4th international conference

Logic and Applications

LAP 2015

September 21 – 25, 2015,
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

CEI
CENTRAL EUROPEAN INITIATIVE

Contents

Conditions for pursuing research

Henk Barendregt, Radboud University, Nijmegen, The Netherlands

Some personal memories will be presented how these conditions were working in my case. Important ones are: curiosity, relaxation, and concentration.

On Kolmogorov–Gödel–type Interpretations of Classical Logic

Branislav Boričić, Faculty of Economics, University of Belgrade, Serbia

Keywords:

classical logic, intuitionistic logic, superintuitionistic logics, interpretation.

A simple and immediate connection between the classical and the Heyting's logic was first given by the Glivenko's Theorem [9]: for every propositional formula A, A is classically provable iff $\neg\neg A$ is provable intuitionistically. This theorem does not hold for first–order predicate calculi, and D. M. Gabbay [7] proved that the extension of Heyting's first–order logic by the axiom $\neg(\forall x\neg\neg A\wedge\neg\forall xA)$ is the minimal superintuitionistic logic for which Glivenko's theorem holds. Glivenko's Theorem can be understood as a possible way of intuitionistic interpretation of the classical reasoning. Let us define the next two interpretations. The first one, here denoted by k, was described by A. N. Kolmogorov [12], and the second interpretation, denoted by g, was introduced by K. Gödel [10]. These interpretations, $k, g : For \to For$, are defined inductively as follows:

$$\begin{array}{ll} k(A) & = \neg\neg A, \text{ if } A \text{ is an atom} \\ k(\neg A) & = \neg\neg\neg k(A) \\ k(A \circ B) & = \neg\neg(k(A) \circ k(B)), \text{ if } \circ \text{ is } \wedge, \vee \text{ or } \to \end{array}$$

and

$$\begin{array}{ll} g(A) & = \neg\neg A, \text{ if } A \text{ is an atom} \\ g(\neg A) & = \neg g(A) \\ g(A \circ B) & = g(A) \circ g(B), \text{ if } \circ \text{ is } \wedge \text{ or } \to \\ g(A \vee B) & = \neg(\neg g(A) \wedge \neg g(B)) \end{array}$$

where the set of all propositional formulae is denoted by For. We note that the original interpretation g defined by Gödel had the clause $g(A \to B) = \neg(g(A) \wedge \neg g(B))$ and that the version presented above was redefined by Gentzen in [8]. These mappings may be extended on the first–order language in a quite natural way:

$$\begin{array}{ll} k(\forall xA) & = \neg\neg\forall xA \\ k(\exists xA) & = \neg\neg\exists xk(A) \end{array}$$

and

$$\begin{array}{ll} g(\forall xA) & = \forall xA \\ g(\exists xA) & = \neg\forall x\neg g(A) \end{array}$$

Some of their variations were considered by B. Boričić [3], [5] and [6], in connection with the first–order superintuitionistic logics characterized by the axioms $M : \neg A \vee \neg\neg A$ and $E : \neg\neg\exists x \neg A \to \exists x \neg A$. Let us denote by $\mathbf{H}M$, $\mathbf{H}E$ and $\mathbf{H}ME$ the extensions of the Heyting first–order predicate calculus $\mathbf{H}$ by the above axiom–schemata. If $b_{ME}, b_m, b_E, g : For \to For$ are the interpretations defined as the Gödel's one g, except the cases with disjunction and existential quantifier, as follows:

$$\begin{aligned} b_{ME}(R) &= \neg\neg R \text{ (if } R \text{ is an atomic formula)} \\ b_{ME}(A \star B) &= b_{ME}(A) \star b_{ME}(B) \text{ (where } \star \text{ is } \wedge, \vee \text{ or } \to) \\ b_{ME}(\neg A) &= \neg b_{ME}(A) \\ b_{ME}(QxA) &= Qx b_{ME}(A) \text{ (where } Q \text{ is } \forall \text{ or } \exists) \end{aligned}$$

b_M is same as b_{ME}, with the only difference that:

$$b_M(\exists xA) = \neg\forall x \neg b_M(A)$$

b_E is same as b_{ME}, with the only difference that:

$$b_E(A \vee B) = \neg(\neg b_E(A) \wedge b_E(B))$$

b is same as b_{ME}, with the only difference that:

$$g(\exists xA) = \neg\forall x \neg g(A)$$

and

$$g(A \vee B) = \neg(\neg g(A) \wedge g(B))$$

Embedding of the implicative fragment of classical logic into the implicative fragment of the Heyting's logic was considered by J. P. Seldin [14], B. Boričić [1] and L. C. Pereira, E. H. Haeusler, V. G. Costa, W. Sanz [13]. Seldin's interpretation essentially depends on the presence of conjunction, but another two are obtained in the pure language of implication. Here we define, in spirit of Kolmogorov's interpretation, a mapping of the pure implicational propositional language enabling to prove the corresponding result.

Let $p_1, \ldots, p_n$ be a list of all propositional letters occurring in formula $A \to B$ and q any propositional letter not occurring in $A \to B$. Then the image $b(A \to B)$ of $A \to B$ is defined inductively as follows:

$$\begin{aligned} b(p) \quad &= (p \to q) \to q, \text{ for each } p \in \{p_1, \ldots, p_n\} \\ b(A \to B) \quad &= b(A) \to b(B) \end{aligned}$$

Namely, $b(A \to B)$ is obtained by replacing each occurrence of a propositional letter p in $A \to B$ by $(p \to q) \to q$, where q is a new letter.

Let us also note that this embedding can be considered a rough combination of Kolmogorov's, Gödel's and Johansson's translations (see [10], [11] and [12]).

Embedding Lemma 1. *For every first–order formula A, A is provable in classical logic iff*

(a) $k(A)$ is provable in Heyting logic;
(b) $g(A)$ is provable in Heyting logic;
(c) $b_{ME}(A)$ is provable in $\mathbf{H}ME$;
(d) $b_E(A)$ is provable in $\mathbf{H}E$;
(e) $b_M(A)$ is provable in $\mathbf{H}M$.

Theorem. *The minimal superintuitionistic predicate logic in which the classical logic is embedable by b_X is $\mathbf{H}X$, where X stands for M, E or ME.*

Embedding Lemma 2. *For every propositional implicational formula A, A is provable in classical logic iff $b(A)$ is provable in Heyting logic.*

The above statements present a sublimation of some results contained in papers [1], [2], [3], [5] and [6] dealing with relationships of classical logic with superintuitionistic logics.

References

[1] B. Boričić, *On interpretation of logical sistem, (serbocroatian: O interpretaciji logičkog sistema),* Matematika XIX (1990), Br. 3, pp. 40–44.

[2] B. Boričić, *Some modifications of the Goedel translation of classical into intuitionistic logic,* Bulletin of the Section of Logic, Polish Acad. of Sci. 19 (1990), No. 3, pp. 84–86. (Zbl. 712.03004)

[3] B. Boričić, *On some interpretations of classical logic,* Zeitschrift für mathematishe Logik und Grundlagen der Mathematik 38 (1992), pp. 409–412. (MR 94k:03010; Zbl 794:03011)

[4] B. Boričić, *Logic and Proof,* Ekonomski fakultet, Beograd, 2011, 154+iv p. (Zbl 1214.03043)

[5] B. Boričić, M. Ilić, *An Alternative Normalization of the Implicative Fragment of Classical Logic,* Studia Logica 103 2 (2015), pp. 413-446.

[6] B. Boričić, M. Ilić, *An Intuitionistic Interpretation of Classical Implication,* The Bulletin of Symbolic Logic 21 (2015) pp. 60-61. (Abstract)

[7] D. M. Gabbay, *Applications of trees to intermediate logics,* Journal of Symbolic Logic 37 (1972), pp. 135–138.

[8] G. Gentzen, *Collected Papers,* (ed. M. E. Szabo), North–Holland, Amsterdam, 1969.

[9] M. V. Glivenko, *Sur quelques points de la logique de M. Brouwer',* Bulletins de la classe des sciences, Academie Royale de Belgique ser. 5, vol. 15 (1929) pp.183–188.

[10] K. Gödel, *Zur intuitionistischen Arithmetik und Zahlentheorie, Ergebnisse eines Mathematischen Kolloquiums, vol. 4 (1932-33), pp. 34–38; English transl. in The Undecidable (M. Davis, ed.), Raven Press, New York, 1965, pp. 75–81; reprinted, with additional comment in* Kurt Gödel, Collected Works, Vol. I, ed. S. Feferman et al, Oxford University Press, New York, 1986, pp. 282–295.

[11] I. Johansson, *Der Minimalkalkül, ein reduzierter intuitionistische Formalismus,* Comp. Math. 4 (1937) pp. 119–136.

[12] A. N. Kolmogorov, *On the principle of excluded middle,* (Russian) Math. Zbor. vol. 32 (1925), pp. 646–667; English transl. in From Frege to Gödel: A Source–Book in Mathematical Logic (J. van Heijenoort, ed.) Harvard University Press, London 1967, pp. 414–437.

[13] L. C. Pereira, E. H. Haeusler, V. G. Costa, W. Sanz, *A new normalization strategy for the implicational fragment of classical propositional logic,* Studia Logica 96 (2010), no. 1, pp. 95–108.

[14] J. P. Seldin, *Normalization and excluded middle I,* Studia Logica 48 (1989), no. 2, pp. 193–217.

A calculus of sequents with probability

Marija Boričić, Faculty of Organizational Sciences, University of Belgrade

Keywords:

sequent calculus, probability, models

Gentzen's approach to deductive systems (see [5] and [13]), and Carnap's and Popper's treatment of probability in logic (see [3], [7], [8] and [9]), were two fruitful ideas of logic in the mid–twentieth century. By combining these two concepts, the notion of sentence probability, and the deduction relation formalized in the sequent calculus, we introduce the notion of 'probabilized sequent' $\Gamma \vdash_a^b \Delta$ with the intended meaning that "the probability of truthfulness of $\Gamma \vdash \Delta$ is into the interval $[a,b] \cap I$', where I is a finite subset of reals $[0,1]$". The usual approach to treating the probability of a sentence leads to a kind of polymodal logic with iterated (or not iterated) probability operators over formulae (see [10], [11] and [12]). On the other hand, there were some papers dealing with probabilistic form of inference rules (see [1], [2], [3], [6] and [14]). Roughly, our system **LKprob** of classical propositional sequents with probability is defined as follows. Sequents in **LKprob** are of the form $\Gamma \vdash_a^b \Delta$, meaning that 'the probability of provability of $\Gamma \vdash \Delta$ belongs to the interval $[a,b] \cap I$', where I is a finite subset of reals $[0,1]$. The axioms of **LKprob** are the following sequents: $\Gamma \vdash_0^1 \Delta$, $\vdash^0$, $A \vdash_1 A$, for any words Γ and Δ, and any formula A. We also present structural and logical inference rules of **LKprob**. The system **LKprob**, an extension of Gentzen's sequent calculus for classical propositional logic (see [5] and [13]), is sound and complete with respect to a kind of Carnap–Popper–Leblanc–type probability logic semantics (see [3], [7], [8] and [9]).

Let Seq be the set of all sequents of the form $\Gamma \vdash \Delta$. A model for **LKprob** is any mapping $p : \text{Seq} \to [0,1]$ satisfying:

(i) $p(A \vdash A) = 1$, for any formula A;

(ii) if $p(AB \vdash) = 1$, then $p(\vdash AB) = p(\vdash A) + p(\vdash B)$, for any formulas A and B;

(iii) if sequents $\Gamma \vdash \Delta$ and $\Pi \vdash \Lambda$ are equivalent in **LK**, in sense that there are proofs for both sequents $\bigwedge \Gamma \to \bigvee \Delta \vdash \bigwedge \Pi \to \bigvee \Lambda$ and $\bigwedge \Pi \to \bigvee \Lambda \vdash \bigwedge \Gamma \to \bigvee \Delta$ in **LK**, then $p(\Gamma \vdash \Delta) = p(\Pi \vdash \Lambda)$.

The satisfiability relation in a model for the probabilized sequents is defined by clause:

$$\models_p \Gamma \vdash_a^b \Delta \text{ iff } a \leq p(\Gamma \vdash \Delta) \leq b.$$

We say that a theory $\mathbf{LKprob}(\sigma_1, \ldots, \sigma_n)$ is inconsistent if there are two sequents $\Gamma \vdash_a^b \Delta$ and $\Gamma \vdash_c^d \Delta$ both provable in $\mathbf{LKprob}(\sigma_1, \ldots, \sigma_n)$ such that $[a, b] \cap [c, d] = \emptyset$; otherwise, $\mathbf{LKprob}(\sigma_1, \ldots, \sigma_n)$ is consistent. By $\mathbf{LKprob}(\sigma_1, \ldots, \sigma_n)$ we denote an extension of $\mathbf{LKprob}$ by sequents $\sigma_1, \ldots, \sigma_n$. We cite some propositions concerning necessary and sufficient conditions for consistency.

The soundness is proved. Also, we prove that each consistent theory can be extended to a maximal consistent theory and we describe the canonical model, which leads us to the proof of the completeness theorem.

The sequent calculus **LKprob** can be also observed as a program which input data are, besides the three axioms of the system, the additional "axioms" $\sigma_1, \ldots, \sigma_n$, with output a theory $\mathbf{LKprob}(\sigma_1, \ldots, \sigma_n)$. The next step is to build up a subsystem of **LKprob** in Suppes style, namely a system concerning sequents with high probabilities.

References

[1] M. Boričić, *Hypothetical syllogism rule probabilized*, Bulletin of Symbolic Logic, vol. 20 (2014), pp. 401–402, Abstract, Logic Colloquium 2012.

[2] M. Boričić, *Models for the probabilistic sequent calculus*, Bulletin of Symbolic Logic, vol. 21 (2015), pp.60, Abstract, Logic Colloquium 2014.

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

[4] A. M. Frisch, P. Haddawy, *Anytime deduction for probabilistic logic*, Artificial Intelligence, vol. 69 (1993), pp. 93–122.

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

[6] T. Hailperin, *Probability logic*, Notre Dame Journal of Formal Logic, vol. 25 (1984), pp. 198–212.

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

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

[9] 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.

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

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

[12] M. Rašković, *Classical logic with some probability operators*, Publications de l'Institut Mathématique , vol. 53 (67) (1993), pp. 1–3.

[13] G. Takeuti, *Proof Theory*, North–Holland, Amsterdam, 1975.

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

Sequential algorithms (old and new)

Pierre-Louis Curien, CNRS, Univ. Paris Diderot, and INRIA

Keywords:

sequentiality, primitive recursion, bar recursion.

This talk will offer both a reminder on Berry and Curien's sequential algorithms (37 years old) and their various equivalent presentations (as programs, as configurations of a cds, as abstract pairs (function, computation strategy), as observationally sequential functions, as bistable functions (Laird)), and some discussion of interesting examples: primitive recursive functions, bar recursion, where they can play a structuring and computational role. In particular, we shall give a new proof of Colson's ultimate obstinacy theorem and show a conjecture that it might extend to the whole of Gödel's system T. To give an idea of what this relatively confidential theorem is about, let me just mention here that a consequence of Colson's result is that one can prove that there is no primitive recursive way of programming the min of two natural numbers by decreasing the two arguments althernatively by one until one of them gets 0.

Acknowledgements

Thanks to René David, whose proof of ultimate obstinacy inspired me for the present one.

References

[1] L. Colson, About Primitive Recursive Algorithms, *Theoretical Computer Science* 83(1), 57-69 (1991).

[2] R. David, On the asymptotic behaviour of primitive recursive algorithms, *Theoretical Computer Science* 266, 159-193 (2001).

Galois Connections in Clone Theory

Jelena Čolić Oravec, University of Novi Sad, Serbia

Keywords:

Galois connection, clone, hyperclone, maximal hyperclones

Galois connections appear in various areas of mathematics and computer science, since they are extremely useful in relating distinct mathematical objects, while being fairly easy to construct. For arbitrary non-empty sets A and B, and a relation $R \subseteq A \times B$ we can define mappings $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$ and $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$ by

$$\begin{aligned} \overrightarrow{R}(X) &= \{y \in B : (\forall x \in X)\,(x,y) \in R\},\ X \subseteq A, \\ \overleftarrow{R}(Y) &= \{x \in A : (\forall y \in Y)\,(x,y) \in R\},\ Y \subseteq B. \end{aligned}$$

Then the pair $(\overrightarrow{R}, \overleftarrow{R})$ is a Galois connection between sets A and B.

One Galois connection plays a crucial role in clone theory. Although clones are usually considered to be composition closed sets of operations that include all projections, an alternative approach is to define them as the sets of all operations that preserve all the relations from a given set, which is a consequence of a well-known Galois connection (Pol, Inv). This approach proved to be extremely useful in describing the clone lattice, especially its coatoms, which are called maximal clones. Namely, I. G. Rosenberg (1970) proved that the clone is maximal if and only if it is of the form $Pol\rho$, where ρ is a relation belonging to one of the following classes:

(R1) bounded partial orders;

(R2) prime permutations;

(R3) prime-affine relations;

(R4) non-trivial equivalence relations;

(R5) central relations;

(R6) h-regular relations.

This theorem is considered to be one of the most significant contributions in clone theory.

An n-ary hyperoperation on a set A is a mapping that assigns to every n-tuple of elements from A a non-empty subset of A. Hence there is more than one possibility to expand the notion of preservation between operations and relations to that between hyperoperations and relations. In particular, an ℓ-ary relation ρ on a set A may be extended to the relation on the power set of A in several different ways:

$$\begin{aligned}
\rho_d &= \{(A_1, \ldots, A_\ell) : A_1 \times \ldots \times A_\ell \subseteq \rho\}, \\
\rho_m &= \{(A_1, \ldots, A_\ell) : (\forall\, i \in \{1, \ldots, \ell\})\ (\forall\, a \in A_i) \\
&\qquad (\exists\, \boldsymbol{a} \in (A_1 \times \cdots \times A_\ell) \cap \rho)\ \ e_i^{\ell,A}(\boldsymbol{a}) = a\}, \\
\rho_h &= \{(A_1, \ldots, A_\ell) : (A_1 \times \cdots \times A_\ell) \cap \rho \neq \emptyset\}.
\end{aligned}$$

Each of these extensions yields a Galois connection between hyperoperations and relations. The first one, denoted by $(dPol, dInv)$, was independently studied by F. Börner and B. A. Romov, the second one, denoted by $(mPol, mInv)$, is due to T. Drescher and R. Pöschel and the third one, denoted by $(hPol, hInv)$, was introduced by I. G. Rosenberg, and also studied by H. Machida and J. Pantović. We used this last Galois connection in order to describe four classes of maximal hyperclones, determined by Rosenberg's relations from (R1),(R4),(R5) and (R6).

This is a joint work with Jovanka Pantović and Hajime Machida.

References

[1] F. Börner, *Total Multifunctions and Relations*, Contributions to General Algebra 13, pp. 23–36, 2001.

[2] J. Čolić, H. Machida, J. Pantović, *Maximal Hyperclones determined by Monotone Operations*, Proceedings of 41st IEEE International Symposium on Multiple-Valued Logic (ISMVL 2011), pp. 160–163, 2011.

[3] J. Čolić, H. Machida, J. Pantović, *On Hyper Co-Clones*, Proceedings of 43rd IEEE International Symposium on Multiple-Valued Logic (ISMVL 2013), pp. 182-185, 2013.

[4] J. Čolić, H. Machida, J. Pantović, *Upward Saturated Hyperclones*, Multiple-Valued Logic and Soft Computing 24(1-4), pp. 189–201, 2015.

[5] T. Drescher, R. Pöschel, *Multiclones and Relations*, Multiple-Valued Logic. An International Journal 7(5-6), pp. 313–337, 2001.

[6] D. Lau, *Function Algebras on Finite Sets - A Basic Course on Many-Valued Logic and Clone Theory*, Springer Monographs in Mathematics, 2006.

[7] H. Machida, J. Pantović, *Three Classes of Maximal Hyperclones*, Journal of Multiple Valued Logic and Soft Computing 18(2), pp. 201–210, 2012.

[8] R. Pöschel and L.A. Kalužnin, *Funktionen und Relationenalgebren*, Deutscher Verlag der Wiss, Birkhäuser Verlag, Basel u. Stuttgart, 1979.

[9] B.A. Romov, *Restriction-closed Hyperclones*, ISMVL, page 8. IEEE Computer Society, 2007.

[10] I.G. Rosenberg, *Algebraic Structures and Relations: a short survey*, Contributions to general algebra 15, Proceedings of the Klagenfurt Conference AAA2003, Verlag Johannes Heyn, Klagenfurt, pp. 161–176, 2004.

[11] Á. Szendrei, *Clones in Universal Algebra*, Seminaire de Mathematiques Superieures, Les Presses de l'Universite de Montreal, Montreal, 1986.

On Compensation Primitives as Adaptable Processes

Jovana Dedeić, University of Novi Sad, Serbia
Jovanka Pantović, University of Novi Sad, Serbia
Jorge A. Pérez, University of Groningen, The Netherlands

Keywords:

Process calculi, long running transactions, compensations, adaptation, encodings

Modern business applications support *long running transactions* (LRTs). Usually, LRTs are interactive and cannot be check-pointed, therefore cannot be based on locking. Instead, they use *compensations*: activities programmed to recover the partial execution of transactions. In case of error notification, a compensation execution is launched in order to take the system back to a consistent state. The emergence of paradigms such as service-oriented computing motivated the proposal of different formalisms with compensation handling primitives; see, e.g., [5].

On a related but different vein, a calculus of *adaptable processes* has been put forward [2] as a process calculus approach to describe dynamic evolution of communicating, concurrent systems. A calculus of adaptable processes is represented as a variant of CCS [3] where rules for restriction and relabelling are omitted and extended with a *located process* (denoted $l[P]$) and a *dynamic update* (denoted $l\{(X).Q\}$). Adaptable processes have locations and are sensitive to actions of dynamic update at runtime. This behaviour allows adaptable processes to express a wide range of evolvability patterns for concurrent processes. Located processes can be updated and relocated at runtime.

Our starting point for a language with compensations is the calculus investigated in [1]. The calculus of compensable processes is a variant of the π-calculus [4], extended with primitives for static and dynamic recovery processes. Static recovery is created by adding constructs for *transaction scopes* (denoted $t[P,Q]$) and *protected block* (denoted $\langle Q \rangle$) in standard π-calculus; dynamic recovery processes are static recovery processes extended with *compensation updates* (denoted $\texttt{inst}\lfloor \lambda X.R \rfloor.P$).

In concurrency theory, and in process calculi, a relevant topic is the identification of a uniform way to formally compare different languages from expressiveness point of view. We compare, in the sense of encoding, expressive power of compensable and adaptable processes. We define an encoding of compensable processes into adaptable processes. Essentially, the encoding needs to reflect and preserve as many semantic properties as possible (the decidability of properties, notions of equivalence, existence of matching transitions according to the operational semantics etc.). In compensable processes we differ three semantics: *aborting*, *preserving* and *discarding*. We consider encoding with respect to *static* and *dynamic* compensations. Therefore, for each semantics two categories of encodings are introduced. As such, we offer six different encodings into adaptable processes, each one equipped with appropriate operational correspondence results.

We provided correct encodings of processes with static and dynamic compensation into adaptable processes. More precisely, we proved that transitions introduced in the compensation calculus match reductions in the calculus of adaptable processes, and vice versa. The following two theorems are the main theorems of the paper, which provide correctness of encoding.

Theorem 1. Let P be a compensable process. If $P \xrightarrow{\tau} P'$ then $[\![P]\!]_\rho \rightarrow^* [\![P']\!]_\rho$, for any path ρ.

Theorem 2. Let P be a compensable process. If $[\![P]\!]_\rho \rightarrow Q$, for some ρ, then there is P' such that $P \xrightarrow{\tau} P'$ and $Q \rightarrow^* [\![P']\!]_\rho$.

In future work, we aim to extend our study to consider variants of adaptable and compensable processes with *session types*, exploiting already developed extensions of adaptable processes with session types [6, 7].

Acknowledgements

This work was partially supported by Cost Action BETTY, and the presented results were obtained during stay Jovan Dedeić at the University of Groningen and Jorge A. Pérez at the University of Novi Sad.

References

[1] I. Lanese, C. Vaz, C. Ferreira, *On the expressive eower of primitives for compensation handling*, In Proc. of ESOP 2010, volume 6012 of LNCS, pp. 366-386. Springer, 2010.

[2] M. Bravetti, C. D. Giusto, J. A. Pérez, G. Zavattaro, *Adaptable processes*, Logical Methods in Computer Science 8(4), 2012.

[3] R. Milner, *Communication and concurrency*, Prentice Hall, 1989.

[4] R. Milner, J. Parrow, D. Walker, *A calculus of mobile processes*,I. Inf. Comput. 100(1), pp. 1-40, 1992

[5] C. Ferreira, I. Lanese, A. Ravara, H. T. Vieira, G. Zavattaro, *Advanced mechanisms for service combination and transactions*, In: Results of the SENSORIA Project, Lecture Notes in Computer Science 6582, Springer, pp. 302–325, 2011

[6] C. D. Giusto, J. A. Pérez, *Disciplined structured communications with disciplined runtime adaptation*, Sci. Comput. Program. 97: 235-265, 2015.

[7] C. D. Giusto, J. A. Pérez, *An event-based approach to runtime rdaptation in communication-centric systems*, In *Proc. of* WS-FM 2014, LNCS. Springer, 2015. To appear.

Overview of the publication *“Selected Topics in Logic in Computer Science”*

Silvija Ghilezan, University of Novi Sad, Serbia

Keywords:

Logic in computer science

Mathematical logic is a fundamental area both of mathematics and computer science, being at the frontier between them, which encompasses complex mathematical reasoning about its objects of study and provides rigorous tools for concrete realization.

This edition of *Collection of articles, Zbornik radova Matematičkog instituta SANU* [2] brings together researchers from different topics of mathematical logic with focus on applications to computer science. It is complementary to the issue *Collection of articles, Zbornik radova 12(20), 2009,* [1], edited by Zoran Ognjanović and presents novel research in the area. The articles are meant to a wide mathematical audience from doctoral students and early stage researchers to specialist in the fields. Each of the articles gives an introductory overview of the topics, develops the obtained results, points to open problems and further work and gives a comprehensive bibliography of the related work.

This collection comprises six articles that range through different topics of category proof theory, first-order probabilistic logics, clones and hyper-clones, computational interpretations of logics, switching theory and logical design, and interactive theorem proving.

- Zoran Petrić (Mathematical Institute SANU).

  - 270 Minutes on Categorial Proof Theory.

- Nebojša Ikodinović (Faculty of Mathematics, University of Belgrade), Zoran Ognjanović, Miodrag Rasković, Zoran Marković (Mathematical Institute SANU).

  - First-order Probabilistic Logics and their Applications.

- Silvia Ghilezan, Jelena Ivetić (Faculty of Technical Sciences, University of Novi Sad), Silvia Likavec, Pierre Lescanne, (École normale supérieure de Lyon, France).

  - Structural Rules and Resource Control in Logic and Computation.

- Jelena Čolić-Oravec, Jovanka Pantović (Faculty of Technical Sciences, University of Novi Sad), Hajime Machida (International Christian University, Tokyo, Japan), Gradimir Vojvodić (University of Novi Sad).

  - From Clones to Hyper-Clones.

- Radomir S. Stanković (Faculty of Electronic Engineering, University of Niš), Jaakko Astola (Tampere University of Technology, Tampere, Finland), Claudio Moraga (European Center for Soft Computing, Mieres, Spain).

  - Pascal Matrices, Reed-Muller Expressions and Reed-Muller Error Correcting Codes.

- Filip Marić (Faculty of Mathematics, University of Belgrade).

  - A Survey of Interactive Theorem Proving.

The authors from Serbia are involved in three national projects of the Ministry of Education, Science and Technological Development of Serbia in the period 2011-2015 and the articles present overviews of results obtained within these projects: “Representations of logical structures and formal languages and their application in computing”, 174026, “Development of new information and communication technologies, based on advanced mathematical methods, with applications in medicine, telecommunications, power systems, protection of national heritage and education”, 44006, and “Automated Reasoning and Data Mining”, 174021.

The articles are internationally co-authored, which provides a wide international framework and increases the prominence of the presented work.

References

[1] Z. Ognjanović, ed., *Zbornik radova Matematičkog instituta SANU - Logic in Computer Science* 12(20), 2009.

[2] S. Ghilezan, ed., *Zbornik radova Matematičkog instituta SANU - Selected Topics in Logic in Computer Science* , 2015.

An optimisation of lambda type assignments via resource control

Silvija Ghilezan, University of Novi Sad, Serbia
Jelena Ivetić, University of Novi Sad, Serbia
Nenad Savić, University of Novi Sad, Serbia

Keywords:

lambda calculus, type assignment, resource control

Abstract

The size of a lambda term's type assignment is traditionally interpreted as the number of involved typing rules, since that interpretation corresponds to the complexity of underlying logical proof. However, it can be also assessed using some finer-grained measures such as the number of involved type declarations, or even as the sum of the sizes of all types in involved type declarations. These quantitative properties of type assignments are relevant for implementation issues, e.g. for compiler construction.

We propose a type assignment method that relies on the translation of a typeable lambda term to the corresponding term of the resource control lambda calculus. This calculus, introduced by Ghilezan et al. in [1], contains operators for variable duplication and erasing, and linear substitution, whereas its typed version corresponds to intuitionistic logic with explicit structural rules of contraction and thinning.

We prove that the translation preserves the type of a term, and that all output resource control lambda terms are in their $\gamma\omega$-normal forms, meaning that resource control operators are put in optimal positions considering the size of type assignments. The translation output of a given lambda term is often syntactically more complex and therefore more rules need to be used for its type assignment in the target resource control calculus. However, we show that two finer grained measures decrease when types are assigned to terms satisfying a certain minimal level of complexity.

Acknowledgements

This work was supported by the Serbian Ministry of Education and Science through projects ON174026, III44006 and ON174008.

References

[1] S. Ghilezan, J. Ivetić, P. Lescanne, and S. Likavec. Intersection types for the resource control lambda calculi. In A. Cerone and P. Pihlajasaari, editors, *8th International Colloquium on Theoretical Aspects of Computing, ICTAC '11*, volume 6916 of *Lecture Notes in Computer Science*, pages 116–134. Springer, 2011.

Proof-Theoretic Analysis of the Quantified Argument Calculus

Norbert Gratzl, LMU, Munich
Edi Pavlović, CEU, Budapest

Keywords:

Quarc, LK, Deductive Equivalence, Cut Elimination

This paper is a part of a larger work which explores the proof-theoretic properties of the Quantified Argument Calculus (Quarc). Here we focus on the more formal and technical results concerning the system. Quarc, in its formal presentation used here, was developed by Hanoch Ben-Yami in [2]. Quarc is a quantified logic system distinct from the standard Predicate Calculus, most notably, in allowing both the singular and the quantified expressions in the argument position of a predicate. Moreover, it models some ubiquitous features of a natural language, like anaphors and reordered predicates in its base language. It also includes a rule for instantiation, which allows the derivation of particular from a corresponding universal statement. The focus here will be specifically on what we label Quarc$_B$, or base Quarc, which does not contain the rules for identity or instantiation.

In the first section of the paper, after presenting Quarc$_B$, we develop LK-Quarc$_B$, a sequent-calculus representation of Quarc$_B$. We then demonstrate the deductive equivalence of the two, which will also serve to demonstrate the completeness of the system, given [3]. In the second section we then prove the Cut elimination theorem fo LK-Quarc$_B$. The proof is adapted from [1] and focuses mostly on the specifics of Quarc. From the Cut elimination theorem the Subformula property immediately follows. In the third section of the paper, we employ the Cut elimination theorem to demonstrate that instantiation is not derivable in LK-Quarc$_B$, and thus likewise in Quarc$_B$.

In the final section of the paper we indicate some implications of Quarc and the proof-theoretic properties of LK-Quarc$_B$, as well as discuss how this formal paper fits into the broader body of work.

References

[1] G. Gentzen, *The Collected Papers of Gerhard Gentzen*, ed. M. Szabo, Amsterdam: North-Holland, pp. 68-131, 1969.

[2] H. Ben-Yami, *The Quantified Argument Calculus*, The Review of Symbolic Logic, pp. 120-146, 2014.

[3] H. Ben-Yami, E. Pavlovic, *Completeness of the Quantified Argument Calculus*, manuscript.

Some applications of probabilistic first-order logics

Nebojša Ikodinović, Faculty of Mathematics, University of Belgrade, Serbia
Miodrag Rašković, Mathematical Institute SANU, Belgrade, Serbia
Zoran Marković, Mathematical Institute SANU, Belgrade, Serbia
Zoran Ognjanović, Mathematical Institute SANU, Belgrade, Serbia

Keywords:

Probabilistic first-order logic, approximate probability, strong completeness, decidability, nonmonotonic reasoning

In our talk we will briefly describe a first-order probabilistic logic, denoted $L_{\omega\omega}^{\mathrm{P},\mathbb{I}}$ and obtained by extending classical first-order logic with a list of Keisler-style (binary) conditional probability quantifiers of the form: $(\mathrm{CP}\vec{x} \leqslant r)$, $(\mathrm{CP}\vec{x} \geqslant r)$ and $(\mathrm{CP}\vec{x} \approx r)$. The intended meaning of $(\mathrm{CP}\vec{x} \leqslant r)(\alpha \mid \beta)$ is that the probability of the set of tuples $\vec{x}$ satisfying $\alpha \wedge \beta$ divided by the probability of the set of tuples satisfying β is at most r. The corresponding semantics consists of a classical first-order structure $\mathfrak{A} = (A, \cdots)$ with addition of $\mathcal{F}_n$ - a field of subsets of A^n, and μ_n - a probability measure on $\mathcal{F}_n$, for each $n = 1, 2, \ldots$. Furthermore, the probability measures is required to have, as the range, the unit interval $\mathbb{I}$ of some recursive non-archimedean field containing all rational numbers (e.g., Hardy field $\mathbb{Q}(\varepsilon)$, where ε is an infinitesimal). Thanks to this, the meaning of, e.g., $(\mathrm{CP}\vec{x} \approx 1)(\alpha \mid \beta)$ is roughly: the probabilities of $\{x : \alpha(x)\} \cap \{x : \beta(x)\}$ and $\{x : \beta(x)\}$ are infinitesimally close (i.e., almost the same). A formal system consisting of axioms and rules of inference (two of them are infinitary, i.e. have countably many premisses and one consequence), is provided and proved (in our recent work [2]) to be sound and strongly complete with respect to the proposed semantics. It should be noted that the system is finitary in the sense that all formulas are finite strings of symbols; only the proofs may be infinite. The infinitary rules are applied to infinite sets of formulas, not to infinite formulas of $L_{\omega_1\omega}$.

We will also present two $L_{\omega\omega}^{\mathrm{P},\mathbb{I}}$-fragments which are decidable. The first fragment consists of Boolean combinations of sentences of the form $(\mathrm{CP}\vec{x} \diamond r)(\alpha(\vec{x}) \mid \beta(\vec{x}))$, where $\diamond \in \{\leqslant, \geqslant, \approx\}$ and $\alpha(\vec{x})$ and $\beta(\vec{x})$ are classical formulas (without function symbols and equality sign) with at most four classical quantifiers, but only one alteration (i.e., the quantifier prefix is at most $\exists\exists\forall\forall$ or $\forall\forall\exists\exists$). The second fragment is similar except that now formulas α and β may contain equality sign (and one unary function symbol), but the quantifier prefix is restricted to $\forall\exists$ or $\exists\forall$.

These fragments are based on well-known decidable classes $[\exists^*\forall^2\exists^*, \text{all}]$ (Gödel) and $[\exists^*\forall\exists^*, \text{all}, (1)]_=$ (Shelah).

The central part of the talk will be devoted to possible applications of our logic. In particular, we will focus how $L_{\omega\omega}^{\mathrm{P},\mathbb{I}}$ can be used to model default reasoning and analyse some properties of the corresponding consequence relation. It turns out that System P (which occupies a central position in the hierarchy of nonmonotonic systems, [4]) can be represented in $L_{\omega\omega}^{\mathrm{P},\mathbb{I}}$, where the quantifier $(\mathrm{CP}\vec{x} \approx 1)$ plays a crucial role. Finally, we will discuss the possibility of representing some other formal systems in $L_{\omega\omega}^{\mathrm{P},\mathbb{I}}$-framework.

Acknowledgements

The work presented here is partially supported by the Serbian Ministry of Education and Science through projects 174026 and III044006.

References

[1] Egon Börger, Erich Grädel, and Yuri Gurevich, *The Classical Decision Problem*, Springer, Berlin, Heidelberg, 1997

[2] N. Ikodinović, M. Rašković, Z. Marković, Z. Ognjanović, *A first-order probabilistic logic with approximate conditional probabilities*, Logic Journal of the IGPL 22(4), pp. 539–564, 2014.

[3] H. J. Keisler, *Probability quantifiers*, In J. Barwise and S. Feferman, editors, Model Theoretical Logics, Chapiter XIV, Springer, NY, 1985.

[4] S. Kraus, D. Lehmann, and M. Magidor, *Nonmonotonic reasoning, preferential models and cumulative logics*, Artificial Intelligence 44, pp. 167-207, 1990.

[5] Z. Ognjanović, M. Rašković, and Z. Marković, Probability logics, in Zbornik radova, subseries Logic in computer science 12(20), pp. 35-111, 2009.

Cut in positive relevant logics with permutation

Mirjana Ilić, University of Belgrade, Serbia

Keywords:

relevant logics, sequent calculi, cut rule

The first sequent calculi for positive relevant logics were formulated by Dunn and Minc in [4] and [6]. In those calculi, the cut rule has the following form:

$$\frac{\Pi \vdash \varphi \qquad \Gamma[\varphi] \vdash \gamma}{\Gamma[\Pi] \vdash \gamma}\ (\mathrm{cut})$$

where $\Gamma[\Pi]$ is the result of replacing arbitrarily many occurrences of φ in $\Gamma[\varphi]$ by Π if Π is non–empty, and otherwise by $'t'$. The constant truth $'t'$ is needed to disable the inference of the modal fallacy $\vdash \alpha \to (\beta \to \beta)$. Really, without $'t'$, we would have:

$$\dfrac{\dfrac{\vdash \beta \to \beta \qquad \dfrac{\beta \to \beta \vdash \beta \to \beta}{\alpha, \beta \to \beta \vdash \beta \to \beta}\ \text{(extensional thinning)}}{\alpha \vdash \beta \to \beta}\ \text{(cut)}}{\vdash \alpha \to (\beta \to \beta)}\ (\to \mathrm{r})$$

However, with $'t'$, the admissibility of modus ponens:

$$\frac{\vdash \alpha \qquad \alpha \vdash \beta}{\vdash \beta}$$

cannot be proved. This is the is reason why, once Cut–elimination is established, the occurrences of $'t'$ need to be eliminated.

We propose another formulation of the cut rule, for positive relevant logics with permutation, where the constant $'t'$ is not needed. Our cut rule is of the following forms:

$$\frac{\Pi \vdash \varphi \qquad \Gamma[\varphi] \vdash \gamma}{\Gamma[\Pi] \vdash \gamma}\ (\mathrm{cut{-}i})$$

$$\frac{\vdash \varphi \qquad \varphi \vdash \gamma}{\vdash \gamma}\ (\mathrm{cut{-}iii})$$

$$\frac{\vdash \varphi \qquad \Gamma[\varphi; \Pi] \vdash \gamma}{\Gamma[\Pi] \vdash \gamma}\ (\mathrm{cut{-}ii})$$

where Π is non–empty. In (cut-i), $\Gamma[\Pi]$ is the result of replacing exactly one occurrence of φ in $\Gamma[\varphi]$ by Π, in (cut-ii) the single occurrence of φ in $\Gamma[\varphi; \Pi]$ is replaced by an empty multiset and similarly in (cut-iii).

The various versions of our cut rule, ensure that the modal fallacy remains unprovable. Furthermore, they are enough for the proof of the equivalence between Hilbert–style formulation and the corresponding sequent calculus (e.g., this form of cut is used in the the sequent calculus formulation for the positive contraction–less relevant logic RW_{+}°, in [5]). However, it should be mentioned that the use of $'t'$ remains crucial in sequent calculus for TW_{+} and in sequent calculi for other weaker, permutation–less, relevance logics such as B_{+}, E_{+} and even $T_{\to}$ (there is a sequent calculus for $T_{\to}$ without $'t'$ in [2], however the one with $'t'$ is much easier to use), where $'t'$ precludes intensional structures from becoming scrambled, see e.g. [3].

Acknowledgements

This work is supported by the Ministary of Science and Technology of Serbia, grant number ON174026.

References

[1] A. Anderson, N. Belnap Jr., *Entailment: the logic of relevance and necessity*, vol. 1, Princeton University Press, Princeton, New Jersey, 1975.

[2] K. Bimbó, *Relevant logics*, Philosophy of logic (D. Jacquette, editor), Handbook of the Philosophy of science (D. Gabbay, P. Thagard and J. Woods, editors), vol. 5, Elsevier, pp. 723–789, 2007.

[3] K. Bimbó, J. M. Dunn, *On the decidability of implicational ticket entailment*, The Journal of Symbolic Logic, 78(1), pp. 214–236, 2013.

[4] J. M. Dunn, *A 'Gentzen system' for positive relevant implication*, The Journal of Symbolic Logic 38, pp. 356-357, 1973.

[5] M. Ilić, *An alternative Gentzenization of RW_{+}°*, Mathematical Logic Quarterly, to appear

[6] G. Minc, *Cut elimination theorem for relevant logics,* Journal of Soviet Mathematics 6, pp. 422-428, 1976.

Computational interpretations of the classical Axiom of Choice

Danko Ilik, Inria, France

Keywords:

axiom of choice, proofs-as-programs correspondence, control operators,
type-directed partial evaluation

Hilbert's Program had as the goal to interpret all ideal principles used in mathematical proofs by elementary notions. While Gödel's Incompleteness theorems showed that those notions cannot be finitistic, Gödel's own work on the Dialectica interepretation also showed a way forward: to interpret proofs of classical Arithmetic it suffices to enrich the interpreting language by computation based on primitive recursive functionals in higher types (System T).

Far from being buried by incompleteness phenomena, we can today admire the achievements of the modified Hilbert Program in Algebra (ex. [1]) or Analysis (ex. [2]). The notions of computation that are needed for interpreting classical Analysis, i.e. classical Arithmetic plus the Axiom of Choice, are nevertheless a priori non-trivial extensions of System T. There are two existing approaches. The classic one, that goes back to Kreisel and Spector's extension of T with the schema of *bar recursion* [3], and the newer one using *computational side-effects* from the theory of programming languages (ex. [4]). In this talk, I will briefly survey the two approaches, and then present my own one [5, 6, 7]; this work merges the two existing approaches since it shows that the interpreting language for classical Analysis needs not contain computation schema beyond System T itself.

References

[1] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods*. Springer, 2015.

[2] Ulrich Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics: Proof Interpretations and Their Use in Mathematics*. Springer Science & Business Media, 2008.

[3] Clifford Spector. Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles formulated in current intuitionistic mathematics. *Recursive function theory*, pages 1–27, 1962.

[4] Jean-Louis Krivine. Dependent choice, ‘quote’ and the clock. *Theoretical Computer Science*, 308(1):259–276, 2003.

[5] Danko Ilik. Delimited control operators prove double-negation shift. *Annals of Pure and Applied Logic*, 163(11):1549 – 1559, 2012.

[6] Danko Ilik and Keiko Nakata. A direct version of Veldman’s proof of open induction on Cantor space via delimited control operators. *Leibniz International Proceedings in Informatics (LIPIcs)*, 26:188–201, 2014.

[7] Danko Ilik. An interpretation of the Sigma-2 fragment of classical Analysis in System T. *arXiv*, 1301.5089, 2014.

Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols

**Max Kanovich, Queen Mary, University of London & University College, UK
and National Research University Higher School of Economics
Tajana Ban Kirigin, University of Rijeka, Croatia
Vivek Nigam , Federal University of Paraiba, Brazil
Andre Scedrov, University of Pennsylvania
Carolyn Talcott, SRI International, USA**

Keywords:

Cyber-Physical Security Protocols, Multiset Rewriting, Computational Complexity

Many security protocols rely on the assumptions on the physical properties in which its protocol sessions will be carried out. For instance, Distance Bounding Protocols take into account the round trip time of messages and the transmission velocity to infer an upper bound of the distance between two agents. We classify such security protocols as Cyber-Physical. Time plays a key role in design and analysis of many of these protocols. This paper investigates the foundational differences and the impacts on the analysis when using models with discrete time and models with dense time. We show that there are attacks that can be found by models using dense time, but not when using discrete time. We illustrate this with a novel attack that can be carried out on most distance bounding protocols. In this attack, one exploits the execution delay of instructions during one clock cycle to convince a verifier that he is in a location different from his actual position. We propose a Multiset Rewriting model with dense time suitable for specifying cyber-physical security protocols. We introduce Circle-Configurations and show that they can be used to symbolically solve the reachability problem for our model. Finally, we show that for the important class of balanced theories the reachability problem is PSPACE-complete.

References

[1] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott, *Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols*, 4th Conference on Principles of Security and Trust (POST), London, UK, April 2015. Springer LNCS, Volume 9036, Springer-Verlag, 2015, pp. 259 - 279.

A Rewriting Framework and Logic for Activities Subject to Regulations

Max Kanovich, Queen Mary, University of London & University College, UK
and National Research University Higher School of Economics
Tajana Ban Kirigin, University of Rijeka, Croatia
Vivek Nigam , Federal University of Paraiba, Brazil
Andre Scedrov, University of Pennsylvania
Carolyn Talcott, SRI International, USA
Ranko Perovic, Clinical Research Manager, USA

Keywords:

Multiset Rewriting, Linear Logic, Computational Complexity, Clinical Investigations

Activities such as clinical investigations or financial processes are subject to regulations to ensure quality of results and avoid negative consequences. Regulations may be imposed by multiple governmental agencies as well as by institutional policies and protocols. Due to the complexity of both regulations and activities there is great potential for violation due to human error, misunderstanding, or even intent. Executable formal models of regulations, protocols, and activities can form the foundation for automated assistants to aid planning, monitoring, and compliance checking. We propose a model based on multiset rewriting where time is discrete and is specified by timestamps attached to facts. Actions, as well as initial, goal and critical states may be constrained by means of relative time constraints. Moreover, actions may have non-deterministic effects, i.e., they may have different outcomes whenever applied. We present a formal semantics of our model based on focused proofs of linear logic with definitions. We also determine the computational complexity of various planning problems. Plan compliance problem, for example, is the problem of finding a plan that leads from an initial state to a desired goal state without reaching any undesired critical state. We consider all actions to be balanced, i.e., their pre and post-conditions have the same number of facts. Under this assumption on actions, we show that the plan compliance problem is PSPACE-complete when all actions have only deterministic effects and is EXPTIME-complete when actions may have non-deterministic effects. Finally, we show that the restrictions on the form of actions and time constraints taken in the specification of our model are necessary for decidability of the planning problems.

References

[1] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott, R. Perovic *A Rewriting Framework and Logic for Activities Subject to Regulations*, Mathematical Structures in Computer Science, 2015, 44 pages, Published online 02 June 2015. http://journals.cambridge.org/article_S096012951500016X,

Probabilistic Justification Logic

Ioannis Kokkinis, Institute of Computer Science, University of Bern, Switzerland

Keywords:

probabilistic logic, justification logic, soundness, strong completeness, decidability, complexity

Traditional modal epistemic logic uses formulas of the form $\Box\alpha$ to express that an agent believes α. The language of justification logic [1, 2] 'unfolds' the $\Box$-modality into a family of so-called *justification terms*, which are used to represent evidence for the agent's belief. Hence, instead of $\Box\alpha$, justification logic includes formulas of the form $t : \alpha$ meaning "the agent believes α for reason t". The term t could represent some informal justification or even a mathematical proof for α. Of course, not all justifications for belief are equal. For example we may believe α because some friend of ours has heard about α or because we read about α in the New York Times. It is natural that we cannot put the same credence in both justifications for α. We can reflect this differentiation in credulity by adding to our language an operator that expresses the degree r for which a piece of evidence t can serve as a justification for α, in our notation $P_{\geq r}(t : \alpha)$.

In my talk I am going to introduce the probabilistic justification logics PJ and PPJ, two logics in which we can reason about the probability of justification statements. I will present their syntax and semantics, prove strong completeness theorems and establish their decidability. In the case of logic PJ I am going to establish upper and lower complexity bounds.

The logic PJ is designed as the probabilistic logic LPP_2 [7]. PJ [4] is a a probabilistic logic over the basic justification logic J, that makes it possible to adequately model different degrees of justification. We consider a language that features formulas of the form $P_{\geq s}\alpha$ to express that the justification logic formula α has probability equal to or greater than the rational number s. It is important to note that there is an unpleasant consequence of a finitary axiomatization (i.e. an axiomatization where the proofs are always finite) in such a language: there exist consistent sets that are not satisfiable. This results from the inherent non-compactness of such systems. Consider for example the set $X = \{\neg P_{=0}\alpha\} \cup \{P_{<1/n}\alpha \mid n \in \mathbb{N}\}$. Although it is obvious that X cannot be satisfied, in a finitaty axiomatization it would be consistent: it is impossible to derive falsity from X since every proof from X would contain only a finite number of X's elements.

However, if proofs are allowed to be infinite, we can define an axiomatization in which X would not be consistent. Hence, our axiomatization of PJ should have an infinitary rule, i.e. a rule that has countably infinite premises and one conclusion.

Our semantics consists of a set of possible worlds, each a model of justification logic and a probability measure $\mu(\cdot)$ on sets of possible worlds. As a model for justification logic we use the so-called basic modular models. We assign a probability to a formula α of justification logic as follows: we first determine the set $[\alpha]$ of possible worlds that satisfy α. Then we obtain the probability of α as $\mu([\alpha])$, i.e. by applying the measure function to the set $[\alpha]$. Hence our logic relies on the usual model of probability.

Soundness of our infinitary rule follows from the archimidean property of the real numbers. Strong completeness is established by a canonical model construction.

It is known that the satisfiability problem for the justification logic J belongs to the second level of the polynomial hierarchy [6]. By using some techniques from linear programming we can prove that the satisfiability problem for the logic PJ belongs to the same complexity class [3], i.e. adding probability operators to the language of justification logic J does not increase the complexity of the logic.

The logic PPJ is designed as the probabilistic logic LPP_1 [7]. PPJ [5] is a probabilistic justification logic that allows iterations of the probability operator as well justification operators over probability operators. The axioms of PPJ consist of the axioms of the logic PJ augmented with the axioms of J. The semantics of PPJ is similar to the semantics of PJ. Strong completeness for PPJ is obtained by modifying the completeness proof for PJ. We can establish decidability for the logic PPJ by extending the decidability proof for the logic J. Observe that this extension is not trivial due to the presence of formulas of the form $t : P_{\geq s}\alpha$. However the problem of establishing complexity bounds for the logic PPJ remains open. Another interesting direction for further research is the addition of statistical evidence to our language. For example if the conditional probability of α given β is 0.1 it makes sense to consider β, or better a justification term obtained from β, as a justification for α with probability 0.1.

This a joint work with Petar Maksimović, Zoran Ognjanović and Thomas Studer.

References

[1] Artemov, S.N.: Operational modal logic. Tech. Rep. MSI 95–29, Cornell University (Dec 1995)

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

[3] Kokkinis, I.: On the complexity of probabilistic justification logic, ArXiv e-prints, 2015.

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

[5] Kokkinis, I., Ognjanović, Z., Studer, T.: Probabilistic justification logic. Submitted, 2015.

[6] R. Kuznets. On the complexity of explicit modal logics. In P. G. Clote and H. Schwichtenberg, editors, *Computer Science Logic, 14th International Workshop, CSL 2000, Annual Conference of the EACSL, Fischbachau, Germany, August 21–26, 2000, Proceedings*, volume 1862 of *Lecture Notes in Computer Science*, pages 371–383. Springer, 2000.

[7] Ognjanović, Z., Rašković, M., Marković, Z.: Probability logics. Zbornik radova, subseries "Logic in Computer Science" 12(20), 35–111 (2009)

Local inference rules and simple proof search – a survey

Marcel Maretić, University of Zagreb
Ante Đerek, University of Zagreb

We conduct a survey of local inference rules and their relation to simple proof search in corresponding logical calculus. Our interest in local inference rules is motivated by analytic proof procedures, where proofs are assembled from analytic parts. Proof search is divided in two phases – analysis and synthesis.

We start with a calculus MK – a calculus of natural deductions for classical logic that is based on multiple conclusion inference rules. MK has local inference rules in propositional case, and as-local-as-possible in first order case. Proof search in MK is analytic and actually nothing but a notational variant of Beth's tableau method (details in [3]). Inference rules of first order MK have local appearance, but some these inference rules come with global restrictions which complicate proof assembly. In first order MK these complications are avoided in analysis, leaving synthesis simple (identical to propositional case).

Our approach in modifications to calculus is:

(1) to modify/adapt inference rules of logical calculus to be as local as possible (to at least appear local)

(2) to circumvent complications with careful analytic phase.

In this work we survey how to extend this approach to minimal, intuitionistic and modal logics.

References

[1] Fitting, M., *Proof Methods for Modal and Intuitionistic Logics*, Synthese, 1983.

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

[3] M. Maretić, *On Multiple Conclusion Deductions in Classical Logic*, Glasnik matematički, 2014. submitted.

[4] D. Prawitz, *Natural Deduction: A Proof-Theoretical Study*, Dover reprint, 2006.

[5] Shoesmith D.J., Smiley T.J., *Multiple Conclusion Logic*, Cambridge University Press, 1978.

[6] Smullyan R. M., *First Order Logic*, Courier Dover Publications, 1995.

Representation of Algebraic Structures by Boolean Functions

Smile Markovski, SS Ciryl and Methodius University in Skopje
Simona Samardjiska, Faculty of Computer Sciences and Engineering, Macedonia

Keywords:

Boolean function, conjunction, exclusive disjunction, XOR, algebraic structures, groupoids, groups, quasigroups

Boolean functions are mappings $\{0,1\}^n :\to \{0,1\}$, where 0 and 1 can be interpreted as false and true constant, n is a positive integer. It is well known that each Boolean function $f(x_1,\ldots,x_n)$ with n variables can be presented in its algebraic normal form (ANF)

$$f(x_1,\ldots,x_n) = a_0 + \sum_{I \subset \{1,2,\ldots,n\}} a_I x^I,$$

where $a_0, a_I \in \{0,1\}$, $x^{k_1,k_2,\ldots,k_p} = x^{k_1}x^{k_2}\ldots x^{k_p}$. Here xy means conjunction, while $x+y$ means exclusive disjunction, i.e., XOR function.

If $(G,*)$ is a groupoid of order 2^n, then the operation $*$ can be interpreted as a vector valued Boolean function $*_{v.v.} : \{0,1\}^{2n} :\to \{0,1\}^n$. By using the function $*_{v.v.}$ we can characterize different properties of the groupoid. Interesting results are obtained when the groupoid is a group, a loop, a quasigroup.

References

[1] D. Gligoroski, V. Dimitrova and S. Markovski, *Quasigroups as Boolean Functions, their Equation Systems and Gröbner Bases*, Sala, M.; Mora, T.; Perret, L.; Sakata, S.; Traverso, C. (Eds.), Gröbner Bases, Coding, and Cryptography, Springer 2009.

Impact of Random Bits Injection on the Computational Complexity Based Security of Certain Encryption Approaches

Miodrag Mihaljević, Mathematical Institute SANU, Belgrade, Serbia

Keywords:

encryption, security evaluation, computational complexity, random bits injection, mutual information, the probability of error.

1 Introduction and Preliminaries

We consider effect of a channel with random bits injection regarding security of certain encryption approaches. The work has been motivated by a number encryption approaches including the ones reported in [3], [4] and [5]. We point out that the encryption based on employing the binary insertion channel $\left[X^n \to Y^{(n)}\right]$ provides enhanced security compared to the basic scheme that outputs only X^n.

A definition of security consists of two distinct components: a specification of the assumed power of the adversary, and a description of what constitutes a "break" of the scheme. Generally speaking, a cryptographic scheme is secure in a computational sense, if for every probabilistic polynomial-time adversary $\mathcal{A}$ carrying out an attack of some specified type, and for every polynomial $p(n)$, there exists an integer N such that the probability that $\mathcal{A}$ succeeds in this attack (where success is also well-defined) is less than $\frac{1}{p(n)}$ for every $n > N$. Accordingly, the following two definitions specify a security evaluation scenario and a security statement.

Definition 1: The Adversarial Indistinguishability Experiment. consists of the following steps:

1. The adversary $\mathcal{A}$ chooses a pair of messages $(_0;_1)$ of the same length n, and passes them on to the encryption system for encrypting.

2. A bit $b \in \{0,1\}$ is chosen uniformly at random, and only one the two messages $(_0;_1)$, precisely $_b$, is encrypted into ciphertext $\mathrm{Enc}(_b)$ and returned to $\mathcal{A}$;

3. Upon observing $\mathrm{Enc}(_b)$, and without knowledge of b, the adversary $\mathcal{A}$ outputs a bit b_0;

4. The experiment output is defined to be 1 if $b_0 = b$, and 0 otherwise; if the experiment output is 1, denoted shortly as the event $(\mathcal{A} \to 1)$, we say that $\mathcal{A}$ has succeeded.

Definition 2. An encryption scheme provides indistinguishable encryptions in the presence of an eavesdropper, if for all probabilistic polynomial-time adversaries $\mathcal{A}$

$$\Pr[\mathcal{A} \to 1|\mathrm{Enc}(_b)] \leq \frac{1}{2} + \epsilon \;, \tag{1}$$

where $\epsilon = \mathrm{negl}(n)$ is a negligibly small function.

Definitions 1 and 2 are more precisely discussed in [2].

2 Evaluation of the Security Gain

Our goal is to estimate the advantage of $\mathcal{A}$ in the indistinguishability game in Definition 1 when $\; = \mathrm{Enc}(_b)$ is a particular realization of $Y^{(n)}$. Thereby, we assume that the advantage of $\mathcal{A}$ equals $\frac{1}{2} + \epsilon$ when $_0$ and $_1$ are two chosen realizations of M^n and the corresponding realization of X^n is known.

Theorem: Let the encrypted mapping of M^n into X^n be such that $\frac{1}{2}+\epsilon$ equals the advantage of the adversary $\mathcal{A}$ (specified by Definition 2) to win the indistinguishability game (specified by Definition 1), and let the mutual information $\mathcal{I}_{iud}(X;Y)$ be known. Under these assumptions, for large n,

$$\Pr[\mathcal{A} \to 1|Y^{(n)} = \,] = \frac{1}{2} + \epsilon \cdot \delta, \quad \text{where}$$

$$\delta < \mathcal{I}_{iud}\left(X;Y\right) + \frac{\log_2 \left[\frac{8\pi \mathrm{e} \cdot i \cdot n}{(1-i)^2}\right]}{2n} + O\left(n^{-2}\right).$$

Proof: *Let the index b of the selected message be a realization of the random variable B. The probability that the adversary wins the game equals* $\Pr[\mathcal{A} \to 1|Y^{(n)}{=}\,]{=}\Pr(B{=}b|Y^{(n)}{=}\,)$*, which we further manipulate as follows*[1]

$$\begin{aligned}\Pr[\mathcal{A}{\to}1|\,] = \Pr(b|\,) = \frac{\Pr(b,\,)}{\Pr(\,)} = \frac{\sum \Pr(b,\,,\,)}{\Pr(\,)} \\ = \frac{\sum \Pr(b|\,,\,)\Pr(\,,\,)}{\Pr(\,)} = \frac{\sum \Pr(b|\,)\Pr(\,,\,)}{\Pr(\,)}.\end{aligned} \tag{2}$$

According to the proposition's assumption we have

$$\Pr(b|_b) = \frac{1}{2} + \epsilon \;,$$

[1] When no confusion arises, in order to simplify the notation, we drop the random variable notation when denoting probabilities. For example, we write $\Pr(b|\,)$ to denote $\Pr(B{=}b|Y^{(n)}{=}\,)$. Or, as another example, we write $\Pr(\,,\,)$ to denote $\Pr(Y^{(n)} = \,, X^n = \,)$.

where ${}_b$ corresponds to the selected ${}_b$, and

$$\Pr(b|) = \frac{1}{2}\ , \text{ for any } \neq {}_b\ .$$

Consequently, (2) becomes

$$\begin{aligned}\Pr[\mathcal{A}\to 1|] &= \Pr(b|)\\ &= \frac{\Pr(b|{}_b)\Pr(,{}_b)}{\Pr()} + \frac{\sum_{:\neq_b}\Pr(b|)\Pr(,)}{\Pr()}\\ &= \frac{\left[\frac{1}{2}+\epsilon\right]\Pr(,{}_b)}{\Pr()} + \frac{\frac{1}{2}\sum_{:\neq_b}\Pr(,)}{\Pr()}\\ &= \frac{1}{2}+\epsilon\cdot\Pr({}_b|) = \frac{1}{2}+\epsilon\cdot\delta.\end{aligned}$$

Next, we have the following general upper bound on the entropy (see [6] or [1], for example):

$$H(X^n|Y^{(n)}) \leq h(P_{err}) + P_{err}\log_2(2^n-1)$$

where $h(\cdot)\leq 1$ is the binary entropy function and $P_{err} = 1-\Pr({}_b|)$, implying

$$\begin{aligned}\delta \overset{\Delta}{=} \Pr({}_b|) &< \frac{1}{n}+1-\frac{1}{n}H(X^n|Y^{(n)})\\ &= \frac{1}{n}+\frac{1}{n}I\left(X^n,Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}.\end{aligned} \tag{3}$$

Hence, the information-theoretic quantity of interest is the iud information rate *defined as the information rate between X^n and $Y^{(n)}$ when the symbols X_k are independent and uniformly distributed (iud)*

$$\mathcal{I}_{\text{iud}}\left(X;Y\right) \overset{\Delta}{=} \lim_{n\to\infty}\frac{1}{n}I\left(X^n;Y^{(n)}\right)\Big|_{p(x^n)=2^{-n}}. \tag{4}$$

*The information rate $\mathcal{I}_{\text{iud}}\left(X;Y\right)$ represents the amount of information that the eavesdropper can "*learn*", on average, about X after observing Y. The information rate $\mathcal{I}_{\text{iud}}\left(X;Y\right)$ is not computable in closed-form, but is attainable using Monde-Carlo techniques and bounded as follows*

$$\mathcal{I}_{\text{iud}}(X;Y) \geq \frac{1}{n}I\Big(X^n;Y^{(n)}\Big)\Big|_{p(x^n)=2^{-n}} - \frac{1}{n}H\Big(\mathcal{L}\Big(Y^{(n)}\Big)\Big) \tag{5}$$

$$\mathcal{I}_{\text{iud}}(X;Y) \leq \frac{1}{n}I\Big(X^n;Y^{(n)}\Big)\Big|_{p(x^n)=2^{-n}}. \tag{6}$$

For large n, the correction term $\frac{1}{n}H\big(\mathcal{L}\big(Y^{(n)}\big)\big)$ in (5) equals

$$\frac{1}{n}H\Big(\mathcal{L}\Big(Y^{(n)}\Big)\Big) = \frac{1}{2n}\log_2\left(\frac{2\pi\mathrm{e}\cdot i\cdot n}{(1-i)^2}\right) + O\left(n^{-2}\right)). \tag{7}$$

Substitution of (5) and (7) into (3) finalizes the proof. QED

Accordingly, the encryption mapping $M^n \to Y^{(n)}$ enhances security by a factor δ in comparison to the encryption mapping $M^n \to X^n$ because the probability that $\mathcal{A}$ wins the game becomes closer to $\frac{1}{2}$, which corresponds to random guessing.

Acknowledgements

This work has been supported by the projects ON174008 and III43008 of the Ministry for Education, Science and Technological Development, Republic of Serbia.

References

[1] M. Feder and N. Merhav, "Relations Between Entropy and Error Probability", *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 259-266, Jan. 1994.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC PRESS, Boca Raton, 2007.

[3] M.J. Mihaljević and H. Imai, "An approach for stream ciphers design based on joint computing over random and secret data", *Computing*, vol. 85, no. 1-2, pp. 153-168, June 2009.

[4] M.J. Mihaljević, "A Framework for Stream Ciphers Based on Pseudorandomness, Randomness and Error-Correcting Coding", in *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, Editors B. Preneel, S. Dodunekov, V. Rijmen and S. Nikova, Vol. 23 in the *NATO Science for Peace and Security Series - D: Information and Communication Security*, pp. 117-139, IOS Press, Amsterdam, The Netherlands, June 2009.

[5] F. Oggier and M.J. Mihaljevic, "An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 158-168, Feb. 2014.

[6] D. L. Tebbe and S. J. Dwyer III, "Uncertainty and the Probability of Error", *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 516-518, May 1968.

The ARX structure of π-Cipher

Hristina Mihajloska, FCSE, UKIM, Skopje, Macedonia
Danilo Gligoroski, Department of Telematics, NTNU, Trondheim, Norway
Smile Markovski, SS Ciryl and Methodius University in Skopje
Simona Samardjiska, FCSE, UKIM, Skopje, Macedonia

Keywords:

Authenticated encryption, ARX

The interest for authenticated encryption with associated data was recently intensified with the announced new competition "CAESAR" for authenticated ciphers [1]. The scope of this competition is not just to seek for authenticated modes of operations for AES, but also for proposals of new ciphers that offer advantages over AES-GCM and are suitable for widespread adoption.

π-Cipher is a proposal for an authenticated cipher with associated data for the ongoing "CAESAR" crypto competition. The recent developments with the introduction of AES-NI instructions in latest Intel CPUs [4] made AES-GCM mode really efficient.

The core part of every sponge construction is the permutation function, and the whole security of the primitive relies on it. The design goal for our sponge construction was to obtain a strong permutation, which for different values of the parameter ω (the bit size of the words) provides different features, i.e. to be very efficient when $\omega = 64$ and lightweight when $\omega = 16$.

π-Cipher has an ARX based permutation function which we denote as π function. It uses similar operations as the ones used in the hash function Edon-R [3] but instead of using 8–tuples here we use 4–tuples. The permutation operates on a b bits state and updates the internal state through a sequence of R successive rounds. The state IS can be represented as a list of N 4-tuples, each of length ω-bits, where $b = N \times 4 \times \omega$, i.e.,

$$IS = (\underbrace{(IS_{11}, \dots, IS_{14})}_{I_1}, \underbrace{(IS_{21}, \dots, IS_{24})}_{I_2}, \dots, \underbrace{(IS_{N1}, \dots, IS_{N4})}_{I_N}). \qquad (1)$$

The general permutation function π consists of three main transformations $\mu, \nu, \sigma : \mathbb{Z}_{2^\omega}^4 \to \mathbb{Z}_{2^\omega}^4$, where $\mathbb{Z}_{2^\omega}$ is the set of all integers between 0 and $2^\omega - 1$. These transformations perform diffusion and nonlinear mixing of the input. It uses the following operations:

- Addition + modulo 2^{ω};

- Left rotation (circular left shift) $ROTL^{r}(X)$, where X is an ω–bit word and r is an integer, $0 \leqslant r < \omega$;

- Bitwise XOR operation $\oplus$ on ω–bit words.

Let $= (X_0, X_1, X_2, X_3)$, $= (Y_0, Y_1, Y_2, Y_3)$ and $= (Z_0, Z_1, Z_2, Z_3)$ be three 4-tuples of ω–bit words. Further, let $*$ be defined as:

$$= * \equiv \sigma(\mu() \boxplus_4 \nu()) \tag{2}$$

where $\boxplus_4$ is the component-wise addition of two 4-dimensional vectors in $\left(\mathbb{Z}_{2^{\omega}}\right)^4$.

Table 1: An algorithmic description of the ARX operation $*$ for ω–bit words.

```
**$*$ operation for $\omega$–bit words**

**Input:** $= (X_0, X_1, X_2, X_3)$ and $= (Y_0, Y_1, Y_2, Y_3)$ where $X_i$ and $Y_i$ are $\omega$–bit variables.
**Output:** $= (Z_0, Z_1, Z_2, Z_3)$ where $Z_i$ are $omega$–bit variables.
**Temporary $\omega$–bit variables:** $T_0, \ldots, T_{11}$.

$\mu$–transformation:
    1.  $T_0 \leftarrow ROTL^{r_{1,\omega,1}}(const_{1,\mu\omega} + X_0 + X_1 + X_2)$;
        $T_1 \leftarrow ROTL^{r_{1,\omega,2}}(const_{2,\mu\omega} + X_0 + X_1 + X_3)$;
        $T_2 \leftarrow ROTL^{r_{1,\omega,3}}(const_{3,\mu\omega} + X_0 + X_2 + X_3)$;
        $T_3 \leftarrow ROTL^{r_{1,\omega,4}}(const_{4,\mu\omega} + X_1 + X_2 + X_3)$;
    2.  $T_4 \leftarrow T_0 \oplus T_1 \oplus T_3$;
        $T_5 \leftarrow T_0 \oplus T_1 \oplus T_2$;
        $T_6 \leftarrow T_1 \oplus T_2 \oplus T_3$;
        $T_7 \leftarrow T_0 \oplus T_2 \oplus T_3$;
$\nu$–transformation:
    1.  $T_0 \leftarrow ROTL^{r_{2,\omega,1}}(const_{1,\nu\omega} + Y_0 + Y_2 + Y_3)$;
        $T_1 \leftarrow ROTL^{r_{2,\omega,2}}(const_{2,\nu\omega} + Y_1 + Y_2 + Y_3)$;
        $T_2 \leftarrow ROTL^{r_{2,\omega,3}}(const_{3,\nu\omega} + Y_0 + Y_1 + Y_2)$;
        $T_3 \leftarrow ROTL^{r_{2,\omega,4}}(const_{4,\nu\omega} + Y_0 + Y_1 + Y_3)$;
    2.  $T_8 \leftarrow T_1 \oplus T_2 \oplus T_3$;
        $T_9 \leftarrow T_0 \oplus T_2 \oplus T_3$;
        $T_{10} \leftarrow T_0 \oplus T_1 \oplus T_3$;
        $T_{11} \leftarrow T_0 \oplus T_1 \oplus T_2$;
$\sigma$–transformation::
    1.  $Z_3 \leftarrow T_4 + T_8$;
        $Z_0 \leftarrow T_5 + T_9$;
        $Z_1 \leftarrow T_6 + T_{10}$;
        $Z_2 \leftarrow T_7 + T_{11}$;
```

An algorithmic definition of the $*$ operation over two 4–dimensional vectors and for ω-bit words is given in Table 1. The values of the rotation vectors $r_{1,\omega}$ and $r_{2,\omega}$ and of the constants $const_{i,\mu\omega}$, $const_{i,\nu\omega}$, $i = 1, 2, 3, 4$ used in the μ and

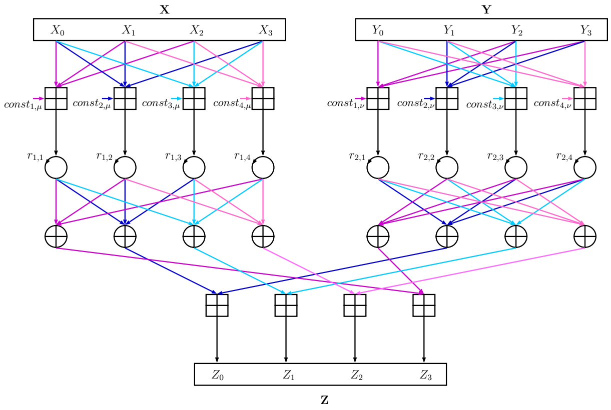

Figure 1: Graphical representation of the ARX operation $*$.

ν transformations are given in the official documentation of the π-Cipher [2]. A graphical representation of the $*$ operation is given in Figure 1.

One round of the cipher is graphically described in Figure 2. In the figure, the diagonal arrows can be interpreted as $*$ operations between the source and destination, and the vertical or horizontal arrows as equality signs " $=$ ".

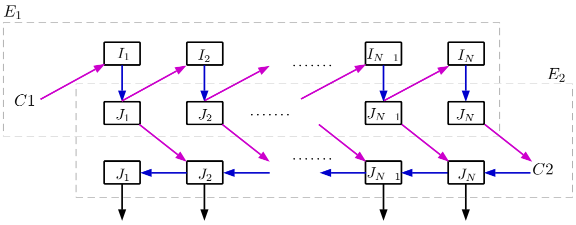

Figure 2: One round of π-Cipher

References

[1] D. J. Bernstein., Caesar: Competition for authenticated encryption: Security, applicability, and robustness. CAESAR web page, 2013. `http://competitions.cr.yp.to/index.html`.

[2] Danilo Gligoroski, Hristina Mihajloska, Simona Samardjiska, Hakon Jacobsen, Mohamed El-Hadedy, and Rune Erlend Jensen. π-cipher v1. Cryptographic competitions: CAESAR, 2014. `http://competitions.cr.yp.to/caesar-submissions.htmls`.

[3] Danilo Gligoroski, Rune Steinsmo Ødegård, Marija Mihova, Svein Johan Knapskog, Ljupco Kocarev, Aleš Drápal, and Vlastimil Klima. Cryptographic hash function EDON-$\mathcal{R}'$. In *1st International Workshop on Security and Communication Networks*, pp. 85–95, Trondheim, Norway.

[4] Shay Gueron., Intel's new aes instructions for enhanced performance and security. In Orr Dunkelman, editor, *FSE*, LNCS vol. 5665, pp. 51–66. Springer, 2009.

On the various definitions of cyclic operads

Pierre-Louis Curien, PPS Laboratory, CNRS, Université Paris Diderot, and Inria, France
Jovana Obradović, PPS Laboratory, Université Paris Diderot, Inria, France, and Faculty of Technical Sciences, University of Novi Sad, Serbia

Keywords:

symmetric operads, cyclic operads, symmetric monoidal category, monad of trees, μ-syntax, species of structures, microcosm principle

The formalism of cyclic operads was originally introduced by Getzler and Kapranov in [1], as an outcome of the *renaissance of operads* that occurred in the early nineties of the last century. They established the notion in the unbiased manner, i.e. by first constructing a monad of unrooted trees, and then defining a cyclic operad to be an algebra over this monad. The motivation came from the framework of cyclic homology: a cyclic operad structure is precisely the enrichment of the (ordinary) operad structure needed to define a cyclic homology for algebras over a given operad. Because of the very nature of their initial purpose, the first biased characterization of cyclic operads (i.e. description by means of individual operadic composition operations) [1, Theorem 2.2] was not given in the "entries only" fashion (according to which operations have entries that are neither input or output), but rather starting from the definition of an ordinary symmetric operad, i.e. from operations with multiple inputs and one output, and then allowing for this output to be exchanged with an input. Moreover, this presentation was skeletal: the arguments of operations were natural numbers rather than finite sets. In [2, Proposition 42] Markl gave a more graspable version of a biased definition of cyclic operads, by means (and with the notation) of explicit partial composition, i.e. by composing only two adjacent operations (as opposed to the classical, i.e. monoidal one, where an operation is composed with "all its neighbours"). Finally, in the appendix of [3], Markl defines (non-skeletal) cyclic operads as structures combining operations that have only (named) entries and no distinguished output.

Our objective is to follow the main line of this evolution, to summarize all the (equivalent) definitions of cyclic operads, and most importantly, to further furnish it by introducing new means of describing them (both from the syntactic and algebraic standpoint) and ultimately linking all concepts into a clear, unified and comprehensive account. Although the ambience for defining cyclic operads can be an arbitrary symmetric monoidal category, we decided to formally introduce them only for the category . More precisely, our cornerstone will be the unital version of the "entries only" approach of Markl in a particular case of a contravariant (and non-skeletal) version $\mathcal{S} : {}^{op} \rightarrow$ of Joyal's species of structures. The reason for choosing the non-skeletal setting is merely the clarity of the presentation we obtain when working with formulas with "named" variables.

The formalisms we deliver and advocate were initially developed with two main goals in mind: to provide cyclic operads with a lightweight syntax on one side, and with a "microcosm principle" modeled definition on the other, both for their biased presentation.

As for the syntactic approach, we wanted to provide a λ-calculus-style syntax which allows for a crisp description of the (somewhat cumbersome) laws of partial composition operation for cyclic operads. Contrary to the common *combinator-style* syntax, whose tokens are operations $f \in \mathcal{S}(X)$ only, the *μ-syntax* we propose has two different kinds of expressions:

$$\frac{c : X}{c ::= \langle s \,|\, t\rangle \;\mid\; \underline{f}\{t_x \,|\, x \in X\}} \qquad \text{and} \qquad \frac{X \,|\, s}{s, t ::= x \;\mid\; \mu x.c}\;,$$

called *commands* (which mimick operations themselves, with no entry selected), and *terms* (representing operations with one selected entry), respectively. The typing rules are as follows:

$$\frac{}{\{x\} \,|\, x} \qquad \frac{f \in \mathcal{S}(X) \qquad \ldots Y_x \,|\, t_x \ldots}{\underline{f}\{t_x \,|\, x \in X\} : \bigcup Y_x} \qquad \frac{X \,|\, s \quad Y \,|\, t}{\langle s \,|\, t\rangle : X \cup Y} \qquad \frac{c : X}{X \backslash \{x\} \,|\, \mu x.c}\;,$$

while the equations are $\langle s \,|\, t\rangle = \langle t \,|\, s\rangle$ and (oriented from left to right):

$$\langle \mu x.c \,|\, s\rangle = c[s/x] \qquad \mu x.\langle x \,|\, y\rangle = y\,.$$

The proof of equivalence of the μ-syntax with the (unbiased) definition of cyclic operads as algebras for a monad (over the category of unrooted trees) revealed a connection to yet another equivalent formalism of cyclic operads: a *reversible term syntax*, introduced by Lamarche as a syntactical approach for defining contexts in linear logic. This proof is also interesting from the perspective of rewriting: the equations of the μ-syntax constitute a non-confluent and terminating system, with the distinct normal forms of a command corresponding in a natural way to different tree traversals of the underlying tree. Combined with the proof of the equivalence of μ-syntax with the usual combinator-style syntax for cyclic operads, our syntactic route consolidates the equivalence of the unbiased and biased standpoints (usually taken for granted in the literature).

On the other hand, our algebraic approach has as a cornerstone the category of species of structures, and is guided by the "microcosm principle" of higher algebra. We introduce two monoidal-like definitions of cyclic operads, one for the original "exchangable single output" characterisation and the other for the "entries only" version.

The product on species needed to formulate the "entries only" definition algebraically is

$$S\blacktriangle T := (\partial S)\cdot(\partial T),$$

where the expression on the right-hand side denotes the (usual) product of derivatives of the species S and T. It turned out that this product satisfies the identity given by the isomorphism

$$\gamma : (S\blacktriangle T)\blacktriangle U + T\blacktriangle(S\blacktriangle U) + (T\blacktriangle U)\blacktriangle S \to S\blacktriangle(T\blacktriangle U) + (S\blacktriangle U)\blacktriangle T + U\blacktriangle(S\blacktriangle T),$$

which, when "unfolded", consists of six terms on each side. By adequately pairing these terms, we were able to define a cyclic operad as a pair $(S, \rho : S\blacktriangle S \to S)$, such that ρ commutes in the appropriate way with γ. The other definition will be discussed in the talk.

Starting from these two definitions, and relying on a result of Lamarche coming from the descent theory of species, we efficiently obtained an unambiguous correspondence between the two points of view on cyclic operads.

References

[1] E. Getzler, M. Kapranov, *Cyclic operads and cyclic homology*, (Geom., Top., and Phys. for Raoul Bott), International Press, Cambridge, MA, pp. 167–201, 1995.

[2] M. Markl, *Operads and PROPs*, arXiv:math/0601129.

[3] M. Markl, *Modular envelopes, OSFT and nonsymmetric (non-Σ) modular operads*, arXiv:1410.3414.

Finite model property of interpretability logics via filtrations

Tin Perkov, Polytechnic of Zagreb, Croatia
Mladen Vuković, University of Zagreb, Croatia

Keywords:

modal logic, interpretability logic, generalized Veltman semantics, finite model property, filtration

The filtration method is often used to prove the finite model property of modal logics. We adapt this technique to the generalized Veltman semantics for interpretability logics. In order to preserve the defining properties of generalized Veltman models, we use bisimulations to define adequate filtrations. Shehtman [2] used a similar modification of the filtration method to prove the finite model property for some products of modal logics. We give an alternative proof of the finite model property of interpretability logic **IL** w.r.t. Veltman models, and we prove the finite model property of the systems and $\mho$ w.r.t. generalized Veltman models.

Provability logic **GL** (Gödel, Löb) is a standard modal logic interpreted on transitive and reverse well–founded Kripke frames, which treats provability predicate as a modal operator. The axioms of **GL** are all instances of classical tautologies, $\Box(A \to B) \to (\Box A \to \Box B)$, and $\Box(\Box A \to A) \to \Box A$. The inference rules are modus ponens and necessitation $A/\Box A$.

The interpretability logic **IL**, introduced by Visser [3], is an extension of provability logic with a binary modal operator $\rhd$. This operator stands for interpretability, considered as a relation between extensions of a fixed theory. It is a nonstandard modal logic, and the basic semantics are Veltman models. These are built over standard transitive and reverse well–founded Kripke models, enriched by binary relations S_w between worlds accessible from each world w. Axioms of **IL** are all axioms of **GL** and the following: $\Box(A \to B) \to A \rhd B$, $(A \rhd B \wedge B \rhd C) \to A \rhd C$, $(A \rhd C \wedge B \rhd C) \to (A \vee B) \rhd C$, $A \rhd B \to (\Diamond A \to \Diamond B)$, and $\Diamond A \rhd A$. The inference rules are modus ponens and necessitation. De Jongh and Veltman [1] proved the completeness of the system **IL** w.r.t. finite Veltman models.

Our aim is to apply the filtration technique to prove finite model property of **IL** and its extensions w.r.t. *generalized* Veltman semantics, introduced by de Jongh. We were not successful in defining filtration of Veltman models. Generalized Veltman models also have relations S_w, but between R–successors and *sets* od R–

successors of w. This feature allows more freedom in constructing S_w–successors, which was essential at a certain point in the proof of the main result.

References

[1] D. de Jongh, F. Veltman, Provability logics for relative interpretability, in: P. P. Petkov (ed.), *Mathematical Logic, Proceedings of the 1988 Heyting Conference*, Plenum Press, New York, 1990, pp. 31–42.

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

[3] A. Visser, Interpretability logic, in: P. P. Petkov (ed.), *Mathematical Logic, Proceedings of the 1988 Heyting Conference* Plenum Press, New York, 1990, pp. 175–210.

A logic with upper and lower probability operators

Nenad Savić, Faculty of Technical Sciences, University of Novi Sad, Serbia
Dragan Doder, Computer Science and Communications, University of Luxembourg
Zoran Ognjanović, Mathematical Institute SANU, Serbia

Keywords:

Probabilistic Logic, Upper and Lower Probabilities, Axiomatization, Completeness theorem.

Abstract

We present a propositional logic with unary operators that speak about upper and lower probabilities. We describe the corresponding class of models and discuss decidability issues. We provide an infinitary axiomatization for the logic and we prove that the axiomatization is sound and strongly complete. For some restrictions of the logic we provide finitary axiomatic systems.

Acknowledgements

This work was supported by the National Research Fund (FNR) of Luxembourg through project PRIMAT, and by the Serbian Ministry of Education and Science through projects ON174026, III44006 and ON174008.

References

[1] B. Anger, J. Lembcke, *Infnitely subadditive capacities as upper envelopes of measures*, Zeitschrift fur Wahrscheinlichkeitstheorie und Verwandte Gebiete, pp. 403-414, 1985.

[2] R. Fagin, J. Halpern, N. Megiddo, *A logic for reasoning about probabilities*, Information and Computation, pp. 78-128, 1990.

[3] J. Y. Halpern, R. Pucella, *A Logic for Reasoning about Upper Probabilities*, Journal of Artificial Intelligence Research, pp. 57-81, 2002.

[4] Z. Ognjanović, M. Rašković, *Some probability logics with new types of probability operators*, Journal of Logic and Computation, pp. 181-195, 1999.

What is Probability Logic?

Zvonimir Šikić, University of Zagreb

Keywords:

mathematical probability, probability logic

The question is what are the (contentwise) factual and historical relations between mathematical probability theory and probability logic.

A Noncommutative Continuum: Brower and Weyl Revisited

Vladimir Tasić, University of New Brunswick, Fredericton, Canada

Keywords:

Brouwer, Weyl, continuum, semigroup algebras, C^*-dynamical systems

The goal of this experiment is to partially emulate in the standard foundational framework some features of the intuitionist continuum, loosely based on the ideas of Brouwer and Weyl. The approach is philosophically promiscuous and freely uses non-intuitionistic mathematics. In particular, it relies on the theory of semigroup C^*-algebras and semigroup crossed products. The philosophical abomination is perhaps mitigated by an intriguing discovery: algebras arising in this inquiry turn out to be of independent interest operator theory, noncommutative geometry and, rather unexpectedly, mathematical physics

According to Brouwer (and, for a time, Weyl), the continuum should be regarded as the collection of 'sequences of nested intervals whose measure converges to zero.' These nested interval sequences *themselves* should be considered the real numbers: 'We call such an indefinitely proceedable sequence of nested intervals a point P or a real number P. We must stress that the point P *is* the sequence [...] *itself*; not something like "the limiting point" to which, according to the classical view, the intervals converge' ([3]).

Further, in Brouwer's view, shaped by his philosophy of mathematics, the interval sequences should be viewed as developing or unfolding: the continuum should be seen as *dynamical*. Absent the dynamics introduced by choice acts of Brouwer's 'ideal mathematician', an algebraic structure that partly reflects these views within the framework of standard (that is, non-intuitionist) mathematics should have the following features: (1) it represents descending interval sequences; (2) it is a dynamical system; and (3) it has enough algebraic and analytic structure to allow for interesting connections with contemporary mathematics.

The 'models' of the continuum proposed here are C^*-dynamical systems: crossed products of a commutative C^*-algebra by a semigroup associated in a natural way to descending sequences of intervals. To motivate the idea, we borrow a starting point from numerical analysis and computer arithmetic, which are naturally concerned with interval computations.

Each interval is determined by its centre and its radius, and hence can be written uniquely in the form $x + \varepsilon y = [x - y, x + y]$. Discarding pure points (intervals of radius $y = 0$), intervals can be identified pairs (x, y) and hence with the connected component of identity of the real affine group, $\mathrm{Aff}_0(\mathbb{R}) \cong \mathbb{R} \rtimes \mathbb{R}_+^\times$. We now impose the group multiplication on intervals. The significance of this choice is that reverse inclusion of intervals corresponds to right multiplication by subintervals of $\varepsilon = [-1, 1]$. Subintervals of ε form a submonoid $M_\mathbb{R}$ of $\mathrm{Aff}_0(\mathbb{R})$, and it is not difficult to see that semigroup words represent descending sequences of intervals: for $s_1, \ldots, s_n \in M_\mathbb{R}$,

$$s_1 \supseteq s_1 s_2 \supseteq \cdots \supseteq s_1 s_2 \cdots s_n.$$

Since matrix addition takes us outside of the group, addition is introduced by artifice. Rather than making an arbitrary choice, take the most general algebra containing the affine group. We are not bound by Brouwer's foundational outlook, so we can introduce analytic structure by passing to the group C^*-algebra. This is not quite the model we want but it is remarkable that viewing $C^*(\mathrm{Aff}_0(\mathbb{R}))$ as an interval algebra resolves certain difficulties with physical interpretations of λ-Miknowski space-time, a noncommucative algebra of interest in mathematical physics (see [1]). Namely, the momentum algebra $\mathcal{M}_\lambda$ of λ-Minkowski spacetime is essentially the unique (up to the sign of λ) noncommucative representation of the interval algebra $C^*(\mathrm{Aff}_0(\mathbb{R}))$.

To move a little closer to Brouwer and Weyl, we should look at rational intervals, identified as above with the rational affine group. Further, to reflect the descending sequences, we must work with a *semigroup* algebra rather than the full group algebra. The set of subintervals of $[-1, 1] \cap \mathbb{Q}$ is a submonoid of $\mathrm{Aff}_+(\mathbb{Q})$. The monoid M 'encodes' descending chains of rational intervals by right multiplication. This motivates the main definition:

Definition 1. *A 'model' of the continuum is defined as the semigroup C^* algebra $\mathcal{C}(M)$ of the submonoid M of the rational affine group: the restriction to $\ell^2(M)$ of the left regular representation of* $\mathrm{Aff}_+(\mathbb{Q})$.

The situation corresponds exactly to Nica's construction of semigroup C^*-algebras for quasi-lattice ordered groups [2]. The structure of the algebra $\mathcal{C}(M)$ can be described as follows. For every interval $x \in M$, let P_x denote the projection on the subspace $\ell^2(xM) \subseteq \ell^2(M)$. Since the principal right ideal $xM \lhd M$ consists of intervals contained in x, P_x is the projection onto the subspace generated by subintervals of x. These projections generate an abelian algebra B_M since $P_x P_y = P_{x \cap y}$ (with the convention that $P_{x \cap y} = 0$ if $x \cap y$ is empty or a point). The monoid M acts on the algebra B_M by endomorphisms $\varphi_x(P_y) = P_{xy}$. The endomorphisms are implemented by isometries v_x such that $v_x P_y v_x^* = P_{xy}$ (and hence $v_x v_x^* = P_x$). $\mathcal{C}(M)$ is the C^*-algebra generated by the isometries v_x, and is the semigroup crossed product $B_M \rtimes_\varphi M$: a semigroup dynamical system.

It is useful to have in mind a dual description. Let Ω_M be the space of filters on M (considered as a poset). With the product topology induced from 2^M, Ω_M is a compact space now known as the Nica spectrum, and $C(\Omega_M)$ is the dual of the commutative algebra generated by projections $P_x = v_x v_x^*$, $x \in M$. By Nica's results, $\mathcal{C}(M)$ is isomorphic to the crossed product $C(\Omega_M) \rtimes M$.

Proposition 1. *The maximal abelian subalgebra of the continuum $\mathcal{C}(M)$ provides a natural Heyting algebra semantics, with propositions represented by projections associated to right ideals of the monoid M.*

Submonoids $S \subseteq M$ can induce a partial order on $\mathrm{Aff}_+(\mathbb{Q})$ in the same way as M. The monoid M gives the finest 'graining" of the continuum, with all descending sequences of rational intervals allowed; submonoids $S \subseteq M$ can be viewed as inducing coarser discretizations of the continuum.

For example, the submonoid F_2 generated by the partition into two subintervals $[-1, 0]$ and $[0, 1]$ is free; the 'continuum' corresponding to F_2 is known as the Cuntz-Toeplitz algebra $\mathcal{T}_2$: its maximal abelian subalgebra is the algebra of continuous functions on the Cantor space (the Cayley tree of F_2), and the monoid acts by shifts.

Brouwer and Weyl preferred dyadic intervals of the form $\frac{m}{2^n} + \frac{1}{2^n}\varepsilon = [\frac{m-1}{2^n}, \frac{m+1}{2^n}]$. The group generated by these intervals is the Baumslag-Solitar group, also known as the 'wavelet group'. As a dynamical system, it is the dyadic solenoid (bilateral Bernoulli shift). Since the Baumslag-Solitar group is not free, it follows that different discretizations can lead to non-isomorphic algebras.

It is fascinating that algebras arising in this experiment relate to Cuntz and Cuntz-Toeplitz algebras, as well to the Bost-Connes dynamical system, objects of independent interest in mathematical physics and non-commutative geometry. The situation becomes even more remarkable in higher dimensions. In 3 dimensions, the monoid acts on continuous functions on a compactification of the space of future cones in the sense of special relativity.

References

[1] A. Agostini, *κ-Minkowski representations on Hilbert spaces*, Journal of Mathematical Physics 48, 052305, 2007.

[2] A. Nica, *C^*-algebras generated by isometries and Wiener-Hopf operators*, Journal of Operator Theory 27, pp. 17–52, 1992.

[3] W. P. van Stigt, *Brouwer's Intuitionism*, North-Holland, 1990.

Proving formal properties of the Chord protocol using Isabelle

Milan Todorović, Mathematical Institute SANU, Serbia
Aleksandar Zeljić, Department of Information Technology, Uppsala University, Uppsala, Sweden
Bojan Marinković, Mathematical Institute SANU, Serbia
Paola Glavan, University of Zagreb, Croatia
Zoran Ognjanović Mathematical Institute SANU, Serbia

1 Summary

An overlay network [9] is a structure that is independent of the underlying network that is actually connecting devices. It represents a logical look on organization of the resources. Usually, the nodes of an overlay network form a well defined structure and one of the most important aspects for proper functioning of that system is to maintain the correct organization of the resources in the desired structure, i.e., to be structurally correct.

Some of the overlay networks are realized in the form of Distributed Hash Tables (DHT). DHTs provide a lookup service similar to a hash table; $\langle key, value \rangle$ pairs are stored inside a DHT, and any participating node can efficiently retrieve the value associated with a given key. DHT can scale to extremely large number of nodes and to handle continual node arrivals, departures, and failures.

The Chord protocol [6, 7, 8] is one of the first, simplest and most popular DHTs. The specification of the Chord analyzed here has been written following the specification given in [5], which was developed according to [8, 2, 10].

Authors of [6, 7, 8, 4] proposed a probabilistic approach to analyze the (structural) correctness of the Chord protocol. They proved that in a model of executions without failure of nodes, after any sequence of the join operations, the considered network will be brought to a stable state.

Our aim is to verify correctness of the Chord protocol using Isabelle/HOL proof assistant. This is motivated by the obvious fact that it is difficult to reproduce errors in concurrent systems only by program testing, and the fact that several non-relational database management systems (NRDBMS) [3, 1] have been developed based on the Chord like technology. To analyze their behavior, it might be useful to characterize situations when correctness of the underlying protocol holds.

We define a maximal set of executions, called regular runs, that satisfy a minimal set of constraints, for which we prove correctness, i.e., that after any sequence of operations (with possible failures of nodes), the network will be brought to a stable state.

References

[1] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach, M. Burrows, T. Chandra, A. Fikes, R. E. Gruber. *Bigtable: A distributed storage system for structured data.* In *Proceedings of the* 7^{th} *Conference on Usenix Symposium on Operating Systems Design and Implementation*, Volume 7, pages 205–218, 2006.

[2] Distributed and Mobile Systems Group Lehrstuhl für Praktische Informatik Universität Bamberg. *open-chord v. 1.0.5 implementation*, 2008.

[3] A. Lakshman, P. Malik. *Cassandra - A Decentralized Structured Storage System.* In *ACM SIGOPS Operating Systems Review*, Volume 44, Issue 2, pages 35–40, 2010.

[4] 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.

[5] B. Marinković, P. Glavan, Z. Ognjanović. *Description of the Chord Protocol using ASMs Formalism.* `arXiv:1208.0712v1`, (in review).

[6] 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.

[7] 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.

[8] 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.

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

[10] V. Tru'o'ng. *Testing implementations of Distributed Hash Tables.* MSc thesis, IT Univesity of Göteborg, 2007.