6TH INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2017

September 18 - 22, 2017
Dubrovnik, Croatia

Book of Abstracts

Course directors:

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

Book of Abstracts of the 6^{th} International Conference on Logic and Applications - LAP 2017, held at the Inter University Center Dubrovnik, Croatia, September 18 - 22, 2017.

LaTeX book of abstracts preparation and typesetting:

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

LAP 2017 Web site: `http://imft.ftn.uns.ac.rs/math/cms/LAP2017`
Maintained by Nenad Savić, University of Bern and University of Novi Sad

Contents

Sequent calculus as a programming language

Zena M. Ariola

University of Oregon

We will present and demonstrate the usefulness of the sequent calculus as a formal model of computation based on interactions between producers and consumers of results. This model leads to a better understanding of call-by-name evaluation by reconciling the conflicting principles of extensionality and weak-head evaluation, thus internalizing a known parametricity result. It allows one to explore two dualities of computation: the duality between call-by-name and call-by-value, and the duality between construction and deconstruction. This ultimately leads to a better linguistic foundation for co-induction as dual to induction. From a more practical point of view, the sequent calculus provides a useful inspiration for the design of intermediate languages.

This is joint work with Paul Downen, Philip Johnson-Freyd, Luke Maurer and Simon Peyton Jones

Acknowledgements

This work was supported by the National Science Foundation

References

[1] Paul Downen, Zena M. Ariola. *A Tutorial on Computational Classical Logic and the Sequent Calculus.* To appear in Journal of Functional Programming.

[2] Luke Maurer, Paul Downen, Zena M. Ariola, Simon Peyton Jones. *Compiling without continuations.* Programming Language Design and Implementation, 482-494 (PLDI 2017)

[3] Paul Downen, Philip Johnson-Freyd, Zena M. Ariola. *Call-by-name extensionality and confluence.* Journal of Functional Programming, Volume 27, 127-139 (JFP 2017)

[4] Paul Downen, Luke Maurer, Zena M. Ariola, Simon Peyton Jones. *Sequent calculus as an intermediate language.* International Conference on Functional Programming, 74-88 (ICFP 2016)

[5] Philip Johnson-Freyd, Paul Downen, Zena M. Ariola. *First call stacks: exploring head reduction.* Workshop on Continuations, 18-35 (WoC 2015)

[6] Paul Downen, Philip Johnson-Freyd, Zena M. Ariola. *Structures for structural recursion.* International Conference on Functional Programming, 127-139 (ICFP 2015)

[7] Paul Downen, Zena M. Ariola. *The Duality of Construction.* European Symposium on Programming, Volume 8410: 249-269 (ESOP 2014)

Secure channel coding scheme based on LDPC codes over the BEC

Aleksandra Arsić

Mathematical Institute SASA, Belgrade, Serbia

E-mail: aleksandra@mi.sanu.ac.rs

Keywords:
BEC, channel coding scheme, LDPC codes, QC-LDPC codes

Low density parity check (LDPC) codes were discovered by Gallager [1]. In last years, they have been the topic of significant research and attracted considerable attention due to their promising performance and the reasonable complexity. One of the most attractive class of LDPC codes for practical applications is the class of quasi-cyclic (QC) LDPC codes [3], [4], [5]. QC-LDPC codes have encoding advantage over other types of LDPC codes. They can be encoded using shift-registers in linear time, which permits low-complexity encoding [6]. These codes also decrease the memory for storage, because there is no need to store the complete parity check matrix. Instead, only the first column of circulant matrix is saved in memory. That provides reducing the key size [7].

The topic of this research is combining security and channel coding.Reasons for that are reduce the overall processing cost and providing a faster and more efficient implementation. Cryptosystem based on coding theory is secure, argument for that is because decoding process for linear code is NP-complete problem [8]. Benefits of this model are higher encryption/decryption speed and lower memory size for key. These schemes are also known like code-based cryptosystems. Idea is to use code that allows low computation complexity of the decoder and encoder, decreasing the key size and increasing information rate. We used a class of QC-LDPC codes which was describe in [9].

This research introduces code-based cryptosystem with two components. The first component is binary QC-LDPC code and the second one is binary erasure channel (BEC). After message was encoded by parity check matrix, it passed to the BEC and some bits have been deleted. Sender and receiver have the same deterministic procedure for determining if some bit will be deleted. Positions of deleted bits are known only to them. In that way, attacker has some binary vector but doesn't know the positions of removed bits. He is unable to reconstruct message.

There are a lot of techniques to design BEC and that will be a subject of

this presentation, also. It is important that chosen technique does not affect to key size significantly and to improved security of scheme. Although the attacker knows some part of the key, this cryptosystem is secure and that will be shown.

Acknowledgment

The research reported in the paper is supported by the Ministry of Education and Science of the Republic of Serbia, project III44006 (2011-2017).

References

[1] R.G. Gallager, "Low Density Parity Check Codes"; MIT Press: Cambridge, MA, USA, 1963

[2] Zongwang Li, Lei Chen, Lingqi Zeng, S. Lin and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes", in IEEE Transactions on Communications, vol. 54, no. 1, pp. 71-81, Jan. 2006.

[3] R. Michael Tanner, "On quasi-cyclic repeat-accumulate codes", i in Proc. 37th Allerton Conf. Communication, Control and Computing, Sep. 1999, pp. 249259.

[4] Heng Tang, Jun Xu, Yu Kou, S. Lin and K. Abdel-Ghaffar, "On algebraic construction of Gallager and circulant low-density parity-check codes", in IEEE Transactions on Information Theory, vol. 50, no. 6, pp. 1269-1279, June 2004.

[5] L. Chen, I. Djurdjevic and J. Xu, "Construction of quasicyclic LDPC codes based on the minimum weight codewords of Reed-Solomon codes", International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings., 2004, pp. 239

[6] Zongwang Li, Lei Chen, Lingqi Zeng, S. Lin and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes", in IEEE Transactions on Communications, vol. 54, no. 1, pp. 71-81, Jan. 2006.

[7] Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, Ayoub Otmani, "Reducing key length of the McEliece cryptosystem", Progress in Cryptology AFRICACRYPT 2009,Springer-Verlag, 2009 (LNCS, 5580), pp. 7797

[8] E. Berlekamp, R. McEliece and H. van Tilborg, "On the inherent intractability of certain coding problems", in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978.

[9] A. A. S. Afshar, T. Eghlidos and M. R. Aref, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes", in IET Communications, vol. 3, no. 2, pp. 279-292, February 2009.

Deduction rules for probabilized formulae

Marija Boričić[1]

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

Keywords:

inference rules, probability, soundness, completeness

We introduce a system of inference rules **NKprob** combining Gentzen's and Prawitz's approach to deductive systems, and Carnap's and Popper's treatment of probability in logic (see [1, 2]). This probability logic, based on classical propositional calculus (see [7, 8]), enables manipulating with propositions of the form $A[a, b]$ with the intended meaning that 'the probability c of truthfulness of a sentence A belongs to the interval $[a, b] \subseteq [0, 1]$'.

For each propositional formula A provable in classical logic, the probabilized formula $A[1, 1]$ is an axiom of the system **NKprob**. The system **NKprob** consists of inference rules covering each propositional connective by at least one introduction rule, and one elimination rule, with the best possible probability bounds. For instance, the rules treating implication are as follows:

implication:

$$\frac{A[a,b] \quad B[c,d]}{(A \to B)[\max(1-b,c), 1-a+d]}(I \to) \qquad \frac{A[a,b] \quad (A \to B)[c,d]}{B[a+c-1,d]}(E_1 \to)$$

$$\frac{B[a,b] \quad (A \to B)[c,d]}{A[1-d,1-c+b]}(E_2 \to)$$

An characteristic rule for probability logic is the additivity rule:

$$\frac{A[a,b] \qquad B[c,d] \qquad (A \wedge B)[e,f]}{(A \vee B)[a+c-f, b+d-e]}(ADD)$$

Also, we present two specific rules for our system, treating inconsistency:

$$\frac{\dfrac{[A[c_1,c_1]]}{A\emptyset} \quad \dfrac{[A[c_2,c_2]]}{A\emptyset} \cdots \dfrac{[A[c_m,c_m]]}{A\emptyset}}{A\emptyset}(I\emptyset) \qquad \frac{A\emptyset}{B[a,b]}(E\emptyset)$$

for any propositional formulae A and B, and any $a, b \in I = \{c_1, c_2, \ldots c_m\}$.

The models are defined as follows (see [3, 4, **?**, 6]):

Definition. Let For be the set of all propositional formulae and I a finite subset of reals $[0,1]$ closed under addition, containing 0 and 1. Then a mapping $p : \text{For} \to I$ will be an **NKprob**–*model* (or, simply, *model*), if it satisfies the following conditions:

(i) $p(\top) = 1$ and $p(\bot) = 0$;
(ii) if $p(A \wedge B) = 0$, then $p(A \vee B) = p(A) + p(B)$;
(iii) if $A \leftrightarrow B$ in classical logic, then $p(A) = p(B)$.

Our system is sound and complete with respect to the just described models.

References

[1] M. Boričić, *Hypothetical syllogism rule probabilized*, Bulletin of Symbolic Logic 20, No. 3, 2014, pp. 401–402, Abstract, Logic Colloquium 2012, University of Manchester, 12th-18th July 2012.

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

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

[4] H. Leblanc, B. C. van Fraassen, *On Carnap and Popper probability functions, The Journal of Symbolic Logic*, vol. 44 (1979), pp. 369–373.

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

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

[7] Z. Ognjanović, M. Rašković, *A logic with higher order probabilities*, Publications de l'Institut Mathématique, vol. 60 (74) (1996), pp. 1–4.

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

A probabilistic temporal logic with countably additive semantics

Dragan Doder
University of Belgrade, Faculty of Mechanical Engineering
dragan.doder@gmail.com
Zoran Ognjanović
Mathematical Institute of Serbian Academy of Sciences and Arts
zorano@mi.sanu.ac.rs

The study of temporal logics started with the seminal work of Arthur Prior [12]. Temporal logics are designed in order to analyze and reason about the way that systems change over time, and have been shown to be a useful tool in describing behavior of an agent's knowledge base, for specification and verification of programs, hardware, protocols in distributed systems etc. [1, 2]. In many practical situations the temporal information is not known with certainty. A typical example is formal representation of information about tracking moving objects with GPS systems, in the case in which the locations or the identities of the objects are not certainly known [5].

Many different tools are developed for representing, and reasoning with, uncertain knowledge. One particular line of research concerns the formalization in terms of probabilistic logic. After Nilsson [10] gave a procedure for probabilistic entailment which, given probabilities of premises, calculates bounds on the probabilities of the derived sentences, researchers from the field started investigation about formal systems for probabilistic reasoning. [3] provided a finitary axiomatization for reasoning about linear combinations of probabilities, and they proved weak completeness (every consistent formula is satisfiable). Their formulas are Boolean combinations of the expressions of the form $r_1 w(\alpha_1) + \ldots + r_n w(\alpha_n) \geq r_{n+1}$, where w is the probability operator and α_i's are propositional formulas. The semantics of the logic use finitely additive probabilities, since σ-additivity cannot be expressed by a formula of their language.

In this work, we extend the approach from [3]. We start with the propositional linear time logic (LTL) [4] with the "next" operator $\bigcirc$ and "until" operator U. The meaning of the formula $\bigcirc\alpha$ is "α holds in the next time instance", and $\alpha U \beta$ we read "α holds in every time instance until β holds". We apply the probabilistic operator w to the formulas of LTL and define probabilistic formulas using the linear combinations, like in [3]. In our logic there are two types of formulas, LTL formulas and probabilistic formulas, with the requirement that if an LTL formula is true, then its probability is equal to 1.

The main technical challenge in axiomatizing such a logic lies in the fact that the set of models of the formula $\alpha U \beta$ can be represented as a countable union of models of temporal formulas which are pairwise disjoint. As a consequence, finitely additive semantics is obviously not appropriate for such a logic, and we propose σ-additive semantics for the logic. On the other hand, expressing σ-additivity with an axiom would require infinite disjunctions, and the resulting logic would be undecidable. We shown in Section 3.1 that any finitary axiomatic system wouldn't be complete for the σ-additive semantics.

In order to overcome this problem, we axiomatize our language using infinitary rules of inference. Thus, in this work the term "infinitary" concerns the meta language only, i.e., the object language is countable and the formulas are finite, while only proofs are allowed to be infinite. We prove that our axiomatization is sound and strongly complete (every consistent set of formulas is satisfiable). We also prove that the logic is decidable, and we show that the satisfiability problem is $PSPACE$-complete, no harder then satisfiability for LTL.

There are several logics which combine time and probability in different ways [6, 7, 8, 9, 11, 13]. However, to the best of our knowledge, this is the first complete axiomatization for the σ-additive probabilistic semantics.

Acknowledgements

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

References

[1] Allen E. Emerson. Temporal and modal logic. pages 995–1072, 1990.

[2] E. Allen Emerson. Automated temporal reasoning about reactive systems. In *Logics for Concurrency - Structure versus Automata (8th Banff Higher Order Workshop, August 27 - September 3, 1995, Proceedings)*, pages 41–101, 1995.

[3] Ronald Fagin, Joseph Y. Halpern, and Nimrod Megiddo. A logic for reasoning about probabilities. *Inf. Comput.*, 87(1/2):78–128, 1990.

[4] Dov M. Gabbay, Amir Pnueli, Saharon Shelah, and Jonathan Stavi. On the temporal basis of fairness. In *Conference Record of the Seventh Annual ACM Symposium on Principles of Programming Languages, Las Vegas, Nevada, USA, January 1980*, pages 163–173, 1980.

[5] John Grant, Francesco Parisi, Austin Parker, and V. S. Subrahmanian. An agm-style belief revision mechanism for probabilistic spatio-temporal logics. *Artif. Intell.*, 174(1):72–104, 2010.

[6] Dimitar P. Guelev. Probabilistic neighbourhood logic. In *Formal Techniques in Real-Time and Fault-Tolerant Systems, 6th International Symposium, FTRTFT 2000, Pune, India, September 20-22, 2000, Proceedings*, pages 264–275, 2000.

[7] Peter Haddawy. A logic of time, chance, and action for representing plans. *Artif. Intell.*, 80(1-2):243–308, 1996.

[8] Joseph Y. Halpern and Riccardo Pucella. A logic for reasoning about evidence. *J. Artif. Intell. Res. (JAIR)*, 26:1–34, 2006.

[9] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Asp. Comput.*, 6(5):512–535, 1994.

[10] Nils J. Nilsson. Probabilistic logic. *Artif. Intell.*, 28(1):71–87, 1986.

[11] Zoran Ognjanovic. Discrete linear-time probabilistic logics: Completeness, decidability and complexity. *J. Log. Comput.*, 16(2):257–285, 2006.

[12] Arthur Prior. *Time and Modality.* Clarendon Press, Oxford, January 1957.

[13] Paulo Shakarian, Austin Parker, Gerardo I. Simari, and V. S. Subrahmanian. Annotated probabilistic temporal logic. *ACM Trans. Comput. Log.*, 12(2):14, 2011.

On the Computational Complexity of the Discrete Pascal Transform

Dušan B. Gajić[1], Radomir S. Stanković[2]

[1] *University of Novi Sad, Faculty of Technical Sciences, Dept. of Computing and Control*
Trg Dositeja Obradovića 6, 21000 Novi Sad, Serbia
[2] *University of Niš, Faculty of Electronic Engineering, Dept. of Computer Science*
Aleksandra Medvedeva 14, 18000 Niš, Serbia
E-mail: [1]dusan.gajic@uns.ac.rs, [2]radomir.stankovic@gmail.com

Keywords:
Discrete Pascal transform, spectral transforms, computational complexity, fast algorithms, parallel computing, GPU computing.

In this talk, we discuss the computational complexity of different algorithms for computing the discrete Pascal transform (DPT) [1].

The DPT is a spectral transform proposed in 2005 [1], but it is based on the concept of the Pascal's triangle which has been known for centuries [2, 10]. The DPT was introduced by an ad hoc multiplication with -1 of every other column of the Pascal's matrix [1]. The applications of the DPT are found in digital image processing [7], digital filter design [11, 12], pattern recognition [6], digital watermarking [9], and related areas.

However, practical applications of the DPT are limited by the $\mathcal{O}(N^2)$ complexity of best current algorithms for its computation (where N is the size of the processed function) [4, 8, 14]. In this talk, we further elaborate on the computational features of a method for the fast computation of the DPT, proposed in [3], which is characterized by an $\mathcal{O}(N \log N)$ asymptotical time complexity. We also show that the considered approach is especially well-suited for highly-parallel computation on graphics processing units (GPUs) [3].

The discussed method for the efficient computation of the DPT is based on a modification of the factorization of the Pascal's matrix which was proposed by Kailath and Sayed [5]. We modify the before-mentioned factorization by using the Hadamard product with the vector consisting of ± 1 integers to convert the Pascal's matrix into the DPT matrix. Using this algorithm, the DPT matrix is factorized into a product of three matrices with special structure - two diagonal matrices and a Toeplitz matrix. The Toeplitz matrix is further embedded into a circulant matrix of order $2N$ [15]. The diagonalization of the circulant matrix by the Fourier matrix permits the use of the fast Fourier transform (FFT) for

performing computations [13, 15, 16]. This leads to an algorithm with the asymptotical time complexity of $\mathcal{O}(N \log N)$ [15, 16].

As a result, the discussed method can significantly extend the practical applicability of the discrete Pascal transform.

Acknowledgment

The research reported in the paper is partly supported by the Ministry of Education and Science of the Republic of Serbia, projects ON174026 (2011-2017) and III44006 (2011-2017).

References

[1] Aburdene, M. F., Goodman, T. J., "The discrete Pascal transform and its applications", *IEEE Signal Proc. Letters*, Vol. 12, No. 7, 2005, 493–495.

[2] Edwards, A. W. F., *Pascal's Arithmetical Triangle: The Story of a Mathematical Idea*, Johns Hopkins University Press, 2002.

[3] Gajić, D. B., Stanković, R. S., "Fast Computation of the Discrete Pascal Transform", in *Proc. 2017 IEEE* 47^{th} *Intl. Symp. Multiple-Valued Logic*, Novi Sad, Serbia, May, 22-24, 2017, 149–154.

[4] Goodman, T. J., Aburdene, M. F., "A hardware implementation of the discrete Pascal transform for image processing", *Proc. SPIE* 6064, *Image Processing: Algorithms and Systems, Neural Networks, and Machine Learning*, 60640H, February 16, 2006.

[5] Kailath, T., Sayed, A. H., *Fast Reliable Algorithms for Matrices with Structure*, SIAM, Philadelphia, USA, 1999.

[6] Li, B., Shen, J., "Range-image-based calculation of three-dimensional convex object moments", *IEEE Trans. Robot. Autom.*, Vol. 9, No. 4, 1993, 484–490.

[7] Lin, R. S., "A simple edge detection method by discrete Pascal transformation", Research Report, Suang Chuang University, Taiwan, 2006.

[8] Lv, X. G., Huang, T. Z., Ren, Z. G., "A new algorithm for linear systems of the Pascal type", *J. Computational and Applied Mathematics*, Vol. 225, 2009, 309–315.

[9] Martin, J. R. H., Kutter, M., "Information retrieval in digital watermarking", *IEEE Commun. Mag.*, Vol. 39, No. 8, 2001, 110–116.

[10] Moraga, C., Stanković, R. S., Stanković, M., "The Pascal Triangle (1654), the Reed-Muller-Fourier Transform (1992), and the Discrete Pascal Transform (2005)" in *Proc. 2016 IEEE* 46^{th} *Intl. Symp. Multiple-Valued Logic*, Sapporo, Japan, May, 18-20, 2016, 229–234.

[11] Pšenička, B., Garcia-Ugalde, F., "Z transform from lowpass to bandpass by Pascal matrix", *IEEE Signal Processing Letters*, Vol. 11, No. 2, 2004, 282–284.

[12] Pšenička, B., Garcia-Ugalde, F., Herrera-Camacho, A., "The bilinear Z transform by Pascal matrix and its application in the design of digital filters", *IEEE Signal Processing Letters*, Vol. 9, No. 11, 2002, 368–370.

[13] Rao, K. R., Kim, D. N., Hwang, J. J., *Fast Fourier Transform: Algorithms and Applications*, Springer, 2010.

[14] Skodras, A. N., "Fast discrete Pascal transform", *Electronics Letters*, IET, UK, Vol. 42, No. 23, 2006, 1367–1368.

[15] Tang, Z., Duraiswami, R., Gumerov, N., "Fast algorithms to compute matrix-vector products for Pascal matrices", Technical Reports from the University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland, USA, UMIACS-TR-2004-08, 2004.

[16] Van Loan, C., *Computational Frameworks for the Fast Fourier Transform*, Society for Industrial Mathematics, 1992.

Sound and complete subtyping on intersection and union types

Silvia Ghilezan

University of Novi Sad, Mathematical Institute SANU, Serbia

The notion of subtyping has gained an important role both in theoretical and applicative domains: in lambda and concurrent calculi as well as in programming languages. The soundness and the completeness, together referred to as the preciseness of subtyping, can be considered from two different points of view: denotational and operational. The former preciseness is based on the denotation of a type which is a mathematical object that describes the meaning of the type in accordance with the denotations of other expressions from the language. The latter preciseness has been recently developed in [3] with respect to type safety, i.e. the safe replacement of a term of a smaller type when a term of a bigger type is expected.

We present the technique for formalising and proving operational preciseness of the subtyping relation in the setting of a concurrent lambda calculus with intersection and union types given in [1]. An overview of preciseness of subtyping in other frameworks will be given ([2]).

This is a joint work with Mariangiola Dezani-Ciancaglini.

Acknowledgements

This work was partly supported by the Serbian Ministry of Education, Science and Technological Development under the projects ON174026 and III44006.

References

[1] Mariangiola Dezani-Ciancaglini, Silvia Ghilezan. *Preciseness of subtyping on intersection and union types.* Typed Lambda Calculus and Application, RTA and TLCA 2014, Lecture Notes in Computer Science 8560: 194-207 (2014).

[2] Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, Svetlana Jaksic, Jovanka Pantovic, and Nobuko Yoshida. *Denotational and Operational Preciseness of Subtyping: A Roadmap.* Theory and Practice of Formal Methods, Lecture Notes in Computer Science 9660: 155-172 (2016).

[3] Jeremy Blackburn, Ivory Hernandez, Jay Ligatti, and Michael Nachtigal. *Completely Subtyping Iso-recursive Types.* Technical Report CSE-071012, University of South Florida, (2012).

Proving Properties of Peer-to-Peer Protocols using ASMs Formalism - An Overview

Paola Glavan, Bojan Marinković, Zoran Ognjanović

Our aim is to describe how to use Abstract State Machine (ASM) [5, 9, 10] in specification of Peer-to-Peer protocols, with special emphasis to Chord and Synapse protocol. We will also show how to prove correctness properties of the Chord protocol and several properties of Synapse protocol.

We decided to use ASM framework for specification of Peer-to-Peer protocols because of its simplicity (which is unique), and the freedom it offers the practitioners to choose for each problem an appropriate combination of concepts, techniques and notations, which are integrated by the framework in a coherent way as elements of a uniform mathematical background. The ASM method enables us to base the foundation for a reliable software engineering discipline on standard mathematics, avoiding the introduction of complicated specification languages and theories of language semantics.

As is characteristic for mathematical disciplines, the ASM method is not bound by the straightjacket of a particular formal language, but allows one to freely use any standard algorithmic and mathematical notation. The only condition to use any useful description techniques is a mathematically rigorous definition of its meaning.The ASM method allows one the coherent separation and integration of defining a model and proving of model properties.

ASMs are versatile machines which are able to simulate arbitrary algorithms in a direct and essentially coding-free way. Here the term algorithm is taken in a broad sense including programming languages, architectures, distributed and real-time protocols, etc. The simulator is not supposed to implement the algorithm on a lower abstraction level; the simulation should be performed on the natural abstraction level of the algorithm, and thus enables us to skip proof of the correctness of the formalization with respect to the algorithm. Also, a vast literature on ASMs shows how to model closely and faithfully real complex systems and how to use models in order to verify their properties (see for example [5, 12], Bakery algorithm [4], Rail road crossing problem [11], Kerberos algorithm [3], Java formalization [7], [8], a special issue devoted to the method [6], etc).

ASMs constitute a computation model on structures. The program of an ASM is - like the program of a Turing machine - the description of how to modify the current configuration of a machine in order to obtain a possi-

ble successor configuration. The main difference between ASM and Turing machine is that the ASM states are mathematical structures (first order structures) rather than strings. ASM preform computation on structures, in the sense that they obtain a structure as input, modify this structure step by step, and output the resulting structure if they reach a halting state. The fact that ASMs operate on structures rather then on strings has an important consequence: the ASM computational model is more flexible then standard computational models in theoretical computer science.

In the talk we will consider how to model Chord and Synapse protocol with ASM. The Chord protocol [16, 17, 18] is one of the first, simplest and most popular distributed hash table (DHT). DHT provides a lookup service similar to a hash table; $\langle key, value \rangle$ pairs are stored in a DHT, and any participating peer can efficiently retrieve the value associated with a given key. The formalization concerns Chord actions that maintain ring topology and manipulate distributed keys. We define a minimal set of deterministic constraints and prove the correctness of the Chord protocol.

The Synapse protocol is a scalable protocol designed for information retrieval over inter-connected heterogeneous overlay networks. In this talk, we show a formal description of Synapse using the Abstract State Machines framework. The formal description pertains to Synapse actions that manipulate distributed keys. Based on this formal description, we present results concerning the expected exhaustiveness for a number of scenarios and systems maintained by the Synapse protocol, and provide comparisons to the results of the corresponding simulations and experiments. We show that the predicted theoretical results match the obtained experimental results, and give recommendations on the design of systems using Synapse.

References

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

[2] E. Börger, Y. Gurevich, D. Rosenzweig. *The Bakery Algorithm: Yet Another Specification And Verification.*, In *Specification and Validation Methods*, Oxford University Press, pages 231–243, 1995.

[3] E. Börger, R. Stärk. *Abstract State Machines A Method for High-Level System Design and Analysis.*, Springer-Verlag, 2003.

[4] E. Börger, A. Prinz. *Quo Vadis Abstract State Machines?* In *Journal of Universal Computer Science*, vol. 14, no. 12, pages 1921–1928, 2008.

[5] M. Botinčan, P. Glavan, D. Runje. *Distributed Algorithms.A Case Study of the Java Memory Model.* In *Proc. of the 14th Int. ASM Workshop*(ASM 2007), 2007.

[6] M. Botinčan, P. Glavan, D. Runje. *Verification of causality requirements in Java memory model is undecidable PPAM.* In *Parallel Processing and Applied Mathemat-*

ics 8th International Conference, Wroclaw, Poland, September 13-16, 2009, Part II, LNCS 6068, 62 – 67, 2010.

[7] Y. Gurevich. *Evolving Algebras 1993: Lipari Guide.* In *Specification and Validation Methods*, Oxford University Press, pages 9–36, 1995.

[8] Y. Gurevich. *Sequential Abstract State Machines capture Sequential Algorithms.* In *ACM Transactions on Computational Logic*, Volume 1, Number 1, pages 77–111, 2000.

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

[10] L. Liquori, C. Tedeschi, L. Vanni, F. Bongiovanni, V. Ciancaglini, B. Marinković. *Synapse: A Scalable Protocol for Interconnecting Heterogeneous Overlay Networks.* In *Networking 2010*, Lecture Notes in Computer Science, vol. 6091 (p. 410), pages 67–82, 2010.

[11] B. Marinkovic, V. Ciancaglini, Z. Ognjanovic, P. Glavan, L. Liquori, P. Maksimovic. *Analyzing the Exhaustiveness of the Synapse Protocol.* In *Peer-to-Peer Networking and Applications*, 8(5), p. 793 – 806, doi:10.1007/s12083-014-0293-z, 2015.

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

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

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

[15] W. Reisig. *The Expressive Power of Abstract-State Machines.* In *Computing and Informatics*, vol. 22, pages 209 – 219, 2003.

[16] P. Zave. *Using lightweight modeling to understand Chord.* In ACM SIGCOMM Computer Communication Review, Vol. 42, Issue 2, pages 50–57, April 2012.

[17] V. Ciancaglini, L. Liquori, L. Vanni. *CarPal: interconnecting overlay networks for a community-driven shared mobility.*, in *Trustworthy Global Computing 2010.*

[18] L. Liquori, C. Tedeschi, L. Vanni, F. Bongiovanni, V. Ciancaglini and B. Marinković. *Synapse: A Scalable Protocol for Interconnecting Heterogeneous Overlay Networks.* In Networking 2010, Lecture Notes in Computer Science, vol. 6091 (p. 410), pages 67–82, 2010.

[19] V. Ciancaglini, G.N. Hoang and L. Liquori. *Towards a Common Architecture to Interconnect Heterogeneous Overlay Networks.* In ICPADS 2011, IEEE, pages 817 – 822, 2011.

[20] V. Ciancaglini, G.N. Hoang, P. Maksimović and L. Liquori. *An Extension and Cooperation Mechanism for Heterogeneous Overlay Networks.* In Networking 2012, Lecture Notes in Computer Science, vol. 7291, pages 10 – 18, 2012.

A Probability Logic for Reasoning About Quantum Observations

Angelina Ilić Stepić[1] and Zoran Ognjanović[1]

[1]Mathematical Institute of the Serbian Academy of Sciences and Arts

Keywords:

Quantum logic, Modal logic, Quantum Observations.

In this paper we present the logic QLP suitable for reasoning about quantum observations. The notion of measurement can be expressed using the modal operator $\Box$, so that, instead of non-distributive structures (i.e., non-distributive lattices), it is possible to relay on classical logic extended with the corresponding modal laws for the modal logic **B**. Using formulas of the form $\Box\varphi$, it is possible to overcome the well known "non distributivity problem" of quantum mechanics.

QLP extends the modal logic **B** with probability formulas of the form $CS_{z_1,\rho_1;\ldots;z_m,\rho_m}\Box\Diamond\alpha$. The meaning of the formula $CS_{z_1,\rho_1;\ldots;z_m,\rho_m}\Box\Diamond\alpha$ is related to some observable O and some world (vector) w. If Δ is a subspace related to measuring the observable O, a is an eigenvalue of O, and $w_1, \ldots, w_m$ is the chosen base of eigenvectors that correspond to the eigenvalue a, then $\Box\Diamond\alpha$ means "It is measured that $O = a$", while $CS_{z_1,\rho_1;\ldots;z_m,\rho_m}\Box\Diamond\alpha$ means "$w = c_1 \cdot w_1 + \ldots + c_m \cdot w_m$ for some $c_i \in \mathbf{C}$ such that $\|c_1 - z_1\| \leq \rho_1$, $\ldots \|c_m - z_m\| \leq \rho_m$, and the probability of obtaining a while measuring O in the state w is equal to $\Sigma_{i=1}^{m}\|c_i\|^2$".

Formulas are interpreted in reflexive and symmetric Kripke models equipped with probability distributions over possible worlds. We give an infinitary axiom system which contains axioms and rules for probabilistic reasoning, and prove the corresponding soundness and strong completeness theorems. We show that the logic QLP is decidable.

References

[1] Nonson S. Yanofsky, Mirco A. Mannucci. Quantum computing for computer scientists. Cambridge university press. 2008.

[2] R.I. Goldblatt, *Semantic analysis of orthologic*, Journal of Philosophical Logic, Vol. 3, No. 1/2, pp. 19–35., 1974.

[3] Rohit Chadha, Paulo Mateus, Am lcar Sernadas and Cristina Sernadas, *Extending Classical Logic for Reasoning about Quantum Systems*, Handbook of quantum logic and quantum structures, pp. 325–371, 2009.

[4] Angelina Ilić-Stepić, Zoran Ognjanović, *Complex valued probability logics*, Publications de l'Institut Mathematique 95, pp.73–86 2014.

[5] Simon Kramer, *Quantum Logic as Classical Logic*, arXiv:1406.3526, 2015.

[6] A. Sernadas, J. Rasga, C. Sernadas, L. Alcace, A.B. Henriques, *Probabilistic logic of quantum observations*, arXiv:1607.08369v1, 2016.

[7] Ron van der Meyden, Manas Patra, *A Logic for Probability in Quantum Systems*, Lecture Notes in Computer Science, Volume 2803, pp. 427–440, 2003.

[8] Nonson S. Yanofsky, Mirco A. Mannucci, *Quantum computing for computer scientists*,Cambridge university press. 2008.

Starlike neighbourhoods and computability

Zvonko Iljazović and Lucija Validžić

University of Zagreb, Croatia

Keywords:

computable topological space, computable set, semicomputable set

A compact subset of $\mathbb{R}^n$ is computable if it can be effectively approximated by a finite set of points with rational coordinates with arbitrary precision. Let $f : \mathbb{R}^n \to \mathbb{R}$ be a computable function such that $f^{-1}(\{0\})$ is a compact set. Now the question is, is this set computable, i.e. is the set of solutions to the equation $f(x) = 0$ necessarily a computable set? The answer to this question is negative in general, but some topological properties of the set $f^{-1}(\{0\})$ can imply its computability.

It can be shown that a compact set $S \subseteq \mathbb{R}^n$ is a set of zero-points of some computable function if and only if we can effectively enumerate all finite unions of rational balls which cover S. This characterisation gives us a clear topological property of these sets and allows us to investigate sets which have the same property, but in more general ambient spaces. These spaces are computable topological spaces and semicomputable sets are the generalisation of previously mentioned compact sets of zero-points.

We show how notion of computability can be extended to topological spaces and investigate the conditions under which the implication

$$S \text{ semicomputable } \Rightarrow \ S \text{ computable}$$

holds in a computable topological space. In this study we examine the notion of local computable enumerability and concentrate especially on sets which have topological type of 1-polyhedron.

References

[1] Z. Iljazović, L. Validžić, *Computable neighbourhoods of points in semicomputable manifolds*, Annals of Pure and Applied Logic, 168(4):840–859, 2017.

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

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

[4] T. Kihara, *Incomputability of Simply Connected Planar Continua*, Computability 1(2), pp. 131–152, 2012.

[5] J.S. Miller, *Effectiveness for Embedded Spheres and Balls*, Electronic Notes in Theoretical Computer Science 66, pp. 127–138, 2002.

[6] M. Pour-El, I. Richards, *Computability in Analysis and Physics*, Springer-Verlag, Berlin-Heielberg-New York, 1989.

[7] E. Specker, *Der Satz vom Maximum in der rekursiven Analysis*, Constructivity in Mathematics (A. Heyting, ed.), North Holland Publ. Comp., Amsterdam, pp. 254–265, 1959.

[8] K. Weihrauch, *Computable Analysis*, Springer, Berlin, 2000.

Dense Time Multiset Rewriting Model in the Verification of Time-Sensitive Distributed Systems

Max Kanovich[1,5], Tajana Ban Kirigin[2], Vivek Nigam[3], Andre Scedrov[4,5] and Carolyn Talcott[6]

[1]University College London, UK
[2]University of Rijeka, HR
[3]Federal University of Paraíba, Brazil
[4]University of Pennsylvania, USA
[5]National Research University Higher School of Economics, Russian Federation
[6]SRI International, USA

Keywords:

Multiset Rewriting, Distributed Systems, Computational Complexity, Maude, Real Time

We propose a Multiset Rewriting language with explicit dense (real) time for specifying and analysing Time-Sensitive Distributed Systems (TSDS). Discrete time models for the verification of TSDSes were introduced in [2]. Due to the foundational differences between models with discrete and models with real time [1], in the formal analysis of properties, such as security properties of Cyber-Physical Systems, some phenomena can only be captured by real time models.

In order to specify dense time, we follow [1] in formalizing dense time in the multiset rewriting framework. We investigate real time TSDSes and their relevant properties and introduce adequate notions of time sampling and compliant traces.

Properties of TSDSes are often specified using explicit time constraints which must be satisfied by the system *perpetually*. For example, drones carrying out the surveillance of some area must always have *recent pictures* Possible environment interference (*e.g.*, winds) are taken into account, *e.g.*, autonomous drones achieve goals under possible interference of winds. Hence, we consider infinite traces over dense time domains in which goals are perpetually satisfied and which have some good properties with relation to time. Namely, we are interested in infinite traces which represent infinite periods

of time where only a finite number of actions can be applied in any bounded time interval.

One of the main challenges in the transition from discrete to dense time models of TSDSes is the additional non-determinism in the dense time model provided by the choice of a positive real value ε in time advancement rule, $Time@T \to Time@(T + \varepsilon)$, which may lead to Zeno type phenomena.

We investigate properties of *realizability* (some trace is good) and *survivability* (where, in addition, all admissible traces are good) in models with dense time. We prove that for the class of *progressive timed systems* (PTS) both the realizability and the survivability problems have the same complexity as in the discrete time model case, both for infinite time versions as well as for the bounded time versions of the problems.

References

[1] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. *Discrete vs. dense times in the analysis of cyber-physical security protocols*, In 4th Conference on Principles of Security and Trust (POST), pages 259–279, 2015.

[2] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott, *Timed Multiset Rewriting and the Verification of Time-Sensitive Distributed Systems*, 14th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), 2016.

[3] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott, *Timed Multiset Rewriting and the Verification of Time-Sensitive Distributed Systems*, arXiv:1606.07886

On the Accuracy of Formal Verification of Selective Defenses for TDoS Attacks

Marcilio O. O. Lemos[1], Yuri Gil Dantas[2], Iguatemi E. Fonseca[1] and Vivek Nigam[1]

[1]Federal University of Paraíba, João Pessoa, Brazil.
[2]Technische Universität Darmstadt, Darmstadt, Germany

Telephony Denial of Service (TDoS) attacks target telephony services, such as Voice over IP (VoIP), not allowing legitimate users to make calls. There are few defenses that attempt to mitigate TDoS attacks, most of them using IP filtering, with limited applicability. In our previous work, we proposed to use selective strategies for mitigating HTTP Application-Layer DDoS Attacks demonstrating their effectiveness in mitigating different types of attacks. Developing such types of defenses is challenging as there are many design options, e.g., which dropping functions and selection algorithms to use. Our first contribution is to demonstrate both experimentally and by using formal verification that selective strategies are suitable for mitigating TDoS attacks. We used our formal model to help decide which selective strategies to use with much less effort than carrying out experiments. Our second contribution is a detailed comparison of the results obtained from our formal models and the results obtained by carrying out experiments. We demonstrate that formal methods is a powerful tool for specifying defenses for mitigating Distributed Denial of Service attacks allowing to increase our confidence on the proposed defense before actual implementation.

References

[1] Cyber Threat Bulletin: Boston Hospital TDoS Attack, http://voipsecurityblog.typepad.com/files/cyber-threat-bulletin-13-06-boston-hospital-telephony-denial-of-service-attack.pdf, accessed: 2015-27-09.

[2] TDoS – Extortionists Jam Phone Lines of Public Services Including Hospitals, https://nakedsecurity.sophos.com/pt/2014/01/22/tdos-extortionists-jam-phone-lines-of-public-services-including-hospitals/, accessed: 2015-27-09.

[3] Situational Advisory: Recent Telephony Denial of Services (TDoS) Attacks, http://voipsecurityblog.typepad.com/files/ky-fusion_tdos_3-29-13-2.pdf/, accessed: 2015-27-09.

[4] Y. G. Dantas, V. Nigam, I. E. Fonseca, A Selective Defense for Application Layer DDoS Attacks, in: JISIC 2014, 2014, pp. 75–82.

[5] The Surging Threat of Telephony Denial of Service Attacks, http://voipsecurityblog.typepad.com/files/tdos_paper_4-11-13.pdf.

[6] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, C. Talcott, All About Maude: A High-Performance Logical Framework, Vol. 4350 of LNCS, Springer, 2007.

[7] K. Sen, M. Viswanathan, G. Agha, On Statistical Model Checking of Stochastic Systems, in: CAV, 2005, pp. 266–280.

[8] M. AlTurki, J. Meseguer, PVeStA: A Parallel Statistical Model Checking and Quantitative Analysis Tool, in: CALCO, 2011, pp. 386–392.

[9] A. Lipowski, D. Lipowska, Roulette-wheel selection via stochastic acceptance, CoRR abs/1109.3627.

[10] T. Blickle, L. Thiele, A Mathematical Analysis of Tournament Selection, in: Proceedings of the 6th International Conference on Genetic Algorithms, San Francisco, CA, USA, 1995, pp. 9–16.

[11] L. Brown, N. Gans, A. Mandelbaum, A. Sakov, H. Shen, S. Zeltyn, L. Zhao, Statistical Analysis of a Telephone Call Center: A Queueing-Science Perspective, Journal of the American Statistical Association 100 (2005) 36–50.

[12] P. Galiotos, T. Dagiuklas, S. Kotsopoulos, Call-Level VoIP Traffic Modelling Based on Data from a Real-Life VoIP Service Provider, in: Globecom Workshops, 2015, pp. 1–7.

[13] I. Digium, "SAsterisk Private Branch eXchange", http://www.asterisk.org/, accessed: 2015-09-28 (2015).

Decidability and complexity of some interpretability logics

Luka Mikec[1], Tin Perkov[2] and Mladen Vuković[3]

[1]University of Rijeka, Department of Mathematics
[2]University of Zagreb, Faculty of Teacher Education
[3]Department of Mathematics, University of Zagreb

Keywords:

interpretability logic, decidability, complexity

The usual way to prove decidability of a modal logic with relational (Kripke-style) semantics is to prove it has the finite model property. Interpretability logics are usually interpreted on classes of Veltman models, or generalized Veltman models, which are both extensions of Kripke models.

We will describe an approach to proving the finite model property by defining a certain filtration of generalized Veltman models. We use this approach to prove decidability of the logic ILM_0 and ILW*.

We also study computational complexity of logics based on Veltman models. We prove that the logic IL is in PSPACE; and since it was already known to be PSPACE-hard, we conclude that it is PSPACE-complete. We will comment on complexity of some other interpretability logics with finite model property.

References

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

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

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

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

[5] A. Chagrov, M. Zakharyaschev, *Modal Logic*, Clarendon Press, Oxford, 1997.

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

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

[8] D.H.J. de Jongh and F. Veltman. Modal completeness of ILW, In *Essays dedicated to Johan van Benthem on the occasion of his 50th birthday*, J. Gerbrandy et al. eds., Amsterdam University Press, 1999.

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

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

[11] T.A. Hakoniemi, J.J. Joosten. Labelled tableaux for interpretability logics. In *Liber Amicorum Alberti*, J. van Eijck et al. eds., pp. 141–154. College Publications, 2016.

[12] G. Japaridze, D.H.J. de Jongh. The logic of provability. In *Handbook of Proof Theory*, S.R. Buss, ed., pp. 475–546. Elsevier, 1998.

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

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

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

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

[17] V. Shehtman. Filtration via bisimulation. In *Advances in modal logic, Volume 5*, R. Schmidt et al. eds., pp. 289–308. King's College Publications, 2005.

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

[19] V. Švejdar. Some independence results in interpretability logic. *Studia Logica*, **50**, 29–38, 1991.

[20] A. Visser. An overview of interpretability logic. In *Advances in modal logic, Volume 1*, M. Kracht et al. eds., pp. 307–359. CSLI Publications, 1998.

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

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

[23] M. Vuković. Some correspondences of principles in interpretability logic. *Glasnik Matematički*, **31(51)**, 193—200, 1996.

[24] M. Vuković. The interpretability logic ILF. *Mathematical Communications*, **2**, 205–210, 1997.

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

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

A Proof Theory for Model Checking: An Abstract

Dale Miller
Inria and LIX, École Polytechnique

While model checking has often been considered as a practical alternative to building formal proofs, we argue here that the theory of sequent calculus proofs can be used to provide an appealing foundation for model checking. Since the emphasis of model checking is on establishing the truth of a property in a model, we rely on the proof theoretic notion of additive inference rules, since such rules allow provability to directly describe truth conditions. Unfortunately, the additive treatment of quantifiers requires inference rules to have infinite sets of premises and the additive treatment of model descriptions provides no natural notion of state exploration. By employing a focused proof system, it is possible to construct large scale, synthetic rules which qualify as additive although they are built using some multiplicative inferences. These additive synthetic rules—essentially rules built from the description of a model—allow a direct treatment of state exploration. This proof theoretic framework provides a natural treatment of reachability and non-reachability problems, as well as tabled deduction, bisimulation, and winning strategies. [This work is joint with Quentin Heath.]

References

[1] D. Baelde and D. Miller. Least and greatest fixed points in linear logic. In N. Dershowitz and A. Voronkov, editors, LPAR 2007, LNCS 4790, pages 92–106, 2007. doi: 10.1007/978-3-540-75560-9_9.

[2] Z. Chihani, D. Miller, and F. Renaud. A semantic framework for proof evidence. *Journal of Automated Reasoning*, 2016. doi: 10.1007/s10817-016-9380-6.

[3] Q. Heath and D. Miller. A framework for proof certificates in finite state exploration. In C. Kaliszyk and A. Paskevich, editors, *Proceedings of the Fourth Workshop on Proof eXchange for Theorem Proving*, EPTCS 186, pages 11–26, August 2015. doi: 10.4204/EPTCS.186.4

[4] Q. Heath and D. Miller. A proof theory for model checking: An extended abstract. In I. Cervesato and M. Fernández, editors, *Proceedings Fourth*

International Workshop on Linearity (LINEARITY 2016), EPTCS 238, January 2017. doi: 10.4204/EPTCS.238.1

Constructive Semigroups with Apartness: Foundations of the Order Theory

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

Siniša Crvenković,
Department of Mathematics and Informatics, University of Novi Sad, Serbia
e-mail: sima@sbb.rs

Branislav M. Randjelović
Faculty of Electronic Engineering, University of Niš, Serbia
branislav.randjelovic@elfak.ni.ac.rs

Keywords: Set with apartness, semigroup with apartness, coequivalence, cocongruence.

The theory of constructive semigroups with apartness are a **new approach** to semigroup theory, and not a new class of semigroups. Of course, our work is partly inspired by classical semigroup theory, but, on the other hand, it is distinguished from it by two significiant aspects: first, we use intuitionistic logic rather than classical, secondly, our work is based on the notion of apartness (between elements, elements and sets). Here, the focus is on E. Bishop's approach to constructive mathematics (**BISH**), [2]. Constructive algebra is (relatively) old discipline developed among others by L. Kronecker, van der Waerden, A. Heyting, [6], [7]. Following [1], the principal novelty in treating basic algebraic structures constructively is that apartness becomes a fundamental notion, i.e. one axiomatizes rings, groups, and fields with apartness.

Following [2], to define a set S we have to give a property that enables us to construct members of S and to describe the equality between elements of S. We will consider a set S as endowed with a prescribed equivalence relation $=$, called the *equality* of S. Furthermore, we will be interested only in properties $P(x)$ which are *extensional* in the sense that for all $x_1, x_2 \in S$ with $x_1 = x_2$, $P(x_1)$ and $P(x_2)$ are equivalent. Let $(S, =)$ be a nonempty set (i.e. we can construct an element of S). By an **apartness** on S we mean a binary relation $\#$ on S which satisfies the axioms of irreflexivity, symmetry and cotransitivity: $\neg(x \# x)$; $x \# y \Rightarrow y \# x$; $x \# z \Rightarrow \forall_y (x \# y \vee y \# z)$. Then $(S, =, \#)$ is called *a set with apartness*. A tuple $(S, =, \#, \cdot)$ is a **semigroup with apartness** with $(S, =, \#)$ as a set with apartness, $\cdot$ an associative binary operation on S which is strongly extensional, i.e. $\forall_{a,b,x,y \in S} (a \cdot x \# b \cdot y \Rightarrow (a \# b \vee x \# y))$. As it is shown in [3], apartness does

not have to be tight. An important result from [4] is **constructive version of Cayley's theorem** for semigroups with apartness.

Theorem 0.1 *Every semigroup with apartness se-embeds into the semigroup of all strongly extensional self-maps on a set.*

Presence of apartness implies appearence of different types of substructures connected to it. Some of these substructures, and, especially, their role in foundations of the order theory for semigroup with apartness are the main objectives of this paper. Some basic concepts of sets and semigroups with apartness such as special subsets and special orders as well as some of our basic results in connection with them will be given.

Let $\bowtie$ be a relation between an element $x \in S$ and a subset Y of S defined by $x \bowtie Y \Leftrightarrow \forall_{y \in Y}(x \# y)$. A subset Y of S has two natural complementary subsets:

– *the logical complement* of Y: $\neg Y = \{x \in S : x \notin Y\}$;

– *apartness complement* of Y: $\sim Y = \{x \in S : x \bowtie Y\}$.

The properties of $\#$ ensures that, in general, $\sim Y \subseteq \neg Y$. A subset T of S is

– a *detachable* (*d-subset*) in S: $\forall_{x \in S}\,(x \in T \vee x \in \neg T)$;

– *an strongly extensional* (*an se-subset*) of S: $\forall_{x \in S}\,(x \in T \vee x \in \sim T)$.

Proposition 0.1 *Any se-subset T of S satisfies $\sim T = \neg T$.*

In what follows se-subsets will be one of the main objects of investigation.

A binary relation τ defined on semigroup with apartness S is

– consistent if $\tau \subseteq \#$;

– cotransitive if $(x, z) \in \tau \Rightarrow \forall_y\,((x, y) \in \tau \vee (y, z) \in \tau)$;

– coquasiorder if it is consistent and cotransitive.

Proposition 0.2 *Any coquasiorder τ on S is an se-subset of $S \times S$.*

Quotient structures are not part of **BISH**. Quotient structure does not have, in general, a natural apartness relation. Like the machinery described in [7] for groups and commutative rings with tight apartness, here the machinery of equivalences for a set with apartness is presented in 'dual' terms in analogy with the relation apartness/equality. It turns out that coquasiorders are the tool for introducing an apartness relation on a factor set.

A binary relation κ defined on semigroup with apartness S is

– coequivalence if it is symmetric coquasiorder;

– cocongruence if it is coequivalence that is cocompatible with multiplication, i.e. that is $\forall_{a,b,x,y \in S}\,((ax, by) \in \kappa \Rightarrow (a, b) \in \kappa \vee (x, y) \in \kappa)$.

Now we can formulate one of the main results - **Apartness Isomorphism Theorem** for semigroups with apartness.

Theorem 0.2 *Let $f : S \longrightarrow T$ be an se-homomorphism between semigroups with apartness. Then:*

(i) *the relation* $\operatorname{coker} f \equiv \{(x,y) \in S \times S : f(x) \# f(y)\}$ *is a cocongruence on* S *associated with* $\ker f$*;*

(ii) $(S/\ker f, =, \#, \cdot)$ *is a semigroup with apartness, where*

$$\begin{aligned} a(ker\, f) = b(ker\, f) &\Leftrightarrow (a,b) \in ker\, f, \\ a(ker\, f) \# b(ker\, f) &\Leftrightarrow (a,b) \in \operatorname{coker} f, \\ a(ker\, f)\, b(ker\, f) &= (ab)(ker\, f); \end{aligned}$$

(iii) *the mapping* $\theta : S/ker\, f \longrightarrow T$*, defined by* $\theta(x(ker\, f)) = f(x)$*, is an se-embedding such that* $f = \theta \circ \pi$*; and*

(iv) *if* f *is onto, then* θ *is an apartness isomorphism.*

Although the presentation given above is based on material given in [3], [4], it is, by no means an attempt to give a complete overview of our existing results. Results of several years long investigation, presented in [3], [4], present a semigroup facet of some relatively well established direction of constructive mathematics. Important sourse of ideas and notions of our work is [2]. An example of application(s) of these ideas can be found in [5]. The standard reference for constructive algebra is [6].

References

[1] M. J. Beeson, *Foundations of Constructive Mathematics*, Springer-Verlag, 1985.

[2] D. S. Bridges, L. S. Vîţā, *Apartness and Uniformity - A Constructive Development*, CiE series on Theory and Applications of Computability, Springer, 2011.

[3] S. Crvenković, M. Mitrović, D. A. Romano, *Semigroups with Apartness*, Mathematical Logic Quarterly, 59 (6), 2013, 407-414.

[4] S. Crvenković, M. Mitrović, D. A. Romano, *Basic Notions of (Constructive) Semigroups with Apartness*, Semigroup Forum, June 2016, Volume 92, Issue 3, 659-674.

[5] H. Geuvers, R. Pollack, F. Wiedijk, J. Zwanenburg, *A Constructive Algebraic Hierarchy in Coq*, J. Symbolic Computation (2002) 34, 271-286.

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

[7] A.S. Troelstra, D. van Dalen, *Constructivism in Mathematics, An Introduction*, (two volumes), North - Holland, Amsterdam 1988.

Towards Relevant Justifications

Nenad Savić[1] and Thomas Studer[1]

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

September 4, 2017

Keywords:

Justification Logic, Relevant Logic, Soundness and Completeness, Realization

Justification logic replaces the $\Box$-operator of modal logic by explicit justifications [2, 4]. That is justification logic features formulas of the form $t : A$ meaning *A is believed for reason t*; hence we can reason with and about explicit justifications for an agent's belief. The framework of justification logic has been used to formalize and study a variety of epistemic situations [3, 5, 6, 7, 8].

However, traditional justification logic is based on classical logic, which can lead to the following paradoxical situation. Consider a person A visiting a foreign town, which she does not know well. In order to get to a certain restaurant, she asks two persons B and C for the way. Person B says that A can take path P to the restaurant whereas person C replies that P does not lead to the restaurant and A should take another way. Person A now has a reason s to believe P and a reason t to believe $\neg P$. We can formalize this in justification logic by saying that both

$$s : P \qquad \text{and} \qquad t : \neg P \tag{1}$$

hold. However, then there exists a justification $r(s, t)$ such that

$$r(s, t) : (P \wedge \neg P)$$

holds. Now this implies (under certain natural assumptions) that for any formula F, there is a justification u such that

$$u : F \tag{2}$$

holds. That means for any formula F, person A has a reason to believe F, which, of course, is an undesirable consequence.

It is the aim of this paper to introduce a justification logic, RJ, in which situations of this kind cannot occur, in particular, that means a logic in which (2) does not follow from (1). We achieve this by combining the relevant logic R with the justification logic J4.

Relevant logics are non-classical logics that avoid the paradoxes of material and strict implication and provide a more intuitive deductive inference. The central systems of relevant logic, according to Anderson and Belnap [1], are the system of relevant implication R, as well as the logic of entailment E.

Meyer [9] proposed the logic NR, which is the relevant logic R equipped with an $S4$-style theory of necessity, in order to investigate whether the resulting theory coincides with the theory of entailment provided by Anderson and Belnap [1]. Adapting the semantics for the logic R [10], Routley and Meyer provided a complete semantics for the logic NR [11].

Our logic RJ is similar to NR but instead of the $\Box$-operator, we use explicit justifications and since we deal with beliefs, we do not include the truth principle $t : A \to A$ in the list of axioms.

Conjecture 1.[Soundness and Completeness] Let CS be any constant specification. For each formula A we have

$$\mathsf{RJ}_{\mathsf{CS}} \vdash A \quad \text{iff} \quad A \text{ is } \mathsf{CS}\text{-valid.}$$

There is a close relationship between NR and our logic of relevant justifications. Let RLP be the system RJ plus the axiom $t : A \to A$ based on the total constant specification, i.e., every constant justifies every axiom (including $t : A \to A$). A *realization* is a mapping from modal formulas to formulas of justification logic that replaces each $\Box$ with some expression t: (different occurrences of $\Box$ may be replaced with different terms).

Conjecture 2.[Realization] There is a realization r such that for each modal formula A

$$\mathsf{NR} \vdash A \quad \text{implies} \quad \mathsf{RLP} \vdash r(A).$$

References

[1] A. R. Anderson and N. D. Belnap. *Entailment: The Logic of Relevance and Neccessity, Vol. I.* Princeton University Press, 1975.

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

[3] S. N. Artemov. The logic of justification. *RSL*, 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. *APAL*, 165(1):6–25, 2014.

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

[7] S. Bucheli, R. Kuznets, and T. Studer. Realizing public announcements by justifications. *Journal of Computer and System Sciences*, 80(6):1046–1066, 2014.

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

[9] R. K. Meyer. Entailment and relevant implication. *Logique et Analyse*, 11(44):472–479, 1968.

[10] R. Routley and R. Meyer. The semantics of entailment. *Studies in Logic and the Foundations of Mathematics*, 68:199 – 243, 1973. Truth, Syntax and Modality.

[11] R. Routley and R. K. Meyer. The semantics of entailment: II. *Journal of Philosophical Logic*, 1(1):53–73, 1972.

Lambek Calculus with Bracket Modalities and Subexponentials

Andre Scedrov

1 Introduction

The Lambek calculus is a well-known logical formalism for modelling natural language syntax. The calculus is a logical foundation of categorial grammar, a linguistic paradigm of grammar as logic and parsing as deduction. Pentus (2010) gave a polynomial-time algorithm for determining provability of bounded depth formulas in the Lambek calculus with empty antecedents allowed. Pentus' algorithm is based on tabularisation of proof nets.

The original calculus covered a substantial number of intricate natural language phenomena. In order to address more subtle linguistic issues, the Lambek calculus has been extended in various ways. For instance, an extension with bracket modalities introduced by Morrill (1992) and Moortgat (1995) is suitable for the modeling of so-called islands. The syntax is more involved than the syntax of a standard sequent calculus. Derivable objects are sequents of the form Gamma –> A , where the antecedent Gamma is a structure called meta-formula and the succedent A is a formula. Meta-formulae are built from formulae (types) using two metasyntactic operators: comma and brackets. In joint work with Max Kanovich, Stepan Kuznetsov, and Glyn Morrill [1] we give an algorithm for provability in the Lambek calculus with brackets allowing empty antecedents. Our algorithm runs in polynomial time when both the formula depth and the bracket nesting depth are bounded. The algorithm combines a Pentus-style tabularisation of proof nets with an automata-theoretic treatment of bracketing.

Morrill and Valentin (2015) introduce a further extension with so-called exponential modality, suitable for the modeling of medial and parasitic extraction. Their extension is based on a non-standard contraction rule for the exponential, which interacts with the bracket structure in an intricate way. The standard contraction rule is not admissible in this calculus. In joint work with Max Kanovich and Stepan Kuznetsov [2] we show that provability in this calculus is undecidable and we investigate restricted decidable fragments considered by Morrill and Valentin. We show that these fragments belong to NP.

References

[1] Max Kanovich, Stepan Kuznetsov, Glyn Morrill, and Andre Scedrov. A polynomial-time algorithm for the Lambek calculus with brackets of bounded order. In: D. Miller, ed., Second International Conference on Formal Structures for Computation and Deduction (FSCD 2017). Leibniz International Proceedings in Informatics (LIPIcs), 2017. Technical report in arXiv:1705.00694.

[2] Max Kanovich, Stepan Kuznetsov, and Andre Scedrov. Undecidability of the Lambek calculus with subexponential and bracket modalities. In: R. Klasing and M. Zeitoun, eds., 21st International Symposium on Fundamentals of Computation Theory (FCT 2017). Springer LNCS Volume 10472, 2017. Technical report in arXiv:1608.04020.

What is logical consequence?

Zvonimir Šikić

FSB, Sveučilište u Zagrebu

Abstract

A singular logical consequence relation is a closure operator on a set of sentences. A multiple logical consequence relation is not. We argue that the multiple one is more natural.

We also discuss singular and multiple logical consequence relations generated by rules of inferences and their characterization theorems. We offer an explanation of Tarski's "more general" definition of logical consequence generated by rules of inferences.

References

[1] D. Scott. Completeness and axiomatizability in many-valued logic. In Henkin, L. et al. (eds) Proceedings of Tarski Symposium. Proceedings of Symposia in Pure Mathematics, vol. 25, 411–436, 1974.

[2] D. J. Shoesmith, T. J. Smiley, Multiple-Conclusion Logic, CUP, 1978.

[3] Z. Sikic, A proof of the characterization theorem for consequence relations, Zeitschr. fur math. Logik und Grundlagen der Mathematik 37, 1991.

[4] Z. Sikic, Singular consequence relations and order relations, Grazer Mathematische Berichte 304, 1989.

[5] Tarski, Alfred (1930) Über einige fundamentale Begriffe der Metamathematik, Comptes Rendus des séances de la Société des Sciences et des Lettres de Varsovie, Vol. 23, Cl. III, pp. 22–29

[6] Tarski, Alfred (1930a) Fundamentale Begriffe der Methodologie der deduktiven Wissenschaften I, Monatshefte für Mathematik und Physik, Vol. 37, pp. 361–404.

Standard classical logic as protocol for process communication

Dragiša Žunić

Carnegie Mellon University in Qatar

Keywords:

Classical logic, process calculi, asterix calculus, pi calculus, session types

Introduction

We propose a process calculus for classical logic with explicit structural rules. Rather than going though linear logic we use a standard classical logic formalized in the sequent calculus. In this ongoing research, we illustrate that classical logic has potential to naturally serve as protocol for concurrent process communication.

Being in the era of concurrent, distributed and parallel computing, we are concerned with searching for a calculus for concurrency - which fits naturally the concurrent setting and which is rooted in logic, in the manner λ-calculus is a foundation for functional programming. This paradigm is thus the following: proofs are processes; propositions are session types; proof-transformation (here cut-elimination) is communication.

As in the works of Wadler [1, 2] and Caires and Pfenning [3], we let logic guide the design of the "right" process calculus (let us mention a more recent work dealing with multiparty sessions [4]). The logic we consider here is classical logic with explicit structural rules formalized in two-sided sequent calculus (close to Gentzen's LK). This is a promising logical setting for concurrency because it features symmetry, non-confluence and control over erasing and duplicating terms. Moreover, this research itself (process communication being of spatial nature) provides new insight into the essence of logic. Building upon the work by Bierman and Urban [5], we have previously explored classical computation with explicit structural rules at different levels of abstraction [6, 7], and similarly in the intuitionistic setting [8].

$$P, Q \;::=\; -x- \;\mid\; (\nu x)(P \mid Q) \;\mid\; x[y,z].(P \mid Q) \;\mid\; x(y,z).P$$
$$\mid\; x^e[\,].P \;\mid\; x^e(\,).P \;\mid\; x^d[y,z].P \;\mid\; x^d(y,z).P$$

Figure 1: Syntax

$$\frac{}{-x- \;:\cdot\; x : A \vdash x : A}\,(\mathrm{Ax}) \qquad \frac{P \;:\cdot\; \Gamma \vdash x : A, \Delta \qquad Q \;:\cdot\; \Gamma', x : A \vdash \Delta'}{(\nu x)(P \mid Q) \;:\cdot\; \Gamma, \Gamma' \vdash \Delta, \Delta'}\,(\mathrm{Cut})$$

$$\frac{P \;:\cdot\; \Gamma \vdash y : A, \Delta \qquad Q \;:\cdot\; \Gamma' \vdash z : B, \Delta'}{x[y,z].(P \mid Q) \;:\cdot\; \Gamma, \Gamma' \vdash x : A \wedge B, \Delta, \Delta'}\,(\wedge_R) \qquad \frac{R \;:\cdot\; \Gamma, y : A, z : B \vdash \Delta}{x(y,z).R \;:\cdot\; \Gamma, x : A \wedge B \vdash \Delta}\,(\wedge_L)$$

$$\frac{P \;:\cdot\; \Gamma \vdash \Delta}{x^e[\,].P \;:\cdot\; \Gamma \vdash x : A, \Delta}\,(\mathrm{W}_R) \qquad \frac{Q \;:\cdot\; \Gamma \vdash \Delta}{x^e(\,).Q \;:\cdot\; \Gamma, x : A \vdash \Delta}\,(\mathrm{W}_L)$$

$$\frac{P \;:\cdot\; \Gamma \vdash y : A, z : A, \Delta}{x^d[y,z].P \;:\cdot\; \Gamma \vdash x : A, \Delta}\,(\mathrm{C}_R) \qquad \frac{Q \;:\cdot\; \Gamma, y : A, z : A \vdash \Delta}{x^d(y,z).Q \;:\cdot\; \Gamma, x : A \vdash \Delta}\,(\mathrm{C}_L)$$

Figure 2: The type system

Classical logic as process calculus

We will see that this setting has a particular flavor comparing to what is seen before. We have explicit weakening which introduces a tool (call it channel-eraser) that a process can, under certain assumptions, use to erase other processes. However, this will happen only when another process tries to establish a communication over that channel-eraser.

Also we have explicit contraction which implements a tool (channel-duplicator) that a process can use (provided that it has one) for duplication of processes that try to communicate over that channel.

We present a blueprint on how all this works through providing syntax, type assignment rules and several reduction rules.

Elements of the syntax are given in Fig. 1. They are assigned types as presented in Fig 2, thus setting up to have classical propositions as session types, i.e., a protocol for process communication.

We have the reduction rules of type β (logical reduction rules) and of type σ (structural reduction rules). Few of the reduction rules are given in Fig. 3. We assume that free names in Q are u and v, and that free names of P are r, s. Computation preserves free names and types.

$$
\begin{array}{lcll}
(\sigma_{W_R}) & : & (\nu x)(x^e[\,].P \mid x(w).Q) & \rightarrow \quad u^e[\,].v^e[\,].P \\
(\sigma_{W_L}) & : & (\nu x)(x[w].P \mid x^e(\,).Q) & \rightarrow \quad r^e(\,).s^e(\,).Q \\
(\sigma_{C_R}) & : & (\nu x)(x^d[y,z].P \mid x(w).Q) & \rightarrow \quad u^d[u_1,u_2].v^d[v_1,v_2].(\nu z)((\nu y)(P \mid Q\{y/w\}) \mid Q\{z/w\}) \\
(\sigma_{C_L}) & : & (\nu x)(x[w].P \mid x^d(y,z).Q) & \rightarrow \quad r^d(r_1,r_2).s^d(s_1,s_2).(\nu z)((\nu y)(Q \mid P\{y/w\}) \mid P\{z/w\})
\end{array}
$$

Figure 3: Partial reduction rules for process calculus

Acknowledgements

This paper was made possible by NPRP 7-988-1-178 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] P. Wadler, *Propositions as sessions*, ACM SIGPLAN International Conference on Functional Programming, ICFP 2012, pp. 273–286, 2012.

[2] P. Wadler, *Propositions as sessions*, Journal of Functional Programming, Vol. 24, No. 2-3, pp. 384–418, 2014.

[3] L. Caires, F. Pfenning, *Session Types as Intuitionistic Linear Propositions*, CONCUR 2010, pp. 222–236, 2010.

[4] M. Carbone, S. Lindley, F. Montesi, C, Schürmann, P. Wadler, *Coherence Generalises Duality: A Logical Explanation of Multiparty Session Types*, CONCUR 2016, pp. 33:1-33:15, 2016.

[5] C. Urban, *Classical Logic and Computation*, University of Cambridge (PhD thesis), 2000.

[6] D. Zunic, *Computing With Sequent and Diagrams in Classical Logic - Calculi $^*\mathcal{X}$, $©\mathcal{X}$ and $d\mathcal{X}$*, ENS Lyon (PhD thesis), 2007. (`https://tel.archives-ouvertes.fr/tel-00265549`)

[7] D. Zunic, P. Lescanne, *A congruence relation for restructuring classical terms*, ICTCS 2017, accepted.

[8] S. Ghilezan, J. Ivetic, P. Lescanne and D. Zunic, *Intuitionistic Sequent-Style Calculus with Explicit Structural Rules*, TbiLLC 2009, pp. 101–124, 2009.