

ALC MEETING 2022

19 DECEMBER 2022

PROGRAMME

09:20 - 09:30 Welcome

09:30 - 10:20 Maria de Lurdes Teixeira, "Why do we study finite semigroups?"

10:20 - 10:40 Bruna Calisto "Formalization in Coq of the Standardization Theorem for Lambda-calculus"

10:40 - 11:00 Filipa Mendes, "Variations on the call-by-value lambda-calculus"

11:00 - 11:30 Coffee Break

11:30 - 12:00 Maria Antónia Forjaz, António Mário Almeida and Jorge Pamplona, "Vale das 7 Fontes: a motto to talk about Science"

12:00 - 12:30 Carlos Freitas, Cláudia Mendes-Araújo, Suzana Gonçalves, "**A**micable and **L**udic **C**ryptography - ALC at NEI"

12:30 - 13:00 Rui Ralha, "Linear algebra in Data Science"

13:00 - 15:00 Lunch

15:00 - 15:30 Yulin Zhang, "Inseparable Gershgorin discs and the existence of conjugate complex eigenvalues of real matrices"

15:30 - 16:00 Luís Pinto, "A coinductive approach to proof search"

16:00 - 16:30 Conceição Nogueira, "The overlap gap between left-infinite and right-infinite words"

16:30 - 17:00 Coffee Break

17:00 - 17:30 Catarina Sousa, "Proof search in natural deduction: towards human-centered theorem proving"

17:30 - 18:00 Pedro Patrício, "From Brown-McCoy to orthogonality"

ABSTRACTS

Maria de Lurdes Teixeira, “Why do we study finite semigroups?”

ABSTRACT: The first results about finite semigroups date from the beginning of the 20th century. The characterization of simple and 0-simple finite semigroups can be considered the first relevant result on finite semigroups and it is due to A. Suschkewitsch (1928) and D. Rees (1940). At that stage, studying semigroups that were finite was not a goal in itself. The motivation for the develop of this area, that leads to its autonomous existence, is not inherent. The richness of its results is consequence of applications, namely in the areas of formal languages and automata theory.

In this communication we will talk about the evolution of Finite Semigroups Theory. We will point out some of the main results, starting with those of S. Kleene (1956) and of M. Rabin and D. Scott (1959) that are considered an essential part of the fundamentals of the theory of computation and trace the development of Finite Semigroups Theory from the 1950s onwards, in parallel with the development of electronic computers and computer sciences.

Bruna Calisto, “Formalization in Coq of the Standardization Theorem for lambda-calculus”

ABSTRACT: The Standardization Theorem is a fundamental result in the theory of reduction of the lambda-calculus establishing that one term t reduces to another term t' if and only if t reduces to t' following a specific sequence of reductions said "standard". In this talk we will overview a formalization of a proof of this theorem in the Coq proof assistant that we have conducted, following a proof of a standardization theorem in a lambda-calculus for a fragment of the intuitionistic modal logic IS4 by Espírito Santo-Pinto-Uustalu. Additionally, we will also consider an independent and more traditional notion of standard reduction sequence for (call-by-name) lambda-calculus studied by Plotkin, and illustrate a formalization in Coq that the characterizations of standard reduction in Plotkin's approach and in the approach we followed are indeed equivalent.

Filipa Mendes, “Variations on the call-by-value lambda-calculus”

ABSTRACT: In 1975 Plotkin presented the very first call-by-value lambda-calculus, a formal system that models a call-by-value programming language. However, this system turned out to be incomplete for the CPS semantics. In other words, there are terms with the same semantics that are not proved equal in Plotkin's lambda-calculus. In this talk, we will present Moggi's computational lambda-calculus and a simplified version of Dyckhoff-Lengrand's lambda-calculus, two formal systems with different origins that are an answer to Plotkin's incompleteness problem. We will also analyse how these two systems relate to each other.

Maria Antónia Forjaz, António Mário Almeida and Jorge Pamplona, “Vale das 7 Fontes: a motto to talk about Science”

ABSTRACT: An itinerary composed of a visit along the "Vale das 7 Fontes", so that Nature is unveiled to the different Sciences from different *angles*, sometimes (almost) geometrically equal, sometimes complementary. (Join work with Isabel Correia Neves and Isabel Aguiar Mina.)

Yulin Zhang, “Inseparable Gershgorin discs and the existence of conjugate complex eigenvalues of real matrices”

ABSTRACT: We investigate the converse of the known fact that if the Gershgorin discs of a real n -by- n matrix may be separated by positive diagonal similarity then the eigenvalues are real. In the 2-by-2 case, with appropriate signs for the off-diagonal entries, we find that the converse is correct, which raises several questions. First, in the 3-by-3 case, the converse is not generally correct, but, empirically it is frequently true. Then, in the n -by- n case, $n \geq 3$, we find that if all the 2-by-2 principal submatrices have inseparable discs ("strongly inseparable discs"), the full matrix must have a nontrivial pair of conjugate complex eigenvalues (i.e., cannot have all real eigenvalues). This hypothesis cannot generally be weakened.

Carlos Freitas, Cláudia Mendes-Araújo, Suzana Gonçalves, “Amicable and Ludic Cryptography - ALC at NEI”

ABSTRACT: In June 2022, CMAT presented a proposal for FCT's special support "Verão com Ciência", with the aim of stimulating the initiation to scientific activity of students of first cycle degrees associated with DMAT and to disseminate scientific and technical knowledge to society. Under the theme "Cryptographic systems and digital signatures with elliptic curves", activities and dissemination material for the European Researchers' Night (ERN) 2022 were developed under the scope of 5 BII grants supervised by CMAT members. The whole experience, from the submission of the application for special support to the implementation of the activities in ERN 2022, will be described.

Rui Ralha, “Linear algebra in Data Science”

ABSTRACT: We will illustrate the importance of linear algebra and matrix computations in the statistical treatment of data: the least squares method and PCA (principal component analysis) as well as, if time allows, the Linear Discriminant Analysis. The main focus will be the mathematics, from numerical linear algebra, involved in these techniques.

Luís Pinto, “A coinductive approach to proof search”

ABSTRACT: The Curry-Howard correspondence relates proof and type systems, and, in particular, provides a representation of proofs as (typed) lambda-terms. In our coinductive approach to proof search this paradigm of representation is extended to solutions of proof-search problems, where a solution is a run of the proof search process that does not fail to apply bottom-up an inference rule, so it may be an infinite object. The approach considers two typed lambda-calculi, one obtained by a coinductive reading of the grammar of proof terms (acting as the universe for the mathematical definition of proof search concepts), the other by enriching the grammar of proof terms with a formal fixed-point operator to represent cyclic behaviour (acting as the finitary setting, where algorithmic counterparts of those concepts can be found). Both calculi feature formal (finite) sums, which are employed to represent choice points in the proof search process, and allow the representation not only of individual solutions, but also of entire solution spaces.

In this talk we will give an overview of this coinductive approach to proof search, illustrating it in the case of intuitionistic implication, and showing some applications to inhabitation and counting problems in simply-typed lambda-calculus (e. g., results ensuring uniqueness of inhabitants, related to coherence in category theory).

The talk is based on joint work with José Espírito Santo (Centro de Matemática, University of Minho) and Ralph Matthes (IRIT, CNRS and University Toulouse III, France).

Conceição Nogueira, “The overlap gap between left-infinite and right-infinite words”

ABSTRACT: In this talk I will present ultimate periodicity properties related to

overlaps between the suffixes of a left-infinite word λ and the prefixes of a right-infinite word ρ . I will talk about a result that states that the set of minimum lengths of words x and x' such that $x\lambda_n = \rho_n x'$ or $\lambda_n x = x'\rho_n$ is finite, where n runs over positive integers and λ_n and ρ_n are respectively the suffix of λ and the prefix of ρ of length n , if and only if λ and ρ are ultimately periodic words of the form $\lambda = \dots uv$ and $\rho = wuu\dots$ for some finite words u , v and w . This is a joint work with José Carlos Costa (Universidade do Minho) and M. Lurdes Teixeira (Universidade do Minho).

Catarina Sousa, “Proof search in natural deduction: towards human-centered theorem proving”

ABSTRACT: In the context of interactive theorem proving, the goal of my thesis project is the theoretical clarification of human-readable output in the conceptual network that goes from the formal proof objects handled by theorem provers to the natural language proofs developed by mathematicians. In this presentation, I will guide you through the history that leads to the problems/questions raised in my project: we will start with Hilbert's ideas, then talk about the formalization of reasoning through the deductive systems proposed by Gentzen; we will touch upon automatic and, later, interactive theorem proving and finally we will explain how and why issues related to human-centered theorem proving and human-readable outputs arose and how I plan to study them.

Pedro Patrício, “From Brown-McCoy to orthogonality”

ABSTRACT: A von Neumann inverse of a matrix A is a solution to the matrix equation $AXA=A$. Although the row reduced echelon form allows to prove that any matrix over a field has a von Neumann inverse, a different approach has to be taken whilst considering matrices over a general (possibly non-commutative) ring. The Brown-McCoy Lemma comes to our help. In this talk, I will show that this lemma is a special case of some sort of orthogonality of matrices which delivers another method to construct a von Neumann inverse.

Joint work with R.E. Hartwig, NCSU, USA.