Proposta de Minissimpósio para o CNMAC 2018

Aplicações Computacionais de Álgebra Linear

Resumo

Luis Menasché Schechter
Professor Adjunto
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro (UFRJ)

1 Motivação

O estudo de matemática é muito importante para o desenvolvimento de diversas aplicações e ferramentas em Ciência da Computação. Em particular, neste minissimpósio, composto por quatro palestras, nosso objetivo é mostrar a enorme utilidade do estudo de Álgebra Linear para a área de Computação. A Álgebra Linear é o alicerce fundamental para várias aplicações computacionais, em um leque grande de diversidade. Por exemplo, ela é importante em aplicações relacionadas a comunicações em redes de computadores, aplicações relacionadas à computação gráfica e processamento de imagens e aplicações relacionadas à simulação computacional de fenômenos físicos, químicos, biológicos ou de engenharia, onde a eficiência computacional do processamento de matrizes pode ser utilizada de modo a obter resultados com nível de aproximação muito bom e com baixo tempo de processamento. Neste minissimpósio, buscamos apresentar um leque bem diverso de exemplos de aplicações de Álgebra Linear à Ciência da Computação.

2 Financiamento

Os quatro palestrantes irão buscar auxílio junto a suas respectivas Universidades para os custos de diárias e passagens.

3 Palestras

Palestrante: Luziane Ferreira de Mendonça (UFRJ)
Título: Aplicações de Álgebra Linear em Processamento de Imagens
Resumo:

Partindo do fato que uma imagem bidimensional pode ser tratada como uma matriz cujas componentes são as unidades de cores (pixels), operações envolvendo seus elementos afetam diretamente a imagem que ela representa, permitindo desde manipulações simples (como a rotação, expansão e contração) até redução de ruídos, detecção de contornos, extração de trechos, etc.. Nesta apresentação veremos o uso de técnicas de álgebra linear para realizar compressão de imagens e transmissão de dados (transmissão de dados em internet e circuitos internos para monitoramento em tempo real), sensoriamento remoto (monitoramento e detecção de características geográficas e recursos naturais, análise de crescimento urbano, etc.), medicina (análise e aprimoramento de imagens de raio-x, ressonância, ultrassonografias, para detecção e monitoramento de órgãos e tumores), robótica, visão computacional, etc.

Palestrante: Charles Figueredo de Barros (UFSJ)

Título: Códigos Corretores de Erros

Resumo:

Códigos corretores de erros são ferramentas que permitem, como o próprio nome sugere, detectar e corrigir erros em informações armazenadas ou transmitidas em meios digitais. Por exemplo, aparelhos de CD, DVD ou Blu-ray são capazes de reproduzir normalmente o conteúdo de discos, ainda que estes possuam pequenos arranhões em sua superfície. Isto só é possível porque as informações são gravadas nesses discos utilizando-se alguma técnica de detecção e correção de erros. Nesta palestra, discutiremos os fundamentos e aplicações dos códigos corretores de erros, a partir da noção de código linear como subespaço de um dado espaço vetorial sobre um corpo finito. Será abordado o conceito de matriz geradora, que consiste essencialmente na matriz cujas linhas (ou colunas) são os vetores da base de um código linear. Outros aspectos fundamentais, como distância de Hamming e matriz de paridade, também serão apresentados. Ainda serão discutidas técnicas de decodificação, que consiste em detectar e corrigir erros num determinado código. Alguns códigos conhecidos e suas propriedades serão brevemente apresentados, como os códigos de Hamming, códigos de Hadamard e códigos de Reed-Solomon.

Palestrante: Luis Menasché Schechter (UFRJ)

Título: Criptografia Baseada em Reticulados

Resumo:

Comércio eletrônico e *internet banking* são atividades essenciais atualmente. Elas são viabilizadas pelo uso de criptografia de chave pública. A segurança destes métodos baseia-se na alta complexidade computacional para a resolução de um dado problema matemático. Uma ameaça latente é um eventual advento dos Computadores Quânticos, pois eles podem resolver de forma eficiente os problemas subjacentes aos principais métodos de criptografia utilizados atualmente. Dentre as alternativas disponíveis, temos a Criptografia Baseada em Reticulados. Um reticulado é semelhante a um espaço vetorial, mas seus elementos são apenas as combinações lineares com coeficientes inteiros dos vetores da base. Desta forma, um reticulado pode ser pensado como uma malha discreta de pontos. Os métodos de criptografia baseados em reticulados têm a sua segurança baseada em problemas computacionalmente difíceis da teoria de reticulados, como o Problema do Vetor Mais Curto (SVP, na sigla em inglês) e o Problema do Vetor Mais Próximo (CVP). Nesta palestra, iremos apresentar os conceitos básicos de criptografia de chave pública e da teoria de reticulados, os problemas SVP e CVP e utilizaremos estes conceitos na discussão de um método concreto de criptografia baseada em reticulados, o método GGH.

Palestrante: Juliana Vianna Valério (UFRJ)

Título: Análise de Estabilidade de Escoamentos Viscosos

Resumo:

Escoamentos podem tornar-se instáveis mediante a pequenas perturbações e para controla-los é fundamental entender sua sensibilidade em relação a essas perturbações. Em várias situações práticas esse controle é importante, como por exemplo na industria de revestimento, pois impacta diretamente na qualidade do produto revestido. Interessante perceber que as equações que descrevem a estabilidade de escoamentos laminares dão origem a um problema de autovalor generalizado envolvendo matrizes singulares e consequentemente autovalores no infinito. Nesse tipo de problema, o interesse está no espectro finito, pois os autovalores correspondem à taxa de crescimento das perturbações e as autofunções à amplitude da perturbação. Para evitar os autovalores no infinito, que naturalmente são valorizados pelos métodos numéricos por serem os de maior módulo, desenvolvemos um método que reduz a dimensão do problema e ainda elimina todos os autovalores no infinito. O método consiste em aplicar transformações lineares desenvolvidas com esse objetivo que tiram proveito das estruturas das matrizes envolvidas. Vamos mostrar as transformações e o ganho computacional, que é muito expressivo, na análise de estabilidade em um escoamento de Couette.