9TH INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2020

September 21 - 25, 2020
Dubrovnik, Croatia

held as a hybrid meeting

Book of Abstracts

Course directors:

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

Book of Abstracts of the 9^{th} International Conference on Logic and Applications - LAP 2020, held as a hybrid meeting hosted by the Inter University Center Dubrovnik, Croatia, September 21 - 25, 2020.

LaTeX book of abstracts preparation and typesetting:

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

LAP 2020 Web site: `http://imft.ftn.uns.ac.rs/math/cms/LAP2020`
Maintained by Nenad Savić, University of Bern

Contents

Modelling Resource and Timing Aspects of Security Protocols

Abraão Aires Urquiza[1], **Musab A. AlTurki**[2,3], **Max Kanovich**[4,5], **Tajana Ban Kirigin**[6], **Vivek Nigam**[7,1], **Andre Scedrov**[8,5], **Carolyn Talcott**[9]

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

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

Formal methods in protocol security verification led to discovery of a number of attacks and countermeasures. Even though valid protocol verification should rely on the careful formalization of all the relevant assumptions of the protocol execution, some aspects important to protocol security, such as time and resources, are not covered by many formal models. While timing issues involve *e.g.*, network delays and timeouts, resources such as memory, processing power, or network bandwidth are at the root of Denial of Service (DoS) attacks which have been a serious security concern. It is particularly useful in practice and more challenging for formal protocol verification to determine whether a service is vulnerable not only to powerful intruders, but also to resource-bounded intruders that cannot generate or intercept arbitrarily large volumes of traffic.

This paper introduces a multiset rewriting model for the specification and verification of resource and timing aspects of protocols, such as network delays, timeouts, distance bounding properties, and DoS attacks. We propose timed protocol theories that specify service resource usage during protocol execution. Also, a refined Dolev-Yao intruder model is proposed, that can only consume at most some specified amount of resources in any given time window.

We formally define the *DoS problem* that takes into account the duration of the attack. It is shown that the proposed DoS problem is undecidable in general and is PSPACE-complete for the class of balanced resource-bounded systems. Additionally, protocol theories for protocols particularly susceptible to time, such as *e.g.*, distance-bounding protocols, are proposed and some decidable fragments of related verification problems, such as the *secrecy problem*, are described.

Acknowledgments

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

References

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

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

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

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

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

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

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

Beyond Geometric Validity - Two levels of relative validity

Matthaios Bournazos

In the last 60 years there have been numerous attempts by logicians and computer scientist for a mathematical formalism of argumentation, usually focusing on logically valid argumentation. While really useful when the goal is that of decision-making, these proposals have little to offer when we seek to formalise real-life argumentation, because the latter usually consist of incomplete, or even fallacious arguments. Inspired by the philosophical work of the pragma-dialecticians, we introduced in [3] a definition for the concept of argument which allows for the inclusion of invalid and incomplete argumentation, based on the work first presented in [2]. In this paper we present two proofs regarding, on the one hand, the inclusion in our approach of the concept of logically valid argument, as the latter was formalised by Besnard and Hunter[1] and, on the other, the substantially wider range of our definition for an argument.

References

[1] Besnard, P. , Hunter, A. *"Elements of Argumentation"*, *The MIT Press*, 2008

[2] Bournazos, M. *"Logic and Rhetoric"*, *Diploma Thesis (supervisor: Petros Stefaneas)*, National Technical University of Athens, Department of Mathematics, Athens 2019

[3] Bournazos, M., Stefaneas, P. *"ON ARGUMENTS, FALLACIES AND CRITICAL VALIDITY"*, *Algebra and Model Theory 12*, Novosibirsk State Technical University, 2019

[1] See [1].

Universal frames for GL and IL

Vedran Čačić [1]

[1] *Department of Mathematics, University of Zagreb*
Bijenika cesta 30, Zagreb
E-mail: [1] veky@math.hr

Keywords:
Provability and interpretability logic, Kripke and Veltman frames, universality

Provability logics are modal logics developed as an attempt to characterize and generalize the Gödel's incompleteness theorems, enumerating what axioms a provability predicate must satisfy so Gödel's proofs work. The most famous, and most successful, of these systems is GL (the Gödel–Löb system). It is the provability logic of various mathematical theories.

Further generalizations were made by A. Visser, trying to define a framework to answer the finer questions of interpretability (relative strength) of extensions of theories, not just black-and-white questions about provability, refutability or consistency. Such developments gave rise to Interpretability logic (IL) and its various extensions. As opposed to GL, there is no one single framework, but different mathematical theories have different interpretability logics. However, all of these are supersystems of IL.

As a modal logic with standard $\Box$ and $\Diamond$ operators, GL has the ordinary Kripke frames (worlds and accessibility relation) as the back-bone for its models. IL, having a binary modal operator $\rhd$, has accordingly more complicated structures in their place, named *Veltman frames*.

The usual notion of Kripke/Veltman *model* is the frame with the forcing relation, which relates worlds to propositional variables (and by extension, modal formulas). Here we aren't concerned with models, since we look only at closed fragments (without propositional variables).

Usually, for each satisfiable modal formula we must find a separate model (or a frame if the formula is closed), *and* a world within it, such that the formula is forced there. But we can ask whether there is one "global" frame, such that it has the representative worlds for every satisfiable formula. The similar concept is captured in graph theory by the notion of *random graph*.

We define one natural notion of universality for frames of various modal logics, and we prove that GL has a universal frame, while IL doesn't.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation, project CompStruct (IP-2018-01-7459).

Logical formalization of Bayesian concepts of confirmation

Šejla Dautović [1], Dragan Doder [2], Zoran Ognjanović [3]

[1,3] *Mathematical Institute of Serbian Academy of Sciences and Arts*
Kneza Mihaila 36, 11000 Belgrade, Serbia
[2] *Utrecht University, Department of Information and Computing Sciences*
Buys Ballotgebouw, Princetonplein 5, 3584 CC Utrecht, The Netherlands
E-mail: [1] shdautovic@mi.sanu.ac.rs, [2] d.doder@uu.nl, [3] zorano@mi.sanu.ac.rs

Keywords:
Probabilistic logic, Measure of confirmation, Completeness theorem, Decidability.

Although contemporary Bayesian confirmation theorists investigated degrees of confirmation developing a variety of different probability-based measures, that field attracted little attention from the logical side, probably because of complexity of a potential formal language that would be adequate to capture those measures. In Carnap's book [2], one of the main tasks is "the explication of certain concepts which are connected with the scientific procedure of confirming or disconfirming hypotheses with the help of observations and which we therefore will briefly call *concepts of confirmation*". Carnap distinguished three different semantical concepts of confirmation: the classificatory concept ("a hypothesis A is confirmed by an evidence B"), the comparative concept ("A is confirmed by B at least as strongly as C is confirmed by D") and the quantitative concept of confirmation. The third one, one of the basic concepts of inductive logic, is formalized by a numerical function c which maps pairs of sentences to the reals, where $c(A, B)$ is the *degree of confirmation* of the hypothesis A on the basis of the evidence B. Bayesian epistemology proposes various candidate functions for measuring the degree of confirmation $c(A, B)$, defined in terms of subjective probability. They all agree in the following qualitative way: $c(A, B) > 0$ iff the posterior probability of A on the evidence B is greater than the prior probability of A (i.e., $\mu(A|B) > \mu(A)$), which correspond to the classificatory concept ("A is confirmed by B") [10]. Up to now, only the classificatory concept of confirmation is logically formalized, in our previous work [4].

In this paper, we formalize the quantitative concept of confirmation, first within a propositional logical framework $\mathrm{LPP}_1^{\mathrm{conf}}$, and then using its first-order extension $\mathrm{LFOP}_1^{\mathrm{conf}}$. We focus on the most standard (according to Eells and

Fitelson [8]) measure of degree of confirmation, called *difference* measure:

$c(A, B) = \mu(A|B) - \mu(A)$. Our formal languages extend classical (propositional/first order) logic with the unary probabilistic operators of the form $P_{\geq r}$ ($P_{\geq r}\alpha$ reads "the probability of α is at least r"), where r ranges over the set of rational numbers from the unit interval [15], and the binary operators $c_{\geq r}$ and $c_{\leq r}$, which we semantically interpret using the difference measure. The corresponding semantics consists of a special type of Kripke models, with probability measures defined over the worlds.

Our main results are sound and strongly complete (every consistent set of formulas is satisfiable) axiomatizations for the logics. We prove completeness using a modification of Henkin's construction. Since the logics are not compact, in order to obtain the strong variant of completeness, we use infinitary inference rules. An obvious alternative to an infinitary axiomatization is to develop a finitary system which would be weakly complete ("a formula is a theorem iff it is valid"). However, already for the logics which need to express conditional probabilities, that task turned out to be very hard to accomplish. Fagin, Halpern and Meggido [9] faced problems when they tried to represent conditional probabilities via a logical language with polynomial weight formulas that allow products of terms (e.g., $w(p_1 \wedge p_2) \cdot (w(p_1) + w(p_2)) \geq w(p_1) \cdot w(p_2)$ represents the sentence "the conditional probability of p_2 given p_1 plus the conditional probability of p_1 given p_2 is at least 1"). They observed that even for obtaining the weak completeness additional expressiveness is needed, and they introduced a first-order language such that variables can appear in formulas. As an alternative, the researchers from the field of probability logic use the infinitary approaches [3] and fuzzy approaches [13]. In the case of first-order probability logics the situation is even worse, since the set of valid formulas of the considered logics is not recursively enumerable [1, 11]. As a consequence, no finitary axiomatization, which would be even weakly complete, is possible.

From the technical point of view, we modify some of our earlier methods presented in [5, 6, 7, 14, 16, 17]. We point out that our formal languages are countable and all formulas are finite, while only proofs are allowed to be infinite. However, for some restrictions of the logics we provide finitary axiomatic systems. We also prove that our propositional logic $\mathrm{LPP}_1^{\mathrm{conf}}$ is decidable.

Acknowledgment

This work was supported by the Serbian Ministry of Education, Science and Technological Development trough the Mathematical Institute of the Serbian Academy of Sciences and Arts.

References

[1] Abadi, M., Halpern, J.Y., *Decidability and Expressiveness for First-Order Logics of Probability*, Inf. Comput., 1994.

[2] Carnap, R., *Logical Foundations of Probability*, The University of Chicago Press, 1962.

[3] Doder, D., Marinković, B., Maksimović, P., Perović, A., *A Logic with Conditional Probability Operators*, Publications de L'Institut Mathematique, 2010.

[4] Doder, D., Ognjanović, Z., *Probabilistic logics with independence and confirmation*, Springer, 2017.

[5] Doder, D., *A logic with big-stepped probabilities that can model nonmonotonic reasoning of system P*, Publications de L'Institut Mathematique, 2011.

[6] Doder, D., Ognjanović, Z., *A Probabilistic Logic for Reasoning about Uncertain Temporal Information*, AUAI Press, 2015.

[7] Doder, D., Ognjanović, Z., Marković, Z., *An Axiomatization of a First-order Branching Time Temporal Logic*, Journal of Universal Computer Science, 2010.

[8] Eells, E., Fitelson, B., *Measuring Confirmation and Evidence*, Journal of Philosophy, 2000.

[9] Fagin, R., Halpern, J.Y., Megiddo, N., *A logic for reasoning about probabilities*, Information and Computation, 1990.

[10] Fitelson, B., *The Plurality of Bayesian Measures of Confirmation and the Problem of Measure Sensitivity*, University of Chicago Press, 1999.

[11] Halpern, J.Y., *An Analysis of First-Order Logics of Probability*, Artif. Intell., 1990.

[12] Hughes, G.E., Cresswell, M. J.,*A companion to modal logic*, Methuen London, 1984.

[13] Marchioni, M., Godo, L., *A Logic for Reasoning About Coherent Conditional Probability: A Modal Fuzzy Logic Approach*, Springer, 2004.

[14] Marinković, B., Ognjanović, Z., Doder, D., Perović, A., *A propositional linear time logic with time flow isomorphic to* ω^2, J. Appl. Log., 2014.

[15] Ognjanović, Z., Rašković, M., *Some first-order probability logics*, Theoretical Computer Science, 2000.

[16] Savić, N., Doder, D., Ognjanović, Z., *Logics with lower and upper probability operators*, Int. J. Approx. Reason., 2017.

[17] Tomović, S., Ognjanović, Z., Doder, D., *Probabilistic Common Knowledge Among Infinite Number of Agents*, Springer, 2015.

Kripke-style semantics for Full Simply Typed Lambda Calculus

Simona Kašterović [1], **Silvia Ghilezan** [2,3]

[1,2] *University of Novi Sad*
[3] *Mathematical Institute SASA*
E-mail: [1] simona.k@uns.ac.rs, [2] gsilvia@uns.ac.rs

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

In [1] we have introduced a Kripke-style semantics for *full simply typed lambda calculus*, i.e. simply typed lambda calculus extended with product types and sum types. We have proved that the type assignment system is sound with respect to the proposed semantics and we conjectured the completeness of type assignment system.

Since then, we proved the completeness. Meanwhile, we have decided to work on the refinement of the proposed semantics. The motivation for the refinement was the fact that with the semantics of [1] there are bases which are inconsistent and satisfiable. Our goal was to define a semantics such that inconsistent bases are not satisfiable. We have defined a new Kripke-style semantics for full simply typed lambda calculus in [2] and proved soundness and completeness of the type assignment system for full simply typed lambda calculus with respect to the proposed semantics. In this talk, we discuss the approach and results presented in [2] and highlight the improvements with regard to results in [1].

We recall some basic notions of full simply typed lambda calculus, $\Lambda^{\rightarrow,\times,+}$([4], [5]). The language of the full simply typed lambda calculus is generated by the following grammar:

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

where x is a term-variable. Types are generated by the grammar:

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

where a is a type-variable. We say that a statement $M : \sigma$ is derivable from a basis Γ, denoted by $\Gamma \vdash M : \sigma$ if the typing judgment $\Gamma \vdash M : \sigma$ can be derived by the rules in Figure 1.

$$\frac{x:\sigma \in \Gamma}{\Gamma \vdash x:\sigma}\ (\text{Ax}) \qquad \frac{\Gamma, x:\sigma \vdash M:\tau}{\Gamma \vdash \lambda x.M:\sigma\to\tau}\ (\to \text{intro})$$

$$\frac{\Gamma \vdash M:\sigma\to\tau \qquad \Gamma \vdash N:\sigma}{\Gamma \vdash MN:\tau}\ (\to \text{elim}) \qquad \frac{\Gamma \vdash M:\sigma \qquad \Gamma \vdash N:\tau}{\Gamma \vdash \langle M,N\rangle:\sigma\times\tau}\ (\times \text{ intro})$$

$$\frac{\Gamma \vdash M:\sigma\times\tau}{\Gamma \vdash \pi_1(M):\sigma}\ (\times \text{ elim1}) \qquad \frac{\Gamma \vdash M:\sigma\times\tau}{\Gamma \vdash \pi_2(M):\tau}\ (\times \text{ elim2})$$

$$\frac{\Gamma \vdash M:\sigma}{\Gamma \vdash \text{in}_1(M):\sigma+\tau}\ (+ \text{ intro1}) \qquad \frac{\Gamma \vdash M:\tau}{\Gamma \vdash \text{in}_2(M):\sigma+\tau}\ (+ \text{ intro2})$$

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

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

Figure 1: Type Assignment System for $\Lambda^{\to,\times,+}$

The semantics we introduced in [2] are motivated by semantics introduced in [3] and [5]. As in [3] and [5], we also start by defining a Kripke applicative structure. We consider only Kripke applicative structures which are extensional and have combinators (see [5]). Then, a Kripke lambda model $\mathcal{K}_\rho = \langle \mathcal{K}, \rho\rangle$, is defined as a Kripke applicative structure $\mathcal{K}$ which is extensional and has combinators provided with ρ, a partial mapping from term-variables and worlds to domains, such that: if $\rho(x,w) \in D_w$ and $w \leq w'$, then $\rho(x,w') = i_{w,w'}(\rho(x,w))$.

The main difference between the semantics introduced in [2] and in [1] is in the definition of Kripke applicative structure and in the definition of the interpretation of lambda terms. In [1], a Kripke applicative structure is defined as a tuple $\mathcal{K} = \langle W, \leq, \{A^\sigma_w\}, \{i^\sigma_{w,w'}\}\rangle$, which consists of:

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

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

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

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

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

This structure is not rich enough to give a unique meaning to all lambda terms. For that reason, in [2] we define a Kripke applicative structure as a tuple

$$\langle W, \leq, \{D_w\}, \{A^\sigma_w\}, \{App_w\}, \{Proj_{1,w}\}, \{Proj_{2,w}\}, \{Inl_w\}, \{Inr_w\}, \{i_{w,w'}\}\rangle$$

where $W, \leq, \{D_w\}, \{A^\sigma_w\}, \{App_w\}, \{i_{w,w'}\}$ are as in the previous definition and $\{Proj_{1,w}\}, \{Proj_{2,w}\}, \{Inl_w\}, \{Inr_w\}$ are families of functions such that:

- $Proj_{1,w}, Proj_{2,w} : D_w \to D_w$ and for all $\sigma, \tau \in \mathsf{Type}$, $Proj_{1,w} \restriction A_w^{\sigma\times\tau} : A_w^{\sigma\times\tau} \to A_w^{\sigma}$ and $Proj_{2,w} \restriction A_w^{\sigma\times\tau} : A_w^{\sigma\times\tau} \to A_w^{\tau}$
- $Inl_w, Inr_w : D_w \to D_w$ and for all $\sigma, \tau \in \mathsf{Type}$, $Inl_w : A_w^{\sigma} \to A_w^{\sigma+\tau}$, and $Inr_w : A_w^{\tau} \to A_w^{\sigma+\tau}$.
- The application functions, the projection functions and the injection functions commute with the transition in a natural way, i.e. $(\forall f \in D_w)\ (\forall a \in D_w)\ (\forall w' \in W, w \leq w')$, $i_{w,w'}(App_w(f,a)) = App_{w'}(i_{w,w'}(f), i_{w,w'}(a))$. Similarly for functions $Proj_{1,w}, Proj_{2,w}, Inl_w$, and Inr_w.

The meaning of the term M in world w in valuation ρ, denoted by $[\![M]\!]^w_\rho$, is defined inductively (induction on the structure of the term).

The proof that the map $[\![\ ]\!]^w_\rho$ is well-defined is based on the translation of lambda calculus into combinatory logic. We have proved that type assignment system for full simply typed lambda calculus is sound and complete with respect to the proposed semantics.

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

Theorem 2 (Completeness) *Let* Γ *be a consistent basis. If* $\Gamma \models M : \sigma$*, then* $\Gamma \vdash M : \sigma$*.*

Acknowledgment

This work has been partly supported by the Ministry of Education, Science and Technological Development, Republic of Serbia.

References

[1] Kašterović, S., Ghilezan, S., *Kripke semantics for lambda calculus with pairs and disjoint sums*, LAP 2019 - 7th Conference on Logic and Applications, September 23-27, 2019, Dubrovnik, Croatia

[2] Kašterović, S., Ghilezan, S., *Kripke semantics and completeness for full simply typed lambda calculus,* to appear in Journal of Logic and Computation Volume 30, issue 8 (2020).

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

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

[5] Mitchell, J. C., *Foundations for programming languages*, Foundation of computing series. MIT Press, 1996.

Constructive HMR-order theory for semigroups with apartness

Melanija Mitrović

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

Mahouton Norbert Hounkonnou

International Chair in Mathematical Physics and Applications
(ICMPA-UNESCO Chair), University of Abomey-Calavi, Cotonou, Benin
e-mail: norbert.hounkonnou@cipma.uac.bj

Marian Alexandru Baroni

"Dunarea de Jos" University of Galati, Romania
e-mail: marianbaroni@yahoo.com

Keywords:
Semigroup with apartness, set with apartness, co-quasiorder

We have to emphasize that Errett Bishop - style constructive mathematics, **BISH**, forms the framework for our work. Let us remember, we regard classical mathematics as Bishop-style mathematics plus the law of excluded middle, **LEM**. Several consequences of **LEM** are not accepted in **BISH**. We will state here two of them for future reference. *The limited principle of omniscience*, **LPO**: for each binary sequence $(a_n)_{n\geq 1}$, either $a_n = 0$ for all n, or else there exists n with $a_n = 1$, and *Markov's principle*, **MP**: for each binary sequence $(a_n)_{n\geq 1}$, if it is impossible that $a_n = 0$ for all n, then there exists n with $a_n = 1$.

Inspired by results obtained in interactive theorem proving the approach of formal verifications, we created the new constructive algebraic theory - *the theory of semigoups with apartness*. Contrary to the classical case, a set exists only when it is defined. We define a set S by giving an algorithm for constructing members of S, together with a prescribed equivalence relation $=$, called the *equality* of S. Let $(S, =)$ be an *inhabited* set, that is, one in which we can construct an element. By an *apartness* on S we mean a binary relation $\#$ on S which satisfies the axioms of irreflexivity, symmetry and cotransitivity: $\neg(x\#x)$, $x\#y \Rightarrow y\#x$, $x\#z \Rightarrow \forall_{y\in S}\,(x\#y \vee y\#z)$. The apartness on a set S is *tight* if $\neg(x\#y) \Rightarrow x = y$. A set with apartness $(S, =, \#)$ with given equality and apartness independently of each other as the basic relations is the starting point of further considerations. A tuple $(S, =, \#, \cdot)$ is a **semigroup with apartness** with $(S, =, \#)$ as a set with apartness, $\cdot$ an associative binary operation on S which is strongly extensional, i.e. $\forall_{a,b,x,y\in S}\,(a\cdot x\# b\cdot y \Rightarrow (a\# b \vee x\# y))$. As it is shown in [1], apartness does not have to be tight. The order theory provides one of the most basic tools of semigroup theory within classical mathematics. In particular, the structure of semigroups is usually most clearly revealed through the analysis of the behaviour of their appropriate orders. Going through [1], [3], we can conclude that one of the main objectives of those papers is to develop an

appropriate constructive order theory for semigroups with apartness. Based on material given in [2], constructive **HMR**(Hounkonnou-Mitrović-Romano)-order theory developed for sets and semigroups with apartness will be presented.

The presence of apartness implies the appearence of different types of substructures connected to it. A subset Y of S has two natural complementary subsets: *the logical complement* $\neg Y \stackrel{\text{def}}{=} \{x \in S : x \notin Y\}$, and *apartness complement*, or, shortly, *a-complement* $\sim Y \stackrel{\text{def}}{=} \{x \in S : \forall_{y \in Y}(x \# y)\}$. In general, we have $\sim Y \subseteq \neg Y$. However, even for a tight apartness, the converse inclusion entails the Markov principle, **MP**. The complements are used for the classification of subsets of a given set. A subset Y of S is: *a detachable* subset or, shortly, *d-subset* in S if $\forall_{x \in S}\, (x \in Y \vee x \in \neg Y)$; *a strongly detachable* subset or, shortly, *an sd-subset* of S if $\forall_{x \in S}\, (x \in Y \vee x \in \sim Y)$, *a quasi-detachable* subset or, shortly, *a qd-subset* of S if $\forall_{x \in S} \forall_{y \in Y}\, (x \in Y \vee x \# y)$. The relations between detachable, strongly detachable and quasi-detachable subsets are partially described in [3], Proposition 2.1. A complete description of the relationships between those subsets of a set with apartness is given in the next theorem which is one of the main results of this presentation.

Theorem 1 *Let Y be a subset of S. Then:*

(i) *Any sd-subset is a qd-subset of S. The converse implication entails* **LPO**

(ii) *Any qd-subset Y of S satisfies $\sim Y = \neg Y$.*

(iii) *If any qd-subset is a d-subset, then* **LPO** *holds.*

(iv) *If any d-subset is a qd-subset, then* **MP** *holds.*

(v) *Any sd-subset is a d-subset of S. The converse implication entails* **MP**.

(vi) *If any subset of a set with apartness S is a qd-subset, then* **LPO** *holds.*

A relation τ defined on a set with apartness S is a *co-quasiorder* if it is strongly irreflexive ($\tau \subseteq \#$), and co-transitive. By Proposition 2.3 [3], a co-quasiorder τ is a qd-subset of $S \times S$, and, by Theorem 1, $\sim \tau = \neg \tau$. Generally speaking, for a co-quasiorder defined on a set with apartness, we cannot prove that its left and/or right classes are d-subsets or sd-subsets. More precisely, we can prove the following result.

Proposition 1 *Let τ be a co-quasiorder. If $a\tau$ ($a\tau$) is a d-subset (an sd-subset) of S for any $a \in S$, then* **LPO** holds.

The relations defined on a semigroup S are distinguished one from another according to the behaviour of their related elements to the multiplication. Following the classical results, as much as possible, we can start with the following definition. A co-quasiorder τ on a semigroup S is *complement positive* if $(a, ab), (a, ba) \in \sim \tau$ for any $a, b \in S$. The description of a complement positive co-quasiorder via its classes follows.

Theorem 2 *Let τ be a co-quasiorder τ on a semigroup S.*

(i) *If τ is complement positive, then $\forall_{a,b\in S}\,(\tau(ab) \subseteq \tau a \cap \tau b)$.*

(ii) *If τa is an sd-ideal of S and $a \bowtie \tau a$ for every $a \in S$, then τ is complement positive and $\forall_{a,b\in S}\,(a\tau \cup b\tau \subseteq (ab)\tau)$.*

(iii) *If $a\tau$ is an sd-convex subset of S, and $a \bowtie a\tau$ for every $a \in S$, then τ is a complement positive co-quasiorder.*

The theory of semigroups with apartness is, of course, in its infancy, but it promises a prospective of applications in other (constructive) mathematics disciplines, certain areas of computer science, social sciences, economics. On the other hand, in order to have profound applications, a certain amount of the theory, which can be applied, is first necessary. Among priorities, besides growing the general theory, are further developments of: constructive relational structures - (co)quotient structures in the first place, constructive **HMR**-order theory, theory of **HMR**-ordered semigroups with apartness, etc.

Acknowledgment

M. M. is supported by the Faculty of Mechanical Engineering, University of Niš, Serbia, Grant "Research and development of new generation machine systems in the function of the technological development of Serbia". M. N. H. is supported by TWAS Research Grant RGA No. 17 - 542 RG / MATHS / AF / AC _G -FR3240300147. The ICMPA-UNESCO Chair is in partnership with Daniel Iagolnitzer Foundation (DIF), France, and the Association pour la Promotion Scientifique de l'Afrique (APSA), supporting the development of mathematical physics in Africa.

References

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

[2] M. Mitrović, M. N. Hounkonnou, M. A. Baroni, *Theory of constructive semigroups with apartness - foundations, development and practice*, arXiv:2008.11008.

[3] M. Mitrović, S. Silvestrov, S. Crvenković, D. A. Romano., *Constructive semigroups with apartness: towards new algebraic theory*, Journal of Physics : Conference Series (JPCS) , Volume 1194, 2019, 012076, doi:10.1088/1742-6596/1194/1/012076.

Constructive cut elimination in geometric logic

Sara Negri[1,2], **Eugenio Orlandelli**[2]

[1] *Department of Mathematics University of Genoa.*
Via Dodecaneso 35, Genoa, Italy
[2] *Department of Philosophy, University of Helsinki.*
Unioninkatu 40A, Helsinki, Finland.
E-mail: [1] sara.negri@unige.it, [2] eugenio.orlandelli@helsinki.fi

Keywords:
Geometric axioms; Axioms-as-rules; Infinitary logic; G3 calculi; Constructive cut elimination.

Notable parts of algebra and geometry can be formalized as *coherent theories* over first-order classical or intuitionistic logic. Their axioms are *coherent implications*, i.e., universal closures of implications $D_1 \supset D_2$, where both D_1 and D_2 are built up from atoms using conjunction, disjunction and existential quantification. Examples include all algebraic theories, such as group theory and ring theory, all essentially algebraic theories, such as category theory [3], the theory of fields, the theory of local rings, lattice theory [12], projective and affine geometry [12, 9], the theory of separably closed local rings (aka "strictly Henselian local rings") [4, 9, 15].

Although wide, the class of coherent theories leaves out certain axioms in algebra such as the axioms of torsion abelian groups or of Archimedean ordered fields, or in the theory of connected graphs, as well as in the modelling of epistemic social notions such as common knowledge. All the latter examples can however be axiomatized by means of *geometric axioms*, a generalization of coherent axioms that allows infinitary disjunctions.

Coherent and geometric implications form sequents that give a Glivenko class [10], as shown by Barr's Theorem.[1]

Theorem 1 (Barr's Theorem [1]) *If $\mathcal{T}$ is a coherent (geometric) theory and A is a sentence provable from $\mathcal{T}$ with (infinitary) classical logic, then A is provable from $\mathcal{T}$ with (infinitary) intuitionistic logic.*

[1] Barrs theorem is often alleged to achieve more in that it also allows to eliminate uses of the axiom of choice, but see [11].

Barr's Theorem has its origin, through appropriate completeness results, in the theory of sheaf models, with the following formulation:

Theorem 2 ([6], Ch.9, Thm.2) *For every Grothendieck topos $\mathcal{E}$ there exists a complete Boolean algebra $\mathbf{B}$ and a surjective geometric morphism $Sh(\mathbf{B}) \longrightarrow \mathcal{E}$.*

If we limit our attention to first-order coherent theories $\mathcal{T}$, an extremely simple and purely logical proof of Barr's Theorem has been given in [7] by means of **G3**-style sequent calculi. [7] shows how to express coherent implications by means of rules that preserve the admissibility of the structural rules of inference. As a consequence, Barr's theorem is proved by simply noticing that a proof in **G3cT** is also a proof in the intuitionistic multisuccedent calculus **G3iT**.

This simple and purely logical proof of Barr's Theorem has been extended to geometric theories in [8]. This work considers the **G3**-style calculi for classical and intuitionistic infinitary logic $\mathbf{G3}[\mathbf{ci}]_\omega$ (with finite sequents instead of countably infinite sequents) and their extension with rules expressing geometric implications $\mathbf{G3}[\mathbf{ci}]_\omega\mathbf{T}$. To illustrate, the geometric axiom $\forall x. \bigvee_{n>0} .nx = 0$ is expressed by the the infinitary rule:

$$\frac{\{nx = 0, \Gamma \Rightarrow \Delta \mid n > 0\}}{\Gamma \Rightarrow \Delta}$$

The main results in [8] are that in $\mathbf{G3}[\mathbf{ci}]_\omega\mathbf{T}$ all rules are height-preserving invertible, the structural rules of weakening and contraction are height-preserving admissible, and cut is admissible. Hence, Barr's Theorem for geometric theories is proved in [8] as it was done in [7] for coherent ones: a proof in $\mathbf{G3c}_\omega\mathbf{T}$ is also a proof in the intuitionistic multisuccedent calculus $\mathbf{G3i}_\omega\mathbf{T}$.

One weakness of the results in [8] is that the cut-elimination procedure given in Sect. 4.1 is not constructive. This is a typical limitation of cut eliminations in infinitary logics [2, 5, 13]. The problem is that the proof makes use of the 'natural' (or Hessenberg) commutative sum of ordinals $\alpha\#\beta$ (see [14, 10.1.2B]),

> [whose] definition utilizes the Cantor normal form of ordinals to base ω. This normal form is not available in **CZF** (or **IZF**) and thus a different approach is called for. [11, p.369]

We constructivize the cut-elimination proof for $\mathbf{G3}[\mathbf{ci}]_\omega\mathbf{T}$ by giving a procedure that replaces induction on sums of ordinals with induction on well-founded trees.[2] In this way we are able to give a proof of Barr's Theorem for geometric theories that uses only constructively acceptable proof-theoretic tools. Moreover, our proof strategy should allow to constructivize the cut-elimination procedure for other infinitary calculi.

Acknowledgment

The research reported in the paper is partly supported by the Academy of Finland, research project no. 1308664.

[2] See [11, §7] for a different constructive proof of cut elimination in infinitary logic.

References

[1] Michael Barr. Toposes without points. *J. Pure Appl. Algebra*, 5(3):265–280, 1974.

[2] Solomon Feferman. Lectures on Proof Theory. In *Proceedings of the Summer School in Logic (Leeds, 1967)*, pages 1–107. Springer, Berlin, 1968.

[3] Peter Freyd. Aspects of topoi. *Bull. Austral. Math. Soc.*, 7(1):1–76, 1972.

[4] Peter T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium. Vol. 1 & 2.* Oxford University Press, New York, 2002.

[5] E. G. K. Lopez-Escobar. An interpolation theorem for denumerably long formulas. *Fund. Math.*, 57:253–272, 1965.

[6] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in Geometry and Logic. A First Introduction to Topos Theory.* Springer-Verlag, 1994.

[7] Sara Negri. Contraction-free sequent calculi for geometric theories with an application to Barr's theorem. *Arch. Math. Logic*, 42(4):389–401, 2003.

[8] Sara Negri. Geometric rules in infinitary logic. In O.Arieli and A. Zamansky, editors, *Arnon Avron on Semantics and Proof Theory of Non-Classical Logics.* forthcoming. Springer.

[9] Sara Negri and Jan von Plato. *Proof Analysis. A contribution to Hilbert's last problem.* Cambridge University Press, Cambridge, 2011.

[10] V.P. Orevkov. Glivenko's sequence classes. In V.P. Orevkov, editor, *Logical and logico-mathematical calculi. Part 1*, pages 131–154. Leningrad, 1968.

[11] Michael Rathjen. Remarks on Barr's theorem. Proofs in geometric theories. In D. Probst and P. Schuster, editors, *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, pages 347–374. de Gruyter, 2016.

[12] Thoralf Skolem. Logisch-kombinatorische Untersuchungen. *Videnskapsselskapets skrifter, 1. Mat.-naturv. klasse*, 4, 04 1920.

[13] Gaisi Takeuti. *Proof Theory.* North-Holland, 1987[2].

[14] Anne S. Troelstra and Helmut Schwichtenberg. *Basic Proof Theory.* Cambridge University Press, Cambridge, 2nd edition, 2000.

[15] Gavin Wraith. Generic Galois theory of local rings. In M. P. Fourman et al., editor, *Applications of Sheaves*, pages 739–767. Springer-Verlag, 1979.

A proof-theoretic approach to formal epistemology

Sara Negri [1,2], **Edi Pavlović**[3]

[1] *University of Genoa*
via Dodecaneso 35, 16146 Genova, Italy
[1] *University of Helsinki*
Unioninkatu 40, Helsinki, Finland
[2] *University of Helsinki*
Unioninkatu 40, Helsinki, Finland
E-mail: [1]sara.negri@unige.it, [2]sara.negri@helsinki.fi, [2]edi.pavlovic@helsinki.fi

Keywords:
Knowledge, belief, neighbourhood models, labelled calculi, conditional doxastic logic.

Ever since antiquity, attempts have been made to characterize knowledge through belief augmented by additional properties such as truth and justification. These characterizations have been challenged by Gettier counterexamples and their variants.

A modern proposal, what is known as defeasibility theory, characterizes knowledge through stability under revisions of beliefs on the basis of true or arbitrary information [3, 6]. A formal investigation of such a proposal calls for the methods of dynamic epistemic logic: well developed semantic approaches to dynamic epistemic logic have been given through plausibility models [1, 5] but a corresponding proof theory is still in its beginning.

We shall recast plausibility models in terms of the more general neighbourhood models and develop on their basis complete proof systems, following a methodology introduced in [4] and developed for conditional doxastic notions in [2].

An inferential treatment of various epistemic and doxastic notions such as safe belief and strong belief will give a new way to study their relationships; among these, the characterization of knowledge as belief stable under arbitrary revision will be grounded through formal labelled sequent calculus derivations..

Acknowledgment

This work was partially supported by the Academy of Finland, research project no. 1308664.

References

[1] Baltag, A. and S. Smets, *The logic of conditional doxastic actions*, in *Texts in Logic and Games, Special Issue on New Perspectives on Games and Interaction*, vol. 4, pp. 9–31, 2008.

[2] Girlando, M., S. Negri, N. Olivetti, and V. Risch, Conditional beliefs: From neighbourhood semantics to sequent calculus, *The Review of Symbolic Logic*, vol. 11, pp. 736–779, 2018.

[3] Hintikka, J., *Knowledge and belief: An introduction to the logic of the two notions*, vol. 4, Ithaca: Cornell University Press, 1962.

[4] Negri, S., Proof theory for non-normal modal logics: The neighbourhood formalism and basic results, *IfCoLog Journal of Logics and their Applications*, vol. 4, pp. 1241–1286, 2017.

[5] Pacuit, E., Dynamic epistemic logic I: Modeling knowledge and belief, *Philosophy Compass*, vol. 8, pp. 798–814, 2013.

[6] Stalnaker, R., Belief revision in games: Forward and backward induction, *Mathematical Social Sciences*, vol. 36, pp. 31–56, 1998.

Recent advances in logics of lying

Dusko Pavlovic

University of Hawaii

Logic has many applications. A logical theory is applied if it modifies the states of the world. By changing the state of the world, applied logical theories may change their own truth-values. While it has been known since Goedel that consistent logical theories cannot prove their own consistency, it was clear even before Goedel that the inconsistent logical theories can in fact prove their consistency. Although such consistency claims are initially false, a genuinely applied logical theory may modify the state of the world in such a way that the truth value of its consistency claim will change from false to true. Closely related logical processes play a central role on the market, on the web, and in everyday life. E.g., to start up its services, a social network must attract some initial members. To achieve that, it must convince them that their friends are already members. Initially, this statement must be false. But if enough people are convinced that it is true, then they will join the social network, and the statement will become true. The social network can then provide its services, and expand them using a variety of tools from applied logic. In this talk, I will provide an overview of general methods of lying and deceit on the industrial scale.

Resolving finite indeterminacy

Peter Schuster[1], **Daniel Wessel**[2]

[1,2] *Dipartimento di Informatica, Università degli Studi di Verona*
Strada le Grazie 15, 37143 Verona, Italy
E-mail: [1]peter.schuster@univr.it, [2]daniel.wessel@univr.it

Keywords:
dynamical proof, non-deterministic axiom, proof-theoretic conservation, finite tree, computational content, inductive generation, Krull's Lemma

Abstract algebra abounds with ideal objects and the invocations of transfinite methods, typically Zorn's Lemma, that grant those object's existence. Put under logical scrutiny, ideal objects often serve for proving the semantic conservation of additional non-deterministic sequents, that is, with finite but not necessarily singleton succedents. By design, dynamical methods in algebra [2, 3, 7] allow to eliminate the use of ideal methods by shifting focus from semantic model extension principles to syntactic conservation theorems, which move has enabled Hilbert's Programme for modern algebra.

A paradigmatic case, which to a certain extent has been neglected in dynamical algebra proper, is Krull's Lemma for prime ideals. A particular form of this asserts that a multiplicative subset of a commutative ring contains the zero element if and only if the set at hand meets every prime ideal. Prompted by Kemper and Yengui's novel treatment of valuative dimension, the authors of the present note together with Yengui have recently put Krull's Lemma under constructive scrutiny. This development has eventually helped to unearth the underlying general phenomenon [6]: Whenever a certificate is obtained by the semantic conservation of certain additional non-deterministic axioms, there is a finite labelled tree belonging to a suitable inductively generated class which tree encodes the desired computation.

The present study was carried out within the projects "A New Dawn of Intuitionism: Mathematical and Philosophical Advances" (ID 60842) funded by the John Templeton Foundation, and "Reducing complexity in algebra, logic, combinatorics - REDCOM" belonging to the programme "Ricerca Scientifica di Eccellenza 2018" of the Fondazione Cariverona. (The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of those foundations.) Both authors are members of the Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA) within the Italian Istituto Nazionale di Alta Matematica (INdAM). Last but not least, the authors wish to express their gratitude to Ulrich Berger, Stefan Neuwirth and Iosif Petrakis for interesting discussions, as well as to the anonymous referees of [6] for expertly and insightful remarks.

Recall that a *consequence relation* on a set S is a relation $\rhd$ between finite subsets[1] and elements of S, which is *reflexive, monotone* and *transitive*:

$$\frac{U \ni a}{U \rhd a}\ (\mathrm{R}) \qquad \frac{U \rhd a}{U, V \rhd a}\ (\mathrm{M}) \qquad \frac{U \rhd b \quad U, b \rhd a}{U \rhd a}\ (\mathrm{T})$$

where the usual shorthand notations are in place. The *ideals* of a consequence relation are the subsets $\mathfrak{a}$ of S *closed* under $\rhd$ in the sense that if $\mathfrak{a} \supseteq U$ and $U \rhd a$, then $a \in \mathfrak{a}$. If U is a finite subset of S, then its *closure* is an ideal:

$$\langle U \rangle = \{\, a \in S \mid U \rhd a \,\}$$

A decisive aspect of our approach is the notion of a regular set for certain non-deterministic axioms over a fixed consequence relation, where by a *non-deterministic axiom* on S we understand a pair (A, B) of finite subsets of S. A subset $\mathfrak{p}$ of S is *closed* under (A, B) if $A \subseteq \mathfrak{p}$ implies $\mathfrak{p} \between B$, where the latter is to say that $\mathfrak{p}$ and B have an element in common.

Let $\mathcal{E}$ be a set of non-deterministic axioms over $\rhd$. A *prime ideal* is an ideal of $\rhd$ that is closed under every element of $\mathcal{E}$. For instance, if $\rhd$ denotes deduction, and $\mathcal{E}$ consists of all pairs $(\emptyset, \{\, \varphi, \neg\varphi \,\})$ for sentences φ, then the (prime) ideals are exactly the (complete) theories.

A subset R of S is *regular* with respect to $\mathcal{E}$ if, for all finite subsets U of S and all $(A, B) \in \mathcal{E}$,

$$\frac{(\forall b \in B)\, \langle U, b \rangle \between R}{\langle U, A \rangle \between R}$$

Abstracted from the multiplicative subsets occurring in Krull's Lemma, regular sets haved proved the right concept for our *Universal Prime Ideal Theorem*:

Proposition 1 (**ZFC**). *A subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when $R \between \mathfrak{p}$ for all prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$.*

Regular sets further account for the constructive version of Proposition 1. To this end, given an ideal $\mathfrak{a}$, we next define a collection $T_{\mathfrak{a}}$ of *finite* labelled trees such that the root of every $t \in T_{\mathfrak{a}}$ be labelled with a finite subset U of $\mathfrak{a}$, and the non-root nodes with elements of S. The latter will be determined successively by consequences of U along the elements of $\mathcal{E}$.

We understand paths, which necessarily are finite, to lead from the root of a tree to one of its leaves. Given a path π of $t \in T_{\mathfrak{a}}$, we write $\pi \rhd a$ whenever $U, b_1, \ldots, b_n \rhd a$ where U labels the root of t and $b_1, \ldots, b_n$ are the labels occurring at the non-root nodes of π.

Definition 1. Let $\mathfrak{a}$ be an ideal. We generate $T_{\mathfrak{a}}$ inductively according to the following rules:

1. For every finite $U \subseteq \mathfrak{a}$, the trivial tree (i.e., the root-only tree) labelled with U belongs to $T_{\mathfrak{a}}$.

[1] We understand a set to be *finite* if it can be written as $\{\, a_1, \ldots, a_n \,\}$ for some $n \geqslant 0$.

2. If $(A, B) \in \mathcal{E}$ and if $t \in T_{\mathfrak{a}}$ has a path π such that $\pi \rhd a$ for every $a \in A$, then add, for every $b \in B$, a child labelled with b at the leaf of π.

We say that $t \in T_{\mathfrak{a}}$ *terminates* in $R \subseteq S$ if for every path π of t there is $r \in R$ such that $\pi \rhd r$.

Our *Constructive Universal Prime Ideal Theorem* works in (a fragment of) Constructive Zermelo–Fraenkel set theory **CZF** :

Proposition 2 (**CZF**)**.** *A subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when there is a tree $t \in T_{\mathfrak{a}}$ which terminates in R.*

We thus uniformise many instances of the dynamical method and generalise the universal proof-theoretic conservation criterion offered before [5], which by Scott–style entailment relations [1] unifies numerous phenomena, e.g. [4].

References

[1] Jan Cederquist and Thierry Coquand. Entailment relations and distributive lattices. In Samuel R. Buss, Petr Hájek, and Pavel Pudlák, editors, *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*, volume 13 of *Lect. Notes Logic*, pages 127–139. A. K. Peters, Natick, MA, 2000.

[2] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[3] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*, volume 20 of *Algebra and Applications*. Springer Netherlands, Dordrecht, 2015.

[4] Sara Negri, Jan von Plato, and Thierry Coquand. Proof-theoretical analysis of order relations. *Arch. Math. Logic*, 43:297–309, 2004.

[5] Davide Rinaldi, Peter Schuster, and Daniel Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 29(1):226–259, 2018. Communicated first in *Bull. Symb. Logic* 23 (2017), 181–200.

[6] Peter Schuster and Daniel Wessel. Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS 20, page 820830, New York, NY, USA, 2020. Assoc. for Computing Machinery.

[7] Ihsen Yengui. *Constructive Commutative Algebra. Projective Modules over Polynomial Rings and Dynamical Gröbner Bases*, volume 2138 of *Lecture Notes in Mathematics*. Springer, Cham, 2015.

An Overview of Mathematical Models for Data Privacy

Tamara Stefanović[1], Silvia Ghilezan [2,3]

[1,2] *University of Novi Sad*

[3] *Mathematical Institute SASA*

E-mail: [1] tstefanovic@uns.ac.rs, [2] gsilvia@uns.ac.rs

For centuries, people have shared information with each other and with institutions. In the last few decades the development of technology has made possible to manipulate a large amount of data, but at the same time it has developed data privacy problems. The problem of data privacy concerns how data is collected and stored, whether and how data is shared with a third party, as well as which laws are governing data sharing in areas such as health care, education and financial services ([6]). We give an overview of two fundamental mathematical models for describing data privacy problems that significantly differ from the traditional privacy approach - privacy in context ([1]) and differential privacy ([2]).

Privacy in context. Contextual integrity represents a philosophical account of privacy in terms of transfer of personal information. Here the term personal information" refers to any information related to an identified or identifiable natural person, as Helen Nissenbaum defined in [4]. A formal framework for expressing norms of transmission of personal information, inspired by contextual integrity, was presented in [1]. A temporal logic is used to capture the principles of information transmission. Formulas are generated by the following grammar:

$$\varphi ::= send(p_1, p_2, m) | contains(m, q, t) | inrole(p, r) |$$

$$incontext(p, c) | t \in t' | \varphi \wedge \varphi | \neg\varphi | \varphi \mathcal{U} \varphi | \varphi \mathcal{S} \varphi$$

$$\bigcirc\varphi | \exists x : \tau . \varphi .$$

Information about a subject is transmitted through a communication action from a sender to a recipient:

- $send(p_1, p_2, m)$ holds if agent p_1 sent the message m to agent p_2
- $contains(m, q, t)$ holds if message m contains the attribute t of agent q.

For simplification, it is assumed that information describes a single individual. However, the model includes computation rules enabling communicating agents to combine messages to compute additional information: $t \in t'$ holds

if attribute t can be computed from attribute t'. Communicating agents are associated with roles as a part of contexts, and depending on the role, communication can be permitted or prohibited:

- $inrole(p, r)$ holds if agent p is active in role r
- $incontext(p, c)$ holds if agent p is active in a role of context c.

This model is convenient for formalizing privacy laws because each privacy law is drawn to protect certain types of information in particular contexts, such as health care, employment, the marketplace and so on. Up to now, it has been used to formalize several privacy laws, such as GLBA (Gramm-Leach-Bliley Act), HIPAA (Health Insurance Portability and Accountability Act) and COPPA (Children's Online Privacy Protection Act).

Differential privacy. Privacy can also be considered from the perspective of statistical analysis of data or the release of statistics derived from personal data. Suppose a trusted curator is managing a sensitive database and needs to release some statistics from this data to the public. Also suppose there is an adversary who wants to reveal or to learn some of the sensitive data. Differential privacy ([2]) proposed by Cynthia Dwork relies on incorporating random noise so that everything an adversary receives is noisy and imprecise. The question is what kind of random noise to use so that the results still can be useful. The main challenge is achieving privacy while minimising the utility loss.

Let $D \in \mathcal{D}^n$ be a database. A query q is a function applied on a database D ([2]). We say $\mathcal{M}$ is a *privacy mechanism* or simply *mechanism* obtained by adding noise if for every query q, $\mathcal{M}$ creates a new randomized query $q^*(D) = q(D) + noise$. Let $D, D' \in \mathcal{D}^n$ be two databases that differ in at most one entry, we call them *adjacent databases*.

Definiton. Let $\varepsilon > 0$. A mechanism $\mathcal{M}$ is ε -differentially private iff for every pair of adjacent databases D, D' and for every $S \subseteq range(\mathcal{M})$:

$$Pr[\mathcal{M}(D) \in S] \leq exp(\varepsilon) Pr[\mathcal{M}(D') \in S],$$

where the probability space is over the coin flips of the mechanism $\mathcal{M}$.

The following example shows what differential privacy actually provides. Suppose Alice obtains database $D \in \mathcal{D}^n$ with n entries. She provides Bob with output o of a mechanism $\mathcal{M}(D)$. Bob knows the values of $n-1$ entries (database D_1), and has to guess the value of the n-th entry (d_n). For each possible value x of d_n, Bob can learn the distribution induced by $\mathcal{M}(D_1 \cup \{x\})$ and then pick x assigned to highest probability of the output. But, if $\mathcal{M}$ is ε -differentially private, for every $x, y \in \mathcal{D}$ holds

$$Pr[\mathcal{M}(D_1 \cup \{x\}) = o] - Pr[\mathcal{M}(D_1 \cup \{y\}) = o] \leq \varepsilon.$$

Therefore, Bob cannot do better than random guessing. In fact, if an individual is considering to allow her/his data to be used or not, by the promise of differential privacy, she/he can be almost indifferent between these two choices, because participating will not cause any additional harm.

Differential privacy has also been used to formalize privacy laws, for example FERPA (Family Educational Rights and Privacy Act), but the best known users of differential privacy models are certainly Apple and Google.

A brief comparison of the methods. The contextual integrity framework considers privacy from the perspective of information flow and uses temporal logic formulas to model privacy norms. On the other hand, differential privacy considers privacy from the perspective of statistical analysis and releasing statistics of personal data. The fundamental difference between these two approaches is in underlying mathematical methods: logic and probability. Also, formal logical model may allow sharing some personal information depending on agents role, for example: a doctor can share patients private medical information with that patient. What is not included in the formal logical model is the communication about aggregate statistics. For example, communication restriction such as the average salary of bank managers can be released only if it does not identify a particular individuals salary" cannot be expressed in formal logical model, but it is precisely the type of restriction expressed in the differential privacy model ([5]).

Future work. We are currently exploring the possibilities of combining different kinds of privacy formalization including inverse privacy ([3]).

Acknowledgment. This work has been partially supported by the Science Fund of the Republic of Serbia under grant AI4TrustBC (6526707).

References

[1] A. Barth, A. Datta, J. C. Mitchell and H. Nissenbaum, Privacy and Contextual Integrity: Framework and Applications, in *Symposium on Security and Privacy*, (Berkeley, California), pp. 184-198, IEEE, Computer Society, 2006.

[2] C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, *Foundations and Trends in Theoretical Computer Science*, vol. 9, pp. 211-407, 2014.

[3] Y. Gurevich,E. Hudis and J. M. Wing, Inverse Privacy, *CoRR*, vol. 1510.03311, 2015.

[4] H. Nissenbaum , *Privacy in Context - Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010.

[5] K. Nissim, A. Bembenek, A. Wood, M. Bun, M. Gaboardi, U. Gasser, D. R. O'Brien, T. Steinke and S. Vadhan Bridging the Gap between Computer Science and Legal Approaches to Privacy,*Harvard Journal of Law & Technology*,vol. 31, pp. 689-713, 2018.

[6] D. J. Solove, A taxonomy of privacy, and the Integrity of Social Life, *University of Pennsylvania Law Review*, vol. 154, pp. 477-560, 2010.

A modal logic formalization of controlled query evaluation

Thomas Studer [1]

[1] *Institute of Computer Science*
University of Bern, Switzerland
E-mail: [1] thomas.studer@inf.unibe.ch

Keywords: Impossibility theorem, data privacy, controlled query evaluation, modal logic.

Controlled query evaluation (CQE) is an approach to guarantee data privacy for database and knowledge base systems [1, 2, 3, 4, 9]. CQE-systems feature a censor function that may distort the answer to a query in order to hide sensitive information. In the present work, we use modal logic to present a highly abstract model for dynamic query evaluation systems like CQE. We formulate several desirable properties of CQE-systems in our framework and establish two no-go theorems saying that certain combinations of those properties are impossible. Note that some particular instances of our general impossibility results have already been known [1, 9].

There are many different notions of privacy available in the literature. For our results, we rely on provable privacy [5, 6], which is a rather weak notion of data privacy. Using a weak definition of privacy makes our impossibility theorems actually stronger since they state that under certain conditions not even this weak form of privacy can be achieved.

This work has already been presented at CRYPTOLOGY 2020 [7]. A full version is available in [8].

Acknowledgment

The research presented here is supported by the Swiss National Science Foundation grant 200020_184625.

References

[1] J. Biskup. For unknown secrecies refusal is better than lying. *Data and Knowledge Engineering*, 33(1):1–23, 2000.

[2] J. Biskup and P. A. Bonatti. Lying versus refusal for known potential secrets. *Data and Knowledge Engineering*, 38(2):199–222, 2001.

[3] J. Biskup and P. A. Bonatti. Controlled query evaluation for enforcing confidentiality in complete information systems. *International Journal of Information Security*, 3(1):14–27, 2004.

[4] J. Biskup and T. Weibert. Keeping secrets in incomplete databases. *International Journal of Information Security*, 7(3):199–217, 2008.

[5] K. Stoffel and T. Studer. Provable data privacy. In K. V. Andersen, J. Debenham, and R. Wagner, editors, *Database and Expert Systems Applications*, pages 324–332. Springer, 2005.

[6] P. Stouppa and T. Studer. A formal model of data privacy. In I. Virbitskaite and A. Voronkov, editors, *Perspectives of Systems Informatics*, pages 400–408. Springer, 2007.

[7] T. Studer. No-go theorems for data privacy. In *Proceedings of the 7th International Cryptology and Information Security Conference 2020*, pages 74–84, 2020.

[8] T. Studer. No-go theorems for data privacy. E-print 2005.13811, arXiv.org, 2020.

[9] T. Studer and J. Werner. Censors for boolean description logic. *Transactions on Data Privacy*, 7:223–252, 2014.

The Evolution of Logic-based Static Analysis

Pavle Subotić

Amazon

Datalog has been successfully applied to a range of applications including program analysis. By expressing analyses declaratively, Datalog can largely reduce the burden of defining new static analyses. Moreover, by using state-of-the-art Datalog engines, for instance Soufflé, this approach can remain competitive with hand-crafted static analysers. In this talk I will give an overview of the design of Soufflé, in particular the aspects of the engine that have allowed Datalog-based static analysis to scale to industrial scale problems. I will describe some notable use cases where Soufflé has successfully been used and end with on-going work which aims to make Souffle even more powerful for static analysis use cases.

Soft Subexponentials and Multiplexing

Andre Scedrov

University of Pennsylvania

Linear logic [1] and its refinements have been used as a specification language for a number of deductive systems. This has been accomplished by carefully studying the structural restrictions of linear logic modalities. Examples of such refinements are subexponentials [8, 5], light linear logic [2], and soft linear logic [3]. We bring together these refinements of linear logic in a non-commutative setting. We introduce a noncommutative substructural system with subexponential modalities controlled by a minimalistic set of rules [7]. Namely, we disallow the contraction and weakening rules for the exponential modality and introduce two primitive subexponentials. One of the subexponentials allows the multiplexing rule in the style of soft linear logic and light linear logic. The second subexponential provides the exchange rule. For this system, we construct a sequent calculus, establish cut elimination, and also provide a complete focused proof system. We illustrate the expressive power of this system by simulating Turing computations and categorial grammar parsing for compound sentences. Using the former, we prove undecidability results. The new system employs Lambeks non-emptiness restriction [4], which is incompatible with the standard (sub)exponential setting [6]. Lambeks restriction is crucial for applications in linguistics: without this restriction, categorial grammars incorrectly mark some ungrammatical phrases as being correct. This is joint work with Max Kanovich, Stepan Kuznetsov, and Vivek Nigam.

References

[1] Jean-Yves Girard. Linear Logic. Theoretical Computer Science 50(1) (1987) 1101.

[2] Jean-Yves Girard. Light linear logic. Information and Computation 143(2) (1998) 175204.

[3] Yves Lafont. Soft linear logic and polynomial time. Theoretical Computer Science 318(12) (2004) 163180.

[4] Joachim Lambek. The mathematics of sentence structure. American Mathematical Monthly 65 (1958) 154170.

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

[6] Max Kanovich, Stepan Kuznetsov, and Andre Scedrov. Reconciling Lambek's restriction, cut-elimination, and substitution in the presence of exponential modalities. Journal of Logic and Computation 30(1) (2020) 239 - 256.

[7] Max Kanovich, Stepan Kuznetsov, Vivek Nigam, and Andre Scedrov. Soft Subexponentials and Multiplexing. In: N. Peltier and V. Sofronie-Stokkermans, eds., Automated Reasoning, 10th International Joint Conference, IJCAR 2020, Paris, France, July 1-4, 2020, Proceedings, Part I, Springer LNAI Volume 12166, Springer-Verlag, 2020, pp. 500 - 517.

[8] Vivek Nigam and Dale Miller. A framework for proof systems. Journal of Automated Reasoning 45(2) (2010) 157188.

Rules of thumb for test results

Zvonimir Šikić

It is well known that tests are not 100% accurate at classifying individuals. The actual condition of an individual (e.g. diseased, or not diseased) does not coincide with her test result (positive, or negative). Nevertheless, it is often presupposed that individuals with negative results can be ruled out, if screening test is highly sensitive. This has led to the mnemonic SNNOUT - SeNsitive Negative OUT. Similarly, it is often thought that if screening test is highly specific, individuals with positive results can be ruled in. This has led to the mnemonic SPPIN - SPecific Positive IN. But simple probabilistic analysis of SNNOUT and SPPIN immediately reveals that the rules are incorrect. We devise the correct and easily applicable rules of thumb that could be of great help to doctors and patients:

Positive rule – PASSAP (Positive: Add Sensitivity/Specificity And Prevalence)
If a patient is positive you need to calculate two sums: sensitivity + prevalence and specificity + prevalence. If both sums are less than 100% then the probability of the patient being diseased is less than 50%.
For example, if prevalence of disease is 4%, test specificity is 85% and test sensitivity is 95%, your chances of being diseased if positive are still less than 50%, because $85\% + 4\% < 100\%$ and $95\% + 4\% < 100\%$.

Negative rule – NUFSS (Negative: Upward From Sensitivity/Specificity)
If a patient is negative and the prevalence of disease is less than 50% then the probability of the patient not being diseased is greater than the smaller of the two values of sensitivity and specificity.
For example, if prevalence of disease is less than 50%, test specificity is 90% and test sensitivity is 95% your chances of not being diseased if negative are greater than 90%.

Neighborhood semantics and proof theory for infinitary intuitionistic logic*

Matteo Tesi

Scuola Normale Superiore
Piazza dei Cavalieri 7
E-mail: matteo.tesi@sns.it

Keywords:
Infinitary logic, Intuitionistic logic, Neighborhood semantics, Proof theory.

Intuitionistic infinitary logic is intuitionistic logic extended with countable disjunctions and conjunctions. Its only known semantics is the algebraic one [3]. The natural extension of Kripkean semantics to the infinitary setting is not adequate to deal with infinitary intuitionistic logic, as intuitionistic Kripke frames correspond to Alexandroff topologies, i.e. topologies closed under infinitary intersections, and thus they validate the infinitary distributive axiom:

$$\bigwedge_{k>0}(A_k \vee B) \to \bigwedge_{k>0} A_k \vee B$$

which is not intuitionistically valid.

To start with, we introduce a topological semantics and we prove completeness with respect to countable fragments of infinitary intuitionistic logic. We then present a neighborhood semantics for infinitary intuitionistic logic[1] and we show that the standard sequent calculus for intuitionistic infinitary logic is sound and complete with respect to it: in particular, completeness is established via the transformation of a topological model in a neighborhood one. The key point is that neighborhood frames have a more fine grained structure in comparison to Kripkean frames: in particular, we consider neighborhood frames which contain the unit and are closed under supersets and finite intersections. The latter condition maintains the validity of the finite distributivity law, but does not entail the validity of the infinitary version.

The new semantics is exploited in order to obtain a labelled sequent calculus $G3I_\omega$ for intuitionistic infinitary logic and we investigate its structural

*This work is partly in collaboration with Sara Negri.

[1] A neighborhood semantics for intuitionistic (finitary) logic was first introduced in [2], but frames were closed under infinite intersections and corresponded to Alexandroff spaces, rather than to topological spaces.

properties along the lines of [4]. As in the tradition of labelled sequent calculi, it enjoys height-preserving admissibility of weakening and contraction as well as cut admissibility. Furthermore every rule is height-preserving invertible differently from the unlabelled sequent calculus in which the right rule for the implication and the right rule for infinitary conjunction are not invertible due to the context restrictions imposed on the premises of the rules.

By exploiting the structural properties of the calculus we obtain a Takeuti-style form of completeness via the construction of a reduction tree and the extraction of a neighborhood countermodel. Finally we introduce an extension of Gödel-McKinsey-Tarski translation from intuitionistic infinitary logic to an infinitary version of the $S4$ modal system. The translation is proved to be sound, in the sense that if a formula is a theorem of intuitionistic infinitary logic, then its translation is a theorem of the infinitary $S4$ system. The converse direction, namely the faithfulness of the translation, is proved via proof-theoretic methods by transfinite induction on the height of derivations [1] in the labelled calculus for infinitary modal logic $G3S4_\omega$ based on neighborhood semantics.

Acknowledgment

This work is partly in collaboration with Sara Negri.

References

[1] Dyckhoff, R., Negri, S., *Proof analysis in intermediate logics*, Archive for Mathematical Logic 51, pp. 71-92, 2012.

[2] Moniri, M., Maleki, F. S., *Neighborhood semantics for basic and intuitionistic logic*, Logic and Logical Philosophy 24, pp. 339-355, 2015.

[3] Nadel, M., *Infinitary intuitionistic logic from a classical point of view*, Annals of Mathematical Logic 14, pp. 159-191, 1978.

[4] Negri, S., *Proof theory of non-normal modal logic: the neighborhood formalism and basic results*, IfCoLog Journal of Logics and their Applications 4 (4), 2017.

3rd workshop Formal Reasoning and Semantics (FORMALS 2020)

a satellite workshop of 9th conference Logic and Applications (LAP 2020)

Inter-University Center, Dubrovnik

21–25 September 2020

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

The 1st workshop (FORMALS 2018) was also co-located with Logic and Applications conference (LAP 2018) in Dubrovnik. The 2nd workshop (FORMALS 2019) was held at the Faculty of Teacher Education, University of Zagreb.

Contributions to the 3rd workshop present continuation of work on project topics presented at previous editions, including:

- semantics and completeness of interpretability logics (L. Mikec, S. Horvat)
- advances in social choice theory (A. Hatzivelkos)
- formal methods in ontological study of cognitive and linguistic concepts (B. Perak, T. Ban Kirigin)
- security in cyber-physical systems (V. Nigam, invited talk)

Another invited talk (S. Jelić) is about advances in M-system theory, previously presented in a contributed talk at FORMALS 2019 workshop. We are also happy to host a contributed talk on a novel approach to Russell's Paradox (L. Conti). The workshop is organized in a hybrid form, part of the contributors being present in Dubrovnik, while others participate online, due to COVID-19 pandemic, which also affects the content of the workshop in one of the talks (M. Maretić).

We thank the directors of LAP for agreeing this workshop to be a part of the conference once again.

On behalf of the FORMALS project research group,

Tin Perkov

A Model for a Free Way Out of Russell's Paradox

Ludovica Conti

University of Pavia, Italy

As is well-known, Russell's Paradox blocks Frege's logicist foundation of arithmetic, intended as the reconstruction of Peano Arithmetic into – what we can call – Frege's Logic (FL), namely second-order logic augmented with Basic Law V (BLV). However, we know that such result does not properly prevent the foundational issue involved in this project because we are able to achieve the same or even a stronger result, namely deriving FA in a system – which we will call T-FL – that is doubly weaker than FL, since it is composed by a weakened logical framework and a restricted version of the non-properly-logical axiom (BLV). I briefly present the formal features of (a schematic version of) such weak version of Logicism and its main syntactical results. Finally, I provide a model-theoretic proof of its consistency.

1 A Free Fregean Logic – *T-FL*

This theory involves, as the logical core of the theory (FL) the complete set of axioms and inference rules of first-order logic without identity (FOL) for unrestricted first-order quantification and the axioms and inference rules of non-inclusive negative free logic with identity ($NFL^{=}$) for restricted quantification and identity. Additionally, it involves an axiom-schema of universal instantiation for second-order variables ($\forall X\phi(X) \rightarrow \phi(Y)$), a rule of universal generalisation (*GEN)*), second-order comprehension axiom schema (CA[1]) and *modus ponens* (MP).

The only non-logical abstraction principle that characterises this theory is the result of a weakening of Basic Law V. I propose a *Positive* restriction of BLV, namely a weakening that is explicitly devoted to avoid set-theoretic paradoxes, by excluding their common feature, namely the circular syntactic mixture of quantification and negation. I would like to emphasise that, in this Fregean context, the restriction deals with a second-order version of Russell's paradox and then is formulated into, namely inscribed in, the range of a second order quantifier.

T-BLV: $\epsilon x.Xx = \epsilon x.Yx \leftrightarrow \Pi x(Xx \leftrightarrow Yx) \wedge (\phi(X) \wedge \phi(Y))$ – where ϕ means "*positive*", i.e. it must be specifiable by a *positive* comprehension formula, namely a formula ϕ which (even if we replace predicative constants with

[1] CA) $\exists X \Pi x(Xx \leftrightarrow \alpha)$

their comprehension formula) considered in its primitive form[2], contains bound second-order variables only in the scope of an even number of negation symbols.

Such theory allows us to define a Fregean version of arithmetical vocabulary. Additionally, we are able to derive Hume's principle. Then, we can observe that the derivation of Hume's Principle (HP) from a restricted version of BLV does not imply its corresponding limitation. This means that, ideally, HP is true also of cardinal terms which (by corresponding to non-*positive* extensions terms) are empty. However, the original Fregean formulation of arithmetical vocabulary does not involve such sort of the extensional – and then cardinal – terms. Finally, we are able to prove, in the usual Fregean way, also the existence of each cardinal number and a free version of *Frege's Theorem*[3].

2 A model

In this section, I describe a model of $T\text{-}FL$, in order to prove the consistency of such system[4]. Before starting, it could be useful providing some preliminary definitions. We inductively define the *Degree* n of an extension term $\epsilon\phi_n$ as follows[5]: $\epsilon\phi_0$, if ϕ does not contain second-order quantifiers – namely if ϕ is a *Predicative* formula; $\epsilon\phi_1$, if ϕ does contain second-order quantifiers but it does not contain extension terms that contain second-order quantifiers; $\epsilon\phi_{n+1}$, if ϕ does contain extension terms that contain second-order quantifiers whose highest Degree is n. Furthermore, we inductively define the *Rank* n of an extension term $\epsilon\phi^n$ as follows: $\epsilon\phi^0$, if ϕ does not contain other extension terms; $\epsilon\phi^n + 1$, if ϕ does contain extension terms whose highest Rank is n.

2.1 Interpretation of the terms

First-order domain D and *Non-Positive* extension-terms The full first-order domain D consists in the set of natural numbers $\mathbb{N}$ augmented with the singleton $\{-1\}$. Such domain – $D = \mathbb{N} \cup \{\text{-}1\}$ – is the domain of unrestricted quantification (Π and Σ). Its proper subset, constituted by the set of natural numbers alone – $\mathbb{N} \subset D$ – is the domain of restricted quantification ($\forall$ and $\exists$).

In this case, -1 represents the conventional denotation of every "improper" (extensional) term – which, for sake of simplicity, we will call *Non-Positive* extension term. As we have seen, the semantic clauses (as consequences of the axioms themselves) states that such object belongs to the counter-extension of every predicate.

[2]We will consider primitive a formula which contains only primitive symbols of our language L_F ($\neg, \wedge, \vee, =, \exists$) - i.e. $\forall X \exists x(\neg(\neg Xx))$ is not primitive because its expression could be reduced to $\exists X \exists x(\neg Xx)$. For such reason, other formulas, logically equivalent to the Russellian formula (e.g. $\neg\forall X(\neg(x = \epsilon X \vee Xx))$), are not positive because they could be reduced to $\exists X(x = \epsilon X \wedge \neg(Xx))$.

[3]Cfr. [2]

[4]This model is deeply influenced by the Heck's model for the predicative subsystem of Frege's *Grundgesetze*(cfr. [5]) and by the Frege-Carnap theory of the "chosen object", which admit that "improper" terms could receive, as denotation, some (and the same) purely conventional denotation.

[5]Regarding our notation, we anticipate that the Rank of the extension terms will be indicated by apices, while their Degree by subscripts.

***Positive* and *Predicative* extension-terms – $\epsilon\phi_0$.** Order all the $\epsilon\phi_0$ in a $\omega \times \omega$-sequence:
- the terms of every Rank constitute an ω-sequence;
- the relation of increasing Rank of the terms holds on the ω-sequence ($<\epsilon\phi^0$, $\epsilon\phi^1$, ..., $\epsilon\phi^n>$)
- the relation of increasing syntactical complexity of the formulas holds on the terms of every ω-sequence ($<\epsilon\phi^{00}$, $\epsilon\phi^{01}$, ..., $\epsilon\phi^{0n}>$, $<\epsilon\phi^{10}$, $\epsilon\phi^{11}$, ..., $\epsilon\phi^{1n}>$, ..., $<\epsilon\phi^{n0}$, $\epsilon\phi^{n1}$, ..., $\epsilon\phi^{nn}>$);
- if two terms have the same Rank and the same syntactical complexity, assign them two distinct and consecutive (second) apices – except in cases where their formulas are semantically equivalent.

Let $J(m, n)$ be a pairing function that assigns a natural number to every ordered pair of natural number (m, n) and define a function $J^0(m, n) := 2J(m, n)$.

Domain of second-order variables – $\wp(\mathbb{N} \cup \{-1\})$ Remember that every set α, which is the extension of a *Positive* and *Predicative* formula $A(x)$, not containing free second-order variables, belongs to $\wp(\mathbb{N})$: $\forall x(x \in \alpha \leftrightarrow A(x)$ is true). The same set must be assigned to all the semantically equivalent formulas.

Define a formula $A(x)$ – (*Positive* or not) *Predicative* and containing free second-order variables – and a formula $A^*(x)$ – (*Positiva* or not) *Predicative* and not containing free second-order variables – *I/x-equivalent* if and only if they are semantically equivalent under an interpretation I_n of the first-order variables x that they contain.

Show that, for every formula $A(x)$, *Predicative* and containing free second-order variables, exists a formula $A^*(x)$, *Predicative* and not containing free second-order variables, I/x-equivalent to it – under an interpretation I_n of their first-order variable x: let α be the set assigned to the free second-order variable X in $A(x)$; since such set is in the considered domain, there is another first-order formula $A^*(x)$ and there is an assignment I to the variables x in $A^*(x)$ such that α is also the denotation of $A^*(x)$.

***Positive* and *Predicative* Extension-terms – $\epsilon\phi_0$ – containing free second-order variables** Let $\epsilon\phi_0$ be an extension-term obtained by applying the extension operator to a *Positive* and *Predicative* formula, containing free second-order variables. Consider a formula ϕ_0^* – *Positive*, *Predicative* but not containing free second-order variables – which is I/x-equivalent to ϕ_0. Assign, to $\epsilon\phi_0$, the same denotation of $\epsilon\phi_0^*$.

***Positive* and not *Predicative* extension terms – $\epsilon\phi_n$ where n>0 (containing bound second-order variables)** Order all the $\epsilon\phi_{n>0}$ in a $\omega \times \omega$-sequence by the Rank and the Degree:
- the terms of every Degree (in the subscript) constitute a ω-sequence;
- the relation of increasing Degree of the terms holds on the ω-sequences ($<\epsilon\phi_1$, ..., ...>, $<\epsilon\phi_2$, ...,...>, ..., $<\epsilon\phi_n$, ..., ...>);
- the relation of increasing Rank of the terms (in the apex) holds on the terms of every ω-sequence ($<\epsilon\phi_1^0$, $\epsilon\phi_1^1$, ..., $\epsilon\phi_1^n>$, $<\epsilon\phi_2^0$, $\epsilon\phi_2^1$, ..., $\epsilon\phi_2^n>$, ..., $<\epsilon\phi_n^0$, $\epsilon\phi_n^1$, ..., $\epsilon\phi_n^n>$);
- if two terms have the same Degree and the same Rank, assign them two distinct

and consecutive apices, except in cases where their formulas are semantically equivalent.

Define another pairing function $K(m,n)$ such that $K(m,n) := 2J(m,n)+1$.

Inductively prove that $K(m,n)$ assigns a denotation to every *Positive* and not *Predicative* extension term – $\epsilon\phi_{n>0}$.

2.2 Verifying the axioms

In the last part of the talk, I show that, in this model, every instance of T-BLV and of CA is true.

References

[1] Boccuni, F. (2011). On the consistency of a plural theory of Frege's Grundgesetze. Studia Logica, 97(3), 329-345.

[2] Conti, L. (forthcoming). Russell's Paradox and Free Zig Zag Solutions, Journal Foundations of Science - Springer

[3] Ferreira, F. and K. F. Wehmeier (2002). On the Consistency of the Δ^1_1-CA Fragment of Frege's Grundgesetze. Journal of Philosophical Logic, 31, 301-311.

[4] Halbach, V. (2014). Axiomatic theories of truth. Cambridge University Press.

[5] Heck, R. K. (1996). The Consistency of Predicative Fragments of Frege's Grundgesetze der Arithmetik. History and Philosophy of Logic 17, 209–220.

[6] Jinxian Liu (2012). Second-order positive comprehension and Frege's basic law V. Frontiers of Philosophy in China, 2012, 7.3: 367-377.

[7] Pasniczek, J. (1998). The Logic of Intentional Objects: A Meinongian Version of Classical Logic, Dordrecht: Kluwer

Multi-valued logic in M-system theory

Mario Essert[1], Ivana Kuzmanović Ivičić[2], **Slobodan Jelić**[3], Tihomir Žilić[4], Juraj Benić[5]

[1,4,5] *Faculty of Mechanical Engineering and Naval Architecture, University of Zagreb*
Ivana Lučića 5, 10000 Zagreb, Croatia
[2,3] *Department of Mathematics, J.J. Strossmayer University of Osijek*
Trg Lj. Gaja 6, 31000 Osijek, Croatia
E-mail: [1]messert@fsb.hr, [2]ikuzmano@mathos.hr, [3]sjelic@mathos.hr, [4]tzilic@fsb.hr, [5]jbenic@fsb.hr

Keywords:
M-system, multi-valued logic, Dunn/Belnap, Shramko/Wansing, isomorphism

M-system theory, originaly defined in [2, 1], comes from the field of electric circuitry. In this talk we present multi-valued logic that is derivable from this theory. Even more, results from [1] are systemized, formalized and extended. Results about connection of obtained multi-valued logic with known logical systems, like Dunn/Belnap's four valued logic and Shramko/Wansing's sixteen valued logic, are given. New formal results about isomorphisms between M-system theory and above-mentioned multi-valued logical systems are the main results that will be presented in this talk.

References

[1] Mario Essert, Ivana Kuzmanović, Ivan Vazler, and Tihomir Žilić. Theory of m-system. *Logic Journal of the IGPL*, 25(5):836–858, 2017.

[2] Miro Šare. *Jorbologija*. Element, 2000.

Axiomatic modelling of notion of compromise in social choice theory

Aleksandar Hatzivelkos

University of Applied Sciences Velika Gorica, Croatia

Keywords:

social choice, axiom, compromise

Main goal of this paper is definition of a new axiom of social choice theory which would determine if a given social choice function has the property of electing compromise winner, where compromise is modelled as a version of Sorites paradox, as in my previous work [2, 3, 4, 5]. Additional motivation comes from work of Chatterji, Sen and Zeng [1]. In their paper they propose a social choice axiom that is satisfied if a social choice function can elect the middle candidate as the winner on the following profile of preferences:

$\lfloor \frac{n}{2} \rfloor$	$\lceil \frac{n}{2} \rceil$
A	C
B	B
C	A

Table 1: Basic motivation profile

In their work, Chatterji and others analyze a class of random social choice functions, and therefore, an axiom formulation is adjusted to that context. Nevertheless, it clearly shows that there is a scientific interest in an approach to the notion of compromise formulated upon such basic profile of preferences.

However, an axiom of social choice theory should be stated generally, not just for three candidates scenario. The question arises: what general form should take an axiom which would be a generalization of described three case scenario. This leads us to the following definition:

Definition (Weak Compromise Axiom (WCA))**.** *Social choice function* Φ *satisfies the Weak Compromise Axiom if on every set of three or more candidates, there is a profile of preferences* α*, such that the set of winning candidates of social choice function* Φ *contains a candidate which is not placed first in any preference of the profile* α*.*

In definition of Weak Compromise Axiom, we request that there should be a profile (for every set of three or more candidates) such that social choice function elects a candidate which is never top-ranked in the set of winning

candidates. Strong version of the axiom should require that set of winning candidates contains just one candidate.

Definition (Strong Compromise Axiom (SCA)). *Social choice function Φ satisfies the Strong Compromise Axiom if on every set of three or more candidates, there is a profile of preferences α, such that the set of winning candidates of social choice function Φ contains* only *a candidate which is not placed first in any preference of the profile α.*

From those definitions, we can see that if social choice function satisfies SCA, then it also satisfies WCA. It is also clear that those definitions are generalizations of the motivation idea from the beginning of the paper; in three candidates scenario only profiles of type from Table 1 can be used.

In this paper we will show that both definitions are well defined. We will provide a criterion which positional scoring social choice function must satisfy in order to satisfy WCA (SCA). Furthermore, we will show that axioms WCA and SCA are independent of other established axioms of the social choice theory: namely, Pareto axiom (PA) and positive responsiveness axiom (PRA). Logical connection of WCA (SCA) and axiom of independence of irrelevant alternatives (IIA) is also given.

Acknowledgements: This work has been supported in part by Croatian Science Foundation under the project UIP-2017-05-9219 and by the University of Applied Sciences Velika Gorica.

References

[1] Chatterji S., Sen A., Zeng H. *A characterization of single-peaked preferences via random social choice functions*. Theoretical Economics, 11(2):711–733, 2016.

[2] Hatzivelkos A. *The Mathematical Look at a Notion of the Compromise and Its Ramifications*, Proceedings of the Central European Conference on Information and Intelligent Systems (2017) pp. 301–308.

[3] Hatzivelkos A. *Borda and plurality comparison with regard to compromise as a Sorites paradox*, Interdisciplinary Description of Complex Systems 16 (2018) 465–484.

[4] Hatzivelkos A. *Mathematical model for notion of compromise in social choice theory.* Logic and Applications (LAP 2018) Book of Abstracts, pp. 50–52, Dubrovnik, 2018.

[5] Hatzivelkos, A., Stojanović B. *Minimization of the d-measure of divergence from the compromise.* Book of Abstracts of the 8th International Conference on Logic and Applications - LAP 2019, pp. 17–18, Dubrovnik, 2019.

Smart labels in proofs of completeness of interpretability logics

Sebastijan Horvat

Department of Mathematics, University of Zagreb

E-mail: sebastijan.horvat@math.hr

This talk is based on the paper [1]. Albert Visser [6] introduced system **IL** in 1988. In 1990. de Jongh and Veltman proved modal completeness of that logic. The question arises whether various extensions, such as **IL**W or **IL**M are complete. De Jong and Veltman in [3] and [4] proved modal completeness of logics **IL**M, **IL**P and **IL**W.

Evan Goris, Marta Bilkova and Joost J. Joosten [1, 5] in 2004. presented relatively simple proof of modal completeness and decidability of **IL**W. They did that by introducing so called assuring succesors.

In this talk, we will give a brief overview on Goris and Joosten [2, 5] construction method for proving completeness of some interpretability logics and we will see some properties of assuringness. We will use this to give an overview of the proof of completeness of interpretability logic **IL**W.

Acknowledgment

The research reported in the paper is partly supported by Croatian Science Foundation (HRZZ) under the projects UIP-2017-05-9219 and IP-2018-01-7459.

References

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

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

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

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

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

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

A Survey of Online Exam Proctoring

Marcel Maretić

University of Zagreb

E-mail: marcel.maretic@foi.unizg.hr

Keywords:
online exams, proctoring.

The coronavirus COVID-19 pandemic is the defining crisis of our time. Traditional universities are forced to transition to online universities at a moment's notice, opening many challenges in the process. Challenges of transitioning online require new approaches about course delivery and assessment in almost every possible aspect.

Majority of traditional universities already have some experience in online teaching because of the prevalence of blended learning. Blended learning usually includes a Learning Management System (LMS) which supports online teaching. Combined with webinars (video conferencing solution) LMS makes a solid foundation for teaching fully online. Most universities seem to have handled the migration of the teaching process reasonably well albeit with a considerable strain on the staff and resources. On the other hand, most of the assessment process has not moved from the classroom (face to face). Migration of assessment to fully online presents a much greater challenge.

Online exam proctoring tools exist, but because these are commercial they all suffer common shortcomings: high cost, considerable maintenance demands, closed black-box behaviour. These solutions have had little appeal for traditional universities because conducting classroom examinations with students on-site has simply been a better option in every way. Finally, the closed nature of these tools prevents academic inquiry about their reliability.

A development of an open sourced, automated, secure and unobtrusive proctoring solution for online examinations is needed, with the following desiderata:

i. low maintenance,

ii. integrated with LMS,

iii. unobtrusive and browser based (no need for additional client software),

iv. adaptable/modular (suitable in a variety of scenarios),

v. open source (to ensure low entry costs and to prevent vendor lock-in) and open for improvement by the academic community.

In its nature, online exam proctoring is adversarial. A suitable metaphor is an "arms race". With high enough stakes motivated cheaters will emerge,

find holes in the system and gain advantage. Unfortunately, cheating in online exams scales well. Therefore, openness and adaptability of the system is crucial. It must be designed for constant improvement in this "arms race setting.

The development of such a tool poses challenges and presents opportunities for research in several scientific fields. It seems that technological requirements for this to work today are attainable. The need for such a tool undeniably exists now. Therefore, the single remaining obstacle is to develop this software. The solution could originate from academia as it fits one of the principles of Open Source: it scratches a personal itch (see [2]).

References

[1] Tony Bates, *Tools to prevent online cheating*, Online Learning and Distance Education Resources - Moderated by Tony Bates,
available on 2020-08-20 at
`https://bit.ly/31UuKd3`

[2] Raymond, E., *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* , O'Reilly Media, 1999.

On ILWR-frames

Luka Mikec [1], Joost J. Joosten [2] and Mladen Vuković [3]

[1,3] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenika 30, 10000 Zagreb, Croatia
[2] *Department of Philosophy, University of Barcelona*
Carrer Montalegre 6, 08001 Barcelona, Spain
E-mail: [1] lmikec@math.hr, [2] jjoosten@ub.edu, [3] vukovic@math.hr

Keywords:
Formalised interpretability, interpretability logic, modal logic.

Interpretability logics are propositional modal logics extending provability logics with a binary modality $\rhd$ denoting formal interpretability over some base theory T. A Veltman frame is a structure $(W, R, \{S_w : w \in W\})$, where (W, R) is a Kripke frame for the provability logic **GL**. We use various forms of Veltman semantics to interpret interpretability logics. By an **IL**X-frame we mean (a regular, if not stated otherwise) Veltman frame such that no theorem of **IL**X can be refuted using this frame.

In [6] the logic known as **IL**R (**IL** $+ A \rhd B \to \neg(A \rhd \neg C) \rhd B \wedge \Box C$) was proven to be modally complete (w.r.t. generalised semantics); and another, known as **IL**W (**IL** $+ A \rhd B \to A \rhd B \wedge \Box\neg A$), was known to be modally complete much earlier [1]. Problems occurred while trying to prove that the combination of these two logics, **IL**WR, is modally complete (see [2] for the statement of the problem and a discussion on how to overcome the problem). At the moment we believe **IL**WR is modally complete if it can prove principles contained in a certain ("W-flavoured") series of principles.

We define the series of principles $(\mathsf{W}_n)_{n\in\omega}$ by stating $\mathsf{W}_0 := \mathsf{W} = A \rhd B \to A \rhd B \wedge \Box\neg A$ and for $n > 0$:

$$\begin{aligned} & \mathsf{U}_n := \Diamond C_{n-1} \vee \cdots \vee \Diamond C_1; \\ & \mathsf{V}_1 := A; \\ \text{for } n > 1: \quad & \mathsf{V}_n := \neg(C_{n-1} \rhd \Diamond A \vee B_{n-1} \vee \mathsf{U}_{n-1} \to \mathsf{V}_{n-1} \rhd B_{n-1}); \\ \text{for } n > 0: \quad & \mathsf{W}_n := A \rhd \Diamond A \vee B_n \vee \mathsf{U}_n \to \mathsf{V}_n \rhd B_n. \end{aligned}$$

Thus, the first few principles are (W_0 actually being equivalent to W_1):

$$\begin{aligned} \mathsf{W}_1 :& A \rhd \Diamond A \vee B_1 \to A \rhd B_1; \\ \mathsf{W}_2 :& A \rhd \Diamond A \vee B_2 \vee \Diamond C_1 \to \neg(C_1 \rhd \Diamond A \vee B_1 \to A \rhd B_1) \rhd B_2; \\ \mathsf{W}_3 :& A \rhd \Diamond A \vee B_3 \vee \Diamond C_2 \vee \Diamond C_1 \to \\ & \to \neg(C_2 \rhd \Diamond A \vee B_2 \vee \Diamond C_1 \to \neg(C_1 \rhd \Diamond A \vee B_1 \to A \rhd B_1) \rhd B_2) \rhd B_3. \end{aligned}$$

Earlier this year we gave a talk at the Advances in Modal Logic 2020 conference where we showed that the principles W_n are arithmetically valid [7]. We do not yet know e.g. if they are independent from other known principles. Here we discuss their Veltman semantics.

Acknowledgment

The first author is supported by the Croatian Science Foundation (HRZZ) under the projects UIP-2017-05-9219 and IP-2018-01-7459. The second author is supported by the Spanish Ministry of Science and Universities under grant number RTC-2017-6740-7, Spanish Ministry of Economy and Competitiveness under grant number FFI2015-70707P and the Generallitat de Catalunya under grant number 2017 SGR 270. The third author is supported by the Croatian Science Foundation (HRZZ) under the project IP-2018-01-7459.

References

[1] de Jongh, D. and F. Veltman, *Modal completeness of IL*W, in: J. Gerbrandy, M. Marx, M. Rijke and Y. Venema, editors, *Essays dedicated to Johan van Benthem on the occasion of his 50th birthday*, Amsterdam University Press, Amsterdam, 1999 .

[2] Goris, E., M. Blkov, J. Joosten and L. Mikec, *Assuring and critical labels for relations between maximal consistent sets for interpretability logics* (2020). URL `https://arxiv.org/2003.04623`

[3] Goris, E. and J. Joosten, *A new principle in the interpretability logic of all reasonable arithmetical theories*, Logic Journal of the IGPL **19** (2011), pp. 14–17.

[4] Joosten, J., L. Mikec and A. Visser, *Feferman axiomatisations, definable cuts and principles of interpretability*, forthcoming (2020).

[5] Joosten, J. and A. Visser, *How to derive principles of interpretability logic, A toolkit*, in: J. v. Benthem, F. Troelstra, A. Veltman and A. Visser, editors, *Liber Amicorum for Dick de Jongh*, Intitute for Logic, Language and Computation, 2004 Electronically published, ISBN: 90 5776 1289.

[6] Mikec, L. and M. Vuković, *Interpretability logics and generalised Veltman semantics*, The Journal of Symbolic Logic (to appear).

[7] Mikec, L., Joost J. Joosten, and Mladen Vuković. A W-flavoured series of interpretability principles. In *13-th Advances in Modal Logic, AiML 2020, Short papers (accepted)*, 2020.

[8] Visser, A., *An overview of interpretability logic*, in: M. Kracht, M. d. Rijke and H. Wansing, editors, *Advances in modal logic '96*, CSLI Publications, Stanford, CA, 1997 pp. 307–359.

Incremental automated safety and security reasoning with patterns

Vivek Nigam

fortiss GmbH, Munich, Germany & Federal University of Paraíba, João Pessoa, Brazil

The development of safety-critical systems requires the control of hazards that can potentially cause harm. To this end, safety and security engineers rely during the development phase on architectural solutions, called patterns, such as safety monitors, voters, and watchdogs. The goal of these patterns is to control (identified) faults and threats that can trigger hazards. Safety patterns can control such faults by e.g., increasing the redundancy of the system, while security patterns mitigate threats by, e.g., controlling information flows. Currently, the reasoning of which pattern to use at which part of the target system to control which hazard is documented mostly in textual form or by means of models, such as GSN-models, with limited support for automation.

This paper proposes the use of logic programming engines for automated reasoning about system safety and security. We propose a domain-specific language for embedded system safety and security and specify as disjunctive logic programs reasoning principles used by safety and security engineers to deploy patterns, e.g., when to use safety monitors, or watchdogs. Our machinery enables two types of automated reasoning:

(1) identification of which hazards can be controlled and which ones cannot be controlled by the existing patterns; and

(2) automated recommendation of which patterns could be used at which place of the system to control potential hazards.

Finally, we apply our machinery to two examples taken from the automotive domain: an adaptive cruise control system and a battery management system.

ConGraCNet 0.3: Corpus-based graph syntactic-semantic relations analysis

Benedikt Perak[1], **Tajana Ban Kirigin**[2]

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

Keywords: Natural Language Processing, Conceptual Similarity, Word Sense Induction, Corpus.

The paper will demonstrate the ConGraCNet application [1] for distinguishing word senses and identifying semantically related lexemes in a corpus by using the syntactic-semantic patterns of language usage. This unsupervised tagged corpus graph analysis method is based on the construction grammar approach to syntactic dependencies. ConGraCNet relies explicitly on the coordinated [X and|or Y] [4, 2] and [X_is_a_Y] syntactic grammatical relations between the lexical co-occurrences for the construction of the network representation. For a given source lexeme in a corpus, the method yields associated communities of collocation lexemes that represent the sense structure and different meanings based on the context of its usage. By projecting semantic value to a coordinated syntactical relation [X and|or Y], we can filter the lexical collocates with high conceptual similarity from a corpus and construct clustered lexical networks that reveal ambiguous referential meanings of a source lexeme. The members of a cluster are processed with an iterative graph function that finds best candidates for abstracted class label using [X_is_a_Y] syntactic-semantic construction.

For instance, the lexeme ASSERTIVENESS-n with 20809 occurrences in English Timestamped JSI web corpus 2014-2019, when processed with n=15 collocates used to construct a second-degree coordination graph (pruned with: degree$\geq$ 2, clustering method: leiden, partition type: mvp), yields the network of 43 elements and 4 clusters (Figure 1). The [X_is_a_Y] syntactic-semantic construction reveals the class labels in the first and the second degree. In relation with the members of class 1: [*'self-confidence-n' 'self-esteem-n' 'confidence-n' 'self-advocacy-n' 'self-worth-n' 'self-respect-n' 'self-image-n' 'esteem-n' 'self-awareness-n' 'self-reliance-n' 'independence-n' 'pride-n' 'Pride-n' 'motivation-n' 'skill-n'*], ASSERTIVENESS-n is related to ['PRIDE-n', 'PRIDE-n']1 ['EMOTION-n', 'MOTIVATION-n']2. In relation with the members of class 2: [*'aggressiveness-n' 'aggression-n' 'sociability-n' 'talkativeness-n' 'impulsivity-n' 'passivity-n' 'hyperactivity-n' 'hostility-n' 'irritability-n' 'impulsiveness-n' 'shyness-n' 'restlessness-n' 'agitation-n' 'euphoria-n'*], ASSERTIVENESS-n is related to ['AGGRESSION-n', 'TRAIT-n'], ['FEAR-n', 'REACTION-n']2. In relation with the members of class 3: [*'decisiveness-n' 'directness-n' 'boldness-n' 'optimism-n' 'extraversion-n' 'courage-n' 'bravery-n' 'clarity-n' 'frankness-n'*], ASSERTIVENESS-n is ['COURAGE-n', 'BRAVERY-n'] 1, [FAITH-n', 'VIRTUE-n']2. In relation with the members of class

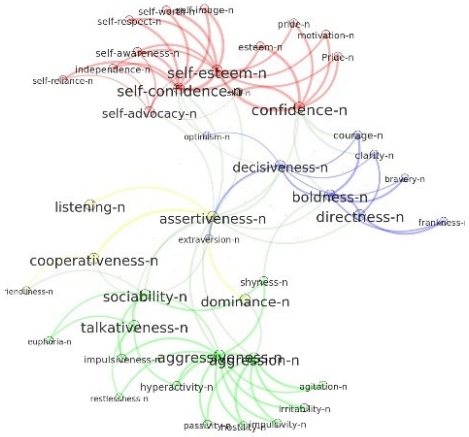

Figure 1: Second-degree coordination graph of source lexeme assertiveness-n pruned with: degree ≥ 2, clustering method: leiden, partition type: mvp. Network of 43 elements and 4 clusters.

4: [*'assertiveness-n' 'cooperativeness-n' 'dominance-n' 'listening-n' 'friendliness-n'*], ASSERTIVENESS-n is related to ['LISTENING-n', 'SKILL-n'] 1, ['ISSUE-n', 'PROBLEM-n']2.

We will explain the impact of the modulation of the linguistic and graph parameters, exemplify the application of the procedure on several lexemes in different languages and corpora and present the implementation of the WordNet external knowledge databases for further refinement of the results.

Acknowledgments

This work has been supported in part by the Croatian Science Foundation under the project UIP-2017-05-9219 and the University of Rijeka under the project Initial Grants 1016-2017.

References

[1] ConGraCNet application `http://emocnet.uniri.hr/congracnet/`. 2020.

[2] Dorow B. and Widdows D. Discovering corpus-specific word senses. In *Proc. EACL*, pages 79-82, 2003.

[3] Sketch Engine. `https://www.sketchengine.eu/`.

[4] Van Oirsouw R.R. The syntax of coordination. *Routledge*, 2019.