8$^{\text{TH}}$ International Conference

Logic and Applications

LAP 2019

September 23 - 27, 2019
Dubrovnik, Croatia

Book of Abstracts

Course directors:

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

IUC Inter University Centre Dubrovnik

Book of Abstracts of the 8$^{\text{th}}$ International Conference on Logic and Applications - LAP 2019, held at the Inter University Center Dubrovnik, Croatia, September 23 - 27, 2019.

LaTeX book of abstracts preparation and typesetting:

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

LAP 2019 Web site: `http://imft.ftn.uns.ac.rs/math/cms/LAP2019`
Maintained by Nenad Savić, University of Bern and University of Novi Sad

Contents

(In)Efficiency
and Reasonable Cost Models

Beniamino Accattoli

Inria & École Polytechnique

E-mail: beniamino.accattoli@inria.fr

Keywords: lambda calculus, cost models, functional programming.

The aim of the talk is explaining the problem of reasonable time cost models for the λ-calculus. *Reasonable* here is a technical word that essentially means polynomially equivalent to the time cost model of Turing machines. It is a fundamental problem, easily explainable to most computer scientists, and its solutions are technically demanding. Still, for a long time it attracted surprisingly little attention. The reason—we believe—is the fact that some of its facets are subtle, if not counterintuitive.

In the last few years the study of cost models for the λ-calculus has made considerable advances, starting in 2014 with the proof by Accattoli and Dal Lago that the leftmost-outermost (LO) evaluation strategy is reasonable [1]—a strategy is reasonable when its number of steps provides a reasonable cost model. On the one hand, that result strengthened results about weak strategies (in which evaluation does not enter into function bodies) by Blelloch and Greiner in 1995 [6], by Sands, Gustavsson, and Moran in 2002 [11], and those followed by combining the results by Dal Lago and Martini in 2009 in [10] and [7]. On the other hand, it counter-balanced Asperti and Mairson's 1998 result that Lévy's optimal strategy does not provide a reasonable cost model [4]. The advance required a new understanding of the problem, that in turn triggered a more systematic and still ongoing exploration, that clarified various points. This talk tries to sum them up and present them to a not-so-specialised audience.

Reasonable and efficient strategies. One of the motivations behind this talk is the fact that the problem is generally misunderstood, even by experts of the λ-calculus, as being about the efficient evaluation of λ-terms. In the λ-calculus evaluation is non-deterministic and different evaluation strategies may indeed behave very differently with respect to the number of steps. The situation is subtle: the λ-calculus is *confluent*, that is, the result is unique when it exists, therefore non-determinism is not about different results, but about different ways of obtaining the result. Moreover, some evaluation strategies may diverge even when the result exists, so that the way the result is computed is essential.

At first look then, the problem is about the choice of the evaluation strategy, and one would assume that a reasonable strategy must be an efficient one. Intuition, however, is misleading: *reasonable* and *efficient* are unrelated properties of strategies. Roughly, efficiency is a *comparative* property, it makes sense only if there are many strategies and one aims at comparing them. Being reasonable instead is a property of the strategy itself, independently of any other strategy, and it boils down to the fact that the strategy can be implemented with a negligible overhead.

Efficiency for reasonable strategies. Saying that *reasonable* and *efficient* are orthogonal properties of strategies is however slightly misleading, because it underestimates the value of the study of reasonable cost models. The study of efficiency, indeed, strikingly simplifies for reasonable strategies. For a reasonable strategy, one can take the number of its steps as a reasonable cost model because, roughly, every step can be considered to have cost 1, *i.e.* to be an atomic operation. Then two reasonable strategies can be compared for efficiency by simply comparing how many steps they take on the same term. When strategies are not known to be reasonable, instead, it is not clear how to compare them for efficiency, because their steps cannot be assumed to have cost 1. The idea that the efficiency of a strategy is given by its number of steps is indeed based on the hidden assumption that the strategy is reasonable.

Very few evaluation strategies have been proved reasonable, and there is at least one example of unreasonable strategy. As proved by Asperti and Mairson, a single step of Lévy's optimal strategy can have exponential cost (in the size of the initial term and the number of previous steps). For unreasonable strategies the natural way then is to compare how many steps *their implementations* take on the same term. Such a way of proceeding has however various drawbacks. First, it depends very much on the implementation of the fixed strategies, and so it hardly is a property of the strategy itself. Second, the cost is much harder to analyse, because it depends on the many details of the fixed implementation. Last, it is an approach that somewhat clashes with the machine-independent character of the λ-calculus. There can be other ways of comparing unreasonable strategies, but far from the simplicity provided by reasonable strategies. For Lévy's optimal strategy, for instance, some works [3, 5, 8, 9] have been able to shed some light on some aspects of its efficiency, and there are examples where it provides a considerable speed-up. Nonetheless, after almost 40 years since its introduction, it is still unclear whether in the general case it is efficient or not.

Reasonable optimisations. There is a further reason why the study of reasonable cost models turns out to be relevant for efficiency. Proving that a strategy is reasonable always requires some form of sharing, because the naive way of implementing β-reduction suffers of exponential overhead. Different strategies however require different forms of sharing and different optimisations. A close look shows that these techniques are general optimisation principles independent from the efficiency of the strategy, and composable in a modular way. In particular, some of them have been first developed for the inefficient case of LO evaluation, but they apply to more efficient strategies such as call-by-value or call-by-need. One of them, called *substituting abstractions on demand*—

introduced without a name by Accattoli and Dal Lago in [1] and then studied more closely by Accattoli and Guerrieri in [2]—is essential for reasonable implementations of strong strategies, but—to the best of our knowledge—no tool based on the λ-calculus implements it. Therefore, no such tool, like for instance Coq or Isabelle, relies on a reasonable implementation: the study of cost models may thus impact on the theory of implementations, providing more efficient implementations of given strategies.

References

[1] Beniamino Accattoli and Ugo Dal Lago. (Leftmost-Outermost) Beta-Reduction is Invariant, Indeed. *Logical Methods in Computer Science*, 12(1), 2016.

[2] Beniamino Accattoli and Giulio Guerrieri. Implementing open call-by-value. In *FSEN 2017*, pages 1–19, 2017.

[3] Andrea Asperti, Paolo Coppola, and Simone Martini. (optimal) duplication is not elementary recursive. In *POPL 2000*, pages 96–107, 2000.

[4] Andrea Asperti and Harry G. Mairson. Parallel beta reduction is not elementary recursive. In *POPL*, pages 303–315, 1998.

[5] Patrick Baillot, Paolo Coppola, and Ugo Dal Lago. Light logics and optimal reduction: Completeness and complexity. *Inf. Comput.*, 209(2):118–142, 2011.

[6] Guy E. Blelloch and John Greiner. Parallelism in sequential functional languages. In *FPCA*, pages 226–237, 1995.

[7] Ugo Dal Lago and Simone Martini. Derivational complexity is an invariant cost model. In *FOPARA 2009*, pages 100–113, 2009.

[8] Stefano Guerrini, Thomas Leventis, and Marco Solieri. Deep into optimality – complexity and correctness of sharing implementation of bounded logics. Proceedings of the DICE 2012 Workshop.

[9] Stefano Guerrini and Marco Solieri. Is the optimal implementation inefficient? elementarily not. In *FSCD 2017*, pages 17:1–17:16, 2017.

[10] Ugo Dal Lago and Simone Martini. On constructor rewrite systems and the lambda calculus. *Logical Methods in Computer Science*, 8(3), 2012.

[11] David Sands, Jörgen Gustavsson, and Andrew Moran. Lambda calculi and linear speedups. In *The Essence of Computation*, pages 60–84, 2002.

A Multiset Rewriting Model for the Specification and Verification of Resource and Timing Aspects of Security Protocols

Abraão Aires Urquiza[1], **Musab A. AlTurki**[2,3], **Max Kanovich**[4,5], **Tajana Ban Kirigin**[6], **Vivek Nigam**[10,1], **Andre Scedrov**[8,5], **Carolyn Talcott**[9]

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

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

[3] *Runtime Verification Inc., USA*

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

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

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

[10] *fortiss, Munich, Germany*

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

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

Keywords:

Security Protocols, Dolev-Yao Intruder, Denial of Service Attacks, Distance-bounding protocols, Multiset Rewriting, Computational Complexity.

Protocol security verification is one of the best success stories of formal methods. Tools can automatically discover logical attacks and many new attacks have been found by existing methods. However, other aspects important to protocol security are not covered by many formal models. Time and resources are some of such aspects. For example, Denial of Service (DoS) attacks have been a serious security concern, as no service is, in principle, protected against them. Although a Dolev-Yao intruder with unlimited resources can trivially render any service unavailable, DoS attacks do not necessarily have to be carried out by such (extremely) powerful intruders. It is useful in practice and more challenging for formal protocol verification to determine whether a service is vulnerable even to resource-bounded intruders that cannot generate or intercept arbitrary large volumes of traffic. Similarly, formal intruder models should take into account the physical properties related to time, such as message transmission time and processing delays. Other timing aspects of protocols, such as timeouts, may affect protocol execution and security.

This paper describes the use of Multiset Rewriting for the specification and verification of resource and timing aspects of protocols, such as network delays, timeouts, distance bounding properties and DoS attacks. We propose a novel, more refined intruder model where the intruder can only consume at most some specified amount of resources in any given time window. Additionally, we propose protocol theories that may contain timeouts and specify service resource usage during protocol execution.

We detail these timed features with a number of examples and describe decidable fragments of related secrecy problem as well as false acceptance and false rejection problems related to distance bounding protocols.

We also illustrate the power of our approach by representing a number of classes of DoS attacks, such as, Slow, Asymmetric and Amplification DoS attacks, exhausting different types of resources of the target, such as, number of workers, processing power, memory, and network bandwidth. We show that the proposed DoS problem is undecidable in general and is PSPACE-complete for the class of resource-bounded, balanced systems.

Acknowledgments

Part of this work was done during the visits to the University of Pennsylvania by Alturki, Ban Kirigin, Kanovich, Nigam, and Talcott, which were partially supported by ONR grant N00014-15-1-2047 and by the University of Pennsylvania. Ban Kirigin is supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219. Scedrov is partially supported by ONR grants N00014-15-1-2047 and N00014-18-1-2618. The participation of Kanovich and Scedrov in the preparation of this article was partially within the framework of the HSE University Basic Research Program funded by the Russian Academic Excellence Project '5-100'. Talcott is partly supported by ONR grant N00014-15-1-2202 and NRL grant N0017317-1-G002. Nigam is partially supported by NRL grant N0017317-1-G002, and CNPq grant 303909/2018-8.

References

[1] A. Aires Urquiza, M.A. AlTurki, M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Resource-Bounded Intruders in Denial of Service Attacks. 32nd IEEE Computer Security Foundations Symposium, Hoboken, New Jersey, USA, June 2019.

[2] Musab A. Alturki, Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, Carolyn Talcott. A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols. In J.D. Guttman et al., eds., Foundations of Security, Protocols, and Equational Reasoning, Springer LNCS Volume 11565, Springer-Verlag, pp-1-22, 2019.

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

[4] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Compliance in real time multiset rewriting models. Available at *https://arxiv.org/abs/1811.04826*.

[5] M. I. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Time, computational complexity, and probability in the analysis of distance-bounding protocols. *Journal of Computer Security*, 25(6):585–630, 2017.

[6] C. A. Meadows. A cost-based framework for analysis of denial of service networks. *Journal of Computer Security*, 9(1/2):143–164, 2001.

[7] J. Mirkovic and P. Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

EXPTIME-completeness of CPDL$^{(\neg)}$

E. V. Kostylev[1], J. L. Reutter[2], D. Vrgoč[3], V. Čačić[4]

[1] *Oxford University*
Oxford Road, Oxfordshire, Oxford, UK
[23] *PUC Chile and Center for Semantic Web Research*
Vicuna Mackenna 4860, Edificio San Agustin, 4to piso, Macul 7820436, Santiago, Chile
[4] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail:[1] egor.kostylev@cs.ox.ac.uk,[23] {jreutter,dvrgoc}@ing.puc.cl,[4] veky@math.hr

LAP, Dubrovnik — September 2019

Keywords:
Description logic, CPDL, EXPTIME

One of applications of modal logic in computer science is the theoretical foundation of *description logic*, which was born out of need to represent knowledge; precisely, to construct basic building blocks that are reusable in representing similar knowledge. The language DL-Lite was developed [1] in an attempt to bring description logic closer to potential applications, such as web ontologies (OWL is the most famous one). A modern trend in representing ontologies of description logics is the use of the language Xpath (XML Path Language), which is a natural fit for this purpose due to its intended idea of supporting the forming and answering of queries over a concrete graph, the DOM tree (Document Object Model), for describing the structure of documents on the Web. This idea was developed in [2].

An important, long known relationship between modal and description logic connects the multimodal system K (basic Kripke system with multiple modal operators) with the basic description logic $\mathcal{ALC}$ (Attributive concept Language with Complements). By adding queries over paths in graphs expressed by regular expressions, we get the logic $\mathcal{ALC}_{\mathrm{reg}}$, which corresponds to modal propositional dynamic logic (PDL); concepts correspond to propositional variables, and roles to programs. However, PDL has a wide variety of extensions, and it is not always clear which description logics they correspond to. Currently the "taxonomy" of description logics is better developed than of modal logics, and we often do not have as precise complexity results as we might want, i.e. as we might surmise based on what we know from applications.

One example is the logic CPDL$^{(\neg)}$, in which it is possible (apart from the usual operators from propositional dynamic logic, like negation, conjunction and disjunction of concepts, and tests, unions, compositions and iterations of programs) to consider the converses of programs (interpreted as inverses of binary relations) and the negations of atomic programs. We know from [3] that

PDL$^{(\neg)}$ (i.e. PDL with negations of atomic programs, but with no converses) is EXPTIME-complete, and we prove the same thing for CPDL$^{(\neg)}$.

Last year, at LAP2018, we laid the path to the proof, but it still lacked a big part of work: construction of Büchi automata recognizing the Hintikka trees for a CPDL$^{(\neg)}$-formula. Since the emptyness problem of Büchi-recognizable languages is decidable in polynomial time, and Hintikka trees exist for all (and only for) satisfiable formulas, the only thing left to prove is that the automaton size is exponentially bounded by the size of the starting formula. In order to do that, we need to employ some technical tricks: for example, instead of path formulas as regular expressions, we represent them as nondeterministic finite automata—the benefit being that it's much easier to control the size of "intermediate" automata, than the size of regular expression "derivatives" [5], which would otherwise be a much more natural and "mathematical" way to describe the problem.

References

[1] Diego Calvanese et al., *DL-Lite: Tractable Description Logics for Ontologies*, 2005

[2] Egor V. Kostylev, Juan L. Reutter, Domagoj Vrgoč, *XPath for DL Ontologies*, 2015

[3] Carsten Lutz, Dirk Walther, *PDL with Negation of Atomic Programs*, 2005

[4] Vedran Čačić, *Complexity of some fragments of description logics*, 2018

[5] Janusz A. Brzozowski, *Derivatives of regular expressions*, 1964

Rearranging absolutely convergent well-ordered series in Banach spaces

Vedran Čačić[1], Marko Doko[2], Marko Horvat[3]

[1,3] *Department of Mathematics, University of Zagreb*
Bijenička 30, Zagreb, Croatia
[2] *MPI-SWS*
Paul-Ehrlich-Str. 26, Kaiserlautern, Germany
E-mail: [1] veky@math.hr, [2] mdoko@mpi-sws.org, [3] mhorvat@math.hr

Keywords:
Well-ordered series, summability, absolute convergence, reordering, Banach spaces, ordinals.

Jointly with Domagoj Vrgoč, we showed that for every absolutely convergent series of real numbers, if its terms are rearranged with respect to any countable ordinal, the newly formed well-ordered series is also absolutely convergent and has the same sum:

Let $\alpha, \beta \in \omega_1 \backslash \omega$ and let $\Sigma(a_i)_{i\in\alpha}$ be an absolutely convergent well-ordered series. Then for all bijections $f\colon \beta \to \alpha$, the well-ordered series $\Sigma(a_{f(i)})_{i\in\beta}$ absolutely converges and

$$\sum_{i\in\beta} a_{f(i)} = \sum_{i\in\alpha} a_i \,.$$

However, our definition of well-ordered series as well as the proof were tailored to the setting of real numbers. Now we present an elegant proof of a consequently more general reordering principle, where the definition of well-ordered series is extended to Banach spaces.

Acknowledgment

This work is supported by the Croatian Science Foundation, project no. 7459 (CompStruct).

On uniqueness of gradual semantics for abstract argumentation

Dragan Doder

IRIT, University Paul Sabatier, Toulose
dragan.doder@irit.fr

Argumentation is a reasoning approach based on the justification of claims by arguments. It has been used for solving different Artificial Intelligence problems, including decision making, reasoning with defeasible information and classification. An argumentation framework is a directed graph, in which the nodes represent arguments, and the edges represent attacks between pairs of arguments.

Gradual semantics are methods of evaluating arguments in graphs, that assign to each argument a numerical value, representing its strength. They are usually defined by a set of equations relating the strengths of arguments. Those equations impose that the strength of an argument a is calculated by composing two functions: the first *aggregates* the strengths of all direct attackers of the argument a, calculating the overall strength of attacks toward a, and the other for computing the *effect* of the overall attack on the strength of a. The main problem in this approach is whether those equations define a unique gradual semantics, i.e., if the set of equations has an unique solution.

In this talk, I will present different approaches for defining gradual semantics from the literature, and investigate if those approaches uniquely characterize a semantics. Then I will propose a set of properties for the aggregation and effect functions, which ensures the uniqueness of the corresponding semantics. I will also analyze the properties against the set of postulates for gradual semantics proposed in the literature.

Justifications and Incomplete Information

Dragan Doder[1], **Zoran Ognjanović**[2], **Nenad Savić**[3], **Thomas Studer**[3]

[1] *Université Paul Sabatier – CNRS, IRIT, Toulouse, France*
[2] *Mathematical Institute of SASA, Belgrade, Serbia*
[3] *Institute of Computer Science, University of Bern, Bern, Switzerland*

Since the seminal paper about justification logics was published, [2], a whole family of justification logics has been established, including logics with uncertain justifications, see [4, 5, 7, 8].

The main feature of justification logics are formulas of the form $t : \alpha$ meaning that *t justifies α*. We are interested in logics with incomplete information distuinguishing the following three cases how $t : \alpha$ can contain incomplete information:

1) *"t" is incomplete.* A friend tells me that she read in *some* newspaper that α is true. I know that she reads only newspapers A and B and that newspaper B provides more reliable information than A meaning that if α was read in A, my degree of belief is equal to r and if α was read in B, my degree of belief is equal to s, where $r < s$. As a consequence of incomplete justification t (she read in *some* newspaper and did not specify in which one), my degree of belief that α is true lies in an interval $[r, s]$.

2) *":" is incomplete.* I see a friend across the street and shout out to him. Another person, standing close to him turns her head. The reason why she turned her head can be that she saw something in that direction or she thought that I was calling her. In this case, both t (I shout) and α (she turned her head) are clear, the only thing that is questionable is if t is the justification for α and thus my degree of belief for the whole formula $t : \alpha$ belongs to some interval.

3) *"α" is incomplete.* Throwing a stone over the wall towards two glass bottles and then hearing a crack sound tells me that either one of the two bottles cracked or both of them. In this case, t (I threw a stone) is certain, as well as ":" (stone hit bottle(s)). The incompleteness arises from the fact that formula α is of the form $\beta \vee \gamma$ since we do not know which bottle cracked.

The third case can be formalized by extending the justification logic J, see e.g. [6], by a list of unary operators, $P_{\geq s}$, with an intended meaning 'the probability is greater or equal to s'. Thus, saying that justification t is a justification for a formula $\alpha \equiv \beta \vee \gamma$ can be represented by associating the probabilities r to β and s to γ. Written in this language it would have the following form: $t : P_{=r}\beta$ and $t : P_{=s}\gamma$. This formalization has already been done in [5].

In this paper we formalize the first two cases. Namely, we provide a new logic, ILUPJ[1], as an extension of the justification logic J with two families of unary operators $L_{\geq s}$ and $U_{\geq s}$, for $s \in \mathbb{Q} \cap [0, 1]$. The intended meanings of these operators are that 'the lower (upper) probability is greater or equal to s'. Therefore, saying that our degree of belief lies in an interval $[r, s]$ is represented by saying that the lower probability is equal to r and the upper probability is equal to s.

The first case, when "t" is incomplete and therefore our belief that α is true belongs to an interval $[r, s]$ we can represent in the logic ILUPJ with $t : L_{=r}\alpha$ and $t : U_{=s}\alpha$. The second case, when ":" is incomplete, i.e., situations in which we are not sure if t is the justification for α, can be represented by $L_{=r}(t : \alpha)$ and $U_{=s}(t : \alpha)$.

Semantically, lower and upper probabilities are captured as follows: For a given set of finitely additive probability measures, P, the upper probability of an event X is given by the function

$$P^*(X) = \sup\{\mu(X) \mid \mu \in P\},$$

and the lower probability of an event X is given by the function

$$P_*(X) = \inf\{\mu(X) \mid \mu \in P\}.$$

Models are Kripke-style models where we assign to each world a (lower and upper-)probabilistic space, that is a non-empty set of worlds equipped with:

a) an algebra; b) basic J_{CS}-evaluations;

c) a *set* of finitely additive probability measures.

Using Anger and Lembcke's characterization of upper and lower probabilities with a finite number of properties, [1], we provide an axiomatization of our logic similar to the axiomatization of the logic ILUPP, see [3]. The difference lies in the fact that we need to take care that all axioms and inference rules of the logic J are included. The soundness theorem is proved in a straightforward way and for the strong completeness theorem we use a strategy that is a combination of the completeness proofs for the logics J and ILUPP, [3, 7, 9]. Namely we:

1) Prove the Deduction Theorem, as well as a few auxiliary lemmas.

2) Prove Lindenbaum's Lemma: Every consistent set of formulas can be extended to a maximal consistent set.

[1] I stands for iterations, LUP for lower and upper probabilities and J for the justification logic J.

3) Prove strong completeness by a canonical model construction.

Our last goal is to prove that the logics PJ and PPJ, from [5] and [4], respectively, are special cases of the logic ILUPJ. From the semantic point of view, it is clear that our semantics is a generalization of the semantics of PJ and PPJ since we have sets of finitely additive probability measures. Thus, setting that these sets must be singletons, we obtain the models of PJ and PPJ.

Axiomatization is a bigger challenge. Namely, the idea is to add an additional axiom of the form $\vdash U_{\geq r}(t:\alpha) \to L_{\geq r}(t:\alpha)$, basically saying that these two operators coincide (since it can easily be proved that $\vdash L_{\geq r}(t:\alpha) \to U_{\geq r}(t:\alpha)$). In that sense we have an extension of the logic J with "one" operator and the idea is to infer all of their axiom from ours.

References

[1] B. Anger, J. Lembcke. Infinitely subadditive capacities as upper envelopes of measures. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 68: 403–414. 1985.

[2] S. N. Artemov. Explicit provability and constructive semantics. *BSL*, 7(1):1–36, Mar. 2001.

[3] D. Doder, N. Savić, Z. Ognjanović. A Decidable Multi-agent Logic with Iterations of Upper and Lower Probability Operators. In: Proc. of FoIKS, Lecture Notes in Computer Science, Springer 170–185. 2018.

[4] I. Kokkinis, P. Maksimović, Z. Ognjanović, and T. Studer. First steps towards probabilistic justification logic. *Logic Journal of IGPL*, 23(4):662–687, 2015.

[5] I. Kokkinis, Z. Ognjanović, and T. Studer. Probabilistic justification logic. In S. Artemov and A. Nerode, editors, *LFCS 2016*, volume 9537 of *LNCS*, pages 174–186. Springer, 2016.

[6] R. Kuznets and T. Studer. Justifications, ontology, and conservativity. In T. Bolander, T. Braüner, S. Ghilardi, and L. Moss, editors, *Advances in Modal Logic, Volume 9*, pages 437–458. College Publications, 2012.

[7] R. Kuznets and T. Studer. *Logics of Proofs and Justifications.* College Publications.

[8] R. S. Milnikel. The logic of uncertain justifications. *APAL*, 165(1):305–315, 2014.

[9] N. Savić, D. Doder, Z. Ognjanović. Logics with Lower and Upper Probability Operators. *International Journal of Approximate Reasoning*, 88: 148–168. 2017.

Minimization of the d-measure of divergence from the compromise

Aleksandar Hatzivelkos[1], **Branimir Stojanović**[2]

[1] *University of Applied Sciences Velika Gorica*
Zagrebačka 5, Velika Gorica, Croatia
[2] *University of Zagreb, Faculty of Teacher Education*
Savska 77, Zagreb, Croatia
E-mail: [1]hatzi@vvg.hr, [2]branimir.stojanovic@ufzg.hr

Keywords:
social choice theory, compromise, measure of divergence from compromise.

This work is based on a mathematical model for description of a compromise within social choice theory. With d-measure of divergence from a compromise that certain candidate is placed on certain position, new mathematical structure is introduced. In order to maximize compromise (or minimize a d-measure of divergence from compromise), different methods can be used. In this paper we explore properties of a social welfare function TdM, which is defined as a function which minimizes total sum of d-measures of divergence over all possible linear orderings.

Motivation for this work comes form the exploration of the mathematical model for the notion of compromise over lineary ordered profiles [1, 2]. In this model, d-measure of divergence from a certain position (for a given candidate) is introduced as follows.

Let $M = \{M_1, ..., M_m\}$ be a set of m candidates, and let $\alpha \in \mathcal{L}(M)^n$ be a profile of n voters over those candidates (i.e. n-tuple of permutations of M). We define *d-measure of divergence from j-th position* for a candidate M_k by

$$\beta_j^d(M_k) = \sum_{i=1}^{n} \left|\alpha_i^k - j\right|^d$$

where α_i^k is the position of the candidate M_k in the preference of i-th voter, and $d > 1$ a fixed real number.

The idea behind such approach is that when measuring a divergence from a certain position (over a given profile) for some candidate, placement of the candidate in some preference should contribute with more than just its distance. Therefore, power $d > 1$ is being introduced. Such model "punishes" great distances between appointed place in resulting linear ordering and the actual placement of the candidate in preferences that form a profile. Value of parameter $d > 1$ represents a social decision of where society chooses to "draw the line" regarding a level of a compromise it finds acceptable.

Such d-measure of divergence provides a tool for comparison between existing social choice functions: does one social choice function select as the winner a candidate with smaller d-measure of divergence form the first position than the other? This question is answered in part in [1], while in [2] a new approach to construction of social welfare functions is proposed. If we define an output of social welfare function as an ordering of the candidates with regard to their d-measure of divergence from the first place, we will have the social choice function that always produces a candidate with the smallest d-measure of divergence from the first place as a winner.

In this talk we present another, more complex way to minimize d-measure of divergence: minimization over all possible permutations of candidates. This means that we will look for ordering, among all possible orderings of candidates, which minimizes total sum (over all candidates) of d-measures of divergence from their position in the observed ordering. Such unique ordering, if it exists, we will take as the result of Total d-Measure (TdM) social welfare function. We show that this function satisfies strict Pareto principle for all $d > 1$. Furthermore, we prove that TdM is positively responsive in three candidates scenario for $d = 2$ (on the other hand, we outline construction of non-monotonic profiles for other values of d), and that in the same scenario TdM has the property of intense independence of irrelevant alternatives (IIIA), as Saari defined it [4, 5]. Note that IIIA is proven to be substantial for characterization of Borda count [3], and TdM is clearly different from Borda count.

Acknowledgment

This work has been supported by Croatian Science Foundation (HRZZ) under the project UIP-05-2017-9219.

References

[1] Hatzivelkos, A.: Borda and Plurality Comparison with Regard to Compromise as a Sorites Paradox. Interdisciplinary description of complex systems, **16**(3-B), 465-484 (2018)

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

[3] Mihara, H. R.: Characterizing the Borda ranking rule for a fixed population. MPRA Paper 78093, University Library of Munich, Germany (2017)

[4] Saari, D. G.: Basic Geometry of Voting, Springler-Verlag, New York (1995)

[5] Saari, D. G.: Disposing dictators, demistifying voting paradoxes, Cambridge University Press, Cambridge (2008)

Smart labels

Sebastijan Horvat [1]

[1] *University of Zagreb, Croatia*
E-mail: [1]`sebastijan.horvat@ufzg.hr`

Keywords:
Interpretability logic, modal completeness, critical successor, assuring successor, maximal consistent set.

System **IL** is a system of modal logic introduced by Albert Visser [7] in 1988. This system contains one unary modal operator $\Box$ and one binary modal operator $\rhd$. Since then, various exstensions of system **IL** have been considered. These exstensions are given by the interpretability priciples, and some od these exstensions are interpretability logics **IL**M, **IL**W, **IL**P, **IL**M$_0$ and **IL**R [6].

Modal completeness of logics **IL**, **IL**M and **IL**P was proven in 1990. by De Jongh and Veltman [3]. Later they also proved modal completeness of the logic **IL**W [4]. In 2004. Evan Goris and Joost Joosten [2] gave new proofs of completeness of logics **IL** and **IL**M using their step–by–step method. Using that method, they also proved modal completeness of logics **IL**M$_0$ and **IL**W*.

In modal completeness proofs in interpretability logics, the central part is the notion of a critical successor. We say that a maximal consistent set Γ is a critical successor of a maximal consistent set Δ if for each formula A we have $\Box A \in \Gamma \Rightarrow A, \Box A \in \Delta$. Evan Goris, Marta Bilkova and Joost J. Joosten [1] [5] introduced in 2004. an alternative notion, that of assuring successor. For set of formulas S and two maximal consistent sets Δ and Γ, we say that Δ is an S–assuring successor of Γ, if for any finite $S' \subseteq S$ we have $A \rhd \bigvee_{S_j \in S'} \neg S_j \Rightarrow \neg A, \Box\neg A \in \Delta$. Using this new type of successor, they have presented relatively simple proof of modal completeness and decidability of **IL**W.

In this talk, we will first give a brief overview on interpretability logics and Goris–Joosten construction method for proving completeness of some interpretability logic. In the second part, we will define assuringness and will see some of its properties. Also, existence lemma for **IL**W will be presented. Because proving the decidability of an interpretability logic is in all known cases done by showing that the logic has the finite model property, we will abandon maximal critical sets and work with truncated parts of them. Here the notion of adequate set will be presented. Finally, in the third and the last part of the talk, we will give an overview of the proof of completeness of interpretability logic **IL**W. More formally, we will prove the following theorem:

Completeness of ILW. ***IL**W is complete with respect to finite Veltman frames (W, R, S) in which, for each $w \in W$, $(S_w; R)$ is conversely well–founded.*

As we will see, the main part in the proof is to show the following truth lemma:

Truth lemma. *For all $F \in \Phi$ and $w \in W$ we have $F \in (w)_1$ iff $w \Vdash F$.*

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] Bilkova, M., Goris, E., Joosten, J. J., *Smart labels*, in J. van Benthem, A. Troelstra, F. Veltman and A. Visser, editors, Liber Amicorum for Dick de Jongh. Institute for Logic, Language and Computation, 2004.

[2] Goris, E., Joosten, J., *Modal Matters in Interpretability Logics*, Logic Journal of IGPL 16 (2008), 371–412

[3] de Jongh, D. H. J., Veltman, F., *Provability logics for relative interpretability*, P. P. Petkov (ed.), Proceedings of the 1988 Heyting Conference, Plenum Press, 1990, pp. 31–42

[4] de Jongh, D. H. J., Veltman, F., *Modal completeness of* $\mathbf{ILW}$, in J. Gerbrandy, M. Marx, M. Rijke, and Y. Venema, editors, Essays dedicated to Johan van Benthem on the occasion of his 50th birthday, Amsterdam University Press, Amsterdam, 1999.

[5] Joosten, J. J., *Interpretability formalised*, PhD thesis, 2004.

[6] Perkov, T., Vukovi, M., *Semantike logika dokazivosti i interpretabilnosti*, Lecture notes, Faculty of science, University of Zagreb, 2017.

[7] Visser, A., *An overview of interpretability logic*, Kracht, Marcus (ed.) et al., Advances in modal logic. Vol. 1. Selected papers from the 1st international workshop (AiML'96), Berlin, Germany, 1996, Stanford, CA: CSLI Publications, CSLI Lect. Notes. 87, 307-359 (1998)

Session Types and Higher-Order Concurrency

Jorge A. Pérez

University of Groningen, The Netherlands

E-mail: `j.a.perez@rug.nl`

Session types are a type-based approach for communication correctness in message-passing, concurrent programs: a session type specifies what should be exchanged along a communication channel and when. Session types have been originally developed as typing disciplines for processes in the π-calculus, the paradigmatic calculus of interaction and concurrency.

While there is substantial value in looking into session types for the π-calculus, it is also insightful to investigate them in the context of core programming calculi that feature a closer link with (functional) programming languages. To this end, we have studied HO, a minimal calculus for higher-order concurrency and sessions. As in the π-calculus, HO features message-passing concurrency governed by session types; unlike the π-calculus, the values exchanged by HO processes are abstractions (functions from names to processes).

In this talk, I will discuss two key expressiveness results for HO processes with session types. First, HO and the session π-calculus are equally expressible: one language can be encoded into the other, up to tight behavioral equivalences. Second, there exists a small fragment of standard session types that suffices to represent all typable HO processes. Combined, these two results provide compelling evidence of the expressive power and convenience of HO as a compact blend of sessions and higher-order concurrency.

References

[1] Alen Arslanagic, Jorge A. Pérez, and Erik Voogd. Minimal Session Types (Pearl). In Alastair F. Donaldson, editor, *33rd European Conference on Object-Oriented Programming, ECOOP 2019, July 15-19, 2019, London, United Kingdom.*, volume 134 of *LIPIcs*, pages 23:1–23:28. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019.

[2] Dimitrios Kouzapas, Jorge A. Pérez, and Nobuko Yoshida. On the relative expressiveness of higher-order session processes. In Peter Thiemann, editor, *Programming Languages and Systems - 25th European Symposium*

on Programming, ESOP 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings, volume 9632 of *Lecture Notes in Computer Science*, pages 446–475. Springer, 2016. Extended version to appear in Information and Computation (Elsevier).

Kripke Semantics for Lambda Calculus with Pairs and Disjoint Sums

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

[1,2] *Faculty of Technical Sciences, University of Novi Sad*
Trg Dositeja Obradovića 6, Novi Sad, Serbia
E-mail: [1] simona.k@uns.ac.rs, [2] gsilvia@uns.ac.rs

Keywords:
Lambda calculus, Kripke semantics, Curry-Howard correspondence, Soundness, Completeness.

The Curry-Howard correspondence is a strong relation between logical systems and computer programs which embodies the formulae-as-types and proofs-as-terms/programs paradigm. It has been established between several logical systems and lambda calculi: the implicational fragment of intuitionistic propositional logic corresponds to the simply typed lambda calculus, the first-order logic corresponds to the lambda calculus with dependent types, the second-order logic corresponds to the lambda calculus with polymorphic types, etc.

Our focus is on the lambda calculus with pairs and disjoint sums which corresponds to the full intuitionistic propositional logic. Since there are soundness and completeness results of intuitionistic propositional logic with respect to Kripke models ([1, 3]), it is reasonable to expect that similar results can be obtained for lambda calculus with pairs and disjoint sums. However, to the best of our knowledge Kripke models have not yet been proposed for the lambda calculus with pairs and disjoint sums nor results on soundness and completeness of this calculus with respect to other semantics have been discussed. Thereby, we present a notion of Kripke semantics for lambda calculus with pairs and disjoint sums, we prove soundness and conjecture completeness.

We recall some basic notions of lambda calculus with pairs and disjoint sums. *Terms* are defined by the following syntax, where x belongs to a countable set of term-variables, V

$$\begin{aligned} M, N ::= & x \mid \lambda x.M \mid MN \mid \langle M, N\rangle \mid \pi_1(M) \mid \pi_2(M) \\ & \mid \mathrm{in}_1(M) \mid \mathrm{in}_2(M) \mid (\mathrm{case}\ M\ \mathrm{of}\ \mathrm{in}_1(x) \Rightarrow N \mid\ \mathrm{in}_2(y) \Rightarrow L) \mid \langle\rangle \mid \mathsf{abort}(M), \end{aligned}$$

Reduction, evaluation of programs, is generated by the usual β-reduction, the reduction rules for pairing and projections, along with the rules for

$$\begin{array}{lcl}\text{case in}_1(M) \text{ of in}_1(x) \Rightarrow N \mid \text{ in}_2(y) \Rightarrow L & \to & N\{M/x\} \\ \text{case in}_2(M) \text{ of in}_1(x) \Rightarrow N \mid \text{ in}_2(y) \Rightarrow L & \to & L\{M/y\}\end{array}$$

Types are generated by the following grammar, where a belongs to a countable set of type-variables

$$\sigma, \tau ::= a \mid \sigma \to \tau \mid \sigma \times \tau \mid \sigma + \tau \mid 0 \mid 1,$$

A statement $M : \sigma$ is derivable from a basis Γ, denoted by $\Gamma \vdash M : \sigma$, if $\Gamma \vdash M : \sigma$ can be produced by the rules in Figure 1.

$$\frac{x : \sigma \in \Gamma}{\Gamma \vdash x : \sigma} \qquad \frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \lambda x.M : \sigma \to \tau} \qquad \frac{\Gamma \vdash M : \sigma \to \tau \quad \Gamma \vdash N : \sigma}{\Gamma \vdash MN : \tau}$$

$$\frac{\Gamma \vdash M : \sigma \quad \Gamma \vdash N : \tau}{\Gamma \vdash \langle M, N \rangle : \sigma \times \tau} \qquad \frac{\Gamma \vdash M : \sigma \times \tau}{\Gamma \vdash \pi_1(M) : \sigma} \qquad \frac{\Gamma \vdash M : \sigma \times \tau}{\Gamma \vdash \pi_2(M) : \tau}$$

$$\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash \text{in}_1(M) : \sigma + \tau} \qquad \frac{\Gamma \vdash M : \tau}{\Gamma \vdash \text{in}_2(M) : \sigma + \tau}$$

$$\frac{\Gamma \vdash M : \sigma + \tau \qquad \Gamma, x : \sigma \vdash N : \rho \qquad \Gamma, y : \tau \vdash L : \rho}{\Gamma \vdash \text{case } M \text{ of in}_1(x) \Rightarrow N \mid \text{ in}_2(y) \Rightarrow L : \rho}$$

$$\frac{}{\Gamma \vdash \langle\rangle : 1} \qquad \frac{\Gamma \vdash M : 0}{\Gamma \vdash \mathsf{abort}(M) : \sigma}$$

Figure 1: Type Assignment System

The notion of *Kripke semantics* we present is motivated by the following:

1. the fact that the intuitionistic propositional logic is sound and complete with respect to Kripke semantics ([1, 3]),
2. the Kripke-style semantics for typed lambda calculus presented in [4] and completeness result with respect to this semantics.

First, we define a Kripke applicative structure.

Definition 1 A Kripke applicative structure *is a tuple* $\mathcal{K} = \langle W, \leq, \{A^\sigma_w\}, \{i^\sigma_{w,w'}\}\rangle$, *which consists of:*

(i) *a set* W *of "possible worlds" partially ordered by* $\leq$,

(ii) *a family* $\{A^\sigma_w\}$ *of sets indexed by types* σ *and worlds* w,

(iii) *a family* $\{i^\sigma_{w,w'}\}$ *of "transition functions"* $i^\sigma_{w,w'} : A^\sigma_w \to A^\sigma_{w'}$ *indexed by types of* σ *and pairs of worlds* $w \leq w'$, *which satisfy the following conditions:*

$$i^\sigma_{w,w} : A^\sigma_w \to A^\sigma_w \textit{ is identity} \qquad \text{(id)}$$

$$i^\sigma_{w',w''} \circ i^\sigma_{w,w'} = i^\sigma_{w,w''} \textit{ for all } w \leq w' \leq w'' \qquad \text{(comp)}$$

Next, we define the notion of *Kripke lambda model* by providing Kripke applicative structure with a valuation of term-variables which will have certain constraint.

Definition 2 (Kripke lambda model) A Kripke lambda model *is a tuple*

$$\mathcal{K}_\rho = \langle W, \leq, \{A^\sigma_w\}, \{i^\sigma_{w,w'}\}, \rho\rangle,$$

where a tuple $\mathcal{K} = \langle W, \leq, \{A^\sigma_w\}, \{i^\sigma_{w,w'}\}\rangle$ *is a Kripke applicative structure and* ρ *is a partial mapping from the product of set of term-variables and set of possible worlds to the elements of* $\mathcal{K}$, *i.e.* $\rho : V \times W \to \bigcup\limits_{\sigma\in\mathsf{Type}, w\in W} A^\sigma_w$, *such that the following condition holds:*

$$\text{If } \rho(x,w) \in A^\sigma_w \text{ and } w \leq w' \text{ then } \rho(x,w') = i^\sigma_{w,w'}(\rho(x,w)). \tag{1}$$

Equation (1) ensures that the following property holds.

Lemma 1 *Let* $\mathcal{K}_\rho = \langle W, \leq, \{A^\sigma_w\}, \{i^\sigma_{w,w'}\}, \rho\rangle$ *be a Kripke lambda model. If* $w \models M : \sigma$ *and* $w \leq w'$ *then* $w' \models M : \sigma$.

We proved that the type assignment system presented in Figure 1 is sound with respect to the proposed semantics. More precisely, we have proved the following theorem.

Theorem 1 (Soundness) *If* $\Gamma \vdash M : \sigma$, *then* $\Gamma \models M : \sigma$.

Our next goal is to prove completeness.

Conjecture 1 (Completeness) *If* $\Gamma \models M : \sigma$, *then* $\Gamma \vdash M : \sigma$.

Acknowledgment

The work is partly supported by the Ministry of Education, Science and Technological Development, Republic of Serbia, under grants ON174026 and III044006.

References

[1] Geuvers, H., Hurkens, T., *Deriving natural deduction rules from truth tables*, In Logic and Its Applications - 7th Indian Conference, ICLA 2017, Kanpur, India, January 5-7, 2017, Proceedings, pages 123138, 2017.

[2] Howard, W. A., *The formulae-as-types notion of construction*, pp. 479490 in To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism, London : Academic Press, 1980 (originally circulated 1969).

[3] Mints, G. E., *A Short Introduction to Intuitionistic Logic*, Kluwer Academic / Plenum Publishers, 2000.

[4] Mitchell, J. C., and E. Moggi, *Kripke-style models for typed lambda calculus*, Annals of Pure and Applied Logic, vol. 51, pp. 99124, 1991.

Complexity of Action Logic

Stepan Kuznetsov

Steklov Mathematical Institute of the RAS, Moscow

By *action logics* we mean inequational theories of residuated Kleene lattices (RKLs), that is, residuated lattices extended with iteration (Kleene star) [11, 9]. A residuated lattice is a partially ordered algebraic structure with two constants, $\mathbf{0}$ and $\mathbf{1}$, and five operations, $\cdot, \backslash, /, \vee, \wedge$, such that: $\vee$ and $\wedge$ are lattice operations w.r.t. the preorder; $\mathbf{0}$ is the minimal element; $\cdot$ and $\mathbf{1}$ form a monoid structure; $\backslash$ and $/$ are residuals of $\cdot$ w.r.t. the preorder:

$$a \preceq c \,/\, b \iff a \cdot b \preceq c \iff b \preceq a \,\backslash\, c.$$

The idea of iteration, or Kleene star, goes back to the seminal paper of Kleene [3]. There are two versions of axiomatisation for Kleene star. In the weaker ("inductive", or fixpoint) version, a^* is defined as the least element b such that $\mathbf{1} \vee a \cdot b \preceq b$. In the stonger, *-continuous, version, a^* is the supremum of $\{a^n \mid n \geq 0\}$. *-continuous RKLs form a subclass of all RKLs; thus (by Galois connection), their logic (inequational theory), $\mathbf{ACT}_\omega$, is an extension of the logic $\mathbf{ACT}$ of all RKLs.

The inequational theory of residuated lattices can be axiomatised by a Gentzen-style calculus, namely, the multiplicative-additive Lambek calculus **MALC** [2]. Formulae of **MALC** are built from variables and constants $\mathbf{0}$ and $\mathbf{1}$ using residuated lattice connectives $(\cdot, \backslash, /, \vee, \wedge)$. Sequents are expressions of the form $\Pi \vdash A$, where A is a formula and Π is a finite (possibly empty) linearly ordered sequence of formulae. Axioms and inference rules of **MALC** are as follows

$$\overline{A \vdash A}$$

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \cdot B, \Delta \vdash C} \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \cdot B}$$

$$\frac{\Pi \vdash A \quad \Gamma, B, \Delta \vdash C}{\Gamma, \Pi, A \,\backslash\, B, \Delta \vdash C} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \,\backslash\, B}$$

$$\frac{\Pi \vdash A \quad \Gamma, B, \Delta \vdash C}{\Gamma, B \,/\, A, \Pi, \Delta \vdash C} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash B \,/\, A}$$

$$\frac{\Gamma, A_1, \Delta \vdash C \quad \Gamma, A_2, \Delta \vdash C}{\Gamma, A_1 \vee A_2, \Delta \vdash C} \qquad \frac{\Pi \vdash A_i}{\Pi \vdash A_1 \vee A_2}$$

$$\frac{\Gamma, A_i, \Delta \vdash C}{\Gamma, A_1 \wedge A_2, \Delta \vdash C} \qquad \frac{\Pi \vdash A_1 \quad \Pi \vdash A_2}{\Pi \vdash A_1 \wedge A_2}$$

Both **ACT** and $\mathbf{ACT}_\omega$ are conservative extensions of **MALC**. For $\mathbf{ACT}_\omega$, the rules for Kleene star are as follows [1]:

$$\frac{(\Gamma, A^n, \Delta \vdash C)_{n=0}^{\infty}}{\Gamma, A^*, \Delta \vdash C} \qquad \frac{\Pi_1 \vdash A \quad \ldots \quad \Pi_n \vdash A}{\Pi_1, \ldots, \Pi_n \vdash A^*}$$

Notice that the left rule here is an ω-rule. Both **MALC** and $\mathbf{ACT}_\omega$ enjoy cut admissibility [1]. For **ACT**, no cut-free calculus is known. This system can be axiomatised using cut:

$$\frac{\Pi \to A \quad \Gamma, A, \Delta \vdash C}{\Gamma, \Pi, \Delta \vdash C}$$

and the axioms and rules corresponding to the fixpoint definition of iteration:

$$\frac{}{\mathbf{1} \vdash A^*} \qquad \frac{}{A, A^* \vdash A^*} \qquad \frac{\mathbf{1} \vdash B \quad A, B \vdash B}{A^* \vdash B}$$

We survey previously known and new results on the algorithmic complexity of the derivability problems for action logics (both in the **ACT** and $\mathbf{ACT}_\omega$ variants) and their fragments.

1. $\mathbf{ACT}_\omega$ is Π_1^0-complete (Buszkowski & Palka 2008 [1]). Moreover, its semilattice fragments, with only one of $\wedge$ and $\vee$ left, are also Π_1^0-complete [1].

2. **ACT** is undecidable (K. 2019 [6]). Moreover, the methods used in the undecidability proof allow to prove Σ_1^0-completeness of **ACT** and its semilattice fragments (K. 2019).

3. In the fragment of only $\cdot, {}^*, \vee$ (Kleene algebras), the logics for the fixpoint and the *-continuous cases coincide, and they are decidable and PSPACE-complete (Kozen 1994 [8]).

4. The fragment of $\mathbf{ACT}_\omega$ without $\vee$ and $\wedge$ is still Π_1^0-complete (K. 2019 [7]).

5. Systems without Kleene star are decidable. **MALC** itself is PSPACE-complete (Kanovich 1994 [4]), as well as its minimal fragments, including only one division and one of the lattice operations, $\vee$ or $\wedge$ (Kanovich, K., Scedrov 2019 [5]). The fragment of **MALC** without $\vee$ and $\wedge$ (the purely multiplicative Lambek calculus) is NP-complete (Pentus 1996 [10]), as well as its fragment with one division and the product (Savateev 2012 [13]). Finally, its one-division product-free fragment is decidable in polynomial time (Savateev 2010 [12]).

References

[1] W. Buszkowski, E. Palka. Infinitary action logic: complexity, models and grammars. Studia Logica 89:1 (2008), 1–18.

[2] N. Galatos, P. Jipsen, T. Kowalski, H. Ono. Residuated Lattices: An Algebraic Glimpse at Substructural Logics. Vol. 151 of Studies in Logic and the Foundations of Mathematics. Elsevier, 2007.

[3] S. C. Kleene. Representation of events in nerve nets and finite automata. In: Automata Studies, Princeton University Press, 1956, pp. 3–41.

[4] M. I. Kanovich. Horn fragments of non-commutative logics with additives are PSPACE-complete. In: Proceedings 1994 Annual Conference of the European Association for Computer Science Logic. Kazimierz, Poland (1994)

[5] M. Kanovich, S. Kuznetsov, A. Scedrov. The complexity of multiplicative-additive Lambek calculus: 25 years later. In: WoLLIC 2019. LNCS vol. 11541, Springer, 2019 (to appear).

[6] S. Kuznetsov. The logic of action lattices is undecidable. In: Proc. 34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, IEEE, 2019 (to appear).

[7] S. Kuznetsov. Complexity of the infinitary Lambek calculus with Kleene star, 2019. Submitted.

[8] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. Information and Computation 110 (1994), 366–390.

[9] D. Kozen. On action algebras. In: Logic and Information Flow, MIT Press, 1994, pp. 78–88.

[10] M. Pentus. Lambek calculus is NP-complete. Theoretical Computer Science 357:1–3 (2006), 186–201.

[11] V. Pratt. Action logic and pure induction. In: JELIA 1990: Logics in AI. LNCS (LNAI) vol. 478, Springer, 1991, pp. 97–120.

[12] Yu. Savateev. Unidirectional Lambek grammars in polynomial time. Theory of Computing Systems 46:4 (2010), 662–672.

[13] Yu. Savateev. Product-free Lambek calculus is NP-complete. Annals of Pure and Applied Logic 163:7 (2012), 775–788.

General variable neighbourhood search approach to MAX-3SAT problem

Luka Matijević

Mathematical Institute of the Serbian Academy of Sciences and Arts
Kneza Mihaila 36, Belgrade
E-mail: luka@mi.sanu.ac.rs

Keywords:
Satisfiability problem, NP-completeness, incomplete solvers, stochastic algorithms, metaheuristic approach

MAX-3SAT problem is a version of MAX-SAT problem where every clause has exactly three literals. It is one of the most important problems of computational complexity theory, and as such, many solvers have been developed for it. Since it belongs to the class of NP-complete problems, it is usually solved by implementing heuristic methods.

In this paper we used general variable neighbourhood search (GVNS) to obtain the best possible solution in a given amount of time. GVNS is neighborhood based search algorithm that involves two main steps: perturbation and improvement. We defined two sets of neighbourhoods, each of them used in the perturbation step with a predefined probability p. For the improvement step we used variable neighbourhood descent (VND), which is a local search heuristic that explores several neighborhood structures in a deterministic way.

The proposed GVNS approach is tested on a set of benchmark instances found at: https://www.cs.ubc.ca/ hoos/SATLIB/benchm.html, and compared with state-of-the-art WalkSAT implementation:
http://www.cs.rochester.edu/u/kautz/walksat/. We concluded that for smaller instances our approach gives similar results as aforementioned WalkSAT implementation, but it performed better for larger instances, given that it finds very good solutions very quickly.

Acknowledgment

This research was supported by the Serbian Ministry of Education, Science and Technological Development under the grant ON174026.

References

[1] Jakšić Krüger, T., Davidović, T. *Empirical Analysis of the Bee Colony Optimization Method on 3-SAT*, Zbornik radova XLIII Simpozijuma o operacionim istraivanjima (SYM-OP-IS 2016)

[2] N. Mladenović and P. Hansen *Variable neighborhood search*, Comput. & OR, 24(11):10971100, 1997

[3] P. Hansen, N. Mladenović, R. Todosijević, and S. Hanaf *Variable neighborhood search: basics and variants*, EURO Journal on Computational Optimization, 5(3):423454, 2017.

[4] Bouhmala N. *A variable neighborhood Walksat-based algorithm for MAX-SAT problems*, TheScientificWorldJournal vol. 2014 (2014): 798323. doi:10.1155/2014/798323

[5] B. Selman, H. Kautz, and B. Cohen *Local Search Strategies for Satisfiability Testing*, Final version appears in Cliques, Coloring, and Satisfiability: Second DIMACS Implementation Challenge, October 1113, 1993. David S. Johnson and Michael A. Trick, eds. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 26, AMS, 1996.

Regular subsets and semilattice decompositions of semigroups. Hereditarness and periodicity

Melanija Mitrović

Faculty of Mechanical Engineering, University of Niš, Serbia
e-mail: melanija.mitrovic@masfak.ni.ac.rs

Sergei Silvestrov

Mälardalen University, Box 883, 72123 Västerås, Sweden
e-mail:sergei.silvestrov@mdh.se

> "Semigroups aren't a barren, sterile flower on the tree of algebra, they are a natural algebraic approach to some of the most fundamental concepts of algebra (and mathematics in general), this is why they have been in existence for more then half a century, and this is why they are here to stay." (B. M. Schein, in Semigroup Forum, 54, 1997, 264-268)

Keywords:

Semilattice decomposition of semigroups, semilattice of archimedean semigroups, *MBC*-semigroup, *GVS*-semigroup, hereditary *GVS*-semigroup.

A *semigroup* is an algebraic structure consisting of a set with an associative binary operation defined on it. We can say that most of the work within theory is done on semigroups with a *finiteness condition*, i.e. a semigroups possessing any property which is valid for all finite semigroups. Some of the most important examples of finiteness conditions include, among others, π-regularity, completely π-regularity, periodicity, finite generation. There are many different techniques for describing various kinds of semigroups. Among the methods with general applications is a *semilattice decomposition* of semigroups. Certain types of semigroups being decomposable into a semilattice of archimedean semigroups occurred in semigroup-theoretic investigations of diverse directions. The main purpose of this short note, based on [1], [2], is the decomposability of a certain type of semigroups with finiteness conditions into a semilattice of archimedean semigroups.

An element e of a semigroup S is *idempotent* if $e^2 = e$, and the set of all idempotents of a semigroup S is denoted by $\boldsymbol{E(S)}$. There is a wide variation in the number of idempotents a semigroup S may contain. A semigroup consisting entirely of idempotents is known as a *band*. A commutative band is a *semilattice*. An element a of a semigroup S is *regular* (*completely regular*) if $a = axa$ ($a = axa$ and $ax = xa$) for some $x \in S$. The set of all regular (completely regular) elements of S is denoted by $\boldsymbol{Reg(S)}$ ($\boldsymbol{Gr(S)}$) and called the *regular part* (the *group part*) of a semigroup S. For a semigroup S we have, in general, $E(S) \subseteq Gr(S) \subseteq Reg(S)$. The study of all distinguished types of special elements (idempotents, regular and group ones) is of interest in its own right, but, it is also evident that the knowledge of these types of elements is often an important tool in the study of structure properties of semigroups.

Let T be a subsemigroup of S. Then $E(T) = E(S) \cap T$ - even more, this is true for any subset T of S. On the other hand, we distinguish the following two subsets: $Reg(T) = \{a \in T : (\exists x \in T)\, axa = a\}$ called *regular part of* T, and $reg(T) = \{a \in T : (\exists x \in S)\ axa = a\}$ called *semigroup regular*, or, shortly, *s-regular* part of T. In general, the inclusion in $Reg(T) \subseteq reg(T) = T \cap Reg(S)$ can be strict. Problem which naturally arise here is to describe class of semigroups with the equality $Reg(T) = reg(T)$, for any subsemigroup T of S. We we characterize first semigroups with such a property where T runs over one of the following families of subsemigroups: $\{Se : e \in E(S)\}$, $\{eS : e \in E(S)\}$.

Theorem 1 *Let S be a semigroup with non-empty set of idempotents. Then $reg(Se) = Reg(Se)$ $(reg(eS) = Reg(eS))$ for any $e \in E(S))$ if and only if $Reg(S) = Gr(S)$.*

In a sequel we want to divide the semigroup into subsets/subsemigroups in such a way that we can understand the semigroup in terms of those parts and their interaction. Semilattice decompositions of semigroups were introduced by A. H. Clifford in 1941. Let $\mathfrak{N}$ be a semilattice congruence on a semigroup S, that is, $Y = S/\mathfrak{N}$ is a semilattice and the $\mathfrak{N}$-class, S_α, $\alpha \in Y$, is a subsemigroup of S. Then it is said that S is *a semilattice Y of semigroups S_α, $\alpha \in Y$*. The fundamental result, celebrated T. Tamura's theorem from 1956, that any semigroup is a semilattice of semilattice-indecomposable semigroups, as well as 1972 T. Tamura's result that an archimedean semigroup is a semilattice-indecomposable make decomposabilty of a given semigroup into semilattice of archimedean semigroups a field of intensive research. Recall, a semigroup S is *archimedean* if $a^k \in S^1aS^1$ for any $a \in S$ and some $k \in \mathbb{N}$. In general, the class of semilattices of archimedean semigroups is not subsemigroup closed. The greatest subsemigroup closed subclass of the class of semilattices of archimedean semigroups in general and in some special cases is first described by M. Mitrović, S. Bogdanović and M. Ćirić in 1995. That is why such semigroup is called *MBC-semigroup.*

Theorem 2 *A semigroup S is an MBC-semigroup if and only if for any $a, b \in S$ there exists $n \in \mathbb{N}$ such that $(ab)^n \in \langle a, b\rangle a^2 \langle a, b\rangle$.*

Having in mind that the definition of finiteness condition may be given, also, in terms of elements of the semigroup, its subsemigroups, in terms of ideals or congruences of certain types, we choose to characterize the decomposability of a certain type of semigroups with finiteness conditions into a semilattice of archimedean semigroups mostly by making connections between their elements and/or their special subsets. A semigroup S is *π-regular*, *completely π-regular* if $S = \sqrt{Reg(S)}$, $S = \sqrt{Gr(S)}$ respectively. (Recall, for any subset A of S we can "make" the following new subset $\sqrt{A} = \{x \in S : (\exists n \in \mathbb{N})\, x^n \in A\}$.) Completely π-regular semigroup which is a semilattice of archimedean semigroups is called *Galbiati-Veronesi-Shevrin semigroup*, shortly *GVS-semigroup.*

Theorem 3 *The following conditions on a semigroup S are equivalent:*

(i) *S is a GVS-semigroup;*

(ii) $(\forall a, b \in S)(\exists n \in \mathbb{N})\ (ab)^n \in (ab)^n bS(ab)^n$*;*

(iii) *S is π-regular and $Reg(S) = Gr(S)$.*

A semigroup S is periodic if $S = \sqrt{E(S)}$. Periodic semigroups which can be decomposed into semilattice of archimedean semigroups are, in fact, *hereditary* GVS-semigroups, or, equivalently, periodic MBC-semigroups.

Theorem 4 *A semigroup S is hereditary GVS-semigroup if and only if $reg(T) = Reg(T) \neq \varnothing$, for each subsemigroup T of S.*

Of all generalizations of the group theory and the ring theory, concept of semigroup is considered as one of the most successful one. The development of semigroup theory in the very beginning was strongly motivated by this fact. Although some notions are derived from group theory, semigroup theory in many ways resembles ring theory more. For example, idempotent elements, ideals, regularity, π-regularity are defined essentially as for rings. But, on the other hand, within the last decades, application of semigroup theoretical methods have occurred naturally in many aspects of ring theory. List some of the applications of presented classes of semigroups and their semilattice decompositions in certain types of ring constructions, in particular in semigroup graded ring theory, can be found in [2]. " This is very pretty mathematics which illustrates the interplay between ring-theoretic and semigroup-theoretic techniques."

Acknowledgment

This work is partially supported by the grants 174 026 (first author) of Ministry of Education and Science of Serbia.

References

[1] M. Mitrović, `Semilattices of Archimedean Semigroups`, University of Niš - Faculty of Mechanical Engineering, Niš (2003).

[2] M. Mitrović, S. Silvestrov, *Semilattice decompositions of semigroups. Hereditarness and periodicity - an overview*, accepted in Stochastic Processes and Algebraic Structures - From Theory Towards Applications, Volume II: Algebraic Structures and Applications, (Eds.: S. Silvestrov, M. Malyarenko, M. Rančić), Springer, 2019.

Proofs and surfaces

Đorđe Baralić[1], Pierre-Louis Curien[2], Marina Milićević[3], Jovana Obradović[4], Zoran Petrić[5], Mladen Zekić[6], Rade Živaljević[7]

[1567]*Mathematical Institute of the Serbian Academy of Sciences and Arts*
[2]πr^2 *team, IRIF (CNRS, University Paris Diderot and INRIA)*
[3]*Production and Management Faculty, Trebinje, Bosnia and Herzegovina*
[4]*Institute of Mathematics of the Czech Academy of Sciences*
E-mail: [1]`djbaralic@mi.sanu.ac.rs`, [2]`curien@irif.fr`,
[3]`marina.milicevic@fpm.ues.rs.ba`, [4]`obradovic@math.cas.cz`,
[5]`zpetric@mi.sanu.ac.rs`, [6]`mzekic@mi.sanu.ac.rs`, [7]`rade@mi.sanu.ac.rs`

Keywords:
Ceva-Menelaus proof, connected sum, cyclic operad, decidability, Δ-complex, incidence theorem, sequent system, simplicial homology

Incidence theorems in Euclidean or projective geometry state that some incidences follow from other incidences, where an incidence is a pair of a line and a point, together with the information whether the point lies on the line or not. A famous example is Desargue's theorem, which states that if ABC and UVW are two triangles such that $A \neq U$, $B \neq V$ and $C \neq W$, if $BC \cap VW = \{P\}$, $AC \cap UW = \{Q\}$ and $AB \cap UV = \{R\}$, then the lines AU, BV and CW are concurrent if and only if the points P, Q and R are colinear.

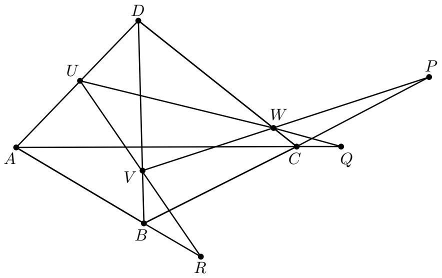
Our intention is to formalise and extend, within proof theory, an idea of Richter-Gebert on incidence theorems, which we paraphrase as follows:

> If $\mathcal{M}$ is a triangulated manifold that forms a 2-cycle, and therefore is orientable, then the presence of Menelaus configurations on all but one of the triangles automatically implies the existence of a Menelaus configuration on the final triangle.

A sextuple (A, B, C, P, Q, R) of points in $\mathbf{R}^2$ *makes a Menelaus configuration* if $(B, C; P)$, $(C, A; Q)$ and $(A, B; R)$ are defined and their product is -1, where, for three mutually distinct points X, Y and Z in $\mathbf{R}^2$, $(X, Y; Z)$ is undefined unless X, Y, Z are colinear, and is otherwise defined as follows:

$$(X, Y; Z) =_{df} \begin{cases} \frac{XZ}{YZ}, & \text{if } Z \text{ is between } X \text{ and } Y, \\ -\frac{XZ}{YZ}, & \text{otherwise.} \end{cases}$$

The Menelaus theorem states that if A, B, C are not colinear, then a Menelaus configuration can be equivalently defined purely in terms of incidences, namely: P, Q, R colinear, as well as B, C, P colinear, C, A, Q colinear and A, B, R colinear. As an example, consider the sphere S^2 triangulated in four triangles (the facets of a tetrahedron) and assume that the vertices A, B, C and D of the tetrahedron, as well as the points P, Q, R, U, V and W, satisfy all the incidences displayed in the picture below.



By Menelaus theorem, we have Menelaus configurations on the triangles BCD, CAD and ABD, i.e., we have $(C, D; W) \cdot (D, B; V) \cdot (B, C; P) = -1$, $(D, C; W) \cdot (A, D; U) \cdot (C, A; Q) = -1$, and $(B, D; V) \cdot (D, A; U) \cdot (A, B; R) = -1$, which, after multiplication and cancellation, delivers $(B, C; P) \cdot (C, A; Q) \cdot (A, B; R) = -1$. By Menelaus theorem again, P, Q, R are colinear.

We introduce a one-sided sequent system, which deals with atomic formulae of the form "this sextuple of points makes a Menelaus configuration". An intuition (formalised in Proposition 1 below) behind the sequents of our system is that an arbitrary formula in a sequent is entailed by the remaining formulae of the sequent. For an arbitrary countable set W, let

$$F^6(W) = W^6 - \{(X_1, \ldots, X_6) \in W^6 \mid X_i = X_j \text{ for some } i \neq j\}.$$

The atomic formulae of our language are the elements of $F^6(W)$. The formulae are built out of atomic formulae by using the connectives ⩙ (simultaneous conjunction and disjunction) and $\leftrightarrow$ (the classical equivalence). A sequent is a finite multiset of formulae, and the sequent consisting of a multiset Γ is denoted by $\vdash \Gamma$. The axiomatic sequents are formed in the following manner. For every triangulated manifold $\mathcal{M}$ with 0-cells $\mathcal{M}_0$, 1-cells $\mathcal{M}_1$ and 2-cells $\mathcal{M}_2$, such that $\mathcal{M}_0, \mathcal{M}_1 \subseteq W$, let $\nu \colon \mathcal{M}_2 \to F^6(W)$ be defined as

$$\nu x = (d_1^1 d_2^2 x, d_0^1 d_2^2 x, d_0^1 d_0^2 x, d_0^2 x, d_1^2 x, d_2^2 x),$$

where $d_i^j : \mathcal{M}_j \to \mathcal{M}_{j-1}$, $1 \leq j \leq 2$, $0 \leq i \leq j$, are the face maps of $\mathcal{M}$. Then $\vdash \{\nu x \mid x \in \mathcal{M}_2\}$ is an axiom of our system. The other axioms are $\vdash (A, B, C, P, Q, R), (A, B, C, P, Q, R)$ (identity), $\vdash (A, B, C, P, Q, R), (B, C, A, Q, R, P)$ and $\vdash (A, B, C, P, Q, R), (A, R, Q, P, C, B)$ (switching of triangles). The rules of inference of the system are the following:

$$\frac{\vdash \Gamma, \varphi \quad \vdash \Delta, \varphi}{\vdash \Gamma, \Delta} \qquad \frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta} \qquad \frac{\vdash \Gamma, \varphi \quad \vdash \Gamma, \psi}{\vdash \Gamma, \varphi ⩙ \psi} \qquad \frac{\vdash \Gamma, \varphi \quad \vdash \Delta, \psi}{\vdash \Gamma, \Delta, \varphi \leftrightarrow \psi}$$

We prove the soundness of our system with respect to Euclidean (resp. projective) *interpretations*, i.e. functions from W to $\mathbf{R}^2$ (resp. to $\mathbf{RP}^2$). We say that an interpretation satisfies the atomic formula (A, B, C, P, Q, R), when its interpretation as a sextuple of points in $\mathbf{R}^2$ makes a Menelaus configuration. Let $\Gamma \models_E \varphi$ (resp. $\Gamma \models_P \varphi$) mean that every Euclidean (resp. projective) interpretation that satisfies every formula in Γ also satisfies φ, where every occurrence of $\parr$ in Γ (resp. ϕ) is interpreted as disjunction (resp. as conjunction), while $\leftrightarrow$ is always interpreted as classical equivalence.

Proposition 1 (Soundness) *If* $\vdash \Gamma, \varphi$ *is derivable, then* $\Gamma \models_E \varphi$ *(resp.* $\Gamma \models_P \varphi$*).*

By normalizing in a particular way the derivations of our system, we prove its decidability:

Proposition 2 (Decidability) *The Menelaus system is decidable.*

We illustrate on examples a general pattern for extracting an incidence result (its formulation and a proof) from derivable sequents of our system: starting from the interpretations that satisfy all but one formulae in a derivable sequent, by the soundness result, such an interpretation satisfies the last formula too. Menelaus theorem is used at both ends to translate from incidences to Menlaus configurations and back.

Finally, we show that the derivable sequents of our system admit a natural cyclic operad structure, thereby answering positively the question of whether cyclic operads appear in general proof-theory, alongside ordinary operads.

Acknowledgment

Jovana Obradović gratefully acknowledges the financial support of the Praemium Academiae of M. Markl and RVO:67985840. Djordje Baralić and Rade Živaljević were supported by the Grant 174020, while Zoran Petrić and Mladen Zekić were supported by the Grant 174026 of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

References

[1] J. Richter-Gebert, *Meditations on Ceva's theorem*, ***The Coxeter Legacy: Reflections and Projections*** (C. Davis and E.W. Ellers, editors), American Mathematical Society and Fields Institute, Providence, 2006, pp. 227-254

Analysis of Distance-Bounding Protocols

Andre Scedrov

University of Pennsylvania
E-mail: scedrov@math.upenn.edu

Many security protocols rely on the assumptions on the physical properties in which its protocol sessions will be carried out. For instance, Distance Bounding Protocols take into account the round trip time of messages and the transmission velocity to infer an upper bound of the distance between two agents. Distance Bounding protocols are, however, vulnerable to distance fraud, in which a dishonest prover is able to manipulate the distance bound computed by an honest verifier. Despite their conceptual simplicity, devising a formal characterization of distance bounding protocols and distance fraud attacks that is amenable to automated formal analysis is non-trivial, primarily because of their real-time and probabilistic nature. We introduce a generic, computational model, based on Multiset Rewriting, for a formal analysis of various forms of distance fraud, including recently identified timing attacks, on the Hancke-Kuhn family of distance bounding protocols through statistical model checking [1, 2]. While providing an insightful formal characterization on its own, the model enables a practical formal analysis method that can help system designers bridge the gap between conceptual descriptions and low-level designs. We use the model to define new attack strategies and quantitatively evaluate their effectiveness under realistic assumptions.

References

[1] Musab A. Alturki, Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. Statistical Model Checking of Distance Fraud Attacks on the Hancke-Kuhn Family of Protocols. In: A. Rashid and N.O. Tippenhauer, eds., Proceedings of the 2018 ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC 2018), Toronto, Ontario, Canada, October 19, 2018, ACM, New York, NY, 2018, pp. 60 - 71.

[2] Musab A. Alturki, Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols. In: J.D. Guttman

et al., eds., Foundations of Security, Protocols, and Equational Reasoning. Essays Dedicated to Catherine A. Meadows. Springer LNCS Volume 11565, Springer- Verlag, 2019, pp. 192 - 213.

Axiomatizations of natural numbers-some old and some new

Zvonimir Šikić

Logics of Badiou's Worlds

Vladimir Tasić

University of New Brunswick, Fredericton, Canada

Keywords:

Badiou, Logic, ZFC, Category Theory.

Mathematics, particularly the fields of mathematics that relate to foundations, play a central role in the philosophy of Alain Badiou. In a process that now spans half a century, Badiou's complex appeal to mathematics evolved from an early study of formal deductive systems in *The Concept of Model* [2] (notes for a lecture canceled due to the events of Paris May in 1968), through his use of ZFC and forcing in *Being and Event* [1], to topos theory and categorical logic in *Logics of Worlds* [3]. In a recent book [4], he announces that his next project may involve paraconsistent logics.

While Badiou's work has found a following in the humanities, it cannot be said to have received comparable attention from mathematicians. There is no paradox, but there is perhaps a curious story of unrequited love, in the fact that a well-respected philosopher, indeed Director of Philosophy at ENS, one of France's most prestigious academic institutions, pens amorous letters to mathematics — e.g. *In Praise of Mathematics* [5] — and promotes it successfully at academic locales not easily accessible to mathematicians, and is in turn largely ignored by the mathematical community.

There has been a slight growth in interest in recent years: some of Badiou's books have been reviewed by logicians and category theorists, including Andrej Bauer [6], Maciej Malicki [7], and Colin McLarthy [8] among others. My own articles [9, 10], part of a longitudinal study of Badiou, focused less on the issue of technical correctness than on the broader questions of "Why does Badiou need mathematics in the first place", and "Why does he use *that* part of mathematics instead of another". On the issue of whether it is all impeccably correct, my view is very similar to Bauer's:

> I shall not criticize a philosopher for not knowing everything when he expended an amazing amount of energy to build not one, but two bridges from his land to mine. I am impressed by the lucidity of Badiou's remarks on the philosophical significance

> of category theory, especially in relation to set theory, and I invite philosophically minded mathematicians to be so too. [6]

Reservations of the mathematical community, especially among logicians, are understandable, since it is difficult to make sense of a number of Badiou's "applications" of concepts imported from mathematics. I recently had the singular pleasure of observing the reactions of an audience that included Wilfred Hodges, Menachem Magidor, John Steel and Hugh Wooden when I quoted and even attempted to explain Badiou's remark that the independence of CH represents "a triumph of politics of the realism of the unions", his identification of the class of all ordinals with "nature", and his view in *Being and Event* that ZFC set theory, due to the Axiom of Separation, is in some sense "materialist":

> language cannot induce existence, solely a split in existence [. . .]. Zermelo's axiom is therefore materialist in that it breaks with the figure of idealinguistry—whose price is the paradox of excess—in which the existential presentation of the multiple is directly inferred from a well-constructed language. [1]

The bafflement does not decrease when in *Logics of Worlds*, a subsequent major philosophical work that invokes topos theory and categorical logic, Badiou turns to sounding almost like Brouwer in an anti-formalist combat mode. Here Badiou writes of "pre-linguistic operators" and states that

> logic, formal logic included, not to mention rhetoric, all appear for what they are: derivative constructions, whose detailed study is a matter for anthropology. [3]

Nevertheless, there is something attractive (to me) in suspending judgment on technical details in order to try to understand the broader philosophical and political purpose of Badiou's complex, fascinating, though sometimes perplexing appeals to mathematics. After all, I have also seen him deliver a talk on (essentially) the construction of reals to a captive and appreciative audience of students and professors of comparative literature at New York University. Few mathematicians are capable of such a feat, and we do have at least that much to learn from Badiou, who at least in this regard deserves to be read, discussed and better understood.

In this presentation I will attempt to explain the historical, philosophical, and political background of Badiou's various "applications" of mathematics and mathematical logic. It is perhaps an impossible task, but one that is true to the 14th of his 21 definitions of happiness, given in *Métaphysique du bonheur réel*: "Real happiness is always an enjoyment of the impossible" [4].

References

[1] Alain Badiou, *Being and Event*, Continuum, London, 2007.

[2] Alain Badiou, *The Concept of Model*, re.press, Melbourne, 2007.

[3] Alain Badiou, *Logics of Worlds*, Continuum, London, 2009.

[4] Alain Badiou, *Métaphysique du bonheur réel*, Presses Universitaires de France, Paris, 2015. (The English translation, *Happiness*, is forthcoming.)

[5] Alain Badiou, *In Praise of Mathematics*, Polity Press, Cambridge, 2016.

[6] Andrej Bauer, "Review of Mathematics of the Transcendental", *Notices of the American Mathematical Society*, Volume **62** Number 9 (2015) 1070–1071.

[7] Maciej Malicki, "Matheme and Mathematics: On the main concepts of the philosophy of Alain Badiou", *Logiue et analyse*, Vol. **58**, No 231 (2015), pages 433-455. Available at https://arxiv.org/pdf/1406.0059.pdf, accessed on January 17, 2017.

[8] Colin McLarty, "Review of Alain Badiou, Mathematics of the Transcendental", *Notre Dame Philosophical Reviews*, 2014.09.31. Available at , accessed on January 17, 2017.

[9] Vladimir Tasić, "Mathematics and Revolutionary Theory: Reading Castoriadis After Badiou", *Cosmos and History: The Journal of Natural and Social Philosophy*, Vol. **8** No. 2 (2012) 60–77.

[10] Vladimir Tasić, "Badiou's *Logics*: Math, Metaphor, and (Almost) Everything", *Journal of Humanistic Mathematics*, Vol. **7**, No. 1 (January 2017) 22–45.

Completeness, finite model property and decidability of interpretability logics

Luka Mikec[1], **Mladen Vuković**[2]

Department of Mathematics, University of Zagreb
Croatia
E-mail: [1]`luka.mikec@math.hr`, [2]`mladen.vukovic@math.hr`

Keywords:
interpretability logics, generalized Veltman semantics, completeness, finite model property, decidability

Interpretability logic $\mathbf{IL}\mathsf{P}_0$ is incomplete w.r.t. ordinary semantics. The completenes of the system $\mathbf{IL}\mathsf{R}$ is an open problem (see [1]). We prove modal completeness of the interpretability logics $\mathbf{IL}\mathsf{P}_0$ and $\mathbf{IL}\mathsf{R}$ w.r.t. generalized Veltman semantics. Our proofs are based on the notion of full labels [1]. We also give shorter proofs of completeness w.r.t. generalized semantics for many classical interpretability logics: $\mathbf{IL}$, $\mathbf{IL}\mathsf{M}$, $\mathbf{IL}\mathsf{M}_0$, $\mathbf{IL}\mathsf{P}$, $\mathbf{IL}\mathsf{W}$ and $\mathbf{IL}\mathsf{W}^*$. We obtain decidability and finite model property w.r.t. generalized semantics for $\mathbf{IL}\mathsf{P}_0$ and $\mathbf{IL}\mathsf{R}$.

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] M. Bilkova, E. Goris, J. J. Joosten, Smart labels, In *Liber Amicorum for Dick de Jongh*, J. van Benthem et al. eds., Institute for Logic, Language and Computation, 2004.

[2] E. Goris, J. J. Joosten, Modal matters in interpretability logics, *Logic Journal of the IGPL*, **16** (2008), 371–412

[3] E. Goris, J. Joosten, *A new principle in the interpretability logic of all reasonable arithmetical theories*, Logic Journal of the IGPL **19** (2011) 1–17

[4] L. Mikec, T. Perkov, M. Vuković, Decidability of interpretability logics $\mathbf{IL}\mathsf{M}_0$ and $\mathbf{IL}\mathsf{W}^*$, *Logic Journal of the IGPL*, **25** (2017), 758–772

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

[6] A. Visser, *An overview of interpretability logic*, In: K. Marcus (ed.) et al., Advances in modal logic. Vol. 1. Selected papers from the 1st international workshop (AiML'96), Berlin, Germany, October 1996, Stanford, CA: CSLI Publications, CSLI Lect. Notes. 87(1998), 307–359

[7] M. Vuković, The principles of interpretability, *Notre Dame Journal of Formal Logic*, **40** (1999), 227–235

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

Reasoning About Financial Trading Systems in CLF

Dragiša Žunić

Carnegie Mellon University in Qatar

Keywords:

Automated reasoning, logical frameworks, CLF, trading systems, market microstructure, regulatory compliance.

This abstract is based on the results presented in [1], co-authored with I. Cervesato, G. Reis and S. M. Khan.

Systems which facilitate trade in an automated way are among the cornerstone concepts in economics and finance. Of particular significance are the underlying rules governing the interaction between buy and sell instructions, i.e., buy and sell orders, thus defining trade dynamics. Whether such system operates as intended relates to regulatory compliance issues. We will refer to such systems as automated trading system, or ATS.

In order to guarantee trading fairness an ATS must meet the requirements of regulatory bodies. However, both specifications and requirements are presented in natural language which leaves space for ambiguity. As a result, it is difficult to guarantee regulatory compliance. The main regulator in USA, the Securities and Exchanges Commission (SEC), has fined several companies, including Deutsche Bank, Barclay's Capital, Credit Suisse, and UBS, in the recent years.

Experience has shown that (possibly unintentional) violations often originate from unforeseen interactions between order types [2, 3]. Formalization and formal reasoning provide methods to verify properties of complex and infinite state space systems with certainty, and have already been applied in different fields.

In this paper we use the logical framework CLF [4], and its implementation Celf, to model and reason about trading systems. CLF is a linear concurrent extension of the long-established LF framework. Linearity enables natural encoding of state transition, where facts are consumed and produced thereby changing the system's state

Encoding orders in a market as linear resources results in straightforward rules that either consume such orders when they are bought/sold, or store them in the market as resident orders. The specification is modular and easy to extend with new order types, which is often required in practice.

Using the formalization we were able to prove two standard properties about a market working under these rules. First we proved that at any given state the bid price is smaller than the ask, i.e., the market is never in a locked-or-crossed state. Secondly we showed that the trade always take place at bid or ask.

The contributions of this research are in that (1) we formally define an archetypal automated trading system in CLF and implement it in Celf, and (2) we outline the verification of several properties an ATS should satisfy, using generative grammars [5], as an important case study towards developing the techniques for meta-reasoning in CLF.

Acknowledgements

The research reported in the paper was made possible by NPRP 7-988-1-178 from the Qatar National Research Fund (a member of Qatar Foundation), and by ON174026 research grant by Ministry of Science of Republic of Serbia.

References

[1] I. Cervesato, G. Reis, S. Khan and D. Zunic, *Formalization of Automated Trading Systems in a Concurrent Linear Framework*, In Proceedings of Linearity & TLLA 2018, Oxford, UK. EPTCS 292, pp. 1–14, 2019.

[2] G. O. Passmore and D. Ignatovich, *Formal Verification of Financial Algorithms*, CADE 26, Gothenburg, Sweden, pp. 26–41, 2017.

[3] D. Ignatovich and G. O. Passmore, *Case Study: 2015 SEC Fine Against UBS ATS*, Aesthetic Integration, Ltd., Technical Whitepaper, 2015.

[4] I. Cervesato, K. Watkins, F. Pfenning and D. Walker, *A Concurrent Logical Framework I: Judgements and Properties*. Technical Report CMU-CS-02-101, CMU Pittsburgh, 2003.

[5] R. J. Simmons, *Substructural Logical Specifications*, Carnegie Mellon University, Ph.D. thesis, 2012.