# Jornada de Iniciação Científica do LNCC

## PIBIC2011

Anais

PIBIC
Programa Institucional de Bolsa Inciação Científica

pibic 13 ANOS

## Laboratório Nacional de Computação Científica – LNCC

Diretor
Pedro leite da Silva Dias

Coordenação de Administração - CAD
Leocadio José da Silva Ramos Netto

Coordenação de Ciência da Computação - CCC
Artur Ziviani

Coordenação de Matemática Aplicada - CMA
Sandra Mara Cardoso Malta

Coordenação de Mecânica Computacional - CMC
Regina Célia Cerqueira de Almeida

Coordenação de Sistemas e Controle - CSC
Marcelo Dutra Fragoso

Coordenação de Sistemas e Redes – CSR
Wagner Vieira Léo

Programa Institucional de Bolsas de Iniciação Científica
Renato Portugal

## Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq

Presidente
**Glaucius Oliva**

Coordenadora Geral do PIBIC
**Lucimar Batista de Almeida**

# V Jornada de Iniciação Científica do LNCC

## Comissão Interna do PIBIC/LNCC

Eduardo Lucio Mendes Garcia
Helio José Correia Barbosa
Jack Baczynski
Renato Portugal

## Avaliador Externo

Celso Melchiades Doria
UFSC

# Apresentação

Apresentamos neste volume a relação dos trabalhos da 6ª Jornada de Iniciação Científica do LNCC, desenvolvidos pelos bolsistas no período de agosto de 2010 a julho de 2011. Estes trabalhos foram apresentados em sessão pôster para, juntamente com as fichas de avaliação do bolsista, serem utilizados como elementos de avaliação do PIBIC/LNCC. Nesta avaliação contamos com o Prof. Dr. Celso Melchiades Doria – UFSC, que em função das entrevistas e exame deste volume preparou e enviou ao CNPq relatório de avaliação do Programa.

Agradecemos o empenho dos Professores Orientadores e dos Bolsistas na preparação das fichas de avaliação e dos pôsteres e da disponibilidade da presença para entrevista, para que nosso programa fosse avaliado. É preciso mencionar que temos sido bem avaliados, estando nosso PIBIC bem colocado entre os melhores do país, conforme divulgação feita pelo CNPq.

Organizamos este volume os resumos dos trabalhos dos bolsistas que nos foram enviados.

Aproveitamos a ocasião para agradecer ao CNPq pelas bolsas concedidas, a Direção do LNCC pelo apoio e a Comissão Interna deste programa no LNCC.

Renato Portugal
Coordenador do PIBIC/LNCC

# Índice


Criptografia pós-quântica : Equações Multivariáveis ..... 1
Bolsista: **Aline Essinger de Oliveira**

**DNA-Based Computation: Solving the Elliptic Curve Discrete Logarithm Problem**..... 2
Bolsista: **Ana Paula Barboza de Lima**

Algoritmo Quântico com Espaço de Dados Polinomial para o Problema do Subgrupo Oculto sobre Grupos Metacíclicos..... 3
**Daniel Gaspar Gonçalves de Souza**

Aplicações de Maple em Geometria Analítica..... 5
Bolsista: **Debora Carolina Kreischer**

Análise Computacional de Modelos Populacionais..... 9
Bolsista: **Flávio Henrique dos Santos**

Implementação de um módulo para o reconhecimento a manipulação de dispositivos sem fio de interação com o usuário ..... 11
Bolsista: **Grazielle Weinchutz Kapps**

Análise de Equações para Estudos em populações aplicadas ao município de Teófilo Otoni ..... 12
Bolsista:**Jéssica Lemos Gomes**

Uso de bibliotecas de Fragmentos em Operadores Genéticos para Predição *Ab Initio* de Estruturas de Proteínas..... 13
Bolsista: **Karina Baptista dos Santos**

Caracterização dos Efeitos da Ionosfera no posicionamento relativo de satélites por GPS ..... 14
Bolsista: **Leandro Baroni**

Métodos Numéricos Multiescala para um Modelo Elíptico e Parabólico com Coeficientes Oscilatórios..... 15
Bolsista: **Luiz Felipe Nascimento Soares**

Estudo e Desenvolvimento de Modelos para Simulação de Problemas com Mudança de Fase..... 16
Bolsista: **Maicon William Niebus Odone**

Método dos Elementos Finitos..... 17
Bolsista: **Marcel Duarte da Silva Xavier**

Portabilidade Java Aplicada a estudos em populações ..... 18
Bolsista: **Marcelo Alves Moreira**

Modelagem Computacional e Simulação Numérica do Sistema Cardiovascular Humano..... 20
Bolsista: **Matheus Vinicius de Oliveira Merabet da Silva**

Quando uma Equação Diferencial Ordinária é Separável?..... 21
Bolsista: **Vinicius José Oliveira Werneck de Carvalho**

# Título: Criptografia pós-quântica: Equações Multivariáveis

**Bolsista: Aline Essinger de Oliveira**
**Orientador: Fábio Borges**
**Co-orientador: Renato Portugal**

**Resumo:**

Neste trabalho revisamos alguns conceitos de extrema importância para a nossa pesquisa, como divisibilidade, números primos e congruências, além dos elementos de álgebra abstrata, Grupos, Anéis e Corpos. Também foram feitos estudos na área de segurança da informação, como o conhecimento de termos técnicos, tipos de ataques ativos e passivos e os principais serviços de segurança na rede.

Seguimos as pesquisas com uma introdução a criptografia pós-quântica, enfatizando os principais sistemas criptográficos que são usados hoje em dia na internet e que virão a ser quebrados caso um computador quântico, de tamanho considerável, seja inventado. Portanto, mostraremos que a criptografia não estará destruída, o método de criptografia pós-quântica, Sistemas de Equações Multivariáveis, está entre um dos mais seguros até o momento, além de ser resistente a ataques de algoritmos que só podem ser executados em computadores quânticos, ele pode ser executado em computadores clássicos.

Também indicaremos o possível método de solucionar os Sistemas de Equações Multivariáveis, através do cálculo das bases de Gröbner, que é um método análogo ao de Gauss para sistemas lineares. Através deste cálculo é possível transformar um sistema de difícil resolução em um sistema equivalente, porém de resolução mais simplificada.

# Título: DNA-Based Computation: Solving the Elliptic Curve Discrete Logarithm Problem

**Bolsista: Ana Paula Barboza de Lima**
**Orientador: Fábio Borges**
**Co-orientador: Laurent Emmanuel Dardenne**

## Resumo

Em 1994, Leonard Adleman em seus trabalhos apresentou a Computação Baseada em DNA como um novo paradigma computacional. Na Computação Baseada em DNA a manipulação é feita em tubos de ensaio e os dados podem ser condificados a partir destes filamento de DNA, que são utilizados como ferramenta para a resolução de problemas matemáticos considerados intratáveis. Uma das vantagens da Computação em DNA consiste em produzir algoritmos paralelos e a capacidade de geração de cópias da fita de DNA. Este trabalho utiliza a computação baseada em DNA empregando operações biológicas que pode ser aplicados em criptoanálise de algoritmos criptográficos para resolver problema do logaritmo discreto em curvas elípticas.

# Algoritmo Quântico com Espaço de Dados Polinomial para o Problema do Subgrupo Oculto sobre Grupos Metacíclicos

**Daniel Gaspar Gonçalves de Souza**
**Demerson Nunes Gonçalves / Renato Portugal**

O Problema do Subgrupo Oculto (PSO) consiste em determinar um subgrupo $H$ de um grupo finito $G$ oculto por um função que é constante nas classes laterais de $H$ e distinta nas diferentes classes laterais. Para ser eficiente, um algoritmo para o PSO tem que ser polilogaritmo na ordem de $G$. É conhecido que se o grupo $G$ é abeliano então o PSO pode ser eficientemente resolvido por um computador quântico, enquanto, nenhuma solução geral é conhecida para o caso de grupos não-abelianos [1].

Neste trabalho, nós apresentamos um algoritmo quântico em tempo sub-exponencial com espaço de dados polinomial para o PSO sobre o grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, onde $p, q$ são números primos distintos e $r, s$ inteiros positivos arbitrários. Usando a classificação dos subgrupos de $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, nós simplificamos o PSO ao problema de encontrar subgrupos cíclicos da forma $\langle x^a y^{q^j} \rangle$, onde $a \in \mathbb{Z}_{p^r}$, $x = (1,0)$, $y = (0,1)$ e $j$ um inteiro positivo $0 \leq j \leq s$ conhecido. Existem $O(p^r)$ subgrupos desta forma, assim, uma busca exaustiva do valor de $a$ é ineficiente.

Fazendo uso da transformada de Fourier abeliana e combinando as idéias apresentadas em Kuperberg [3] e Regev [4] para o PSO no grupo diedral, obtemos um procedimento quântico que gera estados

$$|0\rangle + e^{\frac{2\pi i z^\gamma ak}{p^r}} |1\rangle,$$

onde $0 \leq \gamma \leq \lceil \log p^r \rceil$ e $k \in \mathbb{Z}_{p^r}$ é um número uniformemente randômico. Agora, utilizamos um certo procedimento de medida e combinação. Este procedimento utiliza $l+4$ estados da forma $|0\rangle + e^{\frac{2\pi i z^\gamma ak}{p^r}} |1\rangle$, onde $l = O\left(\left\lceil \sqrt{\log p^r - 1} \right\rceil\right)$, e retorna um novo

estado $|0\rangle + e^{\frac{2\pi i 2^{\gamma} ab}{p^r}}|1\rangle$, onde os $l$ bits mais significativos de $b$ são iguais a zero. Executando esta rotina $l$ vezes, obtemos com probabilidade constante um estado da forma

$$|\psi_1^{2^{\gamma} ap^r}\rangle := |0\rangle + e^{\frac{2\pi i 2^{\gamma} a}{p^r}}|1\rangle.$$

Agora, aplicando a transformada de Fourier inversa ao conjunto de estados quânticos $\{|\psi_1^{2^{\gamma} ap^r}\rangle, \gamma = 0 \ldots, \lceil \log p^r \rceil\}$, obtemos o valor de $a$ com alta probabilidade.

## Abstract

In this paper we present a quantum algorithm with time complexity $2^{O(\sqrt{r \log p})}$ and polynomial space that solves the hidden subgroup problem (HSP) on the semidirect product of cyclic groups $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, where $p, q$ are any odd prime numbers and $r, s$ are any positive integers. Our approach uses the ideas behind Kuperberg and Regev's algorithm for the dihedral groups with a reduction procedure to cyclic subgroups present in some algorithms in the literature. As far as we know, this is the first subexponential-time quantum algorithm with polynomial space for the HSP in this class of groups.

## Referências

[1] C. Lomont, "Hidden Subgroup Problem - Review and Open Problems", *ArqXiv preprint quant-ph/0411037*, 2004.

[2] D. N. Gonçalves, R. Portugal, C.M.M. Cosme, "Solutions to the Hidden Subgroup Problem on some Metacyclic Groups", *Theory of Quantum Computation, Communication and Criptography. Waterloo. Publicação: Lecture Notes in Computer Science (LNCS)*, V. 5906, 2009.

[3] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem", *arXiv:quant-ph/0302112v2*, 2004.

[4] O. Regev, "A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space", *arXiv:quant-ph/0406151v1*, 2004.

# Aplicações de Maple em Geometria Analítica

**Débora Carolina Kreischer**
**Renato Portugal**

Este resumo tem como objetivo estudar a *propriedade de reflexão das cônicas* e as *superfícies quádricas*, com o auxílio do software *Maple* 13.

Com o intuito de analisar essa propriedade reflexiva, foi criado no *Maple* o pacote *reflexaoconica*. Para carregá-lo, é necessário lançar o seguinte comando:

```
>with(reflexaoconica);
```

[*elipse1*, *elipse2*, *hiperbole1*, *hiperbole2*, *parabola1*, *parabola2*]

A sintaxe dos comandos listados acima é dada como:

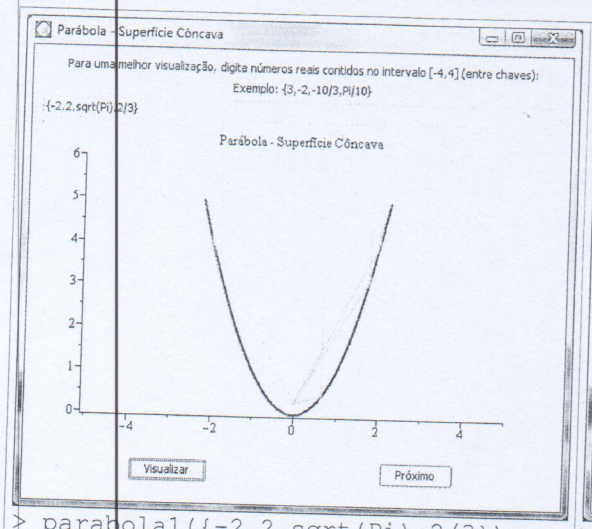
*nomedocomando* $[\{x_1, x_2, x_3, \ldots, x_n\}]$ . A sequência de números que estão entre chaves (conjunto) são as coordenadas $x$ de pontos pertencentes às cônicas. Num conjunto, um usuário pode repetir mais de uma vez um elemento e colocá-los fora de ordem, porque o *Maple* é encarregado de ordenar tais elementos e não repeti-los.

Em todos os comandos houve a necessidade de criar restrições. No lado de cada comando há um comentário indicando em qual intervalo fechado os números devem estar contidos. Isso ocorre porque no momento de criar o programa cada cônica possui um valor fixo.

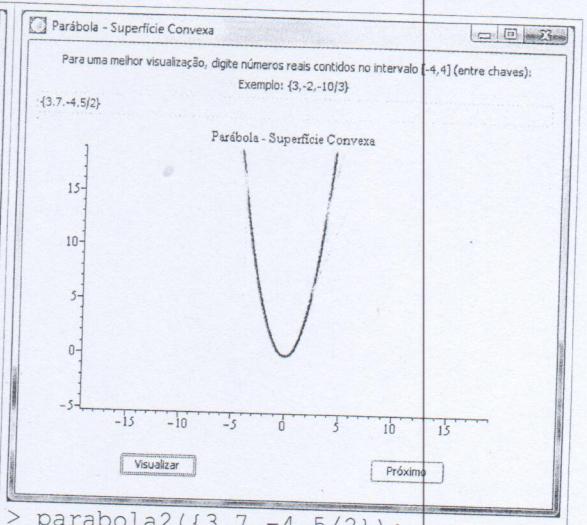
Também foi criado, com o auxílio do *Maple*, o *Maplet* denominado *Propriedade de reflexão das cônicas*. Os *Maplets* são programas com uma aparência bastante amigável destinada àquelas pessoas que não possuem conhecimento do *Maple*. Neste caso, foram implementados os comandos do pacote *reflexaoconica* num *Maplet* a fim de que estudantes de Geometria Analítica consolidem seus estudos referentes a propriedade de reflexão das cônicas, sem a necessidade de conhecer a fundo o *Maple* e linguagens de programação. É constituído de seis janelas, onde cada uma delas realiza, respectivamente, os seguintes comandos: *parabola1*, *parabola2*, *elipse1*, *elipse2*, *hiperbole1* e *hiperbole2*. Tal *Maplet* realiza exatamente as mesmas funções do pacote *reflexaoconica*, mudando somente a aparência que é apresentada em janelas.

A forma de usar esse *Maplet* é bem simples: basta o usuário digitar entre chaves os números de acordo com as instruções dadas na parte superior de cada janela e clicar em *Visualizar*. É necessário ter o *Maple* instalado no computador.

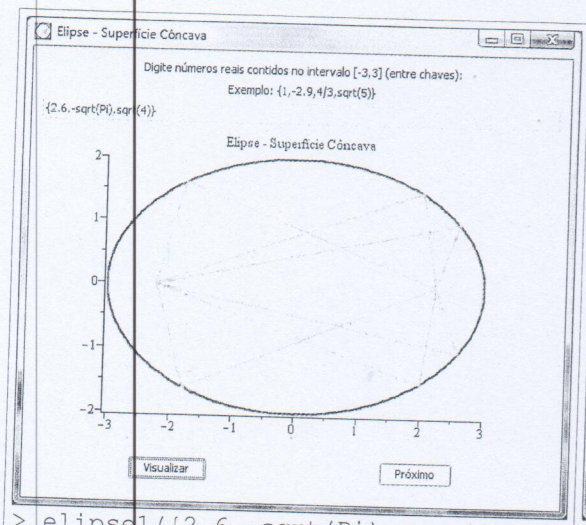
As figuras a seguir representam a sequência de janelas do *Maplet*, assim como os comandos pertencentes ao pacote *reflexaoconica*:



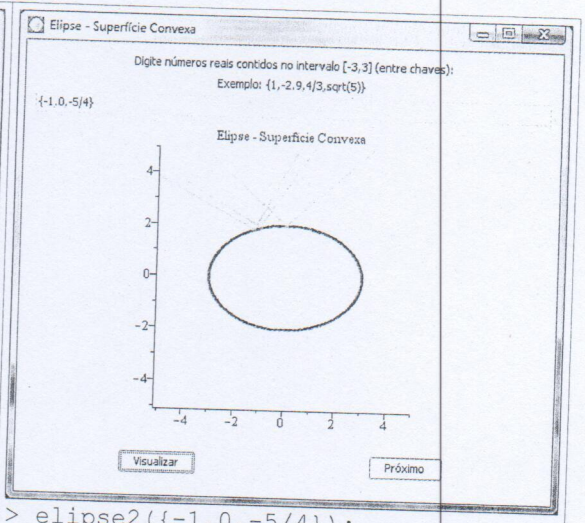

```
> parabola1({-2,2,sqrt(Pi),2/3});
# digite números reais entre [-4,4]
```



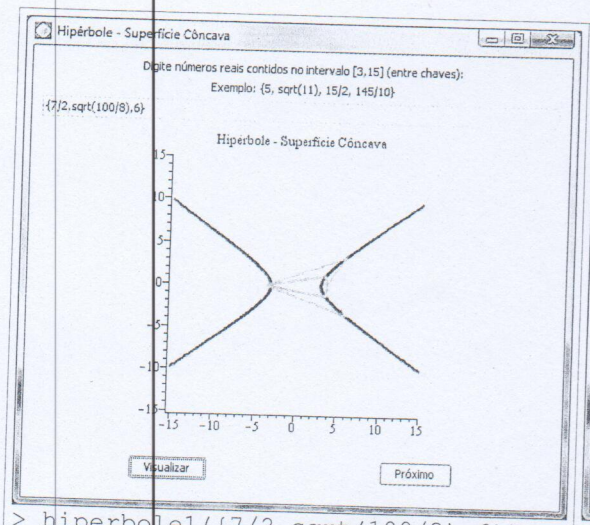

```
> parabola2({3.7,-4,5/2});
# digite números reais entre [-4,4]
```



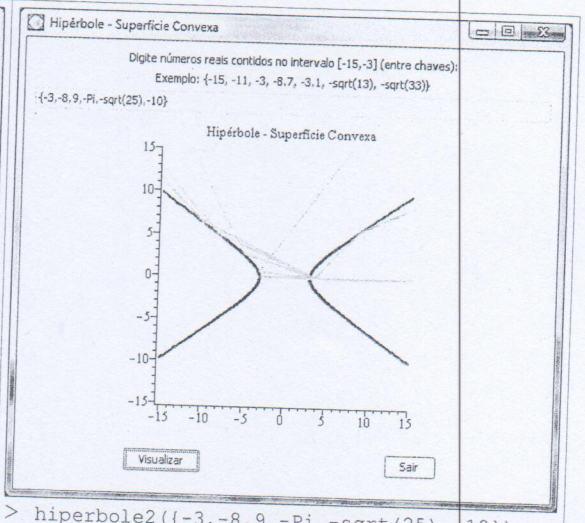

```
> elipse1({2.6,-sqrt(Pi),sqrt(4)});
# digite números reais entre [-3,3]
```




```
> elipse2({-1,0,-5/4});
# digite números reais entre [-3,3]
```




```
> hiperbole1({7/2,sqrt(100/8),6});
```




```
> hiperbole2({-3,-8,9,-Pi,-sqrt(25),-10});
```

```
# digite números reais entre [3,15]
```

```
# digite números reais entre [-15,-3]
```

Para o estudo das superfícies quádricas, foi considerado o caso particular dado pela equação $Ax^2 \square By^2 \square Cz^2 \square Dx \square Ey \square Fz \square G = 0$, para $A$, $B$, $C$, $D$, $E$, $F$ e $G$ constantes escalares reais e $A$, $B$, $C$, $D$, $E$ e $F$ não simultaneamente nulos. Esta equação permitiu o estudo da forma dessas superfícies através de suas seções planas palalelas aos eixos coordenados.

As superfícies quádricas foram definidas no *Maple* através do comando *implicitplot3d*, pertencente ao pacote *plots*. Sua sintaxe é dada por: `>implicitplot3d(expr,x=a..b,y=c..d,z=p..q,opções);`

Os comandos *textplot3d* e *display*, também pertencentes ao pacote *plots*, foram usados para inserir legendas nas figuras e imprimi-las na tela do computador, respectivamente.

As tabelas a seguir mostram o tipo de quádrica e a curva resultante, quando se intercepta um plano com a quádrica, desde que esse plano seja paralelo aos eixos coordenados.

| QUÁDRICA | PLANO | CURVA RESULTANTE |
|---|---|---|
| Elipsóide | $z = k_1 \boxplus c \le k_1 \le c \square$<br>$x = k_2 \boxplus a \le k_2 \le a \square$<br>$y = k_3 \boxplus b \le k_3 \le b \square$ | Elipse<br>Elipse<br>Elipse |
| Cone quádrico | $z = k_1 \square k_1 = 0 \square$<br>$z = k_1 \square k_1 \neq 0 \square$<br>$x = k_2 \square k_2 = 0 \square$<br>$x = k_2 \square k_2 \neq 0 \square$<br>$y = k_3 \square k_3 = 0 \square$<br>$y = k_3 \square k_3 \neq 0 \square$ | Vértice do cone (ponto)<br>Elipse<br>2 retas concorrentes<br>Hipérbole<br>2 retas concorrentes<br>Hipérbole |
| Hiperbolóide de uma folha | $z = k_1$<br>$x = k_2 \square a^2 - k_2^2 = 0 \square$<br>$x = k_2 \square a^2 - k_2^2 \square 0 \square$<br>$x = k_2 \square a^2 - k_2^2 \square 0 \square$<br>$y = k_3 \square b^2 - k_3^2 = 0 \square$<br>$y = k_3 \square b^2 - k_3^2 \square 0 \square$<br>$y = k_3 \square b^2 - k_3^2 \square 0 \square$ | Elipse<br>2 retas concorrentes<br>Hipérbole<br>Hipérbole<br>2 retas concorrentes<br>Hipérbole<br>Hipérbole |
| Hiperbolóide de duas folhas | $z = k_1$<br>$y = k_2$<br>$x = k_3 \square a^2 - k_3^2 = 0 \square$<br>$x = k_3 \square k_3^2 - a^2 \square 0 \square$ | Hipérbole<br>Hipérbole<br>Ponto<br>Elipse |
| Parabolóide elíptico | $z = k_1 \square k_1 = 0 \square$ | Vértice do parabolóide<br>Elipse |

| | | |
|---|---|---|
| | $z = k_1 \quad k_1 \neq 0$<br>$x = k_2$<br>$y = k_3$ | Parábola<br>Parábola |
| Paraboloide hiperbólico | $z = k_1 \quad k_1 = 0$<br>$z = k_1 \quad k_1 \neq 0$<br>$z = k_1 \quad k_1 \neq 0$<br>$x = k_2$<br>$y = k_3$ | 2 retas concorrentes<br>Hipérbole<br>Hipérbole<br>Parábola<br>Parábola |
| Cilindro elíptico | $z = k_1$<br>$y = k_2 \quad k_2 = b$<br>$y = k_2 \quad k_2 \neq b$<br>$x = k_3 \quad k_3 = a$<br>$x = k_3 \quad k_3 \neq a$ | Elipse<br>2 retas paralelas<br>2 retas paralelas<br>2 retas paralelas<br>2 retas paralelas |
| Cilindro parabólico | $z = k_1$<br>$y = k_2 \quad k_2 = 0$<br>$y = k_2 \quad k_2 \neq 0$<br>$x = k_3$ | Parábola<br>Reta<br>2 retas paralelas<br>Reta |

| QUÁDRICA | PLANO | CURVA RESULTANTE |
|---|---|---|
| Cilindro hiperbólico | $z = k_1$<br>$y = k_2$<br>$x = k_3 \quad k_3 = a$<br>$x = k_3 \quad k_3 \neq a$ | Hipérbole<br>2 retas paralelas<br>2 retas paralelas<br>2 retas paralelas |

Observação importante: as constantes mencionadas nas tabelas são pertencentes ao conjunto dos números reais.

Com o auxílio do *Maple* para o estudo das cônicas e das superfícies quádricas, pode-se comprovar que este software correspondeu ao resultado esperado: sua eficiência ao definir e desenhar cada curva e superfície. A precisão que o *Maple* possui foi o fator fundamental para o sucesso do estudo, além da possibilidade da criação de pacotes e programas.

**Palavras-chave:** *cônicas, quádricas, planos*

# Análise computacional de modelos populacionais

**Flávio Henrique dos Santos, Jaqueline Maria da Silva, Maurício Kritz**
**Instituto de Cinência e Tecnologia do Mucuri – UFJVM**
**Laboratório Nacional de Computação Científica - LNCC**

Quando estudamos o crescimento de populações sempre podemos adotar a modelagem matemático-computacional como ferramenta de estudo. Este estudo consiste em utilizar gradativamente cada fator que interfere na população, dependendo do seu grau de importância [1,2]. Neste trabalho analisamos as Equações de Thomas Malthus e Pierre Verhulst para crescimento populacional. Além disso, propomos a prática de simulações computacionais dessas equações utilizando Linguagem de Programação C.

É necessária uma aplicação computacional dos modelos citados, pois muitas vezes os valores numéricos envolvidos são muito grandes, o que torna o resultado mais sucetível a erros. Além disso, o procedimento é demorado e, muitas vezes, exige o uso de ferramentas tal como calculadoras.

No modelo de Malthus consideramos $P$ como a quantidade de indivíduos em uma população, seja ela animal ou vegetal, que será sempre dependente do tempo. Quando o número de indivíduos é suficientemente grande, $P(t)$ pode ser aproximado por uma função contínua [2]. Assim, temos:

$$\begin{cases} P(0) = P_0 \\ P(t) = P_0 e^{t\beta} \end{cases}$$

$$\beta = \ln\left( \sqrt[t]{\frac{P_t}{P_0}} \right)$$

Onde $\beta$ é a taxa de crescimento populacional.

Porém, se fizermos $\lim_{t\to\infty} P(t) = \infty$, e este limite não condiz com a realidade.

O modelo de Verhulst supõe que uma população deverá crescer até um limite máximo, isto é, a população tende a se estabilizar [3]. Então, temos:

$$\frac{dP}{dt} = aP(1 - \frac{P}{L})$$

Onde $a$ é a taxa de crescimento da população e $L$ o número máximo de indivíduos da população. Desenvolvendo a equação, temos:

$$P(t) = \frac{LP_0}{P_0 + (L - P_0)e^{-at}}$$

Neste caso, temos $\lim_{t\to\infty} P(t) = L$, ou seja, a população cresce até um valor máximo de indivíduos.

Os algoritmos elaborados para este trabalho auxiliaram no uso dos modelos matemáticos populacionais citados, facilitando a aplicação de ambos em pesquisas de diversos tipos de populações.

**Referências:**

[1] J.M. Silva, "Modelos para a Dinâmica de Vegetaçãao em Áreas Alagáveis Amazônicas", Tese de Doutorado, LNCC, 2011.

[2] R.C. Bassanezi,"Ensino-aprendizagem com modelagem matemática", Editora Contexto, São Paulo, 2006.
[3] R. N. RONEY. Dinâmica de populações: um breve histórico. In: BIENAL DA SBM - IME/UFG, 3., 2006. Goiânia: Anais eletrônicos. Goiânia, 2006.

# Implementação de um módulo para o reconhecimento e manipulação de dispositivos sem fio de interação com o usuário

**Bolsista:** Graziele Weinchutz Kapps
**Orientador:** Jauvane C. de Oliveira, Ph.D.

## Resumo

Ambientes Virtuais Colaborativos (AVCs) permitem que usuários localizados em posições geográficas distintas colaborem através de uma simulação de um mundo sintético controlado por computadores, utilizando uma infraestrutura de comunicação tal como a Internet.

Ambientes virtuais Colaborativos podem ser pouco-imersivos, quando se utiliza apenas um computador de mesa ou equivalente para interface com o usuário, semi-imersivo onde existe um certo nível de imersão no ambiente, como um imersa-desk, e ambientes imersivos, onde um usuário tem maior sensação de estar de fato imerso no mundo sintético, como quando se utiliza um CAVE. A sensação de imersão é implementada através da exploração dos sentidos humanos, através de dispositivos especiais de entrada e saída ou o uso de técnicas que explorem o modo como os sentidos humanos funcionam.

AVCs podem ser aplicados a diversas áreas do conhecimento, tais como militar, medicina, engenharia, etc. Aplicações de computador em AVCs, são capazes de simular situações que são encontradas no mundo real. O nível de realismo pode ter um aumento significativo se o ambiente oferecer suporte a determinados tipos de dispositivos de interação com o usuário. Esses dispositivos podem ser utilizados para navegação pelo Ambiente Virtual, para manipulação de objetos virtuais, entre outras funcionalidades, resultando em uma maior sensação de imersividade.

Para que dispositivos de interação com o usuário possam ser utilizados em AVCs, torna-se necessário o desenvolvimento de módulos que permitam que a aplicação acesse os recursos disponíveis no dispositivo.

Utilizando os módulos para controle e manipulação de dispositivos de interação, um desenvolvedor pode utilizar todos os recursos oferecidos pelo dispositivo através de funções especificamente implementadas para o mesmo.

A finalidade deste projeto de iniciação foi desenvolver módulos capazes de gerenciar os recursos dos dispositivos de interação sem fio.

Foi implemntado um Sistema de Avaliação de Massagem Cardíaca, utilizando o dispositivo Wii Fit, juntamentecom um bluetooth responsável por passar os sinais do Wii Fit para o computador. Este sistema captura a força, a posição e o ângulo dos braços, bem como a frequência de compressões realizadas em um indivíduo, além de mostrar graficamente esses dados em tempo real. Este sistema permite a auto avaliação do indivíduo que aplica a massagem cardíaca e melhora a qualidade dos treinamentos de massagem cardíacas existentes hoje.

# Análise de equações para estudos em populações aplicadas ao município de Teófilo Otoni

**Jéssica Lemos Gomes, Jaqueline Maria da Silva, Maurício Kritz**
**Instituto de Ciência e Tecnologia do Mucuri, UFVJM**
**Laboratório Nacional de Computação Científica, LNCC**

Nos últimos anos, a cidade de Teófilo Otoni, situada no nordeste mineiro, veio sofrendo notórias mudanças em seu crescimento populacional. Sabe-se que o número de indivíduos que constituem uma população não é fixo, podendo apresentar variações em virtude de circunstâncias, tais como natalidade, mortalidade e migrações [1]. A implantação de um centro de ensino universitário federal em Teófilo Otoni desde 2005 é uma dessas circunstâncias, bem como o comércio de pedras preciosas que durante muitos anos atraiu pessoas de diversas localidades à cidade.

A problemática de prever o crescimento ou decaimento de uma população, ou compreender como estes fatos ocorrem apresentou algumas soluções, na forma de equações e modelos matemáticos propostos por pesquisadores ao longo dos tempos.

A equação do crescimento natural parte do princípio de que uma população cresce ou decai a uma taxa proporcional a seu tamanho e diz que a população com uma taxa de crescimento relativa constante deve crescer exponencialmente [2].

O economista inglês, Thommas. R. Malthus, também criou um modelo, cuja formulação matemática indica que a variação relativa da população é constante, ou seja, é proporcional à própria população em cada período de tempo [3]. Malthus propõe dois modelos distintos: um discreto e um contínuo.

Pierre Verhulst, supondo que uma população, vivendo em um determinado meio, possui um limite máximo de habitantes que, depois de alcançado, faz com que a população tenda a se estabilizar, propõe um novo modelo logístico.

Neste trabalho, utilizamos desses modelos e avaliamos a eficiência de cada um deles aplicando-os no município de Teófilo Otoni e comparando os resultados obtidos com dados oficiais retirados do site do IBGE.

No decorrer dos estudos observamos que a cada novo modelo criado, as equações para estudos em populações foram aperfeiçoadas, tornando o resultado obtido cada vez mais próximo do real por um período de tempo maior. Um exemplo disto está no fato de a equação do crescimento natural não considerar nenhum fator de controle do crescimento populacional, ou seja, a população tende ao infinito. Enquanto Malthus considera a idéia de que uma população necessita de alimento e interação entre seus indivíduos para crescer e evoluir e Verhulst supõe a existência de um limite máximo sustentável até onde uma população poderá crescer, incorporando em sua equação a queda de crescimento da população que deve estar sujeita a um fator inibidor de proporcionalidade [3].

## Referências

[1] http://www.slideshare.net/guest9e1225/dinamica-depopulaes-e-sucesso
[2] J. Stewart, Cálculo, Volume 1, Cengage Learning, São Paulo, 2011.
[3] R.C. Bassanezi, Ensino-aprendizagem com modelagem matemática, Editora Contexto, São Paulo, 2006.

# Uso de Biblioteca de Fragmentos em Operadores Genéticos para Predição *Ab Initio* de Estruturas de Proteínas

**Karina Baptista dos Santos**
**Fábio Lima Custódio**
**Laurent Emmanuel Dardenne**

A predição da estrutura de proteínas é um dos propósitos mais importantes da biologia computacional. Possui como objetivo determinar a estrutura tridimensional de proteínas a partir de suas sequências de aminoácidos. O conhecimento dessa estrutura pode auxiliar na interpretação e obtenção de resultados com importantes impactos na saúde e no bem estar da humanidade. Uma das técnicas de predição usada atualmente é a predição *ab initio* que parte do princípio que a sequência de aminoácidos de uma proteína contém toda a informação necessária para que a cadeia adote sua conformação tridimensional nativa. Esse tipo de predição envolve um problema de otimização que lida com milhares graus de liberdade e com um grande espaço de busca conformacional. Mesmo para uma pequena molécula de proteína, o problema é difícil de ser tratado computacionalmente devido seu alto custo e tempo de execução, além da complexidade da otimização.

Esse trabalho se seguiu em três etapas: I – foi criada uma biblioteca de fragmentos de proteínas para cada uma das sequências estudadas (contendo 3 resíduos de aminoácidos por fragmento e 200 fragmentos para cada posição), através do ProFrager – programa gerador de bibliotecas de fragmentos desenvolvido pelo nosso grupo de pesquisa; II – informações dos ângulos diedrais dos fragmentos foram obtidas para construir uma matriz contendo os ângulos $\varphi$ e $\psi$ de cada aminoácido, em intervalos de 5°, com suas respectivas frequências; III - dois novos operadores foram adaptados ao programa de predição *ab initio* GAPF, também desenvolvido pelo nosso grupo de pesquisa.

A metodologia foi aplicada em um conjunto de cinco proteínas pertencentes às classes somente alfa-hélice, alfa+beta e folha-beta. Os resultados obtidos mostraram que o uso das bibliotecas de fragmentos, na forma dos operadores, foi capaz de reduzir consideravelmente o número de avaliações de função necessário para se obter um resultado equivalente sem o uso desses operadores. Isso é devido à restrição do espaço de busca conformacional, uma vez que o algoritmo passa a levar em consideração apenas os ângulos mais favoráveis de $\varphi$ e $\psi$ para cada tipo de resíduo. Assim, como o tempo de execução do algoritmo torna-se menor, permite-se a realização de experimentos de predição de estruturas para sequências mais longas, contornando uma das maiores limitações dos métodos de predição *ab initio*.

# Caracterização dos efeitos da ionosfera no posicionamento relativo de satélites por GPS

*Paulo Costa Porto de Figueiredo Barbosa, Izabela Batista da Silva, Leandro Baroni*

O voo em formação de satélites é uma das tecnologias mais promissoras para futuras missões espaciais. A distribuição dos sensores e cargas úteis entre os diversos satélites permite maior redundância, flexibilidade, melhorar a cobertura de comunicação entre outras vantagens. Uma das questões fundamentais do voo em formação de veículos espaciais é a determinação precisa da posição e velocidade entre os satélites. A fim de compreender o movimento relativo, é importante entender a dinâmica da órbita relativa, assim como suas perturbações. Para missões em órbita baixa, o sistema GPS pode cumprir o requisito de precisão do posicionamento relativo, desde que a dinâmica seja modelada adequadamente. Desse modo, a estimação precisa do estado de sistemas dinâmicos é extremamente importante. Os algoritmos de navegação por GPS devem levar em conta o aumento dos distúrbios ionosféricos nos próximos anos, devido ao aumento cíclico da atividade solar. Sendo assim, este trabalho visa apresentar um estudo de variabilidade ionosférica em um caso de satélites em voos em formação, tendo como base o uso de medidas fornecidas por receptores GPS. Para isso, serão usados dados reais da missão GRACE e analisados em diferentes cenários. Os resultados serão validados usando os dados de um sistema de medida de distância relativa a bordo dos satélites.

Ao final do trabalho, pretende-se ter um conjunto de parâmetros a respeito do efeito da camada da ionosfera sobre a precisão do posicionamento relativo por GPS de satélites de órbita baixa. Estes resultados poderão ser usados como referência no estudo de implementação de filtros de navegação para futuras aplicações que utilizem receptores GPS para determinação da posição relativa entre satélites em configuração de voo em formação. Isto permitirá a sintonização dos parâmetros do filtro quanto aos componentes de erro ionosférico.

O Brasil pode utilizar-se do conceito de voo em formação para o planejamento de futuras missões de sensoriamento remoto e fotografia espacial, permitindo o imageamento de ângulos diferentes para gerar mapas em três dimensões do terreno. Assim, as fotos podem ser tiradas ao mesmo tempo e com a mesma iluminação. Além disso, missões em formação podem prover uma redundância nos sistemas de retransmissão de informações das Plataformas de Coleta de Dados (PCD) no caso de falha em um dos satélites. Os satélites poderiam ser lançados em um mesmo veículo lançador, devido ao tamanho reduzido dos mesmos.

# MÉTODOS NUMÉRICOS MULTI-ESCALA PARA UM MODELO ELÍPTICO E PARABÓLICO COM COEFICIENTES OSCILATÓRIOS

**Luiz Felipe Nascimento Soares**

**ORIENTADOR: FRÉDERIC VALENTIN**

## RESUMO

A modelagem e a simulação computacional de fluidos contendo múltiplas escalas têm larga aplicação em problemas nas engenharias, física e biologia. Neste trabalho analisamos métodos numéricos adaptados à simulação de escoamentos com características multi-escalas, em razão dos coeficientes da equação. Tais técnicas incorporam com eficiência as pequenas escalas, preservando importantes propriedades das soluções exatas. Em particular, apresentamos um quadro matemático para a resolução de modelos elípticos com coeficientes oscilatórios. A motivação é a simulação de escoamentos mono e bifásicos em reservatórios de petróleo (meios porosos).

O método de Galerkin quando utilizado sobre espaços de interpolação polinomiais é adequado para tratar equações elípticas, como o problema de Poisson com coeficientes constantes ou com variações "*suaves*". Porém, esta abordagem clássica apresenta deficiências quando aplicada a problemas com coeficientes oscilantes, mesmo para operadores do tipo elípticos. Esta deficiência se deve ao fato da solução exata ser caracterizada por aspectos multi-escalas, representado pelo comprimento característico das oscilações $\varepsilon >> 1$, com consequente perda de coercividade da forma bilinear associada ao problema forte.

Este trabalho objetiva incorporar as pequenas escalas, dependentes de $\varepsilon$, na construção das novas funções de base denominadas de multi-escalas. As funções de base multi-escalas são obtidas resolvendo-se problemas de valor de contorno similares ao original em cada elemento. Ao final, o novo método de elementos finitos é constituído pelo método de Galerkin agora definido sobre os espaços gerados pelas funções multi-escalas.

Desta forma parte do trabalho foi feita com a implementação do método de Galerkin para o problema de Poisson 1D com coeficientes oscilantes no Matlab, seguido da implementação do método de elementos finitos multi-escalas 1D com coeficientes oscilantes também no Matlab. Ressaltamos as comparações numéricas da abordagem clássica com o método multi-escala analisando comportamento numérico e físico do fenômeno, além do possível estudo da análise de erro, assim como possíveis extensões ao operador reação-difusão com coeficiente oscilante.

# Estudo e Desenvolvimento de Modelos para Simulação de Problemas com Mudança de Fase

Autor: Maicon William Niebus Odone
Orientador: Elson Magalhães Toledo LNCC/UFJF
Co-orientador: Luis Paulo S. Barra (UFJF)
Laboratório Nacional de Computação Científica

Em muitas aplicações da engenharia um material passa por uma mudança de fase, como na fusão, congelamento, e solda. Problemas de condução de calor com mudança de fase, são caracterizados por uma interface móvel separando as duas fases. Estes problemas são problemas de fronteira livre ou fronteira móvel, tendo o movimento e a localização da interface desconhecidos devendo ser determinados como parte da solução. Durante o processo de mudança de fase materiais termo-condutores recebem calor do sistema ou o cedem para este. Neste trabalho apresentamos o modelo matemático do Problema de Stefan, que trata de um modelo básico para os problemas de mudança de fase.

Problemas mais complexos e realistas podem ser obtidos incluindo-se neste modelo comportamentos físicos desprezados. Abordagens mais elaboradas serão estudadas em trabalhos posteriores, quando então serão considerados procedimentos numéricos necessários a obtenção de soluções aproximadas para casos mais realistas.

# Método dos Elementos Finitos

**Bolsista: Marcel Duarte da Silva Xavier**
**Orientador: André Novotny**
**Co-orientador: Diego Esteves Campeão**

## Resumo

Neste trabalho é apresentado o Método dos Elementos Finitos (MEF) para codução de calor estacionária e elasticidade linear. Trata-se de um método numérico utilizado para obtenção de soluções aproximadas de equações diferenciais parciais ou equações integrais, cuja solução analítica é, em geral, difícil, senão impossível, de ser obtida explicitamente. O método consiste na discretização do problema contínuo em *elementos finitos*. Inicialmente, são apresentados os problemas de elasticidade linear e condução de calor unidimensionais, ambos em sua forma forte e variacional. Em seguida é apresentado o Método de Galerkin para discretização do problema. A formulação de Galerkin conduz a um sistema de equações lineares da forma $Kd = f$, onde $K$ é a matriz de rigidez, $d$ o vetor deslocamento e $f$ o vetor força. Por fim, é apresentado um problema de condução de calor estacionária cuja solução analítica é conhecida. Para verificar o resultado obtido através do MEF, o mesmo problema é resolvido utilizando o PDEtool (*Partial Differential Equation Tool Box)* do MatLab que utiliza o MEF. Observa-se que o resultado obtido numericamente pelo PDEtool corrobora com a solução exata do problema obtida analiticamente.

## Referências Bibliográficas

[1] Thomas J.R. Hughes. The Finite Element Method Linear Static and Dynamic Finite Element Analysis

[2] M.E. Gurtin. *An Introduction to Continuum Mechanics*. Mathematics in Science and Engineering vol. 158. Academic Press, 1981.

# Portabilidade Java aplicada a estudos em populações

**Marcelo Alves Moreira**
**Jaqueline Maria da Silva, Cezar Welter**
**Instituto de Ciência e Tecnologia do Mucuri – UFJVM**

Palavras chaves: populações, gráfico, multiplataforma, orientada, objeto.

O estudo de populações é importante para a compreensão do crescimento populacional ao longo do tempo. A proposta de utilizar a Matemática para estabelecer modelos de crescimento populacional começou com o economista inglês T. R. Malthus em 1978, ele afirmava que uma população aumenta em razão geométrica e os meios de subsistência em razão aritmética. Em 1837 o matemático belga Pierre F. Verhulst desenvolveu o Modelo Logístico que supõe que uma população vivendo num determinado meio deverá crescer até um determinado limite máximo sustentável, isto é, ela tende se a estabilizar [1, 2]. Desta forma, podemos trabalhar com número de habitantes, natalidade e mortalidade da população e adotar a modelagem como ferramenta de estudo e análise de seu comportamento. A tecnologia de programação em Java pode auxiliar a modelagem matemática por oferecer um ambiente de programação gráfico e multiplataforma.

À medida que o número de indivíduos em uma população cresce os modelos matemáticos que analisam o comportamento da mesma se tornam complexos, por tratarem com quantidades que representam populações muito grandes. Uma alternativa para facilitar a análise quantitativa dos modelos de Malthus e Verhulst é através da implementação de algoritmos. Java é uma linguagem de programação lançada em 1995 pela Sun Microsystems e essa tecnologia permite criar vários programas de alta qualidade [3,4].

A principal característica da linguagem Java é ser livre e de orientação a objeto. Esta característica permite a herança e a reutilização de códigos de forma dinâmica e estática. Os programas são desenvolvidos através da criação de classes, instâncias de classes, encapsulamento e hereditariedade. Possui ambiente gráfico de alta qualidade e estabilidade e por ter aplicações mais robustas não ocorrem interrupções, mesmo executando sob condições anormais [3]. O maior benefício de programar em Java é a independência de plataforma, ou seja, o programa em Java poderá funcionar em qualquer computador do mercado. Esta é uma vantagem significativa para os desenvolvedores de software, pois antes era necessário um programa para cada sistema operacional [3].

Neste trabalho foi implantada a plataforma Java para a simulação computacional do modelo de T. Malthus e o desenvolvimento do ambiente gráfico. O algoritmo desenvolvido consiste de um programa simples e prático, onde o usuário seleciona a equação desejada e executa a simulação. O acesso a resultados numéricos e gráficos da população ocorre instantaneamente. A tecnologia é promissora para a modelagem pois facilita a análise dos resultados, favorecendo o estudo do crescimento de populações.

**Referências**

[1] R.C. Bassanezi, Ensino-aprendizagem com modelagem matemática, Editora contexto, São Paulo, 2006.

[2] J.M. Silva, Modelos para a Dinâmica de Vegetação em Áreas Alagáveis Amazônica, Tese de Doutorado, LNCC, 2011.

[3] http://www.inf.puc-rio.br/~java/progjava/protected/siteAluno.html. Acesso 24, junho 2011.

[4] http://coro.cpdee.ufmg.br/attachments/128_Monografia_Diego_Rebelo.pdf. Acesso 26, junho 2011.

# MODELAGEM COMPUTACIONAL E SIMULAÇÃO NUMÉRICA DO SISTEMA CARDIOVASCULAR HUMANO

MATHEUS VINICIUS DE OLIVEIRA MERABET DA SILVA

**Orientador: Pablo Javier Blanco**

Em vista da complexidade que certos problemas da mecânica dos fluidos podem alcançar, atualmente são empregadas técnicas computacionais para a análise deste tipo de fenomenologia. A modelagem computacional consiste na criação de modelos matemáticos no computador, que simulem os fenômenos físicos de forma aproximada.

As atividades realizadas visam os estudo das técnicas de modelagem computacional na mecânica dos fluidos, em particular na modelagem do sistema cardiovascular humano, utilizando-se da formulação variacional como forma de abordagem dos problemas e de métodos numéricos para resolução dos mesmos.

Em posse dos conhecimentos adquiridos até a presente data e com adição do estudo do método dos elementos finitos serão criados modelos da circulação sanguínea em vasos de grande calibre. Como resultado, obtêm-se dados físicos valiosos e imagens bi e tri-dimensionais para análise médica e auxilio na cura e tratamento de patologias relacionadas ao sistema cardiovascular.

# Quando uma Equação Diferencial Ordinária é Separável?

*Vinicius José Oliveira Werneck de Carvalho*[1]

Sandra Mara Cardoso Malta[2] e Carlos Frederico Vasconcellos[3]

Laboratório Nacional de Computação Científica

**RESUMO**

Este estudo é baseado em um artigo do matemático David Scott, que analisa condições para investigar se uma equação diferencial é ou não separável. Apresentamos aqui a condição de separabilidade e a aplicamos às Equações de Ricatti. Concluímos que uma Equação de Ricatti só é separável quando seus coeficientes são múltiplos entre si.

## EDO separável

Quando uma equação diferencial ordinária $y' = f(x,y)$ é tal que $f(x,y) = g(x)/h(y)$, temos uma EDO SEPARÁVEL.

A maioria dos exercícios relacionados a EDO's separáveis apresentam a função $f(x,y)$ na forma fatorada e muitos estudantes não reconhecem, por exemplo, que a EDO $y' = 1 + x + y^2 + xy^2$ é separável.

## Teste de separabilidade de uma EDO

**Notação:** $D$, o domínio de $f$, é um conjunto aberto convexo no plano, $f$ é uma função de valor real, e derivadas parciais de $f$ são indicadas por subscritos.

**Proposição 1.** *Se existem funções diferenciáveis $\phi(x)$ e $\psi(y)$ tais que $f(x,y) = \phi(x)\psi(y)$ para todo $(x,y) \in D$, então $f(x,y)f_{xy}(x,y) = f_x(x,y)f_y(x,y)$, $\forall (x,y) \in D$.*

**Proposição 2.** *Se $f$, $f_x$, $f_y$, $f_{xy}$ são contínuas em $D$, $f(x,y)$ nunca se anula em $D$, e $f_x(x,y)f_y(x,y) = f(x,y)f_{xy}(x,y)$ para todo $(x,y) \in D$, então existem funções continuamente diferenciáveis $\phi(x)$ e $\psi(y)$ tais que $f(x,y) = \phi(x)\psi(y)$ para todo $(x,y) \in D$.*

## Equação de Ricatti

$$y'(x) = f(x) + g(x)y + h(x)y^2.$$

**Proposição 3.** *Uma equação de Ricatti $y'(x) = f(x) + g(x)y + h(x)y^2$ é separável se, e somente se, os coeficientes $f(x)$, $g(x)$ e $h(x)$ são múltiplos.*

*Demonstração.* Suponhamos que $f(x,y)f_{xy}(x,y) = f_x(x,y)f_y(x,y)$ para todo $(x,y) \in D$ com $f(x,y) = f(x) + g(x)y + h(x)y^2$. Temos

$$\begin{aligned} f_x(x,y) &= f'(x) + g'(x)y + h'(x)y^2, \\ f_y(x,y) &= g(x) + 2h(x)y, \\ f_{xy}(x,y) &= g'(x) + 2h'(x)y. \end{aligned}$$

Para analisar as condições entre $f(x)$, $g(x)$ e $h(x)$ para que $f_x f_y = f f_{xy}$, usamos o seguinte fato

Dois polinômios $p(y)$ e $q(y)$ coincidem para todo $y$ se, e somente se, seus coeficientes correspondentes são iguais.

Portanto, se $f_x f_y = f f_{xy}$ devemos ter

$$\begin{cases} f'(x)g(x) = f(x)g'(x) \\ f'(x)h(x) = f(x)h'(x) \\ g'(x)h(x) = g(x)h'(x) \end{cases}$$

Daí, a equação de Ricatti é separável quando os seus coeficientes $f(x)$, $g(x)$ e $h(x)$ são múltiplos.

Se os coeficientes $f(x)$, $g(x)$ e $h(x)$ são múltiplos, é fácil ver que a equação de Ricatti é separável.

**Referência:**

SCOTT, David, When is an Ordinary Differential Equation Separable?, *American Mathematical Monthly*, **92**(6), p. 422-423, 1985.

[1] Aluno IME/UERJ,Bolsista PIBIC-LNCC, viniciusufrj@hotmail.com
[2] Orientadora, CMA/LNCC
[3] Orientador, CTC/IME/Departamento de Análise Matemática

PIBIC CNPq