3rd International Conference

Logic and Applications 2014 (LAP 2014)

September 22-26, 2014,
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 SANU, Belgrade

Arithmetical aspects of generalized power series

Darko Biljaković, University of Zagreb, Croatia
Mladen Vuković, University of Zagreb, Croatia

Rings and fields of generalized formal power series are known more than hundred years and they were used as a tool in many mathematical areas. In spite of that almost nothing was known about its algebraic properties. Only in 2000 Berarducci studied irreducible elements of the ring $\mathbf{k}((\mathbb{R}^{\leq 0}))$, where $\mathbf{k}$ is an ordered field. The existence of irreducibles in that ring has certain arithmetical aspect. Namely if the field $\mathbf{k}$ has an integral part Z, then the field $\mathbf{k}((G))$, where G is an ordered abelian group, has an integer part of the form $\mathbf{k}((\mathbb{R}^{\leq 0}) + Z$. Also if $\mathbf{k}$ is real closed then $\mathbf{k}((\mathbb{R}^{\leq 0}) + Z$ is a model a fragment of arithmetic called Open Induction model (OI). Generally OI does not imply the cofinality of irreducibles (or primes). Henceforth it is of some interest to investigate if there is a model of OI which posesses such property. Berarducci and Pitteloud results give an afirmative answer to such question. Pitteloud (2001) proved that some of the irreducible elements constructed by Berarducci are actually prime. Biljakovic, S. Kuhlmann, Kochetov (2006) showed that such irreducibles (primes) remain irreducible (primes) in wider rings $\mathbf{k}((G^{\leq 0}))$.

One of the necessary results of Berarducci is that the corresponding ring of germs $\mathbf{k}((\mathbb{R}^{\leq 0}))/J$ is integral, where J is an ideal of the ring generated by monomials with negative exponents. This was shown with a wide use of the theory of transfinite ordinals. In this paper, we give an algebraic proof of this result without any use of transfinite ordinals. Namely, we generalize the notion of germ and develop a difference calculus of generalized power series. The simple consequence is that $\mathbf{k}((\mathbb{R}^{\leq 0}))/J$ is entire. We hope that our method will be useful in a better understanding of generalized power series and its applications.

References

[1] A. BERARDUCCI, *Factorization in generalized power series*, Trans. Amer. Math. Soc., 352 (2000), 553–577

[2] A. BERARDUCCI, M. OTTERO, *A recursive nonstandard model of normal open induction*, Jou. Sym. Logic, 61 (1996), 1228–1241

[3] D. BILJAKOVIĆ, M. KOCHETOV, S. KUHLMANN, *Exponential Integer Parts of non–Archimedean Fields*, Paris 7 Logique, 76, Seminaire de structures algebraiques 2002–2003, ordonnees, (Avril 2004) 1-17

[4] D. BILJAKOVIĆ, M. KOCHETOV, S. KUHLMANN, *Primes and Irreducibles in Truncation Integer Parts of Real Closed Fields*, Proceedings of the Workshop and Conference in Logic, Algebra and Arithmetic, October 18-22, 2003, Lecture Notes in Logic 26, A. K. PetersLtd, Wellesley, Massachusetts, 2006.

[5] D. BILJAKOVIĆ, *Exponential models of open induction*, (in Croatian), PhD dissertation, Department of Mathematics, Faculty of Science, University of Zagreb, 2006.

[6] D. PITTELOUD, *Existence of prime elements in rings of generalized power series*, Jou. Sym. Logic, 66 (2001), 1206–1216

[7] D. PITTELOUD, *Algebraic properties of rings of generalized power series*, Ann. of Pure and Appl. Logic, 116 (2002), 39–66

[8] L. VAN DEN DRIES, A. MACINTYRE, D. MARKER, *Logarithmic–Exponential Power Series*, J. London Math. Soc. (2) 56 (1997), 417–434

Logics for probabilistic spatio-temporal reasoning

Dragan Doder, University of Luxembourg, Luxembourg
John Grant, University of Maryland,USA
Zoran Ognjanović, Mathematical Institute SANU, Serbia

Spatiotemporal databases can be used to efficiently store and retrieve information about objects moving in space and time. Probabilities are added to model the case where the locations are not known with certainty. A few years ago a new formalism was introduced to represent such information as atomic formulas. A PST (Probabilistic SpatioTemporal) atom has the form $loc(id, r, t)[\ell, u]$ and stands for the statement that a particular object id is in a particular region r at a particular time t with a probability that is in the probability interval $[\ell, u]$. A PST database is a set of PST atoms. Algorithms were developed, as described in [10] and [5], for the efficient processing of PST databases. A PST database supports only PST atoms. This is analogous to the case of relational databases that allow only atomic facts as tuples in relations. Hence a strictly relational database does not have the capability to state a disjunctive fact such as "Dragan works in Luxembourg or Belgrade" even though the two facts "Dragan works in Luxembourg" and "Dragan works in Belgrade" can be stated. Soon after the formalization of relational databases by E. F. Codd, in the 1970s people started to work on adding null values [3] and various types of incomplete information to the relational formalism [4]. In the 1980s the logical connectives were added to create disjunctive databases (and more generally, disjunctive logic programming) [7]. The starting point of our work was to do something similar for PST databases in a logical framework.

The situation is more complex for PST databases because a PST atom contains more information than an atomic fact in a relational database. Also, previous research in probabilistic databases ([6]) stressed the importance of combining probabilities in probabilistic databases. For instance, using the basic rules of probability, from the two PST atoms $loc(Bus1, Q, 5)[.8, 1]$, $loc(Bus2, R, 6)[.6, .9]$ the compound statement (not expressible in the atomic formalism of PST) $loc(Bus1, Q, 5)$ and $loc(Bus2, R, 6)[.4, 1]$ can be concluded. However, if we allow only the conjunction of PST atoms in the language, we cannot combine the nonprobabilistic portions and can write only the formula $loc(Bus1, Q, 5)[.8, 1]\ and\ loc(Bus2, R, 6)[.6, .9]$ in the expanded language. So there are different ways of combining formulas (even just for conjunction) and what is allowed needs to be defined formally.

We investigate various logics for extending the PST database concept. First we deal with the case where both atomic and probabilistic information can be combined in a general way. We found that the most useful way to accomplish this was by formulating two languages and combining them into a single logical probabilistic formalism. We also found interesting differences among the cases where the probability values (in $[0, 1]$) are all real numbers, all rational numbers, or a finite number of values. We investigate all these cases and obtain fundamental results about them. We mostly deal with propositional logics where the syntax contains atomic formulas and propositional connectives. The first-order version uses predicate symbols, quantifiers, and variables in the usual way. All of our logics extend the PST formalism but with different capabilities. For each logic we provide a formal syntax and semantics as well as a sound and complete axiomatization. We also discuss decidability issues. In addition, we relate these logics to previous axiomatizations of probabilistic logics. Those results are published in [1].

Finally, we discuss the possibility of enriching the logics by adding temporal operators to ST formulas. We pose the question how to combine the approach form [1] and

linear time logic [2, 11]. We also discuss the problem of axiomatizing the probabilistic extension of the ST framework with temporal operators, and the possibility of using the techniques from [8, 9].

Acknowledgements

This work was supported by the Serbian Ministry of Education and Science through projects ON174026 and III44006, and by the National Research Fund (FNR) of Luxembourg through project PRIMAT.

References

[1] D. Doder, J. Grant, Z. Ognjanović. Probabilistic logics for objects located in space and time. Journal of Logic and Computation, 23(3), 487–515, 2013.

[2] D. Gabbay, A. Pnueli, S. Shelah, J. Stavi. On the temporal analysis of fairness. Proc. 7th ACM symp. Princ. of Prog. Lang., 163 – 173, 1980.

[3] J. Grant. Null values in a relational data base. *Information Processing Letters*, 6:156-157. 1977.

[4] J. Grant. Incomplete information in a relational database. *Fundamenta Informaticae*, III 3:363-378. 1980.

[5] J. Grant, F. Parisi, A. Parker, and V.S. Subrahmanian. An agm-style belief revision mechanism for probabilistic spatio-temporal logics. *Artificial Intelligence*, 174:72-104, 2010.

[6] L. V. S. Lakshmanan, N. Leone, R. Ross, and V. S. Subrahmanian. Probview: a flexible probabilistic database system. *ACM Transactions on Database Systems*, 22:419–469. 1997.

[7] J. Lobo, J. Minker, and A. Rajasekar. Foundations of Disjunctive Logic Programming. The MIT Press, Cambridge, Massachusetts. 1992.

[8] Z. Ognjanović. Discrete linear-time probabilistic logics: completeness, decidability and complexity. J. Log. Comput. 16(2), pp 257–285, 2006.

[9] Z. Ognjanović, D. Doder, Z. Marković. A Branching Time Logic with Two Types of Probability Operators. In: SUM 2011, LNCS 6929, 219–232, 2011.

[10] A. Parker, V.S. Subrahmanian, and J. Grant. A logical formulation of probabilistic spatial databases. *IEEE Transactions on Knowledge and Data Engineering*, 19:1541-1556, 2007.

[11] A. Sistla and E. Clarke. The complexity of propositional linear temporal logic. *Journal of the ACM*, 32(3):733–749. 1985.

Display-type calculi[1]

Sabine Frittella, Aix Marseille University, France
Giuseppe Greco, Delft University of Technology, The Netherlands

Keywords: cut elimination, display calculi, multi-type sequent calculi, non-classical logics, modal logic, dynamic logics.

The range of non-classical logics has been rapidly expanding, driven by influences from other fields which have opened up new opportunities for applications. The logical formalisms which have been developed as a result of this interaction have attracted the interest of a wider research community than the logicians, and their theory has been intensively investigated, especially with respect to their semantics and computational complexity.

However, most of these logics lack a comparable proof-theoretic development. More often than not, the hurdles preventing a standard proof-theoretic development for these logics are due precisely to some of their defining features which make them suitable for applications, such as e.g. their not being closed under uniform substitution, or the fact that (the semantic interpretations of) key connectives are not adjoints.

These difficulties caused the existing proposals in literature to be often ad hoc, not easily generalisable, and more in general lacking a smooth proof-theoretic behaviour. In particular, the difficulty in smoothly transferring results from one logic to another is a problem in itself, since these logics typically come in large families (consider for instance the family of dynamic logics), and hence proof-theoretic approaches which uniformly apply to each logic in a given family are in high demand (for an expanded discussion of the existing proof systems for dynamic epistemic logics, see [5, section 3]).

The problem of the transfer of results, tools and methodologies has been addressed in the proof-theoretic literature for the families of substructural and modal logics, and has given rise to the development of several generalisations of Gentzen sequent calculi (such as hyper-, higher level-, display- or labelled-sequent calculi).

In this talk we focus on the core technical aspects of a proof-theoretic methodology and set-up closely linked to display logic [2] and basic logic [1]. Instances of this set-up have appeared in [5] and [6] to account for (non-classical versions of) Baltag-Moss-Solecki's dynamic epistemic logic. In ongoing work, this set-up is being applied to propositional dynamic logic [3], monotone modal logic [4], game logic, and linear logic.

The present set-up, which we refer to as *display-type calculi*, generalizes display calculi in two aspects: by allowing multi-type languages, and by dropping the full display property. The generalisation to a multi-type environment makes it possible to introduce specific tools enhancing expressivity, which have proved useful e.g. for a smooth proof-theoretic treatment of multi-modal and dynamic logics [6, 3]. The generalisation to a setting in which full display property is not required makes it possible to account for logics which admit connectives which are neither adjoints nor residuals [4].

One technical aspect which guarantees the cut elimination meta-theorem to go through for display-type calculi, even in the absence of the full display property, concerns the strengthening of the *separation* property (requiring principal formulas in introduction rules to appear in isolation) to the *visibility* property. Visibility requires *all*

[1] Joint work with: Alexander Kurz, Alessandra Palmigiano, Vlasta Sikimić.

active formulas in introduction rules to occur in isolation. This property was recognized to be crucial for the cut elimination theorem of basic logic [1].

However, in the present set-up of display-type calculi, visibility is also weakened, in the sense that, in order to account for logics that are not closed under uniform substitution [5, 6], principal formulas in axioms are not required to occur in isolation.

In the proposed talk, we will illustrate the basic principles of the multi-type environment, and also how the above combination of weakenings, strengthenings of the separation property concurs to guaranteeing the cut elimination meta-theorem for display-type calculi.

Time permitting, we will also discuss some difficulties that still arise in the case of PDL and some ideas towards treating predicative logics.

References

[1] G. Battilotti, C. Faggian, G. Sambin, *Basic logic: Reflection, Symmetry, Visibility*, Journal of Symbolic Logic 65 (2000).

[2] N. Belnap, *Display logic*, J. of Philosophical Logic 11, pp. 375-417 (1982).

[3] S. Frittella, A. Kurz, A. Palmigiano, *Multi-type Display Calculus for Propositional Dynamic Logic*, JLC - Special Issue on Substructural Logic and Information Dynamics, forthcoming (2014).

[4] S. Frittella, G. Greco, *Display-type Sequent Calculus For Monotone Modal Logic*, Advances in Modal Logic 2014, short presentation (2014).

[5] S. Frittella, G. Greco, A. Kurz, A. Palmigiano, and V. Sikimić, *A Proof-theoretic Semantic Analysis Of Dynamic Epistemic Logic*, JLC - Special Issue on Substructural Logic and Information Dynamics, forthcoming (2014).

[6] S. Frittella, G. Greco, A. Kurz, A. Palmigiano, and V. Sikimić, *Multi-type Display Calculus For Dynamic Epistemic Logic*, JLC - Special Issue on Substructural Logic and Information Dynamics, forthcoming (2014).

[7] R. Goré, *Substructural Logics On Display*, Logic J. of IGPL 6, pp. 451-504 (1998).

[8] H. Wansing, *Sequent Systems For Modal Logics*, Handbook of Philosophical Logic 8, pp. 61-145 (2002).

Lambek's computational approach to conjugation

Silvia Ghilezan[2], **Faculty of Technical Sciences, University of Novi Sad, Serbia**

"For more than 60 years, Jim Lambek has been a profoundly inspirational mathematician, with groundbreaking contributions to algebra, category theory, linguistics, theoretical physics, logic and proof theory... Jim Lambek's ideas keep inspiring upcoming generations of scholars." (Festschrift on the occasion of Lambek's 90th birthday [3])

This is an overview of the work of Joackim, Jim, Lambek on formal grammars for verb conjugation in several languages English, French, Latin, Turkish, Arabic, Hebrew and partly Serbian and Croatian. We will focus on his early work ([8, 9]), which has been further developed and extended by Lambek and his co-authors to Turkish, Arabic and (Biblical) Hebrew ([1, 2, 11]). Lambek's approach was applied to Serbian and Croatian in [6] and to Japanese in [4].

The Latin verb has $3 \times 5 \times 6 = 90$ finite conjugational forms (inflected forms) corresponding to three patterns, five (simple) tenses and six persons. The production grammar given in Lambek [9] associates three matrices (patterns) of the Latin verb (present-active, perfect-active, present-passive) with 30 inflected forms (5 simple tenses $\times$ 6 persons).

The French verb has $7 \times 6 = 42$ finite conjugational forms (inflected forms) corresponding to seven (simple) tenses and six persons. A production grammar of the French verb which generates the 42 inflected forms is presented in Lambek [8]. In Biblic Hebrew each verb has $7 \times 2 \times 10 = 140$ finite conjugational forms corresponding to seven patterns, two tenses and ten persons. A production grammar that generates 140 inflected forms of the Biblic Hebrew verb is given in [11]. The Serbian and Croatian verb has $4 \times 6 = 24$ conjugational forms corresponding to four simple tenses and six person-numbers. there are two patterns, however they conjugate in the same way. As verb may also, as in Latin, be regarded as one-word sentences. A production grammar of Spanish presenting 54 forms of the Spanish verb is given in Mel'čuk [12]. A study of Russian conjugation is given in Jakobson [7].

Language	Inflected forms	Patterns	Simple tenses $\times$ Persons
Latin	90	3	5×6
French	42	1	7×6
Serbian	24	1	4×6
Hebrew B	140	7	2×10
Spanish	54		

Lambek's production grammar is a simple computational method for generating these conjugational forms step by step. The mathematical structure involved is the *finitely generated partially ordered semi-group*, also called "*semi-Thue system*" in mathematics, "*rewriting system*" in computer science and "*production grammar*" or Chomsky's Type zero language ([5]) in linguistics.

With each verb V, there is associated a $p \times n \times m$ matrix of conjugational verb-forms, $C^k_{ij}(V)$. The index $i = 1, ...n$ represents the (simple) tense, and the index $j = 1, ..., m$ represents the person-number and the index $k = 1, ..., p$ represents the

[2]Partially supported by the Serbian Ministry of Education and Science through projects ON174026 and III44006.

pattern. We shall only consider simple tenses here, and shall disregard participles and compound tenses. A production grammar, in general, provides a method for calculating $C_{ij}^k(V)$ for a given (i, j, k, V).

We shall present a simple production grammar developed in [6] for generating these 24 verb forms of Serbian and Croatian verb. This work was supported by the Social Sciences and Humanities Research council of Canada within a project on Mathematical Linguistics led by Jim Lambek during the spring of 1993 at McGill University, Montréal.

References

[1] D. Bargelli, J. Lambek, A Computational View of Turkish Conjugation Linguistic Analysis 29:248–256 (1999).

[2] D. Bargelli, J. Lambek, A Computational Approach to Arabic Conjugation Linguistic Analysis 30:1-22 (2001/2002).

[3] C. Casadio, B. Coecke, M. Moortgat, P. Scott, P. (Eds.) Categories and Types in Logic, Language, and Physics Essays dedicated to Jim Lambek on the Occasion of his 90th Birthday. Lecture Notes in Computer Science 8222 Subseries: Theoretical Computer Science and General Issues (2014).

[4] Kumi Cardinal An algebraic study of Japanese grammar PhD thesis, McGill University (2002).

[5] N. Chomsky, Syntactic structures. The Hague: Mouton. (1957).

[6] S. Ghilezan, Conjugation in SerboCroatian. Linguistic Analysis 24:142–150 (1994).

[7] R. Jakobson, Russian conjugation. In Selected writings II pp. 120–129, The Hague: Mouton. (1971).

[8] J. Lambek, A mathematician looks and French conjugation. Theoretical Linguistics 2:203–214 (1975).

[9] J. Lambek, A mathematician looks and Latin conjugation. Theoretical Linguistics 2/3:221–234 (1979).

[10] J. Lambek, Production grammars, revisited. Linguistic Analysis 23:205–225 (1993).

[11] J. Lambek, Yanofsky, A computational approach to Biblical Hebrew conjugation. Linguistic Analysis 23:205–225 (1996).

[12] I. A. Mel'čuk, A model of Spanish conjugation. In Das Wort, International library of general linguistics 9:210–257 (1976).

Injectivity of relational semantics for (connected) MELL proof-nets via Taylor expansion

Giulio Guerrieri, Université Paris Diderot, France
Lorenzo Tortora de Falco, Università Roma Tre, Italy
Luc Pellissier, Université Paris Nord, France

Abstract

We show that: (1) the Taylor expansion of a cut-free MELL proof-structure R with atomic axioms is the (most informative part of the) relational semantics of R; (2) every (connected) MELL proof-net is uniquely determined by the element of order 2 of its Taylor expansion; (3) the relational semantics is injective for (connected) MELL proof-nets.

1 Introduction

Starting from investigations on denotational semantics of System F (second order typed λ-calculus), in 1987 Girard [7] introduced linear logic (LL), a refinement of intuitionistic logic. He defines two new modalities, ! and ?, giving a logical status to structural rules and allowing to distinguish between linear resources (i.e. usable exactly once during the cut-elimination process) and resources available at will. One of the main features of LL is the possibility of representing proofs (and λ-terms) geometrically by means of particular graphs: *proof-structures*. Among proof-structures it is possible to characterize "in a geometric way" the ones corresponding to proofs in LL sequent calculus through the Danos-Regnier correctness criterion (see [2] but also [9, Def. A.6 and Rmk. A.7] for the definition in a more general case): a proof-structure corresponds to a proof in LL sequent calculus if and only if it is a *proof-net*, i.e. it fulfills some conditions about acyclicity and connectedness (ACC).

Ehrhard [3] introduced finiteness spaces, a denotational model of LL (and λ-calculus) which interprets formulas by topological vector spaces and proofs by analytical functions: in this model the operations of differentiation and Taylor expansion make sense. Ehrhard and Regnier [4, 5, 6] internalized these operations in the syntax and thus introduced differential linear logic DiLL_0 (and differential λ-calculus), where the promotion rule (the only one in LL which is responsible for introducing the !-modality and hence creating resources available at will) is replaced by three "finitary" rules which are perfectly symmetric to the rules for the ?-modality: this allows a more subtle analysis of the resources consumption during the cut-elimination process. At the syntactic level, *Taylor expansion* decomposes a LL proof-structure in a (infinite in general) formal sum of DiLL_0 proof-structures (*diffnets*), each of which contains resources usable only a fixed number of times.

Our contribution aims at looking further into the relationship between Taylor expansion and *relational model* (a well-known and simple denotational semantics of LL and λ-calculus: it interprets LL proof-structures as morphisms in the category of sets and relations). More precisely:

1. We show that, given a *normal* (i.e. cut-free with atomic axioms) proof-structure R of MELL (the multiplicative-exponential fragment of LL, sufficiently expressive to encode the λ-calculus), each element of the Taylor expansion of R can be identified with one and only one element of the set of injective points of the interpretation of R in the relational model, quotiented by the equivalence relation

induced by atoms renaming. This does not hold if π contains cuts, consistently with the idea that the Taylor expansion of a MELL proof-structure can be seen as an object between syntax and semantics (while denotational semantics is invariant under cut-elimination).

2. We show that every MELL proof-structure (no matter with or without cuts) fulfilling the ACC condition (or the more general connectedness condition) is uniquely determined by the element of order 2 of its Taylor expansion. Comparing (intuitively) to mathematical analysis, this would correspond to saying that analytical functions fulfilling some condition are uniquely determined by their second derivatives. In order to obtain this result, we adapt to the DiLL_0 framework some well-known tools of the theory of LL proof-nets (in particular a generalization of the notion of empire, see [7]).

3. As a corollary of points 1 and 2, we show that the relational model is injective with respect to MELL proof-nets: given two ACC (or, more generally, connected) normal MELL proof-structures, if they have the same relational interpretation then they are identical. A similar result has already been conjectured in [9] and proven in [1] but following a completely different (and more complicated) approach.

This study also pushes towards a deeper understanding of the Taylor expansion of MELL proof-structures as a bridge between syntax and semantics (fitting the general perspective of abolishing the old traditional distinction between syntax and semantics), which should lead to a more abstract and synthetic representation of this operation (see also [8]).

This work has already been presented at the workshop Termgraph 2014 (`http://cl-informatik.uibk.ac.at/events/termgraph-2014/`) on July 13th, 2014, as part of Vienna Summer of Logic 2014.

References

[1] Daniel de Carvalho, Lorenzo Tortora de Falco: The relational model is injective for Multiplicative Exponential Linear Logic (without weakenings). Annals of Pure and Applied Logic 163(9), pp. 1210–1236 (2012).

[2] Vincent Danos, Laurent Regnier: The structure of multiplicatives. Archive for Mathematical logic 28(3), pp. 181–203 (1989).

[3] Thomas Ehrhard: Finiteness spaces. Mathematical Structures in Computer Science 15(04), pp. 615–646 (2005).

[4] Thomas Ehrhard, Laurent Regnier: The differential lambda-calculus. Theoretical Computer Science 309(1-3), pp. 1–41 (2003).

[5] Thomas Ehrhard, Laurent Regnier: Differential interaction nets. Theoretical Computer Science 364(2), pp. 166–195 (2006).

[6] Thomas Ehrhard, Laurent Regnier: Uniformity and the Taylor expansion of ordinary lambda-terms. Theoretical Computer Science 403(2-3), pp. 347–372 (2008).

[7] Jean-Yves Girard: Linear logic. Theoretical Computer Science 50(1), pp. 1–102 (1987).

[8] Giulio Guerrieri, Lorenzo Tortora de Falco: A new point of view on the Taylor expansion of proof-nets and uniformity. Technical Report, accepted for presentation at the workshop Linearity 2014. Available at http://www.pps.univ-paris-diderot.fr/ giuliog/prototaylor.pdf (2014).

[9] Lorenzo Tortora de Falco: Obsessional Experiments For Linear Logic Proof-Nets. Mathematical Structures in Computer Science 13(6), pp. 799–855 (2003).

Approaching substructural term calculi via the resource control calculus

Jelena Ivetić, University of Novi Sad, Serbia
Silvia Ghilezan, University of Novi Sad, Serbia
Pierre Lescanne, University of Lyon, France
Silvia Likavec, University of Torino, Italy

In this talk, we propose a new way to obtain a computational interpretation of some substructural logics, starting from an intuitionistic term calculus with explicit control of resources.

Substructural logics [1] are a wide family of logics obtained by restricting or rejecting some of Gentzen's structural rules, such as thinning, contraction and exchange. The most well known substructural logic is the linear logic of Girard [3], in which, due to the absence of contraction and weakening, each formula appears exactly once in the theorem. The other well known substructural logics are the relevant logic (the one without thinning), the affine logic (without contraction) and the Lambek calculus (without all three mentioned structural rules).

From the computational point of view, structural rules of thinning and contraction are closely related to the control of available resources (i.e. term variables). More precisely, contraction corresponds to the duplication of the variable that is supposed to be used twice in a term, whereas weakening corresponds to the erasure of an useless variable. These concepts were implemented into several extensions of the lambda calculus [2, 4, 5, 6].

Here, we use the resource control lambda calculus $\lambda_{\circledR}$, proposed in [2], as a starting point for obtaining computational interpretations of implicative fragments of some substructural logics, namely relevant and affine logic. The corresponding formal calculi are obtained by syntactic restrictions, along with modifications of the reduction rules and the type assignment system.

The *pre-terms* of $\lambda_{\circledR}$ are given by the following abstract syntax:

$$\text{Pre-terms} \qquad f \quad ::= \quad x \mid \lambda x.f \mid ff \mid x \odot f \mid x <^{x_1}_{x_2} f$$

where x ranges over a denumerable set of term variables, $\lambda x.f$ is an *abstraction*, ff is an *application*, $x \odot f$ is a *thinning* and $x <^{x_1}_{x_2} f$ is a *contraction*. $\lambda_{\circledR}$-terms are derived from the set of pre-terms by inference rules, that informally specify that bound variables must actually appear in a term and that each variable occurs at most once. Operational semantics of $\lambda_{\circledR}$-calculus is defined by four groups of reduction rules and some equivalencies. The main computational step is the standard β reduction, executed by substitution defined as meta-operator. The group of (γ) reductions performs propagation of contraction into the term. Similarly, (ω) reductions extract thinning out of the terms. This discipline allows us to optimize the computation by delaying duplication of variables on the one hand, and by performing erasure of variables as soon as possible on the other. Finally, the rules in $(\gamma\omega)$ group explain the interaction between explicit resource operators that are of different nature.

The simple types are introduced to the $\lambda_{\circledR}$-calculus in the following figure.

In the obtained system $\lambda_{\circledR}$ $\rightarrow$, thinning is explicitly controlled by the choice of the axiom, while the control of the contraction is managed by implementing context-splitting style (i.e. requiring that Γ, Δ represents disjoint union of the two bases).

Modifications of the $\lambda_{\circledR}$ $\rightarrow$ system can provide the computational interpretation of some substructural logics, different from the usual approach via linear logic. For

$$\frac{}{x : A \vdash x : A}\ (Ax)$$

$$\frac{\Gamma, x : \alpha \vdash M : \beta}{\Gamma \vdash \lambda x.M : \alpha \to \beta}\ (\to_I) \qquad \frac{\Gamma \vdash M : \alpha \to \beta \quad \Delta \vdash N : \beta}{\Gamma, \Delta \vdash MN : \beta}\ (\to_E)$$

$$\frac{\Gamma, x : \alpha, y : \alpha \vdash M : \beta}{\Gamma, z : \alpha \vdash z <^x_y M : \beta}\ (Cont) \qquad \frac{\Gamma \vdash M : \beta}{\Gamma, x : \alpha \vdash x \odot M : \beta}\ (Thin)$$

instance, if one excludes the $(Thin)$ rule but preserves the axiom that controls the introduction of variables, the resulting system would correspond to the logic without thinning and with explicit control of contraction i.e. to the variant of implicative fragment of relevance logic. Similarly, if one excludes the $(Cont)$ rule, but preserves context-splitting style of the rest of the system, correspondence with the variant of the logic without contraction and with explicit control of thinning i.e. implicative fragment of affine logic is obtained. Naturally, these modifications also require certain restrictions on the syntactic level, changes in the definition of terms and modifications of operational semantics as well.

We also proposed intersection type assignment systems for both the $\lambda_{\circledR}$-calculus and its substructural restrictions, that enable the specification of the role of a variable in a term and therefore can be naturally connected with the resource control term calculi.

Although the proposed systems may be considered naive due to the fact that they only correspond to implicative fragments of relevant and affine logics and therefore are not able to treat characteristic split conjunction and disjunction connectives, they could be useful as a simple and neat logical foundation for the specific relevant and affine programming languages.

Acknowledgements: This work was partially supported by the Serbian Ministry of Education and Science through projects ON174026 and III44006.

References

[1] P.Schroeder-Heister and K.Došen: Substructural Logics. Oxford University Press (1993).

[2] S.Ghilezan, J.Ivetić, P.Lescanne and S.Likavec: Intersection types for the resource control lambda calculi. In A. Cerone and P. Pihlajasaari: *8th International Colloquium on Theoretical Aspects of Computing, ICTAC '11*, LNCS Vol. 6916, pages 116–134. Springer (2011).

[3] J-Y.Girard: Linear logic. Theoretical Computer Science, Vol. 50(1), pages 1–102, North Holland (1987).

[4] D.Kesner and S.Lengrand: Resource operators for lambda-calculus. In: *Information and Computation*, Vol. 205(4):419–473 (2007).

[5] P. Lescanne and D. Žunić: Classical proofs' essence and diagrammatic computation. In: *Proceedings of International Conference on Numerical Analysis and Applied Mathematics - ICNAAM 2011* AIP Conf. Proc., Vol. 1389, pages 792–797 (2011).

[6] V. van Oostrom: Net-calculus. Course notes, http://www.phil.uu.nl/ oostrom/ oudonderwijs/cmitt/00-01/net.ps (2001).

Time-Bounding Needham-Schroeder Public Key Exchange Protocol

Max Kanovich, Queen Mary, University of London, UK
Tajana Ban Kirigin, University of Rijeka, Croatia
Vivek Nigam, Federal University of Paraíba, João Pessoa, Brazil,
Andre Scedrov, University of Pennsylvania, USA

We consider some properties of timed models for protocol specification and verification and address the non-trivial relation between models with discrete time and models with continuous time. Although discrete time is suitable for some applications such as [7], it is just an abstraction of physical time. In other instances normal physical reality plays an essential role. This is the case with *cyber-physical security protocols* which take into account the physical properties of the environment where its protocol sessions are carried out. For instance, Distance Bounding Protocols such as [1] are cyber-physical security protocols which infer an upper bound on the distance between two agents from the round trip time of messages. The common feature in most cyber-physical security protocols is that they mention cryptographic keys, nonces and time.

We investigate the motivation and the need of using continuous time models in protocol verification instead of the more simple discrete ones and show that in protocol verification these models behave differently.

In our recent work [5, 6] we presented some first steps towards building general timed models for cyber-physical security protocols verification. We proposed a language based on multiset rewriting which extends the security protocols framework [2, 4] with continuous time. We also proposed a novel intruder model based on the Dolev-Yao [3] which takes into account the *physical properties* of the environment that the intruder is in. We then showed that the reachability problem for Bounded Memory Cyber-Physical Security Protocols in presence of a Memory Bounded Intruder is PSPACE-complete [5, 6].

We show that protocol verification models with discrete time behave differently when compared to models with continuous time. In particular, there are protocols for which no attack can be found when using a model with discrete time, but there is an attack when using a model with continuous time (or even dense time). This means that, in general, one has to be careful when using models with discrete time in protocol verification as such models may not able to expose some protocol security flaws that models with continuous time would show.

We illustrate the main subtleties by adding the dimension of time to the original flawed *Needham-Schroeder* public key protocol. We address the basic issues that arise in the formalization of protocols with explicit time, namely the time-sensitive features such as the *network delays* and *participants' processing time* are taken into account. Also, protocol execution depends on the round trip time of messages by means of *measuring the response time*.

The intriguing result is that this *Time-bounding Needham-Schroeder protocol* is *secure* in the discrete time model, while it is *insecure* in the continuous time model. We consider various scenario assumptions and show that the security properties of our Time-bounding Needham-Schroeder protocol depend on whether time is considered discrete or continuous as well as on network delay and internal processing time.

These results hold already with respect to an adversary which is able to intercept and send messages, as well as encrypt and decrypt messages providing he has the corresponding keys. Such an adversary does not need to manipulate various submessages

or even create fresh values. Here, as all the participants in the protocol execution, the adversary is subject to non-zero network delays and non-zero processing time.

The actual difference between discrete and continuous time models lays in the fact that inbetween two moments in time, an unbounded number of timed events are possible within continuous time, whereas only a finite number of acts could happen within discrete time model. In other words, discrete time models implicitly impose lower bounds on transmission and processing time. This is not the case in models with continuous time. Indeed, continuous time (or even dense time) allows us to not have such bounds. Nevertheless, lower bounds for delays for both processing time and for traversal time can be introduced in continuous time models. We investigate such scenarios as well, and show that there is a difference between the models even with lower bounds imposed.

In the future work we plan to consider extensions and alternative intruder and protocol models reflecting various technologies and *e.g.* scenarios with agents that are allowed to move. Another assumption of our model is that all agents share a global clock. Although this is reasonable for some applications, such as distance bounding protocols, it is not the case for others such as Network Time Protocols.

Finally, we point out that no rescaling of discrete time units removes the presented difference between the models. Namely, for any discretization of time, such as days, seconds or any other infinitesimal time unit, there is a protocol for which there is an attack with continuous time and no attack is possible in the discrete case. This novel result illustrates the challenges of timed models for cyber-physical security protocol verification.

Acknowledgments: Nigam is supported by the Brazilian Research Agency CNPq. Scedrov is supported in part by the AFOSR MURI "Science of Cyber Security: Modeling, Composition, and Measurement" as AFOSR Grant No. FA9550-11-1-0137. Additional support for Scedrov from NSF Grant CNS-0830949 and from ONR grant N00014-11-1-0555.
During the work on these results Kanovich and Scedrov were visiting the National Research University Higher School of Economics, Moscow. They would like to thank Sergei O. Kuznetsov for providing a very pleasant environment for work.

References

[1] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT*, 1993.

[2] I. Cervesato, N. A. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov. A meta-notation for protocol analysis. In *CSFW*, pages 55–69, 1999.

[3] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[4] N. A. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 12(2):247–311, 2004.

[5] M. I. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, C. L. Talcott, and R. Perovic. A rewriting framework for activities subject to regulations. In *RTA* 2012.

[6] M. Kanovich, T. B. Kirigin, V. Nigam, and A. Scedrov. Towards timed models for cyber-physical security protocols. In *FCS-FCC* 2014.

[7] V. Nigam, T. B. Kirigin, A. Scedrov, C. Talcott, M. Kanovich, and R. Perovic. Towards an automated assistant for clinical investigations. In *IHI* 2012.

The rationality of escalation an unexpected use of coinduction in economics

Pierre Lescanne, University of Lyon, ENS de Lyon, France

Escalation takes place in specific sequential games in which players continue although their payoff decreases. The *dollar auction* game has been presented by [Shubik(1971)] as the paradigm of such a behaviour. He noted that, even though their cost (the opposite of the payoff) basically increases, players may keep bidding. When talking about escalation, [Shubik(1971)] says this is a paradox, [O'Neill(1986)] and [Leininger(1989)] consider the bidders as irrational, [(2000)] speaks of *illogic conflict of escalation* and [Colman(1999)] calls it *Macbeth effect* after Shakespeare's play. In contrast with these authors, we have proved using coinduction that escalation is logic and that agents are rational.

This escalation phenomenon occurs in infinite sequential games and must be studied in a framework designed for mathematical infinite structures. Like [Shubik(1971)] we limit ourselves to two players only. In auctions, this consists in the two players bidding forever. This statement is based on the common assumption that a player is rational if he adopts a strategy which corresponds to a *subgame perfect equilibrium*. To characterize this equilibrium the above cited authors consider a finite restriction of the game for which they compute the subgame perfect equilibrium by *backward induction*[3]. In practice, they add a new hypothesis on the amount of money the bidders are ready to pay, which they call the *limited bankroll*. In the amputated game, they conclude that there is a unique subgame perfect equilibrium. This consists in both agents giving up immediately, not starting the auction and adopting the same choice at each step. In our formalization in infinite games, we show that extending that case up to infinity is not a subgame perfect equilibrium and we found two subgame perfect equilibria, namely the cases when one agent continues at each step and the other leaves at each step. Those equilibria which correspond to rational attitudes account for the phenomenon of escalation.

Like induction, coinduction is based on a fixpoint, but whereas induction is based on the least fixpoint, coinduction is based on the greatest fixpoint. Attached to induction is the concept of inductive definition, which characterizes objects like finite lists, finite trees, finite games, finite strategy profiles, etc. Similarly attached to coinduction is the concept of coinductive definition which characterizes streams (infinite lists), infinite trees, infinite games, infinite strategy profiles etc. An inductive definition yields the least set that satisfies the definition and a coinductive definition yields the greatest set that satisfies the definition. Associated with these definitions we have inference principles. For induction there is the famous *induction principle* used in backward induction. On coinductively defined sets of objects there is a principle like induction principle which uses the fact that the set satisfies the definition (proofs by case or by pattern) and that it is the largest set with this property. [Sangiorgi(2009)] gives a good survey with a complete historical account. To be sure not be entangled, it is advisable to use a proof assistant that implements coinduction to build and check the proof, but reasoning with coinduction is sometimes so counter-intuitive that the use of a proof assistant is not only advisable but compulsory. For instance, we were, at first, convinced that strategy profile consisting in both agents stopping at every step was a Nash equilibrium, like in the finite case, and only failing in proving it mechanically convinced us of the contrary

[3]What is called "backward induction" in game theory is roughly what is called "induction" in logic.

and we were able to prove the opposite. In our case we have checked every statement using Coq (see [Bertot and Castéran(2004)]). The core concept is this of infinite strategy profile which allows us presenting equilibria. The dollar auction game and the escalation will be discussed. In particular, we have proved that the strategy profile consisting in one agent continuing forever and the other abandoning forever is a subgame perfect equilibrium. The mathematical development presented here corresponds to a Coq script which can be found on the url:

`http://perso.ens-lyon.fr/pierre.lescanne/COQ/EscRat/`

This research was presented in two papers [Lescanne and Perrinel(2012), Lescanne(2013)].

Why escalation is rational? Many authors agree that choosing a subgame perfect equilibrium is rational [Aumann(1995)]. Let us show that this can lead to an escalation. Suppose I am Alice in the middle of the auction, I have two options that are rational: one option is to stop right away, since I assume that Bob will continue always. But the second option says that it could be the case that from now on Bob will stop always and I will always continue which is a subgame perfect equilibrium hence rational. If Bob acts similarly this is the escalation. So at each step an agent can stop and be rational, as well as at each step an agent can continue and be rational; both options make perfect sense. We claim that human agents reason coinductively unknowingly. Therefore, for them, escalation is one of their rational options at least if one considers strictly the rules of the dollar auction game, in particular with no limit on the bankroll. Many experiences [Colman(1999)] have shown that human are inclined to escalate or at least to go very far in the auction when playing the dollar auction game. We propose the following explanation: the finiteness of the game was not explicit for the participants and for them the game was naturally infinite. Therefore they adopted a form of reasoning similar to the one we developed here, probably in an intuitive form and they conclude it was equally rational to continue or to leave according to their feeling on the threat of their opponent, hence their attitude. Actually our theoretical work reconciles experiences with logic and human reasoning with rationality.

References

[Aumann(1995)] R. J. Aumann. Backward induction and common knowledge of rationality. *Games and Economic Behavior*, 8:6–19, 1995.

[Bertot and Castéran(2004)] Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development Coq'Art: The Calculus of Inductive Constructions*. Springer-Verlag, 2004.

[Colman(1999)] A. M. Colman. *Game theory and its applications in the social and biological sciences*. London New York : Routledge, 1999. Second edition.

[(2000)] H. Gintis. *Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Interaction*. Princeton University Press, 2000.

[Leininger(1989)] W. Leininger. Escalation and cooperation in conflict situations. *J. of Conflict Resolution*, 33:231–254, 1989.

[Lescanne(2013)] P. Lescanne. A simple case of rationality of escalation. In Reiko Heckel and Stefan Milius, editors, *CALCO*, volume 8089 of *Lecture Notes in Computer Science*, pages 191–204. Springer, 2013. ISBN 978-3-642-40205-0.

[Lescanne and Perrinel(2012)] P. Lescanne and M. Perrinel. "Backward" coinduction, Nash equilibrium and the rationality of escalation. *Acta Inf.*, 49(3):117–137, 2012.

[O'Neill(1986)] B. O'Neill. International escalation and the dollar auction. *J. of Conflict Resolution*, 30(33-50), 1986.

[Sangiorgi(2009)] D. Sangiorgi. On the origins of bisimulation and coinduction. *ACM Trans. Program. Lang. Syst.*, 31(4), 2009.

[Shubik(1971)] M. Shubik. The dollar auction game: A paradox in noncooperative behavior and escalation. *Journal of Conflict Resolution*, 15(1):109–111, 1971.

Non-monotonic extensions of the weak Kleene clone with constants

José Martínez Fernández, University of Barcelona, Spain

A clone on a set A is a set of finitary functions on A that includes the projection functions and is closed for composition. It is called a clone with constants when it contains all the constant functions on A. Every truth-functional propositional language determines the clone generated by the interpretation of its operator symbols. If we consider propositional languages interpreted with a three-valued truth-functional scheme, the clones generated by the weak and strong Kleene operators are specially interesting, because Kleene logics have been applied to the study of several fields, like partial predicates, semantic paradoxes, vagueness, the semantics of programming languages, etc.

The clone with constants generated by the weak Kleene propositional operators and the constant functions will be called the weak Kleene clone and analogously for the strong Kleene clone. It is well known that the strong Kleene clone coincides with the clone of three-valued functions monotonic on the order of information (i.e., the partial order on $0, 1, 2$ determined by $2 \leq 0$, $2 \leq 1$, where 0 represents falsity, 1 represents truth, and 2 is assigned to pathological sentences lacking a classical truth value). The aim of this project is to determine all the clones that are extensions of the weak Kleene clone but are not included in the strong Kleene clone. Equivalently, this amounts to the characterization of all the clones that can be obtained when we add to the weak Kleene clone a set of functions that include some function non-monotonic on the order of information. Using Jablonskij's theorem that determines all three-valued maximal clones and Lau's theorem that characterizes all the three- valued submaximal clones (see [2], II5 and II14), it is easy to check that only two three-valued maximal clones (C_2 and U_2) and three submaximal clones (one of them being the strong Kleene clone) contain the weak Kleene clone.

The talk will have two parts. First, we will motivate the study of this problem by presenting the theorems in [3] that determine all the maximal non-monotonic extensions of the weak Kleene clone with the Gupta-Belnap fixed-point property. Roughly speaking, a clone has the Gupta-Belnap fixed-point property when the languages defined with operators in the clone can consistently express all types of circular sentences (see [1], sect. 2B, 2E). In the second part of the talk we will determine completely all the clones in the interval between the weak Kleene clone and the clone U_2 that are not contained in the strong Kleene clone. As a corollary, this determines all the non-monotonic extensions of the weak Kleene clone with the Gupta-Belnap fixed-point property.

References

[1] ANIL GUPTA AND NUEL BELNAP, ***The Revision Theory of Truth***. MIT Press, 1993.

[2] DIETLINDE LAU, ***Function Algebras on Finite Sets***. Springer, 2006.

[3] JOSÉ MARTÍNEZ-FERNÁNDEZ, Maximal Three-Valued Clones with the Gupta-Belnap Fixed-Point Property. ***Notre Dame Journal of Formal Logic***, 48 (4): 449-472. 2007.

Natural deduction for modal logic of judgment aggregation

Tin Perkov, Polytechnic of Zagreb, Croatia

Judgment aggregation is about producing a group decision based on individual judgments. In particular, social choice or preference aggregation is about aggregating the society's preference based on individual preferences, e.g. rankings of candidates in some elections.

Judgments can be formalized as consistent sets of logical formulas. Mathematical framework for judgment aggregation consists of a set N of n individuals (agents, judges, voters), and the *agenda* – a set of formulas of a fixed underlying logic. In the case of social choice, this can be a first-order theory of strict linear orderings.

A *profile* is an n-tuple $\{R_1, \ldots, R_n\}$, where R_i is a judgment set of agent i. In the case of social choice, R_i is a strict linear ordering of candidates, as ranked by agent i. A *judgment aggregation rule* (JAR) is a function which maps each profile to a judgment set. In social choice theory this is called *social welfare function* (SWF). Given a particular profile as the input, a SWF produces a strict linear ordering of candidates, representing the society's preference (the result of elections). Social choice theory studies properties of social welfare functions, with a motivation to determine which properties make a SWF "fair" or "unfair".

A sound and complete modal logic of judgment aggregation is given in [2], using a Hilbert-style axiomatization. The authors state that it is of additional interest to provide a formal proof of Arrow's Theorem, a famous impossibility result in social choice, and make some steps towards it. I propose an alternative approach, a Jaśkowski-Fitch-style natural deduction system in which proofs are more intuitive, with a particular motivation to formalize a classical proof of Arrow's Theorem adapted from [3], as presented in [1].

The Judgment Aggregation Logic (JAL) is defined w.r.t. a fixed set N of individuals and a fixed agenda $\mathcal{A}$. The atomic symbols are a propositional variable p_i for each individual $i \in N$, a propositional variable q_A for each agenda item $A \in \mathcal{A}$, and a propositional variable σ representing the aggregated judgment. The truth of a formula is defined relative to a JAR, a profile R and an agenda item A, e.g. p_i means that agent i judges A, while σ means that A is the resulting group judgment of R under this JAR. The logic has two modalities $\Box$ and $\blacksquare$, which are read "for all profiles" and "for all agenda items", respectively.

The proofs of the natural deduction system for JAL are sequences of contextualized formulas. A context is a pair of a profile and an agenda item. The rules concerning introduction and elimination of Boolean connectives are classical and do not depend on a context. The rules concerning modalities are defined similarly as it is usually done in natural deduction systems for modal logics using contexts. Additional rules are needed to reflect logical consequence relation of the underlying logic, and the *universal domain assumption*, that is, that any consistent profile is admissible. In the case of preference aggregation this means that each individual can choose any strict linear ordering of candidates, independently of other individuals' choices.

Soundness of the system is proved directly (basically, it follows by induction from the apparent soundness of rules), while the problem of completeness is reduced to proving the axioms and simulating the inference rules from [2].

References

[1] U. Endriss: Logic and social choice theory. In A. Gupta and J. van Benthem, editors, Logic and Philosophy Today. College Publications (2011).

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

[3] A.K. Sen: Social choice theory. In K.J. Arrow and M.D. Intriligator, editors, Handbook of Mathematical Economics, Volume 3. North-Holland, (1986).

Bilattice public announcement logic

Umberto Rivieccio, Delft University of Technology, Netherlands

Dynamic logics are language expansions of classical (modal) logic designed to reason about changes induced by actions of different kinds, such as updates on the memory state of a computer, displacements of a moving robot, belief-revisions changing the common ground among different cognitive agents, knowledge update. Semantically, an action is represented as a transformation of a model describing a given state of affairs into a new one that encodes the state of affairs after the action has been performed.

The logic of public announcements (PAL) [14, 2, 6, 4] is a simple and well-known dynamic logic that models the epistemic change brought about on the cognitive state of a group of agents once a given proposition has become publicly known. To each proposition α one associates a *dynamic* modal operator $\lambda\alpha \rightarrow$ whose semantic interpretation is given by the transformation of models corresponding to its action-parameter α.

The present contribution builds on the logic of public announcements developed in [13, 12, 2] on the one hand and on the bilattice-valued modal logic [11] on the other.

[13, 12] introduce a semantically justified definition of dynamic epistemic logic on a base that is weaker than classical logic. The main methodological feature of these papers is the dual characterization of epistemic updates via Stone-type dualities. It is well known that epistemic updates induced by public announcements are formalized in relational models by means of the relativization construction, which creates a submodel of the original model. In [13] the corresponding submodel injection map is dually represented as a quotient construction between the complex algebras of the original model and of the updated one. This construction allows one to study epistemic updates within mathematical environments having a propositional support that is weaker than classical logic. Here we present a similar study in a context that is yet more general than that of [13]. As propositional base we take the bilattice logic introduced by Arieli and Avron [1], which is both an inconsistency-tolerant and a paracomplete logic, and we model epistemic modalities using the framework of the logic of modal bilattices introduced in [11].

The algebraic framework of bilattices [9] and their associated logic builds on seminal ideas of Belnap [3], motivated by the issue of dealing with incomplete and potentially inconsistent information in a computer setting. This framework has been further developed in [1] and generalized to weaker logics in, e.g., [10], [5]. In particular, [11] expands the language of bilattice logic with modal operators that are interpreted in many-valued analogues of Kripke frames.

Here we generalize the quotient construction of [13] to the algebraic semantics of bilattice modal logic, which allows us to define a natural interpretation of the language of PAL on modal bilattices. In this way we establish which interaction axioms among dynamic modalities are sound with respect to our intended semantics. The resulting calculus defines a bilattice-based version of public announcement logic (called *bilattice public announcement logic*), which we prove to be complete with respect to our algebra-based semantics analogously to classical PAL. We also introduce an equivalent relational semantics based on many-valued Kripke frames, which is obtained from the algebraic semantics via a Stone-type duality.

Our work aims at paving the way to a semantically-grounded analysis of epistemic updates in the presence of incomplete and/or inconsistent information. It is also a contribution to the research line initiated in [13, 12], which aims at introducing methods of algebraic logic, duality and proof theory in the study of the mathematical foundations of dynamic logic (see also [7, 8]).

Preliminary results from our research can be found in the forthcoming papers [15, 16].

References

[1] ARIELI, O., and A. AVRON, 'Reasoning with logical bilattices', *Journal of Logic, Language and Information*, 5 (1996), 1, 25–63.

[2] BALTAG, A., MOSS, L., and S. SOLECKI, ARIELI, O., and A. AVRON, 'The logic of public announcements, common knowledge, and private suspicions', *CWI technical report SEN-R9922*, 1999.

[3] BELNAP, N. D., 'How a computer should think', in G. Ryle, (ed.), *Contemporary Aspects of Philosophy*, Oriel Press, Boston, 1976, pp. 30–56.

[4] VAN BENTHEM, J., *Logical Dynamics of Information and Interaction*, Cambridge University Press, 2011.

[5] BOU, F., and U. RIVIECCIO, 'Bilattices with implications', *Studia Logica*, 101 (2013), 4, 651–675.

[6] VAN DITMARSCH, H., VAN DER HOEK, W., and B. KOOI, *Dynamic Epistemic Logic*, Springer, 2007.

[7] FRITTELLA, S., GRECO, G., KURZ, A., PALMIGIANO, A., and V. SIKIMIC, 'A Proof-Theoretic Semantic Analysis of Dynamic Epistemic Logic', *Journal of Logic and Computation, Special issue on Sub-structural logic and information dynamics*, forthcoming.

[8] FRITTELLA, S., GRECO, G., KURZ, A., PALMIGIANO, A., and V. SIKIMIC, 'Multi-type Display Calculus for Propositional Dynamic Logic', *Journal of Logic and Computation, Special issue on Sub-structural logic and information dynamics*, forthcoming.

[9] GINSBERG, M. L., 'Multivalued logics: A uniform approach to inference in artificial intelligence', *Computational Intelligence*, 4 (1988), 265–316.

[10] JANSANA, R., and U. RIVIECCIO, 'Residuated bilattices', *Soft Computing*, 16 (2012), 3, 493–504.

[11] JUNG, A., and U. RIVIECCIO, 'Kripke semantics for modal bilattice logic', *Proceedings of the 28th Annual ACM/IEEE Symposium on Logic in Computer Science*, IEEE Computer Society Press, 2013, 438–447.

[12] KURZ, A., and A. PALMIGIANO, 'Epistemic Updates on Algebras', *Logical Methods in Computer Science*, 9 (2013), 4. DOI: 10.2168/LMCS-9(4:17)2013.

[13] MA, M., PALMIGIANO, A., and M. SADRZADEH, 'Algebraic semantics and model completeness for Intuitionistic Public Announcement Logic', *Annals of Pure and Applied Logic*, 165 (2014), 963–995.

[14] PLAZA, J., 'Logics of Public Communications', *Proceedings 4th International Symposium on Methodologies for Intelligent Systems*, 1989, 201–216.

[15] RIVIECCIO, U., 'Algebraic Semantics for Bilattice Public Announcement Logic', *Proceedings of the 13th Trends in Logic International Conference*, Łodz (Poland), 2-5 July 2014, forthcoming.

[16] RIVIECCIO, U., 'Bilattice Public Announcement Logic', *Proceedings of the 10th International Conference on Advances in Modal Logic*, Groningen (Netherlands), 5-8 August, 2014, forthcoming.

Certain applications of ultraproducts

Nenad Savić, Faculty of Technical Sciences, University of Novi Sad, Serbia

Ultrafilters and ultraproducts are unavoidable methods in many different mathematical branches. Typical examples are set theory, topology, algebra, model theory and non-standard analysis. For example, in algebra, among other things, they are powerful weapon for testing axiomatizability of some classes of algebras (we can find those examples in works of Malcev from early beginning of model theory). It can easily be proved that classes of nilpotent, solvable and non-Abelian simple groups are not finitely axiomatizable. Further, in model theory, ultraproduct construction is the most popular way for making new models from the existing classes. Ultrapoducts are much more useful than reduced products if we consider axiomatizability because if the existing class is axiomatizable, then new model will belong to the same class. Besides that, one of three equivalent conditions that some class is axiomatizable is that class is closed for formation of ultraproducts. Existence of measurable cardinal is equvivalent with existence of ω^+- complete ultrafilter. In non-standard analysis, if we make an ultrapower of $\mathbb{R}$, where index set is countable, we wiil get the structure much richer than $\mathbb{R}$, but, what is the most important, we will not lose any properties of $\mathbb{R}$ considering it as an ordered field of real numbers. Furthermore, we are able to give explicit examples of infinitesimals and "non-standard big" real numbers.

Cardinality of ultraproducts is also very important to mention, because we obtain new models. It can be shown that cardinality of ultraproducts of finite (non-empty) sets A_i, over countable index set I, is completely determined, strictly:

- if there exists $n \in \omega$ such that $\{i \in I \mid card(A_i) = n\} \in U$, then $card(\prod A_i/U) = n$,
- if there is no such n, then $card(\prod A_i/U) = 2^{\aleph_0}$,

where U is non-principal ultrafilter on I. The most popular classification of ultrafilters, that is the classification on regular, principal, non-principal, uniform etc. gives us a lot of information about cardinality of ultraproducts if observed ultrafilter belongs to any of these classes. For instance, if λ is infinite cardinal and U is regular ultrafilter on I and $card(I) = \gamma$, then:

$$card(\lambda^I/U) = \lambda^\gamma.$$

(For proof see [1, p. 132-133]).

One "imperfection" is that in case of a finite set we know that all ultrafilters are principal and how they look like, but, in case that the set is infinite we don't know how they look like. We know only that there are plenty of them, because the proof of existence of very rich class of ultrafilters is based on Zorn's lemma (which is equvivalent with axiom of choice), and we all know the "troubles" which that axiom brought us. That class is so rich that on an infinite set whose cardinality is λ we have 2^{2^λ} non-principal ultrafilters (proof of this interesting result can be found in [1, p. 108-111]).

Ultrafilters and their applications have become popular in the first half of the 20th century with the works of, among others, Tarski and Malcev. Nowadays, we see that, with the development of mathematics, ultrafilters are extremely powerful mathematical tool used not only in mathematics. For instance, in economics, we have a paper[4] which

[4]G. Bedrosian, F. Herzberg, "Microeconomic Foundations of Representative Agent Models by Means of Ultraproducts", 2014

shows us that ultraproducts have direct applications to economics.

In this work, first of all, we give some basic definitions and theorems about filters and ultrafilters. After that, we give the ultraproduct construction and fundamental theorem about ultraproducts, that is Łoś's theorem (for proof see [1, p. 89-91]) which states that some formula holds on ultraproduct if and only if it holds at "almost all" coordinates, or written by formula:

$$\mathcal{A} \models_\nu \varphi(x_1, \ldots, x_n) \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models_{\nu_i} \varphi(x_1, \ldots, x_n)\} \in U.$$

After that, we give three examples from different areas (to try to emphasize that widespread range of ultraproducts): first of all algebra, proof of the well known theorem which states that every field has an algebraic closure, then non-standard analysis, effective construction of non-standard reals (non-standard big numbers and infinitesimals) and explicit examples (for more details see [2, p. 115-119]), and, in the end, mathematical logic, proof of compactness theorem. These examples are consequences of Łoś's theorem whose importance is really hard to overestimate.

References

[1] Bell, J.L., Slomson, A.B., *Models and Ultraproducts: An Introduction*, North-Holland, Amsterdam, 1969.

[2] Mendelson, E., *Introduction to mathematical logic*, D. Van Nostrand company, 1979.

Information Frames

Dieter Spreen, University of Siegen, Germany and University of South Africa, Pretoria

2 Introduction

In 1982, in a seminal paper [2], Dana Scott introduced information systems as a logic-based approach to domain theory. An information system consists of a set of tokens to be thought of as atomic statements about a computational process, a consistency predicate telling us which finite sets of such statements contain consistent information, and an entailment relation saying what atomic statements are entailed by which consistent sets of these. Theories of such a logic, also called states, i.e. finitely consistent and entailment-closed sets of atomic statements, form a bounded-complete domain with respect to set inclusion, and, conversely, every such domain can be obtained in this way, up to isomorphism. This gives Scott's idea that domains represent information about stages of a computation a precise mathematical meaning.

The role of bounded completeness becomes also clear in this context: States represent consistent information. So, any finite collection of substates must contain consistent information as well, and this fact is witnessed by any of its upper bounds.

Whereas in Scott's approach the consistency witnesses are hidden, in this paper we present an approach that makes them explicit. This allows to consider the more general situation in which there is no longer a uniform global consistency predicate. Instead there is a consistency predicate for each atomic statement telling us which finite sets of atomic statements express information that is consistent with the given statement. As it turns out the theories, or states, of such a more general information system form an L-domain, and, up to isomorphism, each L-domain can be obtained in this way.

Since every token in the just delineated kind of information system has its own consistency predicate, we can also think of each such system as a family of logics, or a Kripke frame.

L-domains form one of the two maximal Cartesian closed full subcategories of the continuous domains. Logic-oriented representations of such domains allow to talk about higher-type functionals or program semantics in proof assistants.

3 Basic definitions

Let $(D, \sqsubseteq)$ be a poset. D is *pointed* if it contains a least element $\bot$. For an element $x \in D$, $\downarrow x$ denotes the principal ideal generated by x, i.e., $\downarrow x = \{\, y \in D \mid y \sqsubseteq x \,\}$. A subset S of D is called *consistent* if it has an upper bound. S is *directed*, if it is nonempty and every pair of elements in S has an upper bound in S. D is a *directed-complete partial order* (*dcpo*), if every directed subset S of D has a least upper bound $\bigsqcup S$ in D, and D is *bounded-complete* if every consistent subset has a least upper bound.

Assume that x, y are elements of D. Then x is said to *approximate* y, written $x \ll y$, if for any directed subset S of D the least upper bound of which exists in D, the relation $y \sqsubseteq \bigsqcup S$ always implies the existence of some $u \in S$ with $x \sqsubseteq u$. Moreover, x is *compact* if $x \ll x$. A subset B of D is a *basis* of D, if for each $x \in D$ the set $\Downarrow_B x = \{\, u \in B \mid u \ll x \,\}$ contains a directed subset with least upper bound x. Note that the set of all compact elements of D is included in every basis of D. A dcpo

D is said to be a *domain* if it has a basis and it is called *algebraic domain* if its compact elements form a basis. A pointed bounded-complete domain is called *bc-domain*. An *L-domain* is a pointed domain in which every principal ideal is a complete lattice. This means in particular that every subset in the ideal has a least upper bound relative to the ideal.

4 Results

An information frame consists of a Kripke frame (A, R), the nodes of which are also called tokens. Associated with each node $i \in A$ is a consistency predicate Con_i classifying the finite sets of tokens which are consistent with respect to node i, and an entailment relation $\vdash_i$ between i-consistent sets and tokens.

The conditions that have to be satisfied are grouped. There are requirements which consistency predicate and entailment relation of each single node have to meet, and which are well known from Scott's information systems. In addition, we find conditions that specify their interplay for nodes related to each other by the accessibility relation.

Definition 1 *Let A be a set, R be a binary relation on A, $\Delta \in A$, $(\mathrm{Con}_i)_{i\in A}$ be a family of subsets of $\mathcal{P}_f(A)$, and $(\vdash_i)_{i\in A}$ be a family of relations $\vdash_i \subseteq \mathrm{Con}_i \times A$. Then $\mathcal{A} = (A, R, (\mathrm{Con}_i)_{i\in A}, (\vdash_i)_{i\in A}, \Delta)$ is an* information frame *if the following conditions hold, for all $i, j, a \in A$ and all finite subsets X, Y, F of A:*

$$\begin{array}{ll}
\{i\} \in \mathrm{Con}_i & Y \subseteq X \wedge X \in \mathrm{Con}_i \Rightarrow Y \in \mathrm{Con}_i \\
\emptyset \vdash_i \Delta & X \vdash_i Y \Rightarrow Y \in \mathrm{Con}_i \\
X, Y \in \mathrm{Con}_i \wedge Y \supseteq X \wedge X \vdash_i a \Rightarrow Y \vdash_i a & X \vdash_i Y \wedge Y \vdash_i a \Rightarrow X \vdash_i a \\
iRj \Rightarrow \mathrm{Con}_i \subseteq \mathrm{Con}_j & \{i\} \in \mathrm{Con}_j \Rightarrow iRj \\
iRj \wedge X \in \mathrm{Con}_i \wedge X \vdash_i a \Rightarrow X \vdash_j a & iRj \wedge X \in \mathrm{Con}_i \wedge X \vdash_j a \Rightarrow X \vdash_i a
\end{array}$$

$$X \vdash_i F \Rightarrow (\exists e \in A) X \vdash_i e \wedge \{e\} \vdash_e F.$$

Here $X \vdash_i Y$ means that $X \vdash_i b$, for all $b \in Y$.

All requirements are very natural: Each token witnesses its own consistency. If the consistency of some set is witnessed by i, the same holds for all of its subsets. Δ is entailed by any set of information and in every node, i.e., it represents global truth. Each entailment relation preserves consistency. If a set X entails a, so does any bigger set. Entailment should be transitive. Consistency and entailment are preserved when moving from a node i to its accessible neighbour j. Moreover, entailment is conservative: what is j-entailed from an i-consistent set is already i-entailed. Finally, we have an interpolation property. As it turns out, iRj, exactly if $\{i\} \in \mathrm{Con}_j$.

Definition 2 *Let $\mathcal{A}$ be an information frame. A subset x of A is a* state *of $\mathcal{A}$ if the following three conditions hold:*

$$(\forall F \subseteq_{\mathrm{fin}} x)(\exists i \in x) F \in \mathrm{Con}_i, \quad (\forall i \in x)(\forall X \subseteq_{\mathrm{fin}} x)(\forall a \in A)[X \in \mathrm{Con}_i \wedge X \vdash_i a \Rightarrow a \in x]$$
$$(\forall a \in x)(\exists i \in x)(\exists X \subseteq_{\mathrm{fin}} x) X \in \mathrm{Con}_i \wedge X \vdash_i a.$$

As follows from the definition, states are subsets of tokens that are *finitely consistent* and *closed under entailment*. Furthermore, each token in a state is *derivable*, i.e. for each token the state contains a consistent set and its witness entailing the token. States are never empty: Choose F to be the empty set. Let $|A|$ denote the set of states of $\mathcal{A}$.

Theorem 3 *Let $\mathcal{A}$ be an information frame. Then $\mathcal{L}(\mathcal{A}) = (|A|, \subseteq, [\emptyset]_\Delta)$ is an L-domain with basis $\{\, [X]_i \mid i \in A \wedge X \in \mathrm{Con}_i \,\}$, where $[X]_i = \{\, a \in A \mid X \vdash_i a \,\}$.*

Conversely, let D be an L-domain with basis B and define

$$\mathrm{Con}_u = \{\, X \subseteq_f B \mid X \subseteq {\downarrow} u \,\}, \quad X \vdash_u v \Leftrightarrow v \ll \bigsqcup\nolimits^u X, \quad uRv \Leftrightarrow u \sqsubseteq v.$$

Theorem 4 *Let D be an L-doman with basis B. Then $\mathcal{F}(D) = (B, R, (\mathrm{Con}_u)_{u\in B}, (\vdash_u)_{u\in B}, \bot)$ is an information frame such that $\mathcal{L}(\mathcal{F}(D))$ and D are isomorphic domains.*

This allows showing the equivalence of the corresponding categories. Note that the exponent of two information frames can explicitly be constructed.

For an information frame $\mathcal{A}$, $\mathcal{L}(\mathcal{A})$ is a bc-domain, respectively algebraic, exactly if Conditions (BC) and (ALG) are satisfied, where for $X, F \subseteq_f A$ and $i, j \in A$

$$X \in \mathrm{Con}_i \cap \mathrm{Con}_j \Rightarrow (\forall a \in A)[X \vdash_i a \Leftrightarrow X \vdash_j a], \tag{BC}$$

$$X \vdash_i F \Rightarrow (\exists k \in A_{\mathrm{refl}}) X \vdash_k k \wedge \{k\} \vdash_k F, \tag{ALG}$$

Here, A_{refl} is the set of reflexive elements of A, where an element j is *reflexive* if $\{j\} \vdash_j j$.

In the presence of Condition (BC) we have a syntactic translation from information frames into continuous information systems introduced by Hoofman [1].

Theorem 5 *Let $\mathcal{A}$ be an information frame satisfying Condition (BC) and define*

$$\mathrm{Con} = \bigcup \{\, \mathrm{Con}_i \mid i \in A \,\} \quad \textit{and} \quad \vdash = \bigcup \{\, \vdash_i \mid i \in A \,\}.$$

Then $(A, \mathrm{Con}, \vdash)$ is a continuous information system, i.e., for all $a \in A$ and all $X, Y \subseteq_f A$ the following requirements are fulfilled:

$$\begin{array}{lll} \emptyset \in \mathrm{Con}, & X \subseteq Y \in \mathrm{Con} \Rightarrow X \in \mathrm{Con}, & \{a\} \in \mathrm{Con}, \\ X \vdash Y \Rightarrow Y \in \mathrm{Con}, & X \vdash a \wedge X \subseteq Y \Rightarrow Y \vdash a, & X \vdash Y \wedge Y \vdash a \Rightarrow X \vdash a, \\ \multicolumn{3}{c}{X \vdash a \Rightarrow (\exists Y \in \mathrm{Con}) X \vdash Y \wedge Y \vdash a.} \end{array}$$

If both (ALG) and (BC) are satisfied, a similar result holds with respect to Scott's algebraic information systems [2].

Theorem 6 *Let $\mathcal{A}$ be an information frame satisfying Condition (BC) and (ALG) and define*

$$\mathrm{Con}_{\mathrm{refl}} = \{\, X \subseteq_f A_{\mathrm{refl}} \mid (\exists i \in A_{\mathrm{refl}}) A \in \mathrm{Con}_i \,\} \quad \textit{and} \quad X \vdash_{\mathrm{refl}} a \Leftrightarrow (\exists i \in A_{\mathrm{refl}}) X \vdash_i a.$$

Then $(A_{\mathrm{refl}}, \mathrm{Con}_{\mathrm{refl}}, \vdash_{\mathrm{refl}})$ is an algebraic information system, i.e., for all $a \in A$ and all $X, Y \subseteq_f A$ the following requirements are satisfied:

$$\begin{array}{lll} \emptyset \in \mathrm{Con}_{\mathrm{refl}}, & X \subseteq Y \in \mathrm{Con}_{\mathrm{refl}} \Rightarrow X \in \mathrm{Con}_{\mathrm{refl}}, & \{a\} \in \mathrm{Con}_{\mathrm{refl}}, \\ X \vdash_{\mathrm{refl}} Y \Rightarrow Y \in \mathrm{Con}_{\mathrm{refl}}, & X \vdash_{\mathrm{refl}} a \wedge X \subseteq Y \Rightarrow Y \vdash_{\mathrm{refl}} a, & X \vdash_{\mathrm{refl}} Y \wedge Y \vdash_{\mathrm{refl}} a \Rightarrow X \vdash_{\mathrm{refl}} a, \\ \multicolumn{3}{c}{a \in X \Rightarrow X \vdash_{\mathrm{refl}} a.} \end{array}$$

References

[1] R. Hoofman. Continuous information systems. *Inform. Computation* 105 (1993) 42-71.

[2] D. Scott. Domains for denotational semantics. In: M. Nielsen et al. (eds.). *Automata, Languages and Programming*, Aarhus, 1982. Lecture Notes in Computer Science, Vol. 140. Springer, Berlin, 1982, pp. 577–613.

Justification Logic

Thomas Studer, Institut für Informatik und angewandte Mathematik, Universität Bern, Switzerland

Justification logics are epistemic logics that feature the 'unfolding' of modalities into *justification terms*. Instead of $\Box A$, justification logics include formulas of the form $t{:}A$ that mean *A is justified by reason t*. One may think of traditional modal operators as *implicit* modalities and justification terms as their *explicit* counterparts. In a statement $t{:}A$, the justification term t may represent a formal mathematical proof of A or an informal reason for A.

Originally, Artemov developed the first justification logic, the Logic of Proofs, to provide a classical provability semantics for intuitionistic logic. In that approach justification terms represent proofs in a formal system like Peano arithmetic. Later justification logic was introduced into formal epistemology where justification terms cannot only represent proofs but evidence in a much more general sense. For instance, an agent's knowledge may be justified by communication with another agent. Mathematical logic and epistemology are the two main sources of justification logic.

In our talk we will introduce justification logic and discuss its origins and applications. For a detailed introduction to justification logic, see, e.g., [4, 12].

Epistemic Tradition

Plato characterized knowledge as *justified true belief*. Epistemic modal logic, however, only works with two of Plato's three criteria for knowledge. Belief is modeled using possible worlds and an indistinguishability relation: one believes what holds in all worlds that are considered possible. Trueness follows from the factivity axiom $\Box A \to A$, respectively from the reflexivity of the indistinguishability relation: if something is known, it must hold in the actual world. What is missing in the modal epistemic representation of knowledge is the justification component. Modal logic does not provide any means to express that there must be a justification for one's knowledge.

While mathematical proofs provide a paradigmatic example of justifications, there are many more forms of justifications that can be considered in a general epistemic setting such as direct observation, public announcements, or private communication. Explicit justifications allow us to analyze (dynamic) epistemic situations in a fine grained way and to formalize and discuss many epistemic problems and puzzles [3, 7, 9, 10, 11].

Justification terms not only keep track of the sources of an agent's knowledge. They also reflect the agent's whole reasoning process that leads to his knowledge. Artemov and Kuznets [5] exploit this important feature to provide a quantitative solution to the logical omniscience problem.

The evidence-tracking mechanism of justification logic makes it possible to formalize justifications for an agent's knowledge. However, it also allows us to distinguish various reasons why something may not be known. For instance, Bucheli et al. [8] provide an analysis of the coordinated attack problem in the language of justification logic where it is possible to distinguish whether the content of a message is not known because the message has not been delivered or because its signature could not be verified.

The notion of knowledge captured by the modal logic S4 is inherently self-referential. Although this fact pops up in sequent-style proofs of certain S4-theorems, it cannot be expressed in the language of S4 directly. This, however, changes when we use

justification logic. Kuznets [6] established that any embedding of S4 into justification logic necessarily requires self-referential justification assertions, that is assertions of the form $c{:}A(c)$ where the justification c occurs in the justified proposition $A(c)$. Self-referential assertions are not only intriguing epistemic objects, they also provide a special challenge from the semantic point of view because of the built-in vicious circle.

Mathematical Logic Tradition

According to Brouwer, truth in intuitionistic logic means constructive provability. Based on this idea, Heyting and Kolmogorov gave an explicit (but informal) definition of intuitionistic truth, which nowadays is known as Brouwer–Heyting–Kolmogorov (BHK) semantics for intuitionistic logic.

This semantics is widely accepted as the intended semantics for intuitionistic logic. However, it is purely informal and does not provide a precise definition of intuitionistic truth. Gödel took the first step towards developing a rigorous proof-based interpretation of BHK semantics. He considered the classical modal logic S4 to be a calculus describing properties of provability, that is he interpreted $\Box A$ as *A is provable*. Based on the idea that intuitionistic truth means provability, Gödel defined a translation $\mathsf{Gt}(\cdot)$ from intuitionistic logic IL into S4. It follows from results of Gödel as well as McKinsey and Tarski that $\mathsf{Gt}(\cdot)$ is indeed a correct and faithful embedding of intuitionistic logic into the modal logic S4. Hence we have an embedding of intuitionistic logic into classical logic with a provability operator.

Still the aim of defining intuitionistic logic in terms of classical provability was not reached for the connection of S4 to the usual mathematical notion of provability was not established. We have the following situation where $X \hookrightarrow Y$ should be read as *X is interpreted in Y*:

$$\mathsf{IL} \hookrightarrow \mathsf{S4} \hookrightarrow \ldots ??? \ldots \hookrightarrow \text{classical proofs} \ .$$

In 1938, Gödel suggested in a public lecture that using explicit proofs could help to obtain a provability interpretation of S4. Unfortunately, his work remained unpublished until 1995, by which time the idea of using explicit proofs had already been rediscovered by Artemov who introduced the Logic of Proofs LP [1, 2]. He showed that S4 can be realized in LP and provided a classical provability semantics for LP.

Thus with LP, intuitionistic logic received the desired classical provability semantics:

$$\mathsf{IL} \hookrightarrow \mathsf{S4} \hookrightarrow \mathsf{LP} \hookrightarrow \text{classical proofs} \ .$$

References

[1] S. N. Artemov. Operational modal logic. Technical Report MSI 95–29, Cornell University, Dec. 1995.

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

[3] S. N. Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, Dec. 2008.

[4] S. N. Artemov and M. Fitting. Justification logic. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2012 edition, 2012.

[5] S. N. Artemov and R. Kuznets. Logical omniscience as infeasibility. *Annals of Pure and Applied Logic*, 165(1):6–25, Jan. 2014.

[6] V. N. Brezhnev and R. Kuznets. Making knowledge explicit: How hard it is. *Theoretical Computer Science*, 357(1–3):23–34, July 2006.

[7] S. Bucheli, R. Kuznets, B. Renne, J. Sack, and T. Studer. Justified belief change. In X. Arrazola and M. Ponte, editors, *Proc. LogKCA-10*, pages 135–155. University of the Basque Country Press, 2010.

[8] S. Bucheli, R. Kuznets, and T. Studer. Justifications for common knowledge. *Journal of Applied Non-Classical Logics*, 21(1):35–60, 2011.

[9] S. Bucheli, R. Kuznets, and T. Studer. Partial realization in dynamic justification logic. In L. D. Beklemishev and R. de Queiroz, editors, *Proc. WoLLIC 2011*, volume 6642 of *LNAI*, pages 35–51. Springer, 2011.

[10] R. Kuznets and T. Studer. Update as evidence: Belief expansion. In S. N. Artemov and A. Nerode, editors, *Proc. LFCS*, volume 7734 of *LNCS*, pages 266–279. Springer, 2013.

[11] B. Renne. Public communication in justification logic. *Journal of Logic and Computation*, 21(6):1005–1034, Dec. 2011. Published online July 2010.

[12] T. Studer. Lectures on justification logic. Lecture notes, Nov. 2012.

On Probable Conditionals

Zvonimir Šikić, University of Zagreb, Croatia

We are interested in probable conditionals which could be pr$(A \to B)$ "probability of, B if A" or pr$(A \mid B)$ "probability of B, if A". Lewis famously proved that they are not the same:

If pr$(A \to B)$ is the same as pr$(B \mid A)$ then

$$\begin{aligned}\text{pr}(B|A) &= \text{pr}(A \to B) = \\ &= \text{pr}(A \to B|B)\,\text{pr}(B) + \text{pr}(A \to B| - B)\,\text{pr}(-B) = \\ &= \text{pr}(B \to (A \to B))\,\text{pr}(B) + \text{pr}(-B \to (A \to B))\,\text{pr}(-B) = \\ &= \text{pr}(AB \to B)\,\text{pr}(B) + \text{pr}(A(-B) \to B)\,\text{pr}(-B) = \\ &= 1 \cdot \text{pr}(B) + 0 \cdot \text{pr}(-B) = \text{pr}(B);\end{aligned}$$

a contradiction.

An even more elementary proof (for classical conditional):

$$\begin{aligned}\text{pr}(A \to B) = \text{pr}(-A \vee B) = \text{pr}(-A \vee AB) = \text{pr}(-A) + \text{pr}(AB) = \\ = \text{pr}(-A) + \text{pr}(A)\,\text{pr}(B \mid A) = 1 - x + xc,\end{aligned}$$

where $x = \text{pr}(A)$ and $c = \text{pr}(B \mid A)$. Hence pr$(A \to B) = \text{pr}(B \mid A)$, i.e. $1-x+xc = c$, only if pr$(A) = x = 1$ or pr$(B \mid A) = c = 1$, i.e. if pr$(A \to B) = \text{pr}(B \mid A) = 1$.

Even more elementary, take $S =$ If "*it is even on the die*" then "*it is two on the die*" $= E \to T$. Then pr$(-(A \to T)) =$ pr("even" & "not two") $= \frac{1}{3}$, i.e. pr$(E \to T) = \frac{2}{3}$, but pr$(T \mid E) = \frac{1}{3}$.

A better candidate for probable conditional is $A \uparrow B$, which means "A *makes* B *more probable*" ("A supports B"), which is defined as pr$(B \mid A) > pr(B)$. We could also define $A \downarrow B$, which means "A *makes* B *less probable*" ("A subverts B"), as pr$(B \mid A) <$ pr(B). The independence relation $A \perp B$, is defined to hold when pr$(B \mid A) =$ pr(B).

It is tempting to transfer the properties of conditionals to the properties of "supports". This error is quite common. One would think: "*if A supports B and B supports C, then A supports C*" (i.e. transitivity of "supports"). But when confronted with a concrete counterexample:

$A =$ "having white hair"
$B =$ "being over 50"
$C =$ "being completely bald",

people change their mind.

One would also think: "*if A supports C and B supports C, then their conjunction supports C even more*". When confronted with (a counterexample): A crime is committed by two men, one in a red jacket another in a black coat.

$A =$ "first witness recognized the suspect as the man in the red jacket"
$B =$ "second witness recognized him as the man in the black coat"
$C =$ "the suspect is guilty",

once again, people change their mind. Other concrete counterexamples are in Carnap's *Logical Foundations of Probability* (chapter 6).

It seems that people don't err in concrete but do err in abstract settings. Abstract analysis of "supports" $\uparrow$ (compared to conditional $\rightarrow$) could be interesting for this reason.

Basic properties of conditionals are:

(1) $A \rightarrow B, B \rightarrow C \Rightarrow A \rightarrow C$ is valid (transitivity)

(2) $A \rightarrow B \Rightarrow B \rightarrow A$ is not valid (converse fallacy)

(3) $A \rightarrow B \Rightarrow -B \rightarrow -A$ is valid (contraposition)

(4) $A \rightarrow B \Rightarrow -A \rightarrow -B$ is not valid (inverse fallacy)

(5) $C \rightarrow A, C \rightarrow B \Rightarrow C \rightarrow A\&B$ is valid (conjunction introduction)

(6) $C \rightarrow A, C \rightarrow B \Rightarrow C \rightarrow A \vee B$ is valid (disjunction introduction)

(7) $A \rightarrow C, B \rightarrow C \Rightarrow A\&B \rightarrow C$ is valid (conjunction elimination)

(8) $A \rightarrow C, B \rightarrow C \Rightarrow A \vee B \rightarrow C$ is valid (disjunction elimination)

Corresponding properties of $A \uparrow B$, except (3), are of exactly opposite validity:

(i) Property (2) is valid for $\uparrow$ (the relation is symmetrical).

(ii) Property (4) is valid for $\uparrow$.

(iii) Property (1) is not valid for $\uparrow$ (the relation is not transitive).

(iv) Properties (5), (6), (7) and (8) are not valid for $\uparrow$.

It is easy to prove that:

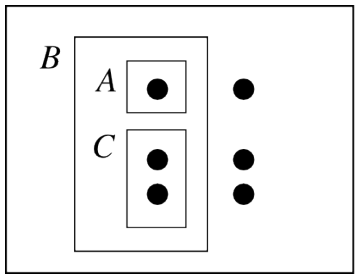
(i) The symmetry of $\uparrow$ and $\downarrow$ follows from

$$\mathrm{pr}(A \mid B)\,\mathrm{pr}(B) = \mathrm{pr}(B \mid A)\,\mathrm{pr}(A)\ .$$

Namely, if $\mathrm{pr}(A \mid B) > \mathrm{pr}(A)$ and $\mathrm{pr}(B \mid A) \leq \mathrm{pr}(B)$ then $\mathrm{pr}(A \mid B)\,\mathrm{pr}(B) > \mathrm{pr}(B \mid A)\,\mathrm{pr}(A)$ (a contradiction). Similarly, supposing $\mathrm{pr}(A \mid B) < \mathrm{pr}(A)$ also leads to contradiction.

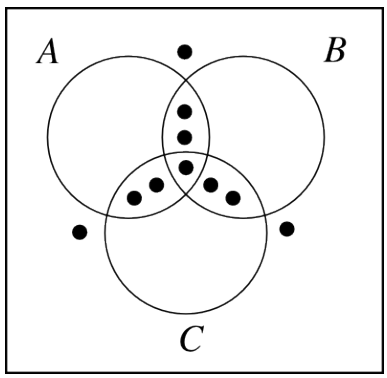
(ii) It is easy to prove that $A \uparrow B \iff A \downarrow -B$ and $A \downarrow B \iff A \uparrow -B$, and (4) then follows by symmetry of $\uparrow$ and $\downarrow$.

(iii)



From the figure follows that pr$(B \mid A) = 1$ and pr$(B) = \frac{1}{2}$, i.e. $A \uparrow B$, pr$(C \mid B) = \frac{2}{3}$ and pr$(C) = \frac{1}{3}$, i.e. $B \uparrow C$ and pr$(C) = \frac{1}{3}$, i.e. $A \downarrow C$; hence "$\uparrow$" is not transitive.

(iv)



From the figure follows that pr$(A \mid C) = \frac{3}{5}$ and pr$(A) = \frac{1}{2}$, i.e. $C \uparrow A$, pr$(B \mid C) = \frac{3}{5}$ and pr$(B) = \frac{1}{2}$, i.e. $C \uparrow B$, but pr$(A\&B \mid C) = \frac{1}{5}$ and pr$(A\&B) = \frac{3}{10}$, i.e. $C \downarrow (A\&B)$. This proves that (5) is not valid for $\uparrow$.

It also follows that pr$(C \mid A) = \frac{3}{5}$ and pr$(C) = \frac{1}{2}$, i.e. $A \uparrow C$, pr$(C \mid B) = \frac{3}{5}$ and pr$(C) = \frac{1}{2}$, i.e. $B \uparrow C$, but pr$(C \mid A\&B) = \frac{1}{3}$ and pr$(A\&B) = \frac{1}{2}$, i.e. $(A\&B) \downarrow C$. This proves (7) is not valid for $\uparrow$.

From nonvalidity of (5) for $\uparrow$ follows that $-C \uparrow -A$, $-C \uparrow -B \Rightarrow -C \uparrow (-A\&-B)$ is not valid. Also, from (ii) follows $C \uparrow A, C \uparrow B \Rightarrow -(-A\&-B)$ is not valid. Hence, $C \uparrow A$, $C \uparrow B \Rightarrow C \uparrow (A \vee B)$ is not valid. This proves nonvalidity of (6) for $\uparrow$.

Finally, nonvalidity of (8) for $\uparrow$ follows (analogously) from nonvalidity of (7) for $\uparrow$.

Lindström's theorem for interpretability logic

Mladen Vuković, Department of Mathematics, University of Zagreb, Croatia

Lindström's theorems characterize logics in terms of model–theoretic conditions such as Compactness and the Löwenheim–Skolem property. Most existing Lindström's theorems concern extensions of first-order logic. On the other hand, many logics relevant to computer science are fragments or extensions of fragments of first-order logic, e.g., k–variable logics and various modal logics. Finding Lindström's theorems for these languages can be challenging, as most known techniques rely on coding arguments that seem to require the full expressive power of first-order logic.

There are several known Lindström–style characterization results for basic modal logic. J. van Benthem showed in [7] that no logic that is compact, bisimulation invariant and has the relativisation property can properly extend basic modal logic. This characterization itself may be seen as a methodological improvement on the characterization by de Rijke [2] (see also [1]), which explicitly stipulated a finite depth condition as a crucial criterion.

M. Otto and R. Piro in [4] established a Lindström type characterization of the extension of basic modal logic by a global modality and of the guarded fragment of first–order logic as maximal among compact logics with the corresponding bisimulation invariance and the Tarski Union Property.

S. Enqvist proved in [3] a generic Lindström's theorem that covers any normal modal logic corresponding to a class of Kripke frames definable by a set of formulas called strict universal Horn formulas. He also proved a negative result showing that the result cannot be strengthened to cover every first–order elementary class of frames.

We consider Lindström–style characterization for interpretability logic (IL). The paper [8] provides the necessary definitions and detailed explanation on IL. In [9] unraveling of Veltman model is defined. Unraveling is an important part of proof of Lindström's theorem.

We have to mentioned that J. van Benthem proved in [7] that Lindström's theorem for modal logic implies modal invariance theorem, i.e. up to logical equivalence, the basic modal formulas are precisely those first-order formulas which are invariant for bisimulation. In [5] the modal invariance theorem for IL is proved. So, we can consider a connection between invariance theorem and Lindström's theorem, too.

References

[1] P. BLACKBURN, M. DE RIJKE, Y. VENEMA, Modal Logic, Elsevier, 2001.

[2] M. DE RIJKE, *A Lindström Theorem for Modal Logic*, in: A. Ponse i dr. (ed.), Modal Logic and Process Algebra, SCLI Publications, 1995.

[3] S. ENQVIST, *A General Lindström Theorem for Some Normal Modal Logics*, Logica Universalis 7 (2013), 233–264

[4] M. OTTO, R. PIRO, *A Lindström Characterisation of the Guarded Fragment and of Modal Logic With a Global Modality*, Advances in Modal Logic, 2008.

[5] T. PERKOV, M. VUKOVIĆ, *A bisimulation characterization for interpretability logic*, Logic Journal of IGPL, to appear

[6] B. TEN CATE, J. VAN BENTHEM, J. VÄÄNÄNEN, *Lindström theorems for fragments of first-order logic*, Logical Methods in Computer Science, 5 (2009), 1–27

[7] J. VAN BENTHEM, *A New Modal Lindström Theorem*, Logica Universalis, 1 (2007)

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

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