XVI Summer Workshop in Mathematics 2024

Theory of Computation Session

Departamento de Matemática - Universidade de Brasília

		Wednesday (7th)	Thursday (8th)	Friday (9th)
Plenary Talks	9:30 - 10:30		David M. Cerna (Czech Academy of Sciences)	Benjamín R. C. Bedregal (UFRN)
	10:30 - 11:00 (Coffee-Break)			
	11:00 - 12:00			
	12:00 - 14:00 (Lunch)			
Theory of Computation Thematic Session	14:00 - 15:00	Christophe Ringeissen (Inria)	Chelsea Edmonds (University of Sheffield)	Daniel L. Ventura (UFG)
	15:00 - 15:40	Hermann Haeusler (PUC-Rio)	Maria Inés de Frutos-Fernández (Universidad Autónoma de Madrid)	Deivid Vale (Radboud University)
	15:40 - 16:00			Ali Khăn C. R. Santos (UnB)
	16:00 - 16:30 (Coffee-Break)			
	16:30 - 17:10	Daniele Nantes-Sobrinho (UnB / Imperial College London)	Mauricio Ayala-Rincón (UnB)	
	17:10 - 17:40	Gabriela de Souza Ferreira (UnB)	Daniella S. M. De Souza (UnB)	
	17:40 - 18:10	Andrés Felipe G. Barragán (UnB)	Nikson B. F. Ferreira (UnB)	
	18:10 - 18:40	Guilherme B. Brandão (UnB)		

Join Zoom Meeting
https://us02web.zoom.us/j/88233010577

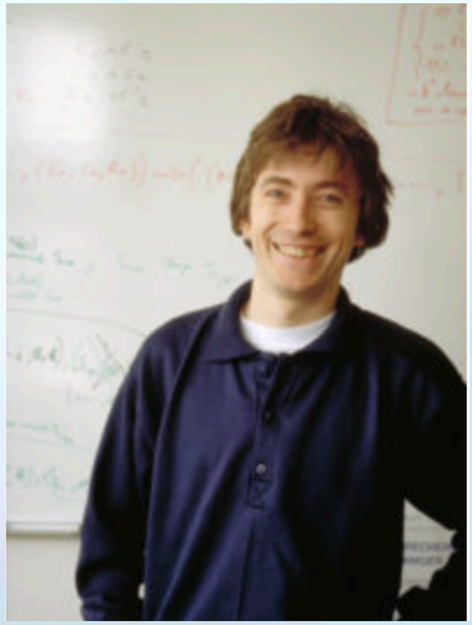
Meeting ID: 882 3301 0577

BRT time zone (GMT-3)

Building and Combining Unification and Matching Procedures

Christophe Ringeissen
Inria, Nancy

Abstract
The concept of unification is ubiquitous in logic programming and in automated reasoning, for instance to perform deduction in theorem proving. Equational unification consists in finding instances of terms so that these instances are equivalent with respect to an equational theory given by some set of axioms. Equational unification being undecidable in general, it is important to identify equational theories and simple cases where it is possible to obtain sound, complete and terminating unification procedures. Matching is a particular (simple) case of unification of greatest interest to execute rule-based programs and to perform simplification in theorem proving. We show a systematic approach to build and to combine unification and matching algorithms for a large class of equational theories. We illustrate the approach on equational theories of practical interest in the analysis of security protocols.



7th February: 14:00 - 15:00 (GMT-3)

Propositional Proofs Compression

Edward Hermann Haeusler
Pontíficia Universidade Católica do Rio de Janeiro (PUC-Rio)

Abstract

This talk presents a novel compressing propositional proofs algorithm and discusses its relevance in solving some computational complexity well-known conjectures.

7th February: 15:00 - 16:00 (GMT-3)

Matching Plans for Frame Inference in Compositional Reasoning

Daniele Nantes-Sobrinho

Universidade de Brasília (UnB) / Imperial College London

Abstract

The use of function specifications and manipulation of user- defined predicates are two essential ingredients of modern compositional verification tools. To execute these operations successfully, these tools must be able to solve the frame inference problem, that is, understand the parts of the state relevant for the operation at hand. We introduce matching plans, which facilitate frame inference and advance the state-of- the-art in that they allow tool users to write intuitive and understandable specifications and the tools to efficiently infer the information required to perform frame inference.

(Joint work with Andreas Lööw, Petar Maksimovic, Philippa Gardner, Sacha Ayoun)

1. 1. Baldoni, R., Coppa, E., D'Elia, D.C., Demetrescu, C., Finocchi, I.: A survey of symbolic execution techniques. ACM Computing Surveys 51(3) (2018)
2. Berdine, J., Calcagno, C., O'Hearn, P.W.: Smallfoot: Modular automatic assertion checking with separation logic. In: FMCO. pp. 115–137 (2005)
3. Berdine, J., Calcagno, C., O'Hearn, P.W.: Symbolic execution with separation logic. In: APLAS. pp. 52–68 (2005)
4. Fragoso Santos, J., Maksimović, P., Sampaio, G., Gardner, P.: JaVerT 2.0: Compositional symbolic execution for JavaScript. PACMPL 3(POPL) (2019). https://doi.org/10.1145/3290379
5. Fragoso Santos, J., Maksimović, P., Ayoun, S., Gardner, P.: Gillian, part I: A multi-language platform for symbolic execution. In: Programming Language Design and Implementation (PLDI) (2020). https://doi.org/10.1145/3385412.3386014, https://doi.org/10.1145/3385412.3386014
6. Jacobs, B., Smans, J., Piessens, F.: The VeriFast Program Verifier: A Tutorial (2017). https://doi.org/10.5281/ZENODO.1068185
7. D., Summers, A.J.: An automatic encoding from VeriFast predicates into implicit dynamic frames. In: Verified Software: Theories, Tools, Experiments (2014). https://doi.org/10.1007/978-3-642-54108-7_11
8. Maksimović, P., Ayoun, S., Santos, J.F., Gardner, P.: Gillian, part II: Real- world verification for JavaScript and C. In: Computer Aided Verification (CAV) (2021). https://doi.org/10.1007/978-3-030-81688-9_38, https://doi.org/10. 1007/978-3-030-81688-9_38

7th February: 16:30 - 17:10 (GMT-3)

Anti-Unification on Terms With Different Types

Gabriela de Souza Ferreira

Universidade de Brasília (UnB)

Abstract

Anti-unification is the problem of expressing the most common structure between two given expressions. The different problems of anti-unification depend on how such commonalities are established and structured. In this talk the focus is in the universe of Typed Lambda Terms, more precisely, in how to identify the common structures of expressions that may have different types. First, a fast presentation of the anti-unification problem for inputs with the same type will be given, with the propose of highlighting the difference between the standard problem and well-known more general problems. Secondly, some preeliminar ideas about how to solve anti-unification for terms with different types will be discussed. The presentation will use several examples and illustrations.

[Barendregt et al.(2013)Barendregt, Dekkers, and Statman] Hendrik Pieter Barendregt, Wil Dekkers, and Richard Statman. Lambda Calculus with Types. Cambridge University Press, 2013. ISBN 978-0-521-76614-2.

[Cerna and Kutsia(2019)] David M. Cerna and Temur Kutsia. A generic framework for higher-order generalizations. In Herman Geuvers, editor, 4th International Conference on Formal Structures for Computation and Deduction, FSCD 2019, June 24-30, 2019, Dortmund, Germany, volume 131, pages 10:1–10:19, 2019. doi:10.4230/LIPICS.FSCD.2019.10.

[Pierce(2002)] Benjamin C. Pierce. Types and programming languages. MIT Press, 2002. ISBN 978-0-262-16209-8.

7th February: 17:10 - 17:40 (GMT-3)

Anti-Unification on Absorption Theories

Andrés Felipe González Barragán
Universidade de Brasília (UnB)

Abstract

Anti-unification or generalization is the process of finding commonalities between expressions. There are many applications of generalization as clone and plagiarism detection. While syntactic forms of anti-unification are enough for many applications, some aspects of software analysis methods are more appropriately modeled by reasoning modulo equational theories. Some important theories include the absorption property; i.e., operators with axioms $f(x, \varepsilon_f) \approx f(\varepsilon_f, x) \approx \varepsilon_f$. This work presents a sound and complete anti-unification algorithm for such theories. Additionally, it shows that anti-unification of absorption theories is of type infinitary, and provides a finitary representation of the minimal complete set of generalizations.

7th February: 17:40 - 18:10 (GMT-3)

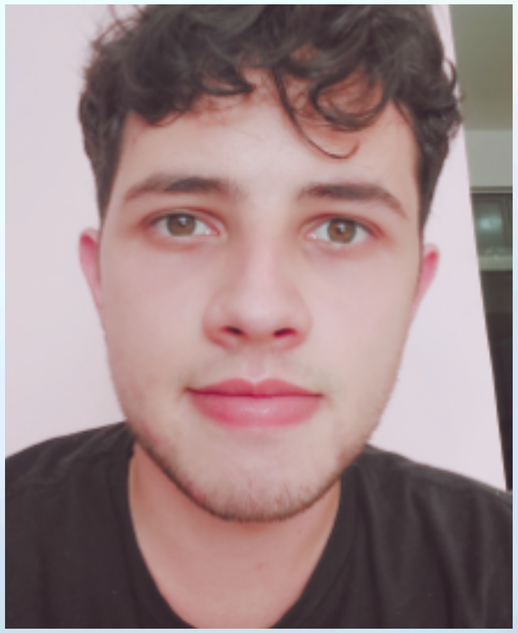
Bounded ACh Unification

Guilherme Borges Brandão
Universidade de Brasília (UnB)

Abstract

E-Unification is a procedure to find solutions to a set of equations between firstorder terms with respect to an equational theory E. ACh theory takes a function symbol h that is an homomorphism over an associative-commutative function symbol. Previous work proved that ACh Unification is an undecidable problem [1]. Recently, however, it was defined an approximation of the problem called Bounded ACh Unification [2], that consists in bounding the number of times that h is applied recursively. In this talk, we will discuss the inference rules for solving this problem and verify the proofs of termination, soundness and completeness.

[1] Narendran, P.: Solving linear equations over polynomial semirings. In: Proceedings, 11th Annual IEEE Symposium on Logic in Computer Science, New Brunswick, New Jersey, USA, July 27-30, 1996, pp. 466–472. IEEE Computer Society(1996). https://doi.org/10.1109/LICS.1996.561463 .
[2] Eeralla, A.K., Lynch, C.: Bounded ach unification. Math. Struct. Comput. Sci. 30(6), 664–682 (2020) https://doi.org/10.1017/S0960129520000183



7th February: 18:10 - 18:40 (GMT-3)

Anti-unification: Introduction, Applications, and Recent Results

David M. Cerna

Czech Academy of Sciences

Abstract

Anti-unification is a method for symbolically generalizing formal expression. It was introduced independently by Plotkin and Reynolds as an operation for inductive inferencing. Though conceptually simple, it is an effective tool for abstraction and templating. Since the seminal work, the number of applications has grown tremendously with uses in program analysis, program repair, library compression, automated reasoning, and beyond. With the growth of applications, there has been an effort to strengthen the theoretical foundations of the subject. In this talk, we introduce anti-unification, overview the existing applications, and discuss recent theoretical results concerning equational and high-order anti-unification.

Plenary talk - 8th February: 9:30 - 10:30 (GMT-3)

Formalising Combinatorial Mathematics: A Modular Approach

Chelsea Edmonds

University of Sheffield

Abstract

Formalised mathematics has historically focussed on the goal of formalising specific well-known theorems, which can lead to issues around reusability and accessibility, especially as formal libraries continue to grow at a rapid pace. My work on formalising combinatorics in Isabelle/HOL presents an approach which places the primary focus on the formalisation of proof techniques and underlying structures, making use of locales, Isabelle's module system. In this talk, I'll give an introduction to the locale-centric methodology for formalising mathematical structures to create flexible, modular and extensible libraries. Additionally, I'll demonstrate how the same locale-centric methods can be applied to set up proof contexts to support general proof techniques. I'll conclude by demonstrating an example probabilistic technique to formalise some results on hypergraphs.

8th February: 14:00 - 15:00 (GMT-3)

Formalizing local fields in the Lean theorem prover

María Inés de Frutos-Fernández
Universidad Autónoma de Madrid

Abstract
Local fields, and more generally fields complete with respect to a discrete valuation, are essential objects in commutative algebra, with applications to number theory and algebraic geometry. We formalize in Lean the basic theory of discretely valued fields, as well as the abstract definition and some fundamental properties of local fields.
This is joint work with Filippo A. E. Nuccio.

8th February: 15:00 - 16:00 (GMT-3)

Exemplifying Contemporary Formal Mathematics

Mauricio Ayala-Rincón
Universidade de Brasília (UnB)

Abstract
Computer-verified theories are the class of "complete" formalizations mathematicians have aimed for centuries. Theorem's proofs formalized in "proof assistants" provide certificates of their "correctness" and the required grade of granularity to be considered "complete." Such proof's mechanizations also come with tools to be ported by mathematicians and other professionals into robust technological tools independently of mathematical intuition, skills, hierarchy, or folklore. Computational formalizations provide absolutely correct proofs except for remote possibilities of computer failures. In this talk, we will select simple mathematical formalizations developed by the local group members to illustrate how such formalizations are developed in the proof assistant PVS.

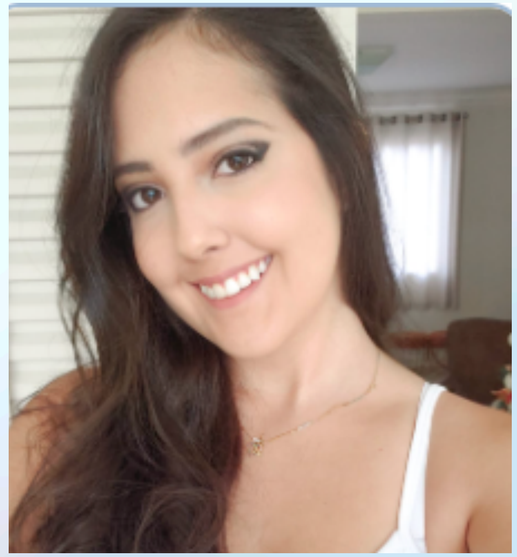
8th February: 16:30 - 17:10 (GMT-3)

Closed Rewriting - Checking overlaps of Nominal Rewriting Rules

Daniella Santaguida Magalhães de Souza
Universidade de Brasília (UnB)

Abstract

Nominal rewriting is not complete for equational reasoning in general; however, closed nominal rewriting is complete for equational reasoning with closed axioms [1]. Intuitively, no free atom occurs in a closed term, and, as a natural assumption, closed axioms do not allow abstracted atoms to become free. In this talk, we will analyze the confluence of nominal rewriting systems (NRS), we will check whether closedness can be useful/essencial to guarantee the confluence of a NRS, and finally we will make some observations on possible extensions for proving confluence modulo equational theories.



[1] M. Fernández and M. J. Gabbay. Closed Nominal Rewriting and Efficiently Computable Nominal Algebra Equality In Proc. of 5th International Workshop on Logical Frameworks and Meta-languages: Theory and Practice (LFMTP), 37–51, 2010.

8th February: 17:10 - 17:40 (GMT-3)

How do PVS strategies help to prove correct float-point implementations?

Nikson Bernardes Fernandes Ferreira
Universidade de Brasília (UnB)

Abstract
Numerical programs are usually taught using real arithmetic but implemented in floating-point arithmetic. The Floats domain does not inherit known Real properties such as distributivity and carries propagating representational errors that can lead to unexpected behaviors. It is hazardous for safety-critical applications such as air traffic management. Following a methodology introduced by M. Moscato, L. Titolo et al., given a logically verified PVS Real specification, it is possible to get a provably correct floating-point implementation, for which it is also possible to obtain mathematical certificates (proofs) ensuring its correct behavior. The proof structure of such certificates is suitable for being fully proved using PVS strategies. This talk will show how we develop PVS strategies to improve proofs' automation degree.

8th February: 17:40 - 18:10 (GMT-3)

Theory and applications of aggregation functions

Benjamín René Callejas Bedregal

Universidade Federal do Rio Grande do Norte (UFRN)

Abstract

The process of combining several numerical values into a single value that somehow represents all of them is called aggregation and the numerical function that carries out this process is called the aggregation function. In the context of fuzzy logic, aggregation functions are always increasing and preserve boundaries, and play an important role in fuzzy logic applications. In this talk we will present theoretical and practical aspects of aggregation functions in computer science, such as fuzzy formal languages, data classification and digital image processing.

Plenary talk - 9th February: 9:30 - 10:30 (GMT-3)

Quantitative Weak Linearisation

Daniel Lima Ventura
Universidade Federal de Goiás (UFG)

Abstract
Weak-linear terms are such that a (syntactic) linearity condition is demanded only on functions that may be applied, i.e consumed during some reduction path, while non-appliable functions, i.e that persists in any reduction path, can be non-linear. Weak linearisation was originally defined through a static characterisation of virtual redices, based on (legal) paths computed from the (syntactical) term tree. We revisit this notion through a quantitative type system, in which minimal typings are characterised through a notion of tightness, where term constructors are classified as either consumable or persistent, thus allowing us to define an expansion relation, between general λ-terms and weak-linear λ-terms, whilst preserving normal forms by reduction.

(Joint work with Sandra Alves, presented at ICTAC2022)

9th February: 14:00 - 15:00 (GMT-3)

A New Characterization of BFFs via Higher-Order Rewriting

Deivid Vale
Radboud University, Nijmegen, NL

Abstract
The class of Basic Feasible Functionals (BFF) is the analog of FP (polynomial time functions) for second-order functionals, that is, functionals that can take (first-order) functions as arguments. BFF can be defined through Oracle Turing machines of running time bounded by a second-order polynomial. On the other hand, higher-order term rewriting provides a powerful and elegant formalism for expressing higher-order computation. In this talk, we address the problem of characterizing BFF by higher-order rewriting. Unrestricted higher-order computation certainly can compute beyond the feasible polytime functionals. We show how to appropriately restrict such computations in our framework to capture exactly those type-2 functionals in BFF. This is achieved by employing the recently introduced notion of cost-size interpretations, and we argue that such a characterization could not have been obtained employing classical integer-based interpretations. Finally, we shed light on the soundness and completeness of such a rewriting-based characterization of higher-order complexity classes.
The results I will present in this talk were obtained by a joint work with Patrick Baillot, Ugo Dal Lago, and Cynthia Kop.

9th February: 15:00 - 15:40 (GMT-3)

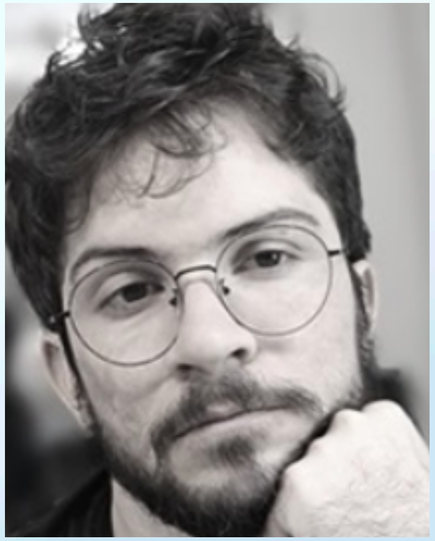
A Strong Nominal Algebra for α Nominal Theory with Fixed-Point Constraints

Ali Khăn Caires Ribeiro Santos

Universidade de Brasília (UnB)

Abstract

Nominal algebra is a framework for interpreting and reasoning about systems with binding, using nominal terms as its term language. Its derivation rules are subject to freshness conditions and extend first-order terms with object-level variables, meta-level variables, and constructs for binding, alpha-equivalence, and capture avoidance. The semantics of nominal algebra are in the class of nominal sets, which have a rich structure for involving names, permutation, and name binding. Previous work has proven the soundness and completeness of nominal algebra, with applications including interpreting solutions to nominal (dis)unification problems. However, recent investigations show that the intentional semantics of nominal algebra with fixed-point constraints is not sound. This talk presents a counterexample and proposes solutions by exploring a subclass of nominal sets called strong nominal sets and necessary modifications in derivation rules.



[1] Christian Urban, Andrew M. Pitts, Murdoch Gabbay: Nominal unification. Theor. Comput. Sci. 323(1-3): 473-497 (2004)
[2] Murdoch James Gabbay: Nominal Algebra and the HSP Theorem. J. Log. Comput. 19(2): 341-367 (2009)
[3] Murdoch James Gabbay, Aad Mathijssen: Nominal (Universal) Algebra: Equational Logic with Names and Binding. J. Log. Comput. 19(6): 1455-1508 (2009)
[4] Mauricio Ayala-Rincón, Maribel Fernández, Daniele Nantes-Sobrinho: On Nominal Syntax and Permutation Fixed Points. CoRR abs/1902.08345 (2019)
[5] Mauricio Ayala-Rincón, Maribel Fernández, Daniele Nantes-Sobrinho, Deivid Vale: On Solving Nominal Disunification Constraints. LSFA 2019: 3-22
[6] Mauricio Ayala-Rincón, Maribel Fernández, Daniele Nantes-Sobrinho: On Nominal Syntax and Permutation Fixed Points. Log. Methods Comput. Sci. 16(1) (2020)
[7] Mauricio Ayala-Rincón, Maribel Fernández, Daniele Nantes-Sobrinho, Deivid Vale: Nominal Equational Problems. FoSSaCS 2021: 22-41

9th February: 15:40 - 16:10 (GMT-3)

Session Committees

Organizing committee

Mauricio Ayala-Rincón
Universidade de Brasília

Scientific committee

Elaine Pimentel
University College London

Thaynara Arielly de Lima
Universidade Federal de Goiás