7TH INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2018

held with
1st Workshop Formal Reasoning and Semantics FORMALS 2018

September 24 - 28, 2018
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 7^{th} International Conference on Logic and Applications - LAP 2018, held at the Inter University Center Dubrovnik, Croatia, September 24 - 28, 2018. LAP 2018 includes a satellite workshop Formal Reasoning and Semantics (FORMALS 2018), as a part of a research project supported by Croatian Science Foundation (UIP-2017-05-9219).

LaTeX book of abstracts preparation and typesetting:

- Dušan Gajić, University of Novi Sad
- Aleksandra Arsić, Mathematical Institute of SASA, Belgrade

LAP 2018 Web site: `http://imft.ftn.uns.ac.rs/math/cms/LAP2018`
Maintained by Nenad Savić, University of Bern and University of Novi Sad

Contents

Type system with constraints for ML type inference with the implementation in Haskell

Alen Arslanagić [1]

[1] *Unversity of Groningen*
Nijenborgh 9, Groningen, The Netherlands
E-mail: [1] alen.arslanagic@gmail.com,

Keywords:
ML, type inference, Haskell.

We examined a constraint language and constraint-based type systems [1] which provide a convenient type inference algorithm for programming languages from the ML functional language family. Type systems with constraints are generalization of Damas-Milner type system [2]. HM(X) [3] represents a family of constraint-based type systems parametrized with respect to the syntax and interpretation of constraints. HM(X) have a generic type inference algorithm. The parameter X stands for constraints syntax, constraints interpretation and instance relation. HM(X) represents an useful framework for experimentation with constraints systems since it provides high-level proofs of soundness and completeness of the type inference. The language of constraints is a logic - it has syntax and interpretation in a model. Constraints as an intermediate representation give rise to a modular representation of well-known type inference algorithm [4].

We adapt the algorithm to develop monadic Haskell implementation of modular type inference algorithm for ML language utlizing the constraint language. We define a core of ML language as a base language. We adapt the constraint language to be suitable for a Haskell representation. In our representation the algorithm consists of three phases: generation, transformation and solving constraints. In the constraint generation phase a ML expression is translated to constraint set. The constraints and types are defined mutually. This phase implements an optimization - avoiding multiple solving of the same constraint set (which can be caused by let expression). In the constraint solving phase the algorithm for first-order unification is implemented.

The main idea is that compiler should only produce a set of constraints and invoke an independent solver. This approach enables easier addition of new constructs to the language in terms of type inference. The strengths of this

representation are readability and extensibility of the algorithm.

Acknowledgment

The research reported in the paper is done as a part of the master project at Faculty of Technical Sciences (Novi Sad) supervised by Prof. Silvia Ghilezan.

References

[1] Benjamin C. Pierce (editor), Didier Rmy, Francois Pottier. *Advanced Topics in Types and Programming Languages*. The MIT Press, Camridge, Massauchesetts, London, England, 2005.

[2] Luis Damas and Robin Milner. *Principal type-schemes for functional programs*. POPL, 1982.

[3] Martin Odersky, Martin Sulzmann, and Martin Wehr. *Type inference with constrained types.* TAPOS, 5(1), 1999.

[4] Robin Milner. *A theory of type polymorphism in programming*. Journal of Computer and System Sciences, 17:348375, 1978.

Self-interpreters without fixed points?

Andrej Bauer[1], **François Pitois**[2]

[1] *University of Ljubljana (Slovenia)*
[2] *École normale supérieure de Lyon (France)*
E-mail: [1] Andrej.Bauer@andrej.com, [2] francois.pitois@ens-lyon.fr

Keywords:
λ-calculus, self-interpreter, fixed point operator.

Abstract: A self-interpreter is a program which evaluates source code for a language, implemented in the same language. Self-interpreters exist in fragments of λ-calculus that have fixed point operators, and in fact one can construct a fixed point operator from a self-interpreter, provided that the type of source code is fixed. Thus, if one wants a self-interpreter in a total language (which of course does not have fixed point operators), the definition of self-interpreter must be weakened. Matt Brown and Jens Palsberg [1] provided one, but theirs seems too relaxed, as we can build self-interpreters even in Gdel's System T, but on the other hand cannot perform certain natural operations on source code. We shall discuss whether there is a more satisfactory notion of self-interpreters for a total λ-calculus. We show how the self-interpreters are related to Löb's theorem in provability logic, and to modal operators.

Acknowledgment: This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-17-1-0326.

References

[1] Brown, M., and Palsberg, P., *Breaking through the normalization barrier: a self-interpreter for F^ω*. Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, St. Petersburg, FL, USA, January, 2016. Pages 5–17.

Natural reasoning with high probabilities

Marija Boričić[1]

[1]Faculty of Organizational Sciences, University of Belgrade, Jove Ilića 154, 11000 Beograd, Serbia

Keywords:

inference rule, probability logic, natural deduction

Two areas from the beginning of the XX century, the proof theory on one side (see [8]), and the probability logic on the other one (see [7], [9], [10], [11], [12], [13], [14], [15]), makes it possible to introduce a probabilized system of natural deductions with high probabilities, denoted by **NKprob**(ε). Namely, inspired by Suppes' treatment of propositions with high probabilities (see [3], [5], [14], [15]), we propose a natural deduction system where the formulas are of the form A^n with the intended meaning that 'the probability of the formula A is greater than or equal to $1 - n\varepsilon$', for a given small real $\varepsilon > 0$ and any natural number n .

The system **NKprob**(ε) is a modification of Gentzen's natural deduction system for classical propositional logic **NK**, and besides inference rules for introducing and eliminating every propositional connective in the scope of probability operator, we also have some specific rules regarding probabilities exclusively (see [1]–[6]). Let ε be any small positive real, n and m natural numbers, and A, B and C propositional formulae. For instance, the rules for introducing and eliminating the conjunction and implication are respectively as follows:

$$\frac{A^n \quad B^m}{(A \wedge B)^{n+m}} \qquad \frac{A^n \quad (A \wedge B)^m}{B^m}$$

$$\frac{A^n \quad B^m}{(A \to B)^m} \qquad \frac{A^n \quad (A \to B)^m}{B^{n+m}}$$

Also, we would point out the hypothetical syllogism rule:

$$\frac{(A \to B)^n \quad (B \to C)^m}{(A \to C)^{n+m}}$$

To justify these rules, we use additivity, which is one of the models characteristics obviously. Models are based on Carnap–Popper–Leblanc probability functions (see [7], [10], [13]).

Lets note that we obtain an extremely elegant system enabling one to work with propositions with high probabilities (see [5]), i.e. to conclude A^n, from hypothesis of the the same form. One of the challenges is to define the notion of consistent theory in **NKprob**(ε), bearing in mind that there are more than two truth values, and the proposition A^k, for every $k \geq \frac{1}{\varepsilon}$, is always valid. After defining this notion, we believe that the soundness and completeness theorem can be proved.

Acknowledgements

This work was supported by the Serbian Ministry of Education and Science through project ON174026.

References

[1] M. Boričić, *Hypothetical syllogism rule probabilized*, Bulletin of Symbolic Logic 20, No. 3, 2014, pp. 401–402, Abstract, Logic Colloquium 2012.

[2] M. Boričić, *Inference rules for probability logic*, Publications de l'Institut Mathématique, vol. 100 (2016), pp. 77–86.

[3] M. Boričić, *Suppes-style rules for probability logic*, Bulletin of Symbolic Logic, Vol. 22, No. 3, 2016b, p. 431, Logic Colloquium 2015

[4] M. Boričić, *Natural deduction probabilized*, Bulletin of Symbolic Logic, Vol. 23, No. 2, 2017a, p. 259, Logic Colloquium 2016

[5] M. Boričić, *Suppes-style sequent calculus for probability logic*, Journal of Logic and Computation 27 (4), 2017b, pp. 1157-1168.

[6] M. Boričić, *Sequent calculus for classical logic probabilized*, Archive for Mathematical Logic (to appear, 2018)

[7] R. Carnap, *Logical Foundations of Probability*, University of Chicago Press, Chicago, 1950.

[8] G. Gentzen, *Untersuchungen über das logische Schliessen*, Mathematische Zeitschrift **39** (1934-35), 176–210, 405–431. (or G. Gentzen, *Collected Papers*, (ed. M. E. Szabo), North–Holland, Amsterdam, 1969)

[9] T. Hailperin, *Probability logic*, Notre Dame Journal of Formal Logic 25 (1984), 198-212.

[10] H. Leblanc, *Probability functions and their assumption sets — the singulary case*, Journal of Philosophical Logic, vol. 12 (1983), pp. 382–402.

[11] Z. Ognjanović, M. Rašković, Z. Marković, *Probability logics*, Logic in Computer Science, Zbornik radova 12 (20), Z. Ognjanović (ed.), Mathematical Institute SANU, Belgrade, 2009, pp. 35–111.

[12] Z. Ognjanović, M. Rašković, Z. Marković, *Probability Logics*. Springer, Berlin (2016)

[13] K. R. Popper, *Two autonomous axiom systems for the calculus of probabilities*, The British Journal for the Philosophy of Science 6 (1955), 51-57, 176, 351.

[14] P. Suppes, *Probabilistic inference and the concept of total evidence*, in J. Hintikka and P. Suppes (eds.), Aspects of Inductive Inference, North–Holland, Amsterdam, 1966, pp. 49–55.

[15] C. G. Wagner, *Modus tollens probabilized*, British Journal for the Philosophy of Science 54(4) (2004), 747–753.

Complexity of some framgents of description logics

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

[1] *Oxford University*

Oxford Road, Oxfordshire, Oxford, UK

[2,3] *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, [2,3] {jreutter,dvrgoc}@ing.puc.cl, [4] veky@math.hr

LAP, Dubrovnik — September 2018

Keywords:
Description logic, CPDL, EXPTIME

An important application of modal logic in computer science is the theoretical foundation of *description logic*, which was born out of need to represent knowledge; the initial development of artificial intelligence depended on what we knew about the functioning of the human brain and the development of cognition and reasoning. Knowledge representation gave rise to two important uses: automated reasoning by using logical formalisms, and the construction of basic building blocks that are reusable in representing similar knowledge. Description logic falls into the first category.

Even though it was used before to model various databases, a large application domain for description logic was uncovered in the early 21st century through the Semantic web movement, whose principal idea was to make the Internet (i.e. its part called the World Wide Web) more structured and therefore more machine-readable. One of the basic languages used for this purpose, OWL (Web Ontology Language), is actually a fragment of description logic of the family $\mathcal{SH}$, where different versions correspond to technically different logics (OWL DL corresponds to $\mathcal{SHOIN}^{(\mathrm{D})}$, OWL Lite corresponds to $\mathcal{SHIF}^{(\mathrm{D})}$, and OWL 2 from 2009 corresponds to $\mathcal{SROIQ}^{(\mathrm{D})}$); this was officially recognized by the W3C (World Wide Web Consortium). In parallel, the language DL-Lite was developed [1] in an attempt to bring description logic closer to potential applications.

A modern trend in teaching 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].

The important questions of the complexity of a logic, such as the complexity of deciding whether a formula is valid or satisfiable, or the validity of a logical inference, are typically formulated in terms of description logics as the complexity of answering queries. Ontologies, i.e. formalized databases in descriptive logic, are naturally represented by graphs; concepts, i.e. formalized classes of objects correspond to vertices in this context, and roles, i.e. formalized relationships between objects, correspond to edges. Queries can be expressed over concepts or over roles, and as such they correspond to two classes of formulas in the corresponding descriptive logic. In graphs they correspond to searching for vertices or paths with certain properties.

To better connect the complexity of responding to queries and the decision of validity or satisfiability, it is prudent to classify what we know about the world into two disjoint parts. In the first part, traditionally called ABox, there are facts, atomic formulas with no variables which are used to state that particular individuals are contained in concepts, or that particular pairs of individuals are contained in roles. In the second, traditionally named TBox, there are axioms: universally quantified sentences with no constants, which state general laws that are true in the world. For example, "Every employee is a person" is part of the TBox, and "Marko is an employee" is part of the ABox.

Why does this classification matter? Because axioms have a higher degree or persistence ("expiration date") than facts, and especially higher than queries. In other words, it is conceivable that while working with a knowledge base we observe various queries and change (update) the facts, while the axioms stay the same. We call the complexity of responses to queries under the assumption of a constant TBox data complexity, while we call the complexity of responses to queries where the query, the ABox and the TBox are parameters combined complexity. Although data complexity is much more relevant in practice, combined complexity is more amenable to theoretical considerations because it better fits the complexity of the logic itself by not separating the facts from the axioms as much.

An important and long known connection of modal and description logic bridges the multimodal system K (basic Kripke system with multiple modal operators) and 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. Even this connection is fairly well explored as far as the basic logic is concerned, but PDL has a wide variety of extensions, and it is not always clear which description logics they correspond to. As a matter of fact, 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.

One example, which we intend to present, 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 [3] that PDL$^{(\neg)}$ (i.e. PDL with negations of atomic programs, but with no converses) is EXPTIME-complete, and we believe that an analogous result can be proved for CPDL$^{(\neg)}$.

Of course, EXPTIME is a highly impractical class for computing over large instances of a problem, but it is of some use. First of all, as we already mentioned, data complexity is far more important in practice as well as often far smaller than combined complexity, and similar proof techniques could be used to prove that the corresponding data complexity is coNP-complete. Second, in such complicated logics, decidability itself, i.e. the existence of an algorithm of any complexity, is an important signal that guides the search for potential applications. Concretely, allowing unrestricted negation (i.e. that of programs obtained via regular expressions from atomic programs) instead of just the negation of atomic programs renders the problem, even without converses and already with respect to data complexity, undecidable.

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

ZW calculi: diagrammatic languages for pure-state quantum computing

Amar Hadzihasanovic

RIMS, Kyoto University, Japan

E-mail: ahadziha@kurims.kyoto-u.ac.jp

Keywords:
quantum computing, categorical quantum mechanics, string diagrams.

This abstract is based on the papers [8] (co-authored with Kang Feng Ng and Quanlong Wang) and [7] (co-authored with Giovanni de Felice and Kang Feng Ng).

Categorical quantum mechanics studies finite-dimensional quantum theory, in particular the structures relevant to quantum computing, as an abstract process theory whose model is a dagger compact closed category [4]. Since its inception, it has used the corresponding string-diagrammatic language both as a calculational tool, and as a heuristic for determining algebraic structures that fit naturally in the framework.

In [3], Coecke and Duncan proposed an axiomatisation of complementary quantum observables in terms of a pair of interacting special Frobenius algebras. These structures, with some additions, seemed to capture enough interesting aspects of pure-state quantum theory, such as non-locality, that the question arose whether they could be the basis of a complete equational axiomatisation of the relevant monoidal categories. The resulting partial diagrammatic axiomatisations have been called *ZX calculi*.

Compared to matrix calculus, which has been compared to "programming with bit strings", string diagrams are a higher-level language, allowing one to focus on the connections between gates and on the flow of information. Complete axiomatisations of fragments of quantum theory could provide quantum programmers with the possibility of understanding the behaviour of a circuit entirely within this language, without resorting to linear algebra.

Most attention has been devoted to qubit computing, and a ZX calculus complete for the stabiliser fragment, and one complete for single-qubit processes in the approximately universal Clifford+T fragment have been presented by Backens [1]. Completeness for the whole of pure-state qubit theory has remained an open problem for a long time.

Observing that the components of the ZX calculi seemed ill-suited to the analysis of finer properties of entangled qubit states, Coecke and Kissinger pro-

posed a variant where one Frobenius algebra is replaced with a different one, satisfying an "anti-specialness" equation. In [5], I extended this theory into a calculus modelled on ZX calculi, keeping some of their most convenient properties, such as the ability to handle diagrams as undirected labelled multigraphs: the *ZW calculus*. The original ZW calculus was a complete axiomatisation of the monoidal category of free abelian groups on 2^n generators ("qubits with integer coefficients"). In [9], Jeandel, Perdrix, and Vilmart used a non-trivial translation of this ZW calculus into a ZX calculus to obtain a complete axiomatisation of the approximately universal Clifford+T fragment.

In my thesis [6, Chapter 5], I extended the ZW calculus to obtain the first complete equational axiomatisation of the monoidal category of qubits and linear maps, with the tensor product as monoidal product. In practice, this means that the equality of the interpretation of any two circuits as linear maps of qubits can be decided by rewriting string diagrams.

The proof of completeness was achieved by the introduction of a normal form for diagrams, and a strategy which rewrites any diagram into the normal form. Soon afterwards, Wang and Ng derived from it a universal completion of the ZX calculus [8], which is directly inter-translatable with the ZW calculus, thus bringing both calculi to their intended limit.

Since its early versions, the ZX calculus has had the advantage of including familiar gates from the circuit model of quantum computing, such as the Hadamard gate and the CNOT gate, either as basic components of the language, or as simple composite diagrams. This facilitates the transition between formalisms and the application to known algorithms and protocols, and is related to the presence of a simple, well-behaved "core" of the ZX calculus, modelling the interaction of two complementary observables. Access to complementary observables is fundamental in quantum computing schemes such as the one-way quantum computer.

The ZW calculus only includes one special commutative Frobenius algebra as a basic component. On the other hand, it has a fundamentally different "core", which is obtained by removing a single component that does not interact as naturally with the rest. This core has the property of only representing maps that have a definite parity with respect to the computational basis: the subspaces spanned by basis states with an even or odd number of 1s are either preserved, or interchanged by a map. This happens to be compatible with an interpretation of the basis states of a single qubit as the empty and occupied states of a *local fermionic mode*, the unit of information of the *fermionic quantum computing* (FQC) model [2].

Fermionic quantum computing is computationally equivalent to qubit computing. The connection with the ZW calculus suggested that an independent fermionic version of the calculus could be developed, combining the best of both worlds with respect to FQC rather than qubit computing: the superior structural properties of the ZW calculus, including an intuitive normalisation procedure for diagrams, together with the superior hands-on features of the ZX calculus.

In [7], De Felice, Ng and I presented such an axiomatisation: the *fermionic*

ZW calculus. This is an equational axiomatisation the monoidal category **LFM** of local fermionic modes and maps that either preserve or reverse the parity of a state, with the tensor product of $\mathbb{Z}_2$-graded Hilbert spaces as the monoidal product.

We described a number of physical gates from which one may build fermionic quantum circuits, and showed that all have simple representations in our language: the beam splitter, the phase gates, the fermionic swap gate, and the empty and occupied state preparations. As a first practical example, we showed how to calculate in the diagrammatic language the statistics of a simple circuit, the fermionic Mach-Zehnder interferometer.

Acknowledgment

Supported by a JSPS Postdoctoral Research Fellowship and by JSPS KAKENHI Grant Number 17F17810.

References

[1] M. Backens. The ZX-calculus is complete for stabilizer quantum mechanics. *New Journal of Physics*, 16(9):093021, 2014.

[2] S.B. Bravyi and A.Y. Kitaev. Fermionic quantum computation. *Annals of Physics*, 298(1):210–226, 2002.

[3] B. Coecke and R. Duncan. Interacting quantum observables. In *International Colloquium on Automata, Languages, and Programming*, pages 298–310, Berlin/Heidelberg, 2008. Springer.

[4] B. Coecke and A. Kissinger. *Picturing quantum processes*. Cambridge University Press, Cambridge, 2017.

[5] A. Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In *Proceedings of the 2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 573–584, Kyoto, Japan, 2015. IEEE.

[6] A. Hadzihasanovic. *The algebra of entanglement and the geometry of composition*. PhD thesis, University of Oxford, 2017.

[7] A. Hadzihasanovic, G. de Felice, and K. F. Ng. A diagrammatic axiomatisation of fermionic quantum circuits, 2018. Accepted at Third International Conference on Formal Structures for Computation and Deduction (FSCD) 2018.

[8] A. Hadzihasanovic, K.F. Ng, and Q. Wang. Two complete axiomatisations of pure-state qubit quantum computing, 2018. Accepted at the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) 2018.

[9] E. Jeandel, S. Perdrix, and R. Vilmart. A complete axiomatisation of the zx-calculus for clifford+t quantum mechanics, 2018. Accepted at Thirty-Third Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) 2018.

Computable type and semicomputable boundary condition

Zvonko Iljazović and Bojan Pažek

We examine conditions under which a semicomputable set in a computable metric space is computable. We know that topology plays an important role in the description of such conditions. Some topological properties can force a semicomputable set to be computable or at least to have computable points. For example, if S is a semicomputable compact manifold with boundary such that ∂S is a semicomputable set, then S needs to be computable [4].

It is also know that a semicomputable continuum chainable from a to b, where a and b are computable points, must be computable [2, 5]. So the question under what conditions implication

$$\partial S \text{ semicomputable } \Longrightarrow S \text{ computable} \tag{1}$$

holds makes sense not just when S is a manifold (with boundary). Even when S is not a manifold, we can naturally consider certain subset of S as its boundary and ask whether (1) holds.

The following definition naturally arises. Let Δ and Σ be some topological spaces such that Σ is a subspace of Δ. We say that the topological pair (Δ, Σ) has **computable type** if for every computable metric space (X, d, α) and every embedding $f\colon \Delta \to X$ such that $f(\Delta)$ and $f(\Sigma)$ are semicomputable sets in (X, d, α) we have that $f(\Delta)$ is a computable set in (X, d, α).

So, if M is a compact manifold with boundary, then $(M, \partial M)$ has computable type; if K is a continuum chainable from a to b, then $(K, \{a, b\})$ has computable type.

It was proved recently in [6] that (D, W) has computable type, where D is the Warsaw disc and W is the Warsaw circle. The Warsaw circle W is defined by

$$W = (\{0\} \times [-2, 1]) \cup \{(x, \sin \frac{1}{x}) \mid 0 < x \leq 1\} \cup (\{1\} \times [-2, \sin 1]) \cup ([0, 1] \times \{-2\}),$$

see Figure 1. The Warsaw disc (see [8]) is the area of the plane bounded by the Warsaw circle (together with the Warsaw circle), see Figure 2.

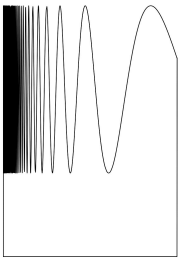

Figure 1.

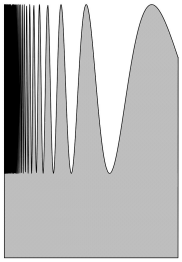

Figure 2.

Note that the Warsaw circle is not a manifold. Also, the Warsaw disc is not a manifold. However, these spaces "look like" a circle and a 2-cell respectively. The same can be said for spaces shown in Figures 3 and 4. It is naturally to ask the following question: does (Δ, Σ) have computable type if Σ is the space shown in Figure 3 (the double Warsaw circle) and Δ is the space bounded by Σ? The same question can be asked for the spaces shown in Figure 4.

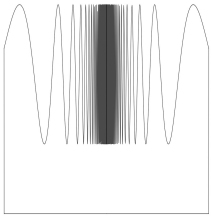

Figure 3.

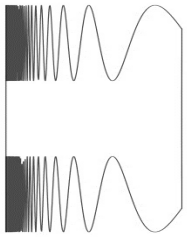

Figure 4.

As an answer to these questions, we have Theorem 1. First, we need the following notation.

Let $I := [0,1]$ and $I^2 := I \times I$. We set

$$S_1 := \{0\} \times I, \quad S_2 := I \times \{0\}, \quad S_3 := \{1\} \times I, \quad S_4 := I \times \{1\},$$

$$S = S_1 \cup S_2 \cup S_3 \cup S_4 \quad \text{and} \quad \mathring{I}^2 := I^2 \setminus S.$$

If (X,d) is a metric space, $A \subseteq X$ and $\varepsilon > 0$, let $N_\varepsilon(A)$ denote the open ε-neighbourhood of A in (X,d). Let d_H denote the Hausdorff metric (on the set of all nonempty compact sets in (X,d)).

Theorem 1. *Suppose that Δ and Σ are compact subsets of $\mathbb{R}^2$ such that $\Sigma \subseteq \Delta$ and such that the following holds:*

(i) there exist compact sets Σ_1, Σ_2, Σ_3 and Σ_4 such that

$$\Sigma = \Sigma_1 \cup \Sigma_2 \cup \Sigma_3 \cup \Sigma_4, \quad \Sigma_1 \cap \Sigma_3 = \emptyset \quad \text{and} \quad \Sigma_2 \cap \Sigma_4 = \emptyset;$$

(ii) for every $\varepsilon > 0$ there exists embedding $f\colon I^2 \to \mathbb{R}^2$ such that

$$f(I^2) \subseteq \Delta, \quad \Sigma \cap f(\mathring{I}^2) = \emptyset,$$
$$\Delta \setminus f(I^2) \subseteq N_\varepsilon(f(S)) \quad \textit{and} \quad d_H(f(S_i), \Sigma_i) < \varepsilon, \ \forall\ i \in \{1,2,3,4\}.$$

Then the topological pair (Δ, Σ) has computable type.

References

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

[2] Iljazović, Z.: Chainable and circularly chainable continua in computable metric spaces, *Journal of Universal Computer Science*, 15(6):1206–1235, 2009.

[3] Iljazović, Z.: Co-c.e. Spheres and Cells in Computable Metric Spaces, *Logical Methods in Computer Science*, Vol. 7(3:05):1–21, 2011.

[4] Iljazović, Z.: Compact manifolds with computable boundaries, *Logical Methods in Computer Science*, Vol. 9(4:19):1–22, 2013.

[5] Iljazović, Z., Pažek, B.: Computable intersection points, *Computability*, Vol. 7, no. 1, pp. 57-99, 2018.

[6] Iljazović, Z., Pažek, B.: Warsaw discs and semicomputability, *Topology and its Applications*, 239 (2018) 308–323.

[7] Miller, J.S., Effectiveness for Embedded Spheres and Balls, *Electronic Notes in Theoretical Computer Science*, volume 66, Elsevier, 2002, 127-138.

[8] Nadler, S.B.: *Continuum theory*, Marcel Dekker, Inc., New York, 1992.

Automated Reasoning in Geometry

Predrag Janičić

Faculty of Mathematics, University of Belgrade

Studentski trg 16

E-mail: janicic@matf.bg.ac.rs

Keywords:

Automated theorem proving, interactive theorem proving, automated reasoning

The history of automated reasoning in geometry begins almost with very first, pioneering days of computers. It is so because of paradigmatic geometrical reasoning and because of omnipresence of geometry. Geometric reasoning is crucial in education, but also has many applications in industry (e.g., in CAD system, in GIS systems, in robotics, etc). Methods and ideas from automated reasoning in geometry have made significant impact on all subareas of automated reasoning, but also on the whole of artificial intelligence.

Automated reasoning in geometry typically deals with *automated* or *interactive* theorem proving. In the former, computers aim to prove theorems completely automatically, while in the latter, the role of the system is to act as a *proof assistant* that verifies the reasoning steps of the user, guides the proving process, and provides some limited automation. These two branches are often connected through methods that can produce geometric proofs automatically, where either the proofs or the methods themselves are fully-verified. There are other subareas of automated reasoning in geometry, such as geometry constraint solving (including construction problems with ruler and compass).

In this talk, an overview of most significant methods and results of automated reasoning in geometry will be given. Methods for automated theorem proving in geometry, including the area method, the full angle method, the deductive database method, Wu's method, Buchberger's method, will be briefly presented. Also, most significant formalisations of geometry within proof assistants will be discussed. The talk will be partly based on a recently published book chapter [1].

Also, a brief overview of author's results in the area of automated reasoning in geometry will be given.

Acknowledgment

The research reported in the paper is partly supported by the research grant 174021 by Ministry of science of Republic of Serbia.

References

[1] Julien Narboux, Predrag Janičić, Jacques Fleuriot, *Computer-assisted Theorem Proving in Synthetic Geometry*, in Sitharam, John, Sidman (eds): Handbook of Geometric Constraint Systems Principles, Chapman and Hall/CRC, 2018.

Towards Probabilistic Testing of Lambda Terms

Simona Kašterović[1], Michele Pagani[2]

[1] *Faculty of Technical Sciences, University of Novi Sad*
Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
[2] *Institute of Research in Computational Computing, University Paris Diderot - Paris 7*
8 place Aurlie Nemours, 75013 Paris, France
E-mail: [1]simona.k@uns.ac.rs, [2]pagani@irif.fr

Keywords:
Bisimulation, Probabilistic Lambda Calculus, Probabilistic Testing.

Probabilistic computation has proved to be useful in many application areas, some examples are: natural language processing, robotics, computer vision and machine learning. It is a new paradigm that deals computationally with probabilistic models by allowing probabilistic choice as primitive, when designing algorithms.

We consider a pure lambda calculus extended with a probabilistic choice operator, called *probabilistic lambda calculus* ($\Lambda_\oplus$). Let
$X = \{x, y, z, \dots, x_1, y_1, z_1, \dots\}$ be a denumerable set of variables. The set of terms ($\Lambda_\oplus$-terms) is generated by the following grammar:

$$M, N ::= x \mid \lambda x.M \mid MN \mid M \oplus N.$$

The probabilistic choice operator $M \oplus N$ is a term which can behave as either M or N, each with probability $\frac{1}{2}$. The call-by-name evaluation is considered.

Using probabilistic operational semantics ([3]) and notion of applicative bisimilarity ([1]), context equivalence ($\simeq_\oplus$) and probabilistic applicative bisimulation ($\sim$) are defined in [2]. Moreover, it is shown that probabilistic applicative bisimulation is a congruence, hence included in context equivalence. However, these two relations do not coincide.

Furthermore, in order to overcome the problem, a coupled logical bisimulation is defined and it is proved that it does coincide with context equivalence in the probabilistic lambda calculus.

On the other hand, a language for testing concurrent processes and probabilistic bisimulation for processes, represented using a probabilistic transition system, were studied in [4]. Our goal is designing a testing semantics, which

correspond to the context equivalence. We will introduce some basic notions, necessary to describe the main idea.

Definition 1 *A probabilistic transition system is a tuple $\mathcal{P} = (Pr, Act, Can, \mu)$, where Pr is a set of processes, Act is a set of (observable) actions, Can is an Act-indexed family of sets of processes, with Can_a we denote set of all processes that can perform an action a, and μ is a family of probability distributions $\mu_{p,a} : Pr \to [0, 1]$.*

The test language is defined in the following way.

Definition 2 *The testing language T has the syntax*

$$t ::= \omega \mid a.t \mid (t_1, \ldots, t_n)$$

where ω is a symbol for termination and $a \in Act$.

For each test, the set of observations, representing a description of experiences at the end of the execution, is defined.

Definition 3 *A test t induces the following observation set O_t:*

$$O_\omega = \{1_\omega\},$$
$$O_{a.t} = \{0_\omega\} \cup \{1_a : e \mid e \in O_t\},$$
$$O_{t_1,\ldots,t_n} = O_{t_1} \times \cdots \times O_{t_n}.$$

The execution of a given test on a particular process p results in some subset of O_t. Since in probabilistic transition system processes are modelled probabilistically, the possible resulting observations will occur with different probabilities. This is described by the probability distribution $P_{t,p}$.

Definition 4 *Let t be a test and p a process. Then, $P_{t,p} : O_t \to [0, 1]$ is the probability distribution defined structurally on t as follows:*

1. $P_{w,p} = 1$
2. $P_{a.t,p}(O_a) = \begin{cases} 1 & if\ p\ can\ not\ perform\ the\ action\ a \\ 0 & otherwise \end{cases}$

   $P_{a.t,p}(1_a : e) = \begin{cases} 0 & if\ p\ can\ not\ perform\ the\ action\ a \\ \sum_{p'} \mu_{p,a}(p') \cdot P_{t,p'}(e) & otherwise \end{cases}$
3. $P_{(t_1,\ldots,t_n),p}((e1, \ldots, e_n)) = \prod_i P_{t_i,p}(e_i)$.

Probabilistic bisimulation ($\equiv$) is defined as an equivalence relation on processes, such that whenever two processes are in a relation, then for all actions a and all equivalence classes $S \in Pr/\equiv$, it holds
$\sum_{p' \in S} \mu_{p,a}(p') = \sum_{q' \in S} \mu_{q,a}(q')$. Two processes are probabilistically bisimilar $p \equiv_p q$ if the pair (p, q) is contained in some probabilistic bisimulation.

The main result presented in [4] is the fact that the limit as to the distinguishing power is captured by notion of probabilistic bisimilarity.

Theorem 1 *Let $\mathcal{P} = (Pr, Act, Can, \mu)$ be a probabilistic transition system satisfying the minimal deviation assumption. Then $p \equiv_p q$ just in case $P_{t,p}(e) = P_{t,q}(e)$, for all test t and observations $e \in O_t$.*

Using the connection between probabilistic lambda calculus and probabilistic transition system, described in [2], it is possible to define a notion of test which will distinguish two non-bisimilar terms. Since probabilistic bisimulation and context equivalence do not coincide, it can happen that two terms are distinguished by a test, but context equivalent. As the example, one can look at the terms $M = \lambda x.\lambda y.(x \oplus y)$ and $N = (\lambda x.\lambda y.x) \oplus (\lambda x.\lambda y.y)$. Our goal is to define a notion of test which will distinguish terms that are not context (observable) equivalent and whose execution on context equivalent terms, will assign the same probability to each evidence.

References

[1] Abramsky, S., *The lazy lambda calculus*, In D. Turner, editor Research Topics in Funtional Programming, pages 65–117, Addison Wesley, 1990.

[2] Dal Lago, U., Sangiorgi, D., and Alberti, M., *On Coinductive Equivalences for Higher-Order Probabilistic Functional Programs,* In 41st International Symposium on Principles of Programming Languages, Proceedings, pages 297-308, 2014.

[3] Dal Lago, U., and Zorzi, M., *Probabilistic Operational Semantics for the Lambda Calculus* , RAIRO - Theoretical Informatics and Applications, 46(3):413-450, 2012.

[4] Larsen, K. G., and Skou, A., *Bisimulation through Probabilistic Testing*, Information and Computation 94: 1-28, 1991.

Statistical Model Checking in the Analysis of Distance-bounding Protocols

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

[1] *King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia*
[2] *University College London, London, UK*
[3] *National Research University Higher School of Economics, Moscow, Russia*
[4] *University of Rijeka, Department of Mathematics, Rijeka, Croatia*
[5] *Federal University of Paraíba, João Pessoa, Brazil*
[6] *fortiss, Munich, Germany*
[7] *University of Pennsylvania, Philadelphia, PA, USA*
[8] *SRI International, Menlo Park, CA, USA*

Keywords:
Distance-bounding protocols, Distance fraud, Probabilistic rewriting, Statistical model checking, Maude.

Proximity based access control systems, such as systems using smart-cards or smart keys, use cryptographic protocols to ensure their security requirements. However, ensuring authentication alone may not meet the security goals. Namely, proximity based access is well-known to be vulnerable to relay attacks, also known as *Mafia fraud*. Distance-bounding (DB) protocols were proposed to prevent such relay attacks on proximity-based access control systems. Besides authentication DB protocols aim to ensure physical proximity between the parties involved, namely between the verifier, controling the access to some resource, and the prover, requesting access.

In a DB protocol, the verifier computes an upper bound on the distance to the prover. This is done by measuring the time needed for a signal to travel to the prover and back, relying on the assumptions on the maximum signal's velocity. DB protocols are, however, vulnerable to *distance fraud*, in which a dishonest prover is able to manipulate the distance estimation computed by the verifier in order to make himself appear closer than he actually is. Distance fraud attacks are timing attacks which are particularly significant as they may appear without collusion with external entities.

Despite their conceptual simplicity, formal analysis of DB protocols is challenging, involving many subtleties. Devising a formal characterization of DB protocols and distance fraud attacks that is amenable to automated formal

analysis is non-trivial, primarily because of their real-time and probabilistic nature.

In this work, we present a framework, based on rewriting logic, for formal analysis of different forms of distance-fraud, including recently identified timing attacks. We introduce a generic, real-time and probabilistic model of DB protocols and use it to (mechanically) establish false-acceptance and false-rejection probabilities through statistical model checking with MAUDE and PVESTA. In the analysis we consider various settings and attacker models.

Using this framework, we firstly accurately confirm known results. We then define and quantitatively evaluate new guessing-ahead attack strategies that would otherwise be difficult to analyze manually.

Acknowledgment

Alturki is partially supported by KFUPM through his sabbatical project SL161003. Ban Kirigin is supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219. Scedrov is partially supported by ONR. The participation of Kanovich and Scedrov in the preparation of this article was partially within the framework of the Basic Research Program at the National Research University Higher School of Economics (HSE) and supported within the framework of a subsidy 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.

References

[1] Agha G., Meseguer J., Sen K., *PMaude: Rewrite-based specification language for probabilistic object systems*, Electronic Notes in Theoretical Computer Science, vol. 153, no. 2, pp. 213239, 2006.

[2] Alturki, M.A., Kanovich M., Ban Kirigin T., Nigam V., Scedrov A., Talcott C., *Statistical Model Checking of Guessing and Timing Attacks on Distance-bounding Protocols*, in Workshop on Foundations of Computer Security, July 2018.

[3] Alturki, M.A., Meseguer J., *PVeStA: A parallel statistical model checking and quantitative analysis tool*, in Algebra and Coalgebra in Computer Science, ser. Lecture Notes in Computer Science, A. Corradini, B. Klin, and C. Crstea, Eds. Springer Berlin / Heidelberg, 2011, vol. 6859, pp. 386392.

[4] M. Clavel, F. Duran, S. Eker, Lincoln P., Mart-Oliet N., Meseguer J., Talcott C. , *All About Maude - A High-Performance Logical Framework*, ser. Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag, 2007, vol. 4350.

[5] Hancke, G.P., Kuhn M.G., *An RFID distance bounding protocol*, in First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM05), Sept 2005, pp. 6773.

[6] Kanovich M., Ban Kirigin T., Nigam V., Scedrov A., Talcott C., *Can we mitigate the attacks on distance-bounding protocols by using challenge-response rounds repeatedly?*, in Workshop on Foundations of Computer Security, June 2016.

[7] Kanovich M., Ban Kirigin T., Nigam V., Scedrov A., Talcott C., *Time, computational complexity, and probability in the analysis of distance-bounding protocols*, Journal of Computer Security, vol. 25, no. 6, pp. 585630, 2017. [Online]. Available: https: //doi.org/10.3233/JCS-0560

Reversible Computation and Principal Types in $\lambda^!$-calculus

Alberto Ciaffaglione [1], Pietro Di Gianantonio[1], Furio Honsell[1], Marina Lenisa[1], Ivan Scagnetto[1]

[1] *DMIF, University of Udine*
Viale delle Scienze, 206 – Udine – Italy
E-mail: [1] name.surname@uniud.it

Keywords:
Games, Geometry of Interaction, Reversible Computations, Lambda Calculus.

In [1], S.Abramsky discusses *reversible computation* in a game-theoretic setting using partial *involutions*, *i.e.* functions such that $f(u) = v \Leftrightarrow f(v) = u$. The construction is a special case of a general categorical paradigm [3, 4], which amounts to defining a *combinatory algebra* starting from a *Geometry of Interaction* (GoI) *Situation* in a traced symmetric monoidal category. Involutions amount to history-free strategies and apply according to *GoI symmetric feedback*/Girard's *Execution Formula*.

We highlight a *duality* between the GoI interpretation of a λ-term as an involution and its *principal type* w.r.t. an *intersection types discipline* for a refinement of λ-calculus inspired by Linear Logic, the $\lambda^!$-calculus.
The grammar of types is: $\mu ::= \alpha \mid \mu \to \mu \mid !\mu \mid ¡\mu \mid \mu \wedge \mu$.
The grammar of $\lambda^!$-terms is: $M ::= x \mid MN \mid \lambda x.M \mid \lambda!x.M \mid !M$, where λ-abstractions can be taken only if x occurs at most once and is not in the scope of a !. Reduction rules are extended with a *!-pattern* β-reduction.

We define inductively the judgements: "$\Vdash M : \sigma$", "the term M has principal type scheme σ", and "$\mathcal{T}(\alpha, \sigma) = u \leftrightarrow v$", "the type-variable α in the principal type σ generates the component $u \leftrightarrow v$ of an involution". We have:

THEOREM. *Given* $M, N \in \Lambda^!$ *such that* $\Vdash M : \sigma_1 \to \sigma_2$, $\Vdash N : \tau$,

$\cdot\ f_N = \{u \leftrightarrow v \mid \exists \alpha \in \tau.\ \mathcal{T}(\alpha, \tau) = u \leftrightarrow v\}$

$\cdot\ f_M \bullet_{GoI} f_N = \{u \leftrightarrow v \mid S = MGU(\sigma_1, \tau) \wedge \exists \alpha \in S(\sigma_2).(\mathcal{T}(\alpha, S(\sigma_2)) = u \leftrightarrow v)\}$,

where f_N *denotes the interpretation of* N *in GoI,* $\bullet_{GoI}$ *denotes application in GoI, and MGU denotes the "most general unifier".*

The above theorem unveils three conceptually independent, but ultimately equivalent, accounts of *application* in the λ-calculus: *β-reduction*, GoI application of involutions, and *unification* of principal types. Furthermore, we prove that involutions are denotations of combinators iff they generate the principal type of a λ-term, thus answering an open question raised in [1].

The present work extends [2], where the purely affine fragment of the GoI combinatory algebra of involutions and purely affine λ-calculus have been investigated.

References

[1] S. Abramsky, *A Structural Approach to Reversible Computation*, ***Theoretical Computer Science***, vol. 347 (2005), no. 3 pp. 441-464.

[2] A. Ciaffaglione, F. Honsell, M. Lenisa, I. Scagnetto, *Linear λ-calculus and Reversible Automatic Combinators*, submitted, Apr. 2018.

[3] S. Abramsky, E. Haghverdi, P. Scott, *Geometry of Interaction and linear combinatory algebras*, ***Mathematical Structures in Computer Science***, vol. 12 (2002), no. 5, pp. 625–665.

[4] S. Abramsky, M. Lenisa, *Linear realizability and full completeness for typed lambda-calculi*, ***Annals Pure Applied Logic***, vol 134 (2005), nos. 2-3, pp. 122-168.

Logical Framework for Proving the Correctness of the Chord Protocol

Bojan Marinković[1], Paola Glavan[2] and Zoran Ognjanović[1]

[1] *Mathematical Institute of the Serbian Academy of Sciences and Arts*
Beograd, Serbia
[2] *Faculty of Mechanical Engineering and Naval Architecture, University of Zagreb*
Zagreb, Croatia
E-mail: [1] [bojanm,zorano]@mi.sanu.ac.rs, [2] pglavan@fsb.hr

Keywords:
IoT, DHT, Chord, correctness, temporal logic, epistemic logic.

Internet of Things (IoT) paradigm can be defined as [1]: "The pervasive presence around us of a variety of things or objects which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals." In this framework the smart objects, which are connected by an Internet-like structure, are able to communicate and exchange information and to enable new forms of interaction among things and people [5]. The core of every IoT system consists of its discovery and control service. Usually, the objects, which participate in an IoT system have limited computing power, memory, and power supply. It is common that various heterogeneous devices participate in the same IoT system. Ordinarily, these devices are highly distributed, therefore they participate in a distributed Peer-to-Peer (P2P) system.

In a homogeneous decentralized P2P system [14], many nodes (peers) run the same application, and share the same properties in terms of computation and storage capacities and network connectivity. Nodes can join or leave the system at any time. In such framework, processes are dynamically distributed to peers, with no centralized control. Thus, P2P systems are highly scalable, as they have no inherent bottlenecks. Also, such systems are resilient to failures, attacks, etc., since there is no single node or a group of nodes that implement a critical functionality, which would render the system unusable, if disrupted. The main applications of P2P systems include file sharing, redundant storage, and real-time media streaming.

P2P systems are frequently implemented in a form of overlay networks [18], a structure, which is completely independent from the underlying network, which is actually connecting devices. An overlay network organizes system resources

in a logical topology. Some of the overlay networks are realized in the form of Distributed Hash Tables (DHTs), which provide a lookup service similar to a hash table; $\langle key, value \rangle$ pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Note that *key* is not used as a cryptographic notion, but (following the common practice in DHT-related papers) to represent identifiers of objects. The functionality of maintaining the mapping from keys to values is implemented by peers in a distributed manner, in such a way that any change in the set of participants causes a minimal amount of disruption. The Chord protocol [15, 16, 17] is one of the first, the simplest and the most popular DHTs implemenattion. The paper [15] which introduces Chord protocol was awarded the SIGCOMM 2011 Test-of-Time Award.

Because of the simplicity and popularity of the Chord protocol, it was used for the realization of the discovery and/or control service of IoT systems described in [4, 5, 6, 13, 19].

We are aware of only a few attempts to formally verify behavior of DHTs and particularly Chord [2, 3, 8, 9, 20].

In [7] a joint frame for reasoning about knowledge and linear time is presented, and the proof of weak completeness for a logic which combines expressions about knowledge with linear time is provided. We will adapt this framework using the known technics presented in [10, 11, 12], introduce the notion of *regular runs* and prove the correctness of the maintenance of the ring topology of the Chord protocol with the respect of it.

Acknowledgment

The work presented here was supported by Serbian Ministry of Education, Science and Technology Development (the projects ON174026 and III44006), through Matematički institut SANU, and Ministarstvo znanosti, obrazovanja i športa republike Hrvatske.

References

[1] L. Atzori, A. Iera, G. Morabito. *The Internet of things: A survey.* In *Computer Networks*, 54.15, 2787–2805, 2010.

[2] R. Bakhshi, D. Gurov. *Verification of Peer-to-peer Algorithms: A Case Study.* Technical report, ICT, 2006.

[3] R. Bakhshi, D. Gurov. *Verification of Peer-to-peer Algorithms: A Case Study.* In *Electronic Notes in Theoretical Computer Science* (ENTCS), Volume 181, 35–47, 2007.

[4] J. J. Bolonio, M. Urueña, G. Camarillo. *A Distributed Control Plane for the Internet of Things Based on a Distributed Hash Table.* In *Mobile Networks and Management*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 125, 108–121, 2013.

[5] S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, L. Veltri. *A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things.* In *IEEE Internet of Things Journal*, Vol. 1, No. 5, 508–521, 2014.

[6] S. Evdokimov, B. Fabian, S. Kunz, N. Schoenemann. *Comparison of Discovery Service Architectures for the Internet of Things.* In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, 2010.

[7] R. Fagin, J. Y. Halpern, Y. Moses, M. Y. Vardi. *Reasoning About Knowledge.* The MIT Press, Cambridge, Massachusetts, 1995.

[8] S. Krishnamurthy, S. El-Ansary, E. Aurell, S. Haridi. *A Statistical Theory of Chord Under Churn.* In *4th International Workshop on Peer-To-Peer Systems*, pages 93–103, 2005.

[9] D. Liben-Nowell, H. Balakrishnan, D. R. Karger. *Analysis of the Evolution of Peer-to-Peer Systems.* In *Proc.* 21^{st} *ACM Symp. Principles of Distributed Computing (PODC)*, pages 233–242, 2002.

[10] B. Marinković, Z. Ognjanović, D. Doder, A. Perović. *A Propositional Linear Time logic with Time Flow Isomorphic to* ω^2. In *Journal of Applied Logic*, 12(2), 208 – 229, 2014.

[11] Z. Ognjanović. *Discrete Linear-time Probabilistic Logics: Completeness, Decidability and Complexity.* In *Journal of Logic Computation*, Vol. 16, No. 2, 257–285, 2006.

[12] Z. Ognjanović, D. Doder, Z. Marković. *A Branching Time Logic with Two Types of Probability Operators.* In *Fifth International Conference on Scalable Uncertainty Management SUM-2011*, Springer LNCS 6929, 219–232, 2011.

[13] F. Paganelli, D. Parlanti. *A DHT-Based Discovery Service for the Internet of Things.* In *Journal of Computer Networks and Communications*, doi:10.1155/2012/107041, 2012.

[14] R. Rodrigues, P. Druschel. *Peer-to-Peer Systems* In *Communications of the ACM*, Vol. 53 Issue 10, pages 72–82, October 2010.

[15] I. Stoica, R. Morris, D. Karger, M. Kaashoek, H. Balakrishnan. *Chord: A Scalable Peer-to-Peer Lookup service for Internet Applications.* In *ACM SIGCOMM*, pages 149–160, 2001.

[16] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan. *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications.* MIT Technical report, TR-819, 2001.

[17] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan. *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications.* In *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, 17 – 32, 2003.

[18] I. Taylor. *From P2P to Web Services and Grids.* Springer-Verlag, 2005.

[19] D. Xu, Z. Wu, Z. Wu, Q. Zhang, L. Qin, J. Zhou. *Internet of Things: Hotspot-based Discovery Service Architecture with Security Mechanism.* In *International Journal of Network Security*, Vol. 17, No. 2, 208–216, 2015.

[20] P. Zave. *Using Lightweight Modeling to Understand Chord.* In ACM SIGCOMM Computer Communication Review, Vol. 42, Issue 2, pages 50–57, April 2012.

High-level and Low-level Languages for Learning Compiler Construction

Marija Mihova, Bojan Ilijoski, Vesna Kjirandziska, Mile Jovanov

University Ss Cyril and Methodious, Faculty of Computer Sciences and Engineering

Skopje

E-mail: {marija.mihova, bojan.ilijoski, vesna.kjirandziska, mile.jovanov}@finki.ukim.mk

Keywords:

Compiler, high-level programming language, target language, BNF for grammar.

A compiler is a computer program by which a high-level programming language is converted into low-level programming language that can be acted upon by a computer. Hence, in order to design a compiler, you need to be familiar with the high-level programming language you want to translate, but also you must have a great understanding of some low-level language, your target language.

The main goal of each course of learning compiler construction is to teach the students to understand all phases of the compiler design. At most Compiler courses lectured at different universities [1], [2], [3], [4], [5], the students design compiler that translates in some version of an assembly programming language. But unfortunately at our faculty, most of the students enrolled in the Compiler course do not have any knowledge about assembly languages, so our problem was to enable them to grasp all necessary concepts in Compilers without need of assembly programming[6].

For this purpose we have created two languages, one high-level programming language, and another target language which is assembly-like low-level programming language. Each year new (similar but different) languages were introduced.

The high-level programming language is based on the procedural high-level programming languages like C, Basic or Pascal (not an object-oriented language). It includes the three most basic statements and other basic features, and the key words are written in Macedonian language. The inspiration for this language comes from turtle-based programming languages used for beginners in programming languages. Indeed, the elementary statements of the languages are actually commands for the movement of the specific turtle object like a frog, robot, bird and so on.

The target language is based on assembly, but has only the most basic statements needed for the translation to be possible. All hardware knowledge for the execution of a program written in this language is excluded.

Here we will introduce both types of languages. We will pay attention on the grammars, that are usually given by syntax diagram, BNF or EBNF form. But also we will explain some concepts connected with parsing, error corrections and translation.

Acknowledgment

The research reported in the paper is partly supported by the Faculty of Computer Sciences and Engineering.

References

[1] Benders F., Haaringm J., Janssen T., Meert D., van Oostenrijk A. *Compiler Construction: A Practical Approach*, 2003.

[2] The University of Virginia Engineering: Compilers Practicum,2014", http://www.cs.virginia.edu

[3] A. Aiken, Compilers, 2014, url = "https://www.coursera.org/course/compilers

[4] University of Waterloo: Compilers",2014, url = "http://uwaterloo.ca/".

[5] G. S. NovakJr., Compiler construction, 2014.

[6] V. Kirandziska, M. Jovanov, M. Mihova, M. Gusev, Lab assessments in undergraduate course in Compilers for students with no prior knowledge in assembly, 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 738 - 743.

On basic constructive algebraic structures with apartness

Melanija Mitrović [1], Sergei Silvestrov [2]

[1] *Department of Sciences and Mathematics, Faculty of Mechanical Engineering, University of Niš, Niš, Serbia*

[2] *Division of Applied Mathematics, School of Education, Culture and Communication, Mälardalen University, Box 883, 72123 Västerås, Sweden*

E-mail: [1] melanija.mitrovic@masfak.ni.ac.rs, [2] sergei.silvestrov@mdh.se

Keywords:
Set with apartness, group with tight apartness, commutative ring with tight apartness, semigroup with apartness

The main purpose of this lecture, based on [2] (which is not, of course, comprehensive one), is to make some sort of understanding of constructive algebra in Bishop's style position. In the context of basic constructive algebraic structures constructive analogous of isomorphism theorems will be given. Although the title of this paper suggest that basic constructive algebraic structures are in the center of consideration, we brought to speak of two points of view on a given subject: classical and constructive. The classical point of view presented in the first part (introductional part of almost all classical abstract algebra books) have useful role as intuition guides and to at least link with the presentations given in the second part written in the style of classical mathematics - **CLASS**.

Within **CLASS** an *algebraic structure* can be described as a set with some (not necessarily, but often, binary) operations for combining them. Centered around an algebraic structure are notions of: substructure, homomorphism, isomorphism, congruence, quotient structure. The relationship between them is described by the celebrated *isomorphism theorems*. Troughout this section we will limited ourselves to groups, rings and semigroups.

Theorem 1 *Let $f : S \to T$ be a mapping between sets S and T. Then, the mapping $\theta : S/ker\, f \to T$ defined by $\theta(x(ker\, f)) = f(x)$ is one-one such that $f = \theta \circ \pi$. If f maps S onto T, then θ is a bijection.*

Theorem 2 *Let N be a normal subgroup of a group G. Then, for every homomorphism of groups $f : G \to H$ whose kernel contains N there exists unique homomorphism $\theta : G/N \to H$ such that $f = \theta \circ \pi$. If, in addition, f is* onto, *then θ is an isomorphism.*

Theorem 3 *Let $f : R \to S$ be a homomorphism of rings, and let I be an ideal of R contained in $\ker f$. Then, there exists unique homomorphism of rings $\theta : R/I \to S$, such that $f = \theta \circ \pi$. If, in addition, f is* onto*, then θ is an isomorphism and $I = \ker f$.*

Last two examples—groups and rings—suggest that any congruence on an algebraic structure might be determined by a single congruence class of that congruence. Study of congruences on semigroups is more complicated - no such device is available. One must study congruences as such.

Theorem 4 *Let $f : S \to T$ be a homomorphism between semigroups S and T. Then, the mapping $\theta : S/\ker f \to T$ defined by $\theta(x(\ker f)) = f(x)$ is an embedding such that $f = \theta \circ \pi$. If f maps S onto T, then θ is an isomorphism.*

One of the main topics in constructive algebra are constructive algebraic structures with apartness. The principal novelty in treating basic algebraic structures constructively is that (tight) apartness (in the sense of [1]) becomes a fundamental notion. In what follows $(S, =, \#)$, $(S, \sharp)$ will denote a set with apartness and a set with tight apartness respectively. A mapping $f : S \to T$ between two sets with (tight) apartness is *strongly extensional* mapping, or, for short, *se-mapping*, if $\forall_{x,y \in S}\,(f(x) \#_T f(y) \;\Rightarrow\; x \#_S y)$. Descriptive definition of a structure with apartness includes two main parts: the notion of certain classical algebraic structure is straighforwardly addopted; a structure is equiped with an apartness with standard operations which are strongly extensional. Quotient structure does not have, in general, a natural apartness relation. In the case of set with apartness, for most purposes we overcome this quotient structure problem, shortly **QSP**, using a *coequivalence* –irreflexive, symmetric and cotransitive relation– instead of an equivalence. For any two relations α and β on S we say that α *defines apartness on* $\mathbf{S}/\beta$ if $x \beta \# y \beta$ if and only if $(x, y) \in \alpha$.

Theorem 5 *If $f : S \to T$ is an se-mapping between sets with apartness then:*

(i) *the relation* $\operatorname{coker} f =_{def} \{(x, y) \in S \times S : f(x) \# f(y)\}$ *is a coequivalence on S (which we call the* ***cokernel*** *of f) which defines apartness on $S/\ker f$, and $\ker f \subseteq \sim \operatorname{coker} f$.*

(ii) *the mapping $\theta : S/\ker f \to T$, defined by $\theta(x(\ker f)) = f(x)$, is a one-one, a-injective se-mapping such that $f = \theta \circ \pi$; and if f maps S onto T, then θ is an apartness bijection.*

Let $(G, \sharp, \cdot, e,)$, $(R, \sharp, +, \cdot, -, 0, 1)$ be a group with tight apartness and a commutative rings with unity and a tight apartness respectively. The solution of **QSP** of these algebraic structures is based on the notion of a normal cogroup (instead of normal group) for groups and on the notion of a coideal (instead of ideal) for rings with tight apartness. Cogroups and codeals are the tools for introducing an apartness relation on quotient groups or quotient rings. The tight apartness isomorphism theorems for groups and rings follow.

Theorem 6 *Let $f : G \to H$ be an se-homomorphism between groups with tight apartness. Then:*

(i) $C_f = \{x \in G : f(x) \sharp e_H\}$ *ia a normal cogroup of* G.

(ii) *Mapping* $\theta : G/(\neg C_f) \to H$, $\theta(x(\neg C_f)) = f(x)$, *is an apartness embedding such that* $\theta \circ \pi = f$.

Theorem 7 *Let $f : R \to S$ an se-homomorphism between commutative rings with tight apartness, then $C_f = \{x \in R : f(x) \sharp 0\}$ is an inhabited coideal. There is a unique apartness embedding $\theta : R/(\neg C_f) \to S$ such that $\theta \circ \pi = f$.*

Let $(S, =, \#, \cdot)$ be a semigroup with apartness. A coequivalence $\boldsymbol{\kappa}$ defined on S is a *cocongruence* if it is *cocompatible*, i.e. $\forall_{a,b,x,y \in S} ((ax, by) \in \kappa \Rightarrow (a, b) \in \kappa \vee (x, y) \in \kappa)$. The Apartness isomorphism theorem for semigroups follows.

Theorem 8 *Let $f : S \to T$ be an se-homomorphism between semigroups with apartness. Then:*

(i) $\operatorname{coker} f$ *is a cocongruence on* S *which defines apartness on* $S/\ker f$, *and* $\ker f \subseteq \sim \operatorname{coker} f$.

(ii) *the mapping* $\theta : S/\ker f \to T$, *defined by* $\theta(x(\ker f)) = f(x)$, *is an apartness embedding such that* $f = \theta \circ \pi$; *and if* f *maps* S *onto* T, *then* θ *is an apartness isomprphism.*

List of some examples of applications of ideas just presented can be found in [2]. The study of (basic) constructive algebraic structures with apartness can have an effect on development of other areas of constructive mathematics. On the other hand, it can make both proof engineering and programming more flexibile. Of course, it is interesting in its own right, and, what is more important, it can be fun and challenging.

Standard reference for constructive algebra is [1].

Acknowledgment

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

References

[1] R. Mines, F. Richman, W. Ruitenburg, *A Course of Constructive Algebra*, Springer-Verlag, New York 1988.

[2] Mitrović M., Silvestrov S., *(Apartness) Isomorphism theorems for basic constructive algebraic structures with special emphasize on constructive semigroups with apartness - an overview*, To appear in: Stochastic Processes and Algebraic Structures – From Theory Towards Applications, Volume II: Algebraic Structures and Applications, Springer.

Categorified cyclic operads in nature

Jovana Obradović[1], Pierre-Louis Curien[2]

[1] *Charles University*
[2] *Université Paris Diderot*
E-mail: [1] obradovic@karlin.mff.cuni.cz, [2] curien@irif.fr

Keywords:
cyclic operads,categorification, coherence, polytopes

In this talk, we introduce the notion of categorified cyclic operad, with a particular focus on their place and use "in nature".

Categorified cyclic operads are like symmetric monoidal categories, in that they guide an interplay of commutativity and associativity, but they are more restrictive, as they allow less instances of these two isomorphisms. In particular, the coherence conditions of symmetric monoidal categories do not ensure coherence of categorified cyclic operads, the hexagon of Mac Lane not even being well-defined in the latter setting. The coherence conditions that we do take from Mac Lane are the pentagon and the requirement that the commutator isomorphism is involutive, but we need much more in order to ensure coherence: we need two more mixed coherence conditions (i.e. coherence conditions that involve both associator and commutator), a hexagon (which is *not* the hexagon of Mac Lane) and a decagon, as well as three more conditions which deal with the action of the symmetric group. The approach we take to treat the coherence problem is of syntactic, term-rewriting spirit and relies on the coherence result of [3]. The coherence theorem that we prove has the form "all diagrams of canonical isomorphisms commute". The proof consists of three faithful reductions, each restricting the coherence problem to a smaller class of diagrams, in order to finally reach diagrams that correspond to diagrams of canonical isomorphisms of categorified non-symmetric skeletal operads, i.e., weak Cat-operads of [3]. Intuitively speaking, the first reduction excludes the action of the symmetric group, the second removes "cyclicity", and the third replaces non-skeletality with skeletality.

We give an example of a categorified cyclic operad in the form of an easy generalisation of the structure of profunctors of Bénabou [1]. Essentially, profunctors admit the structure of a categorified cyclic operad because the cartesian product of sets (figuring in the definition of the composition of profunctors) is neither associative nor commutative on the nose.

We then show how to exploit the coherence conditions of categorified cyclic

operads in proving that the Feynman category for cyclic operads, introduced by Kaufmann and Ward in [4], admits an odd version, which is, in turn, precisely the Feynman category for anticyclic operads.

We finish with combinatorial aspects of categorified cyclic operads, i.e. with their possible characterisations in convex and discrete geometry. This investigation, which is currently in progress, aims at finding polytopes which describe the coherences of categorified cyclic operads, in the same was as the geometry of symmetric monoidal categories is demonstrated by permutoassociahedra, or the geometry of categorified operads by hypergraph polytopes [2]. By changing the set of canonical isomorphisms of categorified cyclic operads, an interesting combinatorial structure emerges: we conjecture that *cyclic operadic polytopes are associahedral, hemiassociahedral and permutohedral arrangements of hypercubes.*

References

[1] J. Bénabou, Les distributeurs, *Université Catholique de Louvain, Institut de Mathématique Pure et Appliquée*, rapport 33 (1973)

[2] K. Došen, Z. Petrić, Hypergraph polytopes, *Topology and its Applications*, 158 (2011), 1405–1444.

[3] K. Došen, Z. Petrić, *Weak Cat-operads*, Logical Methods in Computer Science 11 (1), 1-23 (2015)

[4] R. M. Kaufmann, B. C. Ward, Feynman categories, *Astérisque (Société Mathématique de France)*, Numéro 387 (2017) Vol. 32, No. 12 (2017) 396–436.

Epistemic models, hypertheories and public announcements

Nenad Savić[1] and Thomas Studer[1]

[1]Institute of Computer Science, University of Bern, Switzerland

Artemov suggested modernization of semantics and proof theory of Epistemic Logic. He introduced epistemic models which include Kripke models and are more flexible for epistemic situations. New models are more concise because they are free of the obligation to represent ignorance in Kripke models by adding new states.

A matching framework of theories (called hypertheories) for epistemic reasoning with incomplete information is outlined and it is proved that epistemic models provide a natural possible worlds semantics for hypertheories. Formally:

Definition 1 *An* **epistemic model** *is a tuple* $\mathcal{E} = (W, R_1, \ldots, R_n, \models)$*, where:*

- $W \neq \emptyset$ *is a set of states with a complete truth assignment,* $\models$*, to formulas at each state, respecting Boolean connectives and consistent with a given n-agent modal logic* $\mathsf{S5}_n$*:*

$$u \models F \quad or \quad u \models \neg F;$$

- $R_1, \ldots, R_n$ *are binary relations on* W*, such that for each formula* F

$$u \models K_i F \;\Rightarrow\; R_i(u) \models F. \tag{1}$$

Remark 1 *Truth evaluation in Kripke semantics for epistemic logic is defined inductively, starting from atomic formulas at any world (with natural conditions for Boolean connectives) and the rule:*

$$u \Vdash K_i F \;\Leftrightarrow\; R_i(u) \Vdash F. \tag{2}$$

It is clear that Kripke semantics has as an assumption common knowledge of the model, i.e., so called fully explanatory property:

if a sentence is valid at all possible states, then it is known.

In contrast to Kripke models, the truth value of formulas in epistemic models is provided by $(W, \models)$*, while the condition (1) is only a set of constraints. Also note that in (1) we have only "from left to right" implication, while in (2) we have an equivalence, hence the fully explanatory property does not hold in general for epistemic models.*

Definition 2 *A* **hypertheory** *is a tuple* $\mathcal{H} = (W, R_1, \ldots, R_n, \mathcal{T})$*, where:*

- $(W, R_1, \ldots, R_n)$ *is a frame;*

- $\mathcal{T}$ *is an assignment of a set of formulas* T_u *to each* $u \in W$*.*

An epistemic model $\mathcal{E} = (W, R_1, \ldots, R_n, \models)$ is a **model of** $\mathcal{H}$ if for each $u \in W$

$$u \models T_u.$$

In this talk we will discuss public announcements. The idea is to follow the strategy as in the Kripkean case and provide an axiomatization for the public announcement logic respecting the new setting. Namely, the idea behind public announcements is to change a model, after an agent announces some formula A, and consider a restriction of a model to only those possible worlds, where A holds (preserving the corresponding relations between the worlds). Formally, from semantical point of view:

$$M, s \models [A]B \quad \text{iff} \quad M, s \models A \ \text{ implies } \ M|_A, s \models B, \tag{3}$$

where $[A]B$ is new kind of formulas and stands for: "after announcement of A, it holds that B" and $M|_A$ is above mentioned restiriction of the model (all details can be found in [1], chapter 4). Certain principles of Public Announcement Logic, PA, are stated via semantical validity and on that basis an axiomatization is provided. How this idea reflects on the new setting and which axioms should be changed will be the topic of this talk.

References

[1] H. van Ditmarsch, W. van der Hoek, B. Kooi. Dynamic Epistemic Logic. *Springer*. 2008.

Mathematical methods for privacy protection

Milan Todorović [1], Silvia Ghilezan [1,2], Zoran Ognjanović [1]

[1] *Mathematical institute SASA, Serbia*
[2] *University of Novi Sad, Serbia*
E-mail: [1] mtodorovic@mi.sanu.ac.rs, [2] gsilvia@uns.ac.rs [2] zorano@mi.sanu.ac.rs

Keywords:
Privacy, Internet of Things, Cloud computing, Mathematical models, Formal methods.

This is the age of tremendous development of information technologies that is followed by fast appearance of new disciplines and their application in all parts of everyday life and society. Privacy is one of the most important problems that relates to information technologies. The notion of privacy has a different meaning for everyone. The 20th century brought technological advance that increased the availability and the usage of information, [11], which, in return, led to appearance of new meanings of the term "privacy". Basically, privacy is the ability and possibility to control the way of accessing the data and it's distribution, [12, 7].

The age that we live in can be called information age. Nowadays, different activities that were private in the earlier age, leave **digital trace**, that can be used to learn about individual's interests, characteristics, beliefs, but also about his/her personal information; e.g. phone number, address and even various medical data. Today, almost everyone is an everyday user of e-mail, messaging services (SMS, Skype, Viber, etc.), social networks (Facebook, Twitter, Instagram, etc.), different search engines (Google, Bing), that are used to get answers to everyday, but also to sensitive questions, and e-services (Booking, Amazon, eBay) that are used for online shopping. The usage of this services creates digital trace of the individuals, commercial entities and government institutions in various countries that users may or may not be aware of.

Internet of things is a paradigm that is, in this age, as common as the above mentioned services. This paradigm consists of usage of a large number of sensors, mostly with a help of wireless networks, in order to gather various data like temperature, energy consumption, but also different medical data that comes from the patients. It is clear that the privacy of medical data is important, but on the first glance, privacy of the data like energy consumption may seem unimportant. However, if that data privacy can be compromised, it could, for

example, lead to obtaining information about when a certain object is full with people, and when it is not, which could lead to easier planning of an intrusion.

Cloud computing is another common paradigm nowadays, that represents the computer infrastructure that gives constant access to shared resource pool (storage, services, applications) via network, most commonly via internet. In cloud computing, user data, that is processed (e.g. Google docs), or only stored (e.g. Dropbox), are located on a remote computer that is usually not in the ownership of the user. In this scenario, the question of privacy is even more important, especially since the data can be very sensitive, because other users can be malicious and can compromise the data privacy on the cloud. However, users are not the only one that can endanger privacy. Cloud providers can be malicious as well, or at least curious, so they may access the data of their users. Moreover, they can delegate and disseminate the users' data to a third party which can further use it. A taxonomy to understand privacy violations is thus sorely needed, [9].

All of the above mentioned paradigms and activities have one thing in common - the data (digital trace or user's data) is kept on the provider's side in a permanent way, that makes them practically impossible to be deleted. Taking into account that there are already well-developed methods for processing large data, that can be used to find various sensitive information, it is clear that the privacy problem is an important topic, and it will continue to be so in the future.

Mathematical models and **formal methods** have become the base tools in computer science for developing reliable software and hardware. New paradigms of information technologies, such as internet of things, cloud computing, blockchain, also require reliability that can only be provided by mathematical models.

Basic directions of mathematical methods application to data privacy are:

- computational models for privacy, based on computational models for distributed and concurrent systems [5];
- formal methods for privacy, based on logic, type systems and verification, [10];
- differential privacy, [3] and probabilistic methods of reasoning, [13], [8];
- cryptographic methods for privacy, [6];
- application in social networks, databases, medical data, linked data, [4];
- open data, [2];
- legal aspects of privacy in information systems, [1].

The complexity of this problem requires multidisciplinary teams of mathematicians, computer scientists, information scientists, lawyers, sociologists and psychologists [1, 2]. It is necessary to encourage mathematical and multidisciplinary researches that are relevant to privacy protection, since that will be one of the biggest challenges of the modern society.

Acknowledgment

The research reported in the paper is partly supported by the projects ON174026 and III044006 of the Ministry of Education, Science and Technological Development, Republic of Serbia and CEI grant 1202.018-18.

References

[1] Adam Barth, Anupam Datta, John C. Mitchell, and Hellen Nissenbaum: *Privacy and contextual integrity: Framework and applications*. IEEE Symposium on Security and Privacy: 184198 (2006).

[2] BE-OPEN - Boosting Engagement of Serbian Universities in Open Science, ERASMUS+ 2016-2019, (http://www.beopen.uns.ac.rs/).

[3] Cynthia Dwork: *Differential Privacy: A Survey of Results*. TAMCS 2008 - International Conference on Theory and Applications of Models of Computation, Lecture Notes in Computer Science 4978: 119 (2008).

[4] Svetlana Jakšić, Jovanka Pantović, Silvia Ghilezan: *Privacy for Linked Data*, Mathematical Structures in Computer Science 27(1): 33-53 (2017).

[5] Adrija Majumdar: *Privacy Calculus Theory and Its Applicability for Emerging Technologies*, Springer (2016).

[6] Miodrag J. Mihaljević and Hideki Imai: *Privacy Preserving Light-Weight Authentication Based on a Variant of Niederreiter Public-Key Encryption*, Symposium on Cryptology and Information Security - SCIS 2014.

[7] Helen Nissenbaum: *Privacy in Context*, Stanford University Press (2010).

[8] Zoran Ognjanović, Miodrag Rašković, Zoran Marković: *Probability Logics, Probability-Based Formalization of Uncertain Reasoning*, Springer, 2016.

[9] Daniel J. Solove: A taxonomy of privacy. University of Pennsylvania Law Review, 154(3): 477560 (2006).

[10] Michael Carl Tschantz, Jeannette M. Wing: Formal methods for privacy. International Symposium on Formal Methods: 1-15 (2009).

[11] Samuel Warren, Louis Brandeis: *The Right to Privacy*. Harvard Law Review 4: 193220 (1890).

[12] Alan Westin: *Privacy and Freedom*, New York: Atheneum (1967).

[13] Oliver Williams, Frank McSherry: *Probabilistic Inference and Differential Privacy*. Advances in Neural Information Processing Systems, 2451-2459 (2010).

Subexponentials in non-commutative linear logic

Andre Scedrov[1]

[1]University of Pennsylvania

Linear logical frameworks with subexponentials have been used for the specification of, among other systems, proof systems, concurrent programming languages and linear authorisation logics. In these frameworks, subexponentials can be configured to allow or not for the application of the contraction and weakening rules while the exchange rule can always be applied. This means that formulae in such frameworks can only be organised as sets and multisets of formulae not being possible to organise formulae as lists of formulae. This work investigates the proof theory of linear logic proof systems in the non-commutative variant. These systems can disallow the application of exchange rule on some subexponentials. We investigate conditions for when cut elimination is admissible in the presence of non- commutative subexponentials, investigating the interaction of the exchange rule with the local and non-local contraction rules. We also obtain some new undecidability and decidability results on non-commutative linear logic with subexponentials [1].

Logical frameworks allow the specification of deductive systems using the same logical machinery. Linear logical frameworks have been successfully used for the specification of a number of computational, logics and proof systems. Its success lies on the fact that formulas can be distinguished as linear, which behave intuitively as resources, and unbounded, which behave intuitionistically. Commutative subexponentials enhance the expressiveness of linear logic frameworks by allowing the distinction of multiple contexts. These contexts may behave as multisets of formulas or sets of formulas. Motivated by applications in distributed systems and in type-logical grammar, we propose a linear logical framework containing both commutative and non-commutative subexponentials. Non-commutative subexponentials can be used to specify contexts which behave as lists, not multisets, of formulas. In addition, motivated by our applications in type-logical grammar, where the weakenening rule is disallowed, we investigate the proof theory of formulas that can only contract, but not weaken. In fact, our contraction is non-local. We demonstrate that under some conditions such formulas may be treated as unbounded formulas, which behave intuitionistically [2].

Acknowledgements

This is joint work with Max Kanovich, Stepan Kuznetsov, and Vivek Nigam.

References

[1] Max Kanovich, Stepan Kuznetsov, Vivek Nigam, and Andre Scedrov. Subexponentials in non-commutative linear logic. Mathematical Structures in Computer Science, published online 02 May 2018. Technical report on https://arxiv.org/abs/1709.03607

[2] Max Kanovich, Stepan Kuznetsov, Vivek Nigam, and Andre Scedrov. A Logical Framework with Commutative and Non-Commutative Subexponentials. In: D. Galmiche *et al.*, eds., 9th International Joint Conference on Automated Reasoning (IJCAR 2018), Oxford, UK, July 14-17, 2018. Springer LNCS Volume 10900, Springer-Verlag, 2018, pp. 228 - 245.

A Refutation of CH

Zvonimir Šikić

In his [3] Freiling proposed a probabilistic argument in support of axiom of symmetry:

$$(\forall f : \mathbb{R} \to \mathbb{R}_{\aleph_0})(\exists x, y \in \mathbb{R})(x \notin f(y) \vee y \notin f(x)) \ . \tag{AS}$$

He proved that AS $\equiv -$CH and hence gave "a simple philosophical 'proof' of the negation of CH".

Nevertheless, AS was not accepted as a new axiom of set theory (although there were some positive attitudes on the mathematical side, e.g. Devlin [2], Mumford [4], and philosophical side, e.g. Brown [1]).

Here we offer a probabilistic refutation of CH which does not use AS. The only probabilistic principles used in our refutation are

$$(\forall A \subseteq \mathbb{R})(\forall x \in \mathbb{R})(\operatorname{card} A = \aleph_0 \Rightarrow \operatorname{pr}(X \in A) = 0) \ , \tag{1}$$

$$\operatorname{pr}(S) = \operatorname{pr}(T) = 1 \Rightarrow \operatorname{pr}(S \mid T) = \operatorname{pr}(T \mid S) = 1 \ . \tag{2}$$

The first one is a consequence of countable additivity of pr and zero probability of choosing any particular real number.

The second one is a simple result of elementary probability:

$$\begin{aligned}
&\operatorname{pr}(S) = \operatorname{pr}(T) = 1 \Rightarrow \operatorname{pr}(\overline{S}) = \operatorname{pr}(\overline{T}) = 0 \Rightarrow \\
&\operatorname{pr}(\overline{S} \vee \overline{T}) \leq \operatorname{pr}(\overline{S}) + \operatorname{pr}(\overline{T}) = 0 \Rightarrow \operatorname{pr}(\overline{\overline{S} \vee \overline{T}}) = 1 \\
&\text{i.e. } \operatorname{pr}(ST) = 1 \Rightarrow \operatorname{pr}(S)\operatorname{pr}(T \mid S) = 1 \Rightarrow \operatorname{pr}(T \mid S) = 1 \ .
\end{aligned}$$

To refute CH we first note that

$$\begin{aligned}
&(\exists f : \mathbb{R} \to \mathcal{P}(\mathbb{R}))(\forall x, y \in \mathbb{R}) \\
&\qquad \big[x \in f(x) \ \&\ \operatorname{card} f(x) < \operatorname{card} \mathbb{R} \ \&\ (f(x) \subseteq f(y) \vee f(y) \subseteq f(x))\big]
\end{aligned}$$

is provable in ZFC. Namely, if $(x_\alpha : \alpha < \operatorname{card} \mathbb{R})$ is a well order of $\mathbb{R}$ then f defined by $f(x_\alpha) = \{x_\beta : \beta \leq \alpha\}$ has the desired properties.

If CH is true then $(\forall x) \operatorname{card} f(x) \leq \aleph_0$ and for every $x, y \in \mathbb{R}$ it follows (by (1)) that $pr(x \notin f(y)) = \operatorname{pr}(y \notin f(x)) = 1$ and (by (2)) that

$$\operatorname{pr}(x \notin f(y) \mid y \notin f(x)) = 1 \ .$$

But

$$y \notin f(x) \ \&\ y \in f(y) \Rightarrow f(y) \not\subseteq f(x) \Rightarrow f(x) \subseteq f(y) \ \&\ x \in f(x) \Rightarrow x \in f(y)$$

which means that

$$\operatorname{pr}(x \notin f(y) \mid y \notin f(x)) = 0 \ .$$

This contradiction implies that CH is not true.

References

[1] Brown,, J.R. *Philosophy of Mathematics*, second edition, Routledge, 2008.

[2] Devlin, K. *How many real numbers are there?*, 2001.

[3] Freiling, C. *Axioms of symmetry: throwing darts at the real number line*, Journal of Symbolic Logic 51, pp. 190–200, 1986.

[4] Mumford, D. *The dawning age of stohasticity*, in V. Arnold, M. Atiyah et al. (eds), *Mathematics, frontiers and perspectives*, pp. 197–218, American Math. Society, 2000.

1^{st} Workshop Formal Reasoning and Semantics (FORMALS 2018)

A Satellite Workshop of Logic and Applications (LAP 2018)

Inter University Center, Dubrovnik

24–28 September 2018

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

The aim of the workshop, and also of the entire project, is to bring together researchers whose previous results were mainly in pure logic and those who previously focused on applications. An obstacle to this potentially fruitful communication is the narrow specialization of researchers, which is very often an inevitable consequence of rapid development and the advancement of scientific disciplines. We believe that both sides should benefit from this collaboration: techniques of pure logic may be useful in studying application-driven formalisms, giving inspiration to pure logicians, whose results may again be useful in the application.

The content of workshop talks provides some concrete topics of this potential collaboration, but this does not limit possibilities of future attempts in other fields.

The invited talk V. Nigam, C. Talcott, *Towards the formal verification of Industry 4.0 applications*, provides an example of a recent development of formal methods in computational security.

B. Perak, T. Ban Kirigin, *Corpus-based approach to the extraction of the emotional concepts and their ontological relations using the natural language logic operators*, also describes a work in progress in applying formal methods, namely in ontological study of cognitive and linguistic concepts.

L. Mikec, F. Pakhomov, M. Vuković, *Complexity of the interpretability logic IL*, is a recent result which is a standard step in studying a logical system: computational complexity of the satisfiability problem, in this case regarding a modal logic aimed to formalize the notion of relative interpretability between arithmetical theories.

M. Maretić, *On geometric aspects of multiple conclusion natural deductions*, also from the pure logic side of the project, is a proof-theoretic talk which puts an emphasis on human-readability of logical proofs. This is in accord with the program of FORMALS, which aims for the simplicity as well as the implementability of formalisms.

The remaining three talks share the topic: social choice theory, a study of aggregating a collective choice from individual choices in various contexts, making it an interdisciplinary field, involving economics and mathematics with possible applications in areas like politics and law, but also recently strongly connected to computer science and logic.

A. Hatzivelkos, *Mathematical model for notion of compromise in social choice theory*, presents an idea of a precise definition of compromise collective choice, so far an informal concept in social choice theory. B. Stojanović, *Propositional and first-order logic formalizations of social welfare functions* and T. Perkov: *Formalizations of social choice theory in modal logic*, survey logical formalisms in social choice theory, which will hopefully serve as a starting point of future collaborative research, namely an attempt to formalize concepts such as compromise.

These talks form the part of the workshop open to all participants of LAP, which will hopefully result in broader discussions, helpful for the future work of project research group. The workshop will also have the closed part consisting of work meeting and two 2–3 hours tutorials, aimed to serve as a foundation of future collaboration inside the group. T. Perkov, *Introduction to modal logic: a semantic approach*, is aimed to familiarize other members of the group with the expressive power of modal logic, which is often used for formalization in seemingly very different applications. B. Perak, *Ontology of the language communication and the structure of meaning*, in the first part presents the material, psychological and social components of the language ontology, as conceived in emergent system theory, embodied cognition theory and cognitive linguistics, also with purpose to make other members of the group familiar with basic notions of these theories. The second part is dedicated to practical methods of linguistic analysis, namely syntactic-semantic methods of the meaning analysis.

We are grateful to the directors of LAP for agreeing this workshop to be a part of the conference, as aims of LAP and FORMALS greatly overlap.

On behalf of the FORMALS project research group,

Tin Perkov

Mathematical model for notion of compromise in social choice theory

Aleksandar Hatzivelkos

University of Applied Sciences Velika Gorica, Croatia

Keywords:

social choice, Borda cound, plurality count, compromise

Social choice decision aggregation is a form of complex system modeling which is based upon voters rankings over some set of candidates. Different social choice functions, such as Borda count, plurality count or Condorcet methods model different aspects of social choice decision criteria. One of such criteria that was not fully described or modeled, is a notion of compromise. This paper aims to define a measure which would capture notion of compromise on a given profile of voter preferences, about certain candidate being appointed to the certain position by some social welfare function. The goal is to define what compromise should mean, and proposes so called "d-measure of divergence" as a measure of divergence for some candidate to be positioned to certain position.

Basis of this paper is the mathematical description of the notion of compromise. The need to formally determine how we should interpret the notion of compromise comes from the following example. Let there be an election in which one hundred voters should choose between three candidates: A, B and C. Each voter places the vote by ordering those candidates. That ordering we will call a *preference*, and denote it α_i. Set of all preferences for those hundred voters, a *profile* α is given in Table, where fifty one voters have preference $A \succ B \succ C$, while forty nine voters have preference $C \succ B \succ A$.

51	49
A	C
B	B
C	A

In the core of the notion of compromise lays a need to "punish" or discourage larger distances; this means that when we are looking for a way to describe compromise about a candidate being placed at the winning position, each position should contribute to a sum (of distances) with more than its linear contribution. Therefore, we will take a look at a sum of *weighted* distances, that is, distances to the power of d, d being a real number greater than 1.

We will introduce notion $\beta_j^d(M_i)$ for some candidate M_i, which we will call *a d-measure of divergence from the j-th position.* The idea is that smaller value

of $\beta_j^d(M_i)$ captures notion of the greater level of compromise on a given profile for a candidate to be placed on a j-th place of linear ordering.

Definition. *Let $M = \{M_1, ..., M_m\}$ be set of m candidates, and let $\alpha \in \mathcal{L}(M)^n$ be a profile of n voters over those candidates. We define* a d-measure of divergence from a j-th position *for a candidate M_k, $\beta_j^d(M_k)$, as a $\beta_j^d(M_k) = \sum_{i=1}^{n} \left|\alpha_i^k - j\right|^d$, where α_i^k stands for a position of the candidate M_k in a preference of i-th voter, α_i, and for some real value $d > 1$.*

Given this definition, it is only natural to gather $\beta_j^d(M_k)$ values in a form of a matrix; in j-th column of a matrix M^d we have d-measures of divergence from j-th position for all candidates, while in i-th row of matrix M^d, we have d-measures of divergence from all positions for a candidate M_i.

If we interpret d-measure of divergence from the first position as a measure of compromise for a social choice function winner selection, we can compare results of classical social choice functions. For instance, Borda count is usually considered as a social choice function that emphasizes compromise candidate as a winner, especially when compared to the plurality winner. Does this thesis hold if we use d-measure of divergence from the first position as a measure for selection of the compromise candidate for the winner? Such analysis leads to the following result.

Theorem. *Let α be a profile over the set of candidates $M = \{A, B, C\}$. Let W_{BC} stands for a unique Borda count winner candidate and W_{PC} for a unique plurality winner candidate (if there are such) over some profile α. For every $d > 1$ we have $\beta_1^d(W_{BC}) \leq \beta_1^d(W_{PC})$. Equality holds iff $W_{BC} = W_{PC}$.*

A combinatorial proof of this theorem is given in [1]. Although there are six different preferences over the set of three candidates, number of all possible combinations of preferences that can form a profile can be reduced using Saari technique of removing maximal symmetric sets of preferences from a profile α. On the other hand, similar conclusion cannot be made for profiles over larger sets of candidates (four or more). We can prove that in case with four or more candidates, for every value of d, there is a profile such that Borda winner has greater value of d-measure of divergence from the first position when compared to plurality winner.

d-Measure of divergence enables new approach to the construction of social choice and social welfare functions. Simplest, and the most natural way to use information about d-measure of divergence, is to address a d-measure of divergence from the first position. In most cases, it is only important who is the winner on a given profile. Therefore, we can define social welfare function, SdM ("Simple d-Measure") based only upon d-measure of divergence from the first position, i.e. values in the first column of the d-measure of divergence matrix, M^d. Analysis of SdM leads to following result:

Theorem. *For all $d > 1$, social choice function SdM is a positional score function over a set of m candidates.*

Proof of this theorem comes from Young characterisation of positional score functions, as it can be proven that SdM satisfies anonymity, neutrality, reinforcement and continuity. Another approach to utilization of d-measure of divergence matrix M^d is using greedy approach: first place in linear order we will assign to the candidate with smallest d-measure of divergence from the first position, second place we will assign to the candidate with smallest d-measure

of divergence from the second position (from the set of remaining candidates, of course), and so on. Although algorithm sounds reasonable, it can produce strange results, since social welfare function defined in such way is not Pareto efficient.

Finally, we can use approach which (in a sense) totally minimizes sum of d-measure divergences, by finding the permutation (ordering) of candidates, such that total sum of d-measure divergences from a position in a given permutation of a given candidate is minimal. This function provides an interesting area of research. So far it was proven that TdM function is well behaved asymptotically (a version of continuity), and that it is not positively responsive.

Acknowledgments: This work has been supported in part by Croatian Science Foundation under the project UIP-05-2017-921 and by the University of Applied Sciences Velika Gorica.

References

[1] Hatzivelkos A.: *The Mathematical Look at a Notion of the Compromise and Its Ramifications*, Interdisciplinary Description of Complex Systems (2018) Vol. 16: No. 3

[2] Hatzivelkos A.: *Borda and pluralitycomparison with regard to compromise as a Sorites paradox*, Proceedings of the Central European Conference on Information and Intelligent Systems (2017) pp. 301–308

[3] Saari, D. G., "*Geometry of Voting*", Springler-Verlag, New York (1994)

[4] Young, H. P. *"Social Choice Scoring Functions"*, SIAM Journal on Applied Mathematics, Vol. 28, No. 4 , pp 824-838 (1975)

On geometric aspects of multiple conclusion natural deductions

Marcel Maretić*

University of Zagreb

Multiple conclusion deductions were proposed by Kneale [2] to address the lack of classical symmetries in Gentzen's NK calculus of natural deductions of classical logic. In this work we consider a number of geometrical (graphical) aspects of multiple conclusion deductions (MCD) defined as bipartite directed acyclic graphs (DAG) in [3]. Namely, we primarily investigate the graphical (graph-theoretical) perspective on the decompositions, transformations, orientation, symmetries, "analiticity" and normality of MCD proofs.

MCD proofs are also analyzed and compared next to well-established calculi (sequent systems, resolution-based proofs and tableaux) with respect to the desiderata of simplicity and accessibility to humans of a "good and practical deductive system" (according to [1, 4]).

References

[1] A. Indrzejczak, *Natural Deduction, Hybrid Systems and Modal Logics,* vol. 30 of *Trends in Logic*, Springer, 2010.

[2] W. Kneale, M. Kneale, *Development of Logic*, Clarendon Press, 1956, pp. 538–548.

[3] M. Maretić, *On Multiple Conclusion Deductions in Classical Logic*, Mathematical Communications 23 (1), 79-95, 2018.

[4] F. Poggiolesi, *Gentzen Calculi for Modal Propositional Logic*, Springer Netherlands, 2010.

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

Complexity of the interpretability logic IL

Luka Mikec*[1], Fedor Pakhomov[2] and Mladen Vuković[1]

[1]Department of Mathematics, Faculty of Science, University of Zagreb, Croatia
[2]Steklov Mathematical Institute of Russian Academy of Sciences, Moscow, Russia

Keywords:

interpretability logic, Veltman semantics, decidability, complexity, PSPACE

This talk is based on the paper [MPV18]. Computational complexity of modal logics was first studied by Ladner [Lad77]. Various tableau–based methods were used in proofs of PSPACE–decidability of a number of modal logics (like **K**, **K4**, **S4** etc; see [Lad77] and [Spa93]). PSPACE–completeness of the satisfiability problem (and also of the decision problem, since co-PSPACE = PSPACE) for the closed fragments of modal systems **K4**, **S4**, **Grz** and **GL** is proved by Chagrov and Rybakov [CR03]. Shapirovsky [Sha10] proved the PSPACE–decidability of propositional polymodal provability logic **GLP**. PSPACE–completeness of the closed fragment of the system **GLP** is proved by Pakhomov in [Pak14].

The interpretability logic **IL**, introduced by Visser [Vis90], is an extension of provability logic with a binary modal operator $\triangleright$. This operator stands for interpretability, considered as a relation between extensions of a fixed theory. Bou and Joosten proved in [BJ11] that the decidability problem for the closed fragment of **IL** is PSPACE–hard.

We consider the complexity problem for interpretability logic and prove that the system **IL** is PSPACE–complete. Our constructions can be seen as generalizations of the constructions by Boolos presented in [Boo96] (Chapter 10). If we restrict our work to **GL**, the resulting method is very similiar to the one given by Boolos, up to the terminology. Our method can also be seen as extending the method presented in [Sha10], of proving PSPACE–completeness (monomodal case), and has similarities with the proofs od completeness in [GJ08] and [GJ11].

We will comment on extending this approach to other interpretability logics.

*Supported by Croatian Science Foundation (HRZZ) under the project UIP-05-2017-9219.

References

[MPV18] L. Mikec, F. Pakhomov, M. Vuković. *Complexity of the interpretability logic IL*, Logic Journal of the IGPL (issue not yet assigned) https://doi.org/10.1093/jigpal/jzy015.

[Boo96] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1996.

[BJ11] F. Bou, J. Joosten. The closed fragment of **IL** is PSPACE–hard. Electronic Notes in Theoretical Computer Science, **278** (2011), 47–54

[CR03] A. V. Chagrov, M. N. Rybakov. How Many Variables Does Need to Prove PSPACE–hardness of Modal Logics?. In *Advances in Modal Logic* **4**, P. Balbiani et al. eds., King's College Publications, 2003, 71–82.

[GJ08] E. Goris, J. J. Joosten. Modal matters in interpretability logics. *Logic Journal of the IGPL*, **16** (2008), 371–412.

[GJ11] E. Goris, J. J. Joosten. A new principle in the interpretability logic of all reasonable arithmetical theories. *Logic Journal of the IGPL*, **19** (2011), 1–17.

[Lad77] R. Ladner. The computational complexity of provability in systems of modal propositional logic. SIAM Journal of Computing, **6** (1977), 467–480.

[Pak14] F. Pakhomov. On the complexity of the closed fragment of Japaridze's provability logic. *Archive for Mathematical Logic*, **53** (2014), 949–967.

[Sha10] I. Shapirovsky. PSPACE–decidability of Japaridze's polymodal logic. In *Advances in Modal Logic* **7**, L. Beklemishev, V. Goranko, V. Shehtman, eds., College Publications, 2010, 289–304

[Spa93] E. Spaan. Complexity of modal logics. PhD thesis, University of Amsterdam, 1993.

[Vis90] A. Visser. Interpretability logic. In *Mathematical Logic, Proceedings of the 1988 Heyting Conference*, P. P. Petkov. ed., pp. 175–210. Plenum Press, 1990.

Towards the formal verification of Industry 4.0 applications

Vivek Nigam[1] and Carolyn Talcott[2]

[1]fortiss GmbH, Munich, Germany & Federal University of Paraíba, João Pessoa, Brazil
[2]SRI International, Menlo Park, USA

Industry 4.0 is the new generation of manufacturing where factory stations can collaborate by communicating using the Internet backbone. This allows for new features, such as using the power of the cloud to reduce costs and accelerate production. However, new security concerns result from the greater attack surface due to the fact that devices are now connected to the Internet and hence, to the world. Formal methods have been successful in helping identify security flaws in, for example, criptographic protocols. In this talk, we describe our initial steps towards the formal verification of Industry 4.0 applications for security flaws. In particular, we model in Maude applications specified using the 4diac framework implementing IEC 61499, a domain model specific modeling language for industrial control solutions. We propose different intruder models, depending on the level of abstraction of the scenario as well as defenses that could be used in applications against possible attacks.

Corpus-based approach to the extraction of the emotional concepts and their ontological relations using the natural language logic operators

Benedikt Perak[1] and Tajana Ban Kirigin[2]

[1]Faculty of Humanities and Social Sciences, University of Rijeka
[2]University of Rijeka, Department of Mathematics

The paper deals with the identification, extraction and cross-linguistic comparison of the emotion concepts and their relationship with other material, psychological and socio-cultural concepts. What are the salient semantic domains and conceptual structures of the linguistic construals that are used to express emotions as entities (nouns), processes (verbs) and properties (adjectives, adverbs) in the communication? The methodology of this ontological corpus-based study includes three phases. The first phase deals with the construction of the Ontological Model of Concepts and Linguistic Constructions database that aims to formalize the meta-data about the ontological features of the psychological concepts and their relation with material and socio-cultural concepts. The ontological model is theoretically grounded in the system theory (Emmeche et al. 1997, Baas & Emmeche 1997, El-Hani & Emmeche 2000, Searle 2006, Capra & Luisi 2014), and cognitive approaches to the categorization (Rosch 2005). The ontological model is stored in a graph property database Neo4j (https://neo4j.com/). The second phase includes the extraction of the nominal, adjectival and processual lexical concepts related to the psychological phenomena from the large corpuses of Croatian (hrWaC 2.2) and English (enTenTen13) using the SketchEngine API and UDPipe (http://ufal.mff.cuni.cz/udpipe) tokenizer and parser. The psychological domains are extracted using the syntactic methods of paradigmatic similarity score for the co-occurrences in the coordinated construction [x and y] for nominal lexemes Sketchengine platform (https://the.sketchengine.co.uk) that function as a detector of entities connected with logical operators. Using graph algorithms for community detection the lexemes in the coordinated linguistic constructions are classified for their syntactic-semantic domains.

The third phase examines the ontological status of the lexemes and superimposes logical inferences on the semantic-syntactic constructional relations of the language specific knowledge.

This empirical approach sets the dynamic systems theory as the epistemological basis for studying ontological questions of the syntactic-semantic relations

expressed in language, its metaphoricity, dynamic network relationships, nonlinearity, emergence, complexity, hierarchy, ontological contingency and congruence of the conceptual organization of psychological concepts (Larsen-Freeman 2015).

Acknowledgment

Perak and Ban Kirigin are supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219.

References

[1] Emmeche, C., Køppe, S., Stjernfelt, F., *Explaining Emergence: Towards an Ontology of Levels*, Journal for general philosophy of science, 28(1), 83-117, 1997.

[2] Baas, N. A., Emmeche, C., *On Emergence and Explanation*, Intellectica, 25(2), 67-83, 1997.

[3] Capra, F., Luisi, P. L., *The Systems View of Life: A Unifying Vision*, Cambridge University Press, 2014.

[4] Larsen-Freeman, D., *Ten "Lessons" from Complex Dynamic Systems Theory: What is on Offer*, Motivational dynamics in language learning, 11-19, 2015.

[5] Rosch, E., *Principles of Categorization*, Etnolingwistyka. Problemy języka i kultury, (17), 11-35, 2005.

Formalizations of social choice theory in modal logic

Tin Perkov*

University of Zagreb

Social choice theory is about aggregating a collective choice from given individual choices. It includes a study of strategic behavior in this context, such as declaring an insincere choice so that the outcome of aggregation becomes more preferable. Computational aspects of social choice theory include issues of decidability and complexity of e.g. computing winner of an election under a given voting rule, or regarding strategic issues, of computing a possibility to manipulate an election. To contribute to computational study of social choice, various logical formalizations are developed to reason about problems of social choice theory. This talk is a survey of some such formalizations, namely (some of) those which use modal logic.

The following three logical systems for social choice will be overviewed:

- modal logic of judgment aggregation (i.e. aggregating collective judgment from individual judgments in more general context then elections, e.g. court jury or some board decision making) in Hilbert-style [1] and a natural deduction system for the same logic [4], in particular useful to formalize social welfare functions, voting rules which produce collective preference of candidates from individual preferences
- modal logic of social choice functions [5] which formalize social choice functions, rules which just produce winners from individual judgments, instead of entire collective preference, but still expressive enough to formally prove classical theorems of social choice theory, as demonstrated in [3]
- logic of knowledge and voting [2], a recent attempt of developing a more general language, able to express some strategic aspects of voting, in particular an ability to manipulate having only uncertain or incomplete information.

References

[1] T. Ågotnes, W. van der Hoek, M. Wooldridge: On the logic of preference and judgment aggregation, *Journal of Autonomous Agents and Multi-Agent Systems* 22 (2011) 4–30.

*Supported by Croatian Science Foundation (HRZZ) under the project UIP-05-2017-9219.

[2] Z. Bakhtiarinoodeh: *The Dynamics of Incomplete and Inconsistent Information: Applications of Logic, Algebra and Coalgebra*, PhD thesis, University of Lorraine, Nancy, 2017.

[3] G. Cinà, U. Endriss: Proving classical theorems of social choice theory in modal logic, *Journal of Autonomous Agents and Multi-Agent Systems* 30 (2016) 963–989.

[4] T. Perkov: Natural deduction for modal logic of judgment aggregation, *Journal of Logic, Language and Information* 25 (2016) 335–354.

[5] N. Troquard, W. van der Hoek, M. Wooldridge: Reasoning about social choice functions, *Journal of Philosophical Logic* 40 (2011) 473–498.

Propositional and first order logic formalizations of social welfare functions

Branimir Stojanović*

University of Zagreb, Croatia

Keywords:

First-order logic, social welfare functions, Arrow's Theorem

A concern of social choice theory are voting rules such as *plurality rule*, *Condorcet method* and *Borda rule*. They aggregate individual preferences into a collective preference.

Mathematical models for such rules is based on a set of individuals ($\mathcal{N}$) and a set of alternatives ($\mathcal{X}$), an individual preference is represented by a linear ordering on $\mathcal{X}$ and a voting rule is represented by a social welfare function (SWF), defined as:

$\omega : \mathcal{L}(\mathcal{X})^{\mathcal{N}} \to \mathcal{L}(\mathcal{X})$, where $\mathcal{L}(\mathcal{X})$ denotes the set of linear orders on $\mathcal{X}$.

An element of $\mathcal{L}(\mathcal{X})^{\mathcal{N}}$ is called a *preference profile*.

If we want to understand what Arrow's Theorem is about we have to study the following three properties of SWFs: *unanimity* (**UN**), *independence of irrelevant alternatives* (**IIA**) and *non-dictatorship* (**ND**).

Arrow's Theorem. *If $\mathcal{X}$ and $\mathcal{N}$ are finite and non-empty, and if $|\mathcal{X}| \geq 3$, then there exists no SWF for $\mathcal{X}$ and $\mathcal{N}$ that satisfies **UN**, **IIA** and **ND**.*

In this talk, formalizations of SWFs in first-order logic developed by Grandi and Endriss [1], and in classical propositional logic (Tang and Lin [2]) will be presented.

At the first glance, a first-order formalization has a problem with quantification over all possible linear orders (the set of preference profiles) because this corresponds to a second-order quantification. As a workaround to this problem, so-called situations are introduced to serve as names for different preference profiles. Then the signature of a first-order theory consists of the following components:

1. three unary predicates to mark alternatives (A), individuals (I), and situations (S),

*Supported by Croatian Science Foundation (HRZZ) under the project UIP-05-2017-9219.

2. a predicate p of arity four: $p(z, x, y, u)$ indicates that individual z prefers x over y in situation u,

3. a ternary predicate ω that stands for SWF: $\omega(x, y, u)$ translates as x is collectively preferred to y under the preference profile associated with situation u.

There is an axiomatization over this signature which characterizes the class of SWFs. In this theory we can express Arrow's conditions. For example, unanimity is expressed by the formula

$$\forall u \forall x \forall y \left(S(u) \wedge A(x) \wedge A(y) \rightarrow \left[\left(\forall z \left(I(z) \rightarrow p(z, x, y, u)\right)\right) \rightarrow \omega(x, y, u)\right]\right).$$

In the second part of the talk we present a formalization in classical propositional logic, developed by Tang and Lin with the purpose to obtain a computer-aided proof of Arrow's Theorem. Their method uses two inductive lemmas to reduce the general statement to the base case of 3 alternatives and 2 individuals, and this case is then verified using a computer.

For the base case we can rewrite FOL representation in propositional logic. Predicates $p(z, x, y, u)$ and $\omega(x, y, u)$ become atomic propositions $p_{z,x,y,u}$ and $\omega_{x,y,u}$ respectively. Formulas with universal quantifications become conjuctions and those with existential quantifications become disjunctions. For example, the following formula express the unanimity:

$$\bigwedge_{\substack{i,j \in \{1,2,3\}, i \neq j \\ k \in \{1,\ldots,36\}}} \left(p_{z_1,x_i,x_j,u_k} \wedge p_{z_2,x_i,x_j,u_k} \rightarrow \omega_{x_i,x_j,u_k}\right)$$

References

[1] U. Grandi, U. Endriss: First-order logic formalisation of impossibility theorems in preference aggregation, *J. Phil. Log.*, 42(4), 595–618, 2013.

[2] P. Tang, F. Lin, Computer-aided proofs of Arrow's and other impossibility theorems, *Artificial Intelligence*, 173(11), 473–498, 2009.