12$^{\text{TH}}$ International Conference

Logic and Applications

LAP 2023

September 25 - 29, 2023
Dubrovnik, Croatia

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 12$^{\text{th}}$ International Conference on Logic and Applications - LAP 2023, held in the Inter University Center Dubrovnik, Croatia, September 25 - 29, 2023.

LaTeX book of abstracts preparation and typesetting:

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

LAP 2023 Web site: `https://lap.math.hr/` Maintained by Marko Horvat, University of Zagreb, and Simona Prokić, University of Novi Sad.

Contents

1 *Tin Adlešić*
Dedekind's foundation of arithmetic **4**

2 *Musab A. Alturki, Tajana Ban Kirigin, Max Kanovich, Vivek Nigam, Andre Scedrov, Carolyn Talcott*
Resilience Problems for Cyber-Physical Systems: Formalization and Computational Complexity **5**

3 *Tajana Ban Kirigin, Sanda Bujačić Babić, Benedikt Perak*
Graph Based Sentiment Propagation Algorithm **7**

4 *Péter Battyányi*
On Some Properties of Nonstandard Heyting Arithmetic **9**

5 *Vedran Čačić*
NFU signature expansion **11**

6 *Bojana Femić, Vladimir Grujić, Jovana Obradović, Zoran Petrić*
A calculus for S^3-diagrams of manifolds with boundary **12**

7 *Armand Feuilleaubois, Graham E. Leigh, Dominik Wehr*
Towards Cut Elimination for IPL2 using Hydra Games **15**

8 *Silvia Ghilezan, Simona Prokić*
Kripke-style semantics in computation **18**

9 *Sebastijan Horvat, Tin Perkov, Mladen Vuković*
The selection method for interpretability logic IL with respect to Verbrugge semantics **20**

10 *Stipe Marić, Tin Perkov*
Some results in model theory of inquisitive modal logic **23**

11 *Matej Mihelčić, Adrian Satja Kurdija*
Complexities of selected redescription mining configurations **25**

12 *Borja Sierra Miranda*
Σ_1-provability logic of subsystems
of Heyting Arithmetic **27**

13 *Petar Paradžik, Ante Đerek, Marko Horvat*
Security analysis of AMD SEV-SNP firmware ABI **30**

14 *Jiří Raclavský*
β-Conversion and Type Theory with Quotation and Evaluation Terms **31**

15 *Andrea Sabatini*
Minimization of normal forms **33**

16 *Andre Scedrov*
Non-Associative Non-Commutative Multi-Modal Linear Logic **35**

17 *Zvonimir Šikić*
Is there mathematical concepts that are real? **37**

18 *Tamara Stefanović, Selene Cerna, Héber H. Arcolezi, Karima Makhlouf, Catuscia Palamidessi*
On the Impact of Local Differential Privacy on Simpson's Paradox **39**

19 *Thomas Studer*
New forms of distributed knowledge **42**

20 *Carolyn Talcott*
Reasoning about Cyberphysical Systems using Rewriting Modulo Constraints **43**

Dedekind's foundation of arithmetic

Tin Adlešić [1]

[1] *University of Zagreb, Faculty of Teacher Education*
Savska cesta 77

E-mail: [1]`tin.adlesic@ufzg.hr`

Keywords:
Foundation, Arithmetic, Natural numbers

Dedekind worked on the foundation of arithmetic practically from the start of his mathematical career in 1854. He did not put forward any formal foundational program, but one can be recreated retrospectively. This program reached its culmination point in 1888 when he published his arguably the most important mathematical work *Was sind und was sollen die Zahlen?*.

In it, he tried to precisely define the concept of natural number, and develop all of the arithmetic. His main tools were sets and mappings, which he viewed as purely logical notions. Therefore, he formulated a version of logicism, which turns out not to be much different from Frege's.

In this talk, we will present the content of *Was sind und was sollen die Zahlen?*, and its background. That is, we will show what were Dedekind's main motivational ideas, and why he viewed the notion of sets as the most suitable notion for achieving his goals.

References

[1] Ewald, W. B. *From Kant to Hilbert Volume 2: A Source Book in the Foundations of Mathematics. Vol. 2.* Oxford University Press, 1996.

[2] Ferreirós, J. *Labyrinth of thought: A history of set theory and its role in modern mathematics.* Birkhauser Verlag AG, 2007.

[3] Van Heijenoort, J. *From Frege to Gödel: a source book in mathematical logic, 1879-1931.* Harvard University Press, 1967.

Resilience Problems for Cyber-Physical Systems: Formalization and Computational Complexity

Musab A. Alturki[1,2] **Tajana Ban Kirigin**[3], **Max Kanovich**[4], **Vivek Nigam**[5,6], **Andre Scedrov**[7], **Carolyn Talcott**[8]

[1] *Runtime Verification Inc., Urbana, Illinois, USA*
[2] *KFUPM, Dhahran, Saudi Arabia*
[3] *University of Rijeka, Faculty of Mathematics, Rijeka, Croatia*
[4] *University College London, London, UK*
[5] *Federal University of Paraíba, João Pessoa, Brazil*
[6] *Munich Research Center, Huawei, Munich, Germany*
[7] *University of Pennsylvania, Philadelphia, PA, USA*
[8] *SRI International, Menlo Park, CA, USA*

Keywords: Resilience, Computational Complexity, Cyber-Physical Systems, Multiset Rewriting

Cyber-Physical Systems (CPS) are used to perform complex, safety-critical tasks, often with limited or no human intervention and in disruptive or hostile environments. Examples include applications of autonomous vehicles and drones. Given that the systems themselves and their assigned tasks involve complex specifications, constraints, and inherent non-determinism, the properties of CPS performance are the resut of the interaction between the system design and the influence of the environment. In [2, 3] we considered various verification properties (realizability, survivability, reliability and recoverability), that relate the ability of such systems to function in the face of perturbations that occur in the environment.

In [1] we further consider properties of CPSes that go beyond task realization under nominal conditions, with fixed goals and fixed regulations and policies. Instead, we address possible changes in mission objectives or regulatory updates that may occur during mission execution, and focus on the ability of CPS to adapt to such changes. This capability is informally referred to as *resilience*.

We formalize the intuitive notion of resilience as a formal verification property using timed multiset rewriting. An important innovation in our formalization is the distinction between rules that are under the control of the CPS and those that are not. The latter rules specify the changes in system conditions, e.g., mission goals, to which the system may need to adapt.

We also study the computational complexity of resilience problems. Although undecidable in general, we show that these problems are PSPACE-complete for a class of bounded systems, more precisely, balanced systems where the rules do not affect the number of facts of the configurations and where facts are of bounded size.

References

[1] Musab A. Alturki, T. Ban Kirigin, M. Kanovich, V. Nigam, A. Scedrov, and C. Talcott. On the Formalization and Computational Complexity of Resilience Problems for Cyber-Physical Systems. In *19th International Colloquium on Theoretical Aspects of Computing (ICTAC)*, 2022.

[2] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Timed multiset rewriting and the verification of time-sensitive distributed systems. In *14th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS)*, 2016.

[3] M. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, and C. Talcott. On the complexity of verification of time-sensitive distributed systems. In D. Dougherty, J. Meseguer, S. A. Mödersheim, and P. Rowe, eds., *Protocols, Strands, and Logic*. Springer LNCS Volume 13066, Springer-Verlag, pp. 251 - 275. First Online 19 November 2021.

Graph Based Sentiment Propagation Algorithm

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

[1] *Faculty 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:
complex networks; sentiment analysis; applications of graph data processing; algorithmic sentiment propagation.

The extensive development of modern technologies and artificial intelligence has greatly influenced natural language processing (NLP). The ability of computer programs to interpret spoken and written human language is becoming increasingly useful and practical. Sentiment analysis, a subfield of NLP, deals with large amounts of textual data such as emails, chat transcripts, social media comments, and reviews that are categorized as positive, neutral, or negative. Sentiment analysis allows users to use technology to learn more about the emotional aspects of linguistic expressions, such as customers' attitudes and opinions. With advances in NLP, it already appears that computers understand human language.

One of the pillars of sentiment analysis are sentiment dictionaries, collections of lexemes classified or numerically evaluated according to the emotional characteristics they carry. The coverage of a sentiment dictionary is an important feature in the development of computational sentiment analysis techniques. When dealing with sentiment analysis, one may find that sentiment dictionaries are quite sparse, especially for languages other than English.

This paper describes an iterative, graph-based algorithm for propagation of sentiment values. We offer a novel approach to creating a comprehensive sentiment dictionary, where the existing sentiment dictionaries are utilized to propagate the original dictionary values to a large collection of lexemes, resulting in a considerably broader and multidimensional dictionary coverage. Our solution is applicable to a variety of sentiment dictionaries and languages.

Acknowledgment

This work has been supported by the University of Rijeka within the project UNIRI-human-18-243.

References

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

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

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

[4] T. Ban Kirigin, S. Bujačić Babić, B. Perak.
Semi-Local Integration Measure of Node Importance, Mathematics, 10(3):405, 2022.

On Some Properties of Nonstandard Heyting Arithmetic

Péter Battyányi [1]

[1] *University of Debrecen, Faculty of Informatics, Department of Computer Science*
Kassai út 26., 4028 Debrecen, Hungary
E-mail: [1]battyanyi.peter@inf.unideb.hu

Keywords:
Heyting arithmetic, non-standard arithmetic, realizability.

As early as in 1934, Skolem [5] proved that, if we add the axioms $\underline{n} < c$ ($n \in \mathbb{N}$) to first-order arithmetic, in other words, if we demand the existence of an infinite number, then the resulting theory is consistent [3, 4]. We examine Heyting arithmetic [2, 6], that is, first-order arithmetic with intuitionistic predicate logic, augmented with these axioms of non-standardness together with a predicate expressing the property of being feasible. We define feasibility following [1]. The property of feasibility is a downward closed property, where 0 is feasible, and, for all primitive recursive functions, if the arguments are feasible, then the result should be feasible. Furthermore, the infinite number c is not feasible. Formally:

1. $F(0)$,
2. $\forall x \forall y (F(x) \wedge y < x \supset F(y))$,
3. $\forall x (F(x) \supset x < c)$,
4. $\forall x_1 ... \forall x_n (F(x_1) \wedge ... \wedge F(x_n) \supset F(g(x_1, ..., x_n)))$, for each symbol g standing for a primitive recursive function.

We denote the theory obtained as above by HAF_0. There are two kinds of induction axiom which appear to be reasonable to extend HAF_0 with.

A,
$$A(0) \wedge \forall x (A(x) \supset A(Sx)) \supset \forall x A(x) \quad (Ind^c),$$

where $A(x)$ does not contain F. The new theory will be referred to as HAF^c. We note that nonstandard elements can be present in the induction formula.

B,

$$A(0) \wedge \forall^f x(A(x) \supset A(Sx)) \supset \forall^f x A(x) \quad (Ind^f),$$

where $A(x)$ does not contain F and $\forall^f x A(x)$ means $\forall x(F(x) \supset A(x))$. We denote the new theory by HAF.

We verify some proof-theoretical properties concerning these theories by standard realizability techniques. Namely, we show that both theories are consistent relative to HA and we demonstrate that, under certain restrictions, they admit disjunctive and existential properties.

References

[1] Dragalin, A. G., *Explicit algebraic models for constructive and classical theories with non-standard elements.* Studia Logica, 55 (1), 33–61 (1995)

[2] Dragalin, A. G., *Mathematical Intuitionism. Introduction to Proof Theory.* Translations of AMS, 67, American Mathematical Society, Providence, Rhode Island (1988)

[3] Hájek, P., Pudlák, P., *Metamathematics of First-Order Arithmetic.* Springer-Verlag, Berlin Heidelberg (1993)

[4] Kaye, R., *Models of Peano Arithmetic.* Clarendon Press, Oxford (1991)

[5] Skolem, Th. A., *Über die Nichtcharakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vielen Aussagen mit ausschliesslich Zahlvariablen.* Fundamenta Mathematicae, 23, 150–161 (1934)

[6] Troelstra, A. S., van Dalen, D., *Constructivism in Mathematics.* Vol. I.-II. North-Holland, Amsterdam (1988)

NFU signature expansion

Vedran Čačić [1]

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

Keywords:
signature expansion, New Foundations, type assignment

NFU is an alternative (to ZF) set theory, in which we're concerned with assigning *levels* to variables and terms of formulas defining sets by comprehension. If the levels (*types*) can be assigned in a consistent way, we call the formula or term *stratified*.

In developing set theory, it is usual to name some terms by function (or constant) symbols, and to name some formulas by relation symbols. In NFU, however, we must also ensure that stratification is preserved. We will see what this means for our terms and formulas.

In [1], we have developed two ways of dealing with abstraction terms: *eliminating* them from the language, and *typing* them by extended level assignment. This is an overview of the third approach, *naming* them by expanding the signature.

Acknowledgment

I'd like to thank my colleagues Marko Doko and Tin Adlešić for giving me ideas and implementing my ideas.

References

[1] Tin Adlešić and Vedran Čačić. A modern rigorous approach to stratification in NF/NFU. *Logica universalis*, 16:451–468, 2022.

A calculus for S^3-diagrams of manifolds with boundary

Bojana Femić[1], **Vladimir Grujić**[2], **Jovana Obradović**[3] **and Zoran Petrić**[4]

[1,3,4] *Mathematical Institute of the Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade, Serbia
[2] *Faculty of Mathematics, University of Belgrade*
E-mail: [1] `femicenelsur@gmail.com`, [2] `vgrujic@matf.bg.ac.rs`, [3] `jovana@mi.sanu.ac.rs`, [4] `zpetric@mi.sanu.ac.rs`

Keywords:
knots, links, surgery, Kirby's calculus, 3-manifolds with boundary, gluing

The aim of this paper is to introduce a calculus for a presentation of compact, orientable, connected 3-manifolds with boundary in terms of diagrams embedded in S^3 in a form akin to the standard surgery presentation of closed, orientable, connected 3-manifolds. Our motivation to introduce such a presentation of manifolds is to give a completely combinatorial description of the category 3Cob[1], whose arrows are 3-dimensional cobordisms, which is an ongoing project. We hope this could support further investigations of faithfulness of 3-dimensional Topological Quantum Field Theories. On the other hand, the calculus could be applied within some coherence results in Category theory.

That every closed, orientable, connected 3-manifold may be obtained by surgery on a link in S^3 was proved by Wallace, [10] and (independently) by Lickorish, [5]. This result provides a language for presentation of such manifolds. The rational surgery calculus for this language was introduced by Rolfsen, [8, Chapter 9.H]. This calculus consists of two types of modifications and he proved that two surgery descriptions yield homeomorphic 3-manifolds if one can be transformed into the other by a finite sequence of these modifications. At about the same time, Kirby, [4] introduced another surgery calculus and he proved its completeness, i.e. that two surgery descriptions (with integral framing) yield homeomorphic 3-manifolds if and only if one can be transformed into the other by a finite sequence of operations from this calculus. By relying on Kirby's result, Rolfsen, [9], proved the completeness of his calculus.

[1] By this we mean a diagrammatic presentation of cobordisms and a calculus for composition of diagrams.

Fenn and Rourke, [1], merged two Kirby's operations into an infinite list of integral moves of one type, which is a special case of Rolfsen's second modification. Roberts, [7], developed a calculus for surgery data in arbitrary compact, connected 3-manifold (possibly with boundary, or non-orientable). This calculus consists of moves of three types and he proved its completeness.

The first part of our work uses a generalization of Wallace-Lickorish result to compact, orientable, connected 3-manifolds with boundary in order to establish a diagrammatic language of these manifolds. This language is based on the well known language for closed manifolds that consists of surgery data in S^3 written in terms of framed links. We extend the "alphabet" by introducing some rigid "symbols" in the form of wedges of circles. The intuition behind a wedge of circles in a diagram is that its neighbourhood is removed from S^3 forming one component of the boundary. By the *neighbourhood* of a wedge of circles we mean its regular neighbourhood in terminology of [3, Definition 1.4], which is appropriate for piecewise-linear category, or its graphical neighbourhood in terminology of [2, Definition 6], which is appropriate for smooth category.

The second part adapts Roberts' calculus into a diagrammatic calculus adequate for our language. This adaptation is akin to the adaptation of Kirby's calculus made by Fenn and Rourke. As the Fenn and Rourke local moves can be reduced to a finite list, which is shown by Martelli, [6], our calculus is also presentable by a finite list of local moves. Finally, we develop a rational surgery calculus for our language. We prove the completeness for all the calculi.

Acknowledgment

Bojana Femić, Jovana Obradović and Zoran Petrić were supported by the Science Fund of the Republic of Serbia, Grant No. 7749891, Graphical Languages - GWORDS. Vladimir Grujić was supported by the Science Fund of the Republic of Serbia, Grant No. 7744592, Integrability and Extremal Problems in Mechanics, Geometry and Combinatorics - MEGIC.

References

[1] R.A. Fenn and C. Rourke, *On Kirby's calculus of links*, ***Topology***, vol. 75 (1979), pp. 1-15

[2] S. Friedl and G. Herrmann, *Graphical Neighborhoods of Spatial Graphs*, (J. de Gier, C.E./ Praeger and T./ Tao editors) ***2019-20 MATRIX Annals***, MATRIX Book Series, vol. 4, 2021, pp. 627–646

[3] J. Johnson, ***Notes on Heegaard splittings***, Available at http://www.math.ucdavis.edu/ jjohnson/notes.pdf, 2007

[4] R. Kirby, *A calculus for framed links in S^3*, ***Inventiones Mathematicae***, vol. 45 (1978), pp. 35-56

[5] W.B.R. Lickorish, *A Representation of Orientable Combinatorial 3-Manifolds*, ***Annals of Mathematics***, vol. 76 (1962), pp. 531-540

[6] M. Martelli, *A finite set of local moves for Kirby calculus*, ***Journal of Knot Theory and its Ramifications***, vol. 21 1250126 (2012)

[7] J. Roberts, *Kirby calculus in manifolds with boundary*, ***Turkish Journal of Mathematics***, vol. 21 (1997), pp. 11-117

[8] D. Rolfsen, ***Knots and Links***, Publish or Perish, Berkeley, 1976

[9] ——, *Rational surgery calculus:extension of Kirby's theorem*, ***Pacific Journal of Mathematics***, vol. 110 (1984), pp. 377-386

[10] A.D. Wallace, *Modifications and cobounding manifolds*, ***Canadian Journal of Mathematics***, vol. 12 (1960), pp. 503-528

Towards Cut Elimination for IPL2 using Hydra Games

Armand Feuilleaubois[1], **Graham E. Leigh**[2], **Dominik Wehr**[3]

[1] *University of Bern*
Neubrückstrasse 10, 3012 Bern
[2,3] *University of Gothenburg*
Renströmsgatan 6, 41255 Göteborg
E-mail: [1] `gusfeuar@student.gu.se`, [2] `graham.leigh@gu.se`, [3] `dominik.wehr@gu.se`

Keywords:
Multicuts, Hydra Games, IPL2, Cut Elimination.

Intuitionistic propositional logic with second order quantifiers (IPL2) was introduced by Gabbay [1]. Since then, there has been a substantial body of work produced about various semantics for it, some of which have been shown not to be equivalent [2]. However none of the work so far on IPL2 has introduced a sequent calculus system for IPL2, which is better adapted to doing proof theory, or tackled questions of cut elimination or normalisation. We introduce a sequent calculus for IPL2, on which we attempt to obtain cut elimination.

The calculus we introduce is the same as the sequent calculus for intuitionistic propositional logic, but with the addition of a rule for the propositional quantifier $\forall$. This is sufficient to express $\exists$ as well. The rules for $\forall$ are:

$$(\mathrm{L}\forall)\,\frac{\Gamma, \forall p B(p), B(A) \Rightarrow C}{\Gamma, \forall p B(p) \Rightarrow C} \qquad\qquad (\mathrm{R}\forall)\,\frac{\Gamma \Rightarrow B(p)}{\Gamma \Rightarrow \forall p B(p)}$$

with the condition in the (R$\forall$) rule that p is not free in Γ. In addition to these, we introduce an n-ary branching multicut rule for use within the proof of cut elimination. This is a natural extension of the linear multicut used by Fortier and Santocanale [3], similar to that used by Baelde, Doumane, and Saurin [4]. The n-ary multicut rule essentially groups together multiple cut rule applications, with an associated tree T representing the cut formula relationships between the premise sequents for the multicut.

The usual approach to cut elimination makes use of a number of rewrite operations on proofs with cut, each of which reduces some measure on the proof. Then, induction is carried out in an order derived from these measures so as to reduce them, and thereby eliminate the cut. Instead of using this usual cut elimination process, we will apply Büchholz hydra game methods in a similar style to Hamano and Okada [5]. A hydra game is a 1 player game wherein the player makes use of a number of rewrite operations to rewrite a (possibly labelled) tree T. The player wins if they can reduce the number of edges in the tree to 0 using the rewrite operations. If we can assign a measure to the trees such that each rewrite operation reduces this measure, then no matter what sequence of moves the player uses, the player will win [6] [7]. This process shares much of its structure in common with the usual inductive process. This is given by the supremum of the ordinals used for the unique measure. Here, we have a clear choice for both the tree and the rewrites. These are the multicut tree and rewrites of the same form as those used for the usual cut elimination process. To the multicut tree, we add labels to represent information associated with each cut that will be useful when defining the measure to be reduced. These are a notion of cut formula complexity and local and global notions of hereditary subproof magnitude. This labelled tree is the structure on which the hydra game will be carried out. We then define an appropriate ordinal measure using the information in the labelled tree, with the objective of reducing it to 0 during the hydra game.

However, this cut elimination procedure cannot work for full IPL2, because of the arbitrary increase in cut formula complexity enabled by the rewrite for the principal $\forall$ case. This is because the substituted formula A in the rule (L$\forall$) does not have any restrictions on its complexity, and any increase in its complexity will be inherited by $B(A)$. Thus, if we restrict to fragments of the IPL2 proof system that limit the complexity allowed for A, then cut formula complexity will always decrease. Hence, the measure on the labelled trees will decrease with every rewrite application, and therefore the player must win the hydra game.

We show that termination of this hydra game corresponds to the elimination of a cut from the proof, and obtain single cut elimination results for the appropriate fragments of IPL2. This cut elimination process can be applied repeatedly to obtain cut elimination for these fragments of IPL2. In the talk I will discuss the cut elimination process in more detail.

References

[1] Gabbay, D.M., *On 2nd order intuitionistic propositional calculus with full comprehension*, Archiv für Mathematische Logik und Grundlagenforschung 16.3, Aug 1974.

[2] Polacik, T., *Pitts' Quantifiers Are Not Topological Quantification*, Notre Dame Journal of Formal Logic 39.4, Oct 1 1998.

[3] Fortier, J., Santocanale, L., *Cuts for circular proofs: semantics and cut-elimination*, Computer Science Logic, 2013.

[4] Baelde, D., Doumane, A., Saurin, A., *Infinitary Proof Theory: the Multiplicative Additive Case*, 25th EACSL Annual Conference on Computer Science Logic, 2016.

[5] Hamano, M., and Okada, M., *A Relationship Among Gentzen's Proof- Reduction, Kirby-Paris' Hydra Game and Buchholz's Hydra Game*, Mathematical Logic Quarterly 43.1, 1997.

[6] Kirby, L., Paris, J., *Accessible Independence Results for Peano Arithmetic*, Bulletin of the London Mathematical Society 14.4, July 1982.

[7] Büchholz, W. *An independence result for (*Π^1_1*-CA)+BI*, Annals of Pure and Applied Logic 33, 1987.

Kripke-style semantics in computation

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

[1] *University of Novi Sad, Serbia*
[2] *Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia*
E-mail: [1]`gsilvia@uns.ac.rs`, [2]`simona.k@uns.ac.rs`

Keywords:
Computation, lambda calculus, intuitionistic logic, Kripke semantics

The lambda calculus is a model of computation based on functions introduced by Alonzo Church in the 1930s. Lambda calculus comes in two variants: untyped and typed. The untyped lambda calculus is Turing-equivalent. Types are introduced in lambda calculus to control term formation, i.e. computation. The basic typed lambda calculus is the so called simply typed lambda calculus, where types control function applications. The Curry–Howard correspondence, a.k.a. formulae-as-types, proofs-as-terms or proofs-as-programs, represents a correspondence between simply typed lambda calculus and intuitionistic logic. Intuitionistically provable formulae coincide with inhabited types, proofs coincide with terms/programs and proof normalization represents term reduction. This relationship directly underpins the fundamental relationship between logic and computation. Kripke-style semantics have gained an important role and wide applicability in logic since it was introduced by Saul Kripke in the late 1950s as a semantics for modal logics. In logic, these semantics were later adapted to intuitionistic logic and various other logics. In computation, a class of Kripke-style models was defined for typed lambda calculus [4, 3] and Scott-Ershov model for partial continuous functionals [5]. In this talk, we present a new approach to Kripke semantics for full simply typed lambda calculus, which is the simply typed lambda calculus endowed with product types and sum types. The full simply typed lambda calculus is related to minimal propositional logic with all connectives via the Curry–Howard correspondence. We show soundness and completeness of full simply typed lambda calculus w.r.t. the proposed semantics [1, 2]. The completeness result is proved by an adaptation of the Henkin-style completeness method.

The present talk is based on joint work with Simona Prokić.

References

[1] S. Ghilezan, S. Kašterović: Semantics for combinatory logic with intersection types, Frontiers in Computer Science, volume 4, 2022.

[2] S. Kašterović, S. Ghilezan: Kripke semantics and completeness for full simply typed lambda calculus. Journal of Logic and Computation, 30(8), 2020, 1567–1608.

[3] J. C. Mitchell: Foundations for programming languages. Foundation of Computing Series, MIT Press, 1996.

[4] J. C. Mitchell, E. Moggi: Kripke-style models for typed lambda calculus, Annals of Pure and Applied Logic, 51, 1991, 99–124.

[5] H. Schwichtenberg, S. S. Wainer: Proofs and Computations. Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, 2012.

The selection method for interpretability logic IL with respect to Verbrugge 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@unizg.hr`, [3] `mladen.vukovic@math.hr`

Keywords:

Interpretability logic, Finite model property, Decidability, Filtration, Verbrugge semantics, Selection, Weak bisimulations

The finite model property is a key step in proving decidability of modal logics (see e.g. [1]). In [1] two distinct ways are presented to show that modal logics possesses finite model property: the selection and the filtration method.

Generalised Veltman semantics for interpretability logic, or nowadays called Verbrugge semantics (in honor of Rineke Verbrugge), was developed to obtain certain non-derivability results since Veltman semantics for interpretability logic is not fine-grained enough for certain applications. It has turned out that this semantics has various good properties (see e.g. [3] and [5]).

Vuković and Perkov [6] applied the filtration technique to prove finite model property of interpretability logic IL and some of its extensions with respect to Verbrugge semantics. A filtration is usually the partition generated by logical equivalence over so called *adequate sets* of formulas, i.e. sets of formulas that possess certain properties like being closed under taking subformulas and special negations. In [6] it was proved that ILM_0 has the finite model property with respect to Verbrugge models which satisfy certain condition. Together with the completeness of ILM_0 with respect to Verbrugge models, this suffices to prove that ILM_0 is decidable, by a standard argument ([1], p. 341). In [4] they used the same technique to prove the finite model property of interpretability logics ILW and ILW^* w.r.t. Verbrugge models. Thus they obtained the decidability result for interpretability logics ILM_0 and ILW^*.

It is important to note that in the filtration method they heavily used the properties and results for the notion of bisimulation (and their finite approximation called n-bisimulation) for Verbrugge semantics as defined in [7] and [8]. Namely, they used the following (Lemma 3.1. in [6]):

> *Let $\mathfrak{M}$ and $\mathfrak{M}'$ be two Verbrugge models. Let $w \in \mathfrak{M}$ and $w' \in \mathfrak{M}'$. If there are only finitely many propositional variables then we have: if w and w' are n-modally equivalent, then w and w' are n-bisimilar.*

However, as proved in [2], this statement is not valid in general. So, we have defined in [2] a new notion of weak bisimulation (or short, w-bisimulation) and its finite approximation called n-w-bisimulation. Using that new notion, we proved that the desired statement holds if we use w-bisimulations instead of bisimulations. In that way, all the results from [5] and [6] still hold with the use of w-bisimulations.

In this talk we will prove that interpretability logic IL has the finite model property by using the other method of building finite models - the selection method. The selection method is more straightforward than the filtration method. In short, for every satisfiable IL-formula we know there exists a model that satisfies that formula. Then we will apply *tree unravelling* to obtain a model of finite height that still satisfies that same formula. The resulting model may still be infinite, as it may be infinitely branching. We obtain the finite tree-like model we are looking for by a further selection of points which corresponds to discarding unwanted branches of the tree we have obtained. In that process we will heavily use the w-bisimulations and their properties. Finally, we will point out the main drawback of the selection method: the input model for our construction may satisfy important relational properties, but the end result is always a finite tree-like model, and the desired relational properties are often lost. So if we want to establish the finite model property with respect to a class of models satisfying additional properties - for instance property $(M)_{gen}$ for ILM - we have to do some additional work once we have obtained our finite tree-like model. In such cases, the selection method tends to be harder to use than the filtration method, which is the main reason that the filtration method is much more used (e.g. in [5] and [6]).

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] S. Horvat, T. Perkov, M. Vuković, *Bisimulations and bisimulations games for Vebrugge semantics*, Mathematical Logic Quarterly (2023), to appear

[3] J. J. Joosten, J. Mas Rovira, L. Mikec, M. Vuković, *An overview of Generalised Veltman Semantics*, to appear in S. O. Hansson, M. Kracht, L. Moss, S. Smets, H. Wansing (eds.), **Dick de Jongh on Intuitionistic and Provability Logic**, Outstanding Contributions to Logic, Springer, 2023.

[4] L. Mikec, T. Perkov, M. Vuković, *Decidability of interpretability logics ILM_0 and ILW^**, Logic Journal of the IGPL 25(2017), 758-772

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

[6] T. Perkov and M. Vuković, *Filtrations of generalized Veltman models*, Mathematical Logic Quarterly 62(2016), 412–419

[7] D. Vrgoč, M. Vuković, *Bisimulations and bisimulation quotients of generalized Veltman models*, Logic Journal of the IGPL 18(2010), 870–880

[8] M. Vuković, *Bisimulations between generalized Veltman models and Veltman models*, Mathematical Logic Quarterly 54(2008), 368–373

Some results in model theory of inquisitive modal logic

Stipe Marić [1], Tin Perkov [2]

[1] *University of Split, Faculty of Science, Department of Mathematics*
[2] *University of Zagreb, Faculty of Teacher Education*
E-mail: [1]`smaric@pmfst.hr`, [2]`tin.perkov@ufzg.hr`

Keywords:
inquisitive modal logic, support semantics, filtration, finite model property, decidability, bisimulation, bisimulation quotient.

Inquisitive logic is a generalization of classical logic which, besides statements, also expresses questions. The language of classical propositional logic is extended with a new connective $\mathbin{\vee\!\!\!\vee}$, called *inquisitive disjunction*. For example, $p \mathbin{\vee\!\!\!\vee} q$ can be read as the question "whether p or q is the case". Although intuitively there is no sense for a question to be true or false, there is a sense in which question can be said to be settled by given information. This is achieved by using the so-called *support semantics*, a possible world semantics in which, instead of a satisfaction relation between worlds and formulas, a support relation is established between *sets of worlds* and formulas (cf. [1], [2]).

Since a possible world semantics is used, it is very natural to combine inquisitive and modal logic, so for example in the epistemic context we can express statements like "agent knows whether p", namely by $\Box(p \mathbin{\vee\!\!\!\vee} \neg p)$.

A further enrichment, the inquisitive modal logic InqML, was first introduced in [2]. Its language contains a new modality $\boxplus$, which is a natural analogue of $\Box$ w.r.t. the support semantics, and enables expressing statements like "agent *wonders* whether p" (cf. [2]). This makes the semantics even more complex – not only sets of worlds, but also sets of sets of worlds need to be considered.

In [2], soundness and completeness of InqML is proved. Notions of bisimulations, bisimulation games and translations from InqML to two-sorted first-order logic are developed and analogues of Van Benthem Characterization Theorem are proved in [3] and [4].

Our contributions include the adaptation of filtration technique to support semantics, and definition and properties of bisimulation quotient for InqML. Using filtration, we show that InqML has the finite model property and consequently InqML is decidable.

References

[1] I. Ciardelli, *Inquisitive Logic: consequence and inference in the realm of questions*, Springer (2023)

[2] I. Ciardelli, *Questions in Logic*, Ph.D. thesis, Institute for Logic, Language and Computation, University of Amsterdam (2016)

[3] I. Ciardelli, M. Otto, Inquisitive bisimulation, *The Journal of Symbolic Logic* 86 (2021) 77–109

[4] S. Meissner, M. Otto, A first-order framework for inquisitive modal logic, *The Review of Symbolic Logic* 15 (2021) 1–23

Complexities of selected redescription mining configurations

Matej Mihelčić[1] and Adrian Satja Kurdija[2]

[1]Department of Mathematics, Faculty of Science, University of Zagreb

[2]Department of Electronics, Microelectronics, Computer and Intelligent Systems, Faculty of Electrical Engineering and Computing, University of Zagreb

Redescription mining [4] is a field of data mining with the goals to: a) discover subsets of instances that can be re-described, b) construct appropriate redescriptions, interpretable objects that re-describe these subsets of instances. The execution and the overall results of the task depend on a set of parameters, such as: query language, constraints on redescription accuracy (the Jaccard index) [2], statistical significance [1], allowed support size interval and constraints on the size of redescription queries.

We present the proofs that several decision variants of the task are $\mathcal{NP}$-complete:

- T1: configuration where conjunction and literal level negations are used to construct redescription queries, minimal redescription accuracy equals 1, minimal support size equals δ and the minimal query size equals η.
- T2: configuration where conjunction and disjunction operators are used to construct redescription queries, minimal redescription accuracy equals 1, minimal support size equals δ and the maximal query size equals η.
- T3: configuration where conjunction, disjunction and negation operators are used to construct redescription queries, minimal redescription accuracy (pessimistic or query non-missing) equals 1, minimal support size equals δ and the maximal query size equals η.
- T4: configuration where redescription queries are Horn clauses, minimal redescription accuracy (pessimistic or query non-missing) equals 1, minimal support size equals δ and the maximal query size equals η.
- T5: configuration where conjunction, disjunction and negation operators are used to construct redescription queries, minimal redescription accuracy

(pessimistic or query non-missing) equals 1, minimal support size equals δ, maximal statistical significance equals γ and the maximal query size equals η.

Configurations T1-T3 and T5 have already been presented in [3], whereas T4 is a novel contribution.

We also present a decision variant of the task from [3] that can be solved in polynomial time:

- P1: configuration where conjunction, disjunction and negation operators are used to construct redescription queries, minimal redescription accuracy equals β, minimal support size equals δ, maximal query size equals $\eta \in \{1, 2\}$ and the maximal allowed statistical significance equals γ.

As a consequence of the studied configurations, we deduce that the complexity of the original redescription mining task, aiming to list all possible redescriptions with a pre-defined general constraint set $\mathcal{C}$ and a query language $\mathcal{Q}$ must be $\mathcal{NP}$-hard.

References

[1] Esther Galbrun. "Methods for Redescription Mining. (Menetelmiä jälleenkuvausten louhintaan / Méthodes pour la fouille de redescriptions)". PhD thesis. University of Helsinki, Finland, 2013.

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

[3] Matej Mihelčić and Adrian Satja Kurdija. "On the Complexity of Redescription Mining". In: *Theor. Comput. Sci.* 944.C (2023).

[4] 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.

Σ_1-provability logic of subsystems of Heyting Arithmetic

Borja Sierra Miranda [1]

[1] *ILLC, University of Amsterdam*
Science Park 107, 1098 XG Amsterdam
E-mail: [1]borja.sierra.miranda@student.uva.nl

Keywords:
Intuitionistic Logic, Heyting Arithmetic, Provability Logic.

Provability logic arises from a interaction between proof theory and modal logic. Let T be a theory strong enough to formalize logic. In particular, assume that T is strong enough to codify its formulas and a predicate $\mathsf{prov}_T(x)$ whose intuitive meaning is: "x is a formula provable in T". Using this formula, we can define a modal logic formed by the modal formulas such that, interpreting its variables as T-sentences and $\Box$ as prov_T, we get a theorem of T. This modal logic is called the provability logic of T.

The turning point of provability logic was when Solovay proved in [6] that the provability logic of Peano Arithmetic (PA) is exactly GL, Gödel-Löb's logic. Later, in [7], Visser calculated the Σ_1-provability logic of PA. The idea behind the concept of Σ_1-provability logic is to restrict the interpretation of propositional variables to Σ_1-sentences. More recently, in [2], Ardeshir and Mojtahedi showed that from the Σ_1-provability logic of PA, one can calculate its full provability logic. This provides a new method for calculating provability logics.

In [1], Ardeshir and Mojtahedi, calculated the Σ_1-provability logic of Heyting arithmetic (HA), the intuitionistic version of PA. Mojtahedi in [4] has recently proven the extension of this result to full provability logic, thus calculating the provability logic of HA via its Σ_1-provability logic. This problem has been remarkably hard to solve, being open for four decades. In [11], Visser and Zoethout have given an alternative way of characterizing the Σ_1-provability of HA. This alternative method resembles Solovay's original proof for PA.

In the classical case, we know that Solovay's results have a great stability. In particular, arithmetical completeness holds for any Σ_1-sound extension of EA. The result of Mojtahedi, calculating the provability logic HA, makes this question appear also for the intutionistic case. Will subtheories of HA also behave uniformly with respect to arithmetical completeness? With this project we start to study this question. In particular, we focus in the Σ_1-provability logic of subtheories of HA. The main examples of these theories are: $\mathsf{iEA} + B\Sigma_1$ (intuitionistic elementary arithmetic with Σ_1-collection), $\mathsf{iI}\Sigma_1$ (intuitionistic Robinson's Arithmetic with induction for Σ_1-formulas) and iPRA (intuitionistic primitive recursive arithmetic).

We analyze the theorems that lead to the characterization made by Visser and Zoethout. The proof of this characterization can be divided in two parts: one related to Solovay's construction in the intuitionistic setting and one related to the NNIL algorithm, defined by Visser [9]. One of our main discoveries, is that one of the relevant properties needed for the construction, that is implicitely used for the HA case, is that the theory proves some degree of sentential reflection with provability predicates of its finite subtheories. This makes the tools hard to apply: for iPRA we only know that the first part works and for iEA and $\mathsf{iI}\Sigma_1$ neither of them work in the actual state. We prove that in fact, this happens since both theories are finitely axiomatizable. This mean that for being able to apply Visser and Zoethout construction, it is necessary to obtain a provability predicate whose logic is weaker than intuitionistic first order logic.

As a future work, it is left to study the relation of iPRA with the NNIL algorithm to check if the second part of the construction works. It is also left how to apply these tools to finite axiomatizable theories, which will require either a better understanding of arithmetical theories with fragments of first order logic or a new way of calculating the Σ_1-provability logic in the intuitionistic setting.

Acknowledgment

I would like to thanks Albert Visser for supervising my master thesis, providing insightful comments and ideas accross all the research — too many to list them here. I would also like to thank to Lev D. Blekemishev for the insight that PRA proves the Σ_1-reflection principles of Grzegorczyk arithmetics.

References

[1] Mohammad Ardeshir and Mojtaba Mojtahedi, *The Σ_1-provability logic of HA*, Annals of Pure and Applied Logic, 169(10):997-1043, 2018.

[2] Mohammad Ardeshir and Mojtaba Mojtahedi, *Reduction of provability logics to* Σ1*-provabiltiy logics*, Logic Journal of the IGPL, 23(5):842-847, 2015.

[3] Lev D. Beklemishev, *Bimodal Logics for Extensions of Arithmetical Theories*, The Journal of Symbolic Logic, Vol. 61, pp 91-124, 1996.

[4] Mojtaba Mojtahedi, *On Provability Logic of HA*, arXiv:2206.00445, 2022.

[5] W. Sieg, *Fragments of arithmetic*, Annals of Pure and Applied Logic, Vol. 35, pp. 161-185, 1994.

[6] Robert M. Solovay, *Provability Interpretations of Modal Logic*, Journal of Symbolic Logic, 46(3):661-662, 1981.

[7] Albert Visser, *A propositional logic with explicit fixed points*, Studia Logica, 40:155-175, 1981.

[8] Albert Visser, *On the completeness principle: A study of provability in Heyting's arithmetic and extensions*, Annals of Mathematical Logic, 22(3):263-295, 1982.

[9] Albert Visser, *Substitutions of Σ_1^0-sentences: explrations between intuitionistic propositional logic and intuitionistic arithmetic*, Annals of Pure and Applied Logic, 114(1):227-271, 2002.

[10] Albert Visser, *The Absorption Law, or How to Kreisel a Hilbert-Bernays-Löb*, Archive for Mathematical Logic, 60(3-4):441-468, 2020.

[11] Albert Visser and Jetze Zoethout, *Provability logic and the completeness principle*, Annals of Pure and Applied Logic, 170(6):718-753, 2019.

Security analysis of AMD SEV-SNP firmware ABI

Petar Paradžik[1], **Ante Đerek**[2], **Marko Horvat**[3]

[1,2] *Faculty of Electrical Engineering and Computing, University of Zagreb*
Unska 3, Zagreb, Croatia
[3] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička 30, Zagreb, Croatia
E-mail: [1]`petar.paradzik@fer.hr`, [2]`ante.derek@fer.hr`, [3]`mhorvat@math.hr`

Keywords:
formal verification, security protocols, secure virtualization, trusted execution environment, cloud computing, confidential computing

Building on their previous solutions for confidential computing, namely hardware accelerated memory encryption for data-in-use protection called Secure Encrypted Virtualization (SEV) and SEV with Encrypted State (SEV-ES), AMD recently proposed (in a 2020 white paper [1]) and implemented (in 2021, in their EPYC™ line of processors) an extension called Secure Nested Paging (SEV-SNP). We use the Tamarin prover tool [3] to formally verify the firmware ABI specification [2] of AMD SEV-SNP with respect to desirable security properties under the specified threat model.

Acknowledgment

This work has been supported by the European Union through the European Regional Development Fund, under the grant KK.01.1.1.01.0009 (DATACROSS).

References

[1] AMD. Strengthening VM isolation with integrity protection and more. White paper, `https://www.amd.com/system/files/TechDocs/56860.pdf`, 2020.

[2] AMD. SEV Secure Nested Paging Firmware ABI Specification (Revision 1.54). `https://www.amd.com/en/support/tech-docs/sev-secure-nested-paging-firmware-abi-specification`, 2022.

[3] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The TAMARIN prover for the symbolic analysis of security protocols. In *Computer Aided Verification: 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013.*, pages 696–701. Springer, 2013.

β-Conversion Rules in Simple Type Theory extended by Quotation and Evaluation Terms

Jiří Raclavský[1]

Masaryk University, Arne Novaka 1, Brno, 602 00, the Czech Republic
raclavsky@phil.muni.cz

1. Extension of simple type theory by evaluation terms

To increase expressive power, some programming languages (e.g. Lisp, and its sequels, see [3]), extend the language $\mathscr{L}$ of *simple type theory* (STT)[1] by two new terms (here denoted by):

$\ulcorner X \urcorner$ – *quotation* of the *term* X
$\llbracket X \rrbracket$ – *evaluation* of the *term* X

(For an analogous proposal aiming at natural language processing (NLP), see Tichý [10].)

Motivation of this paper: Investigating the extensions for better understanding (from the logical point of view) of programming and NLP using such $\mathscr{L}$s; see e.g. [3, 4] for more.

Using the familiar *Henkin-style semantics* for STT, let $\mathscr{V}_v(X)$ be short for $[\![X]\!]^{\mathscr{M}}_v$, where v is an *assignment*, $\mathscr{M}$ is a *model* $\langle \mathscr{F}, \mathscr{I} \rangle$, where $\mathscr{I}$ is an *interpretation function* from constants to objects of $\mathscr{F}$, and $\mathscr{F}$ is $\{\mathscr{D}_\tau \,|\, \tau \in \mathscr{T}\}$, where τ is a *type* belonging to the set of types $\mathscr{T}$ (consisting of the well-known hierarchy of function types), $\mathscr{D}_\tau$ is a *domain*, i.e. a set (of τ-objects) that interprets τ. Typically, $\mathscr{V}_v(X) = \mathtt{X}$. The *evaluation rules* for $\ulcorner X \urcorner$ and $\llbracket X \rrbracket$ are:

$\mathscr{V}_v(\ulcorner X \urcorner) = X$, where X/τ (read: X stands for an object $\mathtt{X}$ of type τ, i.e. $\mathtt{X} \in \mathscr{D}_\tau$).
$\mathscr{V}_v(\llbracket X \rrbracket) = \mathscr{V}_v(\mathtt{X})$, where $\mathtt{X} = \mathscr{V}_v(X)$ and (optionally) $\mathtt{X}, \llbracket X \rrbracket/\tau$.

In other words, while X represents $\mathscr{V}_v(X)$ (i.e. $\mathtt{X}$), $\ulcorner X \urcorner$ represents X itself and $\llbracket X \rrbracket$ represents $\mathscr{V}_v(\mathtt{X})$. As noted in [3], employment of $\ulcorner X \urcorner$ and $\llbracket X \rrbracket$ necessiates STT with *partial functions.*

Aims of the paper. Several problems with i. and ii. have recently been observed (some of them solved) by Farmer [3, 4], Tichý and his followers (e.g. [10, 7, 5, 8]). We use here a *partial* STT called TT^* [6] which lies between the systems of [3, 9, 10, 7, 8]). We focus on various *problems* related to β-conversion rules, cf. the next section, and propose *solutions* to them, *distinguishing two notions of β-conversion.*

2. Solutions to problems of β-converting abstractions with $\llbracket X \rrbracket$

Following the *ramified typing* of *procedural semantics* behind [10, 7, 6], $*^n$ is a type of nth-order computations X of objects $\mathtt{X}$ of various types $\tau_1, ..., \tau_m$. Let $x \in \mathscr{D}_{*^1}$ and $c \in \mathscr{D}_{*^2}$. However, $\llbracket c \rrbracket$ is *untypeable* [7], for e.g. $\mathscr{V}_{v_1}(\llbracket c \rrbracket) = x$ and x/τ_1, but e.g. $\mathscr{V}_{v_2}(\llbracket c \rrbracket) = y$ and y/τ_2, $\tau_1 \neq \tau_2$.

Problem 1. In [10, 7], body Y of the *abstraction* $\lambda x.Y$ must fulfil Y/τ, i.e. the above $Y := \llbracket c \rrbracket$ is excluded. Hence one easily avoids the following failure [5] of *β-contraction rule*

$$\beta_c \qquad [\lambda x.Y](Z) \vdash Y_{(Z/x)}$$

where $Y_{(Z/x)}$ is the result of substitution of Z for z in Y. Let $\mathscr{V}_v(x) = \mathtt{X}$ where x/τ (precisely,

[1] By Church [2], Andrews [1] and others ([3, 4]). $\mathscr{L}_{\mathsf{STT}}$: $\mathbf{a}$ (*constants*), x (*variables*), $Y(X)$ (*applications*), $\lambda x.Y$ (*abstractions*); auxiliary expressions: $(,), \lambda x.$ and for $\mathscr{L}_{\mathsf{STT}}$'s extensions by $\ulcorner X \urcorner$ and $\llbracket X \rrbracket$ also $\ulcorner, \urcorner, \llbracket, \rrbracket$.

x/τ^1, so $x \in \mathscr{D}_{*^1}$) and $\mathscr{V}_v(c) = x$ (while $c/*^1$, so $c \in \mathscr{D}_{*^2}$) and $\mathscr{V}_v(Z) = \mathtt{Z}$, Z/τ; keeping it fixed below. Thus, $\mathscr{V}_v([\lambda x.\llbracket c \rrbracket](Z)) = \mathtt{Z}$, for $\mathscr{V}_v(\lambda x.\llbracket c \rrbracket) = \mathtt{Id}$ (the identity mapping for objects of type τ), but $\mathscr{V}_v(\llbracket c \rrbracket_{(Z/x)}) = \mathtt{X}$ (where $\mathtt{X} \neq \mathtt{Z}$), for $x \notin FV(c)$ (read: x is not a free variable of c) and so $\llbracket c \rrbracket_{(Z/x)} = \llbracket c \rrbracket$. The failure of β_c thus: $\mathscr{V}_v([\lambda x.\llbracket c \rrbracket](Z)) \neq \mathscr{V}_v(\llbracket c \rrbracket_{(Z/x)})$.

Problem 2. The above problem with β_c (re)appears in case (2.a) with $\lambda x.(\llbracket c \rrbracket = x)$ which is *typeable* according to [10, 7]; and also in case (2.b) with $\llbracket X \rrbracket_\tau$ that is *restricted to* τ [8] (i.e. the above optional type condition for $\llbracket X \rrbracket_\tau$ is strictly required). Observe again that x which is not present/visible in $\llbracket c \rrbracket_\tau$ is 'activated' when evaluating the abstraction containing $\llbracket c \rrbracket_\tau$.

Solutions (S1) – (S2).

(S1) *Elimination of terms* $\llbracket X \rrbracket_\tau$ – because one may achieve their effect by evaluation functions-as-mappings $\mathtt{Eval}_\tau(\cdot)$ (v-constructed, for any v, by $\mathbf{Eval}_\tau$). Though the key source of Problem 2 (viz. $\llbracket X \rrbracket_\tau$s) was removed, the problem persists if one keeps the idea that $x \in FV(\mathbf{Eval}_\tau(c))$ when $\mathscr{V}_v(c) = x$; and uses the *'natural' evaluation rule for abstractions* ([9], [6]): $\mathscr{V}_v(\lambda x.Y) = \mathtt{f}$ such that for any v' the function $\mathtt{f}$ maps each $\mathscr{V}_{v'}(x)$ to $\mathscr{V}_{v'}(Y)$ where each v' that is distinct from the actual v only differs from v as regards values for x (this evaluation rule works perfectly for STT that is *not extended* by evaluation terms or terms involving $\mathbf{Eval}_\tau$).

(S2) *Different evaluation rules for abstractions.* Recall that on 'natural' evaluation rule for abstractions one considers v and assignments v' such that each v' is like v except for x's value. On *(A)-approach*, which is evidently embraced in [5] where Problem 1 was published, $\llbracket c \rrbracket_\tau$ is v'-evaluated in synchronicity with $v'(x)$. Thus, $\mathscr{V}_v(\lambda x.\llbracket c \rrbracket_\tau) = \mathtt{Id}$, for x is treated as *free* in $\llbracket c \rrbracket_\tau$. But on *(B)-approach*, that synchronicity is broken, for one evaluates $\llbracket c \rrbracket_\tau$ of $\lambda x.\llbracket c \rrbracket_\tau$ w.r.t. v only. $\mathscr{V}_v(\lambda x.\llbracket c \rrbracket_\tau)$ is a *constant mapping*, not $\mathtt{Id}$, for x is *not* treated as *free* in $\llbracket c \rrbracket_\tau$. Hence the above failure is prevented: $\mathscr{V}_v([\lambda x.\llbracket c \rrbracket](Z)) = \mathscr{V}_v(\llbracket c \rrbracket_{(Z/x)})$. In the *extended* STT, (B)-approach requires a *reformulation of evaluation rule for abstractions*, either i. 'substitutional' (using substitution of computations-as-constants; à Church [2]), or ii. 'objectual' (using substitution of computations acquired by quotation function $\mathtt{Quote}^\tau$).

References

[1] Andrews, Peter B. (1986): *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof*, Academic Press.

[2] Church, Alonzo (1940): A Formulation of the Simple Theory of Types, *The Journal of Symbolic Logic* 5(2): 56–68.

[3] Farmer, William M. (2016): Incorporating Quotation and Evaluation into Church's Type Theory: Syntax and Semantics, In: *Intelligent Computer Mathematics. CICM 2016. LNCS, vol 9791*, M. Kohlhase, M. Johansson, B. Miller B., L. de Moura and F. Tompa (eds.), Springer, 83–98.

[4] Farmer, William M. (2017): Theory Morphisms in Church's Type Theory with Quotation and Evaluation, In: *Intelligent Computer Mathematics. CICM 2017. LNCS, vol 10383*, H. Geuvers, M. England, O. Hasan, F. Rabe and O. Teschke (eds.), Springer, 147–162.

[5] Kosterec, Miloš (2021): Substitution Inconsistencies in Transparent Intensional Logic, *Journal of Applied Non-Classical Logics* 31(3–4): 355–371.

[6] Kuchyňka, Petr; Raclavský, Jiří (2023): Completeness in Partial Type Theory. *Journal of Logic and Computation. on-line first.* https://doi.org/10.1093/logcom/exac089

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

[8] Raclavský, Jiří (2022): The Rule of Existential Generalisation and Explicit Substitution, *Logic and Logical Philosophy* 31(1): 105–141.

[9] Tichý, Pavel (1982): Foundations of Partial Type Theory. *Reports on Mathem. Logic* 14: 57–72.

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

Minimization of normal forms

Andrea Sabatini

Scuola Normale Superiore di Pisa
Piazza dei Cavalieri 7
andrea.sabatini@sns.it

Keywords:
Classical logic, Boolean circuits, Proof theory, Structural reasoning.

Kleene's $\mathsf{G4}$ sequent calculus for classical propositional logic is a very manageable proof-theoretic tool, due to its nice structural properties: in particular, it can be used as a tool for decomposing any classically valid formula into a unique (disjunctive or conjunctive) normal form. We consider a variant of $\mathsf{G4}$ with contexts as sets, and extend it with rules for classically invalid sequents, thus taking a hybrid (anti)sequent calculus $\overline{\overline{\mathsf{G4}}}$ for classical logic: we use $\overline{\overline{\mathsf{G4}}}$ to decompose any (anti)sequent into a multiset of atomic (anti)sequents, and thus any classical formula into a unique normal form.

We show that any logical $\overline{\overline{\mathsf{G4}}}$ derivation can be translated into an operation on multisets of atomic (anti)sequents, and that any $\overline{\overline{\mathsf{G4}}}$ derivation of atomic (anti)sequents can be transformed into a derivation where all applications of Weakening (if any) are permuted last. This normal form result for structural $\overline{\overline{\mathsf{G4}}}$ derivations can be further refined for particular classes of atomic (anti)sequents, to the effect that structural $\overline{\overline{\mathsf{G4}}}$ derivations involving them can be put in Goclenian (dually, Aristotelian) normal form: this allows to give syntactical reformulations of results given by Gentzen himself [2, 8, 6].

For any set S of atomic antisequents, maximal application of the rewriting rule

$$\bigcup_{i=1}^{n}\{\Theta_i \dashv \Lambda_i\} \cup \{\Phi, \Theta'_1, \ldots, \Theta_j, \ldots, \Theta'_n \dashv \Lambda'_1, \ldots, \Lambda_k, \ldots, \Lambda'_n, \Psi\} \to \bigcup_{i=1}^{n}\{\Theta_i \dashv \Lambda_i\}$$

with $n \geq 1$, $1 \leq j, k \leq n$ – provided that for any $1 \leq j' \neq j, k' \neq k, j' \neq k' \leq n$, $\Theta'_{j'} = \Theta_{j'} \setminus \{p\}$ and $\Lambda'_{k'} = \Lambda_{k'} \setminus \{p\}$ for any $p \in \Theta_{j'} \cap \Lambda_{k'}$ – yields a reduct under Weakening and Cut [7] of S: we exploit our normal form result to show that a reduct under Weakening and Cut of S is a (possibly) reduced version of S where no antisequent can be dropped *modulo* logical equivalence. Moreover, if S is a consistent set of atomic antisequents and S^* is the closure under Cut of S, then maximal application of the rewriting rules

$$\{\Theta \dashv \Lambda, p\} \to \{\Theta \dashv \Lambda\} \text{ if } p, \Theta' \dashv \Lambda' \text{ with } \Theta' \subseteq \Theta,\ \Lambda' \subseteq \Lambda \text{ belonging to } S^*$$

$$\{p, \Theta \dashv \Lambda\} \to \{\Theta \dashv \Lambda\} \text{ if } \Theta' \dashv \Lambda', p \text{ with } \Theta' \subseteq \Theta,\ \Lambda' \subseteq \Lambda \text{ belonging to } S^*$$

yields a strengthening under Cumulative Cut of S: we prove that a strengthening under Cumulative Cut of a reduct under Weakening and Cut of S is a (possibly) reduced version of S where neither an antisequent nor an atom can be dropped *modulo* logical equivalence. We thus define a sequent-based procedure which decomposes any classically invalid formula into a unique irreducible normal form, and another one which decomposes any classically invalid formula into a minimal normal form – i.e., an irreducible normal form of minimal length. As a result, we get a proof-theoretic reformulation of the consensus method for the minimization of Boolean circuits [4].

We discuss the extension of our method to the case of G4ip sequent calculus for intuitionistic propositional logic [1, 3], and provide an approximate result of minimization for conditional normal forms [5] of intuitionistically invalid formulas.

References

[1] Dyckhoff R., *Contraction-free sequent calculi for intuitionistic logic*, The Journal of Symbolic Logic, 57, 1992.

[2] Gentzen G., *On the existence of independent axiom systems for infinite sentence systems*, in Szabo M. E. (ed.), *The collected papers of Gerhard Gentzen*, North-Holland, 1969.

[3] Hudelmaier J., *Bounds for cut elimination in intuitionistic propositional logic*, Archive for Mathematical Logic, 31, 1992.

[4] Mendelson E., *Theory and problems of Boolean algebra and switching circuits*, McGraw-Hill, 1970.

[5] Mints G., *Gentzen-type systems and resolution rules, part I*, COLOG-88, 1990.

[6] Moriconi E., *Early structural reasoning. Gentzen 1932*, Review of Symbolic Logic, 8, 2015.

[7] Piazza M., Pulcini G., *Uniqueness of axiomatic extensions of cut-free classical propositional logic*, Logic Journal of the IGPL, 24, 2016.

[8] Tennant N., *On Gentzen's structural completeness proof*, in Wansing H. (ed.), *Dag Prawitz on Proofs and Meaning.*

Non-Associative Non-Commutative Multi-Modal Linear Logic

Andre Scedrov

[1] *University of Pennsylvania*

Lambek's two calculi, the associative one [3] and the non-associative one [4], each have their advantages and disadvantages for the analysis of natural language syntax by means of categorial grammar. In some cases, associativity leads to over-generation, i.e., validation of grammatically incorrect sentences. In other situations, associativity is useful.

One approach, developed by Morrill [8] and Moortgat [5], begins with the associative calculus and reconstructs local non-associativity by means of the so-called bracket modalities, ultimately leading to Morrill's CatLog parser [9]. Bracket modalities interact in a subtle way with the subexponential modalities originating in linear logic. Our contributions to this approach include [2]. We have discussed this approach in several presentations at the recent LAP conferences.

Another approach, developed by Moot and Retoré [7], begins with the non-associative calculus and utilizes multi-modalities, ultimately leading to the Grail parser [6]. We enhance the latter approach in [1], showing that local associativity may be expressed by means of subexponentials. We discuss decidability and undecidability results. This is joint work with Eben Blaisdell, Max Kanovich, Stepan L. Kuznetsov, and Elaine Pimentel.

References

[1] Blaisdell, E., Kanovich, M., Kuznetsov, S.L., Pimentel, E., Scedrov, A. (2022). Non-associative, Non-commutative Multi-modal Linear Logic. In: Blanchette, J., Kovács, L., Pattinson, D. (eds) Automated Reasoning. IJCAR 2022. Lecture Notes in Computer Science(), vol 13385. Springer, Cham. https://doi.org/10.1007/978-3-031-10769-6_27

[2] Kanovich, M.I., Kuznetsov, S.G., Kuznetsov, S.L., Scedrov, A. (2022). Decidable Fragments of Calculi Used in CatLog. In: Loukanova, R. (eds) Natural Language Processing in Artificial Intelligence — NLPinAI 2021. Studies in Computational Intelligence, vol 999. Springer, Cham. https://doi.org/10.1007/978-3-030-90138-7_1

[3] Lambek, J.: The mathematics of sentence structure. Am. Math. Monthly 65(3), 154–170 (1958)

[4] Lambek, J.: On the calculus of syntactic types. In: Jakobson, R. (ed.) Structure of Language and Its Mathematical Aspects, pp. 166–178. American Mathematical Society (1961)

[5] Moortgat, M.: Multimodal linguistic inference. J. Logic Lang. Inform. 5(3–4), 349–385 (1996)

[6] Moot, R.: The grail theorem prover: type theory for syntax and semantics. CoRR, abs/1602.00812 (2016). arXiv:1602.00812

[7] Moot, R., Retoré, C.: The Logic of Categorial Grammars. LNCS, vol. 6850. Springer, Heidelberg (2012). `https://doi.org/10.1007/978-3-642-31555-8`

[8] Morrill, G.: Categorial formalisation of relativisation: Pied piping, islands, and extraction sites. Technical report LSI-92-23-R, Universitat Politècnica de Catalunya (1992)

[9] Morrill, G.: Parsing/theorem-proving for logical grammar CatLog3. J. Log. Lang. Inf. 28(2), 183–216 (2019). `https://doi.org/10.1007/s10849-018-09277-w`

Is there mathematical concepts that are real?

Zvonimir Šikić

According to [3], C. F. Gauss said: If $e^{i\pi} = -1$ was not immediately apparent to a student upon being told it, that student would never become a first-class mathematician. We will explore the arguments that support Gauss's claim in order to prove that there are no mathematical concepts that are real in Steiner's sense.

We conform to the position that concept exists if it satisfies the W. O. Quine's condition: Fs exist if $\exists x Fx$ is a theorem of a true theory; cf. [8]. But M. Steiner claims in [10] that it is possible for Fs to satisfy this condition without being real. His inspiration is P. Bridgman's definition of physical reality: Something is physically real if it is connected with physical phenomena independent of those phenomena which entered its definition; cf. [1] p.56.

There is something profoundly right in the idea that the real is that which has properties transcending those which enter its definition and Steiner's aim is to show that mathematical entities can occasionally be said to be real in exactly the same sense.

Quine's condition is applicable to the existence of mathematical entities: scientific theories are committed to the existence of mathematical entities, and since we regard some of them as true, we must regard mathematical entities as existent. However, according to Steiner, this is not an argument for the reality of mathematical entities.

To demonstrate the reality of an entity in the natural sciences one typically shows that the entity is indispensable in explaining some new phenomenon. In this way the entity acquires new and independent descriptions. Steiner applies the same idea in mathematics.

For example, π is real because we have at least two independent descriptions for π. Geometric, $\pi = \frac{C}{2r}$ and analytic, $\pi = \frac{\ln(-1)}{i}$. In the first case π is derived from the formula for the circumference of a circle C with radius r. In the second case π is derived from the special case of Euler's formula, $e^{pii} = -1$.

We know by deductive proof that the descriptions are coreferential (unlike the situation in the physical sciences where this is demonstrated empirically). But then, how can provably coreferential descriptions be regarded as independent? Steiner's answer is to distinguish between two kinds of proof of coreference in mathematics: those which are nonexplanatory and merely demonstrate the coreference, and those which explain it. Descriptions are independent if the proofs of their coreferentiality are nonexplanatory.

We show that the "independence of the descriptions of two mathematical entities" is not additionally explained by the "absence of explanatory proofs of their coreference", so we will stick with "independence" as a less vague criterion.

After a detailed analysis of the "reality status" of π, in the previously described context, we conclude that π is not real in Steiner's sense. As a matter of fact, it is difficult to prove for any mathematical concept that it is real in Steiner's sense. Namely, it is not enough to formulate two descriptions of a concept and find a proof of their coreference which keeps the descriptions independent. It should be proved that all proofs of their coreference are such.

But mathematical theories are deeply connected and in the entire history of mathematics, mathematicians are constantly striving to discover these connections. For example, it is typical for mathematicians to persistently search for new proofs of old theorems in order to discover these intertheoretical dependencies.

Hence, our hypothesis is that no mathematical concept is real in Steiner's sense.

References

[1] Bridgman P. W. The logic of modern physics, Macmillan, 1958.

[2] Bürgi, J. Arithmetische und Geometrische Progreß-Tabulen, Prag, 1620.

[3] Derbyshire, J. Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics, Joseph Henry Press, 2003.

[4] Mercator, N., Pitt, M., Godbid, W. Logarithmo-technia sive Methodus construendi logarithmos nova, accurata, & facilis, London, 1667.

[5] Napier, J. Mirifici Logarithmorum Canonis descriptio, Edinburgh, 1619.

[6] Nagel, E. The Structure of Science: Problems in the Logic of Scientific Explanation, Harcourt, 1961.

[7] Newton, I. De analysi per aequationes numero terminorum infinitas, sent by Dr. Barrow to Mr. Collins in a letter dated July 31. 1669.

[8] Quine, W.O. On What There Is, The Review of Metaphysics 2 (5), 21-38, 1948.

[9] Steiner, M. Mathematical explanation, Philosophical Studies 34 (2), 135 – 151, 1978.

[10] Steiner, M. Mathematical Realism, Nous 17 (3), 383-395, 1983.

[11] Šikić, Z. Differential and integral calculus (in Croatian), Profil, 2008.

On the Impact of Local Differential Privacy on Simpson's Paradox

Tamara Stefanović [1], Selene Cerna [2], Héber H. Arcolezi [2], Karima Makhlouf [2], Catuscia Palamidessi [2]

[1] *Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia*
[2] *Inria and École Polytechnique (IPP), Palaiseau, France*

E-mail: [1] `tstefanovic@uns.ac.rs`, [2] `selene-leya.cerna-nahuis@inria.fr`, [3] `heber.hwang-arcolezi@inria.fr`, [4] `karima.makhlouf@inria.fr`, [5] `catuscia.palamidessi@inria.fr`

Keywords:
Simpson's Paradox, Differential Privacy, Randomized Response.

Human decision-making has relied on statistical analysis for decades. However, several statistical paradoxes have raised questions about human intuition. One of the most well-known paradoxes is Simpson's paradox, also known as the Yule-Simpson effect. Simpson's paradox is a statistical phenomenon that occurs when an association between two variables is observed in sub-populations but disappears or reverses when the sub-populations are combined. This phenomenon is also relevant for the analysis of *fairness*: a decision can appear as biased against one group when examined globally, while it is actually fair, or even biased against the other group, when examined in the sub-population.

There are numerous examples of Simpson's paradox, such as the Berkeley admission [1], kidney stone treatment [2], baseball batting averages [3], COVID-19 death rates in Italy and China, just to cite a few.

Simpson's paradox has been extensively analyzed by mathematicians and statisticians such as Pearson [4], Yule [5], Simpson [6], Blyth [7], Gardner [8], Good and Mittal [9], Lindley and Novick [10], Hand [11], and many others. However, there are still certain aspects of the paradox that have not been sufficiently addressed. One such issue is the quantification of the paradox's strength. Existing classifications on Yule's paradox, Association Reversal, and Amalgamation paradox do not provide enough information about the magnitude of the paradox.

Furthermore, it can be observed that in several examples of Simpson's paradox, sensitive attributes such as gender, vaccination status, etc., play a key role. This type of data should be protected using various privacy techniques before its use. One of these techniques is differential privacy (DP) [12, 13], which involves incorporating controlled random noise into the original data (or analysis). This raises a new question: How does the obfuscation of the data through randomized response (RR) [14, 15] affect the presence of the paradox in a given dataset? RR is a data collection method in which the true value is reported with probability p, while the rest of the probability is distributed uniformly on the other values.

In this paper, we introduce a novel measure to quantify the strength of Simpson's Paradox. Additionally, we analyze the impact of satisfying DP through RR on Simpson's Paradox, both theoretically and empirically.

References

[1] P. J. Bickel, E. A. Hammel, and J. W. O'Connell. Sex bias in graduate admissions: Data from Berkeley. Science, 187(4175):398–404, 1975.

[2] Steven A Julious and Mark A Mullee. Confounding and simpson's paradox. BMJ, 309(6967):1480–1481, 1994

[3] K. Ross. A Mathematician at the Ballpark: Odds and Probabilities for Baseball Fans. Penguin Publishing Group, 2007.

[4] Karl Pearson, Alice Lee, and Leslie Bramley-Moore. Mathematical contributions to the theory of evolution. vi. genetic (reproductive) selection: Inheritance of fertility in man, and of fecundity in thoroughbred racehorses. Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character, 192:257–330, 1899.

[5] G. Udny Yule. Notes on the theory of association of attributes in statistics. Biometrika, 2(2):121–134, 1903.

[6] E. H. Simpson. The interpretation of interaction in contingency tables. Journal of the Royal Statistical Society. Series B (Methodological), 13(2):238–241, 1951.

[7] Colin R. Blyth. On simpson's paradox and the sure-thing principle. Journal of the American Statistical Association, 67(338):364–366, 1972.

[8] Martin Gardner. Mathematical games. Scientific American, 234(3):119–125, 1976

[9] I. J. Good and Y. Mittal. The amalgamation and geometry of two-by-two contingency tables. The Annals of Statistics, 15(2):694–711, 1987

[10] D. V. Lindley and Melvin R. Novick. The role of exchangeability in inference. The Annals of Statistics, 9(1):45–58, 1981.

[11] David J. Hand. Deconstructing statistical questions. Journal of the Royal Statistical Society. Series A (Statistics in Society), 157(3):317–356, 1994.

[12] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography, pages 265–284. Springer Berlin Heidelberg, 2006.

[13] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4):211–407, 2014.

[14] Stanley L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. Journal of the American Statistical Association, 60(309):63–69, 1965.

[15] Peter Kairouz, Keith Bonawitz, and Daniel Ramage. Discrete distribution estimation under local privacy. In Int. Conf. on Machine Learning, pages 2436–2444. PMLR, 2016.

New forms of distributed knowledge

Thomas Studer

Institute of Computer Science
Neubrückstrasse 10, 3012 Bern, Switzerland
E-mail: thomas.studer@unibe.ch

Keywords:
Epistemic logic, distributed systems, simplicial complexes.

In formal epistemology, group knowledge is often modeled as the knowledge that the group would have if the agents share all their individual knowledge. However, this interpretation does not account for relations between agents. In this work, we propose the notion of synergistic knowledge, which makes it possible to model different relationships between agents.

To do so, we present a novel semantics for modal logic that is based on simplicial complexes. In our logic, a group of agents may know more than just the deductive closure of the joint individual knowledge. That is our epistemic operators support a principle that could be paraphrased as *the sum is greater than its parts*, hence the name *synergistic knowledge.*

Synergistic knowledge may occur, for instance, when agents communicate through shared objects. As examples, we investigate the use of consensus objects and the problem of dining cryptographers. Moreover, we show that our logic can also model network topology, which we illustrate with an example of a missing communication link.

This talk is based on [1], which is joint work with Christian Cachin and David Lehnherr.

References

[1] Cachin, C., Lehnherr, D., Studer, T., *Synergistic Knowledge*, submitted, 2023.

Reasoning about Cyberphysical Systems using Rewriting Modulo Constraints

Carolyn Talcott

Modeling cyber-physical systems, such as autonomous vehicles, factory robots, surveillance drones, ..., involves interaction of discrete controllers and continuous evolution of physical state. Traditional verification methods such as reachability analysis and model-checking suffer from state space explosion. Furthermore, each analysis covers one instance, from infinitely many possibilities. The analyses assume a closed system. By using patterns (terms with variables) paired with constraints on values of variables one can begin to address these problems using rewriting modulo constraints.

In this talk we will briefly review rewriting logic and its application to modeling cyberphysical systems. We will introduce the extension of rewriting to rewriting modulo constraints, including its soundness and completenss properties. We will give examples of how rewriting modulo constraints can be used to address some of the challenges in verifying cyber-physical systems and discuss some of the challenges in automating proofs of key properties of such systems.