Days in Logic 2020

FCUL

January 30 – February 1, 2020

http://dil2020.campus.ciencias.ulisboa.pt/

Welcome Address

This year, the biennial meeting Days in Logic has 49 participants and 22 contributed talks. Given the amount of talks, the Organizing Committee decided to have parallel sections. In this way, the speakers have more time to speak (25m) and the pace is more relaxed. We have tried to schedule the parallel sections with nonoverlapping topics but, of course, this is an exercise that has its limitations. The invited addresses and the tutorials are plenary. We believe that, with your willingness to speak and/or participate, we have put together an interesting meeting. We hope you enjoy Days in Logic 2020.

The Organizing Committee
Bruno Dinis, Fernando Ferreira, Gilda Ferreira

P.S.– We are in a position to announce that Days in Logic 2022 will take place at Universidade do Algarve. Our colleague Daniel Graça will organize the meeting. We hope to see you again in two years time in Faro.

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

CMAF CIO
CENTRO DE MATEMÁTICA, APLICAÇÕES FUNDAMENTAIS
E INVESTIGAÇÃO OPERACIONAL

Contents

List of Participants

Name	Affiliation
Ana Borges	Universitat de Barcelona
Andrei Sipos	TU Darmstadt
Andreia Mordido	Universidade de Lisboa
António Marques Fernandes	Universidade de Lisboa
Bruno Dinis	Universidade de Lisboa
Bruno Jacinto	Universidade de Lisboa
Carlos Caleiro	Universidade de Lisboa
Clarence Protin	
Cristina Sernadas	Universidade de Lisboa
Daniel Graça	Universidade do Algarve
Daniel Sousa	Universidade de Lisboa
Diana Costa	University College London
Duarte Costa	Universidade de Lisboa
Étienne Miquey	LSV - CNRS - INRIA
Fernando Ferreira	Universidade de Lisboa
Filipe Casal	Universidade de Lisboa
Francisca Silva	Universidade de Lisboa
Gilda Ferreira	Universidade Aberta
Gonçalo Moreno	Universidade de Lisboa
Imme van den Berg	Universidade de Évora
Isabel Ferreirim	Universidade de Lisboa
Isabel Oitavem	Universidade Nova de Lisboa
Ísis Rodrigues	Universidade de Lisboa
Jaime Gaspar	Universidade de Lisboa
João Miranda	Universidade de Lisboa
João Rasga	Universidade de Lisboa
João Silva	Universidade de Lisboa
José Espírito Santo	Universidade do Minho
Leandro Gomes	Universidade do Minho
Luca Tranchini	University of Tubingen
Lucas Rosenblatt	University of Buenos Aires
Luís Cruz-Filipe	University of Southern Denmark
Luis Pereira	Universidade de Lisboa
Luís Pinto	Universidade do Minho
Mário Edmundo	Universidade de Lisboa
Marta Esteves	Universidade de Lisboa
Miguel Boto	Universidade de Lisboa
Mirna Dzamonja	University of East Anglia
Pantelis Eleftheriou	University of Konstanz
Patrícia Engrácia	DGEC
Paulo Oliva	Queen Mary University of London
Paulo Santos	Universidade Nova de Lisboa
Pedro Filipe	Universidade de Lisboa
Pedro Gonçalves	Universidade de Lisboa
Pedro Pinto	TU Darmstadt
Rafael Monteiro	Universidade de Lisboa
Rodrigo Almeida	ISCTE
Rui Li	Sorbonne University
Sérgio Marcelino	Universidade de Lisboa

Invited speakers

Tutorials

New and old in forcing

Mirna Dzamonja
University of East Anglia

We shall give a tutorial on forcing, starting with no background required, going through some classical results, to finish with some modern preoccupations. Some of the material is based on our upcoming book "Fast Track to Forcing", Cambridge University Press.

Proof translations and interpretations, and their use in proof mining

Paulo Oliva
Queen Mary University of London

In this tutorial we focus on a branch of structural proof theory concerned with translations and interpretations of proofs. We will look at proof translations such as negative (or double-negation) translations and the A-translation, and proof interpretations such as realizability and functional interpretations. These tools have been used for a variety of applications, including relative consistency and independence results, but in this tutorial we will focus on their most recent application in proof mining, i.e. the extraction of computational content from ineffective proofs in mathematics.

Invited addresses

Reduction techniques for proving decidability in logics and their meet-combination

Cristina Sernadas
Instituto Superior Técnico, Universidade de Lisboa

(joint work with João Rasga and Walter Carnielli)

Satisfaction systems and reductions between them are presented as the right context for analyzing the satisfiability and the validity problems. In order to cope with the meet-combination of logics the notion of reduction involves a finite collection of problems as target. Reductions between satisfaction system induce reductions between the respective satisfiability problems and (with mild conditions) also between their validity problems. Suficient conditions are provided for relating satisfiability and validity problems. Preservation results for decidability are shown. The validity problem in the meet-combination is proved to be decidable whenever the validity problems for the components are decidable. Several examples are discussed namely intuitionistic and modal logics as well as the meet-combination of intuitionistic and K modal logic.

On two approaches to the Russell-Prawitz translation

Luca Tranchini
University of Tubingen

(joint work with Mattia Petrolo and Paolo Pistone)

In (proof-theoretic) semantic investigations of natural deduction, it is common to take the conversions defining normalization as inducing an equivalence relation on derivations. In the system for intuitionistic propositional logic (henceforth NI), there are three families of conversions: beta-conversions (those eliminating intro/elim patterns), eta-conversions (sometimes referred to as "immediate expansions") and gamma-conversions (usually called "permutative" or "commuting" conversions).

The equivalence relation induced by these conversions plays an essential role in the categorical semantics of NI, as equivalent derivations are interpreted by the same entity (a morphism in a bi-cartesian closed category). For this reason this equivalence relation is sometimes referred to as identity of proofs.

Since Russell it is well-known that propositional connectives like conjunction and disjunction can be defined using only implication and propositional quantification. In natural deduction, the derivability-preserving mapping from NI into System F (also referred to as NI2) is usually called the Russell-Prawitz translation (henceforth RP-translation).

When not only derivability but also identity of proofs is considered, the RP-translation is not fully satisfactory. Although the RP-translation maps beta-equivalent

NI-derivations onto beta-equivalent NI2-derivations, the images of two eta-equivalent or gamma-equivalent NI-derivations are in general, non-equivalent derivations in NI2.

In talk I will first present a solution to this equivalence-preservation problem obtained by introducing an extension of the standard equational theory of NI2. First I will present a syntactic formulation of a class of equations (called epsilon-equations) for NI2-derivations that arise from the categorical models of System F based on the notion of dinatural transformation. Then I will show how, once the equivalence on NI2-derivation is extended with the epsilon-equations, the RP-translation can be shown to preserve the equivalence of NI-derivations.

In the second part of the talk, I will discuss a proposal by Ferreira and Ferreira to modify the RP-translation to map NI onto System Fat or atomic System F. The latter (to which we will refer to, for uniformity, as NI2at) is the predicative fragment of NI 2 obtained by requiring the witness of each application of the quantifier elimination rule to be an atomic formula.

The starting point of Ferreira and Ferreira's proposal is the discovery that for some quantified formulas, in particular for those that are the RP-translation of some propositional formula, the unrestricted elimination rule is derivable in NI2at.

As Ferreira and Ferreira show, their alternative translation (henceforth FF-translation) does preserve the equivalence generated by eta- and gamma-conversion for disjunction without the need of extending the equational theory of NI2 with the espilon equations.

This fact suggests the existence of a close connection between these two lines of work that will be explored in the third part of the talk.

Contributed talks

Foundational aspects of external numbers

Imme van den Berg
CIMA, University of Évora (Portugal)

The external number system intends to integrate ordinary real numbers and orders of magnitude. The real numbers are called *precise*. The imprecision of an order of magnitude is modelled by a *neutrix*. This is a convex additive group of (nonstandard) real numbers, an example is the external set of infinitesimals $\oslash$: the sum of infinitesimals is infinitesimal. This catches imprecision: if ε is a fixed infinitesimal, then $\oslash+\varepsilon = \oslash$, i.e. $\oslash$ is invariant by small shifts (the Sorites property). Much more neutrices exist and an external number is the sum of a precise number and a neutrix. The external numbers satisfy many algebraic properties, coming close to the real number system. The principal properties served as axioms for a structure called *Complete Arithmetical Solid CAS* [1].

We address here some foundational aspects. In particular, in the axiomatic nonstandard analysis built upon Nelson's Internal Set Theory IST [3] the external numbers do not form a set, but a class. In contrast, a CAS is a set of classical set theory. However, it has a built-in double model of at least the nonstandard rationals, and implies a version of the weak fragment $REPT$ of nonstandard analysis used by Nelson in Radically Elementary Probability Theory [4]. An interesting question is whether the whole of $REPT$ is incorporated. Our approach profited from joint work with Fouad Koudjeti (Groningen) [2] and Bruno Dinis (Lisboa).

References

[1] B. Dinis, I. van den Berg, Neutrices and external numbers. A flexible number system, Chapman and Hall, 2019.
[2] F. Koudjeti, I. van den Berg, Neutrices, external numbers and external calculus, in: Nonstandard analysis in practice, F. and M. Diener, eds., Springer Universitext, Berlin, 1995.
[3] E. Nelson, Internal Set Theory: a new approach to nonstandard analysis, *Bull. Amer. Math. Soc.* **83**(6), pp. 1165–1198, 1977.
[4] E. Nelson, Radically Elementary Probability Theory, Princeton University Press, 1987.

Analytic calculi for monadic PNmatrices

Carlos Caleiro, Sérgio Marcelino
SQIG - Instituto de Telecomunicações, Departamento de Matemática,
Instituto Superior Técnico, Universidade de Lisboa (Portugal)

Analytic calculi are a valuable tool for a logic, as they allow for effective proof-search and decidability results. Using inference rules which can have more than one conclusion, we show how to obtain simple axiomatizations for logics associated to any given monadic partial non-deterministic matrix (PNmatrix). Further, we prove that these axiomatizations are always analytic, which seems to raise a contrast with recent non-analyticity results for sequent-calculi with PNmatrix semantics.

References

[1] D. Shoesmith and T. Smiley, *Multiple-Conclusion Logic*. Cambridge University Press, 1978.
[2] M. Baaz, O. Lahav, and A. Zamansky, Finite-valued semantics for canonical labelled calculi. *Journal of Automated Reasoning*, 51(4):401–430, 2013.
[3] S. Marcelino and C. Caleiro, Axiomatizing non-deterministic many-valued generalized consequence relations. *S*ynthese, doi 10.1007/s11229-019-02142-8, 2019.
[4] C. Caleiro and S. Marcelino, Analytic calculi for monadic PNmatrices. In R. Iemhoff, M. Moortgat, R. de Queiroz, editor, *Logic, Language, Information and Computation (WoLLIC 2019)*, volume 10388 of *LNCS*, pages 84–98. Springer, 2019.

Reasoning over permissions regions in concurrent separation logic

James Brotherston[1], Diana Costa[1], Aquinas Hobor[2],John Wickerson[3]
(1) University College London, UK, (2) National University of Singapore, (3) Imperial College London, UK

We propose an extension of separation logic with *fractional permissions*, aimed at reasoning about permissions over arbitrary regions or data structures in memory. In existing formalisms, such reasoning typically either fails, or is subject to stringent side conditions on formulas (notably *precision*). We suggest two formal syntactic additions that collectively remove the need for such side conditions: first, the use of both "weak" and "strong" forms of separating conjunction; and, second, the use of nominal labels on formulas. We believe that our suggested alterations bring formal reasoning with fractional permissions in separation logic considerably closer to common pen-and-paper intuition, while imposing only a very modest bureaucratic overhead.

References

[1] R. Bornat, C. Calcagno, P. O'Hearn, and M. Parkinson, Permission accounting in separation logic. In *Proceedings of POPL-32*, pages 59–70. ACM, 2005.
[2] J. Boyland, Checking interference with fractional permissions. In *Proceed ings of SAS-10*, pages 55–72. Springer, 2003.

[3] S. Brookes, A semantics for concurrent separation logic. *Theoretical Com- puter Science*, 375(1–3):227–270, 2007.
[4] A. Hobor and J. Villard, The rami
cations of sharing in data structures. In *Proceedings of POPL-40*, pages 523–536. ACM, 2013.
[5] J. C. Reynolds, Separation logic: A logic for shared mutable data structures. In *Proceedings of LICS-17*, pages 55–74. IEEE Computer Society, 2002.
[6] V. Vafeiadis, Concurrent separation logic and operational semantics. In *Proceedings of MFPS-27*, volume 276 of ENTCS, pages 335–351. Elsevier, 2011.

Hypothetical answers to continuous queries over data streams

Luís Cruz-Filipe[1], Graça Gaspar[2], Isabel Nunes[2]
(1) Dept. of Mathematics and Computer Science, University of Southern Denmark (Denmark),
(2) University of Lisbon, Faculty of Sciences & BioISI - Biosystems & Integrative Sciences Institute (Portugal)

Continuous queries over data streams often delay answers until some relevant input arrives through the data stream. These delays may turn answers, when they arrive, obsolete to users who sometimes have to make decisions with no help whatsoever. Therefore, it can be useful to provide hypothetical answers – "given the current information, it is possible that X will become true at time t" – instead of no information at all.

In this talk we build on techniques from logic programming, and introduce a semantics for queries and corresponding answers that covers such hypothetical answers, together with an online algorithm for updating the set of facts that are consistent with the currently available information.

This work has been accepted for publication and presentation at the 34th AAAI Conference on Artificial Intelligence (AAAI-20).

A new cohomology for algebraic varieties over non-achimedean fields

Mário Edmundo
Universidade de Lisboa & CMAFcIO

The interplay between analytic geometry over non-archimedean fields and tropical geometry is a very active area with several applications in fields such as algebraic and arithmetic geometry. Recently, Hrushovski and Loeser introduced a model-theoretic account of the Berkovich's analytification of algebraic varieties: given a variety V over a non-archimedean field K, Hrushovski and Loeser associated to V the space $\hat{V}$, the stable completion of V, and showed a very deep connection between V and the tropical semi-group Γ_∞ where Γ is the value group of K: there is a deformation retraction from $\hat{V}$ to a definable subset of some finite power ofΓ_∞. An analogous result was earlier proved by Berkovich for V^{an} under strong algebraic

restrictions on the variety V. In this talk we report on the ongoing work (with P. Kovacsics and J. Ye) where we develop a sheaf cohomology theory for the spaces $\hat{V}$. When the field K is maximally complete of rank one, the spaces $\hat{V}$ and $|V^{an}|$ are naturally homeomorphic and we recover results proved by Berkovich for the cohomology groups.

Strongly minimal groups in o-minimal structures

Pantelis Eleftheriou
University of Konstanz (Germany)

We prove Zilber's Trichotomy Conjecture for strongly minimal expansions of 2-dimensional groups, definable in o-minimal structures: Theorem [1]. Let R be an o-minimal expansion of a real closed field, $(G, +)$ a 2-dimensional group definable in R, and $D = (G, +, ...)$ a strongly minimal structure, all of whose atomic relations are definable in R. If D is not locally modular, then an algebraically closed field K is interpretable in D. Moreover, the group G, with all its induced D-structure is definably isomorphic in D to an algebraic K-group with all its induced K-structure.

The proof involves topological and analytical arguments in order to recover "complex intersection theory", which allows us to define the field. We will sketch the topological part. Joint work with Assaf Hasson and Ya'acov Peterzil.

References

[1] P. Eleftheriou, A. Hasson, Y. Peterzil, Strongly minimal groups in o-minimal structures, Journal of the European Mathematical Society (to appear), 66 pages.

The call-by-value lambda-calculus with generalized applications

José Espírito Santo
Centre of Mathematics, University of Minho (Portugal)

The ordinary λ-calculus [1] can be qualified naively as being a call-by-name (cbn) system, simply because its β-rule prescribes that, in functional application, functions are called without prior evaluation of arguments. Plotkin [4] argues that the ordinary λ-calculus is *the* call-by-name λ-calculus, due to the standardization theorem and the link it establishes between reduction of λ-terms and the call-by-name evaluation of programs. Plotkin [4] also makes a proposal for the call-by-value λ-calculus - a proposal that has been debated and improved until today.

The λ-calculus with generalized applications [3], also named system ΛJ, corresponds, under the Curry-Howard isomorphism, to the system of natural deduction with generalized elimination rules [5], in the setting of intuitionistic implicational logic. System ΛJ can also be qualified naively as being a call-by-name system. In this talk we present system $\Lambda J_{\mathtt{v}}$, a recently proposed call-by-value variant of system

ΛJ [2], which enjoys the required standardization theorem linking reduction and a certain notion of call-by-value evaluation.

The most prominent feature of the novel system is its simplicity: the definition of proof terms, reduction and typing does not change w. r. t. the original system ΛJ: the only change is in the definition of substitution. In particular, the calling of functions does not require arguments to be values. Besides standardization, confluence and strong normalization have also been proved. A final surprise shows up in the connection between ΛJ and $\Lambda J_{\mathtt{v}}$: mutual simulations are obtained by translations implementing the "protecting-by-a-λ" technique; and these can be typed using a type transformation based on the replacement of a type A by $true \supset A$. Recall Plotkin [4] obtains mutual simulations through continuation-passing-translations - and these, at the type level, require the replacement of a type A by $\neg\neg A$.

References

[1] H. P. Barendregt, The Lambda Calculus: its Syntax and Semantics. North Holland, 1984.
[2] J. Espírito Santo, The call-by-value lambda-calculus with generalized applications. In *Proceedings of 28th International Conference Computer Science Logic 2020*, volume 152 of *Leibniz International Proceedings in Informatics*. Schloss Dagstuhl. To appear.
[3] F. Joachimski and R. Matthes, Standardization and confluence for a lambda calculus with generalized applications. In *Proceedings of 11th International Conference Rewriting Techiques and Applications 2000*, volume 1833 of *Lecture Notes in Computer Science*, pp. 141–155. Springer, 2000.
[4] G. Plotkin, Call-by-name, call-by-value and the λ-calculus. *Theoretical Computer Science*, 1, pp. 125–159, 1975.
[5] J. von Plato, Natural deduction with general elimination rules. *Annals of Mathematical Logic*, 40(7), pp. 541–567, 2001.

Infectious semantics for inclusion logics

Carlos Caleiro, Sérgio Marcelino, Pedro Filipe
SQIG - Instituto de Telecomunicações, Departamento de Matemática,
Instituto Superior Técnico, Universidade de Lisboa (Portugal)

We show that non-determinism can be used to give simple and effective many-valued semantics, by the mere addition of a suitably infectious value, to a range of companions of a given many-valued logic that result from filtering its inferences by requiring that variables, as well as certain other prescribed subformulas, of the premises and conclusion of an inference respect an inclusion requirement. Under a monadicity requirement, analytic calculi for the resulting logics can also be systematically obtained.

References

[1] S. Halldén, *The logic of nonsense*. PhD thesis, Uppsala Universitet, 1949.
[2] J. Dunn, A sieve for entailments. *Journal of Philosophical Logic*, 9(1):41–57,

1980.
[3] D. Bochvar and M. Bergmann, On a three-valued logical calculus and its application to the analysis of the paradoxes of the classical extended functional calculus. *History and Philosophy of Logic*, 2(1-2):87–112, 1981.
[4] H. Omori and D. Szmuc, Conjunction and disjunction in infectious logics. In A. Baltag, J. Seligman, and T. Yamada, editors, *6th International Workshop in Logic, Rationality and Interaction (LORI 2017)*, volume 10455 of *LNCS*, pages 268–283. Springer, 2017.
[5] S. Bonzio, T. Moraschini, and M. Pra Baldi, Logic of left variable inclusion and Płonka sums of matrices. *arXiv e-prints, https://arxiv.org/abs/1804.08897*, Apr 2018.
[6] C. Caleiro, S. Marcelino and P. Filipe. Infectious semantics and analytic calculi for even more inclusion logics. submitted, 2019.

A family of dynamic logics for conditionals in *fuzzy arden syntax*

Leandro Gomes[1], Alexandre Madeira[2], Luis Soares Barbosa[3]
(1) HASLab INESC TEC (Portugal), (2) CIDMA (Portugal), (3) Quantum Software Engineering Group, INL (Portugal)

Fuzzy programming languages emerged to describe systems that reason about information which cannot be evaluated in simple terms of "true" and "false". Typical examples of these languages find its utility in distinct application domains, such as medical diagnosis [3] and robotics [1]. The syntax of these programming languages include variables storing information as fuzzy sets, and a set of conditional rules to describe the behaviour of the system. Such rules, which syntactically are just **if-then-else** and **switch-case** statements do not behave nondeterministically, as it happens in the more classic scenario, presenting instead a parallelism inherent to their execution, due to the nature of the fuzzy information that is evaluated. We introduce a family of dynamic logics for reasoning about fuzzy conditionals, including a semantics where programs (conditionals) are interpreted as *fuzzy binary multirelations*. Such novel mathematical concept generalises binary multirelations [2] to model an execution from one state to a set of states in parallel, with (possible) different weights associated with each branch of execution. The method is parametric on a generic complete residuated lattice, offering a suitable truth space to deal with fuzzy information.

References

[1] P. Cingolani and J. Alcal-fdez, jFuzzyLogic: a java library to design fuzzy logic controllers according to the standard for fuzzy control programming, *International Journal of Computational Intelligence Systems* **6**, pp. 61–75, 2008.
[2] I. Rewitzky, Binary multirelations, In Harrie C. M. de Swart, Ewa Orlowska, Gunther Schmidt, and Marc Roubens, editors, *Theory and Applications of Relational Structures as Knowledge Instruments, COST Action 274, TARSKI, Revised Papers*, volume **2929** of *Lecture Notes in Computer Science*, pp. 256–271, Springer, 2003.

[3] T. Vetterlein H. Mandl and K. Adlassnig, Fuzzy arden syntax: A fuzzy programming language for medicine, *Artificial Intelligence in Medicine*, **49**(1), pp. 1–10, 2010.

Ship of Theseus Paradox: A new solution (?)

Pedro Gonçalves
Mathematics Undergraduate, Sciences Faculty, Lisbon University (Portugal)

For about 2500 years renowned philosophers and thinkers like Heraclitus, Plato, Aristotle, Plutarch, Hobbes, Locke, among others, have discussed and presented both new and more complex scenarios and theories about this paradox, each of which with different advantages and disadvantages, implying the rejection of either one or more of philosophical principles, like transitivity. In short, the paradox deals with metaphysics of identity. It's a thought experiment about the persistence of an object's identity when one or more of its constituent parts are replaced by different ones. My objective is to present an alternative view on the subject, leading to a possible new solution to the paradox, implying the acceptance of two new logical symbols, shifting the core of the discussion around the subject away from the metaphysics of identity to something I could call the metaphysics of heredity (?).

References

[1] `https://www.youtube.com/watch?v=dYAoiLhOuao`, visualized on 07.12.2019, at 11:00 hours.
[2] `https://en.wikipedia.org/wiki/Ship_of_Theseus`, visualized on 07.12.2019, at 11:10 hours.

The set of invertible zeros on the unit ball is computable

Daniel Graça[1], Ning Zhong[2]
(1) Universidade do Algarve (Portugal) & Instituto de Telecomunicações (Portugal) (2) University of Cincinnati (USA)

A common problem in mathematics is to find the zeros of a function. In certain circumstances one is able to explicitly find all the zeros with a formula (e.g. quadratic formula). However that is not possible in general, even if the function is a polynomial. In those cases the usual option is to resort to numerical root-finding algorithms. There are numerous root-finding algorithms such as Newton's method, Bisection method, Secant method, and Inverse Interpolation method, to mention just a few. However these methods are essentially local, since they only approximate a zero with arbitrary precision if they are applied in a suitable neighborhood of a zero. The choice of this neighborhood can nevertheless be a nontrivial problem.

In this talk we investigate the computability of the zero set (i.e. the set of all zeros) of a function defined on a compact set, which we take as the unit ball over $\mathbb{R}^n$. We show that if the function is assumed to be of class C^1, then the zero set is (uniformly) computable if all zeros have an invertible jacobean. This condition is

needed as one can also show that the zero set is not computable over the set of all functions of class C^1.

As a corollary, we also show that one can (uniformly) compute the number of zeros of a C^1 function defined over the unit ball.

Adapted Kreisel's conjecture via reflexion principles on a new provability predicate

Paulo Guilherme Santos, Reinhard Kahle
FCT NOVA & Tübingen University (Portugal, Germany)

Kreisel's Conjecture is the statement: if, for all $n \in \mathbb{N}$, PA $\vdash_{k \text{ steps}} \varphi(\overline{n})$, then PA $\vdash \forall x.\varphi(x)$. Given a recursive function h, we introduce a notion of provability '$\vdash_{\leq h}$' by imposing that PA $\vdash_{\leq h} \varphi$ holds if there is a proof of φ in PA whose code is at most $h(\#\varphi)$—this notion depends on the coding one fixes. We create a provability predicate $\mathcal{P}_h(x)$ that expresses '$\vdash_{\leq h}$' in PA. We prove the existence of a sentence φ and a total recursive function h such that PA $\vdash_{\leq h} \mathcal{P}_{\text{PA}}(\ulcorner \mathcal{P}_{\text{PA}}(\ulcorner \varphi \urcorner) \to \varphi \urcorner)$, but PA $\not\vdash_{\leq h} \varphi$. With the help of reflexion principles on $\mathcal{P}_h(x)$, we construct a non-trivial theory S^h_Γ that extends PA such that a version of Kreisel's Conjecture holds: given a recursive function h and $\alpha(x)$ a Γ-formula (where Γ is an arbitrarily fixed class of formulas) such that, for all $n \in \mathbb{N}$, PA $\vdash_{\leq h} \alpha(\overline{n})$, then $\mathrm{S}^h_\Gamma \vdash \forall x.\alpha(x)$. We study the provability predicate $\mathcal{P}_h(x)$ and we present several properties of it.

"This is a self-reference"

Rui Li
Sorbonne University (France)

Self-reference in proof theory is important enough to be given a talk on. This talk will be composed of two parts: one in which I talk about the self-reference from the point of view of a human; another one is about self-reference on its own right. They certainly have cross reference on each other.

Various developments in philosophy and cognitive science show that the human's brain can be programmed (formalised in the language of logic). We also know that when a theorem in logic is proved, it is in human's brain where it happens. So it can be something in one arithmetic about another arithmetic. What if we prove something about the formalised human arithmetic? Then it is proved by itself, using the same arithmetical language. Formalised human brain is not only able to self-reference, but also in a way that no metalanguage is required. This property might solve many problems in formal arithmetic, such as the unprovability of inconsistency. In my talk, I will characterise the arithmetic for human's brain if it is formalisable. If not, the type of the arithmetic should be interesting to be considered on its own.

I will then turn to the issue of self-reference and self-referencing a self-reference, which will be a relatively philosophical discussion. Here, I would like to stress the importance of self-reference by showing how it can be used to solve the problems

caused by itself. The ideas are assembled from different logicians, but also from myself.

By the end, we should notice that these two parts of the talk are actually addressing the same issue: does there exist an absolute theory such that it can prove itself? This question originated from an old question in philosophy: who created the God who created everything?

References

Ideas by Raymond Smullyan, Thomas Bolander, Jerry Fodor, René Descartes (The list is not exclusive).

Adding axioms

Carlos Caleiro, Sérgio Marcelino

SQIG - Instituto de Telecomunicações, Departamento de Matemática,
Instituto Superior Técnico, Universidade de Lisboa (Portugal)

In this talk we consider the general problem of strengthening the logic of a given PNmatrix with a set of axioms. Our results have three key ingredients: (1) the very general but not very effective method stemming from the theory of combined logics, (2) the technique of rexpansions developed by Avron and coauthors, and most prominently (3) the idea of lookahead values previously used by Ciabattoni, Lahav, Spendier, and Zamansky. Namely, under certain restrictions on the given semantics and the shape of the axioms we provide an effective method for obtaining a neat PNmatrix characterization of the resulting logic, and show that it covers a myriad of examples in the literature. Under a monadicity requirement on the base logic, analytic calculi for the resulting logics can also be systematically obtained.

References

[1] A. Ciabattoni, O. Lahav, L. Spendier, and A. Zamansky, Taming paraconsistent (and other) logics: An algorithmic approach. *ACM Transactions on Computational Logic*, 16(1):5:1–5:23, 2014.
[2] A. Avron and Y. Zohar, Rexpansions of non-deterministic matrices and their applications in non-classical logics. *Review of Symbolic Logic*, 12(1):173–200, 2019.
[3] C. Caleiro and S. Marcelino, On axioms and rexpansions. Submitted, 2019.

Nonstandard analysis in Krivine realizability

Étienne Miquey[1], Bruno Dinis[2]
(1) LSV, CNRS, Inria (France), (2) Universidade de Lisboa & CMAFcIO

Introduced by Robinson in the 60s [8], nonstandard analysis brought the first formal account for the notion of infinitesimal. To do so, he presented a construction to extend usual mathematical sets ($\mathbb{N}$, $\mathbb{R}$, etc.) witnessing the existence of new elements, the so-called *nonstandard* individuals. Later in the 70s, Nelson developed a syntactic approach to nonstandard analysis, introducing in particular three key principles (dubbed idealization, standardization and transfer) [7]. The validity of these principles for constructive mathematics has been studied in different settings, in particular several recent works lead to interpretations of nonstandard theories in intuitionistic realizability models [1,3,2].

In this talk, we propose to contemplate a different approach to nonstandard interpretations in realizability. On the one hand, we would like to deal with nonstandard analysis in the context of Krivine classical realizability [5]. By completely reformulating Kleene's intuitionistic realizability to take into account both terms (the realizers) and stacks (*i.e.* evaluation contexts for terms), Krivine managed to defined a notion of realizability compatible with classical logic that highlighted how new reasoning principles can be obtained by considering new programming primitives in the underlying operational semantics [4,6]. On the other hand, we focus on Robinson's construction of a model for nonstandard analysis via an ultraproduct rather than on Nelson's syntactic approach (as is done in the aforementioned work in intuitionistic realizability). In particular, we add a memory cell to the Krivine machine in order to indicate in which slice of the ultraproduct $\mathcal{M}^{\mathbb{N}}$ the machine is. We will then explain how this product can be quotiented to mimick Robinson's construction, and we shall pay attention to the nonstandard principles (and their computational content) that we can obtain in this setting.

References

[1] B. Berg, E. Briseid, and P. Safarik. A functional interpretation for non- standard arithmetic. *Ann. Pure Appl. Logic*, 163(12):1962–1994, 2012.
[2] B. Dinis and J. Gaspar. Intuitionistic nonstandard bounded modified realisability and functional interpretation. *Ann. Pure Appl. Logic*, 169(5):392–412, 2018.
[3] A. Hadzihasanovic and B. van den Berg. Nonstandard functional interpretations and categorical models. *ND Journal of Formal Logic*, 58(3), 2017.
[4] J.-L. Krivine. Dependent choice, quote and the clock. *Th. Comp. Sc.*, 2003.
[5] J.-L. Krivine. Realizability in classical logic. In Interactive models of computation and program behaviour. *Panoramas et synthèses*, 27, 2009.
[6] A. Miquel. Forcing as a program transformation. In em LICS, 2011.
[7] E. Nelson. Internal set theory: A new approach to nonstandard analysis. *Bull. Amer. Math. Soc*, 1977.
[8] A. Robinson. Non-standard analysis. *Proc. Roy. Acad. Sci.*, 1961.

A ZK proof system for 3-SAT and its applications

Rafael Monteiro[1,2], André Souto[2,3,4], Paulo Mateus[1,2]

(1) Instituto de Telecomunicações (Portugal), (2) Instituto Superior Técnico, Universidade de Lisboa (Portugal), (3) LASIGE (Portugal), (4) Faculdade de Ciências da Universidade de Lisboa (Portugal)

Zero-knowledge proof systems [1] are particular interactive proof systems where no additional knowledge is obtained other than the correctness of a certain proposition.

One of the most useful results is the existence of a zero-knowledge interactive proof system for any NP problem [2,3]. Usually, the construction of such ZK proof systems is based on a ZK proof system for another NP-complete problem (such as G3C), on the existence of one-way functions and on the classical reduction among NP problems.

In this paper, we present a direct zero-knowledge protocol for 3-SAT different from [3]. We prove that our protocol, contrarily to [3], can be made computationally resilient against quantum adversaries by using a quantum computationally concealing commitment scheme, following the results of [4]. As a consequence, we derive ZK proof systems for any NP problem that are computationally secure against quantum computers that, in principle, can be more efficient than the ones known in the literature.

References

[1] S. Goldwasser, S. Micali, and C. Rackoff. 1985. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85)*. ACM, New York, NY, USA, 291-304. DOI: https://doi.org/10.1145/22145.22178

[2] O. Goldreich, S. Micali, and A. Wigderson. 1991. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM* 38, 3 (July 1991), 690-728. DOI: https://doi.org/10.1145/116825.116852

[3] G. Brassard and C. Crepeau, Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond, *27th Annual Symposium on Foundations of Computer Science* (sfcs 1986), Toronto, ON, Canada, 1986, pp. 188-195. doi: 10.1109/SFCS.1986.33

[4] J. Watrous. 2006. Zero-knowledge against quantum attacks. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing (STOC '06)*. ACM, New York, NY, USA, 296-305. DOI: https://doi.org/10.1145/1132516.1132560

Recursion with pointers in implicit complexity

Isabel Oitavem
FCT- Universidade NOVA de Lisboa (Portugal)

In this talk we give an overview of the area, with focus on polynomial time and polynomial space complexity classes.

Depending on the time, we speak also about the role of pointers in approaching probabilistic classes of complexity.

Decidability of several concepts of finiteness for simple types

José Espírito Santo[1], Luís Pinto[1], Ralph Matthes[2]
(1) Centro de Matemática, University of Minho (Portugal),
(2) Institut de Recherche en Informatique de Toulouse (IRIT) & CNRS and University of Toulouse (France)

If we consider as "member" of a simple type the outcome of any successful (possibly infinite) run of bottom-up proof search that starts from the type, then several concepts of "finiteness" for simple types are possible: (i) the finiteness of the search space, (ii) the finiteness of any member, or (iii) the finiteness of the number of finite members (in other words, the inhabitants). These three concepts can be formalized through a coinductive lambda-calculus for proof search and its finitary counterpart.

In this talk we will overview the coinductive approach to proof search introduced by the authors, and recall the two mentioned lambda-calculi. Then, we will see that the three concepts of finiteness for simple types are instances of the same parameterized notion of finiteness, and that a single, parameterized proof shows the decidability of all of them. One instance of this result means that termination of proof search is decidable. A separate result is that emptiness is also decidable (where emptiness is absence of "members" as above, not just absence of inhabitants). This fact is an ingredient of the main decidability result, but it also has a different application, the definition of the pruned search space - the one where branches leading to failure are chopped off. We will conclude with our version of König's lemma for simple types: a simple type has an infinite member exactly when the pruned search space is infinite.

References

[1] J. Espírito Santo, R. Matthes, L. Pinto, Inhabitation in simply typed lambda-calculus through a lambda-calculus for proof search, *Mathematical Structures in Computer Science* 29(8), pp. 1092–1124 (2019)
[2] J. Espírito Santo, R. Matthes, L. Pinto, Decidability of several concepts of finiteness for simple types, *Fundamenta Informaticae* 170(1-3), pp. 111–138 (2019)

Proof mining of a discussion by cases

Pedro Pinto
Technische Universität Darmstadt (Germany) & CMAFcIO

This talk is part of the ongoing program of applying the bounded functional interpretation [3] to concrete cases of proof mining, which in [2,4] prove to be a valid alternative to the usual proof-theoretical technique used by U. Kohlenbach and his collaborators, the monotone functional interpretation.

We will look at a quantitative analysis of a theorem by F. Wang and H. Cui [5, Theorem 1] whose proof follows a discussion by cases (j.w.w. Bruno Dinis, [1]). The original theorem is a strong convergence result of a generalization of the well-known proximal point algorithm, and in its quantitative final version a metastability result (in the sense of T. Tao) was obtained. I will explain the theoretical justification behind the analysis and its most relevant details.

References

[1] B. Dinis, P. Pinto, Quantitative results on the multi-parameters Proximal Point Algorithm, *submitted*
[2] F. Ferreira, L. Leuştean, P. Pinto, On the removal of weak compactness arguments in proof mining, *Advances in Mathematics* 354, 106728 (2019)
[3] F. Ferreira, P. Oliva, Bounded functional interpretation, *Annals of Pure and Applied Logic* 135(1-3), pp. 73–112 (2005)
[4] P. Pinto, Proof mining with the bounded functional interpretation, PhD Thesis, Universidade de Lisboa (2019)
[5] F. Wang, H. Cui, On the contraction-proximal point algorithms with multi-parameters, *Journal of Global Optimization* **54**(3), pp. 485–491 (2012)

Time-stamped claim logic

João Rasga[1], Cristina Sernadas[1], Erisa Karafili[2], Luca Viganò[3]
(1) Departamento de Matemática, Instituto Superior Técnico and CMAFcIO, ULisboa (Portugal),
(2) Department of Computing, Imperial College London, UK
Department of Informatics, King's College London, UK

In this talk we present the Time-Stamped Claim Logic, proposed in [1], for reasoning about distributed time-stamped claims. Such a logic is interesting for theoretical reasons, i.e., as a logic *per se*, but also because it has a number of practical applications, in particular when one needs to reason about a huge amount of pieces of evidence collected from different sources, where some of the pieces of evidence may be contradictory and some sources are considered to be more trustworthy than others. In order to show how the Time-Stamped Claim Logic can be used in practice, we consider a concrete cyber-attribution case study. We present a sound and complete sequent calculus for the logic and analyse some properties and meta-properties of the logic.

Acknowledgments João Rasga and Cristina Sernadas deeply acknowledge the National Funding from FCT (Fundação para a Ciência e a Tecnologia) under the project UID/MAT/04561/2019 granted to CMAFcIO (Centro de Matemática, Aplicações Fundamentais e Investigação Operacional) of Universidade de Lisboa. Erisa Karafili was supported by the European Union's H2020 research and innovation programme under the Marie Curie grant agreement No. 746667.

References

[1] J. Rasga, C. Sernadas, E. Karafili, and L. Viganò, Time-stamped claim logic. Preprint, CMAFcIO and DM, IST - U Lisboa, 1049-001 Lisboa, Portugal, 2019. Submitted for publication.

Expressing consistency consistently

Lucas Rosenblatt
University of Buenos Aires (Argentina)

In the last five decades or so paraconsistent logics have been thoroughly studied. On the one hand, there is the dialetheic tradition, created, developed and staunchly defended over the years by Graham Priest. Priest and other dialetheists claim that some statements are both true and false, and have long argued that paraconsistent logics are attractive to model various philosophically important notions. On the other hand, there is the Brazilian tradition of so-called 'logics of formal inconsistency'. Following Newton da Costa's lead, members of this tradition have focused on the possibility of using paraconsistent logics that incorporate consistency operators.

Unfortunately, there hasn't been much interaction between these traditions. The reason is not only sociological. One of the main applications of dialetheism is to the semantic paradoxes. Dialetheists contend that paradoxical statements are prototypical cases of dialetheias (i.e., statements that are both true and false). Now, it is well-known that the naive truth predicate does not mesh well with a consistency operator. Roughly, if the language is expressively rich enough and the notion of truth satisfies some plausible conditions, then a classical consistency operator cannot be introduced, on pain of triviality.

Recently, this diagnosis has been challenged by a number of theorists. One of these theorists is Priest himself. In his recent paper [2] he suggests that if one expresses Tarski's schema (i.e., the claim that for any statement ϕ, 'ϕ' is true if and only if ϕ) with a non-classical material biconditional—as opposed to a non-classical intensional biconditional—then one is in a position to express consistency, and one can do so in a consistent way. The biconditional in question won't satisfy modus ponens, and thus typical paradoxes won't cause any trouble because one will not be able to detach from the crucial instances of Tarski's schema.

Priest is not alone in thinking that there are ways of making naive truth compatible with expressing consistency consistently. Eduardo Barrio, Federico Pailos and Damián Szmuc (henceforth, BPS) have argued in [1] that it is possible to combine naive truth with consistency; in fact, in their account it is not only the unrestricted Tarski schema that holds, but the stronger property of transparency holds too. In

order to maintain transparency they substantially weaken the underlying syntax theory by employing, in their words, a 'weak self-referential procedure'. Simply put, self-reference is achieved only via material biconditionals, not via identities.

In this talk I will do three things. First, I will offer various arguments against these two proposals. Second, I will try to draw some lessons from their failures. And third, I will briefly sketch an alternative paraconsistent framework where the notion of consistency is allowed to behave inconsistently in certain circumstances.

References

[1] E. Barrio, F. Pailos and D. Szmuc, *Logic Journal of the IGPL* 25(4): 387–401, 2017

[2] G. Priest, What If? The Exploration of an Idea, *Australasian Journal of Logic* 14(1):54–127, 2017

Quantitative inconsistent feasibility for averaged mappings

Andrei Sipoş

Technische Universität Darmstadt (Germany) & Institute of Mathematics of the Romanian Academy (Romania)

Bauschke and Moursi have recently [1] obtained results that implicitly contain the fact that the composition of finitely many averaged mappings on a Hilbert space that have approximate fixed points also has approximate fixed points and thus is asymptotically regular. This followed a long series of papers of Bauschke and his collaborators, where asymptotic regularity was first proven for the compositions of projections onto closed, convex, nonempty sets (a problem known as the 'zero displacement conjecture'), then for compositions of general firmly nonexpansive mappings, and then the result started to be extended to mappings having nonzero minimal displacement.

This ties into the area of proof mining [2], an applied subfield of mathematical logic that concerns itself with finding additional (for example, quantitative) information in concrete mathematical proofs by analyzing them using tools of proof theory. As it may be seen e.g. in the recent survey of Kohlenbach [4], proof mining has been highly successful in the last two decades at extracting rates of asymptotic regularity for widely used iterations of nonlinear analysis. A few years ago, Kohlenbach has analyzed the older results mentioned above, extracted bounds for the approximate fixed points and by combining them with his previous results on strongly nonexpansive mappings, obtained rates of asymptotic regularity [3].

What we do is to update these techniques in order to analyze [1] and give a corresponding rate of asymptotic regularity. In order to do that, we need to give a quantitative version of the crucial fact used in their proof that cocoercive operators are rectangular. That is in turn used to get upper bounds on approximate fixed points of the composition of two, and then of finitely many, averaged mappings. Again by using quantitative results, both old and new, on strongly nonexpansive mappings, we obtain the desired rate.

References

[1] H. Bauschke, W. Moursi, On the minimal displacement vector of compositions and convex combinations of nonexpansive mappings. arXiv:1809.01196 [math.FA], 2018
[2] U. Kohlenbach, *Applied proof theory: Proof interpretations and their use in mathematics*. Springer Monographs in Mathematics, Springer, 2008
[3] U. Kohlenbach, A polynomial rate of asymptotic regularity for compositions of projections in Hilbert space. *Foundations of Computational Mathematics* 19, no. 1, 83–99, 2019
[4] U. Kohlenbach, Proof-theoretic methods in nonlinear analysis. In: B. Sirakov, P. Ney de Souza, M. Viana (eds.), *Proceedings of the International Congress of Mathematicians 2018 (ICM 2018)*, Vol. 2 (pp. 61–82). World Scientific, 2019.

Author Index