10$^{\text{TH}}$ INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2021

September 20 - 24, 2021
Dubrovnik, Croatia

held as a hybrid meeting

Book of Abstracts

Course directors:

- Zvonimir Šikić, University of Zagreb
- Andre Scedrov, University of Pennsylvania
- Silvia Ghilezan, University of Novi Sad
- Zoran Ognjanović, Mathematical Institute of SASA, Belgrade
- Thomas Studer, University of Bern

Book of Abstracts of the 10$^{\text{th}}$ International Conference on Logic and Applications - LAP 2021, held as a hybrid meeting hosted by the Inter University Center Dubrovnik, Croatia, September 20 - 24, 2021.

LaTeX book of abstracts preparation and typesetting:

- Dušan Gajić, University of Novi Sad
- Simona Kašterović, University of Novi Sad

LAP 2021 Web site: `http://imft.ftn.uns.ac.rs/math/cms/LAP2021`
Maintained by Nenad Savić, University of Bern, and Simona Kašterović, University of Novi Sad.

Contents

1 *Tin Adlešić, Vedran Čačić*
Formal approach to stratification in NF/NFU **5**

2 *Musab A. AlTurki, Tajana Ban Kirigin, Max Kanovich, Vivek Nigam, Andre Scedrov, Carolyn Talcott*
Periodic Systems: Safety, Security, and Complexity **7**

3 *Matthias Baaz*
Analytic calculi for quantifier macros **9**

4 *Michael Batanin, Martin Markl, Jovana Obradović*
Minimal models for graphs-related operadic algebras **10**

5 *Vedran Čačić*
$\lambda\mathbf{sz}.\mathbf{s}(\mathbf{s}(\mathbf{sz}))$ topics **13**

6 *Vedran Čačić, Marko Horvat, Zvonko Iljazović*
Computable subcontinua of semicomputable chainable Hausdorff continua **14**

7 *Cezary Cieśliński*
On the principle of disjunctive correctness **16**

8 *Šejla Dautović, Dragan Doder, Zoran Ognjanović*
Logics for Reasoning about Knowledge and Conditional Probability **19**

9 *Giulio Fellin, Sara Negri, Eugenio Orlandelli*
Glivenko classes and constructive cut elimination in infinitary logic **22**

10 *Michał J. Gajda*
Consistent finitist logic **25**

11 *Silvia Ghilezan, Simona Kašterović, Luigi Liquori, Bojan Marinković, Zoran Ognjanović, Tamara Stefanović*
Federating Digital Contact Tracing using Structured Overlay Networks **28**

12 *Sebastijan Horvat, Tin Perkov, Mladen Vuković*
n-bisimulations for generalised Veltman semantics **31**

13 *Angelina Ilić Stepić, Zoran Ognjanović, Aleksandar Perović*
A Probabilistic Temporal Epistemic Logic **33**

14 *Simona Kašterović, Silvia Ghilezan*
Towards Logic of Combinatory Logic **34**

15 *Matej Mihelčić*
Redescription mining **37**

16 *Petar Paradžik, Ante Ðerek*
Restricted Observational Equivalence **39**

17 *Duško Pavlović*
Solution of Lambek's Problem: A construction of Dedekind-MacNeille-type bicompletions of categories **41**

18 *Edi Pavlović, Norbert Gratzl*
Proof theory of free logics **42**

19 *Jiří Raclavský, Petr Kuchyňka*
Natural Deduction for Partial Type Theory with 'Evaluation Terms' **44**

20 *Andre Scedrov*
Language Models and Relational Models of the Lambek Calculus **47**

21 *Peter Schuster, Daniel Wessel*
Radical theory of Scott-open predicates **48**

22 *Zvonimir Šikić*
Kneale's natural deductions as a notational variant of Beth's tableaus **51**

23 *Tamara Stefanović, Silvia Ghilezan*
Differential Privacy and Applications **52**

24 *Matteo Tesi*
A new termination procedure for intuitionistic logic **55**

25 *Zvonko Iljazović, Lucija Validžić*
Computable sequences and isometries **58**

26 *Tin Perkov*
4th workshop Formal Reasoning and Semantics (FORMALS 2021) **61**

27 *Tin Adlešić*
Quine's New foundations and paradoxes **62**

28 *Tajana Ban Kirigin, Sanda Bujačić Babić, Benedikt Perak*
Sentiment Potential Analysis **64**

29 *Tajana Ban Kirigin, Sanda Bujačić Babić, Benedikt Perak*
Building a Sentiment Dictionary for Croatian **67**

30 *Tajana Ban Kirigin, Sanda Bujačić Babić, Benedikt Perak*
Implementing Sentiment Dictionary into Vader sentiment analyis for Croatian **69**

31 *Ludovica Conti*
Abstraction's Logicality and Invariance **72**

32 *Aleksandar Hatzivelkos, Marcel Maretić*
A Note about Disapproval Voting **76**

33 *Sebastijan Horvat*
Bisimulation games for (generalized) Veltman semantics **79**

34 *Luka Mikec, Joost J. Joosten, Albert Visser, Mladen Vuković*
On proving interpretability principles arithmetically sound **81**

35 *Vivek Nigam*
Soft-Agents: A Symbolic Verification Framework for Cyber-Physical Systems **83**

36 *Yaroslav Petrukhin*
Normalisation for some infectious logics with non-standard disjunction elimination rules **84**

37 *Jiří Raclavský*
The Rule of Existential Generalisation, Its Derivability and Formal Semantics **87**

38 *David Lehnherr, Zoran Ognjanović, Thomas Studer*
A Logic of Interactive Proofs **90**

Formal approach to stratification in NF/NFU

Tin Adlešić [1], **Vedran Čačić**[2]

[1]*Faculty of Teacher Education, University of Zagreb*
Savska cesta 77, Zagreb
[2]*Department of Mathematics, University of Zagreb*
Bijenička cesta 30, Zagreb
E-mail: [1]tin.adlesic@ufzg.hr, [2]veky@math.hr

Keywords:
Quine's New Foundations, stratification, stratified formulas

New foundations for mathematical logic (sometimes called Quine's New Foundations and often abbreviated by NF) was introduced in order to eliminate some of the annoying consequences of Russell–Whitehead's type theory, most notably, the one that some classes appear in every type.

NF solves this problem by introducing the notion of stratification and stratified formulas, while retaining all positive aspects of *Principia* like the possibility of developing the arithmetic and forbidding paradoxes. In a way, NF is simple type theory in disguise.

We formally define stratification and prove some intuitive claims about it. Because the notion of stratification is concerned only with variables, in order to simplify further theory development, we extend its notion to encompass abstraction terms. This extension enable us to check whether some complex formula is stratified without rewriting it in the basic language. For every additional term we give a rule what type can be assigned to it, and in what circumstances. We will provide few examples in order to demonstrate the benefits of our formalization.

By formalizing the stratification in full, NF becomes easier to read and comprehend and its exposition becomes more clear.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation (HRZZ) under the project UIP-2017-05-9219.

References

[1] Holmes, M. Randall. Elementary set theory with a universal set. Vol. 10. Bruylant-Academia, 1998.

[2] Forster, Thomas E. ”Set theory with a universal set. Exploring an untyped universe.” Studia Logica 53.4 (1994).

[3] Jensen, Ronald Björn. ”On the consistency of a slight (?) modification of Quine’s New Foundations.” Words and objections. Springer, Dordrecht, 1969. 278-291.

[4] Quine, Willard V. ”New foundations for mathematical logic.” The American mathematical monthly 44.2 (1937): 70-80.

[5] Beeson, Michael. ”Intuitionistic NF Set Theory.” arXiv preprint arXiv:2104.00506 (2021).

[6] Whitehead, Alfred N, and Bertrand Russell. Principia Mathematica. Cambridge [England: The University Press, 1925. Print.

Periodic Systems: Safety, Security, and Complexity

Musab A. AlTurki[1,2],Tajana Ban Kirigin[3], Max Kanovich[4,5], Vivek Nigam[1,7], Andre Scedrov[8], Carolyn Talcott[9]

[1] *King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia*

[2] *Runtime Verification Inc., USA*

[3] *University of Rijeka, Department of Mathematics, Rijeka, Croatia*

[4] *University College London, London, UK*

[5] *National Research University Higher School of Economics, Moscow, Russia*

[6] *Federal University of Paraíba, João Pessoa, Brazil*

[7] *Munich Research Center, Huawei, Munich, Germany*

[8] *University of Pennsylvania, Philadelphia, PA, USA*

[9] *SRI International, Menlo Park, CA, USA*

Keywords:

Formal Methods, Verification, Security, Multiset Rewriting, Industry 4.0, Complexity

Development of automated technological systems has seen the increase in interconnectivity among its components. This includes Internet of Things (IoT) and Industry 4.0 (I4.0) and the underlying communication between sensors and controllers. The combination of flexible interconnectivity and insecure devices also presents opportunities for cyber-attacks. In an industrial setting such attacks lead to serious material or human damage.

This paper is a step toward a formal framework for specifying such systems and analyzing underlying properties including safety and security. Our formal framework is based on multiset rewriting [2]. We introduce *Automata Systems* (AS) motivated by I4.0 applications. We identify various subclasses of AS that reflect different types of requirements on I4.0. For example, *Periodic Automata Systems* (PAS) refine AS by incorporating the assumption that an I4.0 application carries out a collection of tasks by execution of its components periodically.

We investigate the complexity of the problem of *Functional Correctness* of these systems, that is, deciding whether a system does not lead to a critical configuration that may lead to human or financial losses. We also investigate the complexity of the *Security Problem for Functionally Correct Systems* which considers vulnerability of these systems to attacks. We model the presence of various levels of threats to the system by proposing a range of intruder models, based on the number of actions intruders can use [1].

The proposed formal models, verification problems, and complexity results support the automated security verification of I4.0 applications. We demonstrate this by carrying out a number of experiments based on the formalization in the rewriting logic symbolic tool Maude described in [3].

Acknowledgments

Ban Kirigin is supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219. The work of Max Kanovich was partially supported by EPSRC Programme Grant EP/R006865/1: “Interface Reasoning for Interacting Systems (IRIS).” Nigam is partially supported by NRL grant N0017317-1-G002, and CNPq grant 303909/2018-8. Scedrov was partially supported by the U. S. Office of Naval Research under award numbers N00014-20-1-2635 and N00014-18-1-2618. Talcott was partially supported by the U. S. Office of Naval Research under award numbers N00014-15-1-2202 and N00014-20-1-2644, and NRL grant N0017317-1-G002. Nigam has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 830892.

References

[1] Musab A. Alturki, Tajana Ban Kirigin, Max Kanovich, Vivek Nigam, Andre Scedrov, Carolyn Talcott. On Security Analysis of Periodic Systems: Expressiveness and Complexity. In P. Mori et al., eds., ICISSP 2021 Proceedings of the 7th International Conference on Information Systems Security and Privacy, SCITEPRESS, pp.43-54, 2021.

[2] M. Kanovich, T. Ban Kirigin, V. Nigam, and A. Scedrov. Bounded memory Dolev-Yao adversaries in collaborative systems. *Inf. Comput.*, 238:233–261, 2014.

[3] Vivek Nigam, and Carolyn Talcott. Formal security verification of industry 4.0 applications. In *24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Special Track on Cybersecurity in Industrial Control Systems.* pp.1043-1050). 2019.

[4] Vivek Nigam, and Carolyn Talcott. Automated construction of security integrity wrappers for industry 4.0 applications. In *International Workshop on Rewriting Logic and its Applications (WRLA).* Springer, Cham, pp.197-215, 2020.

Analytic calculi for quantifier macros

Matthias Baaz

Vienna University of Technology
[1]baaz@logic.at

In this lecture we discuss the addition of quantifier macros to cut-free LK derivations. It is demonstrated that such extensions depend on a liberalization of the usual eigenvariable conditions of LK. The resulting calculi (LK+ and LK++) admit sometimes non-elementarily shorter cut-free proofs. As application we sketch the construction of partial cut-free calculi for Henkin quantifiers. In addition, we show, that LK cut-free corresponds to standard Skolemization whereas LK+ cut-free corresponds to Andrew's Skolemization resulting in a potential non-elementary speed-up of resolution proofs.

Minimal models for graphs-related operadic algebras

Michael Batanin[1], Martin Markl[2] and Jovana Obradović[3]

[1,2] *Czech Academy of Sciences, Institute of Mathematics*
Žitná 25, 115 67 Prague 1, Czech Republic
[3] *Mathematical Institute of the Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade, Serbia
E-mail: [1]`bataninmichael@gmail.com`, [2]`markl@math.cas.cz`, [3]`jovana@mi.sanu.ac.rs`

Keywords:
operad, minimal model, operadic category, convex polytope

The fundamental feature of Batanin-Markl's theory of operadic categories [1] is that the objects under study are viewed as algebras over (generalized) operads in a specific operadic category. Thus, for instance, ordinary operads arise as algebras over the terminal operad $1_{\mathtt{RTr}}$ in the operadic category $\mathtt{RTr}$ of rooted trees, modular operads are algebras over the terminal operad $1_{\mathtt{ggGrc}}$ in the operadic category $\mathtt{ggGrc}$ of genus-graded connected graphs, &c. Our aim is to construct explicit minimal models for the (hyper)operads governing modular, cyclic and ordinary operads, and wheeled properads. According to general philosophy [5], algebras for these models describe strongly homotopy versions of the corresponding objects whose salient feature is the transfer property over weak homotopy equivalences. This might be compared to the following classical situation.

Associative algebras are algebras over the non-Σ operad Ass. Algebras over the minimal model of Ass are Stasheff's strongly homotopy associative algebras, also called A_∞-algebras. This situation fits well into the framework of the current work, since Ass is the terminal non-Σ operad or, which is the same, the terminal operad in the operadic category of finite ordered sets and their order-preserving epimorphisms.

We begin with the particular case of the operadic category $\mathtt{Grc}$ of connected graphs. Algebras for the terminal operad $1_{\mathtt{Grc}}$ in that category are modular operads without the genus grading. We explicitly define a minimal $\mathtt{Grc}$-operad $\mathfrak{M}_{\mathtt{Grc}} = (\mathbb{F}(D), \partial)$ and a map $\mathfrak{M}_{\mathtt{Grc}} \xrightarrow{\rho} 1_{\mathtt{Grc}}$ of differential graded $\mathtt{Grc}$-operads. Our main theorem states that ρ is a level-wise homological isomorphism, meaning that $\mathfrak{M}_{\mathtt{Grc}}$ is a minimal model of $1_{\mathtt{Grc}}$. The proof of that theorem is a combination of the following facts.

On one hand, using the apparatus developed in [3], we describe the piece $\mathbb{F}(D)(\Gamma)$, $\Gamma \in \mathtt{Grc}$, of the free operad $\mathbb{F}(D)$ as a colimit over the poset $\mathtt{gTr}(\Gamma)$ of graph-trees associated to Γ, which are abstract trees whose vertices are decorated by graphs from $\mathtt{Grc}$ and which fulfill suitable compatibility conditions involving Γ.

On the other hand, to each $\Gamma \in \mathtt{Grc}$ we associate a hypergraph $\mathbf{H}_\Gamma$ and to that hypergraph a poset $\mathcal{A}(\mathbf{H}_\Gamma)$ of its constructs, which are certain abstract trees with vertices decorated by subsets of the set of internal edges of Γ. We prove that the poset $\mathtt{gTr}(\Gamma)$ is order-isomorphic to the poset $\mathcal{A}(\mathbf{H}_\Gamma)$. The results of [4] assert that $\mathcal{A}(\mathbf{H}_\Gamma)$ is in turn order-isomorphic to the face lattice of a convex polytope $\mathcal{G}(\mathbf{H}_\Gamma)$, obtained by truncating the vertices, edges and other faces of simplices, in any finite dimension.

We prove that the polytope $\mathcal{G}(\mathbf{H}_\Gamma)$ satisfies the following 'diamond' condition.

Diamond. If a is a $(k-1)$-dimensional face of $\mathcal{G}(\mathbf{H})$ such that $a \lessdot e', e''$, then there exists a $(k+1)$-dimensional face h of $\mathcal{G}(\mathbf{H})$ such that $e', e'' \lessdot h$.

A concise way to formulate the diamond condition is to say that the existence of e' and e'' with $a \prec e', e''$ implies the existence of some h with $e', e'' \prec h$, diagrammatically

$$\begin{tikzcd}
& h & \\
e' \arrow[ur, hook, dashed] & & e'' \arrow[ul, hook', dashed] \\
& a \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

hence the name. It follows from the properties of abstract polytopes that e' and e'' are the only faces in the interval $[a, h]$, but the diamond condition need not be satisfied in a general polytope.

Finally, by using the diamond property of $\mathcal{G}(\mathbf{H}_\Gamma)$, we prove an 'ingenious' lemma, stating that the faces of $\mathcal{G}(\mathbf{H}_\Gamma)$ can be oriented so that the cellular chain complex of $\mathcal{G}(\mathbf{H}_\Gamma)$ is isomorphic, as a differential graded vector space, to $(\mathbb{F}(D)(\Gamma), \partial)$. Since $\mathcal{G}(\mathbf{H}_\Gamma)$ is acyclic in positive dimension, the same must be true for $(\mathbb{F}(D)(\Gamma), \partial)$. It remains to show that ρ induces an isomorphism of degree 0 homology, but this is simple. The conclusion is that $\mathfrak{M}_{\mathtt{Grc}}$ is indeed a minimal model of $\mathtt{1}_{\mathtt{Grc}}$.

In constructing the minimal models $\mathfrak{M}_{\mathtt{ggGrc}}$, $\mathfrak{M}_{\mathtt{Tr}}$ and $\mathfrak{M}_{\mathtt{Whe}}$ of the terminal operads $\mathtt{1}_{\mathtt{ggGrc}}$, $\mathtt{1}_{\mathtt{Tr}}$ and $\mathtt{1}_{\mathtt{Whe}}$ in the operadic categories $\mathtt{ggGrc}$ of genus-graded connected graphs, $\mathtt{Tr}$ of trees and $\mathtt{Whe}$ of ordered ('wheeled') connected graphs, respectively, we use the fact observed in [2, Section 4] that these categories are discrete operadic opfibrations over $\mathtt{Grc}$. We prove that the restrictions along discrete operadic opfibrations preserve minimal models of terminal operads, which then delivers $\mathfrak{M}_{\mathtt{ggGrc}}$, $\mathfrak{M}_{\mathtt{Tr}}$ and $\mathfrak{M}_{\mathtt{Whe}}$ as the restrictions of the minimal model for $\mathtt{1}_{\mathtt{Grc}}$ along the corresponding opfibration map.

The situation of the terminal operad $\mathtt{1}_{\mathtt{RTr}}$ in the operadic category $\mathtt{RTr}$ of rooted trees is different, since this category is not an opfibration over $\mathtt{Grc}$. It is, however, a discrete operadic fibration with finite fibers, which provides another setting in which the transfer of minimal models of terminal operads works.

In a follow-up to this work we prove that the minimal models described here are the bar constructions over Koszul duals of the (hyper)operads that they resolve, in the sense of [3], which by definition means that those (hyper)operads are Koszul.

Acknowledgment

The authors acknowledge the financial support of Praemium Academiae of M. Markl.

References

[1] M.A. Batanin and M. Markl. Operadic categories and duoidal Deligne's conjecture. *Adv. Math.* 285 (2015) 1630–1687.

[2] M.A. Batanin and M. Markl. Operadic categories as a natural environment for Koszul duality. Preprint. (2021) arXiv:1812.02935

[3] M.A. Batanin and M. Markl. Koszul duality for operadic categories, Preprint. (2021) arXiv:2105.05198

[4] P.-L. Curien, J. Ivanović and J. Obradović. Syntactic aspects of hypergraph polytopes. *J. Homotopy Relat. Struct.* 14 (2019) 235–279.

[5] M. Markl. Homotopy algebras are homotopy algebras. *Forum Matematicum.* 16 (2004) 129 – 160.

λsz.s(s(sz)) topics

Vedran Čačić[1]

[1] *PMF–MO, University of Zagreb*
Bijenička cesta 30
E-mail: [1]`veky@math.hr`

Keywords:
Iterated induction, converses of geometry theorems, relational and functional presentation of structures, fragments of propositional logic

At the beginning of May, prof. Šikić gave a lecture at Seminar for Mathematical Logic and Foundations of Mathematics [1], where he presented three topics that at first glance had nothing in common. However, all of them could be formalized relatively easily in Coq, and in the process many interesting insights were obtained. I intend to present some of them.

Acknowledgment

Thanks to prof. Šikić for making me think long and hard about trivial things.

References

[1] Šikić, Z., *O ekvivalenciji, dokazima obrata i neiterabilnosti indukcije*, SLOM, 2021., `https://meduza.carnet.hr/index.php/media/watch/20739`

Computable subcontinua of semicomputable chainable Hausdorff continua

Vedran Čačić[1], Marko Horvat[2], Zvonko Iljazović[3]

[1–3]*Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, 10 000 Zagreb
E-mail: [1]veky@math.hr, [2]mhorvat@math.hr, [3]zilj@math.hr

Keywords:
computable topological space, computable set, semicomputable set, chainable continuum, decomposable continuum.

In the setting of computable topological spaces, we consider semicomputable, chainable Hausdorff continua. If such a continuum S is decomposable, it can be computably approximated; more precisely, for every open cover $\mathcal{U}$, there exist two computable points and a computable subcontinuum $\hat{S}$ that is chainable from one point to the other and is $\mathcal{U}$-close to S.

Our first step in proving the main result is by considering a more concrete decomposition:

Theorem 1 *Let $\big(X, \mathcal{T}, (I_i)\big)$ be a computable topological space and $S \subseteq X$ a semicomputable, chainable Hausdorff continuum. Let K_1 and K_2 be subcontinua of S such that $S = K_1 \cup K_2$. Finally, let $a \in K_1 \setminus K_2$, $b \in K_2 \setminus K_1$ and $\alpha, \beta \in \mathbb{N}$ such that $a \in I_\alpha$ and $b \in I_\beta$. Then there exist computable points $\hat{a}, \hat{b} \in S$ and a computable subcontinuum $\hat{S}$ of S such that $\hat{a} \in I_\alpha$, $\hat{b} \in I_\beta$ and $\hat{S}$ is chainable from $\hat{a}$ to $\hat{b}$.*

As an aside, this theorem has a nice corollary, so we mention it here and in the manuscript under submission:

Corollary 2 *Let $\big(X, \mathcal{T}, (I_i)\big)$ be a computable topological space and let S be a semicomputable set in this space which is, as a subspace of $(X, \mathcal{T})$, an arc. Then for all $\alpha, \beta \in \mathbb{N}$ such that I_α and I_β intersect S there exist distinct computable points $a \in I_\alpha \cap S$ and $b \in I_\beta \cap S$ such that the subarc of S determined by a and b is a computable set in $\big(X, \mathcal{T}, (I_i)\big)$.*

Subsequently, we lift the concrete decomposition requirement and obtain the desired result:

Theorem 3 *Let $\big(X, \mathcal{T}, (I_i)\big)$ be a computable topological space and $S \subseteq X$ a decomposable, semicomputable, chainable Hausdorff continuum. Then for every open cover $\mathcal{U}$ of $(X, \mathcal{T})$, there exist computable points $\hat{a}, \hat{b} \in S$ and a computable subcontinuum $\hat{S}$ of S such that $\hat{S}$ is chainable from $\hat{a}$ to $\hat{b}$ and $S \approx_{\mathcal{U}} \hat{S}$.*

Acknowledgment

This work was fully supported by the Croatian Science Foundation
under the project #7459 CompStruct.

References

[1] K. Weirauch, T. Grubba, *Elementary computable topology*, Journal of Universal Computer Science 15 (2009) 1381–1422

[2] V. Brattka, G. Presser, *Computability on subsets of metric spaces*, Theoretical Computer Science 305 (2003) 43–76

[3] M. Pour-El, J. Richards, *Computability in Analysis and Physics*, Springer, Berlin, 1989

[4] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. 42 (1936) 230–265

On the principle of disjunctive correctness

Cezary Cieśliński

Faculty of Philosophy, University of Warsaw
Warsaw, Poland
E-mail: c.cieslinski@uw.edu.pl

Keywords:
Truth, conservativity.

The area of axiomatic truth theories analyses the notion of truth by investigating axiomatic theories formalizing this notion (see [1] and [3]). We choose a base theory strong enough to represent syntax. In our case, this will be Peano Arithmetic, PA. Let $\mathscr{L}_{\mathrm{PA}}$ be the arithmetical language, let $Sent_{\mathrm{PA}}(x)$ read "x is an arithmetical sentence" and let Tm^c be the set of closed arithmetical terms. We extend $\mathscr{L}_{\mathrm{PA}}$ with the new predicate $T(x)$ whose intended reading is "x is (a code of) a true arithmetical sentence"; let L_T be $\mathscr{L}_{\mathrm{PA}}$ extended with '$T(x)$'. We now add to PA the following compositional axioms governing the behaviour of the truth predicate:

- $\forall s, t \in Tm^c\big(T(t = s) \equiv val(t) = val(s)\big)$
- $\forall \varphi\big(Sent_{\mathrm{PA}}(\varphi) \to (T\neg\varphi \equiv \neg T\varphi)\big)$
- $\forall \varphi \forall \psi\big(Sent_{\mathrm{PA}}(\varphi \vee \psi) \to (T(\varphi \vee \psi) \equiv (T\varphi \vee T\psi))\big)$
- $\forall v \forall \varphi(x)\big(Sent_{\mathrm{PA}}(\forall v \varphi(v)) \to (T(\forall v \varphi(v)) \equiv \forall x T(\varphi(\dot{x})))\big)$

In this way the truth theory CT^- is obtained. Note that in CT^- we have arithmetical induction only (no induction for formulas with the truth predicate). It is known that CT^- is a conservative extension of PA (see [4]).

We introduce the following notational conventions:

- Let $(\varphi_0 \ldots \varphi_n)$ be a (coded) sequence of formulas. The expression $\bigvee\limits_{i \leq n} \varphi_i$ denotes the disjunction $\varphi_n \vee (\varphi_{n-1} \vee (\varphi_{n-2} \vee (\ldots \varphi_0) \ldots))$. This ordering and this way of bracketing is always assumed here. In effect, $\bigvee\limits_{i \leq n} \varphi_i$ is always $\varphi_n \vee \bigvee\limits_{i \leq n-1} \varphi_i$.

- CT_0 is CT^- with Δ_0 induction for formulas of L_T.

It is known (see [5]) that :

Theorem 1 CT_0 *is not conservative over* PA.

Disjunctive correctness principles are defined in the following way.

Definition 2

- DC *is the sentence:* $\forall(\varphi_0 \dots \varphi_n)[T(\bigvee\limits_{i\leq n} \varphi_i) \equiv \exists k \leq n T(\varphi_k)]$.
- DC-elim *is the sentence:* $\forall(\varphi_0 \dots \varphi_n)[T(\bigvee\limits_{i\leq n} \varphi_i) \rightarrow \exists k \leq n T(\varphi_k)]$.
- DC-intro *is the sentence:* $\forall(\varphi_0 \dots \varphi_n)[\exists k \leq n T(\varphi_k)] \rightarrow T(\bigvee\limits_{i\leq n} \varphi_i)]$.

How strong is DC? The following theorem by Enayat and Pakhomov [2] provides the answer.

Theorem 3 CT^- + DC *is the same theory as* CT_0*, hence it is not conservative over* PA.

It is a striking result, because DC appears to be a mild, natural extension of the compositional axiom for disjunction and yet turns out to carry a full strength of Δ_0-induction.

Ali Enayat had asked whether DC-intro and DC-elim, taken separately, are conservative over Peano Arithmetic (the proof from [2] did not decide the issue). Answering this question, we demonstrate that already DC-elim, when added to CT^-, produces a non-conservative extension. This follows from the fact that DC-intro is provable from DC-elim over CT^-.

Theorem 4 CT^- + DC-elim $\vdash$ DC-intro.

The reasoning employed in the proof is reminiscent of Yablo's paradox (which runs as follows: Consider a sequence of sentences $\varphi_0, \varphi_1 \dots$ such that each φ_n states 'there is a number $k > n$ such that φ_k is false'. Then a simple argument produces a contradiction.)

Proof outline. Working in CT^- + DC-elim, let $\theta_0 \dots \theta_n$ be a sequence of sentences. Fix $m \leq n$ such that $T(\theta_m)$. We claim that $T(\bigvee\limits_{i\leq n} \theta_i)$. We define:

- $\psi_k := \bigvee\limits_{i\leq m+k} \theta_i$.

In effect, ψ_k is $\theta_{m+k} \vee \underbrace{\Big(\theta_{m+k-1} \vee \big(\theta_{m+k-2} \vee \dots \vee \theta_0\big)\Big)}_{\psi_{k-1}}$.

Hence we have: if $\neg T(\psi_k)$, then $\neg T(\psi_{k-1})$.

Define:

- $\varphi_0 = \ulcorner 0 = 0 \urcorner$,
- for $k > 0$, $\varphi_k := \neg\psi_k \rightarrow \bigvee\limits_{i<k} \neg\varphi_i$.

Using DC-elim we obtain:

(1) $\forall k \leq n\big[T(\neg\psi_k) \rightarrow \big(T(\varphi_k) \rightarrow \exists i < k \neg T(\varphi_i)\big)\big]$,

(2) $\forall k \leq n T(\varphi_k)$.

This leads to a contradiction. Let k be such that $T(\neg\psi_k)$. Then by (2) $T(\varphi_k)$. Hence by (1) $\exists i < k T(\neg\varphi_i)$, which contradicts (2) and thus the whole proof is finished. □

A separate (unpublished) result due to Bartosz Wcisło establishes that DC-intro is conservative over PA.

Acknowledgment

The research reported here is based on a joint work with Mateusz Łełyk and Bartosz Wcisło.

References

[1] Cieśliński, C. *The Epistemic Lightness of Truth*, Cambridge University Press, 2017.

[2] Enayat, A., Pakhomov, F. "Truth, disjunction, and induction", *Archive for Mathematical Logic* 58, 753–766, 2019.

[3] Halbach, V. *Axiomatic Theories of truth*, Cambridge University Press, 2011.

[4] Kotlarski, H., Krajewski, S. and Lachlan, A. "Construction of satisfaction classes for nonstandard models", *Canadian Mathematical Bulletin* 24, 283–293, 1981.

[5] Łełyk, M. and Wcisło, B. "Notes on bounded induction for the compositional truth predicate", *Review of Symbolic Logic* 10, 355–480, 2017.

Logics for Reasoning about Knowledge and Conditional Probability

Šejla Dautović [1], Dragan Doder [2], Zoran Ognjanović [3]

[1,3]*Mathematical Institute of Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade, Serbia
[2]*Utrecht University*
Buys Ballotgebouw, Princetonplein 5, 3584 CC Utrecht, The Netherlands
E-mail: [1]shdautovic@mi.sanu.ac.rs, [2]d.doder@uu.nl, [3]zorano@mi.sanu.ac.rs

Keywords:
Probabilistic logic, Epistemic logic, Completeness.

Epistemic logics are formal models designed in order to reason about the knowledge of agents and their knowledge of each other's knowledge. During the last couple of decades, they have found applications in various fields such as game theory, the analysis of multi-agent systems in computer science and artificial intelligence [8, 9, 19]. In parallel, uncertain reasoning has emerged as one of the main fields in artificial intelligence, with many different tools developed for representing and reasoning with uncertain knowledge. A particular line of research concerns the formalization in terms of logic, and the questions of providing an axiomatization and decision procedure for *probabilistic logic* attracted the attention of researchers and triggered investigation about formal systems for probabilistic reasoning [1, 7, 10, 11, 15, 16]. Fagin and Halpern [6] emphasised the need for combining those two fields for many application areas, and in particular in distributed systems applications, when one wants to analyze randomized or probabilistic programs. They developed a joint framework for reasoning about knowledge and probability, proposed a complete axiomatization and investigated decidability of the framework. Based on the seminal paper by Fagin, Halpern and Meggido [7], they extended the propositional epistemic language with formulas which express linear combinations of probabilities, called *linear weight formulas*, i.e., the formulas of the form $a_1w(\alpha_1)+...+a_kw(\alpha_k) \geq r$, where a_j's and r are rational numbers. They proposed a finitary axiomatization and proved weak completeness, using a small model theorem.

In this talk, we propose two logics that extend the logic from [6] by also allowing formulas that can represent conditional probability. First we present a propositional logic for reasoning about knowledge and conditional probability from [2]. Then we discuss how to develop its first-order extension. Our languages contain both knowledge operators K_i (one for each agent i) and conditional probability formulas of the form

$$a_1 w_i(\alpha_1, \beta_1) + ... + a_k w_i(\alpha_k, \beta_k) \geq r.$$

The expressions of the form $w_i(\alpha, \beta)$ represent conditional probabilities that agent i places on events according to Kolmogorov definition: $P(A|B) = \frac{P(A \cap B)}{P(B)}$ if $P(B) > 0$, while $P(A|B)$ is undefined when $P(B) = 0$. The corresponding semantics consists of enriched Kripke models, with a probability measure assigned to every agent in each world.

Our main results are sound and strongly complete (every consistent set of formulas is satisfiable) axiomatizations for both logics. We prove strong completeness using an adaptation of Henkin's construction, modifying some of our earlier methods [3, 5, 4, 15, 16]. Our axiom system contains infinitary rules of inference, whose premises and conclusions are in the form of so called k-nested implications. This form of infinitary rules is a technical solution already used in probabilistic, epistemic and temporal logics for obtaining various *strong necessitation* results [13, 14, 17, 18]. We also prove that our propositional logic is decidable, combining the method of filtration [12] and a reduction to a system of inequalities.

Acknowledgment

This work has been partially funded by the Science Fund of the Republic of Serbia through the project Advanced artificial intelligence techniques for analysis and design of system components based on trustworthy BlockChain technology - AI4TrustBC.

References

[1] Alechina, N.: *Logic with Probabilistic Operators.* In: Proc. of the ACCOLADE '94. pp. 121–138 (1995)

[2] Dautović, Š., Doder, D., Ognjanović, Z.: *An Epistemic Probabilistic Logic with Conditional Probabilities.* In: Logics in Artificial Intelligence - 17th European Conference, JELIA 2021, Virtual Event, May 17-20, 2021, Proceedings. pp. 279–293. Springer (2021)

[3] Doder, D., Marinković, B., Maksimović, P., Perović, A.: *A Logic with Conditional Probability Operators.* Publications de L'Institut Mathematique **Ns. 87(101)**, 85–96 (2010)

[4] Doder, D., Ognjanovic, Z.: A probabilistic logic for reasoning about uncertain temporal information. In: Meila, M., Heskes, T. (eds.) Proceedings of the Thirty-First Conference on Uncertainty in Artificial Intelligence, UAI 2015, July 12-16, 2015, Amsterdam, The Netherlands. pp. 248–257. AUAI Press (2015)

[5] Doder, D., Ognjanovic, Z.: Probabilistic logics with independence and confirmation. Stud Logica **105**(5), 943–969 (2017)

[6] Fagin, R., Halpern, J.Y.: *Reasoning about knowledge and probability.* Journal of the ACM **41(2)**, 340–367 (1994)

[7] Fagin, R., Halpern, J.Y., Megiddo, N.: *A logic for reasoning about probabilities.* Information and Computation **87**, 78–128 (1990)

[8] Fagin, R., Geanakoplos, J., Halpern, J.Y., Vardi, M.Y.: *The hierarchical approach to modeling knowledge and common knowledge.* Int. J. Game Theory **28**(3), 331–365 (1999)

[9] Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: *Reasoning About Knowledge.* MIT Press (2003)

[10] Halpern, J.Y., Pucella, R.: *A Logic for Reasoning about Evidence.* J. Artif. Intell. Res. **26**, 1–34 (2006)

[11] van der Hoek, W.: *Some Considerations on the Logic PFD*$\tilde{}$. Journal of Applied Non-Classical Logics **7**(3) (1997)

[12] Hughes, G.E., Cresswell, M.J.: *A companion to modal logic.* Methuen London; New York (1984)

[13] de Lavalette, G.R.R., Kooi, B., Verbrugge, R.: *A strongly complete proof system for propositional dynamic logic.* In: AiML2002—Advances in Modal Logic. pp. 377–393 (2002)

[14] Marinkovic, B., Glavan, P., Ognjanovic, Z., Studer, T.: *A temporal epistemic logic with a non-rigid set of agents for analyzing the blockchain protocol.* Journal of Logic and Computation **29**(5), 803–830 (2019)

[15] Ognjanović, Z., Rašković, M., Marković, Z.: *Probability logics: probability-based formalization of uncertain reasoning.* Springer (2016)

[16] Savic, N., Doder, D., Ognjanovic, Z.: Logics with lower and upper probability operators. Int. J. Approx. Reason. **88**, 148–168 (2017)

[17] Tomovic, S., Ognjanovic, Z., Doder, D.: *Probabilistic Common Knowledge Among Infinite Number of Agents.* In: Symbolic and Quantitative Approaches to Reasoning with Uncertainty - 13th European Conference, ECSQARU 2015, Compiègne, France, July 15-17, 2015. Proceedings. Lecture Notes in Computer Science, vol. 9161, pp. 496–505. Springer (2015)

[18] Tomovic, S., Ognjanovic, Z., Doder, D.: *A First-order Logic for Reasoning about Knowledge and Probability.* ACM Trans. Comput. Log. **21**(2), 16:1–16:30 (2020)

[19] Wolter, F.: *First order common knowledge logics.* Studia Logica **65**(2), 249–271 (2000)

Glivenko classes and constructive cut elimination in infinitary logic

Giulio Fellin[1, 4, 5], **Sara Negri**[2], **Eugenio Orlandelli**[3]

[1] *Università di Verona, Dipartimento di Informatica*
Strada le Grazie 15, 37134, Verona, Italy
[2] *Università di Genova, Dipartimento di Matematica*
via Dodecaneso, 35, 16146, Genova, Italy
[3] *Univerità di Bologna, Dipartimento di Filosofia e Comunicazione*
via Zamboni 38, 40126, Bologna, Italy
[4] *Univerità di Trento, Dipartimento di Matematica*
[5] *Univerity of Helsinki, Department of Philosophy*
E-mail: [1]`giulio.fellin@univr.it`, [2]`sara.negri@unige.it` [3]`eugenio.orlandelli@unibo.it`

Keywords:

Geometric theories, Glivenko sequent classes, Infinitary logic; Conservativity result; Constructive cut elimination.

Notable parts of algebra and geometry can be formalised as *coherent theories* over first-order classical or intuitionistic logic. Their axioms are *coherent implications*, i.e., universal closures of implications $D_1 \supset D_2$, where both D_1 and D_2 are built up from atoms using conjunction, disjunction and existential quantification. Examples include all algebraic theories, such as group theory and ring theory, all essentially algebraic theories, such as category theory [4], the theory of fields, the theory of local rings, lattice theory [13], projective and affine geometry [13, 10], the theory of separably closed local rings (aka "strictly Henselian local rings") [5, 10, 15].

Although wide, the class of coherent theories leaves out certain axioms in algebra such as the axioms of torsion abelian groups or of Archimedean ordered fields, or in the theory of connected graphs, as well as in the modelling of epistemic social notions such as common knowledge. All the latter examples can however be axiomatised by means of *geometric axioms*, a generalisation of coherent axioms that allows infinitary disjunctions.

Orevokov [11] has established some well-known conservativity results of classical logic over intuitionistic and minimal predicate logics with equality. In particular, [11] isolates seven classes of sequents – the so-called *Glivenko sequent classes* – having this property and it shows that these classes are optimal: any class of sequents for which classical derivability implies intuitionisitc derivability is contained in one of these seven classes. The interest of such conservativity results is twofold. First, since proofs in intuitionistic logic obtain a computational meaning via the Curry-Howard correspondence, such results identify some classical theories having a computational content. Second, since it may be easier to prove theorems in classical than in intuitionistic logic and since there are more well-developed automated theorem provers for classical than for intuitionistic logic, such results simplify the search for theorems in intuitionistic theories.

Coherent and geometric implications form sequents that give a Glivenko class [11], as shown by Barr's Theorem.

Theorem 1 (Barr's Theorem [2]) *If $\mathcal{T}$ is a coherent (geometric) theory and A is a sentence provable from $\mathcal{T}$ with (infinitary) classical logic, then A is provable from $\mathcal{T}$ with (infinitary) intuitionistic logic.*

If we limit our attention to first-order coherent theories $\mathcal{T}$, an extremely simple and purely logical proof of Barr's Theorem has been given in [7] by means of **G3**-style sequent calculi. [7] shows how to express coherent implications by means of rules that preserve the admissibility of the structural rules of inference. As a consequence, Barr's theorem is proved by simply noticing that a proof in **G3cT** is also a proof in the intuitionistic multisuccedent calculus **G3iT**. This simple and purely logical proof of Barr's Theorem has been extended to cover all other first-order Glivenko classes in [8].

A purely logical proof of Barr's Theorem for infinitary geometric theories has been given [9]. This work considers the **G3**-style calculi for classical and intuitionistic infinitary logic $\mathbf{G3[ci]}_\omega$ (with finite sequents instead of countably infinite sequents) and their extension with rules expressing geometric implications $\mathbf{G3[ci]}_\omega\mathbf{T}$. The main results in [9] are that in $\mathbf{G3[ci]}_\omega\mathbf{T}$ all rules are height-preserving invertible, the structural rules of weakening and contraction are height-preserving admissible, and cut is admissible. Hence, Barr's Theorem for geometric theories is proved by showing that a proof in $\mathbf{G3c}_\omega\mathbf{T}$ is also a proof in the intuitionistic multisuccedent calculus $\mathbf{G3i}_\omega\mathbf{T}$.

In this paper we extend this purely logical proof of the infinitary Barr's Theorem to cover all other infinitary Glivenko sequent classes: for each class we give a purely constructive proof of conservativity of classical infinitary logic over intuitionistic and minimal infinitary logics.

One weakness of the results in [9] is that the cut-elimination procedure given in Sect. 4.1 is not constructive. This is a typical limitation of cut eliminations in infinitary logics that are based on ordinal numbers [3, 6, 14]. The main problem is that the proof makes use of the 'natural' (or Hessenberg) commutative sum of ordinals which is not available in **CZF** nor in **IZF** [12, p.369]. We constructivise the proof of (height-preserving) admissibility of the structural rules for $\mathbf{G3[cim]}_\omega\mathbf{T}$ by giving procedures that avoid completely the need for ordinal numbers: inductions on (sums of) ordinals are replaced by inductions on well-founded trees and by Brouwer's principle of bar induction.[1]

[1] See [12, §7] for a different constructive proof of cut elimination in infinitary logic, and see [1] for another ordinal-free proof.

References

[1] Ryota Akiyoshi. An ordinal-free proof of the complete cut-elimination theorem for Π^1_1-CA+BI with the ω-rule. *IfCoLog Journal of Logics and their Applications*, 4(4):867–883, 2017.

[2] Michael Barr. Toposes without points. *J. Pure Appl. Algebra*, 5(3):265–280, 1974.

[3] Solomon Feferman. Lectures on Proof Theory. In *Proceedings of the Summer School in Logic (Leeds, 1967)*, pages 1–107. Springer, Berlin, 1968.

[4] Peter Freyd. Aspects of topoi. *Bull. Austral. Math. Soc.*, 7(1):1–76, 1972.

[5] Peter T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium. Vol. 1 & 2.* Oxford University Press, New York, 2002.

[6] E. G. K. Lopez-Escobar. An interpolation theorem for denumerably long formulas. *Fund. Math.*, 57:253–272, 1965.

[7] Sara Negri. Contraction-free sequent calculi for geometric theories with an application to Barr's theorem. *Arch. Math. Logic*, 42(4):389–401, 2003.

[8] Sara Negri. Glivenko sequent classes in the light of structural proof theory. *Arch. Math. Logic*, 55(3-4):461–473, 2016.

[9] Sara Negri. Geometric rules in infinitary logic. In O.Arieli and A. Zamansky, editors, *Arnon Avron on Semantics and Proof Theory of Non-Classical Logics*, pages 265–293. 2021. Springer.

[10] Sara Negri and Jan von Plato. *Proof Analysis. A contribution to Hilbert's last problem.* Cambridge University Press, Cambridge, 2011.

[11] V.P. Orevkov. Glivenko's sequence classes. In V.P. Orevkov, editor, *Logical and logico-mathematical calculi. Part 1*, pages 131–154. Leningrad, 1968.

[12] Michael Rathjen. Remarks on Barr's theorem. Proofs in geometric theories. In D. Probst and P. Schuster, editors, *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, pages 347–374. de Gruyter, 2016.

[13] Thoralf Skolem. Logisch-kombinatorische Untersuchungen. *Videnskapsselskapets skrifter, 1. Mat.-naturv. klasse*, 4, 04 1920.

[14] Gaisi Takeuti. *Proof Theory.* North-Holland, 1987^2.

[15] Gavin Wraith. Generic Galois theory of local rings. In M. P. Fourman et al., editor, *Applications of Sheaves*, pages 739–767. Springer-Verlag, 1979.

Consistent ultrafinitist logic

Michał J. Gajda [1]

[1] *Migamake Pte Ltd 1*
mjgajda@migamake.com
E-mail: [1]`mjgajda@migamake.com`,

September 15, 2021

Ultrafinitism(Kornai 2003; Podnieks 2005; Yessenin-Volpin 1970; Gefter 2013; Lenchner 2020) postulates that we can only reason and compute relatively short objects(Krauss and Starkman 2004; Sazonov 1995; Lloyd 2002; Gorelik 2010), and numbers beyond certain value are not available. Some philosophers also question physical existence of real numbers beyond certain level of accuracy(Gisin 2019). This approach would also forbid many forms of infinitary reasoning and allow to remove many from paradoxes stemming from countable enumeration.

However, philosophers still disagree of whether such a finitist logic could be consistent(Magidor 2007), while constructivist mathematicians claim that *"no satisfactory developments exist"*(Troelstra 1988). We present preliminary work on a proof system based on Curry-Howard isomorphism(Howard 1980) and explicit bounds for computational complexity.

We believe that this approach may present certain impossibility results as logical paradoxes stemming from a profligate use of transfinite reasoning(Schirn and Niebergall 2005).

Using a bound on cost and depth of the term for each inference, we independently developed a very similar approach to that used for cost bounding in higher-order rewriting(Vale and Kop 2021).

$$
\begin{array}{llll}
\text{Variables:} & v \in V & \text{Positive naturals:} & i \in \mathbb{N} \setminus \{0\} \\
\text{Polynomials:} & \multicolumn{3}{r}{\rho ::= v \mid i \mid \rho + \rho \mid \rho * \rho \mid \rho^{\rho} \mid iter(\rho, \rho, v) \mid \rho[\![\rho/v]\!]} \\
\text{Propositions:} & \multicolumn{3}{r}{P ::= v \mid p \wedge p \mid p \vee p \mid p \rightarrow p \mid \forall_{\alpha} v.p \mid \exists v_{\beta}.p \mid \bot} \\
\text{Environments:} & \Gamma ::= A^{1}{}_{\beta_1}, ..., A^{n}{}_{\beta_n} & \text{Judgements:} & \Gamma \vdash^{\alpha}_{\beta} A : \tau
\end{array}
$$

Here ρ^{ρ} is an exponentation, and $iter(\rho_1, \rho_2, \rho_3)v$ is an iterated function composition with respect to argument variable v that is bound in the polynomial ρ_1, iterated ρ_2 times . The $\rho_1[\![\rho_2/v]\!]$ describes substitution, inside of ρ_1, of all instances of bound variable v with ρ_2.

The polynomials will be standing on one of two roles: as an upper bound on the proof complexity, and there we will use symbol α as placeholder, or to state an upper bound on the number of constructors in the proof indicated by symbol β. That is because number of constructors may sometimes bound a recursive examination of the proof of a proposition.

Notation $\forall x_v : A \implies {}^{\alpha(v)}_{\beta(v)}B$ binds proof variable x with type of A, and then bound in polynomials $\alpha(v)$ for complexity and $\beta(v)$ for depth of the normalized term.

$$\frac{\Gamma \vdash^{\alpha}_{\beta} y : A \quad v \in V}{\Gamma, x_v : A \vdash^{1}_{v} x : A}\ var$$

$$\frac{\Gamma \vdash^{\alpha_1}_{\beta_1} a^1 : A^1 \quad \Gamma \vdash^{\alpha_2}_{\beta_2} a^2 : A^2}{\Gamma \vdash^{\alpha_1+\alpha_2}_{\max(\beta_1,\beta_2)+1} (a^1, a^2) : A^1 \wedge A^2}\ pair \qquad \frac{\Gamma \vdash^{\alpha}_{\max(\beta_1,\beta_2)} e : A^1 \wedge A^2}{\Gamma \vdash^{\alpha+1}_{\beta-1} prj_i\ \ e : A^i}\ prj_i$$

$$\frac{\Gamma \vdash^{\alpha}_{\beta} e : A^i}{\Gamma \vdash^{\alpha+1}_{\beta+1} inj_i\ \ e : A^1 \vee A^2}\ inj_i \qquad \frac{\Gamma \vdash^{\alpha_1}_{\beta_1} e : A \qquad \alpha_1 \leq \alpha_2 \qquad \beta_1 \leq \beta_2}{\Gamma \vdash^{\alpha_2}_{\beta_2} e : A}\ subsume$$

$$\frac{\Gamma \vdash^{\alpha_\vee}_{\beta_\vee} a : A^1 \vee A^2 \qquad \Gamma, x : A^1{}_{\beta_\vee - 1} \vdash^{\alpha_1}_{\beta_1} b : B \qquad \Gamma, y : A^2{}_{\beta_\vee - 1} \vdash^{\alpha_2}_{\beta_2} c : B}{\Gamma \vdash^{\alpha_\vee + max(\alpha_1,\alpha_2)+1}_{\max(\beta_1,\beta_2)} case\ a\ of\ \ inj_1\ \ x \to b;\ inj_2\ \ y \to c : B}\ case$$

$$\frac{\Gamma, x_v : A \vdash^{\alpha(v)}_{\beta(v)} e : B}{\Gamma \vdash^{\alpha(1)+1}_{\beta(1)+1} \lambda x.e : \forall a_v : A \Longrightarrow {}^{\alpha(v)}_{\beta(v)}B}\ abs \qquad \frac{\Gamma \vdash^{\alpha_1}_{\beta_1} e : \forall a : A_v \Longrightarrow {}^{\alpha_2(v)}_{\beta_2(v)}B \quad \Gamma \vdash^{\alpha_3}_{\beta_3} a : A}{\Gamma \vdash^{\alpha_1+\alpha_2(\beta_3)+\alpha_3}_{\beta_2(\beta_3)} e\ a : B}\ app$$

$$\frac{\Gamma \vdash^{\alpha_1}_{\beta_1} f : A_v {\Rightarrow} {}^{\alpha_2(v_1)}_{\beta_2(v_2)}A \quad \Gamma \vdash^{\alpha_3}_{\beta_3} a : A \quad v_2 > \beta_2(v_2)}{\Gamma \vdash^{\alpha_1 + iter(\alpha_2,\beta_3,v_1)[\![v_1/\beta_3]\!]+\alpha_3}_{iter(\beta_2,\beta_3,v_2)[\![v_2/\beta_3]\!]} rec\,f\ a : B}\ rec$$

With exception of *bound* these are all reinterpretations of rules for intuitionistic logic, enriched with bounds on the proof length α and normalized term depth β.

Please note that these rules all maintain bounded depth with no unbounded recursion. We may add rule for recursive definitions (like definition of the closure):

Here the depth of the term must decrease at each step of the recursion.

Our inference rules rely on computing polynomial bounds and their inequality. Given that all variables are positive naturals because they represent the data of non-zero size: $x \geq 1$, we may simplify these polynomials with a set of simple inequalities.

We have shown a possible consistent logic for inference with strictly bounded number of steps. This allows us to limit our statements by the length of acceptable proof, and thus define statements that are not just true, but computable within Bremermann-Gorelik limit(Gorelik 2010)[1] This inference system explicitly bounds both length of the resulting proof, and the bounds on the depth of the normalized result term. This allows to avoid inconsistencies suggested by philosophical work, and at the same time steers away from issues that limit the expressive power of logics with implicit complexity like Bounded Arithmetic(Krajicek 1995).

[1] Computation run by computer the size of Earth within the lifespan of Earth so far. Of the order of 10^{93}.

References

Abel, Andreas, and Christian Sattler. 2019. "Normalization by Evaluation for Call-by-Push-Value and Polarized Lambda-Calculus." http://arxiv.org/abs/1902.06097.

Gefter, Amanda. 2013. "Mind-Bending Mathematics: Why Infinity Has to Go." *New Scientist* 219 (2930): 32–35. https://doi.org/https://doi.org/10.1016/S0262-4079(13)62043-6.

Gisin, Nicolas. 2019. "Indeterminism in Physics, Classical Chaos and Bohmian Mechanics. Are Real Numbers Really Real?" http://arxiv.org/abs/1803.06824.

Gorelik, Gennady. 2010. "Bremermann's Limit and cGh-Physics." http://arxiv.org/abs/0910.3424.

Howard, William A. 1980. "The Formulae-as-Types Notion of Construction." In *To h.b. Curry: Essays on Combinatory Logic, λ-Calculus and Formalism*, edited by J. Hindley and J. Seldin, 479–90. Academic Press.

Kornai, Andras. 2003. "Explicit Finitism." *International Journal of Theoretical Physics* 42 (February): 301–7. https://doi.org/10.1023/A:1024451401255.

Krajicek, Jan. 1995. *Bounded Arithmetic, Propositional Logic and Complexity Theory*. Encyclopedia of Mathematics and Its Applications. Cambridge University Press. https://doi.org/10.1017/CBO9780511529948.

Krauss, Lawrence, and Glenn Starkman. 2004. "Universal Limits on Computation," May.

Lenchner, Jonathan. 2020. "A Finitist's Manifesto: Do We Need to Reformulate the Foundations of Mathematics?" http://arxiv.org/abs/2009.06485.

Lloyd, S. 2002. "Computational Capacity of the Universe." *Physical Review Letters* 88 23: 237901.

Magidor, Ofra. 2007. "Strict Finitism Refuted?"

Podnieks, Karlis. 2005. "Towards a Real Finitism?" 2005. http://www.ltn.lv/%C2%A0podnieks/finitism.htm.

Sazonov, Vladimir Yu. 1995. "On Feasible Numbers." In *Logic and Computational Complexity*, edited by Daniel Leivant, 30–51. Berlin, Heidelberg: Springer Berlin Heidelberg.

Schirn, Matthias, and Karl-Georg Niebergall. 2005. "Finitism = PRA? On a Thesis of w. W. Tait." *Reports on Mathematical Logic*, January.

Troelstra, A. S. 1988. *Constructivism in Mathematics: An Introduction*. Elsevier.

Vale, Deivid, and Cynthia Kop. 2021. "Tuple Interpretations for Higher-Order Rewriting." *CoRR* abs/2105.01112. https://arxiv.org/abs/2105.01112.

Yessenin-Volpin, Aleksandr S. 1970. "The Ultra-Intuitionistic Criticism and the Antitraditional Program for Foundations of Mathematics." In *Studies in Logic and the Foundations of Mathematics*, 60:3–45. Elsevier.

Federating Digital Contact Tracing using Structured Overlay Networks

Silvia Ghilezan [1,2], Simona Kašterović[2], Luigi Liquori [4], Bojan Marinković [3,1], Zoran Ognjanović [1], Tamara Stefanović [2]

[1] *Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia*
[2] *Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia*
[3] *Clarivate, Serbia*
[4] *INRIA & Université Côte d'Azur, France*

Keywords:
Covid-19, Digital Contact Tracing, Structured Overlay Networks.

One of the biggest challenges of today is to slow down the spreading of SARS-CoV-2 virus producing Covid-19 pandemic; *Prevention, Testing and Tracing* are the main pillars of the solution.

Contact Tracing of an infected person is essential to control the spread of the disease. Through this process Health Authorities identify, notify, and monitor people who came in close contact with an individual who was tested positive for an infectious disease, like Covid-19, while he/she was infectious. Also, contact tracing data helps medical experts to find the origin of the virus, learn more about the nature of the virus and estimate the speed of how fast the virus is spreading.

Contact tracing has mostly been done manually since many centuries ago. Identifying contacts is done through an interview with the person infected with the virus, after each contact is called by phone. Due to the highly contagious nature of the SARS-CoV-2 virus and the fact that symptoms can manifest after many days (or even never, e.g. *asymptomatic cases*), manual contact tracing does not give satisfactory results. In the situations when the virus is spreading to fast, Health departments and authorities do not have enough employees to do manual contact tracing.

For these reasons digital contact tracing has been considered already at the beginning of the Covid-19 pandemic. There is a plethora of digital contract tracing application. They are developed on very different paradigms, centralized vs. decentralized, GPS based vs. Bluetooth [1, 7]. The rush to make these applications work in the shortest time led to their great diversity. The most important open problem is their interoperability. There are many ongoing efforts to make a federation of these different systems. Herein, we address this problem and propose a solution based on mathematical models of overlay networks.

We present a design of the system for connecting different digital contact tracing applications, called *BubbleAntiCovid19* (*BAC19*). The model is inspired by Chord [8] and Synapse [3] Structured Overlay Networks. The correctness and efficiency of lookup procedures of this protocols was in the focus of several papers, e.g. [4, 5, 6, 8]. We prove that *BAC19* provides a complete and fully exhaustive retrieving procedure. Hence, *BAC19* is proven to be a simple yet powerful *interconnection* of already existing digital contact tracing applications that - by construction - do not communicate with each others as such providing their efficient interoperability. More details on this work can be found in [2].

Acknowledgment

This work was partly supported by the Science Fund Republic of Serbia #6526707 AI4TrustBC.

References

[1] Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., Seneviratne, A., Hu, W., Janicke, H., Jha, S.K.: *A Survey of COVID-19 Contact Tracing Apps.* IEEE Access 8, 134577–134601 (2020)

[2] Ghilezan, S., Kašterović, S., Liquori, L., Marinković, B., Ognjanović, Z. et al.. *Federating Digital Contact Tracing using Structured Overlay Networks.* 2021. hal-03127890v3

[3] Liquori, L., Tedeschi, C., Vanni, L., Bongiovanni, F., Ciancaglini, V., Marinković, B.: *Synapse: A scalable protocol for interconnecting heterogeneous overlay networks.* In: Crovella, M., Feeney, L.M., Rubenstein, D., Raghavan, S.V. (eds.) NETWORKING 2010, 9th International IFIP TC 6 Networking Conference, Chennai, India, May 11-15, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6091, pp. 67–82. Springer (2010)

[4] Marinković, B., Ciancaglini, V., Ognjanović, Z., Glavan, P., Liquori, L., Maksimović, P.: *Analyzing the exhaustiveness of the synapse protocol.* Peer Peer Netw. Appl. 8(5), 793–806 (2015)

[5] Marinković, B., Glavan, P., Ognjanović, Z.: *Proving properties of the chord protocol using the ASM formalism.* Theor. Comput. Sci. 756, 64–93 (2019)

[6] Marinković, B., Ognjanović, Z., Glavan, P., Kos, A., Umek, A.: *Correctness of the chord protocol.* Comput. Sci. Inf. Syst. 17(1), 141–160 (2020)

[7] Martin, T., Karopoulos, G., Hernandez-Ramos, J.L., Kambourakis, G., Fovino, I.N.: *Demystifying COVID-19 Digital Contact Tracing: A Survey*

on Frameworks and Mobile Apps. Wireless Communications and Mobile Computing 2020(8851429), 29 (2020),

[8] Stoica, I., Morris, R.T., Liben-Nowell, D., Karger, D.R., Kaashoek, M.F., Dabek, F., Balakrishnan, H.: *Chord: a scalable peer-to-peer lookup protocol for internet applications.* IEEE/ACM Trans. Netw. 11(1), 17–32 (2003)

n-bisimulations for generalised Veltman semantics

Sebastijan Horvat[1], **Tin Perkov**[2], **Mladen Vuković**[3]

[1,3] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, Zagreb, Croatia
[2] *Faculty of Teacher Education, University of Zagreb*
Savska cesta 77, Zagreb, Croatia
E-mail: [1] `sebastijan.horvat@math.hr`, [2] `tin.perkov@ufzg.hr`,
[3] `mladen.vukovic@math.hr`

Keywords:
Generalised Veltman semantics, bisimulation, bisimulation games, modal equivalence.

As incompleteness results emerged in modal logic, logicians started to investigate what modal languages actually are, or said differently, what is their position in the logical universe. Van Benthem's characterisation theorem (see e.g. [1]) shows that modal languages correspond to the bisimulation invariant fragment of first-order languages. One can prove that result with use of classical methods of first-order model theory. However, many problems arised when one tries to use such methods to prove a characterisation theorem over the provability logic GL. Because of that, A. Dawar and M. Otto develop a *models-for-games method* in [3], which provides conditions from which a characterisation theorem over particular class of models immediately follows. Using that, not only that characterisation theorem for provability logic GL was proved, but also M. Vuković and T. Perkov proved in [6] that this result can be extended to Veltman models for the interpretability logic IL. To prove that, they used bisimulation games on Veltman models for interpretability logic.

Since Veltman semantics is not fine-grained enough for certain application, the notion of generalised Veltman semantics emerged to obtain certain nonderivability results. It has turned out that this semantics has various good properties (see e.g. [4] and [5]). One question that arises is can *models-for-games method* be used to prove a characterisation theorem with respect to generalised Veltman semantics. In order to do that, one needs to define n-bisimulation and n-bisimulation games for generalised Veltman semantics. We carry that out in this work.

Also, it is easy to show that bisimilar worlds are modally equivalent. But what about other direction, that is, are modally equivalent worlds bisimilar? We negatively answer that question by using counterexamples for Veltman semantics in [2] and turning them into counterexamples for generalised Veltman semantics. Finally, we define n-bisimulation games for generalised Veltman semantics and prove the equivalence between the existence of a winning strategy in the n-bisimulation game and the existence of an n-bisimulation.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation (HRZZ) under the projects UIP-05-2017-9219 and IP-01-2018-7459.

References

[1] P. Blackburn, M. de Rijke, Y. Venema, *Modal Logic*, Cambridge University Press, 2001.

[2] V. Čačić, D. Vrgoč, *A Note on Bisimulation and Modal Equivalence in Provability Logic and Interpretability Logic*, Studia Logica 101(2013), 31–44

[3] A. Dawar, M. Otto, *Modal characterisation theorems over special classes of frames*, Annals of Pure and Applied Logic 161(2009), 1–42

[4] J. J. Joosten, J. Mas Rovira, L. Mikec, M. Vuković, *An overview of Generalised Veltman Semantics*, to appear

[5] L. Mikec, M. Vuković, *Interpretability logics and generalized Veltman semantics*, The Journal of Symbolic Logic, 85(2020), 749–772

[6] T. Perkov, M. Vuković, *A bisimulation characterization for interpretability logic*, Logic Journal of the IGLP 22(2014), 872–879

A Probabilistic Temporal Epistemic Logic

Angelina Ilić Stepić[1], Zoran Ognjanović[1] and Aleksandar Perović[2]

[1]Mathematical Institute of the Serbian Academy of Sciences and Arts, Kneza Mihaila 36, Belgrade, Serbia, {angelina,zorano}@mi.sanu.ac.rs
[2]Faculty of Transport and Traffic Engineering, University of Belgrade,Serbia , {pera}@sf.bg.ac.rs

September 14, 2021

Keywords:

multi-agent systems, temporal epistemic logic with probabilities, blockchain, formal model specification/verification

In this paper we present a probabilistic temporal epistemic logic $PTEL$ suitable to reason about uncertain knowledge of a non-rigid set of agents that can be changed during time. We define semantics for $PTEL$ as Kripke models with epistemic accessibility relations for agents' knowledge, a number of runs consisting of sequences of linearly ordered possible worlds indexed by non-negative integers, and probability functions defined on sets of runs. Also we provide a new formal framework in order to prove a number of properties of the blockchain protocol concerning its uncertain behavior.

The corresponding completeness theorem and decidability of the considered logic are proven.

Acknowledgements

This work was partially funded by the Science Fund of the Republic of Serbia through the project AI4TrustBC (the first and the second author)

References

[1] Z. Ognjanović, Z. Marković, M. Rašković, D. Doder and A. Perović *A propositional probabilistic logic with discrete linear time for reasoning about evidence*, Annals of Mathematics and Artificial Intelligence, 2012.

[2] D. Doder, J. Grant and Z. Ognjanović *Probabilistic logics for objects located in space and time*,Journal of Logic and Computation, 2013.

Towards Logic of Combinatory Logic

Simona Kašterović[1], Silvia Ghilezan[1,2]

[1] *Faculty of Technical Sciences, University of Novi Sad*
Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
[2] *Mathematical Institute of Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade, Serbia
E-mail: simona.k@uns.ac.rs, gsilvia@uns.ac.rs

Keywords:
Combinatory logic, classical propositional logic, simple types, axiomatization, semantics, soundness, completeness.

Typed combinatory logic found its application in various fields of computer science, e.g. program synthesis [1], machine learning, e.g. [2] and artificial intelligence, e.g. [3], etc. Developments of these fields urge for further research and development of typed combinatory logic. Although combinatory logic, both typed and untyped, has been subject of many studies, to the best of our knowledge none of them investigate combining typed combinatory logic with classical propositional logic in order to capture inference of type assignment statements.

We introduce in this paper a classical propositional logic for reasoning about simply typed combinatory logic, called logic of combinatory logic, and denoted by LCL.

First, we revisit a syntax of simply typed combinatory logic [5, 4, 6]. Terms of untyped combinatory logic, called CL-terms, are generated by the following syntax

$$M, N := x \mid \mathsf{S} \mid \mathsf{K} \mid \mathsf{I} \mid MN$$

where x belongs to a countable set of term variables. The constants $\mathsf{S}, \mathsf{K}, \mathsf{I}$ are called primitive combinators. We are mostly interested in typed terms, more precisely we are interested in simply typed terms. Simple types are generated by the following syntax

$$\sigma, \tau := a \mid \sigma \to \tau$$

where a belongs to a countable set of type variables. A type assignment statement is of the form $M : \sigma$, where M is a CL-term and σ is a simple type. Our goal was to build up a logical system for reasoning about simply typed combinatory terms.

We propose extending simply typed combinatory logic with classical logical connectives of negation and conjunction. The obtained system is called *logic of* *combinatory logic* and it is denoted by LCL. The language of the logic LCL is generated by the following syntax

$$\alpha, \beta := M : \sigma \mid \neg\alpha \mid \alpha \wedge \beta$$

We see that logic LCL is actually obtained from classical propositional logic by replacing propositional letters with type assignment statements $M : \sigma$. We argue that logic LCL is a first step towards formalization of meta-language of simply typed combinatory logic.

We give an axiomatic system and propose a semantics for LCL. The axiomatic system of LCL consisting of eight axiom schemes and one inference rule is given in Figure 1. It has emerged as combination of the axiomatic system for classical propositional logic and type assignment system for simply typed combinatory logic.

Axiom schemes:

$$\begin{array}{ll}
\text{(Ax 1)} & \mathsf{S} : (\sigma \to (\tau \to \rho)) \to ((\sigma \to \tau) \to (\sigma \to \rho)) \\
\text{(Ax 2)} & \mathsf{K} : \sigma \to (\tau \to \sigma) \\
\text{(Ax 3)} & \mathsf{I} : \sigma \to \sigma \\
\text{(Ax 4)} & (M : \sigma \to \tau) \Rightarrow ((N : \sigma) \Rightarrow (MN : \tau)) \\
\text{(Ax 5)} & M : \sigma \Rightarrow N : \sigma, \text{ if } M = N \text{ is provable in } \mathcal{EQ}^{\eta} \\
\text{(Ax 6)} & \alpha \Rightarrow (\beta \Rightarrow \alpha) \\
\text{(Ax 7)} & (\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma)) \\
\text{(Ax 8)} & (\neg\neg\alpha \Rightarrow \neg\beta) \Rightarrow ((\neg\neg\alpha \Rightarrow \beta) \Rightarrow \neg\alpha)
\end{array}$$

Inference rule:

$$\frac{\alpha \Rightarrow \beta \qquad \alpha}{\beta}\ \text{(MP)}$$

Figure 1: Axiomatic system of LCL

The first five axiom schemes correspond to axioms and rules of type assignment system for simply typed combinatory logic and the last three axiom schemes are axiom schemes of classical propositional logic. The axiomatic system has one inference rule, called Modus Ponens.

Inspired by Kripke-style semantics for typed lambda calculus introduced in [7, 8], we propose semantics for LCL based on applicative structures extended with special elements corresponding to primitive combinators. The main results of the paper are the soundness and completeness of the axiomatic system with respect to the proposed semantics.

Acknowledgment

The research reported in the paper is partly supported by the Science Fund Republic of Serbia #6526707 AI4TrustBC.

References

[1] Düdder, B., Martens, M., Rehof, J., and Urzyczyn, P., *Bounded combinatory logic*, in Computer Science Logic (CSL'12) - 26th International Workshop/21st Annual Conference of the EACSL, CSL 2012, September 3-6, 2012, Fontainebleau, France, ser. LIPIcs, P. Cégielski and A. Durand, Eds., vol. 16. Schloss Dagstuhl - Leibniz- Zentrum für Informatik, 2012, pp. 243–258. [Online]. Available: `https://doi.org/10.4230/LIPIcs.CSL.2012.243`

[2] Liang, P., Jordan, M. I., and Klein, D., *Learning programs: A hierarchical bayesian approach*, in Proceedings of the 27th International Conference on Machine Learning (ICML-10), June 21-24, 2010, Haifa, Israel, J. Fürnkranz and T. Joachims, Eds. Omnipress, 2010, pp. 639–646. [Online]. Available: `https://icml.cc/Conferences/2010/papers/568.pdf`

[3] Garrette, D., Dyer, C., Baldridge, J., and Smith, N. A., *Weakly-supervised grammar-informed bayesian CCG parser learning*, in Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA, B. Bonet and S. Koenig, Eds. AAAI Press, 2015, pp. 2246–2252. [Online]. Available: `http://www.aaai.org/ocs/index.php/AAAI/AAAI15/paper/view/9835`

[4] Bimboó, K., *Combinatory Logic: Pure, Applied, and Typed*, CRC Press, Taylor and Francis Group, Boca Raton, Florida, 2012.

[5] Barendregt, H. P., *The lambda calculus - its syntax and semantics*, ser. Studies in logic and the foundations of mathematics. North-Holland, 1985, vol. 103.

[6] Barendregt, H. P., Dekkers, W., and Statman, R., *Lambda Calculus with Types*, ser. Perspectives in logic. Cambridge University Press, 2013. [Online]. Available: `http://www.cambridge.org/de/academic/subjects/mathematics/logic-categories-and-sets/lambda-calculus-types`

[7] Mitchell, J. C., Moggi, E., *Kripke-style models for typed lambda calculus*, Ann. Pure Appl. Log., vol. 51, no. 1-2, pp. 99–124, 1991. [Online]. Available: `https://doi.org/10.1016/0168-0072(91)90067-V`

[8] Kašterović, S., Ghilezan, S., *Kripke-style semantics and completeness for full simply typed lambda calculus,* J. Log. Comput., vol. 30, no. 8, pp. 1567–1608, 2020. [Online]. Available: `https://doi.org/10.1093/logcom/exaa055`

Redescription mining

Matej Mihelčić

Department of Mathematics, Faculty of Science, University of Zagreb

Data mining is a field of computer science tasked to develop novel algorithms and techniques for analyses of various types of data. We make an overview of one of the data mining tasks called redescription mining [9]. The main goal of this task is to: a) discover subsets of instances that can be described in more than one way (re-described), b) construct appropriate redescriptions, objects that re-describe these subsets of instances and are somehow understandable to the domain experts. The building blocks of redescriptions are queries which are constructed using some query language. Thus, given a set of instances $\mathcal{I}$, a set of attributes $\mathcal{A}$ describing these instances, a set of views $\mathcal{W}$ (logical mappings of attributes to their natural groups), a query language Q, query similarity relation $\sim$ and a constraint set $\mathcal{C}$, the task of redescription mining is to find all redescriptions that satisfy constraints in $\mathcal{C}$.

A classic formulation of redescription mining constructs queries using formulae of propositional logic with operators constrained to conjunction, disjunction and negation. The Jaccard index [4] is used as a similarity relation and a constraint set $\mathcal{C}$ initially consisted of thresholds on minimal support and a similarity relation (the Jaccard index). This set was later extended with statistical significance of redescriptions computed using the Binomial or Hypergeometric distribution.

Initial algorithms (e.g. [8, 9]) used only one set of Boolean attributes (thus $\mathcal{W}$ was a trivial mapping). In this setting, one can derive some interesting theoretical properties for a strict version of redescription definition which requires perfect similarity of redescription queries. *Impossibility results* show: a) two identical rows always share descriptors, b) full datasets, having all 2^n row combinations where n is the number of attributes, can not have distinct redescriptions of descriptors defined over the columns of this dataset. *Strong possibility results* show that if at least one row is missing from the full dataset, then every descriptor has a redescription. This leads to the dichotomy law that states that either no descriptor has a distinct redescription or all descriptors do, and as a consequence that this also holds for expressions in CNF or DNF.

This strict formulation of a redescription is not useful in practice because it is more common to find redescriptions whose queries do not describe identical but only similar subsets of instances (the similarity is not perfect). Relaxation of query similarity measure is used in various heuristic approaches for redescription mining. These approaches are based on different data mining and machine learning techniques (e.g. [9, 3, 2, 5, 6]), working with data of various generality and different complexity of mapping $\mathcal{W}$.

More complex data containing descriptors of instances and descriptions of relations between them could not be efficiently tackled using standard redescription mining algorithms. This lead to the development of the relational redescription mining approach [1]. This approach enriches the query language with binary relations and transforms redescription queries to graphs. A use-case application [7] of redescription mining to time-evolving gene expression data showed that properly grouped redescriptions, obtained on time-fragmented datasets, can form a Kripke model that supports query, inference, comparative assessment tasks and provides process descriptions.

References

[1] Esther Galbrun and Angelika Kimmig. "Finding relational redescriptions". In: *Machine learning* 96.3 (2014), pp. 225–248.

[2] Esther Galbrun and Pauli Miettinen. "From black and white to full color: extending redescription mining outside the Boolean world". In: *Statistical Analysis and Data Mining: The ASA Data Science Journal* 5.4 (2012), pp. 284–303.

[3] Arianna Gallo, Pauli Miettinen, and Heikki Mannila. "Finding subgroups having several descriptions: Algorithms for redescription mining". In: *Proc. SIAM ICDM'08*. SIAM. 2008, pp. 334–345.

[4] Paul Jaccard. "The distribution of the flora in the alpine zone. 1". In: *New phytologist* 11.2 (1912), pp. 37–50.

[5] Matej Mihelčić, Sašo Džeroski, Nada Lavrač, and Tomislav Šmuc. "Redescription mining augmented with random forest of multi-target predictive clustering trees". In: *Journal of Intelligent Information Systems* 50.1 (2018), pp. 63–96.

[6] Matej Mihelčić and Tomislav Šmuc. "Approaches for Multi-View Redescription Mining". In: *IEEE Access* 9 (2021), pp. 19356–19378. DOI: 10.1109/ACCESS.2021.3054245.

[7] Bhubaneswar Mishra and Samantha Kleinberg. "Remembrance of the experiments past: A redescription based tool for discovery in complex systems". In: *Proc. Complex systems'06*. 2006.

[8] Laxmi Parida and Naren Ramakrishnan. "Redescription mining: Structure theory and algorithms". In: *Proc. AAAI'05*. 2005, pp. 837–844.

[9] Naren Ramakrishnan, Deept Kumar, Bud Mishra, Malcolm Potts, and Richard F. Helm. "Turning cartwheels: An alternating algorithm for mining redescriptions". In: *Proc. KDD'04*. ACM Press, 2004, pp. 266–275.

Restricted Observational Equivalence

Petar Paradžik [1], **Ante Đerek**[2]

[1,2]*Faculty of Electrical Engineering and Computing, University of Zagreb*
Unska ulica 3, Zagreb
E-mail: [1]`petar.paradzik@fer.hr`, [2]`ante.derek@fer.hr`

Keywords:
observational equivalence, multiset rewriting, security protocols

It often happens that we want to compare the behavior of two systems. For example, we want to know whether, for a specific observer, the specification of the system exhibits the same behavior as the implementation, or whether the two security protocol instances behave in the same way. *Behavioral equivalence* can answer these questions.

The systems in mind can be described as *labeled transition systems* consisting of a (multi)set of states and a set of action-labeled transitions (rewrites) between states. Behavioral equivalence is inductively defined as a binary relation between the states of two labeled transition systems: Two states are in a relation if every action from the first state can be simulated by an equivalent action(s) from the second state and if the resulting states are also in a relation. The precise definition depends on what kinds of behaviors the we want to distinguish, i.e., what kind of actions we regard as equivalent. This gives rise to various flavors of equivalences, some of which are (strong) bisimulation, (rooted) branching bisimulation, simulation, (completed) trace equivalence, failure equivalence, and observational equivalence. For example, we say that two labeled transition systems are trace equivalent if they can perform the same sequence of actions — *traces* from their respective initial states.

There is an interesting notion of *behavioral abstraction* — an internal (hidden) actions that can not be directly observed. The motivation for such an abstraction may be, for example, the complexity of the system (state-space explosion) or "black box" computations (an adversary can not observe the internal states of a protocol). Such an internal action in the first system may be behaviorally equivalent to the sequence of internal actions in the second system.

We define abstracted behavioral equivalence called *restricted observational equivalence* by combining observational equivalence [1] with trace properties. We say that two systems P and Q are observationally equivalent under the set of traces (restrictions) ψ_P and ψ_Q respectively if an observer can not distinguish P and Q as long as the taken actions are part of the traces from ψ_P and

ψ_Q. Restrictions can, for example, specify that some actions must precede the others, or that some equality checks must hold. This is important in security protocol verification, as it allows us to enforce a certain behavior on the protocol rules and avoid false attacks while verifying behavioral equivalence. We explore how to automatically verify restricted observational equivalence of security protocols. We define the notion of *restricted bisimulation*, which is much easier to verify, and prove that it is a sound approximation of restricted observational equivalence. We take the security protocol verification tool TAMARIN prover [2], which is already capable of verifying bisimulation of bi-systems [3], extend it so that it can verify restricted bisimulation for a simple class of safety properties (restrictions), and prove the soundness of the extension. Finally, we use restricted bisimulation in TAMARIN prover to automatically verify offline guessing resistance for a well-known password-authenticated key exchange protocol called Encrypted Key Exchange.

References

[1] David Basin, Jannik Dreier, and Ralf Sasse. 2015. Automated Symbolic Proofs of Observational Equivalence. *In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15).* Association for Computing Machinery, New York, NY, USA, 1144–1155. DOI: `https://doi.org/10.1145/2810103.2813662`

[2] David Basin, Cas Cremers, Jannik Dreier, Simon Meier, Ralf Sasse, Benedikt Schmidt, and contributors, *The Tamarin Prover tool*, GitHub repository: `https://github.com/tamarin-prover/tamarin-prover`, accessed on September 2021.

[3] Bruno Blanchet and Martín Abadi and Cédric Fournet, Automated verification of selected equivalences for security protocols. *Journal of Logic and Algebraic Programming*, 75(1):3–51, February–March 2008.

Solution of Lambek's Problem: A construction of Dedekind-MacNeille-type bicompletions of categories

Duško Pavlović

University of Hawaii
E-mail: dusko@hawaii.edu

Dedekind defined the real numbers as the elements of the tight bicompletion of the linear order of the rational numbers. A bicompletion is said to be tight when it preserves any infima and suprema that already exist in the poset. In the 1930s, MacNeille generalized Dedekind's construction to arbitrary partially ordered sets. In his 1966, in his Lectures on Completions Springer Lecture Note in Mathematics 24, Lambek spelled out all of the main categorical generalizations of lattice completions, and left open the problem of characterizing the Dedekind-MacNeille, i.e. tight bicompletions of categories. In 1972, Isbell showed that the group Z_4 cannot have a tight bicompletion under limits and colimits.

However, Isbell's result did not close Lambek's Problem, but opened it slightly wider. For general reasons, categorical tight bicompletions must exist for a canonical family of limits and colimts, albeit not for all of them. To understand why, note that generalizing the Dedekind-MacNeille completion from posets to binary relations between them leads to (a general form of) Formal Concept Analysis. Concepts arise as infima and suprema of contexts just like the real numbers arise as infima and suprema of the rational numbers. Categories, just like posets, approximate suitable concepts from above and from below. In contrast with the posetal infima and suprema, the categorical limits and colimits do not always approximate each another. That is why a poset is complete if and only if it is cocomplete, but a category can be complete but not cocomplete, and cocomplete but not complete. Lambek's Problem thus boils down to characterizing the self-dual family of categorical limits and colimits that approximate each other. The tight bicompletions of categories that Lambek sought to characterize exist with respect to this notion of limit and colimit.

I will present a solution of this problem.

Proof theory of free logics

Edi Pavlović [1], Norbert Gratzl[1]

[1] *MCMP, LMU Munich*

Keywords:
Positive free logic, negative free logic, neutral free logic, sequent calculus, G3.

Free logics are a family of first-order logics which came about as a result of examining the existence assumptions of classical logic [1, 2, 3, 4]. What those assumptions are varies, but the central ones are that (i) the domain of interpretation is not empty, (ii) every name denotes exactly one object in the domain and (iii) the quantifiers have existential import.

Free logics reject the claim that names need to denote in (ii), and *positive* free logic concedes that some atomic formulas containing non-denoting names (including self-identity) are true, *negative* free logic treats them as uniformly false, and *neutral* free logic as taking a third value. There has been a renewed interest in analyzing proof theory of free logic in recent years, based on intuitionistic logic in [5] as well as classical logic in [6], there for the positive and negative variants.

We present a series of G3 sequent calculi from [6], shown to possess all the desired structural properties of a good proof system [7, 8], including admissibility of contraction and cut, for positive and negative free logic.

While these streamline the presentation of free logics and offer a more unified approach to the variants under consideration, they do not cover neutral free logic, since there is some lack of both clear formal intuitions on the status of formulas with empty names, as well a satisfying account of the conditional in this context. We therefore next discuss extending the results to this third major variant of free logics, while maintaining unification and structural properties, and show that clarity is achieved once neutral free logic is conceptualized as consisting of two sub-varieties.

References

[1] J. Hintikka, *Existential presuppositions and existential commitments*, The Journal of Philosophy, vol. 56, pp. 125–137, 1959.

[2] K. Lambert, *Free logic and the concept of existence*, Notre Dame Journal of Formal Logic, vol. 8, pp. 133–144, 1967.

[3] K. Lambert, *Free logics: Their foundations, character, and some applications thereof*, Sankt Augustin: Academia Verlag, 1997.

[4] K. Lambert, *Free logics*, The Blackwell Guide to Philosophical Logic, pp. 258–279, 2001.

[5] P. Maffezioli and E. Orlandelli, *Full cut elimination and interpolation for intuitionistic logic with existence predicate*, Bulletin of the Section of Logic, vol. 48(2), pp. 137–158, 2019.

[6] E. Pavlović and N. Gratzl, *A more unified approach to free logics*, Journal of Philosophical Logic, vol. 50, pp. 117–148, 2021.

[7] S. Negri and J. von Plato, *Structural proof theory*, Cambridge: Cambridge University Press, 2001.

[8] S. Negri and J. von Plato, *Proof analysis*, Cambridge: Cambridge University Press, 2011.

Natural Deduction for Partial Type Theory with 'Evaluation Terms'

Jiří Raclavský[1], **Petr Kuchyňka**[2]

[1] *Masaryk University, Department of Philosophy*
Arne Nováka 1, Brno 602 00, the Czech Rep.
[2] *University of Defence, Division of Communication and Information Systems*
Kounicova 65, Brno 662 10, the Czech Rep.
E-mail: [1]`raclavsky@phil.muni.cz`, [2]`p.kuchynka@gmail.com`

Keywords:
partial type theory, evaluation terms, natural deduction.

Short abstract:
The talk proposes an expressive natural deduction system in sequent style $\mathsf{ND}_{\mathsf{TT}^*}$ *for a higher-order partial type theory* TT^**.* TT^* *treats both total and partial functions-as-graphs and also acyclic algorithmic computations, called constructions (of certain objects of* TT^**). The system is usable e.g. for the analysis of fine-grained hyperintensionality (see e.g. Tichý 1988, Moschovakis 2005) and meta-logical notions. The basic part is adjusted from Tichý's 1982 convenient natural deduction system for his partial type theory; for other approaches, see e.g. Farmer 1990, Muskens 1995.* TT^* *mainly extends his system by admission of 'evaluation terms' (cf. e.g. Tichý 1988, Farmer 2016, Raclavský 2020). Our* $\mathsf{ND}_{\mathsf{TT}^*}$ *provides all basic rules governing those special constructions. Finally, we sketch a Henkin-style completeness proof for* $\mathsf{ND}_{\mathsf{TT}^*}$*.*

Partial type theory, algorithms/constructions. *Simple type theory* (STT) can be extended by admission of *partial functions*(-as-graphs), which (unlike total functions) are *undefined* for at least one element of their argument domain $\mathfrak{D}$.[1] The result is called *partial TT*; see e.g. Tichý [8], Farmer [1] (an extension of the Church-Andrews STT), Muskens [6] (relational version).

We follow Tichý [9], Moschovakis [5] and some others in understanding terms of partial TT as (a) *expressing acyclic algorithmic computations*, called (by Tichý and us) *constructions*; see e.g. Raclavský [7] for a detailed discussion and applications of the approach. Constructions typically construct (lower-order) objects of the object hierarchy, which are (b) *denoted* by the terms. But some constructions, e.g. $\div(3,0)$, are *improper*: they construct nothing at all (since

[1] Domains $\mathfrak{D}_\tau$ interpret types τ that are paired with STT terms. *Models* are indexed families of sets, $\mathfrak{M} := \{\mathfrak{D}_\tau\}_\tau$.

the binary function $\div$ is undefined for $\langle 3, 0\rangle$) and so the term "$\div(3, 0)$" is *non-denoting*.

Such systems are useful e.g. for the *analysis of natural language* which not only harbours non-denoting expressions (e.g. "the greatest prime", "the King of France") but mainly features *fine-grained hyperintensional meanings* – which are best identified with constructions (some of which construct *possible world intensions*). See e.g. Tichý [9], Moschovakis [5], Raclavský [7].

Enrichment by 'evaluation terms', TT^*. The expressivity of such systems can be increased by an adoption of some form of *'evaluation terms'* (constructions): $\ulcorner C \urcorner$ (*acquisitions*) constructs the construction C as such (not its value) and $[\![C]\!]_\tau$ (*immersions*) constructs the value (of type τ; if any) of the construction (if any) constructed by C. We significantly adjust here the original proposal by Tichý [9] and modify his definitions of *type* and *order.* The type hierarchy of orders prevents circularity (there is no loop in constructing).[2] The language of the resulting TT, which we call TT^*, is (let "$\bar{E}_m$" stand for "$E_1, E_2, ..., E_m$" and "$\tilde{E}_m$" stand for "$E_1 E_2 E_m$", for any entity E_i):

$$\mathcal{L}_{\mathsf{TT}^*} \qquad C ::= x \mid \mathrm{c} \mid C_0(\bar{C}_m) \mid \lambda\tilde{x}_m.C_0 \mid \ulcorner C_0 \urcorner \mid [\![C_0]\!]_\tau$$

(x – *variable*, c – *constant*, $C_0(\bar{C}_m)$ – *application*, $\lambda\tilde{x}_m.C_0$ – λ-*abstraction*)

Natural deduction in sequent style, $\mathsf{ND}_{\mathsf{TT}^*}$. Our main result in this paper is a proposal of an appropriate *natural deduction system in sequent style* for TT^*, i.e. $\mathsf{ND}_{\mathsf{TT}^*}$. We adjusted rules from Tichý's [8] ND, but we especially propose here all main rules that govern $\ulcorner C \urcorner$ and $[\![C]\!]_\tau$.

We discuss various interesting properties of $\mathsf{ND}_{\mathsf{TT}^*}$. Perhaps most notably: its 'signed terms', called *matches*, allow to preserve *monotonicity of logical deduction* and even to develop a Henkin-style *completeness proof* which we sketch in the talk. Matches are *congruence statements* of the general form

$$\mathcal{M} := \ C : \underline{\mathbf{x}},$$

where C is either 'annotated' by $\_$ – saying that C is improper ('non-denoting'), or by $\mathbf{x}$ – saying that C is proper and constructs the object X, or an object in the range of x, or the construction X (acquired by $\ulcorner X \urcorner$). Matches which are indeed (im)proper as just described are called *satisfied by valuation* (= assignement).

Rules $\mathcal{R}$ are made from *sequents*, while sequents are made from matches:

$$\mathcal{S} := \ \Gamma \Rightarrow \mathcal{M},$$

where Γ is a set of matches. $\mathcal{S}$ is *valid* iff every valuation which satisfies all members of its *antecedent* Γ satisfies also its *succedent* $\mathcal{M}$.

To show here at least one example of a *derivation* $\mathcal{D}$ using $\mathsf{ND}_{\mathsf{TT}^*}$, here is a proof of a *derived rule* $\Gamma \Rightarrow X{:}\_ \vdash \Gamma \Rightarrow [\![X]\!]_\tau{:}\_$ (where X, x, y constructs objects

[2] Two remarks. Despite the internal ramification, that TT is not a *ramified TT*, as e.g. Kamareddine et al. [3]. Since Farmer 2016 introduced his evaluation terms only inside an STT without any ramification, his system is rather divergent.

of type τ). Our $\mathcal{D}$ utilises four of $\mathsf{ND}_{\mathsf{TT}^*}$'s main *structural rules*: (WR) – weaking r.; (AX) – axiom r., (EFQ) – 'metalinguistic' ex falso quodlibet r., (EXH) – exhaustation r.; and one of the main rules for 'evaluation terms', ($[\![.]\!]$-INST). So called *instantation rules* (denoted by $\star$-INST) substantially break the symmetry of *introduction* and *elimination rules.* Let $\mathcal{M}_1 := X{:}x$; $\mathcal{M}_2 := [\![X]\!]_\tau{:}y$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \Rightarrow X{:}\_}{\Gamma, \mathcal{M}_1, \mathcal{M}_2 \Rightarrow X{:}\_}\,(\mathrm{WR}) \qquad \dfrac{\dfrac{}{\Gamma, \mathcal{M}_1 \Rightarrow X{:}x}\,(\mathrm{AX})}{\Gamma, \mathcal{M}_1, \mathcal{M}_2 \Rightarrow X{:}x}\,(\mathrm{WR})}{\Gamma, \mathcal{M}_1, \mathcal{M}_2 \Rightarrow [\![X]\!]_\tau{:}\_}\,(\mathrm{EFQ})}{\Gamma, \mathcal{M}_2 \Rightarrow [\![X]\!]_\tau{:}\_}\,([\![.]\!]\text{-INST}) \qquad \dfrac{}{\Gamma, [\![X]\!]_\tau{:}\_ \Rightarrow [\![X]\!]_\tau{:}\_}\,(\mathrm{AX})}{\Gamma \Rightarrow [\![X]\!]_\tau{:}\_}\,(\mathrm{EXH})$$

Acknowledgment

The work on this paper was supported by the grant of the Czech Science Foundation (GAČR) registration no. GA19-12420S, "Hyperintensional Meaning, Type Theory and Logical Deduction".

References

[1] Farmer, W.M.: A Partial Functions Version of Church's Simple Theory of Types. *Journal of Symbolic Logic* 55, 1269–1291 (1990).

[2] Farmer, W.M.: Incorporating Quotation and Evaluation into Church's Type Theory: Syntax and Semantics. In: Kohlhase, M. et al. (eds.) *Intelligent Computer Mathematics. CICM 2016.* LNCS, vol. 9791, pp. 83–98. Springer (2016).

[3] Kamareddine, F.; Laan, T.; Nederpelt, R.: *A Modern Perspective on Type Theory. From Its Origins until Today.* Springer (2004).

[4] Kuchyňka, P., Raclavský, J.: β-reduction-by-name, by-value and η-reduction in Partial Type λ-Calculus/Partial Type Theory. *Logical Journal of IGPL*, cond. accepted (2021).

[5] Moschovakis, Y.N.: A Logical Calculus of Meaning and Synonymy. *Linguistics and Philosophy* 29, 27–89 (2005).

[6] Muskens, R.: *Meaning and Partiality.* CSLI, Stanford (1995).

[7] Raclavský, J.: *Belief Attitudes, Fine-Grained Hyperintensionality and Type-Theoretic Logic.* College Publications (Studies in Logic 88), London (2020).

[8] Tichý, P.: Foundations of Partial Type Theory. *Reports on Mathematical Logic* 14, 57–72 (1982).

[9] Tichý, P.: *The Foundations of Frege's Logic.* Walter de Gruyter, Berlin (1988).

Language Models and Relational Models of the Lambek Calculus

Andre Scedrov

University of Pennsylvania

Language and relational models, or L-models and R-models, are two natural classes of models for the Lambek calculus. Completeness w.r.t. L-models was proved by Pentus and w.r.t. R-models by Andreka and Mikulas. It is well known that adding both additive conjunction and disjunction together yields incompleteness, because of the distributive law. The product-free Lambek calculus enriched with conjunction only, however, is complete w.r.t. L-models (Buszkowski) as well as R-models (Andreka and Mikulas). The situation with disjunction turns out to be the opposite: we prove that the product-free Lambek calculus enriched with disjunction only is incomplete w.r.t. L-models as well as R-models, in the non-commutative as well as the commutative (linear) case. The derivability problem for the Lambek calculus with conjunction and disjunction is known to be decidable. Adding the explicit multiplicative unit constant changes things drastically. Namely, if we extend Lambek calculus with conjunction by certain simple rules for the multiplicative unit, sound in L-models, then the system becomes undecidable, even in the small fragment with only one implication, conjunction, and unit. In the language with the unit, the algebraic logic of all L-models is strictly included in (does not coincide with) the algebraic logic of regular L-models. This is joint work with Max Kanovich and Stepan L. Kuznetsov [1].

References

[1] Kanovich, M., Kuznetsov, S., and Scedrov, A.,*Language Models for Some Extensions of the Lambek Calculus*, Information and Computation, available online 6 May, 2021. DOI: `https://doi.org/10.1016/j.ic.2021.104760`

Radical theory of Scott-open predicates*

Peter Schuster[1], **Daniel Wessel**[2]

[1] *Dipartimento di Informatica, Università degli Studi di Verona*
Strada le Grazie 15, 37134 Verona, Italy
[2] *Mathematisches Institut der Universität München*
Theresienstraße 39, 80333 München, Germany
E-mail: [1]`peter.schuster@univr.it`, [2]`wessel@math.lmu.de`

Keywords:
Scott topology, complete lattice, axiom of choice, Teichmüller-Tukey lemma, ultrafilter theorem, Krull's Lemma, syntactical, computational, constructive, binary tree, inductive definition, Jacobson radical, nucleus.

The *Jacobson radical* $\mathrm{Jac}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ of a commutative ring $\mathbf{A}$ with unit is usually defined as the intersection of the maximal ideals of $\mathbf{A}$ which contain $\mathfrak{a}$:

$$\mathrm{Jac}(\mathfrak{a}) = \bigcap \mathrm{Max}/\mathfrak{a}. \tag{1}$$

With the *Axiom of Choice* (AC), $\mathrm{Jac}(\mathfrak{a})$ has a well-known first-order description:

$$\mathrm{Jac}(\mathfrak{a}) = \{\, a \in \mathbf{A} \mid (\forall b \in \mathbf{A})(\, 1 \in \langle a, b\rangle \to 1 \in \langle \mathfrak{a}, b\rangle)\,\} \ .$$

In constructive algebra, the latter is taken [4] as definition of $\mathrm{Jac}(\mathfrak{a})$; whence (1), which we henceforth refer to as the *Jacobson Lemma* (JL), then becomes a theorem that requires AC. With classical logic, in fact, JL is equivalent to Krull's *Maximal Ideal Theorem* (MIT) that every proper ideal is contained in a maximal one, which in turn is tantamount to AC.

The Jacobson radical can also be defined for distributive lattices [1, 2] and thus in propositional logic [3]. In the complete lattice of ideals I of a distributive lattice D, the Jacobson radical of I is defined by analogy to the case of a ring:

$$\mathrm{Jac}(I) = \{\, a \in D \mid ((\forall b \in D)(\, 1 = a \vee b) \to (\exists c \in I)(\, 1 = c \vee b))\,\} \ .$$

Viewed from the angle of syntax, JL shows a certain consequence relation complete with respect to maximal ideals, and thus helps to pin down the computational import of MIT [5]. This has prompted our motivating question: Can

*The present study was carried out within the project "Reducing complexity in algebra, logic, combinatorics - REDCOM" of the Fondazione Cariverona's programme "Ricerca Scientifica di Eccellenza 2018", and within GNSAGA of INdAM.

we find a syntactical counterpart to maximality principles even closer to AC, among which the *Teichmüller–Tukey Lemma* (TTL), in a manner similar to how JL relates to MIT? The resulting challenge thus is to first solve semantically

$$\frac{\mathrm{JL}}{\mathrm{MIT}} \sim \frac{\textbf{?}}{\mathrm{TTL}} \tag{2}$$

and then to give a syntactical interpretation of the solution.

Abstracting from ideals of a ring $\mathbf{A}$ to elements of a complete lattice L, and from comaximality (i.e., the property of a set of ring elements to generate 1) to a fixed but arbitrary Scott-open subset O of L, we are led to a closure operator

$$j : L \to L$$

which generalises all the aforementioned Jacobson radicals. Apart from comaximality of ideals in rings, a typical Scott-open predicate O is inconsistency of theories in logic. Special cases of j had appeared before, e.g., on lattices [1, 2].

In our general context some key features of j can be isolated by an inductive definition. For instance, j is the largest closure operator on L for which O consists of the j-dense elements of L; also, if L is distributive, then O is a filter precisely when j is a nucleus. With AC, moreover, we can prove the following statements for every $x \in L$, where $y \in L$ is *proper* if $\neg O(y)$, and $y \in L$ is O*-complete* if for every $z \in L$ either $z \leqslant y$ or $O(y \vee z)$:

(a) the radical jx is the meet of all proper O-complete $y \geqslant x$; and

(b) if x is proper, then there is a proper O-complete $y \geqslant x$.

As among the ideals of a ring the proper O-complete ones are just the maximal ideals, (a) and (b) generalise JL and MIT, respectively. Moreover, if the complete lattice L is algebraic, then (b) is a generalisation of TTL.

With (a) we thus obtain the desired semantic solution of (2), and can focus on its syntactical interpretation. To this end we rather put (b) in classically equivalent contrapositive form:

(c) O consists of the $x \in L$ for which every O-complete $y \geqslant x$ belongs to O.

Adapting the recent syntactical treatments of prime ideal theorems [7] and of some fairly concrete maximality principles such as Hausdorff's for maximal chains [6], we define inductively a class of finite binary trees labelled by elements of L, together with an appropriate termination concept for paths. All this allows us to prove constructively—in particular, without AC—the following syntactical counterpart of (c) whenever O is a filter, which normally is the case:

(d) $x \in L$ belongs to O iff there is a labelled finite binary tree with root labelled by x such that every branch of the tree terminates in O.

The feasibility of this syntactical characterisation is not obvious at all: unlike prime ideal theorems, which are of binary nature by the very form of the prime ideal axiom, abstract maximality principles such as (b) or (c) equivalent to full AC a priori fall short of lending themselves naturally to a computational simulation by finite binary trees. Our key idea to overcome this barrier, and in fact to get by with binary branching also in cases of AC proper such as TTL, is to complement every $a \in L$ by the O-variant $\overline{a}$ of the pseudo-complement of a.

Much in the spirit of dynamical algebra [4,8], every tree t with root labelled by x represents the course of a dynamic argument *as if* a given $y \geqslant x$ were complete. Every complete $y \geqslant x$ gives indeed rise to a path through t: at each branching, corresponding to some $a \in L$, by way of completeness either $a \leqslant y$ or $O(a \vee y)$, according to which y leads in the direction to pursue: either a or $\overline{a}$.

References

[1] Thierry Coquand. Compact spaces and distributive lattices. *J. Pure Appl. Algebra*, 184:1–6, 2003.

[2] Thierry Coquand, Henri Lombardi, and Claude Quitté. Dimension de Heitmann des treillis distributifs et des anneaux commutatifs. *Pub. Math. de Besançon. Algèbre et Théorie des Nombres*, pages 57–100, 2006.

[3] Giulio Fellin, Peter Schuster, and Daniel Wessel. The Jacobson radical of a propositional theory. In Thomas Piecha and Peter Schroeder-Heister, editors, *Proof-Theoretic Semantics: Assessment and Future Perspectives. Proceedings of the Third Tübingen Conference on Proof-Theoretic Semantics, 27–30 March 2019*, pages 287–299. University of Tübingen, 2019.

[4] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*, Springer, Dordrecht, 2015.

[5] Peter Schuster and Daniel Wessel. Syntax for Semantics: Krull's Maximal Ideal Theorem. In Gerhard Heinzmann and Gereon Wolters, editors, *Paul Lorenzen: Mathematician and Logician.* Springer. Forthcoming.

[6] Peter Schuster and Daniel Wessel. The computational significance of Hausdorff's Maximal Chain Principle. In Marcella Anselmo, Gianluca Della Vedova, Florin Manea, and Arno Pauly, editors, *Beyond the Horizon of Computability. 16th Conference on Computability in Europe*, volume 12098 of *Lect. Notes Comput. Sci.*, pages 239–250. Springer, 2020. Proceedings, CiE 2020, Fisciano, Italy, June 29–July 3, 2020.

[7] Peter Schuster and Daniel Wessel. Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, pages 820–830, New York, NY, USA, 2020. ACM.

[8] Ihsen Yengui. *Constructive Commutative Algebra. Projective Modules over Polynomial Rings and Dynamical Gröbner Bases*, Springer, Cham, 2015.

Kneale's natural deductions as a notational variant of Beth's tableaus

Zvonimir Šikić

Gentzen's singular sequential system of rst-order logic was an alternative notation for his system of natural deductions. His multiple sequential system was his symmetric generalization that was more appropriate to classical logic. Beth's tableaux system was a system that was derived directly from the semantic analysis of connectives and quan-tifiers. It was soon realized that the Beth's system and the Gentzen's multiple system were only notational variants of each other. Kneale's system of multiple natural deductions was a generalization of Gentzen's system of natural deductions. We prove that Kneale's natural deductions are also a notational variant of Beth's tableaux.

References

[1] E. W. Beth, *Semantic Entailment and Formal Derivability*, Mededelingen van de Koninklijke Nederlandse Akademie van Wetenschappen, Afd. Letterkunde n.s. 18, 309–42, 1955.

[2] E. W. Beth, *The Foundations of Mathematics*, Studies in Logic and the Foundations of Mathematics, North-Holland Publishing Company, Amsterdam 1959.

[3] M. Fitting, *Proof Methods for Modal and Intuitionistic Logics*, D. Reidel Pub- lishing Co., Dordrecht, 1983.

[4] G. Gentzen, *Untersuchungen uber das logische Schlieen I*, Mathematische Zeitschrift, 39 (2), 176–210, 1935.

[5] G. Gentzen, *Untersuchungen uber das logische Schlieen II*, Mathematische Zeitschrift, 39 (3), 405–431, 1935.

[6] W. and M. Kneale, *The Development of Logic, Clarendon Press*, 1962.

[7] M. Maretić, *On multiple conclusion deductions in classical logic*, Mathematical communications, 23 (1), 79–95, 2018.

[8] D. J. Shoesmith, T. J. Smiley, *Multiple Conclusion Logic*, Cambridge University Press, 1978.

Differential Privacy and Applications

Tamara Stefanović [1], Silvia Ghilezan [1,2]

[1] *Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia*
[2] *Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia*

E-mail: [1]tstefanovic@uns.ac.rs, [2]gsilvia@uns.ac.rs

Keywords:
Differential Privacy, Privacy on Graphs, Location Privacy, Blockchain.

The right to privacy is considered as a fundamental right. Data privacy generally concerns whether and how data is shared with a third party, how it is collected and stored, as well as the laws governing data sharing in areas such as health care, education and financial services [3]. The problem of defining the right to privacy gained special importance with the development of information technology. The first definition of privacy is given in Warren and Brandeis's 1890 seminal book, "The Right to Privacy" [9] and it is inspired by new photographic and printing technologies and their influence on citizens' personal life. From that moment, new technologies raised new privacy concerns and brought new meanings of the notion "privacy". Although technology has developed data privacy problems, technology can also help solve them.

In order to deal with these problems, we must formalize them first. Jeannette M. Wing highlighted the importance of formal methods in the domain of data privacy in [6]. Mathematical formulations of different notions of privacy are highly important for guiding the development of privacy preserving technologies.

One of the best-known mathematical formulations of privacy is Differential Privacy proposed by Cynthia Dwork. The idea is to start with a statistical database and an adversary who wants to learn some of the sensitive data from the database. Differential privacy relies on incorporating random noise so that everything an adversary receives is noisy and imprecise. Unlike the early proposed techniques of anonymization, the differential privacy is not a property of a database, it is a property of queries, functions applied on a database.

Definition 1 *[1] Let $\varepsilon > 0$. A mechanism $\mathcal{M}$ is ε-differentially private iff for every pair of adjacent databases D, D' and for every $S \subseteq range(\mathcal{M})$:*

$$Pr[\mathcal{M}(D) \in S] \leq \exp(\varepsilon) Pr[\mathcal{M}(D') \in S],$$

where the probability space is over the coin flips of the mechanism $\mathcal{M}$.

In [4] we have compared different models for privacy preserving. In this paper we deal in more detail with the concept of differential privacy and it's applications. One of the recent applications is differential privacy on graphs [2] implemented in social media and recommendation systems [5]. Another current application is in the domain of location privacy and processing of geolocation data like [7]. Finally, we discuss the latest ideas for application in the blockchain technology [8].

Acknowledgment

This work was partly supported by the Science Fund Republic of Serbia #6526707 AI4TrustBC.

References

[1] Dwork., C. Differential privacy: A survey of results. In Manindra Agrawal, Dingzhu Du, Zhenhua Duan, and Angsheng Li, editors, Theory and Applications of Models of Computation, pages 1–19, Springer, Berlin, Heidelberg, 2008.

[2] Kasiviswanathan S.P., Nissim K., Raskhodnikova S., Smith A. : Analyzing Graphs with Node Differential Privacy. In: Sahai A. (eds) Theory of Cryptography. TCC 2013. Lecture Notes in Computer Science, vol 7785. Springer, Berlin, Heidelberg, 2013.

[3] Solove, D.J. : A taxonomy of privacy. University of Pennsylvania Law Review, 154(3):477–564, 2006.

[4] Stefanovic, T., Ghilezan, S. : An Overview of Mathematical Models for Data Privacy, LAP2020-8th Conference on Logic and Applications, September 21-25, 2020, Dubrovnik, Croatia

[5] Steiner, T. A. : Differential privacy in online dating recommendation systems. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, S. Fricker (Eds.), Privacy and Identity Management. Data for Better Living - Revised Selected Papers (pp. 395-410). Springer. IFIP Advances in Information and Communication Technology Vol. 576 LNCS, 2020.

[6] Tschantz, M. C., Wing, J. M.: Formal methods for privacy. In Ana Cavalcanti and Dennis R. Dams, editors, FM 2009: Formal Methods, pages 1–15, Springer, Berlin, Heidelberg, 2009.

[7] Zhang, J., Xiaokui, X., Xie, X.: PrivTree: A Differentially Private Algorithm for Hierarchical Decompositions. In Proceedings of the 2016 International Conference on Management of Data (SIGMOD '16). Association for Computing Machinery, New York, NY, USA, 155–170, 2016.

[8] Ul Hassan, M., Rehmani, M. H., Chen, J.: Differential privacy in blockchain technology: A futuristic approach. Journal of Parallel and Distributed Computing 145, 2020.

[9] Warren, S.D. and Brandeis., L.D.: The right to privacy. Harvard Law Review, 4(5):193–220, 1890.

A new termination procedure for intuitionistic logic

Matteo Tesi

Scuola Normale Superiore
Piazza dei Cavalieri 7
E-mail: `matteo.tesi@sns.it`

Keywords:
Intuitionistic logic, Intermediate logics, Proof theory, Decidability.

Syntactic decision procedures for propositional intuitionistic logic usually exploit a suitably formulated sequent calculus. The approaches known in the literature (see [3] for an extended survey) usually lack one of the following three properties:

- An easy termination procedure with the extraction of a countermodel from a failed proof search.
- Invertibility of every rule which removes the need for backtracking.
- A syntactic cut-elimination procedure.

Furthermore, they are not modular, in the sense that they cannot be easily extended to intermediate logics. We aim at presenting a new method based on labelled sequent calculi [2] which meets the *desiderata* that we have mentioned.

To start with, we introduce a minor variant with respect to the usual Kripke-style semantics for intuitionistic logic. In particular, we introduce *strict* Kripke models, i.e. models based on finite strict (transitive and irreflexive) orders instead of partial orders.

The standard truth condition for the implication is replaced by the following. $x \Vdash A \to B$ if and only if the two conditions:

1. If $x \Vdash A$, then $x \Vdash B$
2. For all y (if $x < y$ and $y \Vdash A$, then $y \Vdash B$).

hold. The two semantics - the standard one and its strict variant - are easily shown to be equivalent with respect to validity and thus intuitionistic propositional logic proves sound and complete with respect to the strict semantics. This is shown by exploiting the fact that intuitionistic logic enjoys the finite model property [1] and by providing an easy transformation of finite partial orders into finite strict orders and vice versa.

Hence we introduce the following abbreviation:

$$x \Vdash A > B \equiv \text{for all } y \text{ (if } x < y \text{ and } y \Vdash A \text{, then } y \Vdash B)$$

and we show that condition 2. is equivalent to:

$$2'. \text{ For all } y \text{ (if } x < y \text{ and } y \Vdash A \text{ and } y \Vdash A > B \text{, then } y \Vdash B)$$

in every strict intuitionistic model by exploiting the finiteness condition imposed on the frames. The new truth condition 1. + 2′. is used to obtain a labelled sequent calculus $\mathbf{G3I}_<$ in which the rules for the implication $\to$ are obtained through those for the new connective $>$.
In particular, we introduce the following rules:

$$\frac{x : A > B, \Gamma \Rightarrow \Delta, x : A \qquad x : B, x : A > B, \Gamma \Rightarrow \Delta}{x : A \to B, \Gamma \Rightarrow \Delta}\, {\scriptstyle L \to} \qquad \frac{\Gamma \Rightarrow \Delta, x : A > B \qquad x : A, \Gamma \Rightarrow \Delta, x : B}{\Gamma \Rightarrow \Delta, x : A \to B}\, {\scriptstyle R \to}$$

$$\frac{x < y, x : A > B, \Gamma \Rightarrow \Delta, y : A \qquad y : B, x < y, x : A > B, \Gamma \Rightarrow \Delta}{x < y, x : A > B, \Gamma \Rightarrow \Delta}\, {\scriptstyle L >} \qquad \frac{x < y, y : A > B, y : A, \Gamma \Rightarrow \Delta, y : B}{\Gamma \Rightarrow \Delta, x : A > B}\, {\scriptstyle R >,\ y \text{ fresh}}$$

Two (equivalent) formulations of the system are then considered and the usual structural properties, namely admissibility of weakening, invertibility of the rules and admissibility of contraction, are established by induction on the height of the derivations.

Furthermore, we show admissibility of the cut rule arguing by induction on lexicographically ordered triples with primary induction the degree of the cut formula, secondary induction on the range of the cut - a measure introduced in [4] - and ternary induction on the sum of the heights of the derivations of the premises of the cut.

Termination of the calculus $\mathbf{G3I}_<$ is proved by showing that proof search ends and yields either a proof or a (finite) strict countermodel. This result yields both a completeness result and also a decision procedure for intuitionistic logic. In particular, completeness of $\mathbf{G3I}_<$ is formulated as:

$$\mathbf{G3I}_< \vdash \Rightarrow x : A \text{ if and only if } A \text{ is intuitionistically valid}$$

for every label x and every intuitionistic formula A, i.e. a formula not containing the connective $>$. The key point in the construction is that the specific formulation of the rule R> prevents the formation of loops.

Finally, as opposed to other syntactic approaches based on sequent calculi, we show that our method is modular in the sense that it can be extended so as to encompass large families of intermediate propositional logics which enjoy the finite model property such as the logics of bounded depth and Gödel-Dummett logic.

References

[1] Chagrov, A., Zakharyaschev, M., *Modal Logic*, Oxford University Press, 1997.

[2] Dyckhoff, R., Negri, S., *Proof analysis in intermediate logics*, Archive for Mathematical Logic 51, pp. 71-92, 2012.

[3] Dyckhoff, R., *Intuitionistic decision procedures since Gentzen*, in Kahle R., Strahm T., Studer T. (eds) Advances in Proof Theory. Progress in Computer Science and Applied Logic, vol 28. Birkhäuser, Cham., 2016.

[4] Negri, S., *Proof analysis in modal logic*, Journal of Philosophical Logic 34, 507, 2005.

Computable sequences and isometries

Zvonko Iljazović[1], **Lucija Validžić**[2]

[1,2]*Department of Mathematics, University of Zagreb*
Bijenička cesta 30, Zagreb
E-mail: [1]`zilj@math.hr`, [2]`lucija.validzic@math.hr`

Keywords:
computability structure, computable metric space, effective separating sequence, computably categorical metric space.

A *computable metric space* is a triple (X, d, α) such that (X, d) is a metric space and α a dense sequence in (X, d) such that the function $\mathbb{N}^2 \to \mathbb{R}$, $(i, j) \mapsto d(\alpha_i, \alpha_j)$ is computable. We say that α is an *effective separating sequence* in (X, d). Using the sequence α, we can define the notions of a computable point, a computable sequence and a computable compact set in (X, d, α). Now the question is, are those notions uniquely determined by the metric space itself i.e., if β is another effective separating sequence in (X, d), are computable points, computable sequences and computable compact sets in (X, d, β) the same as those in (X, d, α)?

The set of sequences which are computable with respect to a fixed effective separating sequence is a *computability structure* (see [1, 2]) on a metric space. Since the computable points and the computable compact sets are determined by the computable sequences, our previous question can be rephrased as:

Is a computability structure on a metric space unique?

In order to simplify this question, we define an equivalence relation $\sim$ on the set of the effective separating sequences in (X, d). We say that α and β are *equivalent* ([1]), $\alpha \sim \beta$, if α is a computable sequence in (X, d, β) and vice versa. It can be shown that if $\mathcal{S}_\alpha$ and $\mathcal{S}_\beta$ are the sets of computable sequences in (X, d, α) and (X, d, β), then $\alpha \sim \beta$ if and only if $\mathcal{S}_\alpha = \mathcal{S}_\beta$. Hence our goal is to find circumstances under which every two effective separating sequences in a metric space are equivalent.

For example, if $x \in \mathbb{R}$ is a noncomputable number and α a computable sequence of real numbers which is dense in $(\mathbb{R}, d)$, where d is the Euclidean metric, then $(\alpha_i + x)$ is an effective separating sequence but x is computable in $(\mathbb{R}, d, (\alpha_i + x))$ and x is not computable in $(\mathbb{R}, d, \alpha)$. So α and $(\alpha_i + x)$ are not equivalent. On the other hand, it is known that the computability structure on $[0, 1]$ (equipped with the Euclidean metric) is unique (Example 10 in [1]).

One obvious difference between $\mathbb{R}$ and $[0,1]$ is that $[0,1]$ is compact, but there are examples of segments in $\mathbb{R}$ which do not have a unique computability structure, so compactness is not a property that is strong enough to imply uniqueness of a computability structure. Therefore we limit our investigation to effectively compact computable metric spaces, i.e. spaces which are complete and there exists a computable function $\varphi : \mathbb{N} \to \mathbb{N}$ such that

$$X = \bigcup_{i=0}^{\varphi(k)} B(\alpha_i, 2^{-k}),$$

for each $k \in \mathbb{N}$.

A metric space (X,d) is called effectively compact if there exists α such that (X,d,α) is an effectively compact computable metric space. It turns out that if (X,d) is effectively compact, then (X,d,β) is an effectively compact computable metric space for any effective separating sequence β in (X,d) ([1]).

A simple example of an effectively compact metric space which does not have a unique computability structure is (S,d), where S is a unit circle in $\mathbb{R}^2$ and d the Euclidean metric on S. If α is a computable sequence in $\mathbb{R}^2$ which is dense in S and if we take a noncomputable point $x \in S$, there is a rotation f with the center $(0,0)$ such that $f(0,1) = x$ and now $f \circ \alpha$ is an effective separating sequence in (S,d) and x is computable with respect to $f \circ \alpha$, so $\alpha \not\sim f \circ \alpha$.

Notice that one obvious difference between S and $[0,1]$ is that S has infinitely many isometries. In [1] it is shown that if there are only finitely many isometries of the underlying metric space, then an effectively compact metric space has a unique computability structure. We improve this result by proving that if two computability structures share a computable set K which has the property that there are only finitely many isometries f of the underlying metric space such that $f(K) \subseteq K$, then these structures have to be the same.

It is easy to see that if α is an effective separating sequence in (X,d) and f is a surjective isometry of (X,d), then $f \circ \alpha$ is an effective separating sequence. Moreover f maps the computability structure induced by α to the computability structure induced by $f \circ \alpha$. Now if a metric space does not have a unique computability structure, are at least all computability structures on that metric space isometric images of a fixed computability structure?

In order to simplify that question, we define a new equivalence relation. We say that two effective separating sequences α and β are *equivalent up to an isometry* if there exists an isometry of the metric space such that $\alpha \sim f \circ \beta$. A metric space is *computably categorical* if every two effective separating sequences in that space are equivalent up to an isometry (see [3]). So the question now becomes, under which circumstances is a metric space computably categorical?

In [1, 3] it is shown that the Euclidean space $(\mathbb{R}^n, d)$ is computably categorical, but also that there are metric spaces which are not (for example, a segment $[0,\gamma]$, for $\gamma > 0$ left computable, but not computable). However, since for any point of the unit circle there are only finitely many isometries which fix that point, using previously mentioned result, we can easily show that the unit circle is computably categorical.

A general question is what can be said about computable categoricity of an effectively compact metric space (X, d) in the case when there are infinitely many isometries $X \to X$.

In order to generalize the result for circles to arbitrary unions of concentric spheres in $\mathbb{R}^n$, we have proved the result that can be used in a broader way: An orbit of a computable point under the isometries of the underlying effectively compact metric space is a co-computably enumerable set. Using this we prove that effectively compact unions of concentric spheres in $\mathbb{R}^n$ are computably categorical. Furthermore, we prove that the same holds for sets in $\mathbb{R}^3$ that are unions of parallel circles which have centers on the same line which is perpendicular to them.

Acknowledgment

This work has been fully supported by Croatian Science Foundation under the project 7459 CompStruct.

References

[1] Zvonko Iljazović. Isometries and Computability Structures. *Journal of Universal Computer Science*, 16(18):2569–2596, 2010.

[2] Zvonko Iljazović and Lucija Validžić. Maximal computability structures. *Bulletin of Symbolic Logic*, 22(4):445–468, 2016.

[3] Alexander Melnikov. Computably isometric spaces. *Journal of Symbolic Logic*, 78:1055–1085, 2013.

[4] Marian Pour-El and Ian Richards. Computability in Analysis and Physics. *Springer-Verlag, Berlin-Heidelberg-New York,* 1989.

[5] Klaus Weihrauch. Computable Analysis. *Springer, Berlin*, 2000.

[6] M. Yasugi, T. Mori and Y. Tsujji. Effective properties of sets and functions in metric spaces with computability structure. *Theoretical Computer Science*, 219:467–486, 1999.

[7] M. Yasugi, T. Mori and Y. Tsujji. Computability structures on metric spaces. *Combinatorics, Complexity and Logic* Proc. DMTCS96 (D.S. Bridges et al), Springer, Berlin, 351–362, 1996.

4th workshop Formal Reasoning and Semantics (FORMALS 2021)

a satellite workshop of 10th conference Logic and Applications (LAP 2021)

Inter-University Center, Dubrovnik

20–24 September 2021

This workshop is organized within the research project Formal Reasoning and Semantics (FORMALS), supported by Croatian Science Foundation (HRZZ), under the project UIP-2017-05-9219.

The 1st and the 3rd workshop (FORMALS 2018, 2020) were also co-located with Logic and Applications conference (LAP 2018, 2020) in Dubrovnik. The 2nd workshop (FORMALS 2019) was held at the Faculty of Teacher Education, University of Zagreb.

The present workshop consists of the project research group members' talks (T. Ban Kirigin, B. Perak, A. Hatzivelkos, M. Maretić, L. Mikec, T. Adlešić, S. Horvat), some with co-authors outside of the group (S. Bujačić Babić, J. Joosten, M. Vuković), an invited talk (V. Nigam) and contributed talks (L. Conti, Y. Petrukhin, J. Raclavsky).

The workshop is organized in a hybrid form, part of the contributors being present in Dubrovnik, while others participate online.

We are grateful to the directors of LAP for agreeing this workshop to be a part of the conference.

On behalf of the FORMALS project research group,

Tin Perkov

Quine's New foundations and paradoxes

Tin Adlešić

Faculty of Teacher Education, University of Zagreb
Savska cesta 77, Zagreb
E-mail: tin.adlesic@ufzg.hr

Keywords:
Quine's New foundations, Stratification, Russell's paradox, Burali-Forti's paradox, Cantor's paradox

New foundations was introduced by Quine in 1937. as an improvement of Russell–Whitehead's type theory. It was envisioned as a general theory of logical classes; in the spirit of Frege. Eventually it's nature shifted, and today it is viewed as an alternative set theory to ZF.

NF is a set theory which allows universal set, and many more sets which are deemed too large in ZF. Nevertheless, it successfully (as far as we know) forbids common set theoretic paradoxes by a clever constraints imposed on the formula construction.

The main goal of this talk is to briefly explain the development of NF. Starting form easy set theoretical constructions and continue towards more complex notions such as ordinal and cardinal numbers. A big stress will be made on set theoretical paradoxes, and how NF alludes them. Also, brief account of how ordinary mathematics can be described in NF will be presented.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation (HRZZ) under the project UIP-2017-05-9219.

References

[1] Holmes, M. Randall. Elementary set theory with a universal set. Vol. 10. Bruylant-Academia, 1998.

[2] Forster, Thomas E. "Set theory with a universal set. Exploring an untyped universe." Studia Logica 53.4 (1994).

[3] Jensen, Ronald Björn. "On the consistency of a slight (?) modification of Quine's New Foundations." Words and objections. Springer, Dordrecht, 1969. 278-291.

[4] Quine, Willard V. "New foundations for mathematical logic." The American mathematical monthly 44.2 (1937): 70-80.

[5] Beeson, Michael. "Intuitionistic NF Set Theory." arXiv preprint arXiv:2104.00506 (2021).

[6] Whitehead, Alfred N, and Bertrand Russell. Principia Mathematica. Cambridge [England: The University Press, 1925. Print.

Sentiment Potential Analysis

Tajana Ban Kirigin[1], Sanda Bujačić Babić[1], Benedikt Perak[2]

[1] *Department of Mathematics, University of Rijeka*
R. Matejčić 2, 51000 Rijeka, Croatia
[2] *Faculty of Humanities and Social Sciences, University of Rijeka*
Sveučilišna avenija 4, 51000 Rijeka, Croatia
E-mail: [1]`bank@uniri.hr`, `sbujacic@uniri.hr`, [2]`bperak@uniri.hr`

Keywords:
lexical graph analysis, corpus, affective computing, sentiment analysis.

The expression of feelings and moods in language is one of the foundations of social communication and the exchange of personal and cultural values. Humans experience the affective quality of linguistic utterances unconsciously and have difficulty objectively assessing the affective value of an utterance. For a computer this is an even more difficult task. Nevertheless, in recent years there has been a surge of natural language processing (NLP) techniques and resources dealing with the sentiment analysis, *i.e.*, affective and subjective phenomena in text analysis.

Sentiment analysis aims at evaluating generalized feelings that people experience when cognitively processing an utterance, without focusing on a specific class of emotions. It relies on a simplified system of classifying and/or assigning a normalized range of values for a particular affective dimension. Sentiment can be evaluated for words, concepts, multi-word phrases, sentences, paragraphs, or entire texts. However, the basic component of sentiment analysis is a word or a lexeme. Lexemes are symbolic representations of conceptual references to a class of things, psychological states, and sociocultural constructs, their relations, processes, and properties. Some lexemes represent concepts that have a predominantly culturally associated positive feeling, such as: *happiness, freedom, flower,* etc., while some lexemes represent concepts associated with negative feelings, such as: *sadness, evil, agression,* etc.

One of the main problems in assigning sentiment values is the inherent subjectivity of evaluating the sentiment of a text, lexical ambiguity, polysemy, and domain- and culture-specific word sense. We address these problems by integrating the corpus-based syntactic-semantic dependency graph layer, lexical semantic and sentiment dictionaries. We develop a graph method for labeling word senses and identifying the lexical sentiment potential of lexemes.

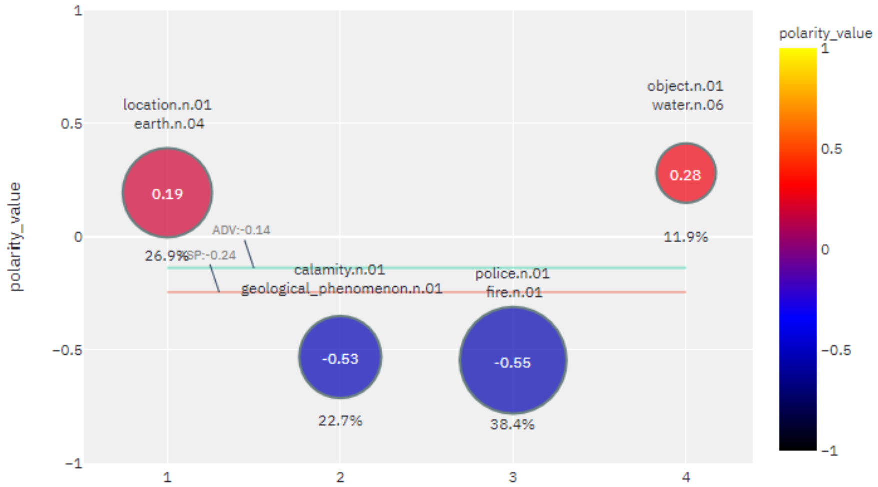

Figure 1: Sentiment potential (*SP*) of lexeme *fire-n* calculated with SenticNet 6 [4] polarity-value; propagated on pruned graph clusters of 15 best ranked collocates in the first degree and 15 collocates in the second degree within ententen13 corpus.

The method, implemented as the ConGraCNet application [2] of the EmocNet project [3] on various languages and corpora, projects a semantic function onto a particular syntactic dependency layer and constructs a seed-lexeme graph with collocates of high conceptual similarity. The seed lexeme graph is clustered into subgraphs that reveal the polysemous semantic nature of a lexeme in a corpus. The construction of the WordNet hypernym graph provides a set of synset labels that generalize the senses for each lexical cluster. By integrating sentiment dictionaries, we introduce graph propagation methods for sentiment analysis. Original dictionary sentiment values are integrated into ConGraCNet lexical graph to compute sentiment values of node lexemes and lexical clusters, and identify the sentiment potential of lexemes with respect to a corpus.

For example, as shown in Figure 1, the sentiment value of the lexeme *fire* is moderately positive when it is considered as a natural entity conceptually related to lexemes such as *water, ice, air, heat, land* or as a concept related to *Earth, sea, sky, moon, sun, planet, universe*. The same lexeme has a more pronounced negative sentiment value when associated with lexemes such as *fire, explosion, police, smoke, theft, rescue* or with natural phenomena such as *flood, earthquake, tornado, storm, landslide, famine, disaster*.

The method can be used to resolve the sparseness of sentiment dictionaries and enrich the sentiment evaluation of lexical structures in sentiment dictionaries by revealing the relative sentiment potential of polysemous lexemes with respect to a given corpus.

Acknowledgment

This work has been supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219 and the University of Rijeka under the project UNIRI-human-18-243.

References

[1] Ban Kirigin, T., Bujačić Babić, S. and Perak, B. *Lexical sense labeling and sentiment potential analysis using corpus-based dependency graph*, Mathematics, 9(12):1449, 2021.

[2] ConGraCNet Application. `https://github.com/bperak/ConGraCNet`

[3] EmoCNet Project. `emocnet.uniri.hr`

[4] Sentic. `https://sentic.net/`

Building a Sentiment Dictionary for Croatian

Tajana Ban Kirigin[1], **Sanda Bujačić Babić**[1], **Benedikt Perak**[2]

[1] *Department of Mathematics, University of Rijeka*
R. Matejčić 2, 51000 Rijeka, Croatia
[2] *Faculty of Humanities and Social Sciences, University of Rijeka*
Sveučilišna avenija 4, 51000 Rijeka, Croatia
E-mail: [1]`bank@uniri.hr`, `sbujacic@uniri.hr`, [2]`bperak@uniri.hr`

Keywords:
lexical graph analysis, corpus, affective computing, sentiment analysis, sentiment dictionary.

In the growing research field of emotions in texts, sentiment lexicons are an important feature for the development of automatic sentiment analysis systems [1, 2, 3, 4]. Sentiment analysis is based on a simplified system of classifying and assigning a normalized range of values for a specific affective dimension, predominantly hedonic valence [5], and others. Assigning a value that can describe the sentiment dimension expressed in a linguistic utterance is at the heart of the process of sentiment analysis. However, apart from the problems related to the subjective nature of value assignment, the resources currently available are rather sparse, especially for low-resource languages such as Croatian.

The work presented in this paper aims to provide the research community with a set of sentiment lexicons constructed by expanding existing sentiment dictionary resources for Croatian. Our corpus-based syntactic dependency graph approach to sentiment value propagation led us to release automatically generated sentiment lexicons. This interdisciplinary dictionary expansion method is structured around the ConGraCNet lexical graph [6, 7], which enables the assignment of sentiment values to a single lexical item or the computation of sentiment values for missing lexemes or entire lexical communities by propagating the values from an existing sentiment dictionary [8]. We present the computational methods and resources used for dictionary expansion as well as the description of the final sentiment dictionary resource.

Acknowledgment

This work has been supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219 and the University of Rijeka under the project UNIRI-human-18-243.

References

[1] Taboada, Maite and Brooke, Julian and Tofiloski, Milan and Voll, Kimberly and Stede, Manfred *Lexicon-based methods for sentiment analysis* Computational linguistics,37, 2: 267-307, 2011.

[2] Cambria, Erik and Li, Yang and Xing, Frank Z and Poria, Soujanya and Kwok, Kenneth *SenticNet 6: Ensemble application of symbolic and subsymbolic AI for sentiment analysis.* Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 105–114, 2020.

[3] Vilares, David and Peng, Haiyun and Satapathy, Ranjan and Cambria, Erik *BabelSenticNet: a commonsense reasoning framework for multilingual sentiment analysis*, 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 1292–1298, 2018.

[4] Sentic. `https://sentic.net/`

[5] Barrett, Lisa Feldman Valence is a basic building block of emotional life, *Journal of Research in Personality*, 40, 1, 35–55, Elsevier, 2006

[6] ConGraCNet Application. `https://github.com/bperak/ConGraCNet`

[7] EmoCNet Project. `emocnet.uniri.hr`

[8] Ban Kirigin, Tajana, Bujačić Babić, Sanda and Perak, Benedikt *Lexical sense labeling and sentiment potential analysis using corpus-based dependency graph*, Mathematics, 9(12):1449, 2021.

Implementing Sentiment Dictionary into Vader sentiment analyis for Croatian

Tajana Ban Kirigin[1], **Sanda Bujačić Babić**[1], **Benedikt Perak**[2]

[1] *Department of Mathematics, University of Rijeka*
R. Matejčić 2, 51000 Rijeka, Croatia
[2] *Faculty of Humanities and Social Sciences, University of Rijeka*
Sveučilišna avenija 4, 51000 Rijeka, Croatia
E-mail: [1]bank@uniri.hr, sbujacic@uniri.hr, [2]bperak@uniri.hr

Keywords:
rule-based sentiment analysis, sentiment dictionary, lexical graph analysis, corpus, affective computing, Vader.

At the heart of inductive rule-based sentiment analysis methods, such as Vader [1], is the sentiment dictionary [2, 3, 4]. A sentiment dictionary consists of values assigned to words representing the subjective class or a normalized range of affective dimensions assigned to a class of things, psychological states and sociocultural constructs, their relations, processes, and characteristics. Obviously, the coverage of a sentiment dictionary is an important feature in the development of computational sentiment analysis methods. A comprehensive sentiment dictionary can be used to compute sentiment values for larger linguistic constructs: multiword phrases, sentences, paragraphs, or entire texts.

This paper describes the adaptation of extended sentiment dictionaries based on a propagation of sentiment values. The method relies on a corpus-based syntactic dependency graph for Vader rule-based sentiment analysis method. This interdisciplinary dictionary expansion method is structured around the ConGraCNet lexical graph [5, 6], which allowes the assignment of sentiment values to a single lexical item or the computation of sentiment values for missing lexemes or entire lexical communities by propagating the values from an existing sentiment dictionary [7]. We describe the processes of 1) sequential propagation of sentiment values of nouns, adjectives, verbs and proper nouns from the multilingual SenticNet 6 sentiment dictionary using ENGRI [8, 9] corpus coordination syntactic-dependency; 2) extrapolation of lemma values to word forms; 3) implementation of the generated sentiment dictionary and Vader rule-based logic on the grammatical structure of Croatian sentence sentiment analysis.

Although Vader has been modified to work with multiple languages using translation [10] and adapted in several languages [11, 12, 13], to the best of our knowledge, this is the first attempt to implement a dictionary resource and adapt the grammar logic to a rule-based sentiment analysis tool Vader for the Croatian language. The work presented in this paper aims at providing the research community with a tool that can be used to extend the range of sentiment analysis tools and resources for the Croatian language.

Acknowledgment

This work has been supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219 and the University of Rijeka under the project UNIRI-human-18-243.

References

[1] Hutto, Clayton and Gilbert, Eric, *Vader: A parsimonious rule-based model for sentiment analysis of social media text*, Proceedings of the International AAAI Conference on Web and Social Media, 8, 1, 2014.

[2] Taboada, Maite and Brooke, Julian and Tofiloski, Milan and Voll, Kimberly and Stede, Manfred *Lexicon-based methods for sentiment analysis* Computational linguistics,37, 2: 267-307,2011.

[3] Cambria, Erik and Li, Yang and Xing, Frank Z and Poria, Soujanya and Kwok, Kenneth *SenticNet 6: Ensemble application of symbolic and subsymbolic AI for sentiment analysis.* Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 105–114,2020.

[4] Sentic. `https://sentic.net/`

[5] ConGraCNet Application. `https://github.com/bperak/ConGraCNet`

[6] EmoCNet Project. `emocnet.uniri.hr`

[7] Ban Kirigin, Tajana, Bujačić Babić, Sanda and Perak, Benedikt *Lexical sense labeling and sentiment potential analysis using corpus-based dependency graph*, Mathematics, 9(12):1449, 2021.

[8] Bogunović, Irena i Mario Kučić. *Korpus hrvatskih novinskih portala ENGRI.* Pomorski fakultet, `https://urn.nsk.hr/urn:nbn:hr:187:920822`, 2021.

[9] Bogunović, Irena; Kučić, Mario; Ljubešić, Nikola and Erjavec, Tomaž, *Corpus of Croatian news portals ENGRI (2014-2018)*, Slovenian language resource repository CLARIN.SI, `http://hdl.handle.net/11356/1416`, 2021.

[10] `https://github.com/brunneis/vader-multi`

[11] Tymann, Karsten and Lutz, Matthias and Palsbröker, Patrick and Gips, Carsten, *GerVADER-A German Adaptation of the VADER Sentiment Analysis Tool for Social Media Texts.*, LWDA, 178–189, 2019

[12] Vilares, David and Peng, Haiyun and Satapathy, Ranjan and Cambria, Erik *BabelSenticNet: a commonsense reasoning framework for multilingual sentiment analysis*, 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 1292–1298, 2018.

[13] Shim, Jae-Geum and Ryu, Kyoung-Ho and Lee, Sung Hyun and Cho, Eun-Ah and Lee, Yoon Ju and Ahn, Jin Hee, *Text Mining Approaches to Analyze Public Sentiment Changes Regarding COVID-19 Vaccines on Social Media in Korea*, International Journal of Environmental Research and Public Health, 18, 12, 6549, Multidisciplinary Digital Publishing Institute, 2021.

Abstraction's Logicality and Invariance

Ludovica Conti

September 15, 2021

In this talk, I aim at discussing a criterion that has been recently suggested in order to prove the logicality of the abstraction operators, when they are understood as arbitrary expressions. My double aim is to inquiry whether this criterion is sufficient to achieve this goal and to use it in order to compare second-order and first-order abstraction principles.

1 Abstraction, Logicality and Invariance

Abstractionist theories are composed by a logical core augment with an abstraction principle, of form: $@_R\alpha = @_R\beta \leftrightarrow R(\alpha, \beta)$ – which introduces and rules an operator term-forming ($@_R$) as a new symbol of the language. Then, the logicality of such theories plainly depends on the logicality of the abstraction principles. The issue of their logicality originally was risen into the seminal abstractionist program, Frege's Logicism. The inconsistency of this project (i.e. a theory equivalent to second-order logic augmented with Basic Law V) seemed to determine the inconsistency and, then (in a classical logic) the non-logicality of Basic Law V and – *a fortiori* – and of the extensions as related abstracts objects.

Recently, the issue of the logicality has been resumed regarding the consistent abstraction principles, in order to clarify that conclusion in light of the intervening studies about logicality. For example, a standard account of logicality has been provided, in semantical terms, by means of the Tarskian notions of invariance under permutation and isomorphism (cfr. [5]). More precisely, in an abstractionist context, the logicality issue can be divided in two horns: on the one hand, the inquiry on the logicality of the abstraction principles; on the other hand, the more controversial issue of the logicality of the abstract objects. I will preliminary argue that these questions can be reduced to those of the logicality respectively of the abstraction relations and of the abstraction functions.

Regarding the abstraction principle, the more informative criterion consists of *contextual invariance*: an abstraction principle AP is *contextually invariant* if and only if , for any abstraction function f_R: $D_2 \to D_1$ and permutation π, $\pi(f_R)$ satisfies AP whenever f_R does (cfr. [1]). I argue that this criterion is not adequate to state the logicality of a principle. I suggest two argument in support of this hypothesis. Firstly, it under-determines the choice between principles that are mutually inconsistent (like Hume's Principle and Nuisance's principle). Secondly, such criterion appears to be – both formally and conceptually dependent on the fulfilment of constraints concerning the abstraction relation: it is provably implied[1] by the weakest form of invariance[2] of the abstraction relation; furthermore, a careful review of the

[1] Cfr. Antonelli 2010, proposition 9: "Suppose R is weakly invariant and D_2 is π-closed; then the principle Ab_R is contextually invariant."

[2] A relation R is *weakly invariant* if and only if, for any permutation π, R(X,Y) if and only if R($\pi[X], \pi[Y]$)

syntactical structure of the abstraction principles shows that abstraction relation is the real "engine" of the abstraction principle.

Regarding the abstraction relation, we can distinguish, at least, four kinds of invariance: *weak invariance*, *double invariance*, *internal invariance* and *double weak invariance* (cfr. [1], [3], [4].). I briefly describe their mutual relations and emphasise that, regarding abstraction relations, a very relevant meaning of logicality is provided in terms of *internal invariance*: an equivalence relation $R(X, Y)$ is *internally invariant* if and only if, for any domain D and permutation $\pi : X \cup Y \to D$, $R(X, Y)$ if and only if $R(\pi[X], \pi[Y])$.

As anticipated *weak invariance* of the abstraction relation is sufficient to have a *contextually invariant* abstraction principle but none of these criteria coincides with or implies the invariance of the abstraction operator.

2 Abstraction operator

Regarding the canonical reading of the abstraction operator, logicality is usually spelled out in terms of *objectual invariance*[3]. Such criterion fails precisely in case of operators related to invariant relations (cf. [1]).

In light of the arbitrary interpretation of the abstraction operator, a new criterion – which we will call *weak invariance* – has been proposed[4]: it consists of a generalised version of the Tarskian isomorphism invariance and turns out to be satisfied, at least on some domains, by all the abstraction operators that index the equivalence classes of partitions obtained by invariant equivalence relation (cf. [7]) and by the (so-called contextually) invariant abstraction principles. If we accepted such criterion of logicality, we would be able to classify many abstraction operators as logical symbols.

My first aim consists in further clarify this criterion – derived (in informal terms) from the standard criterion of isomorphism invariance only by substituting the canonical notion of reference with the arbitrary one. Firstly, I will formally prove that *weak invariance* of the arbitrary denotation of an abstraction operator is nothing but the contextually invariance of the abstraction principle respect to all the possible non-arbitrary denotations of the same operator. We can define all the possible precisifications of the operator on a certain domain as the ordered pair comprising the domain and the choice of a possible (non-arbitrary) denotation of the abstraction operator. Then, we can prove that the arbitrary denotation of the operator is *weakly invariant* on a domain D if and only if every precisification on D makes the principle contextually invariant. Secondly, I will suggest that *weak invariance* do not actually depends only on the arbitrary reading of the abstraction operators but on a specific way of modelling such sort of reference, i.e. as a collection of objects. I will recap different (e.g. semantical, epistimic and metaphysical) meanings of arbitrariness and show that only the first one seems to be plainly able to determine an invariant denotation (cf. [7]). Both epistemic and metaphysical arbitrariness become able to provide the same result only by accepting a non-obvious way of modelling reference as a collection of candidate objects (cf. [2]).

My second aim will consists of considering and eventually answering to some objections pointing against the adoption of such criterion – also in an adequate interpretation of the arbitrariness – as a hallmark of logicality. I will compare the satisfiability of the criterion of

[3] An abstraction operator @ is *objectually invariant* if and only if for any domain D and permutation π of D, $\pi(@_R) = @_R$ – namely, $@_R(\pi(X)) = \pi(x) \leftrightarrow @_R(X) = x$.

[4] Such criterion is available in [7] and [2]: given an isomorphism i from a domain D, let i^+ such that for every set γ of objects from D, $i^+(\gamma) = \{i(x) : x \in \gamma\}$. Then, an expression ϕ is invariant just in case, for all domains D, D' and bijections i from D to D', the denotation of ϕ on D (ϕ^D) is such that $i^+(\phi^D) = \phi^{D'}$.

weak invariance by the abstraction operators and by other variable-binding operators, like ι, ϵ and η (cf. [7]) – which, for brevity, we will call "choice operators". Firstly, the abstraction operators – differently from the choice operators – are not *total*, namely they turn out to be empty whether evaluated on some domains; secondly, logicality (weak invariance) of the abstraction operators do not coincide – differently from the logicality of the choice operators – with their purely logical definability (cf. [6]); thirdly, while the logicality of the choice operators seems to formalise a property of a whole class of similar expressions, then of the intuitive notion of choice, on the contrary, the logicality of the abstraction operators seems to regard only second-order abstraction principles, by excluding any first-order abstraction operator. Such result will be proved as a consequence of a Tarski's theorem about first-order predicates ([5]) and the abovementioned link between *weak invariance* of the abstraction operators and isomorphism invariance of the corresponding equivalence relations ([7]).

However, the weakness of such criterion turns out to identify the crucial meaning of an *undemanding* or *deflationist* interpretation of abstraction (cfr. [1], [7]) – by reducing function symbols to devices for selecting first-order representatives of equivalence classes. For this reason, I suggest to consider such weakened criterion as the formalisation of the necessary semantical condition of the second-order abstraction. I will support this hypothesis by the evidence that, while other logicality criteria are satisfied also by inconsistent abstraction principles[5], such criterion regarding abstraction operator is satisfied by all and only the consistent ones.

2.1 First-order Abstraction

In the last part of the talk, I will compare two schemas of, respectively, second-order and first-order abstraction principles, in order to explore whether some of the limitations mentioned above could be overcome by the adoption of a schematic setting ([4], [7]). On the one side, a schematic second-order abstraction principle – of form $\S(RF) = \S(RG) \leftrightarrow R(F, G)$, where § is a binary abstraction operator and E any isomorphism invariant equivalence relation – defines an abstraction function from $\wp(\wp(D) \times \wp(D)) \times \wp(D) \to D$ that satisfies the criterion of weak invariance and – differently from the specific unary operators – is total ([7]). On the other side, I will focus a schematic first-order abstraction principle – of form $\S(Ra) = \S(Rb) \leftrightarrow R(a, b)$, where § is a binary abstraction operator and E any first-order equivalence relation – and I will show that the abstraction function from $\wp(D \times D) \times D \to D$ that it defines is – differently from the corresponding unary operators – total, but not isomorphism invariant.

References

[1] Antonelli, G. A. (2010). Notions of invariance for abstraction principles. Philosophia Mathematica, 18(3), 276-292.

[2] Boccuni, F., Woods, J. (2018). Structuralist neologicism. Philosophia Mathematica, 28(3), 296-316.

[3] Cook, R. (2016).Abstraction and Four Kinds of Invariance (Or: What's So Logical About Counting), Philosophia Mathematica, 25,1, 3–25.

[4] Fine, K. (2002). The limits of abstraction. Clarendon Press.

[5] Tarski, A. (1956). The concept of truth in formalized languages. Logic, semantics, metamathematics, 2(152-278), 7.

[6] Tennant, N. (1980). On ϵ and η. Analysis 40 (1): 5.

[5] For example, the criterion of *weak invariance* of the equivalence relation is satisfied by the relation of order-isomorphism included in ordinal abstraction – which is inconsistent.

[7] Woods, J. (2014). Logical indefinites. Logique et Analyse, 277-307.

A Note about Disapproval Voting

Hatzivelkos A.[1] and Maretić M.[2]

[1]University of Applied Sciences Velika Gorica, Croatia
[1]The Faculty of Organization and Informatics, Croatia

September 15, 2021

Keywords:

Approval voting, Plurality count, compromise, compromise axiom, Veto vote

One of the common objections to the social choice methods based on linear rankings of the candidates, is that they require too much involvement of the voters. Each voter is required to provide full linear ranking of all candidates, which can be demanding process when there is larger number of candidates. Therefore, there is a demand for providing social choice methods that are based on some partial expression of voters preference.

On the other hand, main interest of our research is a notion of compromise in social choice theory [2, 3, 4]. Since social choice functions presented in [3] are defined over profile of strict linear orderings of the candidates, it was natural next step to explore possible modifications of those methods, such that they are defined over some partial expression of voters preferences. With that goal we are introducing following definition:

Definition 1. [Disapproval score] Let there is a set of k candidates $M = \{M_1, ..., M_k\}$, and n voters. Let $p \in \langle -\infty, 0]$ be a "factor of disapproval". Each voter selects two disjoint subsets of M: subset of all candidates s/he approves A_i, and subset of all candidates s/he disapproves D_i. Collection of those subsets over all voters constitutes a profile α. For each candidate M_k and i-th voter we define:

$$\delta_{k,i} = \begin{cases} 1, & M_k \in A_i \\ p, & M_k \in D_i \\ 0, & M_k \notin A_i \cup D_i \end{cases}$$

Now we define desapproval score for each candidate M_k:

$$DS(M_k) = \sum_{i=1}^{n} \delta_{k,i}.$$

The result of social welfare function Disapproval vote (DV) is (weak) ordering of candidates with respect to their Disapproval score (DS), where candidate with greatest DS is placed first.

Value of parameter p allows DV to approach to the notion of compromise as to the version of Sorites paradox, as presented in [2].
Disapproval vote can be viewed as a generalization of both Approval vote (AV) and Plurality count (PC). Following holds:

- If for every i, set A_i is singleton, and set D_i is empty, then DV equals to PC.

- If for every i, set D_i is empty, then DV equals to AV.

Furthermore, DV offers a formalization of the concept of Veto vote, that is a social welfare (choice) function in which every voter can eliminate one, or more candidates from winning position, regardless of that candidate positions in other preferences of the profile. Such system is achieved when $p \to -\infty$.

With respect to the motivation for definition of such social welfare function, we analyzed if it satisfy Compromise Axiom [4].

Definition 2. Social choice function Φ satisfies a (weak) Compromise Axiom if on every set of three or more candidates, there is a profile of preferences α, such that a set of winning candidates of social choice function Φ contains a candidate which is not placed first in any preference of the profile α.

Since profile of DV is not collection of linearly ordered preferences, interpretation of Compromise Axiom is needed. But such interpretation is natural: a set of winning candidates from CA is set A_i. With that interpretation we can show that DV satisfy CA iff $p \leq -1$.

Regarding other axioms of social choice theory, DV possesses many properties similar to AV. It can be proven that it is positively responsive (monotone) for all values of p; DV satisfies Pareto Axiom and Independence of Irrelevant Alternatives (IIA). Future study of the subject would include analysis of tactical voting methods that can be used against DV (such as Bullet voting, when AV is in question) [1], and relationship between DV and some other methods it shares similarities with (such as Negative voting) [5].

Acknowledgements: This work has been supported in part by Croatian Science Foundation under the project UIP-05-2017-9219 and by the University of Applied Sciences Velika Gorica.

References

[1] Brams, S. and Fishburn, P.: *Approval Voting*, New York: Springer (2007)

[2] Hatzivelkos A.: *Borda and plurality comparison with regard to compromise as a Sorites paradox*, Interdisciplinary description of complex systems, 16 (2018), 3-B; pp. 465-484 doi:10.7906/indecs.16.3.18

[3] Hatzivelkos A.: *The Mathematical Look at a Notion of the Compromise and Its Ramifications*, Central European Conference on Information and Intelligent Systems, Strahonja, V.; Kirinić, V. (ed.), Varaždin: Faculty of Organization and Informatics, University of Zagreb, (2017) pp. 301-308

[4] Hatzivelkos A.: *Axiomatic approach to the notion of compromise*, Proceedings of the 21st International Conference on Group Decision and Negotiation, Fang, L.; Morais, D.C.; Horita, M. (ed.), Toronto: Ryerson University, (2021) pp. 191-203

[5] Pacuit, E., *Voting Methods*, The Stanford Encyclopedia of Philosophy (Fall 2019 Edition), Edward N. Zalta (ed.)

Bisimulation games for (generalized) Veltman semantics

Sebastijan Horvat

Department of Mathematics, Faculty of Science, University of Zagreb
Bijenička cesta 30, Zagreb, Croatia
E-mail: sebastijan.horvat@math.hr

Bisimulation relations in logic may be understood as descriptions of (nondeterministic) winning strategies for one player in corresponding model comparison games. In case of bisimulations for basic modal logic that was illustrated in [2]. In case of bisimulations for provability logic that was done in [1]. Čačić and Vrgoč in [1] used games on Veltman models to show that modal equivalence does not imply bisimilarity.

In this talk, we will give an overview of use of bisimulation games in known results for Veltman semantics. Since Veltman semantics is not fine-grained enough for certain application, the notion of generalised Veltman semantics emerged to obtain certain non-derivability results. It has turned out that this semantics has various good properties (see e.g. [3] and [4]). Because of that, we will define bisimulation games (and their finite approximation - n-bisimulation games) for generalised Veltman semantics. We will alse prove the standard result - equivalence between the existence of a winning strategy in the bisimulation game and the existence of an bisimulation in case of generalised Veltman semantics.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation (HRZZ) under the projects UIP-05-2017-9219 and IP-01-2018-7459.

References

[1] V. Čačić, D. Vrgoč, *A Note on Bisimulation and Modal Equivalence in Provability Logic and Interpretability Logic*, Studia Logica 101(2013), 31–44

[2] V. Goranko, M. Otto, *Model theory for modal logic*, In: P. Blackburn P., J. van Benthem, F. Wolter (eds.) Handbook of Modal Logic, pp.249-329, Elsevier, Amsterdam (2006)

[3] J. J. Joosten, J. Mas Rovira, L. Mikec, M. Vuković, *An overview of Generalised Veltman Semantics*, to appear

[4] L. Mikec, M. Vuković, *Interpretability logics and generalized Veltman semantics*, The Journal of Symbolic Logic, 85(2020), 749–772

On proving interpretability principles arithmetically sound

Luka Mikec Joost J. Joosten Albert Visser
Mladen Vuković

September 22, 2021

Proving the soundness of a modal principle A w.r.t. some theory T translates to proving that all so-called arithmetical realisations A^* are provable in T, i.e. $T \vdash A^*$. However, we are rarely interested in just one theory T; usually the intention is to prove soundness (and completeness) w.r.t. a large class of theories, for example the principle **P** and the class of finitely-axiomatisable Σ_1-sound theories extending $I\Delta_0 + \mathsf{SUPEXP}$ [7], or the principle **M** and the class of essentially reflexive Σ_1-sound theories [6], [1].

The wider the class of theories, the less can be said about the theories within the class. In particular, the class of *all* sequential theories is studied often. Joosten and Visser showed [4] that, despite the size of this class of theories, there are simple ways to prove the soundness for many principles in this class. These methods induce semi-formal systems seemingly related to the aforementioned principles **M** and **P**, which is somewhat surprising as **M** and **P** are *not* sound in this class themselves. In fact, many proofs using **M** and **P** can be adapted for these semi-formal systems using an almost mechanical straightforward procedure. Of course, this cannot be done if these principles were used in an essential way in the proof that is being converted.

In [5] the approach of [4] is extended, and a paper [3] is worked on. The new results concern certain series of principles introduced in [2] and [5]. In this talk we will present some new results developed in [5] that concern arithmetical soundness.

References

[1] A. Berarducci. The interpretability logic of peano arithmetic. *The Journal of Symbolic Logic*, 55(3):1059–1089, 1990.

[2] Goris, E. and J. Joosten, *Two new series of principles in the interpretability logic of all reasonable arithmetical theories*, The Journal of Symbolic Logic **85** (2020), pp. 1–25.

[3] Joosten, J., L. Mikec and A. Visser, *Feferman axiomatisations, definable cuts and principles of interpretability*, forthcoming (2020).

[4] Joosten, J. and A. Visser, *How to derive principles of interpretability logic, A toolkit*, in: J. v. Benthem, F. Troelstra, A. Veltman and A. Visser, editors, *Liber*

Amicorum for Dick de Jongh, Intitute for Logic, Language and Computation, 2004 Electronically published, ISBN: 90 5776 1289.

[5] L. Mikec. *On logics and semantics for interpretability*. PhD thesis, 2021. University of Barcelona and University of Zagreb.

[6] V.Y. Shavrukov. The logic of relative interpretability over Peano arithmetic. Preprint, Steklov Mathematical Institute, Moscow, 1988. In Russian.

[7] A. Visser. Interpretability logic. In P.P. Petkov, editor, *Mathematical Logic, Proceedings of the Heyting 1988 summer school in Varna, Bulgaria*, pages 175–209. Plenum Press, Boston, New York, 1990.

Soft-Agents: A Symbolic Verification Framework for Cyber-Physical Systems

Vivek Nigam

Federal University of Paraíba, João Pessoa, Brazil
& Munich Research Center, Huawei, Germany

Cyber-physical systems are being deployed in safety-critical missions such as applications involving robots, drones, and bots. As their complexity increases, it becomes harder to ensure their well-behavior. In this talk, we describe the rewriting logic framework Soft-Agents for the symbolic specification and verification of such systems. In particular, an agent behavior is reduced to a soft-constraint solving problem. Moreover, these specifications can be executed using the rewriting tool Maude. For verification, we demonstrate how to reduce the checking of verification properties to the checking of satisfiability problems involving non-linear arithmetic constraints.

Normalisation for some infectious logics with non-standard disjunction elimination rules

Yaroslav Petrukhin
University of Lodz

September 15, 2021

Abstract

In this report, we consider natural deduction systems with non-standard disjunction elimination rules for infectious logics and prove normalisation theorem for them.

Infectious logics form a special class of many-valued logics which have the so called infectious value: if an argument of a logical connectives is infectious, then the hole connective is infectious as well. It can be illustrated, e.g., by the following matrices by Deutsch [3]:

A	$\neg$
T	F
B	B
N	N
F	T

$\wedge$	T	B	N	F
T	T	B	N	F
B	B	B	N	F
N	N	N	N	N
F	F	F	N	F

$\vee$	T	B	N	F
T	T	T	N	T
B	T	B	N	B
N	N	N	N	N
F	T	B	N	F

We can see that the value N is infectious here. If under some valuation v for some formula A_i we have $v(A_i) = \mathtt{N}$ $(i \in \{1, 2\})$, than $v(\neg A_i) = \mathtt{N}$, $v(A_1 \wedge A_2) = v(A_1 \vee A_2) = \mathtt{N}$. Notice that if we consider the values T and B as designated, then we get Deutsch's logic $\mathbf{S_{fde}}$ [3].

In a recent paper [1], Belikov offered natural deduction systems for $\mathbf{S_{fde}}$ and yet another infectious logic $\mathbf{dS_{fde}}$ by Szmuc [9]. The logic $\mathbf{S_{fde}}$ has already had a natural deduction system suggested by Petrukhin [6], while $\mathbf{dS_{fde}}$ does not. Belikov compares his natural deduction system for $\mathbf{S_{fde}}$ with Petrukhin's and concludes that his system is better, since it has a standard disjunction elimination rule, while Petrukhin's system has the following rule:

$$\dfrac{A \vee B \qquad \begin{array}{c}[A \wedge \neg B]\\ C\end{array} \qquad \begin{array}{c}[\neg A \wedge B]\\ C\end{array} \qquad \begin{array}{c}[A \wedge B]\\ C\end{array}}{C}$$

At that Belikov's system needs two more rules for disjunction which were not required in Petrukhin's calculus:

$$\frac{A \vee B}{A \vee \neg A} \qquad \frac{A \vee B}{B \vee A}$$

Both authors establish soundness and completeness theorems for their systems, but ignore normalisation theorem which is an analogue of cut elimination for natural deduction and is very important from proof-theoretical point of view. In this talk, we would like to fill this gap. Using the methods from [5], we a bit modify Petrukhin's rules for $\mathbf{S_{fde}}$ to make them more suitable to proof-theoretic investigation (but do not change his version of disjunction elimination) and present the proof of normalisation theorem for it as well as establish that it has the negation subformula property. As for Belikov's system, we show that the rule $A \vee B / B \vee A$ blocks normalisation and destroys the subformula property. Thus, we conclude that although standard disjunction elimination rule is more convenient, non-standard ones can be more useful for infectious logics from a proof-theoretically point of view, since despite of their shape the natural deduction systems with them enjoy normalisation theorem.

The above mentioned non-standard disjunction elimination rule was used also in [8] in a natural deduction system for a three-valued logic $\mathbf{K_3^w}$ (known as weak Kleene logic [4], it is also a fragment of Bochvar's logic $\mathbf{B_3}$ [2]). Thus, we examine $\mathbf{K_3^w}$ as well and prove normalisation for it. Additionally, we consider infectious logics from [7]. These logics have various disjunction elimination rules, we present one of them as an example:

$$\frac{A \vee B \qquad \begin{matrix}[A][\neg B]\\ C\end{matrix} \qquad \begin{matrix}[\neg A][B]\\ C\end{matrix} \qquad \begin{matrix}[A][B]\\ C\end{matrix}}{C}$$

where $\begin{matrix}[D][E]\\ F\end{matrix}$ is understood as follows: F is derivable from the assumption D or the assumption E. We show that normalisation theorem holds for all the infectious logics from [7].

References

[1] Belikov A. On bivalent semantics and natural deduction for some infectious logics. Logic Journal of the IGPL. (2021). Online first article. DOI: 10.1093/jigpal/jzaa071

[2] Bochvar, D.A., 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 (1981): 87-112. (English translation of the paper by 1938).

[3] Deutsch, H., Relevant analytic entailment, The Relevance Logic Newsletter 2(1) (1977): 26–44.

[4] Kleene, S. C., On a notation for ordinal numbers, The Journal of Symbolic Logic, 3 (1938): 150-155.

[5] Kürbis, N., Petrukhin, Y. Normalisation for Some Quite Interesting Many-Valued Logics. Logic and Logical Philosophy, (2021): online first article.

[6] Petrukhin, Y.I. Natural deduction for Fitting's four-valued generalizations of Kleene's logics. Logica Universalis. 11(4) (2017): 525–532.

[7] Petrukhin, Y. Natural deduction for four-valued both regular and monotonic logics. Logic and Logical Philosophy. 27(1) (2018): 53–66.

[8] Petrukhin, Y. Natural deduction for three-valued regular logics. Logic and Logical Philosophy 26(2) (2017): 197–206.

[9] Szmuc, D.E.: Defining LFIs and LFUs in extensions of infectious logics. Journal of Applied Non-Classical Logics 26(4) (2017): 286–314.

The Rule of Existential Generalisation, Its Derivability and Formal Semantics

Jiří Raclavský[1]

[1] *Masaryk University, Department of Philosophy*
Arne Nováka 1, Brno 602 00, the Czech Rep.
E-mail: [1]`raclavsky@phil.muni.cz`

Keywords:
existential generalisation, natural deduction,explicit substitution, fine-grained hyperintensionality.

My contribution addresses three problems concerning *existential generalisation* (EG). My solutions to the problems are framed within a higher order *partial type theory* TT^* that is equipped with a *natural deduction* system in sequent style $\mathsf{ND}_{\mathsf{TT}^*}$.

Problem 1 (Which rule exactly is (EG)?) In logical textbooks and even advanced writing such as Prawitz [1], Negri et al. [2], the ordinary rule (EG) of *natural deduction* (ND) occurs in the following three variants. (I write λx, borrowed from λ-calculus, instead of sole x; $\varphi_{(t/x)}$ reads "φ in which t is *substituted* for x"; φ is a formula, F is a predicate, t a term, x a variable, $\exists$ is the existential quantifier as a 'predicate', $\lambda x.F(x)$ denotes the set of objects x of which $F(x)$ is true.)

$$(\exists\text{-I})\ \frac{F(t)}{\exists(F)} \qquad (\text{EG})\ \frac{\varphi_{(t/x)}}{\exists(\lambda x.\varphi)} \qquad (\exists\text{-I}^{\eta})\ \frac{F(t)}{\exists(\lambda x.F(x))}$$

Problem 2 (Is (EG) a primitive rule or a derivable one?) As indicated by the labels ($\exists$-I), (EG) and ($\exists$-I$^{\eta}$), I consider only one of them being the proper *Rule of Existential Generalisation*, (EG). ($\exists$-I$^{\eta}$) is a variant of the *Rule of* $\exists$*-Introduction*, ($\exists$-I), whose bottom formula is an η-expanded form of ($\exists$-I)'s bottom formula.[1] The choice of (EG) is determined by several logical facts, (F1) – (F4).

Solution to Problem 1 (partiality, explicit substitution)
(F1) ($\exists$-I) cannot be eliminated in *partial logic/partial TT* (TT stands for

[1] By the η-rule of λ-calculus: $F \dashv\vdash \lambda x.F(x)$, where $\dashv\vdash$ indicates variants with $\vdash$ and $\dashv$.

type theory), since it is not interdefinable with ∀ because of *partiality* (see e.g. [5]), i.e. the fact that some expressions are *non-denoting*, e.g. because they express an application of a *partial function* f to an argument for which f is not defined (cf. e.g. "$3 \div 0$"). Thus, (∃-I) is a *primitive rule* of ND for PTT.

(F2) (EG) contains the *substitution operator* (t/x) which can be treated either (a) as a metalinguistic device (then (EG) 'collapses' to (∃-I$^\eta$)), or (b) as a genuine operator of our higher-order logic, as is common in current type theory/λ-calculus (*explicit substitution*). I pursue the latter option, borrowing the essential idea from Tichý [8], while I use a (substantial) modification of his TT with '*evaluation terms*' (one serves as a sort of quotation, one as a picking of some term's denotation). I call the logical system TT^*, its language is

$$\mathcal{L}_{\mathsf{TT}^*} \qquad C ::= x \mid \mathrm{c} \mid C_0(\bar{C}_m) \mid \lambda\tilde{x}_m.C_0 \mid \ulcorner C_0 \urcorner \mid [\![C_0]\!]_\tau$$

where each C (not "C") is not simply a term, but an acyclic *algorithmic computation*, called *construction* of the *denotational value* of the term "C" (see e.g. Tichý [8], Raclavský [5] or even Moschovakis [4] for discussion).[2] Within TT^*, $C_{(D/x)}$ is a notational abbreviation of

$$[\![Sub(\ulcorner D \urcorner, \ulcorner x \urcorner, \ulcorner C \urcorner)]\!]_\tau,$$

where Sub is a logical operator standing for an appropriate *substitution function* Sub which is defined in Curry's manner.

Solution to Problem 2 (derivability of (EG)) As suggested above,
(F3) (EG) is a *derivable rule* in a suitable ND. In the present talk, I show its *intralogical proof* (i.e. not a a metalinguistic demonstration stated in English). The ND system used for proving it is appropriate for TT^*, it is called $\mathsf{ND}_{\mathsf{TT}^*}$.

The *rules* of the system manipulate *sequents* (as valid arguments) of the form $\Gamma \Rightarrow \mathcal{M}$, where $\mathcal{M}$ is a match (see below) and Γ is a set of matches. *Matches* are *congruence statements* of the general form $\mathcal{M} := C : \underline{\mathbf{x}}$, where C is either 'annotated' by $\_$ – saying that C is *improper* (= 'non-denoting'), or by $\mathbf{x}$ – saying that C is *proper* and constructs the object X, or an object in the range of x, or the construction X (acquired by $\ulcorner X \urcorner$).

Now let (k, l) indicate presence or absence of the possible-world variable w and time-instant variable t (preparing thus the rule for possible worlds semantics, see below); let $\mathtt{T}$ be a (constant standing for) the truth value True. The rule (EG) has the *empty set* of initial sequents:

Theorem 1 (The rule (EG)) $$\text{(EG)}\ \frac{}{\Gamma, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow \exists^\tau(\lambda x.C){:}\mathtt{T}}$$

Its *proof* applies $\mathsf{ND}_{\mathsf{TT}^*}$'s 'axiom rule' (AX), the weakening rule (WR), β-expansion rule (β-EXP) (see [7]), (∃-I) and the rule of instantiation of an exposed variable (its proof is rather difficult and it is briefly shown in the talk):

[2] "$\bar{E}_m$" stands for "$E_1, E_2, ..., E_m$" and "$\tilde{E}_m$" stands for "$E_1 E_2 E_m$", for any entity E_i. τ is a *type* interpreted by a set of objects $\mathfrak{D}$; *models* consist of indexed families $\mathfrak{M} := \{\mathfrak{D}_\tau\}_\tau$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow C_{(D_{(k,l)}/x)}{:}\mathtt{T}\ \ ^{1.}}\ \text{(AX)}}{\Gamma, D{:}d, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow C_{(D_{(k,l)}/x)}{:}\mathtt{T}}\ \text{(WR)}}{\Gamma, D{:}d, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow [\lambda x.C](D_{(k,l)}){:}\mathtt{T}}\ (\beta\text{-EXP})}{\Gamma, D{:}d, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow \exists^\tau \lambda x.C{:}\mathtt{T}\ \ ^{2.}}\ (\exists\text{-I})}{\Gamma, C_{(D_{(k,l)}/x)}{:}\mathtt{T} \Rightarrow \exists^\tau \lambda x.C{:}\mathtt{T}}\ \text{(exp-INST) 1.,2.}$$

(F4) Finally, I show two proofs of ($\exists$-I$^\eta$), the longer one does not assume the rule of η-conversion. Thus, both (EG) and ($\exists$-I$^\eta$) are *derivable* in $\mathsf{ND}_{\mathsf{TT}^*}$.

Problem 3 (Is (EG) applicable even within intensional and hyperintensional contexts?) Quine and others (see esp. Kaplan [3]) raised a worry that the rule (EG) cannot be applied within (a) *intensional* and (b) *hyperintensional contexts*, though it is applicable within (c) *extensional contexts.*

Solution to Problem 3 ((EG) and (hyper)intensional contexts) As regards (a), the favourable answer has been known since Montague-like *intensional* (or *possible worlds*) *semantics* was applied to sentences such as "*Necessarily, the number of planets (NP) is greater than 7.*". As regards (b), proposals adequately formalising *also* sentences such as "*Wiles knows that Fermat believed Fermat's Last Theorem.*", exists now, see e.g. Tichý [8], Moschovakis [4], Raclavský [5]. The approaches model *fine-grained hyperintensional meanings* e.g. as constructions.

The approaches may deploy $\mathsf{ND}_{\mathsf{TT}^*}$ with (EG). I show that existential generalisation cannot be applied only to the *de dicto readings* of (a)- and (b)-type sentences, i.e. (EG) cannot *justify* the corresponding arguments. I explain the impossibility by a recourse to the definition of Sub.

References

[1] Prawitz, D.: *Natural Deduction: A Proof-Theoretical Study*, Dover Publications (2006).

[2] Negri, S.; von Plato, J.; Ranta, A.: *Structural Proof Theory.* Cambridge University Press (2001).

[3] Kaplan, D.: Quantifying In. *Synthese* 19(1–2), pp. 178–214, (1968).

[4] Moschovakis, Y.N.: A Logical Calculus of Meaning and Synonymy. *Linguistics and Philosophy* 29, 27–89 (2005).

[5] Raclavský, J.: *Belief Attitudes, Fine-Grained Hyperintensionality and Type-Theoretic Logic.* College Publications (Studies in Logic 88), London (2020).

[6] Raclavský, J.: Existential Generalisation and Explicit Substitution. *Logic and Logical Philosophy*, condit. accepted (2021).

[7] Tichý, P.: Foundations of Partial Type Theory. *Reports on Mathematical Logic* 14, 57–72 (1982).

[8] Tichý, P.: *The Foundations of Frege's Logic.* Walter de Gruyter, Berlin (1988).

A Logic of Interactive Proofs

David Lehnherr [1], Zoran Ognjanović [2],Thomas Studer[3]

[1] *University of Bern*
Baumgartenweg 45 CH-8854 Siebnen
[2] *Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade
[3] *University of Bern*
Neubrückenstrasse 10 CH-3012 Bern
E-mail: [1]`david.lehnherr@students.unibe.ch`, [2]`zorano@mi.sanu.ac.rs`,
[3]`thomas.studer@inf.unibe.ch`

Keywords:
Interactive Proofs, Justification Logic, Non-standard Probabilities.

The introduction of interactive proofs by Goldwasser et al. ([1]) poses an interesting question to the already vividly researched area of uncertain reasoning and justification logic - How can we quantitatively describe an evidence transformation that gets progressively more meaningful and how can we model agents that reason based on such transformed evidence?

In this work, we introduce the probabilistic two-agent justification logic IPJ, a logic in which we can reason about agents that perform interactive proofs. We present its syntax and semantics and provide a soundness proof. Moreover, we investigate how our axiomatisation can be extended in order to capture a weaker notion of the zero-knowledge property of interactive proofs. The foundation of our logic is built on the works of Kokkinis et al. ([2]) and Ognjanović et al. ([3]) who developed a probabilistic justification logic PJ and its extension CPJL which allows for conditional and non-standard probabilities.

We answer the question above by parametrizing our logic over the set of negligible functions $f(n) = n^{-k}$ for all $k \in \mathbb{N}$. This approach enables us to canonically construct the set of formulas that are known by the agents to be interactively provable. By doing so, we closely model the soundness and completeness properties of interactive proofs which are usually stated by using first-order quantifiers. Furthermore, we use non-standard probabilities in order to model the limit cases of the aforementioned properties.

Acknowledgment

Supported by the Swiss National Science Foundation grant 200020184625 and by the Science Fund of the Republic of Serbia project AI4TrustBC.

References

[1] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, page 291–304, New York, NY, USA, 1985. Association for Computing Machinery.

[2] Ioannis Kokkinis, Petar Maksimović, Zoran Ognjanović, and Thomas Studer. First steps towards probabilistic justification logic. *Logic Journal of IGPL*, 23:662–687, 08 2015.

[3] Zoran Ognjanović, Nenad Savić, and Thomas Studer. Justification logic with approximate conditional probabilities. In Alexandru Baltag, Jeremy Seligman, and Tomoyuki Yamada, editors, *Logic, Rationality, and Interaction*, pages 681–686, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.