisores próprios é igual a si mesmo. Por exemplo, 6 é um número perfeito, pois 6=1+2+3, onde 1,2 e 3 são os divisores próprios de 6. O número 28 também é perfeito, assim como 496 e 8128. Sempre que se descobre um número primo da forma 2^n-1 pode se gerar um número perfeito par multiplicando-o por 2^{n-1}.

Euclides, no livro IX dos Elementos, demonstrou que: *Qualquer número da forma* $2^{n-1}(2^n\text{-}1)$ *é par perfeito, se e somente se,* $2^n\text{-}1$ *for primo.*

A existência de um número perfeito ímpar é um dos mais antigos problemas matemáticos ainda sem solução. Conjectura-se com fortes indícios experimentais que não existe nenhum.

Os números M_q=2^q-1 , q número primo, são chamados *números de Mersenne.* O maior número primo conhecido é um Número de Mersenne $2^{32.582.657} - 1$, um gigante com 9.808.358 de dígitos, descoberto pelo time de colaboradores formado pelos doutores Curtis, Cooper e Steve Boone, do Departamento de Ciência da Computação da Universidade Central de Missouri, no dia 4 de setembro de 2006.

5.35.3 Números Primos de Sophie Germain

No início do século XIX o Último Teorema de Fermat era o mais famoso problema da teoria dos números. Muitos matemáticos, inclusive Euler, tinham fracassado ao tentar demonstrá-lo gerando um certo desânimo. Todavia, uma descoberta de Marie-Sophie Germain (1776-1831), matemática francesa, fez com que os matemáticos retomassem a busca pela demonstração. O teorema enunciado por Sophie Germain diz que *"se p é um primo de modo que 2p+1 também seja primo, então não existem inteiros x,y e z, diferentes de zero e não múltiplos de p, tais que* $x^p+y^p= z^p$*."*

Os números p tais que 2p+1 é primo são conhecidos como primos de Sophie Germain.

Esse resultado causou um choque no estudo do Último Teorema de Fermat e era superior aos obtidos pelos matemáticos da época. O choque não foi apenas matemático, mas social também, pois Sophie Germain teve que adotar um pseudônimo masculino Antoine August Le- Blanc para ser aceita pelos matemáticos. Durante muito tempo Sophie Germain se correspondeu com Gauss usando o pseudôni-mo masculino. Porém, em 1807 ela revelou sua identidade e Gauss escreveu-lhe uma carta encantadora. Outro matemático da época que a aprovou foi Adrien-Marie Legendre (1752-1833) que se tornou seu amigo e mentor. Acredita-se que existem infinitos números primos de Sophie Germain.

5.35.4 Primos Gêmeos

Primos Gêmeos são os números primos tais que dado um número primo p, p+2 também será um número primo.

Os números primos gêmeos formam pares, como por exemplo (3,5), (5,7), (11,13), (17,19), (71,73). Os matemáticos acreditam que existem infinitos números primos gêmeos, conjectura ainda não provada. Em 1919, o matemático norueguês Viggo Brun (1885-1978) demonstrou um resultado curioso: *a soma dos inversos dos números primos gêmeos é infinita.* O valor dessa soma é conhecido como constante de Brun.

5.36 Testes de Primalidade

Números Primos são de fundamental importância em matemática em geral, e em teoria dos números em particular. Desta forma, há um grande interesse em estudar diferentes propriedades dos números primos. Especialmente aquelas que permitem determinar eficientemente se um dado número é primo. Um problema clássico em matemática é: dado um número n, como conhecer se ele é primo ou composto?

Não é fácil provar se um determinado número inteiro é primo ou não, mas existem algoritmos muito eficientes que provam a primalidade de um inteiro positivo. Tais algoritmos são chamados Testes de

Primalidade. Os testes de primalidade podem ser: *determinísticos* ou *probabilísticos.*

Os testes de primalidade determinísticos determinam com certeza se um número inteiro dado é primo ou composto. No entanto, é prático apenas para inteiros pequenos ou inteiros que sejam divisíveis por um primo pequeno.

Os testes de primalidade probabilísticos são testes que podem provar que um número é composto, mas podem indicar, apenas com certa probabilidade que um número inteiro é primo. Os testes probabilísticos ainda são muito utilizados por serem mais rápidos, mais eficientes (são executados em tempo polinomial) que os testes determinísticos. Neste trabalho serão apresentados testes de primalidade *determinísticos e probabilísticos.*

5.36.1 Crivo de Eratóstenes

É o método determinístico mais antigo conhecido para encontrar todos os primos até um certo inteiro N específico. A palavra Crivo quer dizer peneira. O algoritmo atua, de fato, como uma peneira separando os múltiplos dos primos em sucessão, deixando passar apenas os que não são divisíveis por estes primos. O método consiste em escre-ver todos os inteiros de 1 a N. Como 1 não é primo, pode ser riscado imediatamente. O algorítmo prossegue, sequencialmente em passos. Em cada etapa, encontramos o primeiro número que não foi riscado, marcamos ele como primo e riscamos todos os seus múltiplos. Enquanto o último número a ser avaliado não excede a raiz quadrada de N, repetimos os passos citados.

Exemplo 5.148. *Construir a tabela de todos os primos menores que 100.*

Crivo de Eratóstenes

~~1~~	*2*	*3*	~~4~~	*5*	~~6~~	*7*	~~8~~	~~9~~	~~10~~
11	~~12~~	*13*	~~14~~	~~15~~	~~16~~	*17*	~~18~~	*19*	~~20~~
~~21~~	~~22~~	*23*	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	*29*	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	*37*	~~38~~	~~39~~	~~40~~
41	~~42~~	*43*	~~44~~	~~45~~	~~46~~	*47*	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	*53*	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	*59*	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	*67*	~~68~~	~~69~~	~~70~~
71	~~72~~	*73*	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	*79*	~~80~~
~~81~~	~~82~~	*83*	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	*89*	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	*97*	~~98~~	~~99~~	~~100~~

Os primos p tais que $p \leq \sqrt{100} = 10$ *são 2, 3, 5 e 7. Vamos eliminar todos os inteiros compostos que são múltiplos de 2, 3, 5 e 7. Os inteiros positivos não riscados são 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 todos números primos menores que 100.*

5.36.2 Divisão por Tentativas

Proposição 5.149. *Todo número inteiro* α *maior que 1 tem um divisor primo.*

Demonstração. O número inteiro α tem um divisor que é maior que 1, ou seja, α. Entre todos os divisores de α que forem maiores que 1, seja p o menor de todos. Então, p tem que ser primo. Caso contrário, p teria um divisor b com $1 < b < p \leq \alpha$. (Contradição).

□

Proposição 5.150. *Se n é um inteiro positivo composto, então n possui um divisor primo p que é menor que ou igual a* $\sqrt{n}$.

Tabela 1: Menor Pseudoprimo

Inteiro a	Menor pseudoprimo para a base a
2	341=11.13
3	91=7.13
4	15=3.5
5	124=2^2
6	35=5.7
7	25=5^2
8	9=3^2
9	28=2^2.7
10	33=3.11

Demonstração. Se n é um inteiro positivo composto então n possui um divisor primo p tal que p$\leq\sqrt{n}$. Como n é composto podemos escrever n=ab, onde a e b são inteiros positivos: a>1 e b>1. Temos que a$\leq\sqrt{n}$ ou b$\leq\sqrt{n}$, do contrário, n=ab>$\sqrt{n}\sqrt{n}$=n. Suponha que a$\leq\sqrt{n}$. Pela proposição 7.2 a tem um divisor primo p. Como p$\leq$a$\leq\sqrt{n}$ $\Rightarrow$ p também é divisor de n. Portanto, n possui um divisor primo p tal que p$\leq\sqrt{n}$. □

A proposição anterior sugere um algoritmo determinístico para testar se n é um número primo. O algoritmo verifica, para todo número primo p que for menor ou igual a $\sqrt{n}$, se ele é um divisor de n. Se for encontrado um divisor primo de n, então n é composto. Do contrário, n é primo. Esse procedimento é chamado Divisão por Tentativas. Na prática este teste é utilizado para testar a primalidade de números inteiros pequenos.

Exemplo 5.151. *43 é um número primo?*

Temos que a raiz quadrada inteira mais próxima de 43 é 6. Logo, devemos testar se um dos números primos p$\leq$6 será divisor de 43. Os números primos p menores que 6 são 2, 3 e 5. Nenhum deles é divisor de 43, portanto 43 é um número primo.

5.36.3 Teste de Fermat

O Pequeno Teorema de Fermat dá origem a um teste de primalidade probabilístico chamado Teste de Fermat. O Teste consiste em:

Dado a>1, escolha p>1 e calculemos a^{p-1} *mod p*. Se o resultado não for 1 mod p, então n é um número composto. Se o resultado encontrado for 1 mod p, então p pode ser um número primo e recebe o nome de *primo provável na base a* ou *pseudoprimo* na base a.

Exemplo 5.152. *O número 341 é pseudoprimo para a base 2, pois* $2^{340}\equiv$ *1 mod 341.*

A existência de pseudoprimos atesta que o Teste de Fermat não é determinístico. Podemos aumentar a eficácia do Teste de Fermat, aplicando-o repetidamente e utilizando várias bases.

O número 341, por exemplo, não passa no teste para a base 3, pois $3^{340}\equiv$56 mod 341. Portanto, 3 é testemunha de que 341 é composto. A Tabela 1 apresenta o menor pseudoprimo para as bases entre 2 e 10.

5.36.4 Números de Carmichael

Existem inteiros compostos que não se consegue provar que são compostos pelo Teste de Fermat com qualquer base, isto é, há inteiros que enganam o Teste de Fermat para todas as bases.

Definição 5.153. *Um número composto ímpar n>0 é um número de Carmichael se* $a^n \equiv a \bmod n$ *para todo 1<a<n-1.*

Portanto, números de Carmichael são pseudoprimos de Fermat para todas as bases.

Exemplo 5.154. *O número 561 é um número de Carmichael. Não é fácil provar esta afirmação usando a definição, pois precisaríamos verificar que* $a^{561} \equiv a \bmod 561$ *para* $a = 2, 3, ..., 559$ *o que dá um total de 558 bases a serem testadas, algumas não tão pequenas.*

Em 1899, uma caracterização para os números de Carmichael foi dada no Teorema de Korselt.

Teorema 5.155. *(**Teorema de Korselt**) Um inteiro positivo ímpar n é um número de Carmichael se, e somente se, cada fator primo p de n satisfaz as duas condições seguintes:* p^2 *não divide n e p-1 divide n-1.*

Não demonstraremos aqui o Teorema de Korselt, a prova exige conhecimentos sobre corpos finitos. Utilizando o Teorema de Korselt podemos mostrar que 561 é um número de Carmichael facilmente.

Exemplo 5.156. *Temos que 561= 3.11.17.*

$3^2 \nmid 561$, $11^2 \nmid 561$, $17^2 \nmid 561$. *Temos que* $3 - 1 = 2$ *e* $2 \mid 560$, $11 - 1 = 10$ *e* $10 \mid 560$ *e* $17 - 1 = 16$ *e* $16 \mid 560$.

Portanto, 561 é um número de Carmichael e é o menor deles. Em 1994, os matemáticos Willian Alford, Andrew Granville e Carl Pomerance provaram que há infinitos números de Carmichael.

5.36.5 Teste de Miller-Rabin

O Teste de Primalidade de Miller-Rabin é um teste probabilístico criado em 1976 por G.L. Miller e modificado por M.O. Rabin. Este teste é uma pequena modificação do teste de Fermat, sendo mais eficiente, ainda que haja uma pequena chance de erro.

Seja n um inteiro positivo ímpar cuja primalidade desejamos testar. O inteiro n-1 é par. Seja s a maior potência de 2 que divide n-1, isto é, n-1=$2^s d$, onde d é ímpar.

Seja $1 < b < n - 1$ um inteiro que será a base para o teste. Considere as seguintes potências de b: b^d, b^{2d}, $b^{2^2 d}$,..., $b^{2^{s-1} d}$, $b^{2^s d}$. Se n for um número primo, então
$b^{2^s d} = b^{n-1} \equiv 1 \bmod n$.

Talvez alguma potência anterior a essa seja congruente a 1 mod n. Seja k o menor expoente tal que $b^{2^k d} \equiv 1 \bmod n$ isto é n| $b^{2^k d}$-1.

Se k=0 então $b^{2^0 d} \equiv 1 \bmod n$ daí $b^d \equiv 1 \bmod n$.

Se $k > 0$, então podemos fatorar $b^{2^k d}$-1 como ($b^{2^{k-1} d}$-1).($b^{2^{k-1} d}$+1). Como n é primo e divide $b^{2^k d}$-1, então divide um dos dois fatores . Mas, n não pode dividir $b^{2^{k-1} d}$-1 pela escolha de k como o menor inteiro tal que n divide $b^{2^k d}$-1. Portanto, n divide $b^{2^{k-1} d}$+1, isto é, $b^{2^{k-1} d} \equiv$ -1 mod n.

Concluimos, pela análise anterior que: se n é primo, então para toda base b 1<b<n-1 escrevendo as d potências b^d, b^{2d}, $b^{2^2 d}$,..., $b^{2^{s-1} d}$, $b^{2^s d}$, ou a primeira é congruente a 1 mod n ou alguma delas será

congruente a -1 mod n. Se nada disso acontecer, então o inteiro n é composto e dizemos que b é uma testemunha de que n é composto. Se um inteiro positivo composto n satisfaz alguma das condições acima para a base b, então n é *pseudoprimo forte* para a base b.

Exemplo 5.157. *Se n=341 temos que n-1=340=*2^2*85, onde d=85 e 0≤s<2. Sendo b = 2 precisamos calcular duas potências:*

$2^{2^0 85}=2^{85}\equiv$ *32 mod 341*

$2^{2^1 85}= 2^{170}=2^{85}\equiv 32^2\equiv$ *1 mod 341.*

Como nem a primeira potência é congruente a 1 mod 341, nem alguma delas é congruente a -1 mod 341, então 2 é testemunha de que 341 é composto.

Exemplo 5.158. *Se n=25 temos que n-1=24=*2^3*3 onde d=3 e 0≤s<3. Calculando as potências para b = 7 obtemos:*

$7^{2^0 3}= 7^3\equiv$ *18 mod 25,* $7^{2^1 3}= 7^6\equiv$*24 mod 25*

e $7^{2^2 3}= 7^{12}\equiv$ *1 mod 25.*

Vemos que 7^3 *não é congruente 1 mod 25, mas temos que* $7^6\equiv$ *24 mod 25 e*

24≡ -1 mod 25. Portanto, 25 é um pseudoprimo forte *para base 7, embora saibamos que 25 é composto.*

5.36.6 Teste de Primalidade *AKS*

Definição 5.159. *Um algorítmo é chamado de tempo polinomial se existirum polinômio f(X), tal que para todo N o tempo necessário para executá-lo, quando o dado inicial é o número N, é limitado por f(N).*

Em 2002, o Professor Manindra Agrawal e dois de seus alunos de graduação, Neeraj Kayal e Nitin Saxena, descobriram um algorítmo determinístico de tempo polinomial para testar se um número é primo ou composto. Esta equipe de jovens pesquisadores do Instituto Indiano de Tecnologia de Kampur, resolveu um problema em Teoria dos Números e Ciência da Computação que desafiou as melhores mentes por décadas. O *AKS* é o primeiro algoritmo determinístico a executar um teste de primalidade em tempo polinomial. O algoritmo *AKS* é baseado na identidade $(X-a)^n \equiv (X^n-a)\ mod\ n$ a qual é verdadeira somente se n é primo. Esta identidade é uma generalização do Teorema de Fermat estendido para polinômios e pode ser provada usando o Teorema Binomial [4] , juntamente com o fato de que $\binom{n}{k} \equiv 0\ mod\ n$ para todo $0 < k < n$ se n é primo.

O *AKS* faz uso da equivalência $(X^n-a) \equiv\ X^n+a(mod\ X^r-1, n)$ a qual pode ser verificada em tempo polinomial. Enquanto todos os primos satisfazem esta equivalência alguns números compostos também a satisfazem. Para corrigir este problema mostra-se que para escolhas apropriadas de r, a equação é satisfeita para vários $a's$ e logo n deverá ser uma potência de um primo. O número de $a's$ e r apropriados são ambos limitados por um polinômio em logn e desta forma, conseguiu-se um *algoritmo determinístico em tempo polinomial.*

Após dois anos da divulgação do artigo *Primes is in P*, onde os pesquisadores indianos detalham o algoritmo, já existem versões
otimizadas e generalizadas.

5.37 Conclusão

Neste mini-curso apresentamos e desenvolvemos alguns fudamentos matemáticos dos Criptosistemas de Chave Pública, além de mostrar que os resultados mais interessantes e curiosos sobre números primos foram obtidos com a utilização do computador, e que o Pequeno Teorema de Fermat é fundamental na criação de testes de primalidade mais modernos.

Referências

[1] ANDERSON, M.A. e BELL, J.M., *Number Theory with Applications,* PRENTICE HALL, New Jersey, 1997.

[2] COUTINHO, S.C., *Números Inteiros e Criptografia RSA,* IMPA/SBM, Série de Computação e Matemática, Rio de Janeiro, 1997.

[3] COUTINHO, S.C., *Primalidade em Tempo Polinomial,* SBM, Coleção Iniciação Científica, Rio de Janeiro, 2004.

[4] HEFEZ, A. e VILELA, M.L.T., *Elementos de Aritmética ,* SBM, Rio de Janeiro, 2006.

[5] KRANAKIS, E. *Prmality and Cryptography,* Teubner, Chichester, New York, Brisbane, Toronto, Singapore: Wiley, 1986.

[6] *Divisibilidade e Números Inteiros,* OBMEP 2005.

[7] ARNAULT, F. , *Rabin-Miller Primality Test: Composite Numbers Which Pass It,* American Mathematical Society, 1995.

[8] AGRAWAL, M.,KAYAL, N. e SAXENA, N., *Primes is in P,* Annals of Mathe matics, 160 (2004), 781-793.

[9] RIBENBOIM ,P., *Números Primos: mistérios e recordes ,* IMPA, Coleção Matemática Universitária, Rio de Janeiro, 2001.

[10] SAUTOY, M., *A Música dos Números Primos,* Editora ZAHAR, Rio de Janeiro, 2003.

[11] SHKLARSKY, D.O., CHENTZOV, N.N. e YAGLOM, I.M.,*THE USSR OLYMPIAD PROBLEM BOOK,* DOVER PUBLICATION, INC, New York, 1994.

[12] ALENCAR FILHO.E., *Teoria Elementar dos Números*, Editora Nobel, São Paulo, 1985.

MC10 - Tópicos em passeios aleatórios

Valdivino Vargas Júnior

USP, Rua do Matão, 1010 - Cidade Universitária

05508-090 São Paulo - SP

E-mail: vvjuniorusp@yahoo.com.br

7.38 Introdução

Considere a seguinte situação hipotética. Um jogador entra em um cassino com X reais em dinheiro para "tentar a sorte". Admita que ele participa de um jogo que consiste de apostas independentes. Em cada aposta ele recebe um real em caso de vitória e caso contrário perde um real. A chance de vitória em cada aposta é p e conseqüentemente de derrota 1-p = q. Admita que os recursos do cassino são ilimitados, isto é, por mais sorte que o jogador tenha, não consegue "quebrar a banca". Suponha que ele jogue indefinidamente, apenas parando em caso de ficar sem dinheiro. Uma questão interessante é saber qual é a probabilidade do jogador em algum momento ficar sem dinheiro. A teoria mostra que mesmo no caso de um "cassino justo"(isto é, p = 0.5), esta probabilidade é 1. Tal problema é conhecido como ruína do jogador. Entretanto, é bom ressaltar que no caso de o jogador ter probabilidade p superior a 50 por cento em cada aposta existe probabilidade positiva do jogador nunca ficar sem dinheiro.

Este é apenas um simples exemplo de processos que podem ser estudados a partir da teoria de passeios aleatórios. Estes são a formalização matemática de uma trajetória (de uma partícula, digamos) a partir de uma seqüência de passos dados de forma aleatória. Diversas áreas do conhecimento como estatística, economia, computação, ecologia, dentre outras fazem uso de resultados oriundos desse majestoso modelo.

Definição 7.160. *Sejam $X_1, X_2, \cdots$ variáveis aleatórias independentes e identicamente distribuídas tal que $E|\ X_i\ | < \infty$. Seja $S_0 = C$ e*

$$S_n = S_0 + \sum_{i=1}^{n} X_i, n \geq 1.$$

O processo $\{S_n, n \geq 0\}$ é chamado passeio aleatório.

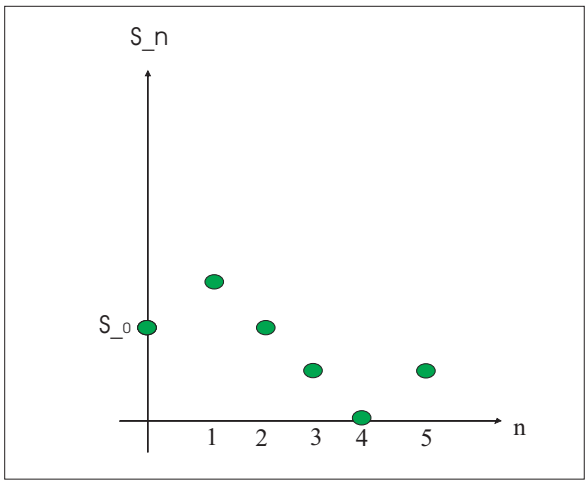
Exemplo 7.161. *Sejam $X_1, X_2, \cdots$ variáveis aleatórias independentes e identicamente distribuídas tal que*

$$\mathbb{P}(X_i = 1) = p \text{ e } \mathbb{P}(X_i = -1) = 1 - p = q.$$

Temos um passeio aleatório simples. Se além disso, $p = q$ temos um passeio aleatório simples simétrico.

Figura 7.2. *Uma realização de um passeio aleatório simples.*

Nesta figura, as elipses representam sucessivas posições do passeio. Nesse caso, $S_0 = 2, S_1 = 3, S_2 = 2$ e assim por diante. O passeio visita a origem no quarto passo. A nomenclatura segue da visualização de S_n como a posição de uma partícula inicialmente em S_0, e então faz uma série de passos unitários independentes, cada passo sendo positivo com probabilidade p ou negativo com probabilidade 1-p. Em alguns momentos usaremos a notação (0,S_0) para (n,S_n) para dizer que um passeio partiu de S_0 no instante 0 e está em S_n no instante n.



É fácil ver que na dinâmica da ruína do jogador, o capital acumulado pelo jogador ao longo das apostas pode ser visto como um passeio aleatório simples. Nesse caso, a variável aleatória X_i representa o ganho do jogador na i-ésima jogada.

Exemplo 7.162. *Defina* $S_0 = i$, $i > 0$ *e*

$$S_{n+1} = 0, \text{ se } S_n = 0 \text{ e}$$
$$S_{n+1} = S_n + X_{n+1} \text{ se } S_n \neq 0, \text{ onde } \mathbf{P}(X_{n+1} = 1) = \mathbf{P}(X_{n+1} = -1) = \frac{1}{2}$$

Temos um passeio aleatório com barreira absorvente na origem.

Exemplo 7.163. *Considere o espaço de estados* $\{0, 1, \cdots, d\}$ *e variáveis aleatórias independentes entre si tais que*

$$\text{Se } S_n \in \{1, 2, \cdots, d-1\} \text{ então } \mathbf{P}(X_{n+1} = 1) = p \text{ e } \mathbf{P}(X_{n+1} = -1) = 1 - p = q$$
$$\text{Se } S_n = 0 \text{ então } \mathbf{P}(X_{n+1} = 1) = p \text{ e } \mathbf{P}(X_{n+1} = 0) = 1 - p = q$$
$$\text{Se } S_n = d \text{ então } \mathbf{P}(X_{n+1} = 0) = p \text{ e } \mathbf{P}(X_{n+1} = -1) = 1 - p = q$$

Temos um passeio aleatório com barreiras de retenção.

Exemplo 7.164. *Seja* $(X_n, n \geq 1)$ *uma coleção de variáveis aleatórias independentes tais que*

$$\mathbf{P}(X_{n+1} = 1) = \lambda_n$$
$$\mathbf{P}(X_{n+1} = -1) = \mu_n$$

onde

$$\lambda_n + \mu_n = 1.$$

Temos um passeio aleatório não homogêneo.

Exemplo 7.165. *Considere uma partícula realizando movimentos aleatórios sobre os vértices de um cubo. Seja* $S = \{i : 1 \leq i \leq 8\}$ *os vértices do cubo e*

$$\mathbf{P}(S_{n+1} = j | S_n = i) = \frac{1}{3} \text{ se } i \text{ e } j \text{ estão conectados e}$$
$$\mathbf{P}(S_{n+1} = j | S_n = i) = 0 \text{ caso contrário.}$$

Temos um passeio aleatório no cubo. Neste, a cada passo a partícula escolhe saltar para um vértice vizinho, tendo a mesma probabilidade de salto para cada um deles.

Exemplo 7.166. *Sejam $(X_n, n \geq 1)$ variáveis aleatórias assumindo valores reais tal que*

$$\mathbf{P}(X_n \leq x) = \Gamma(-\infty, x).$$

Tome $S_{n+1} = S_n + X_{n+1}$. Temos um passeio aleatório sobre a reta.

7.39 Conceitos básicos

7.39.1 Definições

Destacaremos nessa seção alguns conceitos importantes.

Definição 7.167. *Primeira passagem de i para k.*
Seja um passeio aleatório, onde $S_0 = i$. O tempo de primeira passagem é definido por

$$T_{i,k} = \min\{n > 0; S_n = k\}$$

Quando $i = k$, a variável aleatória $T_{k,k}$ é chamada tempo de recorrência de k. Neste caso nós escreveremos simplesmente T_k.

Uma propriedade interessante do tempo de primeira passagem no caso de passeios aleatórios simples é que os passos após a primeira passagem em k é independente das passagens anteriores. Assim, nós podemos escrever, por exemplo

$$T_{0,2} = T_{0,1} + T_{1,2},$$

onde $\mathrm{T}_{0,1}$ e $\mathrm{T}_{1,2}$ são independentes e têm a mesma distribuição já que as X_i são identicamente distribuídas.

Definição 7.168. *Range.*
O range R_n do passeio é a quantidade de valores distintos que o passeio assume até o passo n. Isto é, o número de valores distintos em $(S_0, S_1, ..., S_n)$

Definição 7.169. *Tempo de parada.*
Sejam $X_1, X_2, \cdots$ uma seqüência de variáveis aleatórias independentes. Uma variável aleatória N é dita tempo de parada para esta seqüência se o evento $\{N = n\}$ é independente de $X_{n+1}, X_{n+2}, \cdots$ para todo n=1,2,$\cdots$

No caso de um passeio aleatório o tempo de primeira passagem é um exemplo de tempo de parada. Intuitivamente falando, assistindo ao processo é possível saber o instante em que T_j ocorre. Em outras palavras, se $\{T_j = n\}$ nós paramos após observar $X_1, ..., X_n$ e antes de observar $X_{n+1}, X_{n+2}, ...$

Teorema 7.170. ***Equação de Wald***
Se $X_i i \geq 1$ são v.a.i.i.d. tal que $E|X_i| < \infty$ e se N é um tempo de parada para $X_1, X_2, \cdots$ com E[N] $< \infty$, então

$$E[\sum_{i=1}^{N} X_i] = E[N]E[X_1].$$

Exemplo 7.171. *Considere um passeio aleatório simples assimétrico com $p > \frac{1}{2}$. O número esperado de passos até o passeio alcançar a posição k, $k > 0$ é*

$$E[N] = \frac{k}{2p-1}$$

Demonstração. Observe que $E|X_1| = 1 < \infty$. Além disso

$$\sum_{j=1}^{N} X_j = k \Rightarrow E[\sum_{j=1}^{N} X_j] = k$$

Como $E(X_1) = 2p - 1$ basta usar a equação de Wald para obter o resultado. □

7.39.2 Recorrência e transiência

Seja $(\mathrm{S}_n, n \geq 0)$ um passeio aleatório. Nós dizemos que um estado i é recorrente se

$$\mathbf{P}(S_n = i \text{ para infinitos n }) = 1$$

Nós dizemos que um estado i é transiente se

$$\mathbf{P}(S_n = i \text{ para infinitos n }) = 0$$

Introduza agora o número de visitas V_i ao estado i. Temos:

$$V_i = \sum_{n=0}^{\infty} 1_{\{S_n = i\}}$$

Então

$$E(V_i) = E(\sum_{n=0}^{\infty} 1_{\{S_n=i\}}) = \sum_{n=0}^{\infty} E(1_{\{S_n=i\}}) = \sum_{n=0}^{\infty} \mathbf{P}(S_n = i).$$

Introduza também a probabilidade de retorno

$$f_i = \mathbf{P}(T_i < \infty)$$

É possível mostrar que

$$\text{se } \mathbf{P}(T_i < \infty) = 1, \text{ então i é recorrente e}$$
$$\text{se } \mathbf{P}(T_i < \infty) < 1 \text{ então i é transiente.}$$

Além disso, todo estado, ou é recorrente ou é transiente. Por fim, podemos afirmar que para um estado recorrente a probabilidade de um eventual retorno é 1 enquanto que num estado transiente existe probabilidade de nunca haver retorno.

Proposição 7.172. *Para qualquer passeio aleatório, as seguintes afirmações são equivalentes:*

$$i) f_0 = \mathbf{P}(T_0 < \infty) = 1$$
$$ii) \mathbf{P}(S_n = 0 \textit{ infinitas vezes }) = 1$$
$$iii) \sum_{n=0}^{\infty} \mathbf{P}(S_n = 0) = \infty.$$

Demonstração. Exercício. □

7.40 Passeio Aleatório Simples

Ao longo dessa seção

$$S_n = \sum_{i=1}^{n} X_i, n \geq 1$$

é um passeio aleatório simples. Estamos assumindo sem perda de generalidade, $S_0 = 0$.

7.40.1 Resultados elementares

Teorema 7.173.

$$\mathbf{P}(S_n = k) = \left(\begin{array}{c} n \\ \frac{n+k}{2} \end{array} \right) p^{\frac{n+k}{2}} (1-p)^{\frac{n-k}{2}}$$

Demonstração. Considere uma realização do passeio aleatório de (0,0) para (n,S_n) com r passos positivos e s passos negativos. Se S_n = k então r-s = k e r+s=n. Logo r = $\frac{n+k}{2}$ e s = $\frac{n-k}{2}$. O número de tais realizações é $\left(\begin{array}{c} n \\ r \end{array} \right)$ e cada uma tem a mesma probabilidade, a saber $p^r q^s$. Então

$$\mathbf{P}(S_n = k) = \left(\begin{array}{c} n \\ r \end{array} \right) p^r q^s$$

□

Teorema 7.174. *O passeio aleatório simples simétrico em $\mathbb{Z}$ (p=q= $\frac{1}{2}$) é recorrente.*

Demonstração. Basta mostrar que o estado 0 é recorrente. Sem perda de generalidade assuma $S_0 = 0$. Então, usando a Proposição 7.172 precisamos mostrar que

$$\sum_{n=0}^{\infty} \mathbf{P}(S_n = 0) = \infty$$

É claro que não podemos retornar a 0 em um número ímpar de passos. Isto é

$$\mathbf{P}(S_{2n+1} = 0) = 0 \text{ para todo n.}$$

Note que qualquer seqüência de passos de tamanho 2n de 0 para 0 é constituída de n passos para cima e n passos para baixo e ocorre com probabilidade $(0,5)^n(0,5)^n = (0,25)^n$. Além disso, observe que existem $\left(\begin{array}{c} 2n \\ n \end{array} \right)$ modos de escolher n passos dentre 2n. Então

$$\mathbf{P}(S_{2n} = 0) = \left(\begin{array}{c} 2n \\ n \end{array} \right) (0,25)^n$$

Entretanto, a fórmula de Stirling nos dá uma boa aproximação de $n!$ para n grande:

$$n! \sim \sqrt{2\pi n}(\frac{n}{e})^n \text{ onde } a_n \sim b_n \text{ significa } \frac{a_n}{b_n} \to 1$$

Assim, para algum N suficientemente grande e todo $n \geq N$

$$\mathbf{P}(S_{2n} = 0) \geq \frac{1}{2\sqrt{2\pi}\sqrt{n}}$$

Assim

$$\sum_{n=N}^{\infty} \mathbf{P}(S_{2n} = 0) \geq \sum_{n=N}^{\infty} \frac{1}{2\sqrt{2\pi}\sqrt{n}} = \infty$$

e o passeio é recorrente. □

7.40.2 Dualidade em Passeios aleatórios e Princípio da reflexão

Afirmação 7.1. ***Princípio da dualidade***
$(X_1, X_2, \cdots, X_n)$ tem a mesma distribuição conjunta de $(X_n, X_{n-1}, \cdots, X_1)$

A validade do princípio da dualidade é imediata já que as X_i, $i > 1$ são independentes e identicamente distribuídas.

Proposição 7.175. ***Princípio da Reflexão***
Se x e y são positivos então o número de passeios de (0,x) para (n,y) que tocam o eixo x é igual ao número de passeios de (0,-x) para (n,y).

Demonstração. Exercício. □

Teorema 7.176. ***Teorema do Primeiro acerto***
Seja $b > 0$. Então num passeio aleatório simples

$$\mathbf{P}(T_{0,b} = n) = \frac{b}{n}\mathbf{P}(S_n = b)$$

Demonstração. Seja $N_n(0, x)$ o número de realizações possíveis de (0,0) para (n,x) (número de passeios de comprimento n saindo de 0 e chegando a x). Seja ainda $N_n^b(0, x)$ o número de realizações possíveis de (0,0) para (n,x) que passam em b pelo menos uma vez. Observe que se $T_{0,b} = n$ então $X_n = 1$ e $S_{n-1} = b - 1$. Então existem $N_{n-1}(0, b-1)$ passeios de (0,0) para $(n-1, b-1)$ dos quais $N_{n-1}^b(0, b-1)$ visitam b no trajeto. Cada uma dessas realizações tem probabilidade $p^{\frac{n+b}{2}-1}q^{\frac{n-b}{2}}$. Usando o Princípio da reflexão:

$$\begin{aligned}\mathbf{P}(T_{0,b} = n) &= p(N_{n-1}(0, b-1) - N_{n-1}(0, b+1))p^{\frac{n+b}{2}-1}q^{\frac{n-b}{2}} \\ &= [\binom{n-1}{\frac{n+b}{2}-1} - \binom{n-1}{\frac{n+b}{2}}]p^{\frac{n+b}{2}}q^{\frac{n-b}{2}} = \frac{b}{n}\mathbf{P}(S_n = b)\end{aligned}$$

□

O resultado a seguir mostra uma interessante propriedade do passeio aleatório simples simétrico.

$$\mathbf{P}(T_{0,1} < \infty) = 1, \text{ porém } E[T_{0,1}] = \infty$$

Proposição 7.177. *Num passeio aleatório simples simétrico*

$$E[T_{0,1}] = \infty$$

Demonstração.

$$E(T_{0,1}) = \sum_{m=0}^{\infty}\mathbf{P}(S_{2m+1} = 1) = \sum_{m=0}^{\infty}\binom{2m+1}{m+1}2^{-(2m+1)} = \infty$$

□

Teorema 7.178. ***Teorema de Ballot***
Seja S_n um passeio aleatório simples com $S_0 = 0$. Então

$$\mathbf{P}(\prod_{i=1}^{2n-1} S_i \neq 0 | S_{2n} = 2r) = \frac{r}{n}$$

Demonstração. A prova é semelhante a da prova do teorema do primeiro acerto. Conte o número $\mathrm{N}^0_{2n-1}(1,2r)$ de realizações de (1,1) para (2n,2r) que visitam a origem. A idéia é refletir o passeio antes de seu primeiro 0 no eixo x, e assim mostrar que $\mathrm{N}^0_{2n-1}(1,2r) = \mathrm{N}_{2n-1}(-1,2r)$. Como todas as $\mathrm{N}_{2n}(0,2r)$ realizações são igualmente prováveis, a probabilidade requerida é

$$\frac{N_{2n-1}(1,2r) - N^0_{2n-1}(1,2r)}{N_{2n}(0,2r)} = \frac{N_{2n-1}(1,2r) - N_{2n-1}(-1,2r)}{N_{2n}(0,2r)} = \frac{r}{n}$$

□

Exemplo 7.179. *Considere a seguinte situação. Em uma eleição após a contagem dos votos o candidato A garante a votos e o candidato B, b votos. Suponha $a > b$. Qual a probabilidade de que o candidato A liderou durante toda a contagem? O Teorema de Ballot diz que esta probabilidade é*

$$\frac{a-b}{a+b}.$$

O próximo resultado parece surpreendente porém é verdadeiro.

Teorema 7.180. *Seja $S_n, n \geq 0$ um passeio aleatório simples simétrico com $S_0 = 0$. Então*

$$\begin{aligned} &a)\ \mathbf{P}(T_0 = 2n) = \mathbf{P}(S_{2n-2} = 0) - \mathbf{P}(S_{2n} = 0) \\ &b)\ \mathbf{P}(\prod_{k=1}^{2n} S_k \neq 0) = \mathbf{P}(T_0 > 2n) = \mathbf{P}(S_{2n} = 0) \end{aligned}$$

Demonstração. Primeiro o item a. Pela simetria, princípio da reflexão e usando o teorema do primeiro acerto

$$\begin{aligned} \mathbf{P}(T_0 = 2n) &= \frac{1}{2n-1}\mathbf{P}(S_{2n-1} = 1) = \frac{2^{-(2n-1)}}{2n-1}\begin{pmatrix} 2n-1 \\ n \end{pmatrix} \\ &= \frac{2^{-2n}}{2n-1}\begin{pmatrix} 2n \\ n \end{pmatrix} = 2^{-2n+2}\begin{pmatrix} 2n-2 \\ n-1 \end{pmatrix} - 2^{-2n}\begin{pmatrix} 2n \\ n \end{pmatrix} \\ &= \mathbf{P}(S_{2n-2} = 0) - \mathbf{P}(S_{2n} = 0) \end{aligned}$$

Para o item b, observe que

$$\begin{aligned} \mathbf{P}(T_0 > 2n) &= 1 - \sum_{k=1}^{n} P(T_0 = 2k) = \sum_{k=1}^{n}[\mathbf{P}(S_{2k-2} = 0) - \mathbf{P}(S_{2k} = 0)] \\ &= \mathbf{P}(S_{2n} = 0) \end{aligned}$$

□

O próximo teorema lida com a taxa esperada na qual um passeio aleatório assume novos valores.

Teorema 7.181.

$$\lim_{n\to\infty} \frac{E(R_n)}{n} = \mathbf{P}(\textit{ passeio aleatório nunca retorna a 0})$$

Demonstração. Defina

$$I_k = \begin{cases} 1 \text{ se } S_k \neq S_{k-1}, S_k \neq S_{k-2}, \cdots S_k \neq S_0, \\ 0 \text{ caso contrário} \end{cases}$$

Então

$$R_n = \sum_{k=1}^{n} I_k$$

Logo

$$\begin{aligned} E[R_n] &= 1 + \sum_{k=1}^{n} \mathbf{P}(I_k = 1) = 1 + \sum_{k=1}^{n} \mathbf{P}(S_k \neq S_{k-1}, S_k \neq S_{k-2}, \cdots S_k \neq S_0) \\ &= 1 + \sum_{k=1}^{n} \mathbf{P}(X_k \neq 0, X_k + X_{k-1} \neq 0, \cdots X_k + X_{k-1} + \cdots + X_1 \neq 0) \\ &= 1 + \sum_{k=1}^{n} \mathbf{P}(X_1 \neq 0, X_1 + X_2 \neq 0, \cdots X_1 + X_2 + \cdots + X_k \neq 0) \end{aligned}$$

onde a última desigualdade segue da dualidade. Logo

$$E[R_n] = 1 + \sum_{k=1}^{n} \mathbf{P}(S_1 \neq 0, S_2 \neq 0, \cdots S_k \neq 0) = \sum_{k=0}^{n} \mathbf{P}(T_0 > k)$$

onde T_0 é o tempo do primeiro retorno a 0. Tomando $k \to \infty$

$$\mathbf{P}(T_0 > k) \to \mathbf{P}(T_0 = \infty) = \mathbf{P}(\text{passeio aleatório nunca retorna a 0})$$

Daí segue

$$\lim_{n\to\infty} \frac{E(R_n)}{n} = \mathbf{P}(\text{passeio aleatório nunca retorna a 0})$$

□

Corolário 7.182. *Considere um passeio aleatório simples assimétrico, com* $p > \frac{1}{2}$

$$\lim_{n\to\infty} \frac{E(R_n)}{n} = 2p - 1$$

Demonstração. Exercício. □

Teorema 7.183. *Em um passeio aleatório simples simétrico o número esperado de visitas ao estado k antes de retornar a origem é igual a 1 para todo* $k \neq 0$.

Demonstração. Para k > 0 seja Y o número de visitas ao estado k antes do primeiro retorno a origem. Y pode ser escrito da seguinte forma

$$Y = \sum_{n=1}^{\infty} I_n$$

onde

$$I_n = \begin{cases} 1 \text{ se k é visitado no tempo n e não há retorno a origem antes de n} \\ 0 \text{ caso contrário} \end{cases}$$

Ou de modo equivalente:

$$I_n = \begin{cases} 1 \text{ se } S_n > 0, S_{n-1} > 0, \cdots S_1 > 0, S_n = k, \\ 0 \text{ caso contrário} \end{cases}$$

Logo

$$\begin{aligned} E[Y] &= \sum_{n=1}^{\infty} \mathbf{P}(S_n > 0, S_{n-1} > 0, \cdots, S_n = k) \\ &= \sum_{n=1}^{\infty} \mathbf{P}(X_n + \cdots + X_1 > 0, X_{n-1} \cdots + X_1 > 0, \cdots X_1 = 0, X_n + \cdots + X_1 = k) \\ &= \sum_{n=1}^{\infty} \mathbf{P}(X_1 + \cdots + X_n > 0, X_2 \cdots + X_n > 0, \cdots X_n = 0, X_1 + \cdots + X_n = k) \end{aligned}$$

onde a última igualdade segue da dualidade. Portanto

$$\begin{aligned} E[Y] &= \sum_{n=1}^{\infty} \mathbf{P}(S_n > 0, S_n > S_1, \cdots S_n > S_{n-1}, S_n = k) \\ &= \sum_{n=1}^{\infty} \mathbf{P}(\text{passeio aleatório simétrico acertar k a primeira vez no tempo n}) \\ &\mathbf{P}(\text{passeio aleatório sempre alcançar k}) = 1 \text{ (pela recorrência).} \end{aligned}$$

□

7.40.3 O problema da ruina do jogador

Agora voltaremos nossa atenção para o problema da ruína do jogador descrito na introdução. Lembre que na dinâmica da ruína do jogador, o capital acumulado pelo jogador ao longo das apostas pode ser visto como um passeio aleatório. Nesse caso, a variável aleatória X_i representa o ganho do jogador na i-ésima jogada. Vamos mostrar que mesmo estando em um"cassino justo", com probabilidade 1, o jogador fica sem dinheiro em algum momento.

Demonstração. Seja $h_i = \mathbf{P}_i$(acertar 0). Então h é a solução minimal não negativa de

$$\begin{aligned} h_0 &= 1 \\ h_i &= \frac{1}{2}h_{i+1} + \frac{1}{2}h_{i-1} \text{ para i=1,2,...} \end{aligned}$$

Essa relação de recorrência tem solução geral

$$h_i = A + Bi$$

Mas a restrição $0 \leq h_i \leq 1$ força B = 0. Assim, $h_i = 1$ para todo i. Dando o resultado desejado. □

7.41 Aplicações atuais em passeios aleatórios- Frog model

Dentre uma variedade enorme de trabalhos envolvendo passeios aleatórios apresentaremos como exemplo o modelo dos sapos (Frog Model). Este é um sistema de passeios aleatórios simples sobre um grafo. Este modelo pode ser descrito da seguinte forma. Existem partículas ativas e inativas sobre algum grafo. Cada partícula ativa realiza um passeio aleatório simples a tempo discreto. Quando uma partícula ativa salta sobre uma inativa, esta se torna ativa passando então a realizar um passeio aleatório simples a tempo discreto. No frog model existem algumas variações sobre a maneira pela qual uma partícula ativa desaparece. Em "Phase transition for the frog model"por exemplo, cada partícula ativa tem probabilidade 1-p de desaparecer a cada passo de seu passeio. A seguir apresentaremos a descrição de alguns artigos

recentes envolvendo o frog model. A bibliografia completa destes artigos se encontra nas referências.

Random walks systems with killing em $\mathbb{Z}$

Considere um sistema de passeios aleatórios sobre $\mathbb{Z}$ na qual cada partícula ativa realiza um passeio aleatório simples assimétrico e ativa todas as partículas inativas que encontra. O movimento de uma partícula pára quando ela alcança um certo número de saltos sem ativar nenhuma partícula. Neste artigo é provado que se o processo conta com partículas eficientes (pequena probabilidade de salto para à esquerda) localizadas estrategicamente sobre $\mathbb{Z}$ o processo pode sobreviver, tendo partículas ativas em qualquer instante com probabilidade positiva. Caso contrário, é construído um processo que mesmo contanto com partículas eficientes morre quase certamente. Isto é o que acontece se as partículas estiverem localizadas inicialmente muito longe das outras ou se a sua probabilidade de salto para à direita tende a 1, porém não tão rápido.

CLT for the infected proportion of individuals for an epidemic model on a complete graph

Neste artigo, os autores provam um teorema central do limite para a proporção de indivíduos infectados para um modelo epidêmico constituído por um sistema de passeios aleatórios simples a tempo discreto sobre um grafo completo com n vértices. Cada passeio aleatório faz o papel de um vírus. Um vírus duplica em cada instante em que encontra um indivíduo susceptível e morre se acertar um indivíduo já infectado. O processo pára quando não existem mais vírus. Indivíduos estão todos conectados como vértices em um grafo conexo. Este modelo é próximo a alguns problemas em epidemiologia e disseminação de vírus em uma rede de computador.

The shape theorem for frog model

Neste artigo, os autores provam um teorema de forma para um conjunto crescente de passeios aleatórios simples sobre $\mathbb{Z}^d$. A dinâmica do processo é a seguinte. Existem partículas ativas que realizam passeio aleatório simples a tempo discreto e partículas inativas que não se movem. Quando uma partícula inativa é acertada por uma ativa ela também se torna ativa. No tempo 0, todas as partículas estão inativas, exceto aquela localizada na origem. Os autores provam que o conjunto das posições originais de todas as partículas reescalada pelo tempo converge para algum conjunto convexo compacto.

Phase transition for the frog model

Neste artigo, têm-se um sistema de passeios aleatórios simples sobre um grafo. Existem partículas ativas e inativas sobre o grafo. Cada partícula ativa realiza um passeio aleatório simples a tempo discreto e em cada movimento desaparece com probabilidade 1-p. Quando uma partícula ativa acerta uma partícula inativa, esta se torna ativa. Os autores apresentam resultados de transição de fase e valores assintóticos para parâmetros críticos para $\mathbb{Z}^d$ e árvores regulares.

Self avoiding random walks on homogeneous trees

Neste artigo, os autores consideram um sistema de partículas sobre uma árvore homogênea. No tempo 0 existe uma única partícula sobre cada vértice da árvore estando apenas uma delas ativa. As outras

se encontram inativas. Uma partícula ativa realiza um passeio aleatório simples a tempo discreto independente, tendo probabilidade 1-p de desaparecer em cada passo. Uma partícula inativa se torna ativa quando seu vértice é acertado por uma partícula ativa. Os autores provam resultado de transição de fase para esse modelo exibindo limites para a probabilidade crítica. A criticalidade é com respeito a positividade da probabilidade do evento existir partículas ativas em qualquer instante.

Random walk systems on complete graphs

Neste artigo, os autores estudam duas versões de sistemas de passeios aleatórios sobre grafos completos. No primeiro, os passeios aleatórios têm tempo de vida com distribuição geométrica. Neste caso, é identificado um parâmetro crítico relacionado a proporção de vértices visitados antes do processo morrer. Na segunda versão, o tempo de vida dos passeios dependem do passado do processo de modo não markoviano. Para esta versão são apresentados resultados obtidos de análise computacional, simulações e aproximações de campo médio.

Referências

[1] D. Stirzaker, Elementary Probability, Cambridge University Press, 2003.

[2] F.P. Machado, E. Lebensztayn, M. Z. Martinez (2005) Self avoiding random walks on homogeneous trees

[3] F.P. Machado, E. Lebensztayn, M. Z. Martinez (2008) Random walks systems with killing em $\mathbb{Z}$

[4] F.P. Machado, H. Mashurian, H. Matzinger (2008) CLT for the infected proportion of individuals for an epidemic model on a complete graph

[5] J. Norris, Markov Chains, Cambridge University Press, 1996.

[6] R. Durret, Probability: theory and examples, (2nd edn.), Duxburry, Belmont. Calif.

[7] O.S.M. Alves, F.P. Machado, E. Lebensztayn, M. Z. Martinez (2006) Random walk systems on complete graphs

[8] O.S.M. Alves, F.P. Machado, S.Yu. Popov (2002)Phase transition for the frog model.

[9] .S.M. Alves, F.P. Machado, S.Yu. Popov (2000) The shape theorem for the frog model.

[10] S.H. Ross, Stochastic Processes, Wiley Series in Probability and Mathematical Statistics, 1996.

[11] W. Feller, An Introduction to Probability Theory and its Applications, Wiley, New York,1966.

MC11 - O Lema de Lax-Milgram e Aplicações

Maurílio Márcio Melo

IME/UFG - Campus II

74001-970, Goiânia - GO

E-mail: melo@mat.ufg.br

6.42 Introdução

O principal objetivo destas notas é apresentar algumas técnicas usadas em análise para resolver problemas envolvendo equações diferenciais parciais lineares e não linerares. Apresentaremos e faremos a demonstração do lema de Lax-Milgram em espaços de Hilbert e logo a seguir faremos três aplicações. As duas ferramentas principais a serem usadas no texto são o teorema da representação de Riesz, que pode ser encontrado na referência [13] e o teorema do ponto fixo de Schauder, que pode ser encontrado, por exemplo, nas referências [5] ou [9]. Os conhecimentos básicos para a leitura do texto, embora não são estritamente necessários, são noções de teoria das distribuições e espaços usuais de Sobolev, que podem ser encontrados, por exemplo, nas referências [8] e [1] respectivamente.

6.43 Notações, Definições e Resultados Básicos

No que segue, denotaremos por $C_c^\infty(\Omega)$, $\Omega \subset R^n$ um aberto, o espaço das funções de classe C^∞ com suporte compacto em Ω. Se $\alpha \in N^n$, $D^\alpha u$ é a derivada no sentido das distribuições de u, isto é, $(D^\alpha u, \varphi) = (-1)^{|\alpha|}\ (u, D^\alpha \varphi)$, $\varphi \in C_c^\infty(\Omega)$ e Δ é o operador laplaciano. Por H^k denotaremos o espaço usual de Sobolev modelado em L^2, isto é, $H^k(\Omega) = \{u \in L^2(\Omega) : D^\alpha u \in L^2(\Omega),\ |\alpha| \leq k\}$. A aplicação

$$H^k \times H^k : (u, v) \mapsto \langle u, v \rangle_k = \sum_{|\alpha| \leq k} \langle D^\alpha u, D^\alpha v \rangle_{L^2},$$

define um produto interno em H^k. O número $\|u\|_k$, definido por

$$||u||_k = \sqrt{\langle u, u \rangle_k}$$

é a norma em H^k que provém do produto interno acima. Definimos também o espaço $H_0^k(\Omega)$ como sendo o fecho em $H^k(\Omega)$, na norma de $\|\cdot\|_k$, do espaço $C_c^\infty(\Omega)$, isto é, $H_0^k(\Omega) = \overline{C_c^\infty(\Omega)}^{\|\cdot\|_k}$. Observemos que $H^k(\Omega)$ e $H_0^k(\Omega)$ são exemplos de espaços de Hilbert, isto é, espaço vetorial normado, onde a norma provém de um produto interno e que é completo em relação à norma.

A seguir enunciaremos e demonstraremos o lema de Lax-Milgram, que pode ser encontrado, por exemplo, nas referências [3] ou [5].

Teorema 6.184. *(O lema de Lax-Milgram) Sejam H um espaço de Hilbert e*

$$B : H \times H \to R, \quad (u, v) \to B(u, v)$$

uma forma bilinear, contínua e coerciva, isto é, linear separadamente em cada coordenada e existem $\alpha,\ \beta > 0$ *tais que*

$$\begin{aligned} 1)|B(u,v)| &\leq \alpha \|u\| \|v\|, \quad u,v \in H \text{ (continuidade)} \\ 2)\ \ \beta \|u\|^2 &\leq B(u,u), \quad u \in H \text{ (coercividade).} \end{aligned}$$

Para todo $F \in H'$ ($F : H \to R$, *linear e contínuo*), *existe um único* $u \in H$ *tal que*

$$B(u,v) = F(v), \quad v \in H.$$

Demonstração: Primeiramente demonstremos a unicidade. Suponhamos que existam $u_1,\ u_2 \in H$, tais que

$$B(u_1,v) = F(v), \quad B(u_2,v) = F(v), v \in H.$$

Da linearidade de B, segundo a primeira variável, temos para qualquer $v \in H$, a igualdade

$$B(u_1 - u_2, v) = 0.$$

Em particular, tomando $v = u_1 - u_2$, obtemos a igualdade

$$B(u_1 - u_2, u_1 - u_2) = 0.$$

Da hipótese (2) sobre B, temos que

$$\beta||u_1 - u_2||^2 = 0,$$

portanto $u_1 = u_2$.

Agora demonstraremos a existência; para isto usaremos o teorema da representação de Riesz em espaços de Hilbert. Fixemos $u \in H$ e definimos a aplicação

$$H :\to R,\ v \to B(u,v).$$

Esta aplicação é linear e contínua. Pelo teorema de Riesz, existe um único $w \in H$ tal que

$$B(u,v) = \langle w, v\rangle,\ v \in H.$$

Isto define uma aplicação

$$A : H \to H,\ u \to w = A(u), \quad \text{isto é,}$$

$$B(u,v) = \langle A(u), v\rangle,\ v \in H.$$

Afirmamos que a aplicação A é linear, contínua e bijetora. Realmente,

$$\begin{aligned} \langle A(u_1+u_2), v\rangle &= B(u_1+u_2,v) = B(u_1,v) + B(u_2,v) \\ &= \langle A(u_1), v\rangle + \langle A(u_2), v\rangle = \langle A(u_1) + A(u_2), v\rangle,\ v \in H. \end{aligned}$$

Portanto

$$A(u_1+u_2) = A(u_1) + A(u_2).$$

Claramente $A(ku) = kA(u)$.

Observemos que

$$||A(u)||^2 = \langle A(u), A(u)\rangle = B(u, A(u) \leq \alpha||u||||A(u)||.$$

De onde obtemos a desigualdade

$$||A(u)|| \leq \alpha||u||.$$

Isto demonstra a continuidade.

Para demonstrar a injetividade de A, primeiramente observemos que

$$||A(u)||||u|| \ \geq |\langle A(u), u\rangle| = |B(u, u)| \geq \beta||u||^2.$$

E portanto, temos a desigualdade

$$||A(u)|| \ \geq \beta||u||. \tag{29}$$

Agora, se $A(u_1) = A(u_2)$, então $A(u_1 - u_2) = 0$, e assim

$$0 = ||A(u_1 - u_2)|| \ \geq \beta||u_1 - u_2||,$$

de onde cocluimos que $u_1 = u_2$.

Para provar a sobrejetividade, denotaremos por $R(A)$ a imagem de A e queremos provar que $R(A) = H$. Mostremos que $R(A)$ é fechado. Seja $w_n \in R(A)$ com $w_n \to w$. Existe $u_n \in H$ tal que $A(u_n) = w_n$. A desigualdade (29) fornece a estimativa

$$||u_n - u_m|| \ \leq \frac{1}{\beta}||A(u_n) - A(u_m)|| = \frac{1}{\beta}||w_n - w_m||.$$

Como $\{w_n\}$ é de Cauchy, temos que $\{u_n\}$ é de Cauchy, e devido a complectude de H, existe $u \in H$ tal que $u_n \to u$. Agora a continuidade de A fornece o diagrama

$$\begin{array}{ccc} w_n & = & A(u_n) \\ & & \downarrow \\ w & = & A(u), \end{array}$$

e portanto $w_n \to w$; assim $R(A)$ é fechado em H. A seguir mostraremos que $R(A)$ é denso em H. Para isto usaremos o seguinte resultado da análise em espaços de Hilbert: *Sejam $V_1 \subset V_2$ espaços de Hilbert. Se $v \in V_2$ é tal que $0 =< v, w >$, $w \in V_1$, então $v = 0$, neste caso V_1 é denso em V_2*. Agora seja $v \in H$, tal que v seja ortogonal a $R(A)$, isto é,

$$0 = \langle A(u), v\rangle, \ u \in H, \text{ mas}$$

$$\langle A(u), v\rangle = B(u, v), \ u \in H.$$

Em particular tomemos $u = v$ e teremos $0 = B(v, v)$ e como $\beta||v||^2 \leq B(v, v) = 0$, segue que $v = 0$. Assim $R(A)$ é denso e fechado em H, portanto $R(A) = H$, o que implica na sobrejetividade do operador A.

Voltemos à demonstração da existência. Como $A : H \to H$ é uma bijeção, seja S o seu inverso, isto é,

$$S : H \to H, \ w \to u = S(w) = A^{-1}(w),$$

(operador solução) que é contínuo, pois

$$||u|| \ \leq \frac{1}{\beta}||A(u)|| \quad \text{e como } A(u) = w, \text{ segue que } S(w) = u \text{ e portanto}$$

$$||S(w)|| \leq \frac{1}{\beta}||w||, \quad ||S|| \leq \frac{1}{\beta}.$$

Isto conclui a demonstração do teorema.

A seguir enunciaremos o teorema do ponto fixo devido a Schauder, que será usado no exemplo 6.188.

Teorema 6.185. *Sejam X um espaço de Banach, $B \subset X$ um conjunto convexo, limitado e fechado e $T : B \to B$ uma transformação contínua e compacta, então existe ponto fíxo, isto é, existe $x \in B$ tal que $T(x) = x$.*

6.44 Aplicações

Exemplo 6.186. *Dado $f \in L^2(\Omega)$, $\Omega \subset R^n$ aberto, o problema*

$$\begin{cases} -\Delta u + u = f, em\ \Omega \\ u = 0, \quad em\ \ \partial\Omega, \end{cases} \tag{30}$$

tem única solução $u \in H_0^1(\Omega)$.

Demonstração: faremos inicialmente a formulação variacional do problema (30). para isto multiplicando a equação por $v \in C_c^\infty(\Omega)$, em seguida integrando em Ω e aplicando integração por partes, obtemos a expressão

$$\int_\Omega \nabla u \cdot \nabla v + \int_\Omega uv = \int_\Omega fv.$$

Chamando

$$B(u, v) = \int_\Omega (\nabla u \cdot \nabla v + uv)dx = \langle u, v \rangle_1, \tag{31}$$

temos que $B : H_0^1 \times H_0^1 \to R$ é bilinear. A desiguadade de Cauchy-Schwartz fornece a estimativa

$$|B(u, v)| \leq ||u||_1||v||_1,$$

assim B é contínua. Fazendo $v = u$ em (31), obtemos que

$$|B(u, u)| = ||u||_1^2,$$

portanto a coercividade de B.

Por outro lado, definindo $F : H_0^1 \to R$, por

$$F(v) = \int_\Omega fvdx,$$

temos, imediatamente que F é linear e contínua e portanto, pelo Lema de Lax-Milgram 6.184, existe uma única $u \in H_0^1(\Omega)$, tal que

$$B(u, v) = F(v), \ v \in H_0^1(\Omega).$$

Esta u é a solução de nosso problema.

Exemplo 6.187. *Dado $f \in L^2(\Omega)$, $\Omega \subset R^n$ aberto limitado, o problema*

$$\begin{cases} -\Delta u = f, \ em\ \Omega \\ u = 0, \quad em\ \partial\Omega, \end{cases} \tag{32}$$

tem única solução $u \in H_0^1(\Omega)$.

Demonstração: Seguindo os mesmos passos do exemplo acima, definimos $B : H_0^1 \times H_0^1 \to R$ e $F : H_0^1 \to R$, respectivamente, por

$$B(u,v) = \int_\Omega \nabla u \cdot \nabla v dx \ \text{ e } \ F(v) = \int_\Omega f v dx.$$

A linearidade e continuidade de F já foram verificadas acima. Claramente B é bilinear e

$$|B(u,v)| = |\int_\Omega \nabla u \cdot \nabla v dx| \ \leq ||u||_1 ||v||_1,$$

produzindo portanto a continuidade de B.Usando a desigualdade de Poincaré, dada abaixo, válida em domínios limitados

$$||u||_k \leq C(\Omega, k) \sum_{|\alpha|=k} \langle D^\alpha u, D^\alpha u \rangle_{L^2}, \ u \in H_0^k(\Omega), \tag{33}$$

temos que

$$B(u,u) = \int_\Omega |\nabla u|^2 = |||\nabla u|||_{L^2}^2 \geq \frac{1}{C(\Omega)} ||u||_1^2.$$

Concluimos portanto, que B é coerciva. A solução do problema (32) é obtida via o teorema de Lax-Milgram.

A seguir usaremos o Lema de Lax-Milgram para estudar um problema não linear.

Exemplo 6.188. *Consideremos o seguinte problema: Encontrar p e k de modo que dada $f \in L^p(\Omega)$, existe uma única $u \in H_0^k(\Omega)$ tal que*

$$\begin{cases} -\Delta u = f + u^2, \ em \ \Omega \subset R^n \\ \quad u = 0 \quad em \ \partial\Omega. \end{cases} \tag{34}$$

Na tentativa de resolver este problema, dividiremos o procedimento em quatro passos a seguir

1^0 passo: Dada $g \in L^2(\Omega)$, pelo exemplo (6.187), existe uma única solução $w \in H_0^1(\Omega)$, para o problema

$$\begin{cases} -\Delta w = g, \ em \ \Omega \subset R^n \\ \quad w = 0, \quad em \ \partial\Omega. \end{cases}$$

Na realidade, devido à teoria de regularidade, ver [6], a solução w está também em $H^2(\Omega)$ e pela desigualdade de Poincaré (33), temos a estimativa

$$||w||_2 \leq C||g||_{L^2}. \tag{35}$$

2^0 passo: A solução é ponto fixo da seguinte transformação: Dado $v \in E$ (a ser escolhido), seja $w = T(v)$ a solução do problema

$$\begin{cases} -\Delta w = f + v^2, \ em \ \Omega \subset R^n \\ \quad w = 0, \quad em \ \partial\Omega. \end{cases}$$

O ponto fixo u de T, se existir, é solução do problema (34). Observemos que se $v \in H_0^1(\Omega)$, então

$$||v^2||_{L^2} = (\int_\Omega |v|^4)^{1/2} = [(\int_\Omega |v|^4)^{1/4}]^2,$$

e portanto $||v^2||_{L^2} = ||v||_{L^4}^2$ e assim

$$||v^2||_{L^2} \leq C||v||_1^2 < \infty,$$

onde usamos a imersão de Sobolev $H_0^1(\Omega) \subset L^4(\Omega)$, caso particular da imersão $H_0^k(\Omega) \subset L^q(\Omega)$, $2 \leq q \leq \frac{2n}{n-2k}$, quando $n = 3$ e $k = 1$. Assim se $(f + v^2) \in L^2$, o primeiro passo garante que $w \in H_0^1(\Omega)$, portanto temos a aplicação

$$T : H_0^1(\Omega) \to H_0^1(\Omega).$$

3^0 passo: A seguir demonstraremos que a transformação T definida acima tem um ponto fixo. Para isto uzaremos o teorema do ponto fixo de Schauder, teorema 6.185.

Afirmamos que T dada acima é compacta, isto é, se $D \subset H_0^1(\Omega)$ é limitado, então $T(D)$ é relativamente compacto em $H_0^1(\Omega)$. Realmente, se $v \in D$ temos que $w = T(v)$ satisfaz a desigualdade

$$||w||_2 \leq C||f + v^2||_{L^2} \leq .C(||f||_{L^2} + ||v^2||_{L^2}) \leq C(||f||_{L^2} + C||v||_1^2).$$

Como $H^2 \subset H^1$, segue que $T(D)$ é relativamente compacto em $H_0^1(\Omega)$ ($||w||_1 \leq ||w||_2 \leq C(||f||_{L^2} + C||v||_1^2)$.

Afirmamos que T é contínua; realmente, sejam v_1, $v_2 \in H_0^1(\Omega)$, $w_1 = T(v_1)$ e $w_2 = T(v_2)$, avaliemos $||T(v_1) - T(v_2)||_1$. Temos que

$$\begin{cases} -\Delta w_1 = f + v_1^2, \\ -\Delta w_2 = f + v_2^2. \\ (w_1 - w_2)|_{\partial\Omega} = 0. \end{cases}$$

Da estimativa (35), obtemos as desigualdades

$$\begin{aligned} ||w_1 - w_2||_1 &\leq ||w_1 - w_2||_2 \leq C||v_1^2 - v_2^2||_{L^2} \\ &= C[\int_\Omega |v_1 + v_2|^2|v_1 - v_2|^2]^{1/2} \\ &\leq C(\int_\Omega |v_1 + v_2|^4)^{\frac{1}{4}}(\int_\Omega |v_1 - v_2|^4)^{\frac{1}{4}} \\ &= C||v_1 + v_2||_{L4}||v_1 - v_2||_{L4}. \end{aligned}$$

E assim temos a desigualdade

$$||w_1 - w_2||_1 \leq C||v_1 + v_2||_1||v_1 - v_2||_1. \tag{36}$$

4^0 passo: Encontrar um convexo fechado e limitado adequado. Tentemos bolas centradas na origem. Seja $v \in H_0^1(\Omega)$ tal que $||v||_1 \leq R$. Temos que

$$||w||_1 = ||T(v)||_1 \leq ||w||_2 \leq C||f||_{L^2} + C||v||_1^2 \leq C||f||_{L^2} + CR^2 \leq R.$$

Portanto basta escolher R suficientemente pequeno de modo que

$$C||f||_{L^2} + CR^2 - R \leq 0.$$

Observemos que, para que isto ocorra, basta impor a seguinte condição sobre f

$$4C^2||f||_{L^2} < 1.$$

Assim tomando $p = 2$ e $||f||_{L^2}$ suficientemente pequena (satisfazendo a condição acima) o problema (34) tem solução em $H_0^1(\Omega)$.

Resta mostrar a unicidade. Para isto suponhamos que existam duas soluções u_1 e u_2 de (34). Da desigualdade (36), temos que

$$\begin{aligned} ||u_1 - u_2||_1 &\leq C(||u_1||_1 + ||u_2||_1)||u_1 - u_2||_1 \\ &\leq 2CR||u_1 - u_2||_1. \end{aligned}$$

Escolhendo R tal que $2CR \leq 1$ obtemos, da estimativa acima, que

$$||u_1 - u_2||_1 \leq ||u_1 - u_2||_1,$$

e portanto a unicidade.

Agradecimentos

Gostaria de agradecer aos professores do IME-UFG, pelo incentivo recebido para que estas notas viessem a ser escritas e apresentadas na XXIII semana do instituto.

Referências

[1] R. A. Adams, *Sobolev Spaces,* Academic Press, New York, 1975.

[2] J. Barros Neto, *An Introduction to the Theory of Distributions,* Marcel Dekker Inc., New York, 1973.

[3] H. Brezis, *Analyse Fonctionnelle, Masson, Paris, New York, São Paulo, 1987.*

[4] T. Cazenave & A. Haraux, *Introduction aux Problèmes d'Évolution Semi-Linéaires,* Mathematiques & Applications, Ellipses, Paris 1990.

[5] L. C., Evans, *Partial Diferential Equations, Berkeley Mathematics Lecture Notes,* Berkeley, volume 3B,1993.

[6] G. B., Folland, *Introduction to Partial Diferential Equations, Princeton University Press* · Princeton, New Jersey, *2^a Edition*, 1995.

[7] A. Friedman, *Partial Differential Equations,* Holt, Rinehart and Winston, Inc., New York, 1969.

[8] J. Hounie, *Teoria Elementar das Distribuições,* 12o Colóquio Brasileiro de Matemática, IMPA, 1979.

[9] G. Łukaszewicz, *Micropolar Fluids, Theory and Applications,* Birkhäuser, Boston · Basel · Berlin, 1999.

[10] M. M. Melo, *Introdução à Teoria de Semigrupos,* Publicações IME-UFG, Goiânia, 2004.

[11] A. Pazy, *Semigroups of Linear Operators and Applications to Partial Differential Equations*, Springer-Verlag, New York, 1983.

[12] M. Reed & B. Simon, *Functional Analysis,* Academic Press, Inc., vol. 1, New York, 1973.

[13] W.Rudin, *Real and comlex Analysis,* McGraw-Hill Book Company, New York, 1966.

[14] L. Schwartz, *Théorie des distributions.* Nouvelle ed. Hermann, Paris, 1966.

MC12 - Mapas Mentais como Ferramenta da Apoio a Aprendizagem.

Edinaldo Augusto Lemes Garcia

IME/EEEC-UFG

74001-970, Goiânia - GO

E-mail: prof.edgarcia@gmail.com

1. Conceito: Epistemologia, Ontologia, Semântica, conectores, fluxo de conceito. 2. Meme. 3. CmpaTools, aplicação desenvolvido pelo IHMD ? Institute of Human and Machine Cognition, University of West Florida. 3.1 Criar um Projeto; 3.2 Conceitos e Conectores como Objetos; 3.3 Adicionar e Conectar Conceitos; 3.4 Formatação e Diagramação; 3.5 Agrupamento; 3.6 Links; 3.7 Apresentação; 3.8 Rede Mundial CmapTools; 3.9 Aplicação em sala de aula como ferramenta de apoio; 3.10 Lições Aprendidas.

MC13 - O Produto Entrelaçado e Automorfismos de Árvores

Márcio Roberto Rocha Ribeiro

UFG - Campus de Catalão - Departamento de Matemátic

74001-970, Catalão - GO

E-mail: marcioroberto@unb.br

8.45 Introdução

O produto entrelaçado (wreath) é uma ferramenta poderosa para a obtenção de exemplos de importantes resultados em teoria de grupos. Ele aparece de maneira natural em determinados contextos, como por exemplo na estrutura dos subgrupos de Sylow de grupos simétricos que envolve o resultado de L. Kaloujnine [1], além do famoso Teorema da Imersão de produto entrelaçado [3], que garante que a extensão de um grupo A por um grupo B pode ser imerso no produto entrelaçado de A por B.

O grupo de automorfismos de árvores regulares uni-raiz pode ser representado como um produto entrelaçado. Este grupo tomou notoriedade quando certos exemplos de subgrupos com as propriedades: finitamente gerado, periódico e infinito, foram construídos dentro dele. A partir de então, tem sido crescente o interesse pelo estudo desses grupos. Muitos fatos sobre sua estrutura tem sido esclarecidos e outros exemplos inéditos de grupos satisfazendo certas propriedades específicas foram definidos.

Neste minicurso faremos um estudo introdutório sobre o produto entrelaçado de grupos e apresentaremos o grupo de automorfismos de árvores a partir deste estudo. O objetivo principal é apresentar o produto entrelaçado restrito e permutacional, e observar o grupo de automorfismo de árvores como um produto entrelaçado, propondo uma visualização geométrica possibilitada pelo grafo da árvore.

8.46 Conceitos Básicos

Nesta seção são introduzidos alguns conceitos básicos da teoria de grupos e algumas propriedades são apresentadas.

8.46.1 Ação de Grupos

Definição 8.189. *Se X é um conjunto não vazio, um subgrupo G do grupo simétrico S_X ($Sym(X)$) é chamado um grupo de permutação de X.*

Dois elementos x e y de X são G-equivalentes se existe uma permutação π em G tal que $x\pi = y$. Esta é uma relação de equivalência em X. As classes de equivalência são conhecidas como G-órbitas; a órbita contendo x é $xG = \{x\pi | \pi \in G\}$. G é **transitivo** se dados $x, y \in X$ existe $\pi \in G$ tal que $x\pi = y$. Segue que G é transitivo se, e somente se existe exatamente uma G-órbita.

Se $Y \subset X$, o **estabilizador** de Y em G, $St_G(Y)$ ou G_Y é o conjunto das permutações em G que deixam fixos todos os elementos de Y.

Definição 8.190. *Seja G um grupo e X um conjunto não vazio. Por uma* **ação à direita** *de G em X entendemos uma função $\varphi : X \times G \longrightarrow X$ tal que*

$$(x, g_1g_2)\varphi = ((x, g_1)\varphi, g_2)\varphi, \quad (x, e)\varphi = x.$$

Assim, para $g \in G$ fixo a aplicação $\varphi_g : X \longrightarrow X$, $x \mapsto xg$ é uma permutação de X e, portanto, a ação de grupo determina um homomorfismo $\theta : G \longrightarrow S_X$, $g \mapsto \varphi_g$. Reciprocamente, se $\theta : G \longrightarrow S_X$ é um homomorfismo (uma tal função é denominada uma representação por permutação de G em X), então a aplicação

$$\varphi : X \times G \longrightarrow X,\ (x, g) \mapsto (x)\varphi_g.$$

é uma ação à direita de X. A representação por permutação de G em X, $\theta : G \longrightarrow S_X$ é fiel se $Ker(\theta) = \{e\}$, i.e., G é isomorfo a um grupo de permutação de X.

8.46.2 Produto Semi-direto

Definição 8.191. *Um grupo G é o produto semi-direto de seus subgrupos K e H se:*
(i) $K \lhd G$;
(ii) $G = KH$;
(iii) $K \cap H = e$

Denotamos $G = K \rtimes H$. Notamos que todo produto direto é também semi-direto.

Exemplo 8.192. *O grupo simétrico S_n, $n \geq 3$, é um produto semi-direto do grupo das permutações pares A_n pelo grupo cíclico de ordem dois C_2, escrevemos $S_n = A_n \rtimes C_2$.*

Considere grupos arbitrários H e K, com H agindo sobre K via ψ, isto é,

$$\psi : H \longrightarrow Aut(K), h \mapsto (\psi_h : k \mapsto k^h).$$

Seja $G = \{(k, h) \mid k \in K,\ h \in H\}$ e definamos a operação:

$$(k, h)(k_1, h_1) = (kk_1^h, hh_1)$$

onde $k,\ k_1 \in K$ e $h,\ h_1 \in H$.

Podemos verificar que G é um grupo e além disso temos que $K_1 = \{(k, e) \mid k \in K\}$ e $H_1 = \{(e, h) \mid h \in H\}$ são subgrupos de G tais que $K_1 \lhd G$, $K_1 \cap H_1 = \{e\}$ e $G = K_1H_1$. Assim G é o produto semi-direto de $K_1 \cong K$ por $H_1 \cong H$. Dizemos também que G é o **produto direto externo** de K por H induzido por ψ e denotamos por $G = K \rtimes_\psi H$ ou simplesmente por $G = K \rtimes H$.

8.47 O Produto Entrelaçado Permutacional e Regular

Sejam (A, X) e (B, Y) grupos de permutações, onde o grupo A age sobre o conjunto X e o grupo B sobre y. Denote por Z o produto cartesiano $X \times Y$. Denotaremos:

- A^Y: produto direto irrestrito (ou cartesiano) de cópias de A indexadas por Y;

- $A^{(Y)}$: produto direto restrito (ou produto direto) de cópias de A indexados por Y.

Cada elemento de A^Y será visto como uma função $f : Y \longrightarrow A$. Podemos também vê-lo como um vetor ou uma sequência. Além disso, o elemento $f \in A^Y$ tal que $f(y) = a$ e $f(y') = e$, $\forall\, y \neq y' \in Y$ será algumas vezes escrito como a_y. Em termos de sequência, ou de vetor isto significa que $f = (e, \cdots, e, a, e, \cdots) = a_y$, onde o elemento a ocupa a y-ésima coordenada.

- A^Y é o grupo das funções $f : Y \longrightarrow A$ com a multiplicação usual: $(f.g)(y) = f(y).g(y), \forall f,\ g \in A^Y$.

- Seja $f \in A^Y$. O **suporte** de f é o conjunto $s(f) = \{y \in Y \mid f(y) \neq e\}$.

- $A^{(Y)}$ é o subgrupo de A^Y, onde $f \in A^{(Y)}$ se $f \in A^Y$ e f tem suporte finito.

Definimos uma ação de B em A^Y por

$$\psi : B \times A^Y \longrightarrow A^Y,\ (b, f) \mapsto f^b,$$

onde $f^b : Y \longrightarrow A,\ f^b(y) = f(yb^{-1}),\ \forall y \in Y$.

Podemos interpretar $f(y)$ como um termo da sequência f que se encontra na posição y. Então $f^b(y) = f(yb^{-1})$ é um termo da sequência f^b que se encontra na posição y. Segue que f^b é uma sequência obtida da sequência f permutando suas coordenadas.

Segue do fato de ψ ser ação que, para cada $b \in B$, $\psi_b : A^Y \longrightarrow A^Y,\ f \mapsto f^b$ é uma permutação de A^Y. Temos que

$$\Psi : B \longrightarrow S_{(A^Y)},\ b \mapsto \psi_b,$$

é um homomorfismo. Mais ainda ψ_b é isomorfismo. Segue que ψ_b é automorfismo, para cada $b \in B$. Agora, Ψ pode ser escrita da seguinte forma

$$\Psi : B \longrightarrow Aut(A^Y).$$

Além disso Ψ é injetora (se $A \neq e$). Portanto, B pode ser considerado como um grupo de automorfismos de A^Y.

Estamos aptos a definir o produto semi-direto G de A^Y por B:

$$G = A^Y \rtimes_\Psi B,$$

aqui consideramos a operação

$$(f_1, b_1).(f_2, b_2) = (f_1 f_2^{b_1^{-1}}, b_1 b_2).$$

O produto semi-direto G definido age em $Z = X \times Y$.

8.47.1 Definição de Produto Entrelaçado

Com a mesma notação acima, vamos definir o produto entrelaçado de grupos.

Definição 8.193. *Sejam (A, X) e (B, Y) dois grupos de permutações, definimos o* **produto entrelaçado permutacional** *$AWr_Y B$ de A por B como o produto semi-direto de $A^Y \rtimes_\Psi B$.*

O **produto entrelaçado restrito** $Awr_Y B$ de A e B, é definido de maneira análoga: $Awr_Y B = A^{(Y)} \rtimes_\Psi B$. O grupo A^Y $(A^{(Y)})$ em $AWr_Y B$ $(Awr_Y B)$ é denominado **grupo base**. Existem duas imersões do grupo A no grupo base A^Y que serão de interesse:

- imersão diagonal: $\tau : A \longrightarrow A^Y$, $a \mapsto f_a$, onde $f_a(y) = a,\ \forall y \in Y$;

- imersão em componentes: fixe $y \in Y$ e considere $\psi : A \longrightarrow A^Y$, $a \mapsto f_a$, onde $f_a(y) = a$ e $f(y') = e,\ \forall y \neq y', y' \in Y$.

Note que um grupo age sobre si mesmo por multiplicação à direita. Esta ação produz uma representação por permutação de G em G: $\psi : G \longrightarrow S_G$ denominada **representação regular à direita**.

Definição 8.194. *Sejam A e B dois grupos considerados como grupos de permutações em suas representações regulares (i.e. A e B agem fielmente sobre si mesmos). O* **produto entrelaçado regular** *de A por B é o produto entrelaçado $AWr_BB(Awr_BB)$, geralmente denotado por AWrB (AwrB).*

Apresentamos a seguir dois exemplos de produto entrelaçado regular.

Exemplo 8.195. *C_2wrC_2 é isomorfo ao grupo diedral D_8. De fato considere $C_2wrC_2 = AwrB$ onde $A = \langle x\rangle$ e $B = \langle y\rangle$. Então temos $A^B = \langle x\rangle \times \langle x\rangle = \{(e,e),(e,x),(x,e),(x,x)\} = \{(a_1,a_y) \mid a_1,\ a_y \in \langle x\rangle\}$. A ação de $\langle x\rangle^{\langle y\rangle}$, permuta as coordenadas, por exemplo*

$$(a_1, a_y)^y = (a_y, a_1).$$

Assim, $C_2wrC_2 = (\langle x\rangle \times \langle x\rangle) \rtimes \langle y\rangle = \{((e,e),e),((e,e),y),((e,x),e),$
$((e,x),y),((x,e),e),((x,e),y),((x,x),e),((x,x),y)\}$.

Note que:

- *(i) $a = ((e,e),y)$ tem ordem dois.*

- *(ii) $b = ((e,x),y)$ tem ordem quatro.*

- *(iii) $abab = e$.*

- *(iv) C_2wrC_2 tem ordem oito.*

Segue de (i) a (iv) que C_2wrC_2 é isomorfo ao grupo $D_8 = \langle a,\ b \mid a^2 = b^4 = (ab)^2 = e\rangle$.

Exemplo 8.196. *$\mathbb{R}wr\mathbb{R}$ é um grupo com dois geradores que possui um subgrupo que não é finitamente gerado. De fato, Considere $\mathbb{R}_{(i)}$ a projeção de $\mathbb{R}^{(\mathbb{R})}$ na coordenada i,*

$$\mathbb{R}_{(i)} = \langle f_i \in \mathbb{R}^{(\mathbb{R})} \mid f_i(j) = \delta_{ij}\rangle$$

onde,

$$\delta_{ij} = 1,\ \text{se } i = j \text{ e } \delta_{ij} = 0,\ \text{se } i \neq j$$

Segue que $\mathbb{R}_{(i)} = \langle(\cdots, 0, 1, 0\cdots)\rangle \cong \mathbb{R}$ onde 1 ocupa a i-ésima coordenada e $\mathbb{R}_{(i)} \leq \mathbb{R}^{(\mathbb{R})}$. Observamos ainda que

$$\mathbb{R}wr\mathbb{R} = \mathbb{R}^{(\mathbb{R})} \rtimes \mathbb{R} = \langle \mathbb{R}^{(\mathbb{R})}, \mathbb{R}\rangle = \langle \mathbb{R}_{(i)}, \mathbb{R} \mid i \in \mathbb{R}\rangle = \langle \mathbb{R}_{(i)}, \mathbb{R}\rangle.$$

Temos a ação $\mathbb{R} \times \mathbb{R}^{(\mathbb{R})} \longrightarrow \mathbb{R}^{(\mathbb{R})}$, $(n, f) \mapsto f^n$; $f_i^n(z) = f(z-n)$, *e* $\mathbb{R}$ *age transladando em* n *coordenadas a* f. *Em particular,* $\mathbb{R}$ *age em* $\mathbb{R}_{(i)}$:

$$\mathbb{R} \times \mathbb{R}_{(i)} \longrightarrow \mathbb{R}_{(i)},\ (n, f_i) \mapsto f_i^n;$$

onde $f_i^n(j) = f_i(j-n)$.

Observamos que se $f_i \in \mathbb{R}_{(i)}$, $f_i(j) = \delta_{ij}$. *Para* $n \in \mathbb{R}$, $f_i^n(j) = f_i(j-n) = \delta_{i(j-n)}$, *logo,* $f_i^n(i+n) = f_i(i) = 1$. *Assim, se o valor* 1 *ocupa a coordenada* i *da* f, *então o valor* 1 *ocupará a coordenada* $i+n$ *da* f^n. *Isto mostra que a ação de* $\mathbb{R}$ *sobre* $\mathbb{R}_{(i)}$ *é a de transladar* n *coordenadas o elemento* 1. *Assim,* $f_i^n = f_{i+n}$.

Observamos ainda que o grupo base $\mathbb{R}^{(\mathbb{R})} = \oplus_{i \in \mathbb{R}} \mathbb{R}_{(i)}$ *é um subgrupo de* $\mathbb{R}wr\mathbb{R}$ *(visto como* $\mathbb{R}^{(\mathbb{R})} \rtimes \{0\}$*) que é infinitamente gerado pois a soma direta dos* $\mathbb{R}_{(i)}$, $i \in \mathbb{R}$, *é abeliano livre de posto infinito.*

Agora, vamos mostrar que $\mathbb{R}wr\mathbb{R}$ *é* 2*-gerado, mais especificamente, para* $i \in \mathbb{R}$, i *fixo, temos*

$$\mathbb{R}wr\mathbb{R} = \langle (f_i, 0), (0, 1) \rangle$$

onde $f_i \in \mathbb{R}_{(i)},\ i \in \mathbb{R}$. *De fato, para* $k \in \mathbb{R}$,

$$\begin{aligned}(f_i, 0)^{(0,k)} &= (0, -k)(f_i, 0)(0, k) \\ &= (0 + f_i^k, -k + 0).(0, k) \\ &= (f_i^k, -k + k) \\ &= (f_{i+k}, 0)\end{aligned}$$

Isto mostra que $(f_i, 0)$ *e* $(0, 1)$ *geram os elementos* $(f_j, 0) \in \mathbb{R}wr\mathbb{R},\ \forall j \in \mathbb{R}$.

Segue que $\mathbb{R}_{(i+k)} \hookrightarrow \langle (f_i, 0), (0, 1) \rangle,\ \forall k \in \mathbb{R},\ f_{i+k} \hookrightarrow (f_{i+k}, 0)$ *e* $\mathbb{R} \hookrightarrow \langle (f_i, 0), (0, 1) \rangle,\ z \hookrightarrow (0, z)$.

Assim,

$$\mathbb{R}wr\mathbb{R} = \langle \mathbb{R}_{(i)}, \mathbb{R} \mid i \in \mathbb{R} \rangle \leq \langle (f_i, 0), (0, 1) \rangle \leq \mathbb{R}wr\mathbb{R}.$$

Na verdade $\mathbb{R}wr\mathbb{R}$ não é finitamente apresentado, veja [5].

8.48 Árvores Regulares

Seja Y um conjunto que chamaremos *alfabeto*. Por $M = M(Y)$ denotamos o conjunto

$$\{y_1 y_2 \cdots y_n \ \mid y_i \in Y\}$$

de todas as palavras finitas sobre o alfabeto Y, incluindo a palavra vazia ϕ. Em outros termos, M é o monóide livre gerado por Y. Seja $\mathcal{T}_Y$ o grafo cujo conjunto de vértices é M e tal que dois vértices são conectados se, e somente se eles são da forma v e vy, onde $v \in M$ e $y \in Y$. O grafo $\mathcal{T}_Y$ é uma árvore que chamaremos *árvore regular uni-raiz* ou simplesmente *árvore regular*, onde a palavra vazia é a raiz. Quando $|Y| = n$, escreveremos $\mathcal{T}_Y = \mathcal{T}_n$. Para $Y = \{1, 2\}$ temos a árvore binária $\mathcal{T}_2$, veja figura 16.

Definindo sobre M uma relação de ordem $\leq$ dada por:

$$v \leq u \Longleftrightarrow u \text{ é prefixo de } v,$$

temos que a árvore $\mathcal{T}_Y$ é o grafo de $(M, \leq)$.

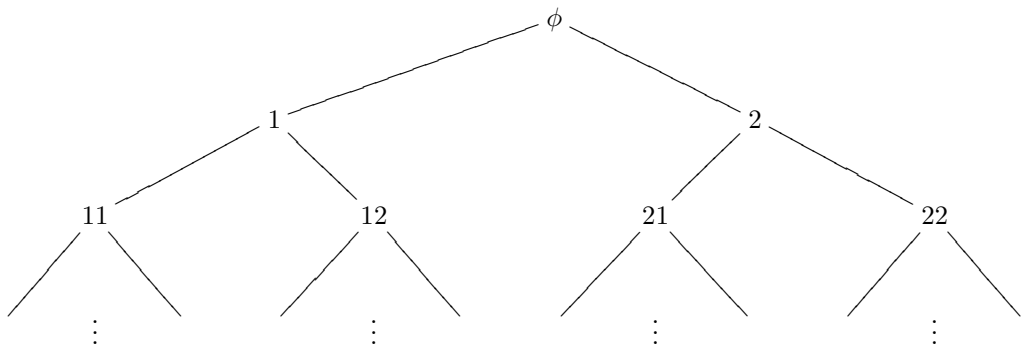


Figura 16: árvore binária $\mathcal{T}_2$

O comprimento de uma palavra $v \in M$ (o número de letras dela) é denotado por $|v|$, onde $|\phi| = 0$. A *função comprimento* $|\ \ | : v \mapsto |v|$ induz uma distância entre os elementos de M dada por:

$$d(u, v) = |u| + |v| - 2|w|,$$

onde w é o maior prefixo comum entre u e v. Assim, (M, d) é um espaço métrico.

Para $k \geq 0$, conjunto $Y^k = \{v \in M \mid |v| = k\}$, é denominado *k-ésimo nível* de $\mathcal{T}_Y$.

8.48.1 O Grupo de Automorfismos de Árvores Regulares

Dados duas árvores $\mathcal{Q}$ e $\mathcal{R}$, uma aplicação $\alpha : \mathcal{Q} \longrightarrow \mathcal{R}$ é um *isomorfismo* se ela é bijetora e preserva a adjacência dos vértices; isto é, se para quaisquer dois vértices adjacentes $v,\ vy \in M$ os vértices $(v)\alpha$ e $(vy)\alpha$ são também adjacentes.

Para cada $u \in M$, considere a subárvore $u\mathcal{T}_Y = \{u.v \mid v \in M\}$ de $\mathcal{T}_Y$ que possui u como raiz. Agora note que $u.v \mapsto v$ é um isomorfismo de $u\mathcal{T}_Y$ em $\mathcal{T}_Y$.

Uma aplicação $\alpha : \mathcal{T}_Y \longrightarrow \mathcal{T}_Y$ é um *endomorfismo da árvore* $\mathcal{T}_Y$ se ela preserva a adjacência dos vértices.

Definição 8.197. *Um automorfismo de uma árvore regular $\mathcal{T}_Y$ é um endomorfismo bijetor de $\mathcal{T}_Y$.*

Equivalentemente, podemos dizer que um automorfismo de uma árvore regular $\mathcal{T}_Y$ é uma bijeção sobre M que preserva a função distância d. Um automorfismo de uma árvore regular $\mathcal{T}_Y$ é também denominado uma *isometria* de $\mathcal{T}_Y$.

O conjunto dos automorfismos de $\mathcal{T}_Y$ forma um grupo que denotaremos por $\mathcal{A} = Aut(\mathcal{T}_Y)$ e chamaremos *grupo dos automorfismos de* $\mathcal{T}_Y$ ou *grupo de isometrias de* $\mathcal{T}_Y$.

Dada uma permutação $\sigma \in \mathcal{P}(Y)$, o grupo das permutações de Y, podemos estendê-la a um automorfismo de $\mathcal{T}_Y$ da seguinte forma:

$$(y.u)\sigma = (y)\sigma.u,\ \forall y \in Y,\ \forall\ u \in M.$$

Por outro lado, um automorfismo $\alpha \in \mathcal{A}$ induz uma permutação $\sigma_\phi(\alpha)$ sobre o conjunto Y. Assim, podemos escrever $\alpha = \alpha'.\sigma_\phi(\alpha)$, onde α' estabiliza Y ponto a ponto. Para cada $y \in Y$, α' induz sobre a subárvore $y.\mathcal{T}_Y$ um automorfismo α'_y. Considerando o isomorfismo $y.\mathcal{T}_Y \longrightarrow \mathcal{T}_Y$ podemos identificar $y.\mathcal{T}_Y$ com $\mathcal{T}_Y$ e assim identificar α'_y como um elemento de $\mathcal{A}$. Desta forma, podemos considerar α' como uma função de Y em $\mathcal{A}$ e assim temos que

$$\mathcal{A} = \mathcal{A}^Y \rtimes \mathcal{P}(Y),$$

onde $A^Y = F(Y, \mathcal{A})$ é o grupo das funções de Y em $\mathcal{A}$. Isto significa que podemos ver o grupo de automorfismos de árvores como um produto entrelaçado: $\mathcal{A} = \mathcal{A}Wr_Y\mathcal{P}(Y)$. Denotamos α'_y por α_y e escrevemos $\alpha = (\alpha_y)_{y\in Y}.\sigma_\phi(\alpha)$. A ação de α em $\mathcal{T}_Y$ é dada por:

$$(yu)\alpha = (y)\sigma_\phi(\alpha).(u)\alpha_y, \ \forall\ y \in Y, \ \forall\ u \in M.$$

Podemos repetir para α_y o mesmo processo de descrição visto para α, assim $\alpha_y = (\alpha_{yx})_{x\in Y}.\sigma_\phi(\alpha_y)$ e podemos repetir novamente o processo para cada α_{yx}. Sucessivos desenvolvimentos de α produzem, para cada $u \in M$, um automorfismo $\alpha_u = (\alpha_{ui})_{i\in Y}.\sigma_\phi(\alpha_u)$. Vamos denotar $\sigma_\phi(\alpha_u)$ por $\sigma_u(\alpha)$ e α por α_ϕ. Podemos então considerar os conjuntos $\Sigma(\alpha) = \{\sigma_u(\alpha) \mid u \in M\}$ e $Q(\alpha) = \{\alpha_u \mid u \in M\}$. O conjunto $Q(\alpha)$ é denominado *conjunto de estados* de α. Um estado α_u de α é dito ser **ativo** se $\sigma_u(\alpha) \neq e$, caso contrário, ele é denominado **inativo**.

Seja $\alpha \in \mathcal{A}$. Escrevemos $\alpha = \alpha^{(0)}$ e denotamos por $\alpha^{(1)}$ o automorfismo de $\mathcal{T}_Y$ onde $(\alpha^{(1)})_y = \alpha$, $\forall\ y \in Y$, e $\sigma_\phi(\alpha^{(1)}) = e$. Indutivamente, para $k > 1$, denotamos por $\alpha^{(k)}$ o automorfismo de $\mathcal{T}_Y$ onde $(\alpha^{(k)})_y = \alpha^{(k-1)}$, $\forall\ y \in Y$, e $\sigma_\phi(\alpha^{(k)}) = e$. Por exemplo, se $Y = \{1, 2, \cdots, n\}$, temos $\alpha^{(1)} = (\alpha, \cdots, \alpha)$ e $\alpha^{(k)} = (\alpha^{(k-1)}, \cdots, \alpha^{(k-1)})$, $\forall\ k \geq 1$, onde os vetores possuem n coordenadas.

Definição 8.198. *Seja $G \leq Aut(\mathcal{T}_Y)$.*
(i) O estabilizador em G de um vértice $v \in \mathcal{T}_Y$, é o subgrupo

$$G_v = \{\alpha \in G \mid (v)\alpha = v\}.$$

(ii) O estabilizador do k-ésimo nível é o subgrupo $St_G(k) = \bigcap_{v\in Y^k} G_v$.
(iii) G é nível-transitivo se ele age transitivamente em todos os níveis da árvore $\mathcal{T}_n$.

Observação 8.199.
(i) Seja $G \leq Aut(\mathcal{T}_Y)$, então $\forall\ k \geq 1$, $St_G(k)$ é um subgrupo normal de índice finito em G; $\bigcap_{k\geq 1} St_G(k) = \{e\}$ e $St_G(k+1) \leq St_G(k)$.
(ii) O grupo de automorfismo $Aut(\mathcal{T}_n)$ é um grupo profinito. Se $\mathcal{T}_{n,j}$ denota a árvore n-ária truncada no nível j, então

$$Aut(\mathcal{T}_n) = \varprojlim Aut(\mathcal{T}_{n,j}).$$

Notamos que $\mathcal{T}_{n,j}$ é finita, $\forall\ j \geq 0$ e portanto $Aut(\mathcal{T}_{n,j})$ é também finito, $\forall\ j \geq 0$. Quando $|Y| = 2$, temos que $Aut(\mathcal{T}_{2,j}) = W_{j-1}wrC_2$, onde W_{j-1} é o produto entrelaçado iterado $j-1$ vezes de C_2, o grupo cíclico de ordem 2. Portanto, $Aut(\mathcal{T}_{2,j})$ é um 2-grupo finito e assim, $Aut(\mathcal{T}_2)$ é um grupo pro-2. Mais detalhes podem ser encontrados em [9].

8.48.2 Automorfismos com um Número Finito de Estados

Um automorfismo de $\mathcal{T}_Y$ pode ser interpretado como um *autômato de Mealy* que é uma *máquina de Turing* definida por uma sêxtupla $(Q, L, \Gamma, f, l, q_0)$, onde:

- Q é o conjunto de estados;
- L é o alfabeto de entrada:
- Γ é o alfabeto de saída;

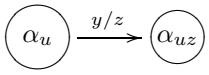


Figura 17: Diagrama de Moore

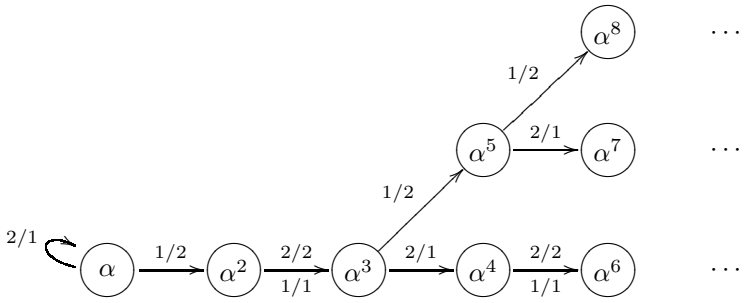


Figura 18: Diagrama de Moore de $A(\alpha)$ onde $\alpha = (\alpha, \alpha^2)\sigma$

- $f : Q \times L \longrightarrow Q$ é a função de transição de estados;
- $l : Q \times L \longrightarrow \Gamma$ é a função de saída;
- q_0 é o estado inicial,

Um autômato é *finito* se o conjunto de estados Q é finito, veja [10] e [4].

Para um automorfismo $\alpha \in \mathcal{A}$, associamos o autômato $A(\alpha)$ dado pela sêxtupla $A(\alpha) = (Q = Q(\alpha), L = Y, \Gamma = Y, f, l, q_0 = \alpha)$, onde as funções $f : Q(\alpha) \times Y \longrightarrow Q(\alpha)$ e $l : Q(\alpha) \times Y \longrightarrow Y$ são dadas por $f(\alpha_u, y) = \alpha_{uz}$ e $l(\alpha_u, y) = z$, onde $z = (y)\alpha_u$. $A(\alpha)$ é denominado o *autômato de* α.

É conveniente definir autômatos usando o *diagrama de Moore*. Para o autômato $A(\alpha)$, $\alpha \in \mathcal{A}$ o diagrama de Moore é um grafo orientado, com os vértices identificados com os estados $Q(\alpha)$. Se $z = (y)\alpha_u$, então temos uma aresta iniciando em α_u, finalizando em α_{uz} e rotulada por y/z, onde $u \in M$ e $y,\ z \in Y$. Veja figura 17.

Exemplo 8.200. *Seja $\alpha = (\alpha, \alpha^2)\sigma \in Aut(\mathcal{T}_2)$ onde $\sigma = (1\ 2)$. Então, $\alpha^2 = (\alpha^3, \alpha^3)$ e*

$$\alpha^{2k} = (\alpha^{3k}, \alpha^{3k}), \quad \alpha^{2k+1} = (\alpha^{3k+1}, \alpha^{3k+2})\sigma.$$

Então $Q(\alpha) = \{\alpha^k \mid k \geq 1\}$ é um conjunto infinito e seu autômato é portanto infinito. O diagrama de Moore de $A(\alpha)$ é dado na figura 18.

Exemplo 8.201. *Seja $\alpha = (e, e, \alpha)\sigma \in Aut(\mathcal{T}_3)$ onde $\sigma = (1\ 2\ 3)$. Então $Q(\alpha) = \{e, \alpha\}$ e seu autômato é portanto finito. O diagrama de Moore de $A(\alpha)$ é dado na figura 19.*

Definição 8.202. *O automorfismo $\alpha \in Aut(\mathcal{T}_Y)$ é denominado um automorfismo com um número finito de estados se Y e $Q(\alpha)$são conjuntos finitos.*

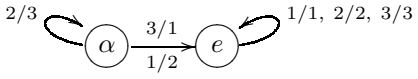


Figura 19: Diagrama de Moore de $A(\alpha)$ onde $\alpha = (e, e, \alpha)\sigma$

Assim, $\alpha \in Aut(\mathcal{T}_Y)$ é um automorfismo com um número finito de estados se, e somente se o autômato $A(\alpha)$ é finito. Para quaisquer automorfismos α e β em $Aut(\mathcal{T}_Y)$ temos que $Q(\alpha^{-1}) = Q(\alpha)^{-1}$ e $Q(\alpha\beta) \subseteq Q(\alpha)Q(\beta)$. Ainda, os autômatos com um número finito de estados formam um conjunto enumerável. Seja $\mathcal{F}_Y$ o conjunto dos automorfismos com um número finito de estados. Então temos a seguinte proposição.

Proposição 8.203. *O conjunto $\mathcal{F}_Y$ é um subgrupo enumerável de $Aut(\mathcal{T}_Y)$.*

Exemplo 8.204. *Um exemplo de grupo gerado por automorfismos de finitos estados pode ser obtido como segue: para um primo p ímpar consideramos σ_p a extensão da permutação $(1, 2, \cdots, p)$ a um automorfismo de $\mathcal{T}_p$. A ação de σ_p em $\mathcal{T}_p$ é a de permutar ciclicamente o primeiro nível. Agora, consideremos $\gamma = (\sigma_p, \sigma_p^{-1}, e, \cdots, e, \gamma) \in Aut(\mathcal{T}_p)$. O grupo $\mathcal{G} = \langle \gamma, \sigma_p \rangle$ é conhecido como* **p-grupo de Gupta-Sidki**. *Este grupo é um p-grupo infinito, possui expoente infinito além de outras propriedades. Se $p = 3$, temos que $\gamma = (\sigma_3, \sigma_3^{-1}, \gamma)$ e $Q(\gamma) = \{e, \sigma_3, \sigma_3^{-1}, \gamma\}$.*

Referências

[1] KALOUJNINE, A., *Sur Les p-groupes de Sylow du groupe symétrique de degré p^n, C. R. Acad. Sci.* Paris, 224 (1947) 253-255.

[2] LOPES, G. L. O., *O produto wreath em classes de grupos*. Dissertação(Mestrado em Matemática) - Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, 2000.

[3] MELDRUM, J. D. P., *Wreath Products of Groups and Semigroups*, Pitman Monographs and Surveys in Pure and Appl. Math., v. 74, 1995.

[4] NEKRASHEVYCH, V., *Self-similar groups. Math. Surveys Monogr.*, 117, 2005.

[5] ROBINSON, D. J. S., *A course in the teory of groups*. Second edition. Springer-Verlag, New York, 1996.

[6] ROTMAN, J. J., *An introduction to the teory of groups*. Fourth edition. Springer-Verlag, New York, 1994.

[7] SIDKI, S. N., Regular trees and their automorphisms, *Monografias em Matemática*, 56, IMPA, Rio de janeiro, 1998.

[8] RIBEIRO, M. R. R., *O grupo finitário de isometrias da árvore n-ária*. Tese(Doutorado em Matemática)- Departamento de Matemática do Instituto de Ciências Exatas da Universidade de Brasília, Brasília, 2008.

[9] BASS, H.; OTERO-ESPINAR, M. V.; ROCKMORE, D.; TRESSER, C., *Cyclic renormalization and automorphism groups of rooted trees*, Lecture Notes in Mathematics, v. 1621, Springer-Verlag, Berlim, 1996.

[10] EILENBERG, S., *Automata, languages and machines*, v. A, New york, Academic Press, 1974.

MC14 -Códigos Corretores de Erros

Mário José de Souza

IME/UFG - Campus II

74001-970, Goiânia - GO

E-mail: mariojsouza@mat.ufg.br

9.49 Introdução

Existem várias maneiras de ocorrência dos corretores de erros em nosso dia-a-dia. Por exemplo, quando assistimos televisão, falamos ao telefone, ouvimos a gravação musical em um CD, ou simplesmente navegando pela INTERNET. Um código corretor de erros é, basicamente, uma forma organizada de acrescentar algum dado a cada informação que precise ser transmitida ou armazenada, de modo que permita, ao recuperar a informação, detectar e corrigir os erros no processo de transmissão da informação. A teoria dos códigos é um campo de pesquisa atual, muito atraente, tanto do ponto de vista científico quanto tecnológico. A teoria dos códigos mistura conceitos e técnicas importantes da Álgebra abstrata com aplicações imediatas da cotidiano, mostrando que sofisticação tecnológica torna cada vez mais imperceptível a relação entre a chamada matemática pura e a matemática aplicada. Este mini-curso tem por objetivo apresentar e desenvolver os fundamentos matemáticos dessa teoria. Como trata-se de um assunto com várias ramificações dentro da matemática, nos ocuparemos com aspectos de natureza algébrica.

9.50 Códigos Corretores de Erros

Todo canal corrompe o sinal transmitido, devido ao ruído inerente. Isto faz com que ocorram erros e, assim, a mensagem originalmente transmitida não pode ser reconstruída no receptor. Para tanto, o codificador de canal faz a adição controlada de redundância, para que a mesma possa ser explorada no decodificador de canal, a fim de corrigir erros, se possível. As técnicas de correção de erros podem ser classificadas em dois grupos: FEC (Forward Error Correction), onde se utilizam códigos corretores de erro para fazer a correção no receptor (daí o forward), e ARQ (Automatic Repeat reQuest), que, na ocorrência de um erro, detectado por um código detetor de erro, emite um pedido de retransmissão da mensagem, ou de parte dela. O melhor desempenho do sistema é atingido utilizando-se ambas as técnicas. Caso não houvesse os códigos corretores de erro, o número de pedidos de retransmissão poderia ser alto, fazendo com que o vazão do sistema caísse demais. Com o uso de códigos corretores de erro, é possível fazer com que a taxa de erro caia a patamares pequenos, de tal forma que o número de retransmissões atinja um ponto aceitável. Contudo, podemos pensar em usar um código bem poderoso para que a taxa de erro caia a valores suficientemente baixos, de forma a tornar praticamente inexistentes os pedidos de retransmissão. Contudo, códigos poderosos exigem uma redundância elevada e, portanto, a taxa de transmissão de dados cai excessivamente. Assim, existe um compromisso entre correção de erro e taxa de retransmissão. No presente capítulo, temos a intenção de fazer uma breve introdução à Teoria de Codificação de Canal, que é uma vasta área de intensa pesquisa e desenvolvimento de técnicas que objetivam adicionar o mínimo de redundância e obter o máximo de proteção contra erros, buscando ficar dentro de certos limites de recursos computacionais no processo de decodificação. Os códigos corretores de erro podem ser divididos

em dois grandes grupos: códigos de bloco e códigos convolucionais. Dentro de cada grupo existe uma vastidão de tipos de códigos, para as mais diversas situações.

9.50.1 Códigos de Bloco

Os códigos de bloco operam sobre sistemas algébricos chamados corpos algébricos. Simplificadamente, um corpo é um conjunto de elementos nos quais podem-se realizar as operações de adição, subtração, multiplicação e divisão sem sair do conjunto. A adição e a multiplicação devem satisfazer as propriedades comutativa, associativa e distributiva. Quando assumimos um conjunto de números inteiros 0,1,2,...,p-1, onde p é um número primo, e usamos as operações de adição módulo-p e multiplicação módulo-p, obtemos um conjunto que obedece às condições para ser um corpo, ao qual se dá o nome de corpo primo, ou Galois Field (GF), em homenagem ao seu descobridor. Este corpo é representado por GF(p) e pode ser estendido, sendo sua extensão denominada de GF(p^m), onde m é um número natural. Nos sistemas de comunicação e armazenamento de dados, os corpos GF(2^m) são amplamente usados. Todas as operações sobre os códigos são feitos sobre GF.

A codificação é feita utilizando-se uma matriz G de um código C(n,k). Essa matriz possui dimensão k x n, com k linhas independentes.

9.50.2 Códigos Convolucionais

Os códigos convolucionais foram introduzidos primeiramente por Elias [3] em 1955 como uma alternativa aos códigos de bloco. Em 1961, Wozencraft [11] propõe o processo de decodificação diferencial como uma forma eficaz de se fazer a decodificação. Dois anos depois, Massey em 1963 propõe uma técnica chamada de decodificação por limiar, que é menos eficiente mas mais simples. Isto tornou possível a implementação prática destes códigos em sistemas de comunicação com e sem fio. Então em 1967, Viterbi [10] propõe um esquema de decodificação por seqüência de máxima verossimilhança, também conhecido por decodificação de Viterbi, que tinha uma implementação relativamente simples para códigos com pouca memória. Essa técnica, juntamente com uma versão aprimorada do processo de decodificação diferencial, fez com que os códigos convolucionais fossem utilizados em sistemas de comunicação via satélite e comunicação de espaço profundo já no começo da década de 70. Os códigos convolucionais costumam ser mais comuns que os códigos de bloco, por terem implementação mais simples. Seu desempenho é igual, quando não é maior, ao dos bons códigos de bloco. Tal desempenho é atribuído usualmente à possibilidade de implementação prática do processo de decodificação suave, que também existe para códigos de bloco, mas tem altíssimo custo computacional. O processo de codificação é feito por meio de deslocadores de registro, que também é utilizado em códigos de bloco (códigos cíclicos). Além disso, com auxílio do método de puncionamento [1], que consiste em se excluir periodicamente algumas saídas do equalizador, a fim de aumentar a taxa do codificador, é possível utilizar um mesmo decodificador para trabalhar com diferentes taxas. É claro que o aumento da taxa tem sua contrapartida pois, ao se excluir algumas saídas do codificador, perde-se em proteção contra erros. Da mesma forma que os códigos de bloco, os códigos convolucionais também possuem uma representação matricial.

9.51 Preliminares

Nesta secção são introduzidos os conceitos básicos da teoria de códigos e algumas propriedades são apresentadas. Um estudo mais detalhado pode ser encontrado em [6],[4]e[8].

Algumas notações:

· $\mathbb{F}_q$ denotará um corpo finito com q elementos.

· $(\mathbb{F}_q)^n = \{\mathbf{x} = (x_1, x_2, ..., x_n) : x_i \in \mathbb{F}_q\}$

9.51.1 Alfabeto

Definição 9.205. *Um alfabeto finito é simplesmente um conjunto finito* $\mathbb{F}_q$.

Definição 9.206. *Diremos que* $\mathbf{C}$ *é um código de comprimento* n *(sobre* $\mathbb{F}_q$*) se* $\mathbf{C} \subset (\mathbb{F}_q)^n$.

Observação 9.207. *Assim,* $\mathbf{C}$ *é dito um código* $q-$*ário. Desse modo, tem-se códigos binários* $(q = 2)$*, ternário* $(q = 3)$*, etc.*

9.51.2 Distância de Hamming

Para se identificar as palavras mais próximas de uma dada palavra recebida com erro e estimar qual foi a palavra código transmitida, apresentaremos um modo de "medir"a distância entre palavras de $(\mathbb{F}_q)^n$.

Definição 9.208. *A* ***distância de Hamming*** *entre* $\boldsymbol{x,y} \in (\mathbb{F}_q)^n$ *é dada por:* $d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}$.

Exemplo 9.209. *Seja* $\mathbb{F}_2$ *e consideremos* $(\mathbb{F}_2)^3$.

$$d((0,0,1),(1,1,1)) = 2$$
$$d((0,0,0),(1,1,1)) = 3$$
$$d((1,0,0),(1,1,0)) = 1.$$

Proposição 9.210. *A distância de Hamming é uma métrica, ou seja:*

(a) $d(\mathbf{x}, \mathbf{y}) = 0 \Longleftrightarrow \boldsymbol{x=y}$;

(b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$, $\forall \boldsymbol{x,y} \in (\mathbb{F}_q)^n$;

(c) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$, $\forall \boldsymbol{x,y,z} \in (\mathbb{F}_q)^n$

Demonstração. Exercício. □

Definição 9.211. *A* ***bola de centro a*** *e raio* $\boldsymbol{r}$ *é definida por* $B_{\mathbf{r}}(\mathbf{a}) = \{\mathbf{x} \in (\mathbb{F}_q)^n : d(\mathbf{x}, \mathbf{a}) \leq \mathbf{r}\}$.

9.51.3 Distância mínima de um código

Definição 9.212. *A distância mínima de um código* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é*

$$d_{\min}(\mathbf{C}) = \min\{d(\mathbf{x}, \mathbf{x}') : \mathbf{x}, \mathbf{x}' \in C : \mathbf{x} \neq \mathbf{x}'\}$$

.

Exemplo 9.213.

$$Seja\ \mathbf{C} = \{(0,0,0,0,0),(0,1,0,1,1),(1,0,1,1,0),(1,1,1,0,1)\} \subset (\mathbb{F}_2)^5 .$$

$\dim(\mathbf{C}) = 3$.

Proposição 9.214. *Seja* $\mathbf{C}$ *um código com distância mínima d. Se* $\boldsymbol{c}$ *e* $\boldsymbol{c'}$ *são palavras distintas de* $\mathbf{C}$*, então* $B_{\mathbf{t}}(\mathbf{c}) \cap B_{\mathbf{t}}(\mathbf{c\prime}) = \varnothing$*, em que* $t = \left[\frac{d-1}{2}\right]$.

Observação 9.215. $[*]$: *parte inteira do número* $*$.

Demonstração. Exercício. □

Teorema 9.216. *Seja* $\mathbf{C}$ *um código com distância mínima d. Então* $\mathbf{C}$ *pode corrigir até* $t = \left[\frac{d-1}{2}\right]$ *erros. Se d é par, o código pode simultaneamente corrigir* $\frac{d-2}{2}$ *erros e detectar até* $\frac{d}{2}$ *erros.*

Demonstração. Exercício. □

Definição 9.217. *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *um código com distância mínima d e seja* $t = \left[\frac{d-1}{2}\right]$*. O código* $\mathbf{C}$ *será dito perfeito se* $\bigcup_{\mathbf{x}\in\mathbf{C}} \mathbf{B}_t(\mathbf{x}) = (\mathbb{F}_q)^n$.

1. O código do **Exemplo 3.9** não é perfeito, pois trata-se de um código $\mathbf{C} \subset (\mathbb{F}_2)^5$ e $\bigcup_{\mathbf{c}\in\mathbf{C}} B_t(\mathbf{c}) \neq (\mathbb{F}_2)^5$

9.52 Códigos Lineares

Na prática, a classe de códigos mais utilizada é a denominada classe dos códigos lineares.

Definição 9.218. *Um código* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é chamado de código linear se for um sub-espaço vetorial de* $(\mathbb{F}_q)^n$.

Nota 9.5. *Assim,* $\mathbf{C}$ *é um espaço vetorial de dimensão finita. Sendo k a dimensão do código* $\mathbf{C}$*, todo elemento de* $\mathbf{C}$ *pode ser escrito de modo único da seguinte maneira:*$(*)\ \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_k u_k, \alpha_i \in \mathbb{F}_q$*,* $i = 1,2,...,k$*; em que* $\{u_1, u_2, \cdots, u_k\}$ *é uma base de* $\mathbf{C}$*. Como* $\alpha_i \in \mathbb{F}_q$*,* $i = 1,2,...,k$*; existem q possibilidades para cada um dos* α_i *em* $(*)$*. Logo existem* q^k *elementos em* $\mathbf{C}$*, isto é,* $M = |\mathbf{C}| = q^k$ *e consequentemente dim*$\mathbf{C} = k\log_q^q = \log_q^{q^k} = \log_q^M$.

Definição 9.219. *Dado u*$\in (\mathbb{F}_q)^n$*, o peso de u é o número inteiro:*
W(u)=$\#\{i : u_i \neq 0\}$*. Ou seja, W(u)=d(u,o)=0, em que o é o vetor nulo de* $(\mathbb{F}_q)^n$.

Definição 9.220. *O peso de um código linear* $\mathbf{C}$*, é o inteiro*

$$W(\mathbf{C}) = min\{W(u) : u \in \mathbf{C} \subset (\mathbb{F}_q)^n\}$$

.

Proposição 9.221. *Dado um código linear* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *com distância mínima d, temos que:*

(i) $\forall u, v \in (\mathbb{F}_q)^n$, $d(u,v) = W(u-v)$

(ii) $d =$W($\mathbf{C}$).

Nota 9.6. *Em virtude desta proposição, a distância mínima de um código linear* $\mathbf{C}$ *será também chamada de peso do código* $\mathbf{C}$.

9.53 Construindo Códigos Lineares

É sabido, em Álgebra Linear, que existem duas maneiras de se escrever sub-espaços vetoriais $\mathbf{C}$ do espaço vetorial $(\mathbb{F}_q)^n$. Uma como imagem e a outra como núcleo de uma transforamação linear.

Obteremos a representação de $\mathbf{C}$ como imagem de uma imagem de uma transformação linear:

$$\begin{array}{ccccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{u} \end{array}$$

em que $\mathbf{x} = (x_1, x_2, ..., x_n)$ e $\mathbf{u} = x_1u_1 + x_2u_2 + \cdots + x_ku_k$. T é uma transformação linear injetora. Assim, dar um código $\mathbf{C} \subset (\mathbb{F}_q)^n$ de dimensão k é equivalente a dar uma transformação linear injetora $T : (\mathbb{F}_q)^k \longrightarrow (\mathbb{F}_q)^n$ e definir $\mathbf{C} = \mathrm{Im}(\mathbf{T})$.

Exemplo 9.222. *Considere a transformação linear*

$$\begin{array}{ccccc} T & : & (\mathbb{F}_2)^2 & \longrightarrow & (\mathbb{F}_2)^5 \\ & & (x_1, x_2) & \longmapsto & (x_1, x_2, x_1, x_1 + x_2, x_2) \end{array}.$$

Temos que

$$T(x_1, x_2) = (0, 0, 0, 0, 0)\,, se\,(x_1, x_2, x_1, x_1 + x_2, x_2) = (0, 0, 0, 0, 0)\,,$$

ou seja, $x_1 = x_2 = 0$. *Logo Ker(T)ˊ* $= \{(0, 0)\}$. *Portanto, T é injetora e daí Im(T)* $= \mathbf{C}$ *(a imagem de T é um código* $\mathbf{C}$*). Como* $x_1, x_2 \in \mathbb{F}_2$, *temos* $|\mathbf{C}| = 2^2$*=4 e*

$$\mathbf{C} = \{(0, 0, 0, 0, 0)\,, (0, 1, 0, 1, 1)\,, (1, 0, 1, 1, 0)\,, (1, 1, 1, 0, 1)\}\,.$$

Além disso, $W(\mathbf{C})$ *=3 e* $\mathbf{C}$ *corrige* $t = \left[\frac{d-1}{2}\right]$*=1 erro.*

9.53.1 Matriz Geradora de um Código

Definição 9.223. *Dado um código linear* $\mathbf{C} \subset (\mathbb{F}_q)^n$, *chamaremos de parâmetros do código linear* $\mathbf{C}$ *os inteiros (n,k,d), em que k é a dimensão de* $\mathbf{C}$ *sobre* $\mathbb{F}_q$, *d representa a distância mínima de* $\mathbf{C}$ *e n é denominado o comprimento do código* $\mathbf{C}$.

Seja o código linear $\mathbf{C}$= $[\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k]$ com $B = \{\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k\}$ base de $\mathbf{C}$. A matriz

$$\mathbf{G}_{k\times n} = \begin{pmatrix} - & \mathrm{u}_1 & - \\ - & \mathbf{u}_2 & - \\ \vdots & \vdots & \vdots \\ - & \mathbf{u}_k & - \end{pmatrix}$$

é chamada de matriz geradora de $\mathbf{C}$ associada à base

$$B = \{\mathrm{u}_1, \mathbf{u}_2, ..., \mathbf{u}_k\}$$

.

Exemplo 9.224. *Do exemplo anterior* $B = \{(0, 1, 0, 1, 1)\,, (1, 0, 1, 1, 0)\}$ *é uma base de* $\mathbf{C}$ *e*

$$\mathbf{G} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

é uma matriz geradora do código linear $\mathbf{C}$. *De fato,*

$$\begin{pmatrix}0 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 0\end{pmatrix} = (0,0,0,0,0),$$
$$\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 0\end{pmatrix} = (1,0,1,1,0),$$
$$\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 0\end{pmatrix} = (0,1,0,1,1),$$
$$\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}0 & 1 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 0\end{pmatrix} = (1,1,1,0,1).$$

De maneira geral, consideramos a transformação linear definida por

$$\begin{array}{rccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{xG} \end{array}$$

Se $\mathbf{x} = (x_1, x_2, ..., x_n)$, temos $T(\mathbf{x}) = \mathbf{xG} = x_1u_1 + x_2u_2 + \cdots + x_ku_k$, ou seja, $T\left((\mathbb{F}_q)^k\right) = \mathbf{C}$. Podemos, então, considerar $(\mathbb{F}_q)^k$ como sendo um código da fonte, $\mathbf{C}$ o código do canal e a transformação T, uma codificação.

Além disso, ressaltamos que a matriz geradora $\mathbf{G}$ não é única, pois ela depende da base B. Portanto, mudando para uma base $\overline{B}$, teremos uma outra matriz geradora $\overline{\mathbf{G}}$ para o mesmo código $\mathbf{C}$. Da Álgebra Linear, sabemos que $\overline{\mathbf{G}}$ pode ser obtida de $\mathbf{G}$ através de operações elementares com as linhas de $\mathbf{G}$ e vice versa.

Os códigos podem ser construídos a partir de matrizes geradoras $\mathbf{G}$. Basta tomar uma matriz cujas linhas sejam linearmente independentes e definir um código como sendo a transformação linear

$$\begin{array}{rccc} T & : & (\mathbb{F}_q)^k & \longrightarrow & (\mathbb{F}_q)^n \\ & & \mathbf{x} & \longmapsto & \mathbf{xG} \end{array}$$

.

Códigos equivalentes

Definição 9.225. *Seja* $\mathbb{F}_q$ *um alfabeto e* n *um número natural. Diremos que uma função* $T : (\mathbb{F}_q)^n \longrightarrow (\mathbb{F}_q)^n$ *é uma isometria de* $(\mathbb{F}_q)^n$ *se ela preserva distâncias de Hamming, isto é:*

$$d(T(u), T(v)) = d(u, v); u, v \in (\mathbb{F}_q)^n.$$

Definição 9.226. *Dados dois códigos* $\mathbf{C}$ *e* $\mathbf{C}'$ *em* $(\mathbb{F}_q)^n$, *diremos que* $\mathbf{C}'$ *é equivalente a* $\mathbf{C}$ *se existir uma isometria* T *de* $(\mathbb{F}_q)^n$ *tal que* $T(\mathbf{C}) = \mathbf{C}'$.

Observamos que dessa definição decorre que dois códigos equivalentes têm os mesmos parâmetros n, k, d,

$$pois \begin{cases} T & é & injetora \Longrightarrow leva\ base\ em\ base\ (k) \\ T & é & isometria \Longrightarrow preserva\ distância\ (d) \\ T & : & (\mathbb{F}_q)^n \longrightarrow (\mathbb{F}_q)^n \end{cases}$$

A equivalência de códigos é uma relação de equivalência (reflexiva, simétrica e transitiva).

Uma forma mais simples de se obter a partir de um código linear $\mathbf{C}$ um código $\mathbf{C}'$ equivalente é efetuando-se sequências de operações sobre a matriz geradora $\mathbf{G}$ do código linear $\mathbf{C}$, do tipo:

- Permutação de duas colunas

- Multiplicação de uma coluna por um escalar não nulo.

Dessa forma, obtém-se uma matriza geradora $\mathbf{G}'$ de um código linear $\mathbf{C}'$ equivalente a $\mathbf{C}$, observando que realizar operações deste tipo em $\mathbf{G}$, implica realizá-las em todas as palavras de $\mathbf{C}$, o que caracteriza a isometria T.

A matriz $\mathbf{G}$ pode ser colocada na forma padrão efetuando-se as operarações elementares sobre as linhas ou colunas de $\mathbf{G}$. Denominaremos $\mathbf{G}^*$ a matriz de $\mathbf{G}$ na forma padrão.

$$\mathbf{G}^* = [I_k \,|A]$$

Assim, dado um código $\mathbf{C}$, existe um código $\mathbf{C}'$ com matriz geradora $\mathbf{G}^*$ na forma padrão.

Exemplo 9.227. *Dado o código* $\mathbf{C}$ *definido sobre* $\mathbb{F}_2$ *pela matriz* $\mathbf{G}$ *abaixo, encontre um código* $\mathbf{C}'$ *equivalente a* $\mathbf{C}$*, com matriz geradora na forama padrão.* $T : (\mathbb{F}_2)^4 \longrightarrow (\mathbb{F}_2)^6$

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

De $\mathbf{G}$, temos que $k = 4$, $n = 6$ e $|\mathbf{C}| = 2^4 = 16$

$$\begin{matrix} L_1 \\ L_2 \\ L_3 \\ L_4 \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} L_1 + L_3 \\ \\ \\ \\ \end{matrix} \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ L3 + L_4 \end{matrix}$$

$$\begin{matrix} \\ c_1 \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ c_2 \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ c_3 \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ c_4 \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ c_5 \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ c_6 \\ \\ \\ \\ \\ \end{matrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} L_2 + L_1 \\ \\ \\ \approx \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} L_4 + L_1 \\ \\ \\ \approx \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} L_2 + L_3 \\ \\ \\ \approx \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} c_3 \leftrightarrow c_4 \\ \\ \\ \approx \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} = [I_4 \,|A] \text{ em que}$$

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ e } A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}_{k \times (n-k) = 4 \times 2}.$$

9.54 Códigos Duais

Dados $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q)^n$, o produto interno de u e v é definido como sendo

$$\langle u, v \rangle = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

Propriedade 9.1. $\langle u, v \rangle = \langle v, u \rangle$

Propriedade 9.2. $\langle u + \lambda w, v \rangle = \langle u, v \rangle + \lambda \langle w, v \rangle$ *para todo* $\lambda \in \mathbb{F}_q$.

Definição 9.228. *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *um código linear, o código*

$$\mathbf{C}^{\perp} = \{v \in (\mathbb{F}_q)^n : \langle u, v\rangle = 0, \forall u \in \mathbf{C}\}$$

é chamado de código dual de $\mathbf{C}$.

Lema 9.229. *Se* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é um código linear, com matriz geradora* $\mathbf{G}$*, então*

(i) $\mathbf{C}^{\perp}$ *é um sub-espaço vetorial de* $(\mathbb{F}_q)^n$
(ii) $x \in \mathbf{C}^{\perp} \Leftrightarrow \mathbf{G}x^t = 0$

Demonstração. (i) Dados $u, v \in \mathbf{C}^{\perp}$ e $\lambda \in K$, temos para todo $x \in \mathbf{C}$, que $\langle u + \lambda v, x\rangle = \langle u, x\rangle + \lambda \langle v, x\rangle = 0$ e portanto, $u + \lambda v \in \mathbf{C}^{\perp}$, provando que $\mathbf{C}^{\perp}$ é um sub-sepaço vetorial de $(\mathbb{F}_q)^n$.

(ii) $x \in \mathbf{C}^{\perp} \Leftrightarrow x$ é ortogonal a todos elementos de $\mathbf{C} \Leftrightarrow \mathbf{G}\mathrm{x}^t = 0$ pois linhas de $\mathbf{G}$ formam uma base de $\mathbf{C}$. □

Proposição 9.230. *Seja* $\mathbf{C} \subset (\mathbb{F}_q)^n$ *é um código linear de dimensão* k *com matriz geradora* $\mathbf{G}$=$[I_k \,|A]$, *na forama padrão. Então*

(i) $dim\mathbf{C}^{\perp} = n - k$
(ii) $\boldsymbol{H}$=$[-A^t \,|I_{n-k}]$ *é uma matriz geradora de* $\mathbf{C}^{\perp}$.

Demonstração. (i) Temos que $v \in \mathbf{C}^{\perp} \Leftrightarrow \mathbf{G}v^t = 0$. Se $v = (v_1, v_2, \ldots, v_n)$ temos o sistema a seguir:

$$\left[\begin{array}{ccccc|ccc} 1 & 0 & 0 & 0 & 0 & a_{1,k+1} & \cdots & a_{1,n} \\ 0 & 1 & 0 & 0 & 0 & a_{2,k+1} & \cdots & a_{2,n} \\ 0 & 0 & \ddots & \vdots & \vdots & \vdots & \cdots & \\ \vdots & \vdots & \vdots & 1 & 0 & \vdots & \cdots & \\ 0 & 0 & \ldots & 0 & 1 & a_{k,k+1} & \cdots & a_{k,n} \end{array}\right]_{k\times n} \cdot \begin{bmatrix} v_1 \\ \vdots \\ \vdots \\ \vdots \\ v_n \end{bmatrix}_{n\times 1} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}_{k\times 1}.$$

Assim:

$$\left\{\begin{array}{ccccccccccc} v_1 & & & & +a_{1,k+1}.v_{k+1} & + & \cdots & + & a_{1,n}.v_n & = & 0 \\ & v_2 & & & +a_{2,k+1}.v_{k+1} & + & \cdots & + & a_{2,n}.v_n & = & 0 \\ & & \ddots & & \vdots & & & & & \vdots & \Longrightarrow \\ & & & \ddots & \vdots & & & & & \vdots & \\ & & & v_k & +a_{k,k+1}.v_{k+1} & + & \cdots & + & a_{k,n}.v_n & = & 0 \end{array}\right.$$

$$\left\{\begin{array}{ccccccccc} v_1 & = & -(a_{1,k+1}.v_{k+1} & + & \cdots & + & a_{1,n}.v_n) \\ v_2 & = & -(a_{2,k+1}.v_{k+1} & + & \cdots & + & a_{2,n}.v_n) \\ \vdots & & & & & & \\ v_k & = & -(a_{k,k+1}.v_{k+1} & + & \cdots & + & a_{k,n}.v_n) \end{array}\right. \Rightarrow \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_k \end{bmatrix} = -A \begin{bmatrix} v_{k+1} \\ v_{k+2} \\ \vdots \\ \vdots \\ v_n \end{bmatrix}$$

Logo:

$$v = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_k \end{bmatrix}$$

$$v = \begin{bmatrix} -(a_{1,k+1}.v_{k+1} + \cdots + a_{1,n}.v_n) \\ -(a_{2,k+1}.v_{k+1} + \cdots + a_{2,n}.v_n) \\ \vdots \\ -(a_{k,k+1}.v_{k+1} + \cdots + a_{k,n}.v_n) \\ v_{k+1} \\ v_{k+2} \\ \vdots \\ v_n \end{bmatrix}$$

$$v = v_{k+1} \begin{bmatrix} -a_{1,k+1} \\ -a_{2,k+1} \\ \vdots \\ -a_{k,k+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + v_n \begin{bmatrix} -a_{1,n} \\ -a_{2,n} \\ \vdots \\ -a_{k,n} \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

em que $v_{k+1\in}, v_{k+2}, \ldots, v_n \in \mathbb{F}_q$. Como $\mathbb{F}_q$ possui q elementos, existem $q^{n-(k+1)+1} = q^{n-k}$ possibilidades para v, ou seja, $\mathbf{C}^\perp$ possui q^{n-k} elementos, o que significa que sua dimensão é $n-k$.

(ii) As linhas de $\mathbf{H}$ são linearmente independentes, devido ao bloco I_{n-k}. Portanto geram um subespaço vetorial de dimensão $n-k$. Desse modo, a $i-$*ésima* linha de $\mathbf{H}$, denotada por $\mathbf{H}_i; 1 \leq i \leq n-k$, é dado por:

$$\mathbf{H}_i = \big(-a_{1i}, \quad -a_{2i}, \quad \ldots, \quad -a_{ki}, \quad 0, \quad 0, \quad \ldots \quad 1, \quad 0, \quad \ldots, \quad 0\big)$$

$$\nearrow$$

Posição i

e a $j-$*ésima* linha de $\mathbf{G}$, denotada por $\mathbf{G}_j; 1 \leq i \leq k$ é dada por

$$\mathbf{G}_j = \big(0, \quad 0, \quad \ldots \quad 1, \quad 0, \quad \ldots, \quad 0, \quad a_{j1}, \quad a_{j2}, \quad \ldots, \quad a_{jn-k}\big)$$

$$\uparrow$$

Posição j

Daí, $\langle \mathbf{H}_i, \mathbf{G}_j \rangle = -a_{ji} + a_{ji} = 0$, ou seja, todas as linhas de $\mathbf{H}$ são ortogonais às linhas de $\mathbf{G}$. Logo, o espaço gerado pelas linhas de $\mathbf{H}$ está contido em $\mathbf{C}^\perp$, e como esses dois espaços têm a mesma dimensão, eles coincidem, mostrando assim que $\mathbf{H}$ é uma matriz geradora de $\mathbf{C}^\perp$. □

Proposição 9.231. *Seja* $\mathbf{C}$ *um código com dimensão* k *em* $(\mathbb{F}_q)^n$ *com matriz geradora* $\mathbf{G}$. *Uma matriz* $\mathbf{H}$ *de ordem* $(n-k) \times n$, *com coeficientes em* $\mathbb{F}_q$ *e com linhas linearmente independentes, é uma matriz geradora de* $\mathbf{C}^\perp$ *se, e somente, se* $\mathbf{G}\mathbf{H}^t = 0$.

Demonstração. Exercício. □

Corolário 9.232. $\left(\mathbf{C}^\perp\right)^\perp = \mathbf{C}$

Demonstração. Exercício. □

Como consequência temos a seguinte

Proposição 9.233. *Seja* $\mathbf{C}$ *um código linear e consideremos* $\mathbf{H}$ *uma matriz geradora de* $\mathbf{C}^\perp$. *Temos então que:* $v \in \mathbf{C} \Leftrightarrow \mathbf{H}v^t = o$.

Demonstração. $v \in \mathbf{C} \Leftrightarrow v \in \left(\mathbf{C}^{\perp}\right)^{\perp} \Leftrightarrow \mathbf{H}\mathrm{v}^t = o.$ □

Esta proposição fornece uma maneira de caracterizar os elementos de um código $\mathbf{C}$ por uma condição de anulamento. A matriz $\mathbf{H}$, geradora de $\mathbf{C}^{\perp}$, é chamada *matriz verificação de paridade* de $\mathbf{C}$.

Exemplo 9.234. *Seja dado o código* $\mathbf{C}$ *sobre* $\mathbb{F}_2$ *com matriz geradora* $\mathbf{G} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array}\right)$. *Verifique se o vetor* $v = \begin{pmatrix} 0, & 1, & 1, & 1 \end{pmatrix} \in (\mathbb{F}_2)^4$ *pertence a* $\mathbf{C}$.

Solução 9.235. *Nesse caso, temos* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *e* $-A^t = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *e daí*

$$\mathbf{H} = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right).$$

Além disso,

$$\mathbf{H}v^t = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}_{3\times 4} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$\therefore v \notin \mathbf{C}$.

Definição 9.236. *Dados um código* $\mathbf{C}$ *,com matriz de verificação de paridade* $\mathbf{H}$*, e um vetor* $v \in (\mathbb{F}_q)^n$ *, chamamos o vetor* $\mathbf{H}v^t$ *de sídrome de* v.

A matriz de verificação de paridade de um código $\mathbf{C}$ determina ,de maneira simples, se um vetor $v \in (\mathbb{F}_q)^n$ pertence ou não a ele. Além disso, contém, de forma muito simples, informações sobre o valor do peso W do código $\mathbf{C}$.

Proposição 9.237. *Seja* $\mathbf{H}$ *a matriz de verificação de paridade de um código* $\mathbf{C}$*. Temos que o peso de* $\mathbf{C}$ *é maior do que ou igual a* s *se, e somente se, quaisquer* $s-1$ *colunas de* $\mathbf{H}$ *são linearmente independentes.*

Demonstração. ($\Leftarrow$)Admitamos que cada conjunto de $s-1$ colunas de $\mathbf{H}$ é linearmente independente.

Seja $v \in \mathbf{C} - \{o\}$, $v = (v_1, v_2, \ldots, v_n)$ e sejam $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_n$ as colunas de $\mathbf{H}$. Como $\mathbf{H}v^t = o$, temos que $v_1\mathbf{H}_1 + v_2\mathbf{H}_2 + \cdots + v_n\mathbf{H}_n = 0$. Além disso, sabemos que $W(\mathbf{C})$ é o número de $v_i \neq 0$; $i = 1, \ldots, n$. Logo se $W(\mathbf{C}) \leq s-1$ teríamos uma combinação de $s-1$ ou menos colunas de $\mathbf{H}$ igual ao vetor nulo, com coeficientes v_i não todos nulos. Mas contraria a nossa hipótese. Logo, $W(\mathbf{v}) \geq s \; \forall \; v \in \mathbf{C}$ e, portanto $W(\mathbf{C}) \geq s$.

($\Rightarrow$) Admitamos que $W(\mathbf{C}) \geq s$.

Suponhamos por absurdo que $\mathbf{H}$ tenha pelo menos um conjunto com $s-1$ colunas linearmente dependentes, digamos, $\mathbf{H}_{i,1}, \mathbf{H}_{i,2}, \ldots, \mathbf{H}_{i,s-1}$. Logo, existiria $v_{i,1}, v_{i,2}, \ldots, v_{i,s-1} \in \mathbb{F}_q$, nem todos nulos, tais que

$$v_{i,1}\mathbf{H}_{i,1} + v_{i,2}\mathbf{H}_{i,2} + \cdots + v_{i,s-1}\mathbf{H}_{i,s-1} = 0$$

o que é equivalente a $\mathbf{H}v^t = o$, com

$$v = (0, \ldots v_{i,1}, 0, \ldots, v_{i,s-1}, 0, \ldots, 0) \in (\mathbb{F}_q)^n .$$

Nesse caso, $v \in \mathbf{C}$ e $W(\mathbf{C}) = s-1$, o que contraria a nossa hipótese. □

Teorema 9.238. *Seja* $\mathbf{H}$ *a matriz de verificação de paridade de um código* $\mathbf{C}$*. O peso de* $\mathbf{C}$ *é igual a* s*, se e somente se, quaisquer* $s-1$ *colunas de* $\mathbf{H}$ *são linearmente independentes e existem* s *colunas de* $\mathbf{H}$ *linearmente dependentes.*

Demonstração. ($\Rightarrow$) Admitamos $W(\mathbf{C}) = s$.

Pela **Proposição 6.10** todo conjunto de $s-1$ colunas de $\mathbf{H}$ é linearmente independente. Se não existir pelo menos um conjunto com s colunas de $\mathbf{H}$ linearmente dependentes, ter-se-ia pela proposição anterior que $W(\mathbf{C}) \geq s+1$, o que é absurdo.

Portanto, existe pelo menos um conjunto com s colunas de $\mathbf{H}$ que é linearmente dependentes.

($\Leftarrow$) Todo conjunto com $s-1$ colunas de $\mathbf{H}$ é L.I. e existe um conjunto com s colunas de $\mathbf{H}$ que é $L.D.$

Pela proposição anterior tem-se que $W(\mathbf{C}) \geq s$. Mas $W(\mathbf{C})$ não pode ser estritamente maior do que s, pois pela proposição anterior, todo conjunto com s colunas de $\mathbf{H}$ seria linearmente independente, o que é absurdo. Portanto, $W(\mathbf{C}) = s$. □

Corolário 9.239. *Limitante de Singleton: Os parâmetros (n,k,d) de um código linear satisfazem à desigualdade* $d \leq n-k+1$.

Demonstração. Seja $\mathbf{H}$ uma matriz de verificação de paridade de um código linear $\mathbf{C}$, com parâmetros (n,k,d). Então o posto de $\mathbf{H}$ é $n-k$, pois a mesma é uma matriz de ordem $(n-k)\times n$, isto é, $n-k$ linhas linearmente independentes. Logo, cada coluna de $\mathbf{H}$ tem $n-k$ entradas, ou seja, comprimento $n-k$, ou ainda estão em $(\mathbb{F}_q)^{n-k}$. Pelo teorema anterior, quaisquer $d-1$ colunas de $\mathbf{H}$ são linearmente independentes.

Como um conjunto de vetores de $(\mathbb{F}_q)^{n-k}$ que é $L.I.$ tem no máximo $n-k$ vetores, então $d-1 \leq n-k$. Daí $d \leq n-k+1$. □

9.55 Decodificação

Decodificação é o procedimento de detecção e correção de erros num determinado código.

Inicialmente, define-se o vetor $\mathbf{e}$ como sendo a diferença entre o vetor recebido $\mathbf{r}$ e o vetor transmitido $\mathbf{v}$.

$$\mathbf{e} = \mathbf{r} - \mathbf{v}$$

Se $\mathbf{H}$ é a matriz de verificação de paridade do código, temos que:

$$\mathbf{H}\mathbf{e}^t = \mathbf{H}(\mathbf{r}-\mathbf{v})^t = \mathbf{H}\mathbf{r}^t - \mathbf{H}\mathbf{v}^t = \mathbf{H}\mathbf{r}^t, \text{pois } \mathbf{H}\mathbf{v}^t = o$$

Portanto, a palavra recebida $\mathbf{r}$ tem a mesma síndrome do vetor erro $\mathbf{e}$.

Seja $\mathbf{H}_i$ a $i-ésima$ coluna de $\mathbf{H}$. Se $\mathbf{e} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ então

$$\sum_{i=1}^{n} \alpha_i \mathbf{H}_i = \mathbf{H}\mathbf{e}^t = \mathbf{H}\mathbf{r}^t.$$

Lema 9.240. *Seja* $\mathbf{C}$ *um código linear em* $(\mathbb{F}_q)^n$ *com capacidade de correção de erros igual a k. Se* $\boldsymbol{r} \in (\mathbb{F}_q)^n$ *e* $\mathbf{v} \in \mathbf{C}$ *são tais que* $d(\boldsymbol{v},\boldsymbol{r}) \leq k$, *então existe um único vetor* $\mathbf{e}$ *com* $W(\mathbf{e}) \leq k$ *cuja sídrome é igual à síndrome de* $\boldsymbol{r}$ *e tal que* $\boldsymbol{v}=\boldsymbol{r}$-$\mathbf{e}$.

Demonstração. De fato, **v=r-e** tem a propriedade do Lema, já que

$$W(\mathbf{e}) = d(\mathbf{v},\mathbf{r}) \leq k.$$

Para provar a unicidade, suponhamos que $\mathbf{e} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ e
$\mathbf{e}' = (\alpha_1', \alpha_2', \ldots, \alpha_n')$ sejam tais que $W(\mathbf{e}) \leq k$ e $W(\mathbf{e}') \leq k$ e tenham a mesma síndrome que $\mathbf{r}$. Então, se $\mathbf{H}$ é uma matriz de verificação de paridade de $\mathbf{C}$, temos

$$\mathbf{He}^t = \mathbf{He}'^t \Longrightarrow \sum_{i=1}^{n} \alpha_i \mathbf{H}_i = \sum_{i=1}^{n} \alpha_i' \mathbf{H}_i,$$

o que nos dá uma relação de dependência linear entre $2k(\leq d-1)$ colunas de $\mathbf{H}$. Como quaisquer $d-1$ colunas de $\mathbf{H}$ são linearmente independentes, temos $\alpha_i = \alpha_i'$ para todo i, logo $\mathbf{e} = \mathbf{e}'$. □

Exemplo 9.241. *Determine* $\mathbf{e}$ *quando* $W(\mathbf{e}) \leq 1$. *Admitamos que o código* $\mathbf{C}$ *tenha distância mínima* $d \geq 3$ *e que o vetor erro* $\mathbf{e}$*, introduzido entre a palavra transmitida* $\boldsymbol{v}$ *e a palavra recebida* $\boldsymbol{r}$*, seja tal que* $W(\mathbf{e}) \leq 1$. *Isto é, o canal introduziu no máximo um erro. Se* $\mathbf{He}^t = o$*, então* $\boldsymbol{r} \in \mathbf{C}$ *e se toma* $\boldsymbol{v} = \boldsymbol{r}$. *Suponhamos* $\mathbf{He}^t \neq o$*, então* $W(\mathbf{e}) = 1$ *e, portanto,* $\mathbf{e}$ *tem apenas uma coordenada não nula. Nesse caso, consideremos que* $\mathbf{e} = (0, \ldots, \alpha, \ldots, 0)$ *com* $\alpha \neq 0$ *na* $i-$*ésima posição. Logo,*

$$\mathbf{He}^t = \alpha \mathbf{H}_i.$$

Portanto, não conhecendo

$$\mathbf{He}^t = \mathbf{Hr}^t = \alpha \mathbf{H}_i,$$

podemos determinar $\mathbf{e}$ *como sendo um vetor com todas as componentes nulas exceto a* $i-$*ésima componente que é* α. *Note que* i *acima é bem determinado, pois* $d \geq 3$.

Ilustração 9.242. *Seja* $\mathbf{C}$ *o código do* ***Exemplo 5.3****. Esse código tem matriz teste de paridade*

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Seja $\boldsymbol{r}$=$(1,0,1,0,0)$ *uma palavra recebida, logo,*

$$\mathbf{He}^t = \mathbf{Hr}^t = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1.\mathbf{H}_4$$

Portanto, $\mathbf{e}$=$(0,0,0,1,0)$ *e, consequentemente,*

$$\mathbf{v} = \mathbf{r} - \mathbf{e} = (1,0,1,1,0.$$

Com base no exemplo anterior, será estabelecido um algoritmo de decodificação para códigos corretores de um erro.

Considere $\mathbf{H}$ a matriz de verificação de paridade do código $\mathbf{C}$ e seja $\mathbf{r}$ o vetor recebido.(Admitamos $d \geq 3$)

(a) Calcule $\mathbf{Hr}^t$.

(b) Se $\mathbf{Hr}^t = o$, aceite $\mathbf{r}$ como a palavra transmitida.

(c) Se $\mathbf{Hr}^t = \mathbf{s} \neq o$ compare $\mathbf{s}$ com colunas de $\mathbf{H}$.

(d) Se existirem i e α tais que $\mathbf{s}^t = \alpha \mathbf{H}_i$, para $\alpha \in \mathbb{F}_q$, então $\mathbf{e}$ é a $n = upla$ com α na posição i e zeros nas outras posições. Corrija $\mathbf{r}$ pondo $\mathbf{v} = \mathbf{r} - \mathbf{e}$.

(e) Se o contrário de **(d)** ocorrer, então mais de um erro foi cometido.

Considere $\mathbf{C}$ um código corretor de erros em $(\mathbb{F}_q)^n$ cuja matriz de verificação de paridade é $\mathbf{H}$. Sejam d a distância mínima de $\mathbf{C}$ e $k = \left[\frac{d-1}{2}\right]$. Recorde que $\mathbf{e}$ e $\mathbf{r}$ têm a mesma síndrome e se

$$W(\mathbf{e}) = d(\mathbf{r}, \mathbf{v}) < k,$$

então $\mathbf{e}$ é univocamente determinado por $\mathbf{r}$.

Seja $u \in (\mathbb{F}_q)^n$. Defina

$$u + \mathbf{C} = \{u + v : v \in \mathbf{C}\}.$$

Lema 9.243. *Os vetores u e v de $(\mathbb{F}_q)^n$ têm a mesma síndrome se, e somente se, $u \in v + \mathbf{C}$.*

Demonstração. $\mathbf{H}u^t = \mathbf{H}v^t \iff \mathbf{H}(u-v)^t = o \iff u - v \in \mathbf{C} \iff u \in v + \mathbf{C}$. □

Exemplo 9.244. *Seja $\mathbf{C}$ o (4,2)-código gerado sobre $\mathbb{F}_2$ pela matriz*

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Logo,

$$\mathbf{C} = \{(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,0)\},$$

e as classes laterais segundo $\mathbf{C}$ são:

$$(0,0,0,0) + \mathbf{C} = \{(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,0)\}$$

$$(1,0,0,0) + \mathbf{C} = \{(1,0,0,0), (0,0,1,1), (1,1,0,1), (0,1,1,0)\}$$

$$(0,1,0,0) + \mathbf{C} = \{(0,1,0,0), (1,1,1,1), (0,0,0,1), (1,0,1,0)\}$$

$$(0,1,0,0) + \mathbf{C} = \{(0,0,1,0), (1,0,0,1), (0,1,1,1), (1,1,0,0)\}.$$

Uma correspondência 1-1 entre classes laterais e síndromes é estabelecida pelo Lema acima. Todos os elementos de uma classe lateral têm a mesma síndrome.

Definição 9.245. *Um vetor de peso mínimo numa classe lateral é chamado de elemento líder dessa classe.*

Proposição 9.246. *Seja $\mathbf{C}$ um código linear em $(\mathbb{F}_q)^n$ com distância mínima d. Se $u \in (\mathbb{F}_q)^n$ é tal que*

$$W(u) \leq \left[\frac{d-1}{2}\right] = k,$$

então u é o único elemento líder de sua classe.

Demonstração. Suponhamos que u e $v \in (\mathbb{F}_q)^n$ com $W(u) \leq \left[\frac{d-1}{2}\right]$ e $W(v) \leq \left[\frac{d-1}{2}\right]$. Se $u - v \in \mathbf{C}$, então

$$W(u-v) \leq W(u) + W(v) \leq \left[\frac{d-1}{2}\right] + \left[\frac{d-1}{2}\right] \leq d - 1;$$

Logo, $u - v = o$ e, portanto, $u = v$. □

Observação 9.247. *:Para achar líderes de classes, tomamos os elementos u tais que* $W(u) \leq \left[\frac{d-1}{2}\right]$. *Cada um desses elementos é líder de uma e somente uma classe. Esses líderes são todos aqueles de peso menor ou igual a* $\left[\frac{d-1}{2}\right]$, *os outros líderes não serão considerados. Agora discutiremos um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é* $k = \left[\frac{d-1}{2}\right]$.

Determine todos os elementos de $u \in (\mathbb{F}_q)^n$, tal que $W(u) \leq k$. Em seguida, calcule as síndromes desses elementos e coloque esses dados numa tabela. Seja $\mathbf{r}$ uma palavra recebida.

O Algoritmo de Decodificação

(1) Calcule a síndrome $\mathbf{s}^t = \mathbf{H}\mathbf{r}^t$.

(2) Se $\mathbf{s}$ está na tabela, seja l o elemento líder da classe determinada por $\mathbf{s}$; troque por $\mathbf{r} - l$.

(3) Se $\mathbf{s}$ não está na tabela, então na mensagem recebida foram cometidos mais do que k erros.

Justificativa: Dado $\mathbf{r}$, sejam $\mathbf{v}$ e $\mathbf{e}$, respectivamente, a mensagem transmitida e o vetor erro. Como $\mathbf{H}\mathbf{e}^t = \mathbf{H}\mathbf{r}^t$, temos que a classe lateral onde $\mathbf{e}$ se encontra está determinada pela síndrome de $\mathbf{r}$. Se

$W(\mathbf{e}) \leq k$, temos que $\mathbf{e}$ é o único elemento líder l de sua classe e, portanto, é conhecido e se encontra na tabela. Consequentemente,$\mathbf{v} = \mathbf{r} - \mathbf{e} = \mathbf{r} - l$ é determinado.

Exemplo 9.248. *Considere o código linear definido sobre* $\mathbb{F}_2$ *com matriz de verificação de paridade* $\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. *Observe que*

n-k=3, como n=6, então k=3. Alé disso, duas a duas, as colunas de $\mathbf{H}$ *são L.I. e existem três colunas* $1^a, 2^a$ *e* 4^a *L.D. Logo,* $d = 3$, *pois* $s - 1 = 2$ *e portanto, t=1. Os vetores de* $(\mathbb{F}_2)^6$ *com* $W(u) \leq 1$ *e suas respectivas síndromes estão relacionados na tabela abaixo:*

Líder	*Síndrome*
(0,0,0,0,0,0)	*(0,0,0)*
(0,0,0,0,0,1)	*(1,0,1)*
(0,0,0,0,1,0)	*(0,1,1)*
(0,0,0,1,0,0)	*(1,1,0)*
(0,0,1,0,0,0)	*(0,0,1)*
(0,1,0,0,0,0)	*(0,1,0)*
(1,0,0,0,0,0)	*(1,0,0)*

Suponhamos que a palavra recebida seja:

(a) $\mathbf{r} =$ *(1,0,0,0,1,1). Logo,* $\mathbf{H}\mathbf{r}^t =$*(0,1,0)*^{t} *e, portanto*

$$\mathbf{e} = (0, 1, 0, 0, 0, 0).$$

Consequentemente,

$$\mathbf{v} = \mathbf{r} - \mathbf{e} = (1, 0, 0, 0, 1, 1) - (0, 1, 0, 0, 0, 0) = (1, 1, 0, 0, 1, 1).$$

(b) $\mathbf{r} =$ *(1,1,1,1,1,1). Logo,* $\mathbf{H}\mathbf{r}^t =$*(1,1,1)*^{t} *que não se encontra na tabela. Sendo assim, foi cometido mais do que 1 erro na mensagem* $\mathbf{r}$.

9.56 Conclusão

O mini-curso apresenta e desenvolve os fudamentos matemáticos da Teoria dos Códigos. E por se tratar de um vasto campo tendo várias ramificações em diversas áreas da matemática, concentra-se nos aspectos de natureza algébrica.

Referências

[1] CAIN, J. B.,CLARK, G. C., e GEIST, J.M. *Punctured convolutional codes of rate (n- 1)/n and simplified maximum likelihood decoding*, IEEE Transactions on Information Theory, vol. IT-25, pp. 97-100, janeiro,1979.

[2] CLARK,G.C., e CAIN,J.B., *Error-Correction Coding for Digital Communication,* John Wiley, 1985.

[3] ELIAS P., e CAIN,J.B., *Coding for noisy channels,* IRE Conv. Rec., 4ª Parte, pp. 37-47,1955.

[4] HEFEZ, A. e VILELA, M.L.T., *Códigos Corretores de Erros,* IMPA, Série dee Computação e Matemática, Rio de Janeiro, 2002.

[5] LIN, S. e COSTELLO, Jr. D. J., *Error Control Coding: Fundamentals and Applications,* Prentice-Hall, 1983.

[6] MACWILLIAMS, F.J., E SLOANE, N.J.A., *The Theory of Error-Correcting Codes,* North-Holland, Amsterdã, 1992.

[7] MASSEY, J. L., *Shift Register Synthesis an BCH Decoding,* IEEE Trans. Inform. Theory, VOL. IT-15 pp. 122-127, January 1969.

[8] NIEDERRETER, H., e LIDL, R., *Introduction to Finite Fields and Their Applications,* Cambridge University Press.

[9] SINGH,S.,*O Livro dos Códigos,* Editora Record, Rio de Janeiro - São Paulo, 2003.

[10] VITERBI, A. J., *Error bounds for convolutional codes and an asymptotically optimum decoding algorithm*, IEEE Transactions on Information Theory IT-13 pp. 260- 269, abril,1967.

[11] WOZENCRAFT,J.M., e REIFEN, B., *Sequential decoding,* MIT Press, Cambridge, Massachussets,1961.

Teste da razão de verossimilhanças sinalizada em modelo com erros nas variáveis

Tatiane Ferreira do Nascimento Melo
Doutoranda em Estatística - IME/USP

Orientadora:Profa. Dra. Silvia Lopes de Paula Ferrari IME/USP, Cidade Universitária
São Paulo - SP
E-mail: sferrari@ime.usp.br

Em problemas práticos existem situações em que a covariável (variável explicativa) é observada com erro de mensuração, ou seja, não é observada diretamente. Um exemplo é apresentado por Fuller (1987), em que o interesse consiste em relacionar a produção de um certo cereal com o nível de nitrogênio disponível no solo. A concentração de nitrogênio é obtida indiretamente através de análises laboratoriais, sujeitas a erros. Aoki et al. (2001) realizaram um estudo em que o interesse é comparar a eficácia de dois tipos de escovas de dentes na remoção de placa bacteriana; a covariável é o índice de placa antes da escovação e a variável resposta é o índice de placa após a escovação. Neste caso, é razóavel supor que a covariável está sujeita a erros de medição, pois a quantidade de placa bacteriana é avaliada imprecisamente e é determinada de forma semelhante antes e após a escovação. Nos exemplos apresentados acima os modelos com erros de medição, também chamados de modelos com erros nas variáveis, podem ser usados.

Para definir o modelo linear com erros nas variáveis consideramos primeiramente o modelo de regressão linear simples

$$Y_i = \alpha + \beta x_i + e_i, \tag{37}$$

com $i = 1, 2, \ldots, n$. Neste caso, a quantidade x_i não é observada diretamente mas com erros de medida. Denotaremos tal erro por u_i. Então o valor que se observa é

$$X_i = x_i + u_i, \tag{38}$$

com $i = 1, 2, \ldots, n$. As suposições sobre o modelo são: $\mathrm{E}(e_i) = 0 = \mathrm{E}(u_i)$, $\mathrm{E}(x_i) = \mu_x$, $\mathrm{Var}(e_i) = \sigma_e^2$, $\mathrm{Var}(u_i) = \sigma_u^2$, $\mathrm{Var}(x_i) = \sigma_x^2$, $\mathrm{Cov}(e_i, e_j) = 0 = \mathrm{Cov}(u_i, u_j)$, $i \neq j$ e $\mathrm{Cov}(e_i, u_i) = \mathrm{Cov}(x_i, e_i) = \mathrm{Cov}(x_i, u_i) = 0$. É comum se supor que o vetor aleatório $(x_i, e_i, u_i)^\top$ segue uma distribuição normal trivariada. Aqui, consideramos uma família de distribuições multivariadas que tem como caso especial, a distribuição normal e a distribuição t-Student multivariada. Mais especificamente admitimos que $(x_i, e_i, u_i)^\top$ tem distribuição elíptica trivariada. Assim, o vetor aleatório $Z_i = (Y_i, X_i)^\top$ tem distribuição elíptica bivariada (Fang et al., 1990) com vetor de locação μ, matriz de dispersão Σ, sendo

$$\mu = \mu(\theta) = \begin{pmatrix} \alpha + \beta\mu_x \\ \mu_x \end{pmatrix} \quad \text{e} \quad \Sigma = \Sigma(\theta) = \begin{pmatrix} \beta^2\sigma_x^2 + \sigma_e^2 & \beta\sigma_x^2 \\ \beta\sigma_x^2 & \sigma_x^2 + \sigma_u^2 \end{pmatrix}.$$

Como o modelo definido em (37)-(38) não é identificável é comum supor que a razão $\lambda_e = \sigma_e^2/\sigma_u^2$ ou $\lambda_x = \sigma_x^2/\sigma_u^2$ é conhecida (Fuller, 1987), ou que o intercepto α é conhecido (Aoki et al., 2001).

Inferência em modelos com erros nas variáveis, em particular para o modelo acima, é usualmente baseada em aproximações assintóticas de primeira ordem, que podem ser pouco acuradas quando a amostra é pequena ou mesmo de tamanho moderado. Em geral, esse é o caso do teste da razão de verossimilhanças sinalizada, cuja estatística, r, tem distribuição assintótica normal padrão, sob a hipótese nula, com erro de ordem $n^{-1/2}$, onde n é o tamanho da amostra. Com o objetivo de melhorar esta

aproximação, Barndorff–Nielsen (1986) propôs uma nova estatística de teste, r^*, que, sob a hipótese nula, tem, assintoticamente, distribuição normal padrão com erro de ordem $n^{-3/2}$. A estatística r^* depende de uma estatística ancilar tal que, juntamente com o estimador de máxima verossimilhança, constitua uma estatística suficiente para o modelo. Esta estatística modificada é dada por $r^* = r - (1/r)\log\gamma$, onde γ envolve a matriz de informação observada e quantidades denominadas por derivadas com respeito ao espaço amostral. Nosso objetivo é obter γ no modelo com erros nas variáveis dado em (37)-(38), quando a variável aleatória Z_i segue uma distribuição elíptica bivariada.

Realizamos um estudo de simulação de Monte Carlo para avaliar a eficácia do ajuste de Barndorff–Nielsen. Na Figura 1 temos o gráfico dos quantis exatos versus quantis assintóticos das estatísticas r e r^* quando a distribuição considerada é normal, a razão λ_x é conhecida e $n = 10$. Observamos que o teste baseado em r^* tem desempenho melhor que o baseado na estatística original r, pois a estatística r^* apresenta quantis mais próximos dos quantis da distribuição normal padrão do que a estatística r.

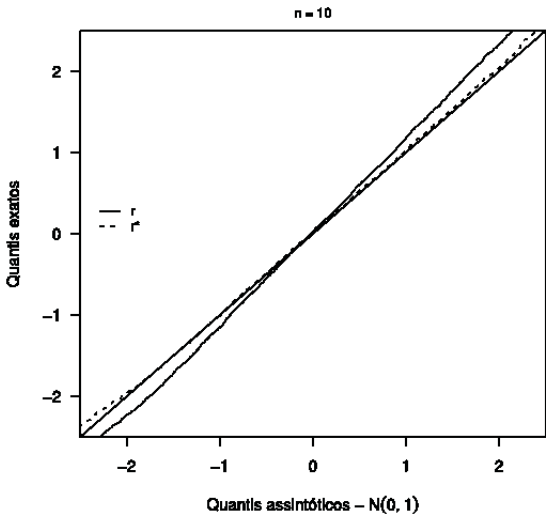


Figura 20: Gráfico dos quantis assintóticos versus quantis das estatísticas r e r^*

Referências

[1] R. Aoki, H. Bolfarine e J. M. Singer, Null intercept measurement error regression models, *Test*, 10 (2001) 441-457.

[2] O. E. Barndorff-Nielsen, Inference on full or partial parameters, based on the standardized signed log likelihood ratio, *Biometrika*, 73 (1986) 307-322.

[3] K. Fang, S. Kotz e K. Wang NG, "Symmetric Multivariate and Related Distributions", Chapman and Hall, 1990.

[4] S. Fuller, "Measurement Error Models", Wiley, 1987.

Problema de Valores de Contorno e Teoria de Sturm-Liouville aplicados ao escoamento de fluido em uma rocha porosa.

Macêdo, A. S., Silva, T. S.
Graduandas em Matemática - UEG/Iporá

Orientador:Prof. Rodrigo Miyasaki
UEG - Iporá
76200-000 Iporá-Go
E-mail: rodrigomiyasaki@yahoo.com.br

Um meio poroso, como por exemplo o solo, uma rocha, ou qualquer outro corpo poroso permite a passagem de algumas substâncias por meio de um solvente. O transporte destas substâncias pode ser causado por alguns processos físicos e químicos, os processos físicos envolvem a advecção, processo pelo qual o soluto é transportado pela água em movimento, dispersão hidrodinâmica e dispersão mecânica. Este trabalho centra-se em um exemplo como os casos citados.

Problema

Pelos poros de uma camada de rocha porosa, flui água com soluto. O soluto é transportado pelo movimento total do fluxo da água que é chamado de avecção. Este transporte também pode ocorrer pela dispersão mecânica, que acontece pelas variações da velocidade da água dentro dos poros, observe a figura 1.

Figura 1: Rocha Porosa

A forma unidimensional da equação de avecção - dispersão para um soluto não reativo dissolvido em um meio poroso saturado, homogêneo isotrópico sob um fluxo uniforme constante é:

$$C_t + vC_x = DC_{xx} \quad 0 < x < L, \quad t > 0$$

Onde $C(x,t)$, é a concentração do soluto, v é a velocidade média linear da água, D é o coeficiente de dispersão hidrodinâmica e x é o comprimento do caminho. Suponha que as condições de contorno sejam

$$C(0,t) = 0 \qquad C_x(L,t) = 0, \qquad t > 0$$

e condição inicial

$$C(x,0) = f(x), \qquad 0 < x < L.$$

utilizando o método de separação de variáveis e Teoria de Sturm-Liouville, admite-se a seguinte solução

$$C(x,t) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n D t} e^{\frac{vx}{2D}} \sin(\beta_n x)$$

ilustrada pelo seguinte gráfico

Gráfico 1: Concentração em função do tempo e espaço

Resultados Obtidos

A superfície ilustrada pelo gráfico tem coordenada Z para a concentração, x é o caminho percorrido e y o tempo. O desenvolvimento da solução em função do tempo e do espaço é justamente aquele proposto pelas condições de contorno que rege como será a solução nas extremidades e a condição inicial que vai se modificando de acordo com a solução dada.

Referências

[1] B. William, R. Diprima, "Equações Diferenciais Elementares e Problemas de Valores de Contorno", LTC, São Paulo, 2006.

[2] C. Edwards, D. Penney, "Equações Diferenciais Elementares com Problemas de Contorno, PHB, Rio de Janeiro, 1995.

A complementaridade entre a linguagem corrente e a linguagem matemática.

Tatiana Marla da Costa
Especialista em Educação Matemática

CEPAE - UFG
Goiânia - GO
E-mail: tatianamarla@hotmail.com

Objetivo da Pesquisa

O objetivo do trabalho será mostrar como se da o processo de formação de conceitos das crianças, no ensino da Álgebra do Ensino Fundamental, e com isso, demonstrar a importância da relação de complementaridade entre a linguagem corrente e a linguagem matemática.

Justificativa

Ao tratarmos de Linguagem e Matemática, é possível perceber a importância da relação entre ambas, pois os primeiros problemas matemáticos foram resolvidos através da linguagem o que possibilitou os mais variados discursos. Com o tempo essas resoluções foram substituídas por símbolos que vem sendo utilizados ate hoje, provocando então uma barreira entre os alunos e a matemática, por isso não ser visível, os objetivos esperados nem sempre vem sendo atingidos de forma satisfatória.

A maioria dos professores de matemática ignora a linguagem, ensinando apenas resoluções com símbolos, e existem vários fatores que contribuem para isso, como o tempo, a falta de recursos didáticos, o Projeto Político Pegagógico da instituição e até mesmo a falta de interesse por parte do educador. Formando então alunos com capacidade insuficiente para interpretar e assimilar conteúdos matemáticos. Logo nos primeiros anos escolares, deveria ser apresentada aos alunos esta relação de complementaridade entre a

Linguagem e a Matemática para que as crianças iniciem seu processo de formação de conceitos, desenvolvendo o raciocínio lógico e intuitivo.

Mas o fato é que o ensino da matemática e da língua materna nunca se articulam para uma ação conjunta, é como se as duas fossem coisas diferentes, e nos próprios alunos podemos observar isto com frases do tipo: "eu sou bom em matemática e péssimo em português´' ou "eu nasci para fazer contas não para ler e escrever".

E como sabemos o discurso não é bem assim, pois na mais simples matemática do dia a dia pressupõem um conhecimento da língua materna, pelo menos em sua forma oral e escrita.

Então podemos observar que tanto a matemática quanto a língua materna, funcionam como um instrumento de intervenção nos processos gerais do conhecimento para a formação cultural do homem.

Segundo Rabelo (2002, pg. 83):

Se um dos principais objetivos de se trabalhar a língua escrita é a formação de um bom leitor e "escritor", um dos principais objetivos de se ensinar matemática é a formação de um bom formulador e resolvedor de problemas. E para alguém se tornar um bom leitor e "escritor", é indispensável inseri-lo em um bom e variável referencial de textos, para que ele se torne um bom formulador e resolvedor de problemas é preciso, igualmente, inseri-lo em um referencial de "textos matemáticos", através dos quais ele poderá ler, interpretar, analisar e produzir textos que constituam desafios matemáticos.

Segundo, D'Ambrosio (in Danyluk, 2002:11):

A leitura matemática do mundo parece ser uma das características da espécie humana...assim como falamos, matematizamos. Linguagem é a capacidade organizacional de expressar o nosso agir. Ao falar damos espaço para que nossa criatividade se manifeste, organizando e transmitindo o imaginário.

A linguagem torna-se um fator importante, pois ao propor uma atividade, a criança tem que interagir os seus pensamentos com o meio, aprendendo uma linguagem especifica e mudando os rumos da atividade e do seu desenvolvimento. Para dar uma base empírica a essa discussão será realizado um estudo de caso em uma escola pública de ensino fundamental e médio da cidade de Goiânia.

O Ensino de Geometria Analítica Utilizando os Softwares WINPLOT, RÉGUA E COMPASSO, VRUM VRUM E MATHGV

da SILVA, C. R., CAETANO, P. H. de O., RODRIGUES, E. C., GOMES, J. J., SILVA, R. S. e S.
Grad. C. Comp. UniEvangélica, Grad. Sist. Inf. UniEvangélica e Graduandos em Mat. da UEG

Orientadora:Profa. Msc. Eliane de Fátima Rodrigues Martins (UniEvangélica)
Centro Universitário de Anápolis,Avenida Universitária 3,5 km Cidade Universitária
Anápolis - GO
E-mail: elianemartins73@hotmail.com

Introdução:

A presente pesquisa tem como objetivo central investigar os processos metodológicos de ensino de Geometria Analítica em ambientes informatizados, contribuindo com a formação dos acadêmicos do curso de licenciatura em Matemática, Bacharelado em Ciência da Computação e Sistemas de Informação da UniEvangélica mediante o estudo dos aspectos teóricos e práticos relacionados à Educação Matemática. Estamos propondo a utilização de softwares como recurso pedagógico para compreender conceitos básicos de Geometria Analítica em especial as cônicas: parábola, elipse e hipérbole. Visto que o aprendizado de Geometria Analítica pode tornar-se mais atrativo com o auxílio de softwares. A interação do usuário com interfaces gráficas valoriza os conceitos matemáticos contínuos utilizando uma abordagem discreta, abordagem que chega ao alcance de nossos aprendizes. O que pode promover uma maior compreensão dos conceitos valorizando a aprendizagem de forma significativa bem como contribuir com o desenvolvimento de habilidades específicas da ciência matemática. Palavras ? chave: Geometria, Geometria Analítica, Softwares, Educação Matemática.

Metodologia:

Para desenvolver nossos estudos utilizamos a metodologia descritiva, com subsídios que proporcionaram o desenvolvimento de conceitos básicos de geometria analítica: plano, espaço e o conceito de função linear e quadrática, bem como as equações das cônicas: parábola, elipse e hipérbole.

Resultados:

Para esta abordagem escolhemos os softwares Winplot, MathGV, Régua e Compasso e Vrum Vrum, por disponibilizar ferramentas para construções de geometria mediante uma interface de menus de construção em uma linguagem própria a esta disciplina. Assim, foi possível criar e analisar construções de funções, equações, animações e esboço de gráficos, que podem ser visualizados em espaços bi e tri-dimensionais.

Este trabalho teve início com um delineamento histórico do desenvolvimento da ciência focando sempre a geometria. Uma linha do tempo foi descrita, proporcionando uma visão histórica do desenvolvimento da geometria, fatos que marcaram a evolução do pensamento matemático e as necessidades que impulsionaram os avanços tecnológicos.

Observamos que o formalismo aliado a uma notação matemática específica, pode e às vezes deixa obscuro o real significado destes conceitos. Essas dificuldades às vezes surgem em incompatibilidades de interpretação das variáveis existentes no mundo real e do mundo da ciência matemática. Faz-se necessário observar que a ciência matemática trabalha conceitos com variáveis contínuas. Neste sentido os softwares possuem uma característica que se adaptam ao mundo real, seus conceitos são matemáticos, mas são descritos com variáveis discretas, as quais em sua maioria representam os problemas do cotidiano.

Reforçando nossa proposta de utilizar os softwares para compreender os conceitos básicos de geometria analítica: plano, espaço e o conceito de função linear e quadrática, bem como as equações das cônicas: parábola, elipse e hipérbole. Assim estamos elaborando uma proposta metodológica que enfatiza a reflexão sobre estes conceitos utilizando os softwares Winplot, MathGV, Régua e Compasso e Vrum Vrum. Inicialmente elaboramos um manual que aborda a estrutura e o funcionamento de alguns comandos para visualização de gráficos em espaços bi e tri-dimensionais.

A presente pesquisa encontra-se em fase de elaboração de atividades contextualizadas que podem ser resolvidas com os softwares. Almejamos a elaboração de uma proposta metodológica que aborda a solução matemática clássica e solução utilizando os softwares. Valorizando a interação entre o usuário e o aplicativo, mas enfatizando que o entendimento dos conceitos é fundamental para uma aprendizagem significativa. CONCLUSÃO:

Observamos que o aprendizado de Geometria Análitica pode tornar-se mais atrativo com o auxílio de softwares. A interação do usuário com interfaces gráficas valoriza os conceitos matemáticos contínuos utilizando uma abordagem discreta, abordagem que chega ao alcance de nossos aprendizes. O que pode promover uma maior compreensão dos conceitos valorizando a aprendizagem de forma significativa.

Referências

[1] ALVES, L. e NOVA, C. Educação a distância: uma nova concepção de aprendizado e interatividade. Rio de Janeiro: Futura, 2003.

[2] REIS, G. L.; SILVA, V. V. Geometria Analítica. 2. ed. Rio de Janeiro. LTC, 1998.

Etnomatemática

Berchol, P. F., Tavares, R. E., Moraes, W. S.
Graduandos Licenciatura em Mat.IME/UFG

Orientador:Prof. Dr. José Pedro Machado Ribeiro
IME/UFG
Goiânia - GO
e-mail: pedro@mat.ufg.br

O projeto trata da concepção de sistemas de troca e comercial, transações comerciais, moedas e valores de produtos comerciáveis e conversões de moedas. Também trata das relações comerciais entre povos/ culturas e suas mudanças ao longo da historia.

Os alunos eram compostos pelos indígenas das seguintes etnias: Apinajé, Javaé, Karajá, Karajá-Xambioá, Krahó, Tapirapé e Xerente.

O objetivo foi de promover situações de aprendizagem por meio do manejo e da reflexão sobre instrumentos lúdicos que abordam as relações monetárias e comerciais presentes nos distintos contextos sócio-culturais. Estabelecer um espaço educativo de discussão e reflexão a respeito das relações comerciais tradicionais e atuais de cada cultura/povo, tomando como orientação suas transfigurações ocorridas ao longo da historia. Abordar as temáticas de sistema comercial e suas transações comerciais de modo a estabelecer relações significativas em prol das expectativas e necessidades dos povos indígenas e não-indígenas.

Projeto Re-vivenciando o Colméia

Canêdo, L. de L.
Graduanda Licenciatura em Mat.IME/UFG

Orientador:Prof. Dr. José Pedro Machado Ribeiro
IME/UFG
Goiânia - GO
e-mail: pedro@mat.ufg.br

O projeto tem por objetivo desenvolver ações que propiciem a formação continuada do professor de matemática da escola-parceira no propósito de repensar sua prática pedagógica e torná-lo multiplicador de novas metodologias de ensino a partir da aplicação da metodologia da pesquisa-ação, contemplando as dimensões de ensino e extensão por meio de discussões acerca da Matemática e Educação Matemática. Este nasce da re-elaboração do projeto Colméia, coordenado pela professora Zaíra da Cunha Melo Varizo, desenvolvido pelo LEMAT/IME no período de 1994 a 1999. Com intuito de compreender a proposta do projeto e suas dimensões, foram realizadas leituras e discussões, além da exposição do conhecimento adquirido nos debates sobre pesquisa qualitativa, promovendo assim, a compreensão dos aportes basilares do Colméia. Além do estagiário e seu orientador, conta com uma equipe executora composta por uma professora colaboradora do IME/UFG, três bolsistas do PETMAT/IME e um bolsista PROLICEN. No momento a equipe está contactando as escolas de menor IDEB (Índice de Desenvolvimento da Educação Básica) apresentando-lhes o projeto a fim de estabelecer uma parceria para a sua execução.

Jogos no Ensino de Matemática

Pinto, F. G., Rodrigues,J. C. P. S., Ferreira, J. do Vale, Melo, T. N., Barra, W. A.
Graduandos Licenciatura em Mat.IME/UFG

Orientadora:Profa. Ms. Maria Bethania Sardeiro dos Santos
IME/UFG
Goiânia - GO
e-mail: bethania@mat.ufg.br

Muito se fala sobre a importância dos jogos no ensino aprendizagem de matemática, mas há ainda poucos elementos para uma reflexão mais profunda com relação a esta utilização no ensino médio. Existe uma vasta bibliografia que relaciona o lúdico com o jogo, a importância do mesmo na formação de valores, entre outros. O projeto de estágio I, Jogos no ensino de Matemática busca propiciar momentos onde o aluno de licenciatura leia, reflita e discuta sobre vários textos que abordam esta temática para que, ao planejar uma aula com jogos, ele saiba o porquê e o para quê da utilização dos mesmos. Durante o projeto os alunos tiveram além de leituras e discussões, a oportunidade de colocar os seus estudos em prática tanto na participação na Amostra Milton Santos como na elaboração de um artigo fundamentado nos teóricos estudados e nas experiências vivenciadas com os jogos.

Jogos matemáticos estratégicos no processo de ensino e aprendizagem da matemática na escola do Ensino Básico

Da Costa, L. L., De Andrade,L. C. C.
Graduandas Licenciatura em Mat.IME/UFG

Orientador:Prof. Dr. José Pedro Machado Ribeiro
IME/UFG
Goiânia - GO
e-mail: pedro@mat.ufg.br

O projeto Jogos matemáticos estratégicos no processo de ensino e aprendizagem da matemática na escola do Ensino Básico consistiu no estudo de alguns jogos estratégicos matemáticos sobre os quais levantamos conhecimentos matemáticos e lógicos. Posteriormente escolhemos um jogo (SEIXOS) e realizamos uma aplicação piloto no Colégio Waldemar Mundim, com a turma do 5º ano, coletando dados e levantando as principais dificuldades no processo de ensino e aprendizagem, especialmente no ensino da matemática.

Promovemos reflexões e discussões a respeito dos saberes matemáticos presentes em alguns jogos, proporcionando situações de aprendizagem cooperativa entre os licenciandos (estagiárias e bolsista) e os alunos do Ensino Básico, oferecendo aos professores elementos para que possam adotar os jogos nas suas salas de aula.

Didática da Matemática à luz de uma abordagem a distância

Da Silva, D. R.,.Ribeiro, D. N.
Graduandos Licenciatura em Mat.IME/UFG

Orientador:Prof. Dr. José Pedro Machado Ribeiro
IME/UFG
Goiânia - GO
e-mail: pedro@mat.ufg.br

Este projeto de estágio proporcionou aos alunos contato com a prática de ensino, mediante o acompanhamento de uma metodologia de ensino-aprendizagem que alterna entre presencial e não presencial. É associado a uma pesquisa participativa desenvolvida na disciplina de Didática da Matemática II do curso de Licenciatura em Matemática do IME/UFG, num curso que desenvolveu atividades presenciais (50%) e atividades não-presenciais (50%). As atividades não-presenciais foram desenvolvidas na Plataforma Moodle, que se caracteriza por ser um AVA (Ambiente Virtual de Aprendizagem). Este AVA serviu como suporte para se pesquisar uma possível mudança comunicacional e a construção de hipertextos pelos sujeitos pesquisados. A metodologia utilizada visou ampliar o leque de atuação do futuro professor, pois, propiciou ao estagiário o contato com tecnologias que podem auxiliar o processo de ensino-aprendizagem mediante o acompanhamento de atividades desenvolvidas nas aulas presenciais e não presenciais; produções de sínteses dos textos trabalhados na disciplina de Didática da Matemática II; anotações de situações pertinentes à pratica pedagógica nas aulas presenciais; participação no planejamento e no replanejamento das atividades desenvolvidas na disciplina. Atualmente a expansão dos cursos à distância vem promovendo mudanças de metodologias de ensino e aprendizagem, portanto é importante que o futuro profissional da área de educação tenha contato e experiências com essa realidade para que sua formação seja de melhor qualidade e, por conseguinte, uma melhor preparação para atuação docente. Contudo, uma contribuição significativa do projeto é sobre a apropriação e utilização do AVA na disciplina pesquisada.

Acompanhamento Pedagógico de Reforço Matemático para Alunos da 2^a Fase do Ensino Fundamental no CEPAE

Araújo, F. M., Moreira, J. A. N., Silva, J. F. A., Miranda, M. A. da S.
Graduandos Licenciatura em Mat.IME/UFG

Orientador:Profa. Ms. Gene Maria Vieira Lyra Silva
CEPAE/UFG
Goiânia - GO

O Centro de Ensino e Pesquisa Aplicada à Educação - CEPAE - oferece aos alunos interessados ou com dificuldades na aprendizagem de Matemática, um acompanhamento extraclasse visando uma melhoria desta aprendizagem, bem como um auxílio ao aluno interessado em desenvolver seus estudos da disciplina. Este acompanhamento é realizado por alunos da graduação do curso de Licenciatura em Matemática que estão cursando a disciplina de Estágio Supervisionado I, sob orientação de um professor do departamento de Matemática do CEPAE. Por meio de estudos e reuniões, desenvolvem-se atividades de ensino, contemplando os alunos que se interessem ou aqueles que não alcancem notas satisfatórias, sendo indicados pelo seu professor para o atendimento. Este acompanhamento realizar-se-á por todo ano letivo e durante este período os alunos estagiários mantêm um enorme contato com o ambiente escolar e com os alunos de 6o ano do ensino fundamental ao 3o ano do ensino médio, proporcionando um grande aprendizado com uma rica experiência educacional. Esta experiência será relatada por meio deste trabalho, com intuito de socializá-la, sempre em prol de uma melhoria da educação do nosso país.

Acompanhamento de alunos do ensino fundamental- 2^a fase

Valeriano, W. P. de O.
Graduanda Licenciatura em Mat.IME/UFG

Orientadora: Profa. Msc. Gene Maria Vieira Lyra Silva
CEPAE/UFG
Goiânia - GO

Este projeto é desenvolvido com alunos do 6o ano/EF do CEPAE/UFG trabalhando com a unidade que trata de Grandezas e Medidas. Visa o desenvolvimento de competência métrica e a ampliação do conceito de medida de uma grandeza. No primeiro semestre foi feita uma pesquisa sobre as mudanças das unidades de medidas desde a antiguidade até os dias de hoje e também foi construído um jogo da memória visando à fixação dos conteúdos. Na conclusão desta etapa, foi montado um painel, em sala de aula, expondo os resumos dos alunos do livro paradidático ?Medir é comparar? e o material de revistas e jornais sobre o tema, levantado pelos alunos. Para o segundo semestre será elaborado um caderno de atividades com situações?problemas que envolvam operações matemáticas e medidas e, ainda, constará no caderno jogos individuais que objetivarão o desenvolvimento do raciocínio lógico e também a fixação de conceitos.

Didática da Matemática à luz de uma abordagem a distância

Porto, D.,.Do Amaral, J. H. S
Graduandos Licenciatura em Mat.IME/UFG

Orientador:Prof. Dr. José Pedro Machado Ribeiro
IME/UFG
Goiânia - GO
e-mail: pedro@mat.ufg.br

Este é um trabalho criado pelo grupo PETMAT/IME com o intuito de sanar a dificuldade dos alunos de matemática na disciplina Cálculo Diferencial e Integral I. Os objetivos deste trabalho são diminuir a evasão no curso, melhorar a aprendizagem e despertar o interesse quanto à importância dessa disciplina no curso de matemática. A metodologia utilizada durante o projeto é a tutoria, que consiste em um estudo em grupo denominado círculo tutorial, desenvolvendo a idéia de reciprocidade, ou seja, aprendizagem entre iguais. Atualmente desenvolvemos atividades com dois círculos tutoriais. Cada círculo é formado por um (1) bolsista do PETMAT (tutor do círculo), um (1) estagiário do curso de licenciatura em matemática e oito (8) alunos de Cálculo. Acontecem duas reuniões semanais planejando e elaborando notas históricas e listas de exercício do conteúdo ministrado pelo professor na sala de aula. Compõe a reunião o professor coordenador do PETMAT, um (1) professor orientador do Estágio Supervisionado I do IME/UFG, dois (2) estagiários e dois (2) bolsistas PETMAT. Nas sextas-feiras são realizados os encontros dos tutores com os alunos para realizar o estudo coletivo promovendo uma discussão sobre as listas de exercícios elaboradas por nós estagiários e elaboração de um plano com todas as atividades a serem realizadas no círculo tutorial.

Apoio: