Seminário em Matemática 2024/25

8 de Julho de 2025 - Ciências ULisboa - Sala 6.2.33

Programa

09h30	Bendegúz Varga	A consistência de ZFC relativamente à de ZF
10h00	Manuel Narigueta	Hilberts Tenth Problem
10h30	Luís G. Oliveira	Números primos na forma da soma de quadrados
11h00	Luís S. Oliveira	Spectral Graph Theory - Regular and Bipartite Graphs
11h30	Rui Prado	Números Reversíveis
12h00	Bernardo Catado	Isometrias do plano e sua aplicação a *Wallpaper Groups*
14h00	Samuel Costa	Método dos elementos finitos e aplicações em C++
14h30	Gabriel Ramos	Almost sure global well-posedness for the defocusing Hartree equation
15h00	Rodrigo Luís	Uncertainty and Symmetry in the Schrödinger Equation: A Bidirectional Exploration
15h30	Francisco Alves	Sharp Hausdorff-Young Inequality
16h00	Rafael Hipólito	Convergência de séries alternadas com oscilações
16h30	Carimo Mohomed	Lattice-based Cryptography and the L.W.E. (Learning with Errors) problem

Lista de Resumos

• Bendegúz Varga

A consistência de ZFC relativamente à de ZF

O objetivo deste seminário é ver que a partir dos axiomas Zermelo-Fraenkel (ZF) não é possível demonstrar a negação do Axioma da Escolha (AC). Em termos formais, a última asserção exprime-se como $\mathsf{ZF} \nvdash \neg\mathsf{AC}$ e trata-se da parte demonstrada por Kurt Gödel do célebre resultado de que AC é independente dos axiomas ZF.

No seminário, reduzimos o resultado anterior a mostrar um resultado de consistência relativa: sob a consistência de ZF tem-se a consistência de ZFC, isto é, $\mathrm{Con}(\mathsf{ZF}) \to \mathrm{Con}(\mathsf{ZFC})$. Para tal seguimos as ideias de Gödel e introduzimos o Universo construtível L, cujas propriedades permitem deduzir que ZFC é válido quando relativizado a L. Este facto de L ser um modelo de ZFC, juntamente com $\mathrm{Con}(\mathsf{ZF})$, permite-nos deduzir a consistência de ZFC.

• Manuel Narigueta

Hilberts Tenth Problem

In 1900 David Hilbert introduced to the world a list of 23 "problems"left for the 20th century mathematicians to solve. Among them, there was the tenth problem he proposed:

Determination of the Solvability of a Diophantine Equation
Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Today we interpret this in the following way: we want to know if there is a general algorithm to determine whether any Diophantine equation has solutions. If the answer

was affirmative, it would suffice to find such an algorithm. However, it turns out that no such algorithm exists. Fortunately, computability theory can help us in the definitions of concepts like "algorithm"and what it means for such an algorithm to be impossible to exist. We will reveal why such an algorithm is impossible by first introducing the concept of Diophantine functions, relations and sets; next, we show that Exponentiation is Diophantine, which was historically the last step to solve Hilberts tenth problem (it was resolved by Matiyasevich in 1970) and is the hardest and most lengthy part of the whole proof; and finally we show that recursive and Diophantine functions are the same, and then prove the MRDP theorem, which states that Diophantine sets and recursively enumerable sets are the same. We can then solve Hilberts tenth problem with this final result.

• Luís Gerald Oliveira

A Proof of the Fermat Theorem

Fermat's theorem states that a prime number that can be written as $1 + 4K$, K being a positive number, can always be decomposed as a sum of two squares. This seminar describes the use of involution functions to prove this statement. We base this work on the proof by Don Zagier and Stan Dolan, and devise methods to determine the exact values of the two squares. The first method is indicated for relatively small prime numbers and a short computer program in **C** is presented. The second method can be used on large prime numbers, using lattice numbers, but some software is needed for a more precise visualisation.

• Luís Simão Oliveira

Spectral Graph Theory - Regular and Bipartite Graphs

Spectral Graph Theory explores the relationships between graphs and linear algebra, such as obtaining results about the graph based on its Adjacency matrix, Laplacian matrix and signless Laplacian matrix. We examine how the eigenvalues and eigenvectors of these matrices reveal whether a graph is regular or bipartite, and how we can infer the spectrum of these matrices directly from the graph's structure. Finally, we compute and analyze the spectra of various common regular and bipartite graphs to demonstrate how we can effectively determine properties of the graph that might not be obvious or hard to compute otherwise.

• Rui Prado

Números Reversíveis

O que é que acontece quando invertemos a ordem de escrita dos números? Quanta Matemática poderemos extrair ou desenvolver a partir desta ideia simples? Procurámos satisfazer esta curiosidade com o presente trabalho. E a exploração não foi menos do que interessante, e os resultados não menos do que satisfatórios. Uma boa parte do trabalho compila e formaliza resultados apresentados no livro "The Little Book of Reversible Numbers"de Michael P. Greaney, resultados esses provenientes de muito trabalho computacional por parte do autor, mas pouco formalismo e quase nenhuma

demonstração. Alguns dos resultados poderão não ter ainda demonstração conhecida, sendo no entanto apresentados como conjeturas, uma vez que há evidência computacional e/ou heurística que os fundamenta.

• Bernardo Catado

Isometrias do plano e sua aplicação a *Wallpaper Groups*

Neste trabalho procurou-se escrever um texto que fosse sustentável sem grandes conhecimentos prévios. O foco esteve, numa fase inicial, em estabelecer os conceitos basilares para uma boa compreensão do texto (conceitos algébricos e também geométricos) e, numa fase mais posterior, no desenvolvimento das ideias preliminares em conceitos mais adjacentes à teoria dos ditos *Wallpaper Groups* e a classificação destes grupos de simetrias (a menos de isomorfismo).

• Samuel Costa

Método dos elementos finitos e aplicações em C++

Neste seminário iremos abordar o método dos elementos finitos para a resolução numérica de equações diferenciais (problemas de valores na fronteira), apresentando aspetos teóricos e implementação numérica através da biblioteca maniFEM, em **C++**.

• Gabriel Ramos

Almost sure global well-posedness for the defocusing Hartree equation

Recently, Oh, Okamoto and Tolomeo (2024) completed the construction of the Gibbs measure with a Hartree-type nonlinearity on the three-dimensional torus $\mathbb{T}^3$. We extend this measure to $\mathbb{R}^3$ in the defocusing case by taking a infinite volume limit using a variational method developed by Gubinelli and Barashkov (2021) for Euclidean quantum fields. We then use it to show, by an invariant measure argument, the almost sure existence of global solutions in a weighted Besov space to the associated Hartree nonlinear Schrödinger equation.

• Rodrigo Luís

Uncertainty and Symmetry in the Schrödinger Equation: A Bidirectional Exploration

Developed in 1925 by the Austrian physicist Erwin Schrödinger, the Schrödinger equation stands as one of the cornerstones of modern quantum mechanics. In spite of its physical applications, it is a rich object from the mathematical point of view, as it relates with deep mathematical areas, such as Functional Analysis and Operator Spectral Theory.

In this project, we aim to look at the Schrödinger equation and exploit an uncertainty principle that will make the solutions vanish. Here we follow the work of [2]. Then, following the work of [1], we go in the reverse direction and exploit the Schrödinger equation's symmetries to arrive at an uncertainty principle. We will also

make a brief contextualization to the topic and with the aid of [3] we will also deduce the Schrödinger group - the group of symmetries of the free equation.

Referências

[1] Cowling, M., Escauriaza, L., Kenig, C., Ponce, G., and Vega, L. The Hardy's uncertainty principle revisited, *arXiv*. 2010.

[2] Escauriaza, L., Kenig, C., Ponce, G., and Vega, L.. Hardy's uncertainty principle, convexity and Schrödinger evolutions, *Journal of the European Mathematical Society*, 10, 883-907, 2008.

[3] Niederer, U., The Maximal Kinematical Invariance Group of the Free Schrödinger Equation, *Helvetica Physica Acta*, 5, 802-810, 1972.

• Francisco Alves

Sharp Hausdorff-Young Inequality

It is fairly simple to prove that the Fourier transform is a bounded operator from L^p to $L^{p'}$ for $1 \leq p \leq 2$ using Riesz-Thorin interpolation theorem to prove the Hausdorff-Young inequality. However this inequality is only sharp for $p = 1,\ 2$. Using the Hermite polynomials, the Mehler Kernel and the Central Limit Theorem we prove a sharp version of the Hausdorff-Young inequality and show functions for which the equality is attained.

• Rafael Hipólito

Convergência de séries alternadas com oscilações

A medida de irracionalidade de um número θ, escrita $\mu(\theta)$, é o ínfimo do conjunto dos números μ para os quais existe apenas um número finito de aproximações racionais $\frac{p}{q}$ de θ com $\left|\theta - \frac{p}{q}\right| < \frac{1}{q^\mu}$.
Em 2011 Alekseyev publicou um artigo em que relaciona a medida de irracionalidade de π e a convergência de séries da forma $\sum_{n=1}^{\infty} \frac{1}{n^u |\sin(n)|^v}$ [1].
Em 2019 o utilizador do MathStackExchange Jack D'Aurizio determinou que a série $\sum_{n=1}^{\infty} \frac{(-1)^n |\sin n|}{n}$ converge, mostrando que sairia de $\mu(\pi) < \infty$ [2].
Motivados por estes dois resultados, decidimos estudar as séries da forma $\sum_{n=1}^{\infty} \frac{(-1)^n \left|\sin\left(\frac{n\pi}{\theta}\right)\right|^\alpha}{n^\beta}$, obtendo ligações entre a sua convergência e $\mu(\theta)$.
Pela teoria de séries de Dirichlet, do mesmo resultado, obtemos ligações entre majorações de $A(N) = \sum_{n=1}^{N} (-1)^n \left|\sin\left(\frac{n\pi}{\theta}\right)\right|^\alpha$ e $\mu(\theta)$.

Referências

[1] Alekseyev, Max A.. On convergence of the flint hills series, 2011.

[2] D'Aurizio, Jack. Convergence of an alternating series: $\sum_{n=1}^{\infty} \frac{(-1)^n |\sin n|}{n}$, Mathematics Stack Exchange. URL: math.stackexchange.com/q/3059137 (version: 2019-01-02).

• Carimo Mohomed

Lattice-based Cryptography and the L.W.E. (Learning with Errors) problem

Many aspects of our daily lives, which are taken for granted - online commerce, communication through electronic devices, home banking, relations between the State and its citizens, military communication and intelligence services (commonly known as espionage and counter-espionage), etc., etc., etc., - are based on cryptography and the belief in its security. Cryptography, as it currently exists, received a huge boost during and, especially, after the 1939-1945 war, based on Number Theory and its applications, disproving the conviction of the British mathematician Godfrey Harold Hardy (1877-1947), who considered this area of Mathematics to be the most useless. Cryptography underwent several developments in subsequent years, with the R.S.A. system (Rivest, Shamir, Adleman) standing out, whose security was based on the difficulty in factoring large numbers, obtained, in turn, by multiplying prime numbers that were also considered large. However, in 1994, Peter Shor, with the algorithm that bears his name, managed to show that such factorisation was possible in polynomial time by a quantum computer, a "threat"which is currently mostly theoretical, but which might one day be realised through the development of quantum computing. This, in turn, led to research in the area of post-quantum cryptography, drawing on many tools from different areas of Mathematics. Lattice-based cryptography stands out, in particular L.W.E. This presentation, divided into two parts, will first address the R.S.A. system and its relationship with Euler's totient function, and then briefly explore the fact that "breaking"lattice-based cryptography involves solving the L.W.E. problem.