

15TH INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2026

September 23 - 27, 2026
Dubrovnik, Croatia

Book of Abstracts

Course directors:

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

Book of Abstracts of the 15th International Conference on Logic and Applications - LAP 2026, held as a hybrid meeting hosted by the Inter University Center Dubrovnik, Croatia, September 23 - 27, 2026.

L^AT_EX book of abstracts preparation and typesetting:

- Dušan Gajić, University of Novi Sad
- Jovana Obradović, Mathematical Institute of SASA, Belgrade
- Simona Prokić, University of Novi Sad
- Anastazia Žunić, Mathematical Institute of SASA, Belgrade

LAP 2026 Web site: <https://lap.math.hr/LAP2026/>

Maintained by Marko Horvat, University of Zagreb, and Simona Prokić, University of Novi Sad.

Contents

1	Branka Arapović, Silvia Ghilezan The Simply Typed Lambda Calculus with Symbolic Public-Key Cryptography	5
2	Tajana Ban Kirigin, Sanda Bujačić Babić Reliable Decision Rules for AI-Assisted Web Security	7
3	Péter Battyányi, Karim Nour Normalization in the $\lambda\mu\mu'$ -calculus using realizability semantics	9
4	Linda Brodo, Roberto Bruni, Emilio Tuosto, Dragiša Žunić Reaction Systems for Trading Venues	12
5	Konrad Burnik, Zvonko Iljazović, Lucija Validžić Metric bases and the existence of computable homeomorphisms	15
6	Matea Čelar, Zvonko Iljazović, Matea Jelić, David Tarandek Effective decomposability of arcs	17
7	Vincenzo Ciancia, Roberto Guanciale, Emilio Tuosto A Cryptographic Infrastructure for Friend-to-Friend Choreographies	18
8	Uli Fahrenberg Elements of Higher-Dimensional Automata Theory	21
9	Mariami Gamsakhurdia The Eliminability of Delta in Gödel Logics	24
10	Silvia Ghilezan, Paaras Padhiar Justification Logic of the Lambda Calculus	27
11	Valentina Harizanov Computable structure theory and asymptotic density	30
12	Sebastijan Horvat A Justification Logic Corresponding to the Interpretability Logic IL	32
13	Zvonko Iljazović, Bojan Pažek A Boundary Criterion for Computability of Co-c.e. Sets with Disconnected Complements	34
14	Zvonko Iljazović, Nikola Pražić Connectedness by Computable Arcs in Effective Peano Continua	37

15	Sándor Jenei Canonical and categorical rigid representations of finite local-unit-aligned totally ordered monoids	39
16	Roman Kuznets, Rojo Randrianomentsoa, Thomas Studer It's common knowledge—eventually?	42
17	Anela Lolić, Stella Mahler Proof Theoretic Applications of CERES	45
18	Helena Marciniš Topological bisimulations and bisimulation games for conservativity and interpretability logics	48
19	José Meseguer An Overview of Maude's NuITP Inductive Theorem Prover	50
20	Matej Mihelčič Mutation and crossover operators for redescription construction	52
21	Jovana Obradović The Bénabou-Roubaud theorem via string diagrams	55
22	Peter Csaba Ölveczky Formalizing and Analyzing Real-Time and Cyber-Physical Systems in Rewriting Logic	58
23	Jiří Raclavský Logic of Descriptions: Non-reference, Intensional Transitives, and Gödel's Slingshot	60
24	Luka Rak, Zvonko Iljazović Computability of creating codimension in the Hilbert cube pseudointerior	63
25	Luigi Santocanale, Gregory Chichery From *-Autonomous to Linearly Distributive via Strengths and Enrichments	65
26	Andre Scedrov Explorations in Infinitary Action Logic	68
27	Borja Sierra Miranda Modern tools for arithmetical completeness: provability models and proofs	70

28	Lutz Straßburger	
	Interpolation via Generalized Splitting	72
29	Teo Šestak	
	Abstract Socratic dialogue and dialectical logic	75
30	Zvonimir Šikić	
	Proof of Church-Turing Thesis	77
31	Carolyn Talcott	
	Logic and Intelligence	78
32	Milica Vučićević, Angelina Ilić Stepić, Nenad Stojanović	
	A Probabilistic-Logical Extension of the WOOP/MCII Method	79
33	Marcel Maretić	
	Rebasing Social Choice Functions	81

The Simply Typed Lambda Calculus with Symbolic Public-Key Cryptography

Branka Arapović¹, Silvia Ghilezan^{1,2}

¹*Faculty of Technical Sciences, University of Novi Sad*

Trg Dositeja Obradovića 6, Novi Sad, Serbia

²*Mathematical Institute of the Serbian Academy of Science and Art*

Kneza Mihaila 36, Belgrade, Serbia

E-mail: ¹`milakovicbranka@uns.ac.rs`, ²`gsilvia@uns.ac.rs`

Keywords: lambda calculus, type systems, private-key cryptography, formal methods, programming language security.

The Simply Typed Lambda Calculus ($\lambda_{\rightarrow}$) [1] provides a foundational framework for reasoning about computation, programming languages, and formal verification. Although its mathematical simplicity makes it suitable for studying type safety and operational semantics, it does not natively support cryptographic operations or secure communication mechanisms. As a consequence, cryptographic protocols and encrypted message exchange cannot be directly represented within the standard calculus.

This paper presents an extension of the Simply Typed Lambda Calculus with symbolic public-key cryptographic primitives. The proposed system introduces explicit language constructs for encryption, decryption, public communication, and terminal execution states. In addition, dedicated types are provided for public keys, private keys, ciphertexts, and messages. These extensions enable direct modeling of cryptographic communication within a typed functional framework while preserving the simplicity of symbolic reasoning.

The syntax of the calculus is extended with the terms

`encr  $s_1 s_2$` , `decr  $s_1 s_2$` , `out  $s$` , `halt`,

representing encryption, decryption, public output, and a distinguished terminal state, respectively. Operational semantics are defined using a call-by-value reduction strategy together with an idealized cryptographic reduction rule that models the correctness of asymmetric encryption. The type system statically enforces disciplined usage of cryptographic primitives by distinguishing public and private keys and restricting the admissible operands of encryption and decryption operations.

While classical information-flow calculi [2] focus on preventing unauthorized flows of confidential information to public channels [3], the proposed framework allows controlled observable dependencies on confidential data and, in return, relies on cryptographic concepts to guarantee the security of such information flows. Security is achieved through symbolic cryptographic protection rather than complete elimination of information flow. Consequently, encrypted values may be transmitted over public channels while preserving confidentiality of the underlying plaintexts within the formal model.

The paper illustrates the use of the calculus through examples of encrypted communication and discusses the security guarantees that can be expressed at the language level. Particular attention is devoted to the distinction between symbolic confidentiality and computational cryptographic security. While the framework captures correctness of cryptographic processing and prevents direct extraction of plaintext data without the corresponding private key, it abstracts away from probabilistic encryption, side-channel attacks, replay attacks, and computational indistinguishability considerations.

The proposed extension demonstrates that cryptographic communication primitives can be incorporated directly into a typed lambda calculus while maintaining a simple and mathematically tractable formal structure. The resulting framework may serve as a basis for future investigations of cryptographic reasoning, security properties, and formally verified communication protocols within typed functional languages.

Acknowledgment

The research reported in the paper is partly supported by project Scientific and Artistic Research Work of Researchers in Teaching and Associate Positions at FTS-UNS 2026 (No. 01-3609/1).

References

- [1] Barendregt, H., *The Simply Typed Lambda Calculus*, in: Lambda Calculus with Types.
- [2] Steve Zdancewic and Andrew C. Myers, *Secure Information Flow and CPS*, in Proceedings of the 10th European Symposium on Programming Languages and Systems (ESOP '01), Springer-Verlag, Berlin, Heidelberg, pp. 46–61, 2001.
- [3] Annalisa Bossi, Damiano Macedonio, Carla Piazza, and Sabina Rossi, *Information flow in secure contexts*, Journal of Computer Security, vol. 13, no. 3, pp. 391–422, May 2005.

Reliable Decision Rules for AI-Assisted Web Security

Tajana Ban Kirigin¹, Sanda Bujačić Babić¹

¹*University of Rijeka, Faculty of Mathematics*

Radmile Matejčić 2, 51000 Rijeka, Croatia

E-mail: ¹bank@math.uniri.hr, ¹sbujacic@math.uniri.hr

Keywords: web security, artificial intelligence, false positives, stochastic processes, formal methods.

Web applications generate heterogeneous traffic, ranging from ordinary user behaviour and legitimate automation to web scraping, bot-generated requests and vulnerability-exploiting interaction patterns. In such an environment, a central difficulty for AI-assisted security is to detect harmful behaviour without producing excessive false positive decisions on legitimate traffic.

We study this problem using a mathematical model in which the observable behaviour of a web application is represented by a stochastic process

$$X = (X_t)_{t \geq 0}.$$

An AI-assisted security mechanism is viewed as a decision rule

$$\delta_t : \mathcal{I}_t \longrightarrow \mathcal{D},$$

where $\mathcal{I}_t$ denotes the information available up to time t , such as request histories, logs, session behaviour or derived statistical features, and $\mathcal{D}$ is a finite decision space. This makes it possible to model different levels of intervention instead of reducing the problem to a binary accept/reject decision.

The quality of such a decision rule is measured not only by its ability to detect harmful behaviour, but also by its behaviour on legitimate traffic. In particular, one of the central quantities is the false-positive probability

$$\mathbb{P}(\delta_t(X_{[0,t]}) \in \mathcal{D}_{\text{int}} \mid X \text{ is legitimate}),$$

where $\mathcal{D}_{\text{int}} \subseteq \mathcal{D}$ denotes the set of intervention decisions. The main problem is to design decision rules for which this probability is small, while still detecting genuinely harmful or policy-violating behaviour.

The proposed framework connects stochastic processes, statistical decision theory, optimisation and formal methods, and provides a basis for analysing AI-assisted web security systems whose decisions are probabilistically interpretable and logically specified.

Acknowledgment

This work is supported by the European Union-NextGeneration EU under the project number uniri-iz-25-74-MMUI, and by the Croatian Science Foundation under the project HRZZ-IP-2024-05-3882.

References

- [1] Basseville, M., Nikiforov, I. V., *Detection of Abrupt Changes: Theory and Application*, Prentice Hall, 1993.
- [2] Berger, J. O., *Statistical Decision Theory and Bayesian Analysis*, Springer, 1985.
- [3] Baier, C., Katoen, J.-P., *Principles of Model Checking*, MIT Press, 2008.
- [4] Olivo, O., Dillig, I., Lin, C., Detecting and exploiting second order denial-of-service vulnerabilities in web applications, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

Normalization in the $\lambda\mu\mu'$ -calculus using realizability semantics

Péter Battyányi¹, Karim Nour²

¹*University of Debrecen, Faculty of Informatics, Department of Computer Science*

Kassai út 26., 4028 Debrecen, Hungary

²*Université Savoie Mont Blanc, CNRS, LAMA, LIMD*

73000 Chambéry, France:

¹`battyanyi.peter@inf.unideb.hu`, ²`karim.nour@univ-smb.fr`

Keywords:

Parigot's $\lambda\mu$ -calculus, weak and strong normalization, Curry-Howard isomorphism, realizability semantics

It was not known until the work of Murthy [11] and Griffin [8] that the Curry-Howard correspondence could be extended to classical logic. Since then, numerous calculi have been proposed to represent natural deduction and Gentzen-style derivations in classical logic [1, 6, 10, 13, 15, 16]. Among them, Parigot's $\lambda\mu$ -calculus [13] stands out for preserving the structure of natural deduction proofs within typing derivations, thereby establishing a direct correspondence between classical proofs and typed terms. Parigot's system provides a computational interpretation of second-order classical propositional logic.

The $\lambda\mu$ -calculus extends the λ -calculus by introducing classical variables (the so-called μ -variables), together with the corresponding term constructors and reduction rules. Our investigation focuses on de Groote's formulation of the $\lambda\mu$ -calculus [9], which generalizes Parigot's original system by allowing μ -abstractions to occur at arbitrary positions within terms. Consequently, the restriction that every μ -abstraction must be immediately followed by a μ -application is removed.

Besides the familiar β -reduction, the $\lambda\mu$ -calculus contains several reduction rules specific to classical logic. These rules are essential, for example, for obtaining uniqueness of data representation in the case of Church numerals [4, 12]. At the same time, they introduce additional proof-theoretic difficulties. In particular, the addition of the μ -, μ' -, and ρ -rules destroys strong normalization.

Strong normalization of the $\lambda\mu$ -calculus has nevertheless been established by various methods, both for second-order propositional types [14] and for the simply typed calculus [3, 7]. However, extending the calculus with further reduction rules substantially changes its normalization properties. In particular,

adding the ρ - or ε -rules causes strong normalization to fail [2]. Nevertheless, it was shown in [4] that the $\beta\mu\mu'\rho\theta\varepsilon$ -reduction still enjoys weak normalization. The proof relies on combinatorial arguments based on the syntactic structure of terms. Although these arguments can be formalized in first-order logic, they do not appear to extend naturally to the second-order propositional setting.

In this talk, based on [5], we present realizability-based proofs of strong and weak normalization for the simply-typed $\lambda\mu\rho\theta\varepsilon$ - and $\lambda\mu\mu'\rho\theta\varepsilon$ -calculi. Unlike the previous combinatorial approach, our method is formulated within the standard realizability framework and is expected to extend to the typed $\lambda\mu$ -calculus with second-order propositional types.

References

- [1] F. Barbanera and S. Berardi. *A symmetric lambda calculus for classical program extraction*, In: M. Hagiya and J.C. Mitchell (editors), Proceedings of theoretical aspects of computer software, TACS '94., Lecture Notes in Computer Science (789), pp. 495-515, Springer Verlag, 1994.
- [2] P. Battyányi. *Normalization properties of symmetric logical calculi*, PhD thesis, University of Chambéry, 2007.
- [3] P. Battyányi and K. Nour. *Normalization proofs for the un-typed $\mu\mu'$ -calculus*, Special Issue: LICMA'19 Lebanese International Conference on Mathematics and Applications., AIMS Mathematics, 5(4), pp. 3702-3713, 2020.
- [4] P. Battyányi and K. Nour. *Normalization in the simply typed $\lambda\mu\mu'\rho\theta\varepsilon$ -calculus*, Mathematical Structures in Computer Science, 32(8), pp. 1066–1098, 2022, <https://doi.org/10.1017/S096012952200041X>.
- [5] P. Battyányi and K. Nour. *Normalization properties of $\lambda\mu$ -calculus using realizability semantics*, Journal of Applied Logics (to appear)
- [6] P.-L. Curien and H. Herbelin. *The duality of computation*, In: M. Odersky, P. Wadler (editors), Proceedings of the Fifth ACM SIGPLAN International Conference on Functional Programming, ICFP '00, pp. 233-243, ACM Press, 2000.
- [7] R. David and K. Nour. *Arithmetical proofs of strong normalization results for the symmetric $\lambda\mu\mu'$ -calculus*, In: P. Urzyczyn (editor), Typed Lambda Calculi and Applications, TLCA '05, Lecture Notes in Computer Science (3461), pp. 162-178, Springer Verlag, 2005.
- [8] T. Griffin. *A formulae-as-type notion of control*, In: F. E. Allen (editor), Conference Record of the Seventeenth Annual ACM Symposium on Principles of Programming Languages, POPL '90, ACM Press, 1990.

- [9] Ph. de Groote. *An environment machine for the $\lambda\mu$ -calculus*, Mathematical Structures in Computer Science 8, pp. 637-669, 1998.
- [10] G. Munch-Maccagnoni. *Syntax and models of a non-associative composition of programs and proofs*, PhD thesis, Université Paris Diderot, 2013.
- [11] C. R. Murthy. *An evaluation semantics for classical proofs*, In: Proceedings of the sixth annual IEEE symposium on logic in computer science, pp. 96-107, 1991.
- [12] K. Nour. *La valeur d'un entier classique en $\lambda\mu$ -calcul*, Archive for Mathematical Logic 36, pp. 461-473, 1997.
- [13] M. Parigot. *$\lambda\mu$ -calculus: an algorithmic interpretation of classical natural deduction*, In: A. Voronkov (editor), Logic Programming and Automated Reasoning, Lecture Notes in Computer Science (624), Springer Verlag, Berlin, pp. 190-201, 1992.
- [14] M. Parigot. *Proofs of strong normalization for second order classical natural deduction*, Journal of Symbolic Logic (62), pp. 1461-1479, 1997.
- [15] N. J. Rehof and M. H. Sørensen. *The λ_{Δ} -calculus*, In: M. Hagiya, J. C. Mitchell (editors), Theoretical Aspects of Computer Software, Lecture Notes in Computer Science (789), pp. 516-542, Springer Verlag, 1994.
- [16] P. Wadler. *Call-by-value is dual to call-by-name*, In: C. Runciman, O. Shivers (editors), Proceedings of the Eighth ACM SIGPLAN International Conference on Functional Programming, ICFP '03, pp. 189-201, 2003.

Reaction Systems for Trading Venues

Linda Brodo¹, Roberto Bruni², Emilio Tuosto³,
Dragiša Žunić⁴

¹ *University of Sassari, Italy*

² *University of Pisa, Italy*

³ *Gran Sasso Science Institute (GSSI), Italy*

⁴ *Institute for Artificial Intelligence R&D of Serbia, Serbia*

E-mail: ¹ brodo@uniss.it, ² robertobruni@di.unipi.it, ³ emilio.tuosto@gssi.it,
⁴ dragisa.zunic@gssi.it

Keywords:

Reaction systems, trading venues, electronic exchanges, market microstructure, concurrency, formal methods.

Financial systems and trading venues. We propose a new variant of reaction systems tailored to models of computations taking place on trading venues. Our goal is to understand how financial systems operate at the core, seen as models of computation, and sometimes to propose how they should operate.

A notable feature of today’s economics is that it is predominantly understood through a quantitative paradigm. For example, we often hear about quantitative finance and almost never about qualitative finance. Our view is that cornerstone financial systems should be understood and (re)designed with a level of rigour comparable to that of theoretical computer science.

There is only a handful of such cornerstone systems; the most notable are trading venues and financial derivative contracts. Trading venues have arguably existed alongside human civilisations, naturally facilitating economic interaction between people. In this regard, “reactions” in that domain should describe this natural interaction between agents, rather than phenomena inside biological or chemical systems. However, at some level, these domains appear to be related.

A trading venue (aka stock exchange, electronic market) can be seen as a point of interaction of buyers and sellers, where trading is primarily based on the price at which agents are prepared to buy or sell the underlying asset.

Similarities and differences. Interactions are concurrent, with a continuous inflow of orders. Matching reflects a form of resource competition: more competitive orders are selected first, while less competitive ones are effectively inhibited by their presence. As higher-priority orders are executed and removed, this inhibition is lifted, enabling subsequent matches. The computation terminates when no further compatible interactions are possible (uncrossed market).

Unlike standard reaction systems, entities that do not participate in interactions are not discarded but persist to the next step. Conversely, entities that participate in a match are removed from the system and recorded in a trade log.

This study is relevant for the modern financial industry because exchanges still predominantly operate on a sequential computational core (*centralised limit order book*, CLOB model, in use since the 1970s). More recently, economists have proposed models that move towards parallel order matching, but these do not fully achieve it (*frequent batch auctions*, FBA model, in 2015).

Reaction systems provide a way to understand parallelism and concurrency at a fine-grained level that is otherwise difficult to reach.

In order to formalise both existing and novel models of exchange, we introduce a new variant of reaction systems, from both a set-theoretical and a process-algebraic perspective.

We model distributed systems with *located entities*, that is, resources that computations consume from or produce to specific locations. Consequently, entities can be either plain or associated with a location, and configurations are collections of such entities distributed across locations.

The set-theoretical perspective distinguishes two kinds of resources. Some entities are *consumable* and may be present in multiple copies, so that reactions compete for them. Others are *non-consumable* and are only checked for presence. To capture this distinction, we use *extended bags*, allowing us to combine quantitative and qualitative aspects within a single framework. Reactions are defined in the standard reaction systems style as triples of reactants, inhibitors, and products, and are applied in a context-sensitive way.

In addition to this set-theoretical view, we provide a process-algebraic formulation that makes explicit the interaction between the system and its environment. In this view, reactions are treated as processes, and computation proceeds in the presence of a *context* that may non-deterministically provide entities.

We consider distributed processes, where each process is located and has its own local reactions and local context. Contexts can be *guarded*, meaning that they introduce entities only when certain conditions are satisfied. This formulation allows us to model systems where multiple agents evolve concurrently across locations, while interacting through shared resources, and provides a natural representation of dynamic inflow and coordination between components.

Contribution summary. We formalize the standard market mechanisms in finance, namely CLOB and FBA, and introduce a model that addresses their limitations while capturing concurrent and parallel interaction on a trading venue. A key property of the model is that, after each computational cycle, the market is guaranteed to be in an *uncrossed* (stable) state. This means that no further trades can be performed until new participants enter.

The talk is based on [1, 2, 3] and on [4, 5, 6].

References

- [1] A. Ehrenfeucht, G. Rozenberg. Reaction systems. *Fundamenta Informaticae*, 75(1–4):263–280, 2007.
- [2] L. Brodo, R. Bruni, M. Falaschi. Enhancing reaction systems: A process algebraic approach. In M. Alvim, K. Chatzikokolakis, C. Olarte, and F. Valencia, editors, *The Art of Modelling Computational Systems*, volume 11760 of LNCS, pages 68–85. Springer, 2019.
- [3] L. Brodo, R. Bruni, M. Falaschi, I. Petre. Simulation and analysis of distributed reaction systems. *IEEE Access*, 13:119709–119725, 2025.
- [4] E. Budish, P. Cramton, J. Shim. The high-frequency trading arms race: Frequent batch auctions as a market design response. *The Quarterly Journal of Economics*, 130(4):1547–1621, 2015.
- [5] I. Cervesato, S. Khan, G. Reis, D. Žunić. Formalization of automated trading systems in a concurrent linear framework. *Electronic Proceedings in Theoretical Computer Science*, 292:1–14, 2019.
- [6] O. Inverso, E. Tuosto, D. Žunić. Emergent behaviour in financial markets. Accepted at the 13th Internat. Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2026).

Metric bases and the existence of computable homeomorphisms

Konrad Burnik¹, Zvonko Iljazović², Lucija Validžić³

¹*Independent researcher*

^{2,3}*University of Zagreb, Faculty of Science, Department of Mathematics*

E-mail: ¹kburnik@gmail.com, ²zilj@math.hr, ³lucija.validzic@math.hr

Keywords:

computable metric space, computable homeomorphism, metric basis.

A computable homeomorphism between two computable metric spaces is one that is itself computable and has a computable inverse. The existence of such a homeomorphism guarantees that the two spaces are not only topologically equivalent, but that this equivalence can be computed algorithmically. Therefore, finding conditions under which a computable metric space is computably homeomorphic to a well-known space is a frequent topic in computable topology.

For example, if we have a segment $[a, b]$ in $\mathbb{R}$, it is computably homeomorphic to $[0, 1]$ if and only if a and b are computable points, which is equivalent to saying that $[a, b]$ is a computable set in $\mathbb{R}$. On the other hand, we do not have the same equivalences in $\mathbb{R}^2$. There exists a computable arc in $\mathbb{R}^2$ which is not computably homeomorphic to $[0, 1]$ and does not have computable endpoints.

One reason these equivalences hold in $\mathbb{R}$ is that the endpoints of a segment possess a crucial property. Namely, if x_0 is an endpoint of a segment I , then any point in I is uniquely determined by its distance from x_0 . We say that x_0 is a *metric basis* for I . This property also holds for an endpoint of a half-closed interval in $\mathbb{R}$.

In this talk, we will show how the existence of a metric basis for a space X , together with some standard computable and topological conditions, ensures the existence of a computable homeomorphism $[0, 1] \rightarrow X$ and $[0, +\infty) \rightarrow X$. Our two main results are the following theorems:

Theorem 1 Assume that (X, d, α) is an effectively compact computable metric space such that (X, d) is connected. If there exists a point $x_0 \in X$ such that x_0 is a metric basis for (X, d) , then there exists a computable homeomorphism $[0, 1] \rightarrow X$.

Theorem 2 Assume that (X, d, α) is computable metric space which has the

effective covering property and such that (X, d) is connected, not compact and has compact closed balls. If there exists a point $x_0 \in X$ such that x_0 is a metric basis for (X, d) , then there exists a computable homeomorphism $[0, +\infty) \rightarrow X$.

Acknowledgment

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026 Institutional grants of University of Zagreb Faculty of Science (PMF-CROFUND, IK IA 1.1.3. Impact4Math).

References

- [1] Joseph S. Miller., *Effectiveness for Embedded Spheres and Balls*, Electronic Notes in Theoretical Computer Science, 66:127–138, 2002.
- [2] R.A. Melter and I. Tomescu, *Metric bases in digital geometry*, Computer Vision, Graphics, and Image Processing, 25:113–121, 1984.
- [3] Z. Iljazović, *Co-c.e. spheres and cells in computable metric spaces*, Logical Methods in Computer Science, 7(3:05):1–21, 2011.
- [4] V. Brattka and G. Presser, *Computability on subsets of metric spaces*, Theoretical Computer Science 305, 43–76, 2003.

Effective decomposability of arcs

Matea Čelar ^{*} Zvonko Iljazović [†] Matea Jelić [‡]
David Tarandek [§]

A continuum (i.e. a compact and connected metric space) (X, d) is said to be decomposable if there exist proper subcontinua K_1 and K_2 of (X, d) such that $X = K_1 \cup K_2$. We examine this notion from the viewpoint of computable topology. Let (X, d, α) be a computable metric space such that (X, d) is a continuum. We say that (X, d, α) is effectively decomposable if there exist proper computable sets K_1 and K_2 in (X, d, α) which are connected and such that $X = K_1 \cup K_2$. If (X, d, α) is effectively decomposable, then it easily follows that (X, d, α) is effectively compact. The main question is the following: if (X, d, α) is an effectively compact computable metric space such that (X, d) is a decomposable continuum, is (X, d, α) effectively decomposable? We prove that (X, d, α) is effectively decomposable if (X, d, α) is an effectively compact computable metric space such that (X, d) is an arc. Moreover, we have the following result.

Theorem 1 *If (X, d, α) is an effectively compact computable metric space such that (X, d) is a decomposable chainable continuum, then (X, d, α) is effectively decomposable.*

Acknowledgment

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026 Institutional grants of University of Zagreb Faculty of Science (PMF-CROFUND, IK IA 1.1.3. Impact4Math).

References

- [1] S.B. Nadler. Continuum theory. Marcel Dekker, Inc., New York, 1992.
- [2] Z. Iljazović and B. Pažek. Computable intersection points. *Computability*, 7, 57–99, 2018.

^{*}University of Zagreb, email: matea.celar@math.hr

[†]University of Zagreb, email: zilj@math.hr

[‡]University of Split, email: matea.jelic@gradst.hr

[§]University of Zagreb, email: david.tarandek@arhitekt.hr

A Cryptographic Infrastructure for Friend-to-Friend Choreographies

Vincenzo Ciancia¹, Roberto Guanciale², Emilio Tuosto³

¹*CNR, Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo", Pisa, Italy*

²*KTH Royal Institute of Technology, Stockholm, Sweden*

³*Gran Sasso Science Institute, L'Aquila, Italy*

E-mail: ¹ vincenzo.ciancia@isti.cnr.it, ² robertog@kth.se,
³ emilio.tuosto@gssi.it

The emergent paradigm of *local-first coordination* [7] envisages distributed computation harnessed by peer-to-peer architectures. The holy grail of local-first coordination is to let applications –and hence their users– to retain control on their computational resources as well as to foster autonomy [5, 6, 3, 4]. In fact, local-first coordination allows applications to continue to operate in isolation; intermittent connectivity is no longer an issue since the computational state is replicated among peers rather than maintained by third-party servers.

The quest for the holy grail imposes to move away, as much as possible, from the so-called cloud computing. Following this principles, we have recently proposed *friend-to-friend choreographies* [2], a new approach to distributed coordination aiming to build applications supporting distributed groupware among communities of trusted users¹ that, with an appropriate cryptographic infrastructure that features dissemination of events while ensuring confidentiality. Our key technical support is Nearbybytes [10], a decentralised infrastructure for local-first communication and storage that organises interactions through cryptographically protected shared logs.

In this work we spell out the cryptographic infrastructure of Nearbybytes, by giving a precise specification that enables us to reason about the security guarantees of our framework. In fact, in [2] we abstracted away from the cryptographic infrastructure necessary to ensure the confidentiality of the communications, and relied on the implementation offered by Nearbybytes. This approach allowed us to separate the concern of designing the application from the concern of confidentiality by taking care of the latter through a projection operation designed to identify which agents must be aware of an interaction and which agents can remain oblivious to it. In our F2F choreographies, the projection operation yields

¹This idea has been proposed in [8, 9] that suggested to base peer-to-peer coordination on trust emerging by “social relationships”.

a set of automata that formalise the behaviour that each agent should follow locally. These step embed master secrets for confidential communication (or for each group of participants interested by a specific projection of the communication). The master secret depends on sub-secrets (e.g. secret unique identifiers, or private keys) that are uniquely linked to each participant and combined for each relevant group of actor, therefore decoupled from each other.

Here we will give a formalisation of this cryptographic infrastructure of Nearbytes and use it to detail how the projection operation in [2] exploits them to ensure confidentiality of our friend-to-friend coordination framework. The strenght of Nearbytes relies upon *deterministic asymmetric keypair generation*, made practical via *ed25519* [1]. An agent independently derives a keypair from the master secret S so that agents sharing the same secrets share the same public-private keypair, say (Pub_S, Prv_S) . Therefore, each communication can use the private key Prv_S to sign messages, which in Nearbytes correspond to a write authorisation token on a channel identified by the public key Pub_S . Messages are also symmetrically encrypted using the master secret, so they can only be read by the participants.

Such infrastructure enables us to structure each channel as a *partially ordered event log*, independent from other channels; the partial ordering is an unavoidable feature, due to asynchronous concurrency. Also, the use of multicast allows multiple writers and multiple readers. The more abstract cryptographic language which is compiled in the way described above features non-deterministic choice and sequence, making together a strong, expressive combination.

Let us review the issue with an example.

Consider for instance four agents A, B, C, D, E . The choreographic language can express protocols such as:

either A sends a confidential message to B and then C sends a confidential message to E

or A sends a message to E and then both C and D send a confidential message to E .

Note that in the first branch above, C is not involved in the interaction between A and B ; likewise in the other branch C and D are not involved in the interaction between A and E . Assuming asynchronous communications, the realisation of this protocol in a traditional setting requires the introduction of hidden interactions in order to “flag” to B or to C and D which branch A had non-deterministically chosen. The choice what “hidden” interactions to add is arbitrary (and inefficient).

Instead, the choice of modelling channels by shared secrets, and deriving the secrets from the participant identities, permits a fully decentralised communication where each interaction is only seen and used by the participants that necessitate them at each step. In our example, there is one channel shared by A, B , and C , so that C can observe whether A has sent a message to B without needing to know the content of that message. Similarly, a secret shared among

A , C , D , and E , allows C and D to observe whether A has sent a message to E without B needing to know that secret, making it inherently decoupled from that interactions.

References

- [1] J. Brendel, C. Cremers, D. Jackson, and M. Zhao. The provable security of ed25519: Theory and practice. Cryptology ePrint Archive, Paper 2020/823, 2020.
- [2] V. Ciancia, R. Guanciale, D. Strollo, and E. Tuosto. Local-first coordination via friend-to-friend choreographies. *Journal of Logic and Algebraic Methods in Programming*, 2026. Submitted.
- [3] F. Furbach, L. Clorius, R. Kuhn, H. Melgratti, A. Scalas, and E. Tuosto. Compositional design, implementation, and verification of swarms. In *ECOOP 2026*, volume 372. LIPIcs, 2026.
- [4] F. Furbach, L. Clorius, R. Kuhn, H. Melgratti, A. Scalas, and E. Tuosto. Compositional design, implementation, and verification of swarms. In *ECOOP 2026*, volume 12. DARTS, 2026.
- [5] R. Kuhn, H. Melgratti, and E. Tuosto. Behavioural types for local-first software. In K. Ali and G. Salvaneschi, editors, *37th European Conference on Object-Oriented Programming, ECOOP 2023*, July 17-21, 2023, Seattle, Washington, United States, volume 263 of LIPIcs, pages 15:1–15:28. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
- [6] R. Kuhn, H. C. Melgratti, and E. Tuosto. Behavioural types for local-first software (artifact). *Dagstuhl Artifacts Ser.*, 9(2):14:1–14:5, 2023.
- [7] R. Kuhn and W. Reisz. Local-First Cooperation: Autonomy at the Edge, Secured by Crypto, 100local-first-cooperation, May 2021. Last access on June 14, 2026.
- [8] J. Li and F. Dabek. F2f: reliable storage in open networks. <https://iptps06.cs.ucsb.edu/papers/Li-F2F06.pdf>, 2006.
- [9] B. C. Popescu, B. Crispo, and A. S. Tanenbaum. Safe and private data sharing with turtle: Friends team-up and beat the system. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Security Protocols*, pages 213–220, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- [10] The Nearbytes Group. Nearbytes: a Local-First Architecture for Post- Cloud Computing, 2026. <https://github.com/nearbytes/community/blob/main/nearbytes-whitepaper-v0.1.pdf>.

Elements of Higher-Dimensional Automata Theory

Uli Fahrenberg

LMF, Paris-Saclay University

ENS Paris-Saclay, 4 avenue des Sciences, 91190 Gif-sur-Yvette, France

E-mail: uli@lmf.cnrs.fr

Keywords:

higher-dimensional automaton, pomset with interfaces, automata theory, concurrency theory.

Higher-dimensional automata (HDAs), introduced by Pratt and van Glabbeek [13, 15], are a general geometric model for non-interleaving concurrency which subsumes, for example, event structures and Petri nets [16]. HDAs of dimension one are standard automata, whereas HDAs of dimension two are isomorphic to asynchronous transition systems [6, 14]. As an example, Figure 1 shows Petri net and HDA models for a system with two events, labeled a and b . The Petri net and HDA on the left side model the (mutually exclusive) interleaving of a and b as either $a.b$ or $b.a$; those to the right model concurrent execution of a and b . In the HDA, this independence is indicated by a filled-in square.

We have recently started to develop the *language theory* of HDAs. [9] introduces languages of HDA as sets of partially ordered multisets with interfaces (ipomsets) [10] which are closed under order refinement (subsumption). [11] shows a Kleene theorem for HDAs, connecting rational and regular ipomset languages (those accepted by finite HDAs). [12] shows a Myhill-Nerode theorem, that ipomset languages are rational iff they have finite prefix (or equivalently, suffix) quotient, and [1, 3] introduce a notion of MSO for ipomsets and show that languages are rational iff they are MSO-definable, of finite width, and subsumption closed. Other recent work shows a Kamp theorem and results on recognizability, closure and decision properties, real-time extensions, and relations with Petri nets [2, 4, 5, 7, 8].

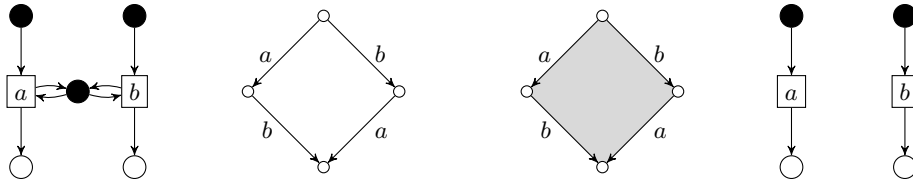


Figure 1: Petri net and HDA models distinguishing interleaving from non-interleaving concurrency. Left: models for $a.b + b.a$; right: models for $a \parallel b$.

I will give an introduction to higher-dimensional automata and their languages, with a focus on their algebraic and categorical properties. I will then say something about their language theory proper and try to convey intuition about where it differs from standard automata theory.

Acknowledgment

I thank my coauthors Amazigh Amrane, Hugo Bazille, Emily Clement, Marie Fortin, Loïc Hélouët, Christian Johansen, Philipp Schlehuber-Caissier, Georg Struth, and Krzysztof Ziemiański.

References

- [1] Amazigh Amrane, Hugo Bazille, Emily Clement, Uli Fahrenberg, Marie Fortin, and Krzysztof Ziemiański. Büchi-Elgot-Trakhtenbrot theorem for higher-dimensional automata. *CoRR*, abs/2505.10461, 2025. Submitted to Fundamenta Informaticae.
- [2] Amazigh Amrane, Hugo Bazille, Emily Clement, Uli Fahrenberg, and Philipp Schlehuber-Caissier. Higher-dimensional timed automata for real-time concurrency. In Andreas Rauh, Bernd Finkbeiner, and Paul Kröger, editors, *Design and Verification of Cyber-Physical Systems*, pages 66–100. Springer-Verlag, 2026.
- [3] Amazigh Amrane, Hugo Bazille, Uli Fahrenberg, and Marie Fortin. Logic and languages of higher-dimensional automata. In Joel D. Day and Florin Manea, editors, *DLT*, volume 14791 of *Lecture Notes in Computer Science*, pages 51–67. Springer-Verlag, 2024.
- [4] Amazigh Amrane, Hugo Bazille, Uli Fahrenberg, Loïc Hélouët, and Philipp Schlehuber-Caissier. Petri nets and higher-dimensional automata. In Elvio Gilberto Amparore and Łukasz Mikulski, editors, *PETRI NETS*, volume 15714 of *Lecture Notes in Computer Science*, pages 18–40. Springer-Verlag, 2025.
- [5] Amazigh Amrane, Hugo Bazille, Uli Fahrenberg, and Krzysztof Ziemiański. Closure and decision properties for higher-dimensional automata. *Theoretical Computer Science*, 1036, 2025.
- [6] Marek A. Bednarczyk. *Categories of Asynchronous Systems*. PhD thesis, University of Sussex, 1987.
- [7] Emily Clement, Enzo Erlich, and Jérémy Ledent. Kamp theorem for pom-set languages of higher dimensional automata. In Stefano Guerrini and Barbara König, editors, *CSL*, volume 363 of *LIPIcs*, pages 43:1–43:22. Dagstuhl LZI, 2026.
- [8] Enzo Erlich, Jérémy Ledent, and Krzysztof Ziemiański. Algebraic characterization of FO-definable languages of higher-dimensional automata. *CoRR*, abs/2605.25253, 2026.

- [9] Uli Fahrenberg, Christian Johansen, Georg Struth, and Krzysztof Ziemiański. Languages of higher-dimensional automata. *Mathematical Structures in Computer Science*, 31(5):575–613, 2021.
- [10] Uli Fahrenberg, Christian Johansen, Georg Struth, and Krzysztof Ziemiański. Posets with interfaces as a model for concurrency. *Information and Computation*, 285(2):104914, 2022.
- [11] Uli Fahrenberg, Christian Johansen, Georg Struth, and Krzysztof Ziemiański. Kleene theorem for higher-dimensional automata. *Logical Methods in Computer Science*, 20(4), 2024.
- [12] Uli Fahrenberg and Krzysztof Ziemiański. Myhill-Nerode theorem for higher-dimensional automata. *Fundamenta Informaticae*, 192(3-4):219–259, 2024.
- [13] Vaughan Pratt. Modeling concurrency with geometry. In *POPL*, pages 311–322. ACM Press, 1991.
- [14] Mike W. Shields. Concurrent machines. *Computer Journal*, 28(5):449–465, 1985.
- [15] Rob J. van Glabbeek. Bisimulations for higher dimensional automata. Email message, 1991. <http://theory.stanford.edu/~rvg/hda>.
- [16] Rob J. van Glabbeek. On the expressiveness of higher dimensional automata. *Theoretical Computer Science*, 356(3):265–290, 2006. See also [17].
- [17] Rob J. van Glabbeek. Erratum to “On the expressiveness of higher dimensional automata”. *Theoretical Computer Science*, 368(1-2):168–194, 2006.

The Eliminability of Delta in Gödel Logics

Mariami Gamsakhurdia

Vienna University of Technology
Vienna, Austria

E-mail: mariami@logic.at

Keywords:

Goedel Logics, Prenex Fragment, Delta Operator, Witnessed Goedel Logic.

Gödel logics G_V , (where set of truth values V is a closed subset of $[0, 1]$ containing 0 and 1) form an essential class of intermediate logics, those that are stronger than intuitionistic logic yet weaker than classical logic. The language is standard (propositional, first-order) with countably infinite propositional variables A_i , connectives $\wedge, \vee, \rightarrow$, and the constants $\perp$ for "false" and $\top$ for "true"; Atomic formulas include propositional variables, and truth constants.

Definition 1. A valuation $\mathcal{I}$ based on V is a function from the set of propositional variables into V given as follows:

- (1) $\mathcal{I}(\perp) = 0$, (2) $\mathcal{I}(\top) = 1$, (3) $\mathcal{I}(A \wedge B) = \min\{\mathcal{I}(A), \mathcal{I}(B)\}$,
- (4) $\mathcal{I}(A \vee B) = \max\{\mathcal{I}(A), \mathcal{I}(B)\}$, (5) $\mathcal{I}(\forall x A(x)) = \inf\{\mathcal{I}(A(u)) \mid u \in U_{\mathcal{I}}\}$,
- (6) $\mathcal{I}(\exists x A(x)) = \sup\{\mathcal{I}(A(u)) \mid u \in U_{\mathcal{I}}\}$, (7) $\mathcal{I}(A \supset B) = \begin{cases} \mathcal{I}(B), & \mathcal{I}(A) > \mathcal{I}(B), \\ 1, & \mathcal{I}(A) \leq \mathcal{I}(B). \end{cases}$

A formula in Gödel logic is valid iff the formula evaluates to 1 under every interpretation. The Gödel logic G_V is defined as the set of valid formulas. Note that the validity and 1-satisfiability are not dual in Gödel logic.

The asymmetry between the truth values 0 and 1 in Gödel logics, stemming from continuity conditions at 1, motivates the introduction of the absoluteness operator Δ [?], which precisely identifies formulas evaluating to 1

$$\mathcal{I}(\Delta A) = \begin{cases} 1 & \text{if } \mathcal{I}(A) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 1. *There is no connective $\triangle$ definable with other connectives and variables*

Proof. There are a finite number of 1-variable functions in Gödel logic.

$$\top, \perp, A, \neg A, \neg A \vee A, \neg A \supset A$$

Assume that $\triangle$ is definable by some of the function F , i.e., $\triangle(A) \leftrightarrow F(A)$. Now we look at the F in G_3 , because if $\triangle$ is not definable in G_3 then it is not definable in all larger Propositional Gödel logics.

The following truth table shows that none of them defines $\triangle$ and they are closed under composition by all connectives:

A	$\neg A$	$\top$	$\perp$	$A \vee \neg A$	$\neg A \rightarrow A$	$\triangle A$
0	1	1	0	1	0	0
1/2	1/2	1	0	1/2	1	0
1	0	1	0	1	1	1

Therefore we introduce the connective $\triangle$ extending the language. $\square$

We present a method for eliminating the absoluteness operator $\triangle$ from propositional Gödel logics by adopting a restricted semantics, where all propositional atoms, except the constant for truth, are interpreted strictly below 1. Although $\triangle$ is not definable from other connectives in standard Gödel logics, we show that under the restricted semantics, every formula with $\triangle$ is equivalent to a disjunction of chains, thus eliminating $\triangle$ entirely.

To indicate the use of such semantics, we denote Gödel logics by G_V^- . The valuation remains the same as defined above.

Proposition 2. *The formula $F(x_1 \dots x_n)$ in Gödel logic G_Δ^- is valid in the restricted semantics iff $(\neg \triangle x_1 \wedge \dots \wedge \neg \triangle x_n) \rightarrow F$ is valid in Gödel logics G_Δ with $\triangle$ in the usual semantics.*

The argument used for the propositional case does not extend to the first-order case. For example, when 1 is not isolated and does not belong to a perfect set, however, 0 is isolated or does belong to a perfect set, the first-order Gödel logic with $\triangle$ is not recursively enumerable, while the first-order Gödel logic without $\triangle$ is. This holds both for standard and restricted semantics. Consequently, in restricted semantics, first-order formulas with $\triangle$ are not (validity) equivalent to those without $\triangle$. Therefore there is not even an effective validity equivalence elimination of $\triangle$, and obviously no valid equivalence as in the propositional case. However, in the witnessed setting, all quantifier-shift principles are available and axiomatized, which allows us to extend the $\triangle$ -elimination algorithm to witnessed Gödel logics.

Acknowledgment

The research reported in the paper is a joint work with Matthias Baaz and is supported by FWF grant P 36571.

References

- [1] Matthias Baaz. Infinite-valued Gödel logic with 0-1-projections and relativisations. In Petr Hájek, editor, *Gödel'96: Logical Foundations of Mathematics, Computer Science, and Physics*, volume 6 of *Lecture Notes in Logic*, pages 23–33. Springer-Verlag, Brno, 1996.
- [2] Matthias Baaz, Mariami Gamsakhurdia. *Goedel logics: Prenex fragments*, arXiv preprint, CoRR abs/2407.16683, 2024
- [3] Matthias Baaz, Mariami Gamsakhurdia. *Goedel Logics: On the Elimination of The Absoluteness Operator*, arXiv preprint, CoRR abs/2605.05016 (2026)
- [4] Matthias Baaz, Norbert Preining. *Gödel–Dummett logics*, in: Petr Cintula, Petr Hájek, Carles Noguera (Eds.) *Handbook of Mathematical Fuzzy Logic* vol.2, College Publications, pp.585–626, chapterVII, 2011.
- [5] Matthias Baaz, Norbert Preining. *On the classification of first order Goedel logics*. *Ann. Pure Appl. Log* 170:36–57, 2019.
- [6] Matthias Baaz, Norbert Preining, and Richard Zach. *Characterization of the axiomatizable prenex fragments of first-order Gödel logics*. In 33rd IEEE International Symposium on Multiple-Valued Logic (ISMVL 2003), pages 175–180, Los Alamitos, IEEE Computer Society, 2003.

Justification Logic of the Lambda Calculus

Silvia Ghilezan¹, Paaras Padhiar²

¹*Faculty of Technical Sciences, University of Novi Sad*

Trg Dositeja Obradovića 6, Novi Sad 21000, Serbia

Mathematical Institute of the Serbian Academy of Sciences and Arts

Kneza Mihaila 36, Beograd 11000, Serbia

²*School of Computer Science, University of Birmingham*

University Rd W, Edgbaston, Birmingham B15 2TT, United Kingdom

E-mail: ¹gsilvia@uns.ac.rs, ²pxp367@student.bham.ac.uk

Keywords:

Justification logic, Lambda calculus.

Justification logic is an explicit modal logic where the $\Box$ modality is replaced with an explicit proof term t . The modal formula $\Box A$ read as ‘ A is *provable*’ is replaced with $[t]A$ interpreted as ‘ t is a *proof* of A ’. Proof terms are then manipulated through *proof operations*. In standard justification logics, the usual operations include the *proof application* operation which *internalises* modus ponens. The first justification logic is the *logic of proofs* (LP) introduced in [?, ?] which is an explicit counterpart to the classical modal logic S4. Via the Gödel translation of intuitionistic propositional logic (IPL) into S4, LP can also be read as a provability semantics for IPL. Under this reading, Hilbert-style proofs of IPL embed directly into LP: a theorem A of IPL is translated to a theorem $[t]A$ of LP for some proof term t . These proof terms can in turn be constructed through the lens of combinatory logic, where they correspond directly to manipulations of axiomatic reasoning and modus ponens [?].

With a similar motivation, we propose a *Justification Logic of the λ -calculus*, J_λ , an intuitionistic logic, where we incorporate terms of the λ -calculus of the negative fragment, more specifically the $(\wedge, \supset)$ -fragment, of IPL (λ IPL). We do so through embedding proofs of the λ -calculus into the logic, similarly to how Hilbert proofs of IPL are embedded into LP.

A feature of justification logic is *internalisation*, where the logic can internally reason about its own proofs. We utilise this for J_λ where the logic is then able to reason about its own computation. As a natural next step, we then explore a natural deduction formulation of J_λ to explore the computational content of that system and see how such content and proof terms relate.

The quest to explore a connection between proof terms and λ -terms began with Artemov [?] where LP was studied on an intuitionistic base giving a Gentzen-style sequent calculus and natural deduction system. The computational content of the resulting intuitionistic logic of proofs (iLP) was investigated through a Curry-Howard interpretation, although only a limited argument for normalisation was given. In [?] strong normalisation for (iLP) is achieved by using an extended natural deduction system which traces ‘historical’ computation through judgements. Other attempts include [?], using ideas of the λ -calculus, and [?] through the lens of type theory.

The system in [?] is later utilised in [?, ?, ?, ?] to study of other justification logics of computations. Of note, [?] studies the *Hypothetical Logic of Proofs*, a logic of natural deduction judgements of justification logic in which terms of the λ -calculus of the traced computation are incorporated into the proof terms of the justification logic. The obstacle that recurs throughout this line of work is that the λ -calculus is strictly more expressive than proof terms of LP: establishing a connection requires notions of term equality that have no direct counterpart on the justification logic side. As our logic is distinct to LP, and is constructed directly from the λ -calculus, we do not need to make such considerations.

Contributions. We introduce J_λ axiomatically, discuss its internalisation features and how the λ -calculus (λ IPL) *embeds* into the logic. We also introduce the typed λJ_λ natural deduction calculus and relate the proof terms of the language of J_λ to the term calculus of λJ_λ . To achieve normalisation, we construct and utilise Gentzen-style proof theory for J_λ (LJ_λ) proving a cut-elimination result. As we are working in the negative fragment, showing cut-elimination holds equates to normalisation. For full details of the results, the reader is referred to [?].

References

- [1] Jesse Alt and Sergei N. Artemov. Reflective λ -Calculus. In *Proof Theory in Computer Science*, pages 22–37. Springer, 2001.
- [2] Sergei N. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, December 1995.
- [3] Sergei N. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, March 2001.
- [4] Sergei N. Artemov. Unified Semantics for Modality and λ -terms via Proof Polynomials. In *Algebras, Diagrams and Decisions in Language, Logic and Computation - Lecture Notes*, pages 89–119. CSLI, 2002.
- [5] Sergei N. Artemov and Eduardo Bonelli. The Intensional Lambda Calculus. In *Logical Foundations of Computer Science*, pages 12–25. Springer, 2007.

- [6] Francisco Bavera and Eduardo Bonelli. Justification Logic and History Based Computation. In *Theoretical Aspects of Computing – ICTAC 2010*, pages 337–351. Springer, 2010.
- [7] Francisco Bavera and Eduardo Bonelli. Justification logic and audited computation. *J. Log. Comp.*, 28(5):909–934, 2018.
- [8] Neil J. DeBoer. Justification logic and type theory as formalizations of intuitionistic propositional logic. *J. Log. Comp.*, 32(8):1531–1557, 2022.
- [9] Silvia Ghilezan and Paaras Padhiar. Justification Logic of the Lambda Calculus, July 2026. arXiv:2607.24433.
- [10] Wilmer Ricciotti and James Cheney. Strongly Normalizing Audited Computation. In *CSL*, pages 36:1–36:21. Schloss Dagstuhl, 2017.
- [11] Daniyar S. Shamkanov. Strong Normalization and Confluence for Reflexive Combinatory Logic. In *WoLLIC*, pages 228–238. Springer, 2011.
- [12] Gabriela Steren and Eduardo Bonelli. Intuitionistic Hypothetical Logic of Proofs. In *IMLA 2013*. Elsevier, 2014.

Computable structure theory and asymptotic density

Valentina Harizanov

*Department of Mathematics, George Washington University
Washington, DC 20052, USA
E-mail: harizanv@gwu.edu*

Keywords: Computably enumerable, computable, asymptotic density, generically computable, coarsely computable

In their seminal paper [1] in 2012, Jockusch and Schupp introduced a systematic study of generically and coarsely computable sets of natural numbers, based on the notion of asymptotic density. While for generic computability we may not have answers on inputs from a subset of asymptotic density zero, for coarse computability we may have wrong answers on inputs from a subset of density zero. These notions were motivated by decision problems in combinatorial group theory. Many problems that are impossible to solve algorithmically on all inputs become easier if we only require that they be solved on a dense subset of inputs. We say that a set is dense if its asymptotic density is one. For example, the word problem for finitely generated groups is coarsely computable.

Together with Cenzer and Calvert, we extended this framework by introducing densely computable structures such as generically and coarsely computable ones (see [2]). We say that a countable (infinite) structure is *generically computable* if it has a computably enumerable (abbreviated as c.e.) substructure the domain of which is a dense set. A structure A is *coarsely computable* if there are a computable structure E and a dense set D such that the structure with domain D is a substructure of both A and E and all relations and functions agree on D . There are generically computable structures that are not coarsely computable and vice versa. These notions are further stratified by natural graded model-theoretic elementarity conditions for dense substructures that approximate structures. For example, a structure A is Σ_n -*generically c.e.* if there is a c.e. dense subset D such that the substructure with the domain D is a c.e. substructure of A and also a Σ_n elementary substructure of A . There are two directions in which these notions could potentially trivialize: either all structures have a densely computable copy, or only those having a computable (or a c.e.) copy.

We investigated dense computability variants for structures in general, and

in particular for equivalence structures, directed graphs induced by a unary one-to-one function, and abelian p -groups (see [2], [4]). For example, while every countable abelian p -group has a generically computable copy, this is not the case with abelian groups in general. More recently, jointly with Calvert, Cenzer, and Gonzalez, we also investigated dense computability for linear orders (see [5]).

In [3], we introduced the notions of densely computable isomorphisms. When computable isomorphic structures are not computably isomorphic, we investigate whether they are densely computably isomorphic ([3], [4]). We say that an isomorphism F from a structure A to a structure B is *generically computable* if there is a substructure of A with a computably enumerable domain C , with both C and its image under F being of asymptotic density one, and there is a partial computable function θ with domain C such that θ is equal to F on C . For example, there are computable abelian p -groups that are countably infinite products of cyclic groups of order p and p^2 , which are not computably isomorphic. However, we gave conditions under which two such groups are generically computably isomorphic.

Acknowledgment

This work has been supported by FRG NSF grant DMS-2152095.

References

- [1] C.G. Jockusch and P.E. Schupp, *Generic computability, Turing degrees, and asymptotic density*, Journal of the London Mathematical Society 85 (2012), pp. 472–490.
- [2] W. Calvert, D. Cenzer, and V. Harizanov, *Densely computable structures*, Journal of Logic and Computation 32 (2022), pp. 581–607.
- [3] W. Calvert, D. Cenzer, and V. Harizanov, *Generically and coarsely computable isomorphisms*, Computability 11 (2022), pp. 223–239.
- [4] W. Calvert, D. Cenzer, and V. Harizanov, *Generically computable Abelian groups and isomorphisms*, Journal of Logic and Computation 35 (2025), exaf044, 21 pp.
- [5] W. Calvert, D. Cenzer, D. Gonzalez, and V. Harizanov. *Generically computable linear orderings*, Annals of Pure and Applied Logic 176 (2025), 103612, 37 pp.

A Justification Logic Corresponding to the Interpretability Logic IL

Sebastijan Horvat

University of Zagreb Faculty of Science, Department of Mathematics

Bijenička cesta 30, Zagreb, Croatia

E-mail: sebastijan.horvat@math.hr

Keywords:

Justification logic, interpretability logic, realization theorem, sequent calculi.

Justification logics are epistemic logics in which modal formulas are replaced by formulas of the form $t : A$ with the intended interpretation *t is a justification for A*. In [1], Artemov introduced the Logic of Proofs LP, in which the expression $t : A$ has an interpretation *t is a proof of A*. He then proved a realization theorem connecting LP and the standard modal logic S4. More precisely, the forgetful projection of any formula of LP is obtained by replacing every subformula of the form $t : A$ with $\Box A$. The realization theorem states that not only the forgetful projection of any formula provable in LP is provable in S4, but also any formula A provable in S4 turns out to be the forgetful projection of a formula B provable in LP. Shamkanov in [3] introduced the justification logic JGL, corresponding to the Gödel-Löb provability logic GL, and proved the corresponding realization theorem. His proof relies on the sequent calculus for GL.

Interpretability logic IL extends the Gödel-Löb provability logic GL with a binary modality formalizing interpretability (see [4]). In [2] we introduced a non-wellfounded sequent calculus for IL and gave a simple proof of cut elimination for IL.

In this talk, I will present a new justification logic corresponding to the interpretability logic IL. In addition, I will briefly outline the proof of the realization theorem establishing the correspondence between these two systems.

Acknowledgment

This work is supported by Croatian Science Foundation under the project HRZZ-IP-2024-05-3882 and by the European Union –NextGenerationEU through the National Recovery and Resilience Plan 2021-2026 Institutional grants of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math).

References

- [1] S. N. Artemov, *Explicit provability and constructive semantics*, **Bulletin of Symbolic Logic**, 7 (1), pp. 1–36, 2001.
- [2] S. Horvat, B. Sierra Miranda, T. Studer, *Non-wellfounded Proof Theory for Interpretability Logic*, In: G. L. Pozzato, T. Uustalu (eds), **Automated Reasoning with Analytic Tableaux and Related Methods**. TABLEAUX 2025. Lecture Notes in Computer Science, vol 15980, Springer, Cham, pp. 201–219, 2026.
- [3] D. Shamkanov, *A realization theorem for the Gödel-Löb provability logic*, **Sbornik: Mathematics**, 207 (9), 2016.
- [4] A. Visser, *Interpretability logic*. In: P. P. Petkov (ed.), **Mathematical Logic**, Springer, Boston, pp. 175—209, 1990.

A Boundary Criterion for Computability of Co-c.e. Sets with Disconnected Complements

Zvonko Iljazović¹, Bojan Pažek²

¹*Department of Mathematics, Faculty of Science
University of Zagreb, Zagreb, Croatia*

²*Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
Josip Juraj Strossmayer University of Osijek, Osijek, Croatia
E-mail: ¹zilj@math.hr, ²bpazek@ferit.hr*

Keywords:

Computable topological space, co-c.e. set, computable set, effective local connectedness, connected components.

A co-computably enumerable set is given by negative information. In the usual metric setting this means that its complement can be effectively covered by rational open balls. Such information alone is not sufficient to obtain computability. In general, a nonempty co-computably enumerable closed set need not contain a computable point, and it need not be computable [5]. Therefore it is natural to ask which additional topological conditions make it possible to pass from negative information about a closed set to full computability of that set. One important source of such additional information is the component structure of the complement. If the complement of a co-computably enumerable closed set is disconnected, then its connected components may carry information about the boundary of the set. In this abstract we isolate a finite-component boundary condition which turns this topological information into an effective enumeration of all basic open sets intersecting the given set. To formulate this precisely, we first fix the framework in which these basic open sets are given.

Let $(X, \mathcal{T})$ be a topological space and let $(I_i)_{i \in \mathbb{N}}$ be a countable basis for $\mathcal{T}$. We say that the triple $(X, \mathcal{T}, (I_i))$ is a computable topological space if there exists a computably enumerable set $C \subseteq \mathbb{N}^2$ such that the following conditions hold:

- (i) If $(i, j) \in C$, then $I_i \subseteq I_j$.
- (ii) Whenever $x \in I_i \cap I_j$, there exists $k \in \mathbb{N}$ such that

$$x \in I_k, \quad (k, i) \in C, \quad (k, j) \in C.$$

Related definitions and approaches to computable topological spaces may be found in [6, 1, 7, 3]. A closed subset S of $(X, \mathcal{T})$ is said to be computably enumerable in $(X, \mathcal{T}, (I_i))$ if

$$\{i \in \mathbb{N} : I_i \cap S \neq \emptyset\}$$

is computably enumerable. A set $S \subseteq X$ is said to be co-computably enumerable (closed) if there exists a computably enumerable set $A \subseteq \mathbb{N}$ such that

$$X \setminus S = \bigcup_{i \in A} I_i.$$

Finally, S is computable (closed) if it is both computably enumerable and co-computably enumerable.

To use the connected components of $X \setminus S$ effectively, we need the basis to be compatible with connected neighbourhoods. This is provided by effective local connectedness. Informally, this means that the space admits an effective basis consisting of nonempty connected open sets. More precisely, it is formulated by requiring a sequence of nonempty connected open sets which is computably equivalent to the given basis (I_i) , following the idea used in the metric case in [4, 2]. The main result is the following boundary criterion.

Main result. *Let $(X, \mathcal{T}, (I_i))$ be an effectively locally connected computable topological space. Let $S \subseteq X$ be co-computably enumerable. Suppose that $X \setminus S$ is disconnected and has finitely many connected components. Assume moreover that each point $x \in S$ lies in the boundary of at least two different connected components of $X \setminus S$. Then S is computable in $(X, \mathcal{T}, (I_i))$.*

This result shows how a purely topological boundary condition on a co-computably enumerable closed set can provide the missing positive information needed for computability. In particular, the condition that each point of S is a boundary point of at least two components of the complement turns the finite component structure of $X \setminus S$ into a computably enumerable criterion for basic open sets to intersect S .

Acknowledgment

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026, within the institutional grant of the University of Zagreb, Faculty of Science (PMF-CROFUND, IK IA 1.1.3. Impact4Math). This work was also funded by the European Union – NextGenerationEU through the project DigSTEM-UP, grant number 581-UNIOS-39.

References

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

- [2] Brattka, V., *Plottable real number functions and the computable graph theorem*, SIAM J. Comput. 38(1), 303–328 (2008).
- [3] Horvat, M., Iljazović, Z., Pažek, B., *Computability of pseudo-cubes*, Annals of Pure and Applied Logic 171(8), 102823, 2020.
- [4] Iljazović, Z., Pažek, B., *Co-c.e. sets with disconnected complements*, Theory of Computing Systems 62, 1109–1124, 2018.
- [5] Specker, E., *Der Satz vom maximum in der rekursiven analysis*, Heyting, A. (ed.) Constructivity in Mathematics, pp. 254–265. North Holland Publica. Comp., Amsterdam (1959).
- [6] Weihrauch, K., *Computable Analysis*, Springer, Berlin, 2000.
- [7] Weihrauch, K., Grubba, T., *Elementary computable topology*, Journal of Universal Computer Science 15(6), 1381–1422, 2009.

Connectedness by Computable Arcs in Effective Peano Continua

Zvonko Iljazović¹, Nikola Pražić²

¹ *University of Zagreb*

² *University of Zagreb*

E-mail: ¹zilj@math.hr, ²nikola.prazic@fsb.unizg.hr

It is known that any two points are arcwise connected in a Peano continuum, which is a connected, compact and locally connected metric space. We examine effective Peano continua - connected, effectively compact and effectively locally connected computable metric spaces - and prove an effective version of this result: in an effective Peano continuum, any two distinct computable points are connected by a computable arc. Using this, we prove the following result.

Theorem 1 *In a connected, effectively compact and effectively locally connected computable metric space (X, d, α) , any arc can be arbitrarily closely approximated by a computable arc with computable endpoints.*

Acknowledgment

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026 Institutional grants of University of Zagreb Faculty of Science (PMF-CROFUND, IK IA 1.1.3. Impact4Math).

References

- [1] C.O. Christenson and W.L. Voxman. *Aspects of Topology*. Marcel Dekker, Inc., New York, 1977.
- [2] S.B. Nadler. *Continuum theory*. Marcel Dekker, Inc., New York, 1992.
- [3] Z. Iljazović and B. Pažek. Computable intersection points. *Computability*, 7:57–99, 2018.
- [4] Z. Iljazović and B. Pažek. Co-c.e. sets with disconnected complements. *Theory of Computing Systems*, 62(5):1109–1124, 2018.

- [5] R.G. Downey and A.G. Melnikov. Computably compact metric spaces. *Bulletin of Symbolic Logic*, 29:170–263, 2023.

Canonical and categorical rigid representations of finite local-unit-aligned totally ordered monoids

Sándor Jenei^{1,2}

¹*Institute of Mathematics and Informatics, Eszterházy Károly Catholic University, Hungary*

²*Institute of Mathematics and Informatics, University of Pécs, Hungary*

E-mail: jenei.sandor@uni-eszterhazy.hu, jenei@ttk.pte.hu

Keywords: finite totally ordered monoids; algebraic semantics; non-classical logics; local units; direct systems; categorical equivalence; rigid representation.

Algebraic semantics for many non-classical logics is built around ordered monoidal structures: residuated chains, BL- and MTL-chains, and closely related totally ordered monoids are typical examples. Decomposition and representation theorems for such structures therefore contribute to the structural study of formal systems and of reasoning in many-valued or substructural settings. This talk reports two connected results on a class of finite totally ordered monoids. The first is an object-level canonical representation theorem, developed in [?]. The second is its categorical refinement, developed in [?], which identifies the morphism classes for which the representation becomes an equivalence of categories.

Let $\mathbf{M} = \langle M, \leq, \cdot, e \rangle$ be a finite totally ordered monoid. For $x \in M$, let $\tau_r(x)$ be the greatest element $z \geq e$ such that $xz \leq x$, and let $\tau_\ell(x)$ be the greatest element $z \geq e$ such that $zx \leq x$. We call $\mathbf{M}$ *local-unit-aligned* if $\tau_r(x) = \tau_\ell(x)$ for every $x \in M$. In that case the common value is denoted by $\tau(x)$, and gives a local-unit map $\tau: M \rightarrow \text{Id}^+(\mathbf{M})$, where $\text{Id}^+(\mathbf{M})$ is the positive idempotent skeleton of $\mathbf{M}$. This definition is deliberately formulated beyond the usual commutative or integral assumptions.

The object-level result starts from the observation that the local-unit map contains enough information to decompose and reconstruct the whole ordered monoid. From τ we extract a canonical partition of $\text{Id}^+(\mathbf{M})$. Among the partitions of the positive idempotent skeleton, we take the finest one for which the block of $\tau(xy)$ depends only on the blocks of $\tau(x)$ and $\tau(y)$. This is the canonical τ -multiplication-coherent partition, denoted $\mathcal{C}_m(\mathbf{M})$. Its induced element-layers form a partition $\mathcal{L}_m(\mathbf{M})$ of M . Each layer carries a natural finite local-unit-aligned totally ordered monoid structure, and the ambient multiplication determines transition maps between the component monoids.

The central representation theorem of [?] states that every finite local-unit-aligned totally ordered monoid admits a canonical finite chain-indexed direct-system representation

$$\mathfrak{D}(\mathbf{M}) = ((\mathbf{M}_A)_{A \in \mathcal{C}_m(\mathbf{M})}, (\rho_{A,B})_{A \leq_{\min} B}),$$

where the index chain is ordered by the minima of the canonical blocks. Conversely, every direct system of the corresponding kind reconstructs a finite local-unit-aligned totally ordered monoid whose universe is the disjoint union of the components,

whose order is the directed lexicographic order, and whose multiplication is computed after transporting both factors to a common upper component. For $x \in M_i$, $y \in M_j$, and $k = \max\{i, j\}$, this product is $xy = \rho_{i,k}(x) \cdot_k \rho_{j,k}(y)$. The reconstruction is canonical: starting with $\mathbf{M}$, forming $\mathfrak{D}(\mathbf{M})$, and reconstructing gives back a monoid canonically isomorphic to $\mathbf{M}$.

A finite rigidity phenomenon turns this direct-system representation into a particularly strong one. The compatibility condition needed for the directed-lexicographic reconstruction to be an ordered monoid forces every proper transition map to be constant at the unit of the target component. Consequently, cross-level multiplication is absorptive: when two elements lie in different canonical components, the higher component controls the product through its local unit. Thus the representation is Clifford-like in two senses. Before rigidity is used, it resembles a component-and-transition-map reconstruction, as in strong-semilattice or Plonka-type representation principles. After finite rigidity is applied, it becomes ordinal-sum-like, in the spirit of Clifford's theory of naturally totally ordered commutative semigroups, but now in a possibly noncommutative setting where the identity need not lie at either endpoint of the chain.

The novelty is that no global multiplicativity law $\tau(xy) = \tau(x)\tau(y)$ is assumed. In the earlier residuated-chain setting of [?], local-unit stratification by the fibres of τ , together with the directed lexicographic order, was governed by such a strong global law. The present theorem replaces this exceptional multiplicativity by block-level multiplication coherence: the canonical quotient $\mathcal{C}_m(\mathbf{M})$ is precisely the quotient of the positive idempotent skeleton from which the components, transition maps, directed lexicographic order, and cross-component multiplication are recovered. This makes the local-unit geometry of $\mathbf{M}$ not merely descriptive, but structurally definitive.

The categorical sequel [?] asks for the categorical content of the same representation. Once a monoid has been replaced by its canonical rigid direct system, one must decide which homomorphisms of monoids are represented exactly by morphisms of systems. There is no single natural answer. Two complementary morphism theories arise. The first uses *strict block morphisms*: isotone unital monoid homomorphisms which send each canonical component into a canonical component and send the distinguished block unit to the corresponding target block unit. If $\mathbf{LUA}_{\text{fin}}^{\text{blk}}$ denotes the resulting category of finite local-unit-aligned totally ordered monoids, and $\mathbf{RigDS}_{\text{fin}}$ denotes the category of finite rigid direct systems with directed-order-compatible system morphisms, then the decomposition and reconstruction assignments form quasi-inverse equivalences $\mathfrak{D}: \mathbf{LUA}_{\text{fin}}^{\text{blk}} \rightleftarrows \mathbf{RigDS}_{\text{fin}}: \mathfrak{M}$. This is the cleanest categorical expression of the object-level theorem: component structure, transition compatibility, and the directed order are all preserved explicitly.

The second morphism theory is intrinsic to the local-unit map. An isotone unital homomorphism $f: \mathbf{M} \rightarrow \mathbf{N}$ is τ -compatible when $\tau_{\mathbf{N}}(f(x)) = f(\tau_{\mathbf{M}}(x))$ for every $x \in M$. Such a map need not preserve individual block units, and it may identify distinct positive idempotents. Hence several source components may collapse into a single target component. On the direct-system side this is encoded by a non-injective isotone index map together with component maps satisfying the corresponding compatibility, unit, and absorption conditions. Rigidity is essential here: the unit-constant transition maps are exactly what make component collapse compatible with multiplication and order. The second categorical theorem states

that the categories of finite local-unit-aligned totally ordered monoids with τ -compatible homomorphisms and of rigid direct systems with τ -compatible collapse morphisms are again equivalent, via quasi-inverse functors $\mathfrak{D}^{\tau^c}$ and $\mathfrak{M}^{\tau^c}$.

The two equivalences are complementary rather than nested. Strict block morphisms remember the canonical components and their distinguished block units component by component; τ -compatible homomorphisms are formulated solely by the equation $\tau_{\mathbf{N}}f = f\tau_{\mathbf{M}}$, and therefore record the same geometry at a more intrinsic level. Examples in [?] show that a τ -compatible homomorphism need not be a strict block morphism, and a strict block morphism need not be τ -compatible. The combined result is therefore both a structural and a functorial classification of finite local-unit-aligned totally ordered monoids: the canonical decomposition is an object-level reconstruction device and also a functorial invariant for the two natural morphism classes controlled by local units.

For the purposes of LAP, the relevance is twofold. First, the work provides new finite algebraic representation tools for ordered monoidal semantics without assuming commutativity or the strong additional hypotheses typically needed in residuated-chain representation theory to obtain meaningful structural decompositions. Second, the categorical refinements clarify which maps preserve the semantic content of the decomposition. Thus local units, positive idempotents, and rigid direct systems provide a common language connecting ordered algebra, many-valued and substructural semantics, and categorical methods in algebraic logic.

References

- [1] S. Bonzio. Dualities for Płonka sums. *Logica Universalis* **12** (2018), 327–339.
- [2] A. H. Clifford. Naturally totally ordered commutative semigroups. *American Journal of Mathematics* **76** (1954), 631–646.
- [3] A. H. Clifford. Totally ordered commutative semigroups. *Bulletin of the American Mathematical Society* **64** (1958), 305–316.
- [4] R. Horčík. Solutions to some open problems on totally ordered monoids. *Journal of Logic and Computation* **20** (2010), 977–983.
- [5] S. Jenei. Group representation for even and odd involutive commutative residuated chains. *Studia Logica* **110** (2022), 881–922. First circulated as arXiv:1910.01404 (2019).
- [6] S. Jenei. A canonical rigid direct-system representation of finite local-unit-aligned totally ordered monoids. Submitted.
- [7] S. Jenei. Categorical forms of the rigid direct-system representation for finite local-unit-aligned totally ordered monoids. Manuscript.
- [8] J. Płonka. On a method of construction of abstract algebras. *Fundamenta Mathematicae* **61** (1967), 183–189.
- [9] A. B. Romanowska and J. D. H. Smith. Duality for semilattice representations. *Journal of Pure and Applied Algebra* **115** (1997), 289–308.
- [10] M. Zawadowski. Generalized Płonka sums and products. *Applied Categorical Structures* **23** (2015), 63–86.

It's common knowledge—eventually?

Roman Kuznets¹, Rojo Randrianomentsoa²,
Thomas Studer²

¹*Institute of Computer Science of the Czech Academy of Sciences*

²*Institute of Computer Science, University of Bern, Switzerland*

E-mail: ¹kuznets@cs.cas.cz, ²{rojo.randrianomentsoa,thomas.studer}@unibe.ch

Keywords:

multi-agent systems, epistemic logic, eventual common knowledge, soundness and completeness

Common knowledge plays a central role in modeling coordination and agreement in distributed and multi-agent systems [5, 3]. Halpern and Moses showed that common knowledge is a prerequisite for certain forms of coordinated action, but also that it is *extremely fragile*: even arbitrarily small uncertainty about message delivery or clock synchronization makes common knowledge unattainable, which is the so-called *Halpern–Moses paradox* [5].

Since real coordination is inherently approximate, a line of work weakens the simultaneity built into common knowledge: ε -common knowledge requires the levels of mutual knowledge within a time window of length ε , and probabilistic and concurrent common knowledge relax it in other ways. We study *eventual common knowledge*, the greatest fixed point of *eventual mutual knowledge* $E_G^\diamond$ (just as common knowledge is the greatest fixed point of mutual knowledge [2]): a group G has eventual mutual knowledge of ϕ if every agent knows ϕ at *some* time, with no simultaneity imposed. In the runs-and-systems framework, $\mathcal{I}, r, m \models E_G^\diamond \phi$ holds iff for every $i \in G$ there is some time m_i with $\mathcal{I}, r, m_i \models K_i \phi$.

Epistemic principles of this kind are in particular used for modelling applications in distributed computing. The Firing Rebels with Relay problem [4] is closely related to eventual common hope, an epistemic notion that lies in a certain sense between belief and knowledge. Bitcoin and other distributed ledger protocols have been studied using Δ - $\Box$ -common knowledge [6] and probabilistic common knowledge [8]. Related analyses of blockchain protocols are, e.g., [1, 9, 10, 11], where the standard notion of common knowledge is used.

We introduce a possible world model for eventual common knowledge and give a sound and complete Hilbert-style axiomatization. The completeness proof is based on a canonical model construction that yields finite countermodels. Hence we obtain the finite model property and decidability. We also show that

eventual common knowledge departs sharply from standard common knowledge: it is strictly stronger than the infinite conjunction of its finite approximants, it is not factive, and it fails normality.

This presentation is based on our paper [7], which contains all details and full proofs.

References

- [1] Brünnler, K., Flumini, D., Studer, T.: A logic of blockchain updates. *Journal of Logic and Computation*, 30(8):1469–1485, December 2020. doi:10.1093/logcom/exaa045.
- [2] Bucheli, S., Kuznets, R., Studer, T.: Two ways to common knowledge. *Electronic Notes in Theoretical Computer Science*, 262:83–98, 2010. Proceedings of the 6th Workshop on Methods for Modalities (M4M-6 2009). doi:10.1016/j.entcs.2010.04.007.
- [3] Fagin, R., Halpern, J.Y., Moses, Y., Vardi, M.Y.: Reasoning About Knowledge. MIT Press (1995) doi:10.7551/mitpress/5803.001.0001
- [4] Fruzsa, K., Kuznets, R., Schmid, U.: Fire! In J. Halpern and A. Perea, editors, *Proceedings of the Eighteenth Conference on Theoretical Aspects of Rationality and Knowledge, Beijing, China, June 25–27, 2021, Beijing, China, June 25–27, 2021*, volume 335 of *Electronic Proceedings in Theoretical Computer Science*, pages 139–153. Open Publishing Association, 2021. doi:10.4204/EPTCS.335.13.
- [5] Halpern, J.Y., Moses, Y.: Knowledge and common knowledge in a distributed environment. *J. ACM* **37**(3), 549–587 (1990) doi:10.1145/79147.79161
- [6] Halpern, J.Y., Pass, R.: A knowledge-based analysis of the blockchain protocol. In J. Lang, editor, *Proceedings of the Sixteenth Conference on Theoretical Aspects of Rationality and Knowledge, Liverpool, UK, 24–26 July 2017*, number 251 in *Electronic Proceedings in Theoretical Computer Science*, pages 324–335, 2017. doi:10.4204/EPTCS.251.22.
- [7] Kuznets, R., Randrianomentsoa, R., Studer, T.: Axiomatizing Eventual Common Knowledge. In: *Logic, Language, Information, and Computation WoLLIC 2026*, in print
- [8] Marinković, B., Glavan, P., Ognjanović, Z., Doder, D., Studer, T.: Probabilistic consensus of the blockchain protocol. In G. Kern-Isberner and Z. Ognjanović, editors, *Symbolic and Quantitative Approaches to Reasoning with Uncertainty: 15th European Conference, ECSQARU 2019, Belgrade, Serbia, September 18–20, 2019, Proceedings*, volume 11726 of *Lecture Notes in Artificial Intelligence*, pages 469–480. Springer, 2019. doi:10.1007/978-3-030-29765-7_39.

- [9] Marinković, B., Glavan, P., Ognjanović, Z., Studer, T.: A temporal epistemic logic with a non-rigid set of agents for analyzing the blockchain protocol. *Journal of Logic and Computation*, 29(5):803–830, September 2019. doi:10.1093/logcom/exz007.
- [10] Ognjanović, Z., Ilić Stepić, A., Perović, A.: A probabilistic temporal epistemic logic: strong completeness. *Logic Journal of the IGPL*, 32(1):94–138, 2024. doi:10.1093/jigpal/jzac072.
- [11] Ognjanović, Z., Ilić Stepić, A., Perović, A.: A probabilistic temporal epistemic logic: Decidability. *Logic Journal of the IGPL*, 32(5):827–879, 2024. doi:10.1093/jigpal/jzac080.

Proof Theoretic Applications of CERES

Anela Lolić¹, Stella Mahler²

¹*Institute of Logic and Computation, TU Wien*

Vienna, Austria

²*Institute of Logic and Computation, TU Wien*

Vienna, Austria

E-mail: ¹anela@logic.at, ²stella@logic.at

Keywords:

cut-elimination, proof analysis.

Cut-elimination is one of the central techniques of proof theory. Beyond establishing consistency, it provides access to the computational content of proofs, enabling the extraction of interpolants, algorithms, and Herbrand information. The traditional *reductive* cut-elimination method of Gentzen [6] is however often computationally expensive and tends to obscure the global structure of proofs.

The *CERES method* (Cut-Elimination by Resolution) [4] approaches cut-elimination from a fundamentally different perspective. Instead of eliminating cuts locally, CERES decomposes a proof φ (of some end-sequent $\Gamma \vdash \Delta$) into two components: a *characteristic formula* F encoding the interaction of cuts and a cut-free *projection* φ^* preserving the local logical structure of the proof. The characteristic formula is unsatisfiable by construction, and its *refutation* ψ determines substitutions $\theta_1, \dots, \theta_n$ that are used to instantiate the projection, obtaining the result of CERES, the *CERES normal form*:

$$\frac{\frac{\frac{(\varphi^*\theta_2)}{\Gamma \vdash \Delta, F\theta_2} \quad \frac{\frac{(\varphi^*\theta_1)}{\Gamma \vdash \Delta, F\theta_1} \quad \frac{(\psi)}{F\theta_1, \dots, F\theta_n \vdash} \text{cut}}{\Gamma, F\theta_2, \dots, F\theta_n \vdash \Delta} \text{cut}}{\Gamma, F\theta_3, \dots, F\theta_n \vdash \Delta} \text{cut} + c^*}{\frac{(\varphi^*\theta_n)}{\Gamma \vdash \Delta, F\theta_n} \quad \vdots}{\Gamma \vdash \Delta} \text{cut} + c^*$$

While the CERES normal form still contains cuts, they are quantifier-free and thus allow for the extraction of crucial mathematical information. A demonstration of the ability of CERES to expose computational content from proofs was given in [3], where Fürstenberg's topological proof of the infinitude of primes was formalized as a sequence of **LK**-proofs. After applying CERES to the entire sequence, Euclid's original argument of prime construction was obtained.

The key conceptual advantage of CERES is the separation of normalization from proof analysis. While the characteristic formula captures the global interaction between cuts, the projection already contains the local proof-theoretic information of the original proof. Consequently, many proof-theoretic constructions can be carried out directly on the projection, without constructing a CERES normal form, i.e. without proof normalization. This is particularly suitable for the extraction of *Herbrand sequents*. Herbrand's theorem [1] characterizes the validity of a first-order formula by the existence of a propositionally valid combination of suitable instances of that formula. In the sequent calculus setting, the essential information is given by the instantiations of quantified formulas occurring in a proof. We show by an adaptation of the results in [8] that this information can be extracted directly from the projection.

Theorem 1.

Given a proof with cuts φ , let $H(\varphi^*)$ be the Herbrand sequent extracted from the projection φ^* alone. Let Θ be the set of substitutions obtained from a refutation of the characteristic formula. Then

$$\times_{\theta \in \Theta} H(\varphi^*)\theta$$

is the Herbrand sequent of the original proof ($\times$ denoting the merge operator on sequents).

While this result yields substantial *complexity improvements*, it also leads to a more general structural characterization of Herbrand extraction via CERES. Indeed, since reductive cut-elimination is non-confluent [2], different reduction strategies may produce different cut-free proofs and therefore different Herbrand sequents. This raises the following question: *Which Herbrand sequents can be extracted from a given proof with cuts?* As CERES simulates Gentzen-style normalization procedures [4], we obtain a static criterion for extractability.

Theorem 2.

Let φ be a proof with cuts and let $H(\varphi^*)$ denote the Herbrand sequent extracted from the projection. Then every Herbrand sequent obtainable from φ by reductive cut-elimination is of the form

$$\times_{\theta \in \Theta} H(\varphi^*)\theta,$$

for some set Θ of substitutions.

If a Herbrand sequent cannot be represented as a combination of substitution instances of $H(\varphi^*)$, then it cannot be obtained from the proof by any form of reductive cut-elimination.

A similar phenomenon appears in *interpolation*. As shown in [5], interpolants of proofs containing cuts can be extracted directly from projections without normalizing the proof. Again, the relevant proof-theoretic information is already present in the cut-free fragments obtained through CERES in its projection.

The scope of these ideas extends beyond ordinary first-order proofs. In [7], *inductive proofs* are represented by proof schemata, finite objects describing

recursively defined sequences of proofs. The schematic version of CERES provides characteristic formulas and projections at the schematic level and thereby enables proof-theoretic analysis of inductive arguments. Herbrand information has been shown to be extractable directly from schematic projections, suggesting that extractability criteria and interpolant constructions developed for ordinary **LK**-proofs can be lifted systematically to the inductive setting.

Taken together, the significance of CERES does not lie solely in providing an alternative route to cut-elimination. Rather, the method isolates projections as canonical carriers of computational information. Herbrand sequents, interpolants, extractability criteria, and schematic proof analyses can all be obtained from these cut-free fragments before normalization is completed. In this sense, CERES should be viewed not only as a method of cut-elimination but as a general framework for proof analysis.

Acknowledgment

This research was funded in part by the Austrian Science Fund (FWF) 10.55776/RIC1287724.

References

- [1] Buss, S.R., On Herbrand’s Theorem, in *Logical and Computational Complexity*, pp. 195–209, 1994.
- [2] Baaz, M., Hetzl, S., On the Non-Confluence of Cut-Elimination, *Journal of Symbolic Logic* 76(1), 313–340 (2011).
- [3] M. Baaz, S. Hetzl, A. Leitsch, C. Richter, and H. Spohr. CERES: An analysis of Fürstenberg’s proof of the infinity of primes. *Theoretical Computer Science*, 403(2–3):160–175, 2008.
- [4] Baaz, M., Leitsch, A., *Methods of Cut-Elimination*, Springer, 2011.
- [5] Corbard, S., Lolić, A., Efficient Interpolation Beyond Cut-Free Proofs: Admissible Cuts and Optimized Extraction, in *Proceedings of ICTAC 2025*, Lecture Notes in Computer Science, pp. 185–201, Springer, 2025.
- [6] Gentzen, G., Untersuchungen über das logische Schließen, *Mathematische Zeitschrift* 39, 176–210, 405–431 (1934–35).
- [7] Leitsch, A., Cerna, D.M., Lolic, A., *First-Order Schemata and Inductive Proof Analysis*, Springer, 2026.
- [8] Leitsch, A., Lolić, A., Extraction of Expansion Trees, *Journal of Automated Reasoning* 62(3), 393–430 (2019).

Topological bisimulations and bisimulation games for conservativity and interpretability logics

Helena Marcioš ¹

¹*Department of Mathematics, University of Zagreb Faculty of Science*

Bijenička cesta 30, 10000 Zagreb

E-mail: ¹`helena.marcioš@math.hr`

Keywords:

Topological semantics, Conservativity logic, Interpretability logic, Bisimulations, Bisimulation games

Conservativity logic **CL**, introduced by Ignatiev [3], and interpretability logic **IL**, introduced by Visser [6], are extensions of provability logic **GL** with a binary modality $\triangleright$. Since these logics are not strongly complete with respect to their relational semantics, Iwata and Kurahashi [4] introduced topological semantics for **CL** and **IL** and proved the strong completeness of these logics with respect to their topological semantics.

In this talk, we define topological bisimulations for this semantics and discuss their properties. We show that bisimilar points are modally equivalent, and we prove the analogue of the Hennessy-Milner theorem.

We also introduce topological bisimulation games and prove that two points are bisimilar if and only if Duplicator has a winning strategy in every topological bisimulation game starting with these points.

Acknowledgment

This work is supported by the Croatian Science Foundation under the project HRZZ-IP-2024-05-3882 and by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021-2026. Institutional grant of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math.)

References

- [1] M. Aiello, J. van Benthem, Logical Patterns in Space. In: D. Barker-Plummer et al. (eds.), *Words, Proofs, and Diagrams*, pp. 5–25, CSLI, Stan-

ford, 2002.

- [2] V. Čačić, i D. Vrgoč, A Note on Bisimulation and Modal Equivalence in Provability Logic and Interpretability Logic. *Studia Logica*, 101:31–44, 2013
- [3] K. N. Ignatiev, *Partial conservativity and modal logics*, Technical Report ITLI Publication Series X-91-04, University of Amsterdam, 1991.
- [4] S. Iwata, T. Kurahashi, Topological semantics of conservativity and interpretability logics, *Journal of Logic and Computation* 31:7 (2021) 1716–1739
- [5] R. de Jonge, IL-modellen en bisimulaties. preprint X-2004-06, ILLC, Amsterdam, 2004.
- [6] A. Visser, *Preliminary notes on interpretability logic*, Logic Group Preprint Series No. 29, 1988.

An Overview of Maude’s NuITP Inductive Theorem Prover

José Meseguer

University of Illinois at Urbana-Champaign, USA

E-mail: meseguer.jose@gmail.com

Keywords: Maude, theorem prover

Verification of equational programs by inductive theorem proving faces a dilemma between program expressiveness and proof automation. On the one hand, equational languages like Maude [1], CafeOBJ [2], and OBJ [3] support sophisticated features such as order-sorted types, conditional equations, and rewriting modulo axioms (of associativity, commutativity, and identity) that allow elegant and concise specifications of complex systems. On the other hand, the high expressiveness of these logics reduces the applicability of fully automated provers, inclining users toward interactive environments that, while powerful, require significant manual effort and expertise.

To bridge this gap, an inductive theorem prover must not only support the full expressiveness of the language’s equational logic, but should also scale up to large proofs by maximizing automation. This requires moving beyond simple rewriting tactics to employ powerful, theory-aware symbolic reasoning. The inductive inference system for order-sorted equational logic modulo axioms used by NuITP was proposed and proved sound in [4] and aims precisely at achieving these goals. This system integrates twenty-one inference rules based on advanced symbolic techniques – including narrowing, constructor variant unification, variant satisfiability, order-sorted congruence closure and ordered rewriting – tailored to work natively modulo axioms. Crucially, the theoretical analysis in [4] identifies that a majority of these rules (12 out of 21) are simplification rules, meaning that they can be applied automatically to discharge or simplify goals without user intervention.

This talk will present NuITP, the first full-scale implementation of the inference system described in [4]. Its main goal is to make the formal verification of programs in expressive equational languages considerably easier and more scalable than up to now by combining high levels of automation based on powerful symbolic methods with a variety of sophisticated explicit induction methods considerably more versatile and effective than standard structural induction.

Acknowledgment

The NuITP is joint work with Francisco Durán, Santiago Escobar and Julia Sapiña.

References

- [1] Clavel, M., Durán, F., Eker, S., Meseguer, J., Lincoln, P., Martí-Oliet, N., Talcott, C.: All About Maude – A High-Performance Logical Framework. Springer LNCS Vol. 4350 (2007)
- [2] Futatsugi, K., Diaconescu, R.: CafeOBJ Report. World Scientific (1998)
- [3] Goguen, J., Winkler, T., Meseguer, J., Futatsugi, K., Jouannaud, J.P.: Introducing OBJ. In: Software Engineering with OBJ: Algebraic Specification in Action, pp. 3–167. Kluwer (2000)
- [4] Meseguer, J.: Inductive reasoning with equality predicates, contextual rewriting and variant-based simplification. J. Log. Algebraic Methods Program. 144, 101036 (2025)

Mutation and crossover operators for redescription construction

Matej Mihelčić^{1,2}

¹*Department of Mathematics, Faculty of Science, University of Zagreb
Bijenička cesta 30, Zagreb, Croatia*

²*Department of Electronics, Ruđer Bošković Institute
Bijenička cesta 54, Zagreb, Croatia
E-mail: ¹matmih@math.hr*

Keywords: redescription construction, mutation, crossover, tournament.

Abstract

Redescription mining [7] is an unsupervised data mining methodology tasked with discovery of subsets of entities that can be characterized by multiple descriptions. These descriptions are presented as tuples of rules and called re-descriptions. Rules that form redescrptions should describe mutually similar subsets of entities, or ideally all describe the same set of entities. Discovery and analyses with redescrptions is increasingly used in a variety of domain tasks, where a set of entities (people, countries, locations, species etc.) can be characterised with multiple mutually disjoint sets of attributes. These sets can portray different aspects of entities, measure their state in different time points or phases of life-time. Redescrptions reveal strong equivalence relations between these different aspects, providing unique rule-based descriptions that can potentially lead to novel domain insights.

The CLUS-RM algorithm [4] is a redescription mining algorithm based on Predictive Clustering trees [3], capable of producing large number of redescrptions. The CLUS-RM algorithm applies a conjunction refinement operation to increase redescription accuracy [4] and utilizes redescription set construction by redescription extraction procedure [4] to create a fixed-sized set of representative redescrptions from a larger pool of candidates. This significantly smaller set of representative redescrptions of user-defined size is ultimately presented to the user. The ability of the CLUS-RM algorithm to produce large number of candidates and the fact it retains many candidates in memory prior final set construction makes it suitable for application of genetic metaheuristics [2]. Genetic operators and selection techniques from the domain of genetic algorithms can introduce modifications into available candidate redescrptions with

the main goal of increasing diversity and accuracy of available candidates, ultimately leading to outputs of superior quality.

In this work, we study genetic selection, mutation and crossover operators of redescrptions, modifying, adapting and extending existing techniques for rule mining [1] and association rule mining [8]. We also develop a tournament strategy [5] that allows using available CLUS-RM candidates and the most promising candidates to produce extended set of candidates with the ultimate goal of improving overall quality of produced output sets of redescrptions. Unlike many applications where genetic operators are applied to a fixed set of candidates, here each iteration brings completely new candidates, thus techniques will need to be adapted in a direction of open-ended evolution [6]. Special attention will be given to efficient incorporation of the developed extensions into the CLUS-RM algorithm.

Acknowledgements

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021-2026. Institutional grant of University of Zagreb Faculty of Science (IK IA 1.1.3. Impact4Math) and (PMF-CROFUND).

References

- [1] Alex Alves Freitas. “A Review of evolutionary Algorithms for Data Mining”. *Soft Computing for Knowledge Discovery and Data Mining*. Ur. Oded Maimon i Lior Rokach. Springer, 2008., str. 79–111. DOI: 10.1007/978-0-387-69935-6_4.
- [2] Sourabh Katoch, Sumit Singh Chauhan i Vijay Kumar. “A review on genetic algorithm: past, present, and future”. *Multim. Tools Appl.* 80.5 (2021.), str. 8091–8126. DOI: 10.1007/S11042-020-10139-6.
- [3] Dragi Kocev i dr. “Tree ensembles for predicting structured outputs”. *Pattern Recognit.* 46.3 (2013.), str. 817–833. DOI: 10.1016/J.PATCOG.2012.09.023.
- [4] Matej Mihelcic i dr. “A framework for redescription set construction”. *Expert Syst. Appl.* 68 (2017.), str. 196–215. DOI: 10.1016/J.ESWA.2016.10.012.
- [5] Efe Precious Onakpojeruo i dr. “Selection Techniques in Genetic Algorithm”. *17th International Conference on Development in eSystem Engineering, DeSE 2024, Khorfakkan, United Arab Emirates, November 6-8, 2024*. IEEE, 2024., str. 411–416. DOI: 10.1109/DESE63988.2024.10912015.
- [6] Norman H. Packard i dr. “Open-Ended Evolution and Open-Endedness: Editorial Introduction to the Open-Ended Evolution I Special Issue”. *Artif. Life* 25.1 (2019.), str. 1–3. DOI: 10.1162/ARTL_E_00282.

- [7] Naren Ramakrishnan i dr. “Turning CARTwheels: an alternating algorithm for mining redescrptions”. *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Seattle, Washington, USA, August 22-25, 2004*. Ur. Won Kim i dr. ACM, 2004., str. 266–275. DOI: 10.1145/1014052.1014083.
- [8] Xiaowei Yan, Chengqi Zhang i Shichao Zhang. “Genetic algorithm-based strategy for identifying association rules without specifying actual minimum support”. *Expert Syst. Appl.* 36.2 (2009.), str. 3066–3076. DOI: 10.1016/J.ESWA.2008.01.028.

The Bénabou-Roubaud theorem via string diagrams

Jovana Obradović

*Mathematical Institute of the Serbian Academy of Sciences and Arts
Belgrade, Serbia*

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

Keywords: string diagrams, monadic descent

Given a fibration $p : \mathcal{E} \rightarrow \mathcal{C}$ and a morphism $f : B \rightarrow A$ in the base category $\mathcal{C}$, Grothendieck's descent theory [3] studies the problem of reconstructing the fiber $\mathcal{E}_A$ from the fiber $\mathcal{E}_B$ via the pullback functor $f^* : \mathcal{E}_A \rightarrow \mathcal{E}_B$. The information lost under f^* is compensated by equipping objects of $\mathcal{E}_B$ with additional structure, called *descent data*. This gives rise to the category $\text{Desc}_p(f)$ together with the comparison functor $\Phi_p^f : \mathcal{E}_A \rightarrow \text{Desc}_p(f)$, yielding the descent factorization

$$\begin{array}{ccc} \mathcal{E}_A & \xrightarrow{\Phi_p^f} & \text{Desc}_p(f) \\ & \searrow f^* & \swarrow U_f \\ & \mathcal{E}_B & \end{array} \quad (1)$$

where U_f is the forgetful functor. The central question is whether Φ_p^f is an equivalence of categories. Morphisms f satisfying this condition are called *effective descent morphisms*.

In their seminal paper [1], Bénabou and Roubaud observed that, whenever $p : \mathcal{E} \rightarrow \mathcal{C}$ is a Beck–Chevalley bifibration, the descent factorization (1) coincides with the Eilenberg–Moore factorization

$$\begin{array}{ccc} \mathcal{E}_A & \xrightarrow{\Phi_p^{T_f}} & \text{EM}_p(T_f) \\ & \searrow f^* & \swarrow U_{T_f} \\ & \mathcal{E}_B & \end{array} \quad (2)$$

associated with the adjunction $f^* \dashv f_! : \mathcal{E}_B \rightarrow \mathcal{E}_A$, up to an equivalence $\text{Desc}_p(f) \simeq \text{EM}_p(T_f)$. Consequently, effective descent morphisms are precisely those morphisms for which the pullback functor is monadic. However, their article did not attempt to provide a proof of the equivalence $\text{Desc}_p(f) \simeq \text{EM}_p(f)$.

In [4], Janelidze and Tholen introduced a third description of the category of descent data, identifying it with the category $\text{Act}_p^{\text{Eq}(f)}$ of actions of the internal category $\text{Eq}(f)$, induced by the kernel pair of f , on p , while treating the Bénabou-Roubaud theorem as folklore.

Over the years, a number of other authors have also returned to the topic, but a complete written proof of the Bénabou–Roubaud theorem has remained elusive. Only very recently, in his 2024 article [7], Kahn filled this gap by presenting a detailed, rigorous proof of the Bénabou–Roubaud theorem in the original 1-categorical context. Nevertheless, in order to simplify the calculations, he rectified the pseudofunctor $f \mapsto f^*$ to an honest functor, which eliminated the need to manage pseudofunctorial coherence isomorphisms. Even with this “bypass”, the proof contains long series of explicit calculations.

The aim of this paper is to provide a different kind of proof of the Bénabou–Roubaud theorem, based entirely on the formal calculus of string diagrams. We introduce a string-diagrammatic 2-category $\mathbf{BiFib}_{\mathcal{C}}$ generated by the *bifibrational signature*, namely the 2-polygraph encoding the pseudofunctorial structure of pullback functors, their adjoints, and the Beck–Chevalley transformations. The key proof-theoretic ingredient is the soundness and completeness theorem of Joyal and Street [6], which identifies equality of 2-cells with equality of isotopy classes of string diagrams. Consequently, equalities between natural transformations can be established by finite sequences of local diagrammatic rewritings rather than by explicit componentwise computations. The three notions of descent data

$$\mathrm{EM}_p(T_f), \quad \mathrm{Desc}_p(f), \quad \mathrm{Act}_p^{\mathrm{Eq}(f)}$$

are obtained by extending the calculus of $\mathbf{BiFib}_{\mathcal{C}}$ in three different ways, each with a single additional generating 2-cell satisfying appropriate relations. Their equivalence is then established entirely within the graphical calculus, making the proof a derivation in a sound and complete rewriting system rather than a sequence of coherence calculations.

Besides yielding a complete proof of the Bénabou–Roubaud theorem, the diagrammatic approach has several conceptual advantages. First, pseudofunctorial coherence is treated explicitly as part of the syntax, rather than eliminated by strictification, and its coherence is established internally in $\mathbf{BiFib}_{\mathcal{C}}$. Second, the soundness and completeness of the graphical calculus allow associativity, functoriality and naturality to be absorbed by the syntax, reducing long algebraic arguments to short rewriting derivations. Finally, we obtain a new characterization of the category $\mathrm{Act}_p^{\mathrm{Eq}(f)}$, providing an explicit bridge between the classical and monadic descriptions of descent data. More generally, we expect that the same proof-theoretic framework will be useful in other contexts involving Beck–Chevalley bifibrations, such as the categorical semantics of dependent type theory (cf. [5, 2]).

Acknowledgment

The author would like to thank François Lamarche who generously shared the idea and motivation to treat the Bénabou–Roubaud result in a studious and novel way. The author would also like to thank Pierre-Louis Curien for very useful conversations concerning this topic.

References

- [1] J. Bénabou and J. Roubaud, Monades et descente, *Comptes Rendus de l'Académie des Sciences* 270, Serie A, 96-98 (1970).
- [2] P.-L. Curien, Substitution up to isomorphism, *Fundamenta Informaticae* 19, 51-85 (1993) (preliminary version appeared as LIENS Technical report 90-9 (1990)).
- [3] A. Grothendieck, Technique de descente et théorèmes d'existence en géométrie algébrique. I. Généralités. Descente par morphismes fidèlement plats, *Séminaire Bourbaki*, Exp. No. 190, vol. 5, Soc. Math. France, Paris, 299-327 (1995).
- [4] G. Janelidze and W. Tholen, Facets of Descent, II, *Appl. categorical struct.* 5, 229-248 (1997).
- [5] B. Jacobs, Categorical logic and type theory, *Studies in logic and the foundations of mathematics*, vol. 141. Elsevier (1999).
- [6] A. Joyal and R. Street, The Geometry of Tensor Calculus. I , *Advances in Mathematics* 88, 55-112 (1991).
- [7] B. Kahn, On the Bénabou-Roubaud theorem, arXiv:2404.00868, (2025).

Formalizing and Analyzing Real-Time and Cyber-Physical Systems in Rewriting Logic

Peter Csaba Ölveczky

University of Oslo

Real-time systems are often formally modeled using timed automata, or timed extensions of Petri nets, process algebras, and similar formalisms. These formalisms tend to sacrifice modeling convenience to support sound analysis. For example, the timed automaton formalism is quite restrictive, to ensure that dense-time systems have discrete abstractions which satisfy the same properties.

However, these formalisms typically do not support features such as user-defined data types, different forms of communication, hierarchical models, unbounded data structures, dynamic object creation and deletion, and so on. These features are all naturally supported by rewriting logic [6], which is an intuitive, general, and expressive logic for distributed systems. The Maude [4] language and tool supports the formal specification, simulation, reachability analysis, and LTL model checking of distributed systems in rewriting logic.

In this talk, I first explain how real-time systems can be modeled in rewriting logic as *real-time rewrite theories* [7] and how they can be formally analyzed in Maude [3]. In particular, real-time rewrite theories provide a natural model for object-based distributed real-time systems. While such theories define a general and expressive formalism for real-time systems, the price to pay is that property-preserving discrete abstractions of dense-time systems may not always exist, which may render Maude analyses of such systems unsound.

The key questions are:

1. Is this expressiveness and modeling convenience (e.g., supporting the above features) needed for real-time and cyber-physical systems?
2. *If* these features are needed for sophisticated real-time systems (which therefore cannot easily, or at all, be modeled as timed automata), can Maude analysis still provide useful results for such complex systems?

In this talk I give a sample of applications which answer the above questions affirmatively; such applications include large transport protocols, wireless sensor networks, scheduling algorithms, cloud-based transaction systems, and so on.

The expressiveness and generality of real-time rewrite theories also make them a suitable semantic framework for modeling languages for real-time and cyber-physical systems. Such theories have been used to provide formal semantics for sophisticated industrial and academic modeling languages, including (subsets of) the avionics modeling standard AADL, the DoCoMo labs language L, the UC Berkeley languages Ptolemy II and Lingua Franca, and timed model transformations. In many cases, we have also integrated automated Maude analyses into the corresponding modeling tools.

The recent integration of SMT solving into Maude has allowed us to regain soundness and completeness of Maude analysis for classes of dense-time systems that include parametric timed automata and parametric time Petri nets [2, 1]. We have also developed a tool, HYBRIDSYNCHAADL, for hybrid systems with complex control programs, and have shown that HYBRIDSYNCHAADL in many cases outperforms leading reachability analysis tools for hybrid systems [5].

The paper [3] gives a fairly recent overview of applications of real-time rewrite theories and Maude to real-time and cyber-physical systems.

References

- [1] J. Arias, K. Bae, C. Olarte, P. C. Ölveczky, L. Petrucci: *A Rewriting-logic-with-SMT-based Formal Analysis and Parameter Synthesis Framework for Parametric Time Petri Nets*, *Fundamenta Informaticae* 192(3-4): 261-312, 2024.
- [2] J. Arias, K. Bae, C. Olarte, P. C. Ölveczky, L. Petrucci, F. Rømming: *Symbolic analysis and parameter synthesis for networks of parametric timed automata with global variables using Maude and SMT solving*, *Science of Computer Programming* 233: 103074, 2024.
- [3] K. Bae, C. Olarte, P. C. Ölveczky: *Modeling and Analyzing Real-Time Systems in Rewriting Logic*, in *Concurrent Programming, Open Systems and Formal Methods*, volume 16120 of *Lecture Notes in Computer Science*, Springer, 2026.
- [4] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, C. L. Talcott: *All About Maude*, volume 4350 of *Lecture Notes in Computer Science*, Springer, 2007.
- [5] J. Lee, S. Kim, K. Bae, P. C. Ölveczky: *HybridSynchAADL: Modeling and Formal Analysis of Virtually Synchronous CPSs in AADL*, in *Proc. CAV'21*, volume 12759 of *Lecture Notes in Computer Science*, Springer, 2021.
- [6] J. Meseguer: *Conditional Rewriting Logic as a Unified Model of Concurrency*, *Theoretical Computer Science* 96(1): 73-155, 1992.
- [7] P. C. Ölveczky, J. Meseguer: *Specification of real-time and hybrid systems in rewriting logic*, *Theoretical Computer Science* 285(2): 359-405, 2002.

Logic of Descriptions: Non-reference, Intensional Transitives, and Gödel's Slingshot

Jiří Raclavský

Masaryk University, Arne Novaka 1, Brno, 602 00, the Czech Republic

E-mail: raclavsky@phil.muni.cz

1 Aim of the present paper

The present paper addresses 3 logical puzzles in the *theory of descriptions* (henceforth TD):

- (A) *non-referring descriptions* (e.g. “the King of France”, “ $\iota y. = (y, \div(x, 0))$ ”, “ $\lim_{x \rightarrow a} f(x)$ ” for some values, ...) (a non-classical semantics is needed);
- (B) *intensional transitives* ITVs (e.g. “seeks D ”, where the ITV’s complement D can be a description – which is typically not intersubstitutable, so special semantics for D is needed);
- (C) (Gödel’s) *slingshot argument* (consisting in a seemingly acceptable substitution and so-called ‘redistribution’ of descriptions that results in collapse of all facts into one Big Fact; so semantics must be nonstandard to prevent the collapse).

All the problems (as well as many others) can be successfully treated by the logic for TD being developed by the present author (partly in his 2020, 2022, 2024). It’s based on the ideas of the TD by the Czech/New-Zealandean logician Tichý, who nevertheless never published it in sufficient details (cf. only few passages in his book 1988). Nevertheless, it uniquely combines Russellian and Fregean–Churchian TD approaches (cf. below). The used logical framework (see the present author’s 2022, 2024 with Kuchyňka), which is a substantial modification of Tichý’s early ND, is an extension of Church–Henkin *type theory*; it’s equipped with *labelled natural deduction in sequent style*. The framework is a sort of *possible worlds semantics*, i.e. it aims to *formalize* the substantial fragment of *natural language*.

Note that the puzzle (A) has its 101st anniversary: Russell (1905). The puzzle (B) is due to Church (1951), but Quine (1956) is usually quoted for

it (70th anniversary) and, finally, (C) comes from the influential analysis of Russell's TD by Gödel (1944) who was born in Brno 120 years ago.

2 Sketch of the solutions

The present abstract naturally neither offer enough room for any details of solutions to (A)–(C), or wider discussion of the approach, whose features are thus only briefly and incompletely suggested below.

(A)

The meaning of a typical description (we omit here possible worlds, cf. (B)) is an *algorithmic computation* (Tichý: construction) of the form (so quite different from Russell's formalization):

$$\lambda x.\varphi(x)$$

for a given type τ of x and φ 's type $\tau \rightarrow o$, where o is a type interpreted as $\mathbb{B} = \{true, false\}$ (note the bivalence, i.e. no 3V-logic). Whether such an algorithmic computation is or isn't *abortive* (= partiality on the level of computations) does affect (i) *reference* (i.e. an individual, truth value, or some function-as-mapping), but not the natural language expression's having a (ii) *meaning* (which is identified with the computation).

The *labelled natural deduction in sequent style* ND_{TT*} (see Kuchyňka and the present author's 2024, elaborated from Tichý's early ideas) couples $\lambda x.\phi(x)$ e.g. with $\perp_\tau$ (which is an arbitrary abortive construction of type τ) into so-called *match* which is definitely satisfied or countersatisfied by an assignement. The use of matches with $\perp$ thus allows relatively easy deduction. (Especially if we compare it with *3V-approach* or *free logic* which must designate which total functions-as-mappings emulate which partial functions-as-mappings.)¹

(B)

As pointed out by Church (1951), Russell's TD cannot solve the *ITV problem* for it lacks tools that prevent undesirable substitutions and existential generalization from sentences whose ITV complements. (which may even fail to refer).

Montaguean ([1970] 1974) solution as adjusted by Tichý (1971,1988) solves ITV as showed below. Let ω (ranged over by variables such as w) be of type for *possible worlds*, and X_w be short for $X(w)$; the remaining types are obvious. Then

$$\lambda w.Seek_w(PonceDeLeon, \lambda w.\lambda x.BeFountainOfYouth_w(x))$$

¹ *Partial functions-as-mappings* of a certain type $\tau_1 \rightarrow \tau_2$ are also adopted in the approach. The functions lack a functional value (of type τ_2) for at least some of its arguments (of type τ_1). The 3V-approach, and even free logics must fill these missing values by *dummy values* $*_\tau$, and so they must place them already in the interpretatins of the respective types; thus, instead of e.g. truth functions above $\mathbb{B} = \{true, false\}$ they treat functions over $\mathbb{B}* = \mathbb{B} \cup \{*_\mathbb{B}\}$.

is a computation from which one cannot derive that $\lambda w.Exists_w(\lambda w.\lambda x.BeFountainOfYouth_w(x))$ since the *existential generalization rule* (see the present author’s 2022) doesn’t allow that for type-theoretic reasons. Likewise, one cannot substitute e.g. the *coreferential* computation (let’s suppose) ‘the brightest place x in Florida’ (see Kuchyňka and present author’s 2024 for the substitution rule).

(C)

As pointed out by Gödel (1944), Russell’s TD may avoid the *slingshot argument* (see e.g. Wikipedia for its terse (Perry’s) formulation), but Russell’s TD cannot handle (B), so we seek for different solution. Setting aside the meticulous treatment of type-theoretic restrictions of rules of substitution and ‘redistribution’ as well as modality and partiality, a collapse into Big Fact is deflected by pointing out that the *subject matter* of the sentences deployed in the slingshot argument are hyperintensional entites (viz. algorithmic computations), not denotata of possible world semantics.

References

- [1] Church, A. (1951): The Need for Abstract Entities in Semantic Analysis, In: *Proceedings of the American Academy of Arts and Sciences*, vol. 80: 100–113.
- [2] Gödel, K. (1944): Russell’s Mathematical Logic, In: Schilpp, P.A., (ed.), *The Philosophy of Bertrand Russell* (Library of Living Philosophers Volume 5) (ed.), Northwestern University, Evanston, 123–153.
- [3] Kuchyňka, P.; Raclavský, J. (2024): Completeness in Partial Type Theory. *Journal of Logic and Computation*. Oxford, UK: Oxford University Press, 34(1): 1–32.
- [4] Raclavský, J. (2020): *Belief Attitudes, Fine-Grained Hyperintensionality and Type-Theoretic Logic*. London: College Publications.
- [5] Raclavský, J. (2022): The Rule of Existential Generalisation and Explicit Substitution. *Logic and Logical Philosophy*. Nicolas Copernicus University Press, 31(1): 105–141.
- [6] Raclavský, J. (2024): Two Cases of Deduction with Non-referring Descriptions. In Indrzejczak, Andrzej; Zawidski, Michal. *EPTCS 415*. Sydney: Open Publishing Association, 48–65.
- [7] Russell, B. (1905): On Denoting. *Mind* 14(4): 479–493.
- [8] Tichý, P. (1988): *The Foundations of Frege’s Logic*, Walter de Gruyter.

Computability of creating codimension in the Hilbert cube pseudointerior

Luka Rak¹, Zvonko Iljazović²

^{1,2}*University of Zagreb, Faculty of Science, Department of Mathematics*

Bijenička cesta 30, 10000 Zagreb

E-mail: ¹luka.rak@math.hr, ²zvonko.iljazovic@math.hr

Keywords: Hilbert cube, computable boundary-preserving homeomorphism, computable compacta

The Hilbert cube Q is the Cartesian product of unit intervals $[-1, 1]$ endowed with the product metric $d(x, y) = \sup_i \{ \frac{1}{2^i} |x_i - y_i| \}$, that is the product space $[-1, 1]^{\mathbb{N}}$. Its geometric topology has some interesting properties that are not exhibited in its finite dimensional counterparts $[-1, 1]^n$. These unique properties seem to stem from the fact that infinite-dimensionality provides enough room to avoid obstructions. One of the fundamental results of this type is the property of creating codimension in one coordinate for the compacta in the pseudointerior. By setting the finite rational sequences as ideal points, Hilbert cube with the product metric is a computable metric space. We prove that the result above can be made computable in the following sense:

Theorem. Let s denote the *pseudointerior* of Q , i.e. $(-1, 1)^{\mathbb{N}}$, and B denote the *pseudoboundary*, i.e. $Q \setminus s$. For every computable compact set A in s , there is a computable homeomorphism $f : Q \rightarrow Q$ such that $f(B) = B$ and $p_1(f(A)) = \{0\}$, where p_1 is the projection on the first coordinate.

Acknowledgment

This research was supported by the European Union – NextGenerationEU through the National Recovery and Resilience Plan 2021–2026 Institutional grants of University of Zagreb Faculty of Science (PMF-CROFUND, IK IA 1.1.3. Impact4Math).

References

- [1] T. A. Chapman, Lectures on Hilbert cube manifolds, Regional Conference Series in Mathematics, No. 28, American Mathematical Society, Providence, RI, 1979.

idence, RI, 1976. Expository lectures from the CBMS Regional Conference held at Guilford College, October 11-15, 1975.

- [2] V. Brattka and G. Presser, *Computability on subsets of metric spaces*, Theoretical Computer Science 305, 43–76, 2003.
- [3] M.B. Pour-El and J.I. Richards, *Computability in Analysis and Physics*, Springer, Berlin, 1989.

From *-Autonomous to Linearly Distributive via Strengths and Enrichments

Luigi Santocanale¹, Gregory Chichery

¹*Aix-Marseille Université, CNRS, LIS*

Marseille, France

E-mail: luigi.santocanale@lis-lab.fr

Keywords:

*-autonomous categories, linearly distributive categories, monoidal strengths, enriched categories, skew monoidal categories.

A *-autonomous category [1] is a model of proofs of multiplicative classical linear logic; a linearly distributive category [2] is a model of proofs of the positive fragment of this logic. It is part of the folklore of category theory that every *-autonomous category is a linearly distributive category, with the par operation defined as $A \wp B := B^\perp \multimap A$. While this statement is immediate at the level of provability, a complete proof of this result — one in which the coherence conditions for the linear distributions are fully verified — has remained absent from the literature. In [2], the authors remark that the verification is “straightforward” but “the diagrams can be pretty horrid”, and leave the full check to the reader. The gap has propagated through subsequent work [3, 4], where the coherence conditions are acknowledged but remain unverified.

Beyond the mere need for a complete proof, any satisfactory mathematical modelling of proofs must engage with the coherence conditions themselves: what they express, where they originate, and why they inevitably hold. The goal of this talk is to present a full, conceptual proof of this result. The key idea is that the coherence conditions are not arbitrary diagram chases: they reduce to the existence of certain *strengths* for the par functor, which in turn follow systematically from the enriched structure of a biclosed monoidal category. This approach relies on the classical correspondence between strengths and enrichments [8, 5, 6, 9], further developed in the ongoing PhD thesis [13].

More precisely, let V be a monoidal biclosed category with left closure $- \otimes$ $Y \dashv Y \multimap -$ and right closure $X \otimes - \dashv - \multimap X$. For any object $0 \in V$, set $A^\perp := A \multimap 0$ and define the par $A \wp B := B \multimap A^\perp$. Recall that a skew monoidal category [11, 12] is like a monoidal category except that the associator

and unitors are not required to be invertible.

Theorem 1 *In any monoidal biclosed category V and for any object $0 \in V$, there exist canonical maps $\alpha^{\mathfrak{A}}, \lambda^{\mathfrak{A}}, \rho^{\mathfrak{A}}$ making $(V, \mathfrak{A}, 0)$ a skew monoidal category.*

A key structural observation is that V acts on itself on both sides, making it a *bimodule over itself* — or, in the terminology of [10], a *biactegory* — a category equipped with compatible left and right actions of a monoidal category. The theory of (bi)actegories, developed in [10], provides the relevant notions of (bi)strong functors and natural transformations, which are precisely what is needed to state and verify the coherence conditions.

An even deeper observation is that V^{op} is a V -bimodule, with left action $X \bullet A := X \multimap A$ and right action $A \bullet Y := A \multimap Y$.

The linear distributions

$$\delta^L : A \otimes (B \mathfrak{A} C) \rightarrow (A \otimes B) \mathfrak{A} C, \quad \delta^R : (A \mathfrak{A} B) \otimes C \rightarrow A \mathfrak{A} (B \otimes C)$$

are constructed as *composed strengths*: the strength of a composition of enriched functors, where the enrichment is that of V over itself. The coherence conditions — the interchange law and the strong naturality of $\alpha^{\mathfrak{A}}$ — then follow from general properties of strengths and natural transformations between enriched functors.

The $*$ -autonomous hypothesis enters only at the end: it makes the skew structural maps invertible, upgrading the skew monoidal structure to a genuine monoidal structure and yielding the main result:

Theorem 2 *Every $*$ -autonomous category [1] $(V, \otimes, I, 0)$ is a planar linearly distributive category [2] $(V, \otimes, \mathfrak{A})$ (planar meaning: without a symmetry assumption on either monoidal structure).*

In particular, the result applies beyond classical linear logic: since neither symmetry of $\otimes$ nor cyclicity of the dualizing object 0 is assumed, it covers fully non-commutative, non-cyclic settings such as the Lambek calculus.

In practice, most of the technical work amounts to recognizing that canonical maps such as

$$\begin{aligned} (X \otimes Y) \multimap Z &\simeq X \multimap (Y \multimap Z), & Z \multimap (X \otimes Y) &\simeq (Z \multimap X) \multimap Y, \\ X \multimap (Y \multimap Z) &\simeq (X \multimap Y) \multimap Z, \\ X \otimes (Y \multimap Z) &\rightarrow Y \multimap (X \otimes Z), \\ X^\perp \otimes Y &\rightarrow (X \multimap Y)^\perp \end{aligned}$$

are each the strength of some specific functor. The fundamental role of strength conditions in logic is well documented: it underlies the fixed-point elimination results of [14] and can be traced back to Peirce’s iteration rule for existential graphs of type Alpha [15]. The logician should therefore not be surprised to find strengths as the key ingredient of the present work.

Acknowledgment

This work is supported by the ANR project RECIPROG (ANR-21-CE48-0019) and by PEPR EPIQ – Technologies Quantiques (AMIDEX).

References

- [1] Barr, M., *Non-symmetric *-autonomous categories*, Theoret. Comput. Sci. **139** (1995), 115–130.
- [2] Cockett, J.R.B., Seely, R.A.G., *Weakly Distributive Categories*, J. Pure Appl. Algebra **114** (1997), 133–173.
- [3] Cockett, J.R.B., Koslowski, J., Seely, R.A.G., *Introduction to Linear Bicategories*, Math. Struct. Comput. Sci. **10** (2000), 165–203.
- [4] Blute, R., Kuzman-Blais, R., Niefield, S., *Constructing Linear Bicategories*, arXiv:2209.05693, 2026.
- [5] Gordon, R., Power, A.J., *Enrichment through Variation*, J. Pure Appl. Algebra **120** (1997), 167–185.
- [6] Janelidze, G., Kelly, G.M., *A Note on Actions of a Monoidal Category*, Theory Appl. Categ. **9** (2001), 61–91.
- [7] Kelly, G.M., *Basic Concepts of Enriched Category Theory*, Reprints in Theory Appl. Categ. (2005).
- [8] Kock, A., *Monads on Symmetric Monoidal Closed Categories*, Arch. Math. **21** (1970), 1–10.
- [9] Ratkovic, K.S., *Morita Theory in Enriched Context*, arXiv:1302.2774, 2013.
- [10] Capucci, M., Gavranović, B., *Actegories for the Working Mathematician*, arXiv:2203.16351, 2024.
- [11] Szlachányi, K., *Skew-monoidal Categories and Bialgebroids*, Adv. Math. **231** (2012), 1694–1730.
- [12] Uustalu, T., Veltri, N., Zeilberger, N., *The Sequent Calculus of Skew Monoidal Categories*, Electron. Notes Theor. Comput. Sci. **341** (2018), 345–370.
- [13] Chichery, G., *Enriched Semantics of Linear Logic*, PhD thesis, Aix-Marseille Université, in preparation.
- [14] Ghilardi, S., Gouveia, M.J., Santocanale, L., *Fixed-point Elimination in the Intuitionistic Propositional Calculus*, ACM Trans. Comput. Logic **21** (2020), 1–37.
- [15] Dau, F., *Some Notes on Proofs with Alpha Graphs*, in: Conceptual Structures: Inspiration and Application, Lect. Notes Comput. Sci. **4068**, Springer, 2006, pp. 172–188.

Explorations in Infinitary Action Logic

Andre Scedrov

University of Pennsylvania

Infinitary action logic ACT_ω [3] is an infinitary substructural logic with product and two residuals, lattice operations, constants 0 and 1, and Kleene star. Infinitary action logic axiomatizes the equational theory of $*$ -continuous action lattices. Natural examples of these algebraic structures are algebras of formal languages and algebras of binary relations. It follows from the work of Kozen [5] that derivability from hypotheses in ACT_ω is $\prod_1^1$ -complete. Buszkowski and Palka proved that theoremhood in ACT_ω is $\prod_1^0$ -complete [3]. For the equational theories of the two specific classes of action lattices mentioned above, Buszkowski proved $\prod_1^0$ lower complexity bounds and left the exact complexity estimation an open question [2]. In recent joint work with Max Kanovich and Stepan L. Kuznetsov [4], we prove that in fact these theories have a significantly higher algorithmic complexity, namely, that they are $\prod_1^1$ -complete. To show this, we consider the product-free fragment of ACT_ω , where there are no product and join, no constants, and Kleene star is replaced by so-called iterative divisions: $A * \setminus B$ and $B / A *$, introduced by Sedlár [8] (in the non-associative setting) and by Kuznetsov and Ryzhkova [7] (in the associative setting considered here). Unlike ACT_ω itself, this fragment is strongly complete w.r.t. the classes of models on formal languages and on binary relations [6]. For this fragment, we strengthen the method of Kozen [5] to prove $\prod_1^1$ -completeness of derivability from hypotheses [4]. The strengthening is carried out by an infinitary version of a technique of Buszkowski [1]. Then we combine this with novel constructions with constants 0 and 1, which allow simulating entailment from finite sets of hypotheses in the classes of models on formal languages and on binary relations. This enables a semantical version of deduction theorem and hence allows reducing entailment to validity in the two classes of models. For the theories in the full language, we also prove the $\prod_1^1$ upper bound [4].

References

- [1] Wojciech Buszkowski: Some decision problems in the theory of syntactic categories, *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, vol. 28 (1982), pp. 539–548.
- [2] Wojciech Buszkowski: On the complexity of the equational theory of relational action algebras. In: R.A. Schmidt (ed.) *Relations and Kleene Algebra*

- in Computer Science. RelMiCS 2006. Lecture Notes in Computer Science, vol. 4136, pp. 106–119. Springer (2006).
- [3] Wojciech Buszkowski, Ewa Palka: Infinitary action logic: complexity, models and grammars, *Studia Logica*, vol. 89 (2008), no. 1, pp. 1–18.
 - [4] Max Kanovich, Stepan L. Kuznetsov, Andre Scedrov: Complexity of equational theories for relational and language action lattices, In: U. Fahrenberg, W. Fussner, L. Santocanale, (eds.) *Relational and Algebraic Methods in Computer Science. RAMICS 2026*. Lecture Notes in Computer Science, vol. 16526, pp. 208–228. Springer, Cham (2026).
 - [5] Dexter Kozen: On the complexity of reasoning in Kleene algebra, *Information and Computation*, vol. 179 (2002), pp. 152–162.
 - [6] Stepan L. Kuznetsov: Strong conservativity and completeness for fragments of infinitary action logic, *Siberian Electronic Mathematical Reports*, vol. 21 (2024), no. 2, pp. 789–809.
 - [7] Stepan L. Kuznetsov, Nadezhda S. Ryzhkova: A restricted fragment of the Lambek calculus with iteration and intersection operations. *Algebra and Logic* 59(2), 129–146 (2020).
 - [8] Igor Sedlár: Iterative division in the distributive full non-associative Lambek calculus. In: L. Soares Barbosa, A. Baltag (eds.) *Dynamic Logic. New Trends and Applications. DaLí 2019*. Lecture Notes in Computer Science, vol. 12005, pp. 141–154. Springer (2020).

Modern tools for arithmetical completeness: provability models and proofs

Borja Sierra Miranda

Universität Bern

Institut für Informatik

E-mail: borja.sierra@unibe.ch

Provability logic is the branch of mathematical logic that studies the notion of proof and provability through the lenses of modal logic. The idea is to interpret the usual box modality $\Box$ as provability inside an arithmetical theory. Then, one of the main problems in the area is, given a theory T , to determine which is the modal logic corresponding to its provability predicate.

The cornerstone result in the area came from Solovay [3], which showed that, for PA (Peano Arithmetic), the answer is GL (Gödel Löb logic). His proof can be divided in two steps:

1. Find a “simple” class $\mathcal{M}$ of Kripke models such that GL is complete with respect to it.
2. Embed this class of models inside the desired arithmetical theory, thus showing that if a formula is refutable in the modal logic, its arithmetical interpretation is also refutable.

However, as it is well known, some provability logics are Kripke incomplete (such as ER or GLP) while others, being Kripke complete, lack a “simple” class that can be embedded in arithmetic via known methods (such as some intuitionistic provability logics).

Mojtahedi in [1] defined a new semantics, now called provability models, for intuitionistic modal logic to amend this problem. Then he used these models to characterize the provability logic of HA (Heyting Arithmetic). In later work [2], we developed these models in the classical setting with the following purposes in mind.

1. Understanding better the notion of provability models. In [1] provability models served mainly a technical purpose. In [2] we hope to prove that they constitute a research topic in their own right.
2. Show that they provide a natural semantics for the family of provability logics and their variants such as interpretability logic.

3. Provide an alternative semantics for known Kripke incomplete provability logics such as GLP.

In this talk, we will give a brief introduction to these models in the classical setting. Additionally, if time allows, we will further discuss a new approach to proving arithmetical completeness that replaces the use of semantics with the use of a sequent calculus instead.

References

- [1] M. Mojtahedi. On the Provability Logic of HA, 2026. URL <https://arxiv.org/abs/2206.00445>.
- [2] M. Mojtahedi and B. Sierra Miranda. Provability Models, 2025. URL <https://arxiv.org/abs/2510.06696>.
- [3] R. M. Solovay. Provability interpretations of modal logic. Israel Journal of Mathematics, 25:287–304, 1976. doi: 10.1007/BF02757006.

Interpolation via Generalized Splitting

Lutz Straßburger

Inria & LIX, Ecole Polytechnique, IP Paris

Palaiseau, France

Webpage: <https://www.lix.polytechnique.fr/Labo/Lutz.Straßburger/>

Keywords: Interpolation, deep inference, cut elimination

Given an implication $A \rightarrow B$, the interpolation theorem by Craig [2] says that there is a formula C , called the *interpolant*, such that the two implications $A \rightarrow C$ and $C \rightarrow B$ hold, and furthermore, the language of C is contained in the intersection of the languages of A and B . A stronger form of this result is Lyndon interpolation [6], which also demands that the propositional symbols appearing in C must have the same polarity as in A and B , i.e., if they occur negated in C , then they also must occur negated in A and in B .

Interpolation has been studied for various logics, including classical first-order logic [2, 6], intuitionistic and intermediate logics [5], various modal logics [3], and also linear logic [8, 9, 10].

A common way to prove an interpolation result for a logic is to use Maehara's method [7], which surgically extracts the interpolant from a cut-free sequent proof of $A \vdash B$.

Recently Saurin [9] strengthened this method to a proof relevant cut-introduction. I.e., given a proof π of $A \vdash B$, the interpolant C comes with two proofs π_1 of $A \vdash C$ and π_2 of $C \vdash B$, such that eliminating the cut from

$$\text{cut} \frac{\begin{array}{c} \triangleleft \pi_1 \\ A \vdash C \end{array} \quad \begin{array}{c} \triangleright \pi_2 \\ C \vdash B \end{array}}{A \vdash B}$$

yields exactly π .

In this talk, I will (i) strengthen Saurin's result using a deep inference formulation, and (ii) propose an alternative proof method for obtaining the interpolation theorem, which is not based on the sequent calculus, but on deep inference. More precisely, our main theorem is the following:

Theorem 1 *Every derivation $\delta \parallel s$ can be decomposed into*

A	A
$\delta_1 \parallel s \uparrow$	$\delta_1 \parallel s \uparrow$
C	C
$\delta_2 \parallel s \downarrow$	$\delta_2 \parallel s \downarrow$
B	B

for some C .

A
Here, $\delta \parallel s$ stands for a derivation δ with premise A and conclusion B , in which
 B

all inference rules come from the proof system S . As in a deep inference system, every inference rule is single premise, this is well-defined. Furthermore, a typical deep inference proof system S is divided into a *down-fragment*, here denoted by $S\downarrow$, and an *up-fragment*, denoted by $S\uparrow$. The rules in the down-fragment correspond to the rules in a cut-free sequent calculus, and the rules in the up-fragment correspond to the cut in the sequent calculus. However, in a deep inference system, there is a perfect up-down duality between these two fragments. And Theorem 1 above says that they can be separated in a derivation.

Since the rules in the down-fragment cannot create new propositional variables while going up in a derivation, and dually, the up-rules cannot create new propositional variables while going down in a derivation, it follows immediately, that the formula C in Theorem 1 must be a Lyndon interpolant.

Corollary 2 *A logic with a proof system S obeying Theorem 1 has Lyndon interpolation.*

Let us now address the question of how we can prove Theorem 1. In [10], there is a proof for the multiplicative and exponential fragments of linear logic (MLL and MELL) based on rule permutations. But as already observed in [10], that proof does not scale to other logics.

In deep inference, the standard method for proving cut elimination is via the *Splitting Lemma*. Since Theorem 1 can be seen as a generalization of cut elimination, it might come as no surprise that its proof is based on a generalisation of the Splitting Lemma. For classical logic, this lemma is formulated as follows, where SKS is the standard system for classical logic in deep inference [1], and SKS_c is the core fragment, i.e., the one with contraction and weakening (and medial) removed:

Lemma 3 (Generalized Splitting) *1. If there is a derivation $\frac{I}{\delta \parallel SKS_c \downarrow}, K \vee (A \wedge B)$*

then there is a context $C[\cdot]$ and formulas K_A, K_B, I_A, I_B , such that

$$\frac{I}{\delta_I \parallel SKS_c \uparrow} \quad \text{and} \quad \frac{C[K_A \vee K_B]}{\delta_K \parallel SKS_c \downarrow} \quad \text{and} \quad \frac{I_A}{\delta_A \parallel SKS_c \downarrow} \quad \text{and} \quad \frac{I_B}{\delta_B \parallel SKS_c \downarrow} \quad .$$

$$\frac{C[I_A \wedge I_B]}{K_A \vee A} \quad \text{and} \quad \frac{C[K_B \vee B]}{K_B \vee B} \quad .$$

2. If there is a derivation $\frac{I}{\delta \parallel SKS_c \downarrow}$, where a is an atom, then there is a context $K \vee a$

$C[\cdot]$, such that either

$$(a) \quad \frac{I}{\delta_I \parallel SKS_c \uparrow} \quad \text{and} \quad \frac{C[\bar{a}]}{\delta_K \parallel SKS_c \downarrow} \quad \text{or} \quad (b) \quad \frac{I}{\delta_I \parallel SKS_c \uparrow} \quad \text{and} \quad \frac{C[\perp]}{\delta_K \parallel SKS_c \downarrow}$$

$$\frac{C[\top]}{K} \quad \text{and} \quad \frac{C[a]}{K} \quad .$$

We have the same lemma also for the deep inference system for full linear logic [10], where the first statement has to be formulated for every connective separately. This generalized splitting lemma now allows us to prove the *Flipping Lemma*:

Lemma 4 (Flipping) *If*
$$\begin{array}{c} H \\ \delta_1 \parallel \text{SKS}_c \uparrow \\ I \end{array}$$
 then there is a derivation
$$\begin{array}{c} H \wedge \bar{A} \\ \theta_1 \parallel \text{SKS}_c \uparrow \\ J \\ \delta_2 \parallel \text{SKS}_c \downarrow \\ K \vee A \end{array}$$
 for some
$$\begin{array}{c} K \end{array}$$

This lemma allows us to prove Theorem 1.

So far, we have this result for classical propositional logic, full propositional linear logic, and the modal logics K, KT, K4, and S4 (details can be found at <https://arxiv.org/abs/2607.23798>). First-order logic is work in progress. Another interesting question might be under which conditions we can obtain a Flipping Lemma, which is the main ingredient to the proof of Theorem 1.

References

- [1] Kai Brännler and Alwen Fernanto Tiu. A local system for classical logic. In *LPAR 2001*, volume 2250 of *LNAI*, pages 347–361. Springer, 2001.
- [2] W. Craig. Linear reasoning: A new form of the Herbrand-Gentzen theorem. *The Journal of Symbolic Logic*, 22:250–268, 1957.
- [3] Melvin Fitting and Roman Kuznets. Modal interpolation via nested sequents. *Ann. Pure Appl. Logic*, 166(3):274–305, 2015.
- [4] Alessio Guglielmi and Lutz Straßburger. Non-commutativity and MELL in the calculus of structures. In *CSL 2001*, volume 2142 of *LNCS*, pages 54–68. Springer-Verlag, 2001.
- [5] Roman Kuznets and Björn Lellmann. Interpolation for intermediate logics via injective nested sequents. *Journal of Logic and Computation*, 31(3):797–831, 04 2021. doi:10.1093/logcom/exab015.
- [6] Roger C. Lyndon. An interpolation theorem in the predicate calculus. 1959. URL: <https://doi.org/10.2140/pjm.1959.9.129>.
- [7] Shoji Maehara. On the interpolation theorem of craig. *Sûgaku*, 12(4), 1960.
- [8] Dirk Roorda. Interpolation in fragments of classical linear logic. *Journal of Symbolic Logic*, 59(2):419–444, 1994. doi:10.2307/2275398.
- [9] Alexis Saurin. Interpolation as Cut-Introduction: On the Computational Content of Craig-Lyndon Interpolation. In *FSCD 2025*, volume 337 of *LIPICs*, pages 32:1–32:21, Dagstuhl, 2025. doi:10.4230/LIPICs.FSCD.2025.32.
- [10] Lutz Straßburger. *Linear Logic and Noncommutativity in the Calculus of Structures*. PhD thesis, Technische Universität Dresden, 2003.
- [11] Andrea Aler Tubella and Lutz Straßburger. Introduction to deep inference. Lecture notes for ESSLLI’19, 2019. URL: <https://hal.inria.fr/hal-02390267>.

Abstract Socratic dialogue and dialectical logic

Teo Šestak ¹

¹*Faculty of Mechanical Engineering and Naval Architecture, University of Zagreb*

Ulica Ivana Lučića 5, Zagreb, Croatia

E-mail: ¹`teo.sestak@fsb.unizg.hr`

Keywords:

Modal logic, dialectical logic, Socratic elenchus, Socratic dialogues, dialectics.

The Socratic dialogue is traditionally understood as a method of philosophical inquiry in which claims are tested through structured questioning, exposing tensions, inconsistencies, and unexamined commitments. Following Vlastos' [5] reconstruction of the Socratic dialogue, we view dialectical inquiry as a process in which an interlocutor's beliefs are examined and shown to conflict with the claim they initially put forward.

The central idea of this talk is to abstract from this and to regard arguments not as static collections of propositions but as dynamic configurations of commitments subject to challenge, revision, and reconciliation, but motivated by the structure of the Socratic dialogue.

Instead of representing commitments as elements successively added to a set, we consider abstract information states $W = \{w, u, v, \dots\}$, related via a binary relation R , which models Socrates' questioning as a transition between information states. Additionally, we consider a ternary relation S , which models Socrates' argumentation and captures his ability to force a transition to a particular information state.

This structure resembles a Kripke frame and naturally motivates a modal-logical treatment of dialectics. We, therefore, treat dialectical contradiction as a modal operator. The idea is that φ dialectically contradicts ψ when every outcome of Socratic questioning that preserves φ provides a line of argumentation leading to the refutation of ψ . We introduce a logical system **DiaL**, in which such contradictions can be formally expressed and analysed. We further show that several familiar modal systems – including normal modal logics and interpretability logics – arise naturally as extensions of **DiaL**.

The resulting framework provides a unified modal perspective on dialectical reasoning and opens a route toward the formal comparison of diverse dialectical traditions, including those of Aristotle [4], Hegel [2], and Marx [3].

Acknowledgments

This work is supported by Croatian Science Foundation under the project HRZZ-IP-2024-05-3882.

References

- [1] Cooper, J. M., *Plato: Complete Works*, Hackett Publishing Company, Indianapolis (1997).
- [2] Hegel, G. W. F., *Hegel's Science of Logic*, tr. A. Miller, London: Allen and Unwin (1969).
- [3] Marx, K., Engels F., *The German Ideology*, in: Marx, K. & Engels, F., *Marx/Engels Collected Works, Vol. 5*, International Publishers. pp. 19–581 (1975).
- [4] Pickard-Cambridge, W. A., *Topics*, in: Barnes, J., *Complete Works of Aristotle, Volume 1: The Revised Oxford Translation*, Princeton University Press (1984).
- [5] Vlastos, G., *The Socratic Elenchus*, Oxford Studies in Ancient Philosophy 1: 27–58 (1983).

Proof of Church-Turing Thesis

Zvonimir Šikić

CLDT, University of Rijeka

During the 20th century, most of the great logicians gave their own definitions of an algorithm (a mechanical procedure). These were the Gödel/Herbrand/Kleene recursive functions, Turing machines, Post systems, Church's λ -calculus, Schönfinkel's combinatory logic, and Smullyan's systems. All these definitions are mutually equivalent. This makes plausible the Church-Turing thesis that each system accurately describes the intuitive notion of a computable function. The prevailing opinion is that it is not provable, because it identifies formally defined systems with an intuitive notion; cf. [1], [5] and [2]. But in accordance with [3] (but also, and unexpectedly, with [1] and [5]), we will define computability logically, and this will enable us to prove Church-Turing thesis as a simple corollary of Gödel's completeness theorem.

References

- [1] Church, A. An unsolvable problem in elementary number theory, American Journal of Mathematics 58, 345-363, 1936.
- [2] Kleene, S. C. Introduction to Metamathematics, Princeton, D. van Nostrand, 1952.
- [3] Kripke, S. The Church-Turing thesis as a special corollary of Gödel's completeness theorem, in J. Copeland, C. Posy and O. Shagrir, eds., Computability: Turing, Gödel, Church and Beyond, Cambridge, MA: MIT Press, 77-104, 2013.
- [4] Smullyan, R. M. Theory of formal systems. Princeton UP, 1961.
- [5] Turing, A. On computable numbers, with an application to the Entscheidungsproblem, Proceedings of the London Mathematical Society (Series 2) 42, 1936.

Logic and Intelligence

Carolyn Talcott

SRI

Menlo Park, CA, USA

E-mail: carolyn.talcott@gmail.com,

Keywords: intelligence, logic, reasoning.

With all the interest in Artificial Intelligence, it seems interesting to understand (Natural) Intelligence, particularly the mechanisms that give rise to different forms of intelligence. It is also interesting to consider features of a logical system that could model and/or exhibit features of intelligence. In this talk we will review the features of and mechanisms underlying intelligence at different stages of development, base on work of Max Bennet [1]. We will discuss features of two logical systems in the context of intelligence mechanisms. The FOL logical system was developed at the Stanford AI Lab. FOL was motivated by understanding intelligence and the challenge of building computer individuals that exhibited features of intelligence [3]. Rewriting Logic and its realization in the Maude system is a logic for representing and reasoning about transistions in distributed systems or in proof search [2].

Acknowledgment

The research reported in the talk was partly supported by DARPA, ONR, NSF.

References

- [1] Max S. Bennet. *A Brief History of Intelligence: Evolution, AI, and the Five Breakthroughs That Made Our Brains*. Mariner Books, October 24, 2023.
- [2] José Meseguer. *Capturing System Designs with Formal Executable Specifications*. FASE 2025: 1-32,
- [3] Richard W. Weyrauch. *Prolegomena to a theory of mechanized formal reasoning*. Artificial Intelligence, 13:133-170, 1980.

A Probabilistic-Logical Extension of the WOOP/MCII Method

Milica Vučićević¹, Angelina Ilić Stepić²,
Nenad Stojanović³

^{1,3}*Faculty of Science, University of Kragujevac
Radoja Domanovića 12, Kragujevac, Serbia*

²*Mathematical Institute of the Serbian Academy of Sciences and Arts
Kneza Mihaila 36, Belgrade, Serbia*

E-mail: ¹milica.vucicevic@pmf.kg.ac.rs, ²angelina@mi.sanu.ac.rs,
³nenad.stojanovic@pmf.kg.ac.rs

Keywords:

probabilistic logic, conditional probability, WOOP, MCII

WOOP is a practical self-regulation strategy based on the MCII framework (Mental Contrasting with Implementation Intentions). This approach is based on the idea that a desired future is mentally contrasted with the present reality that stands in the way of its realization, after which a concrete if-then plan is formulated in order to overcome the obstacle. In its practical form, WOOP guides a person through four steps: Wish, Outcome, Obstacle, and Plan.

In this paper, we propose a probabilistic-logical framework for the formal representation of this method. We start from the fact that the WOOP/MCII method already relies on reasoning about wishes, possible outcomes, obstacles, and if-then plans. The proposed formal language is intended to distinguish between two types of assessments: the intensity of a wish and the subjective conditional probability that an obstacle will be overcome when it occurs and when an appropriate plan has been formulated for it. The main idea is to extend the WOOP method by adding a probabilistic component: in addition to the basic structure Wish–Outcome–Obstacle–Plan, we introduce an assessment of the effectiveness of the plan in overcoming the obstacle.

We introduce two types of operators. The operator $Int_{\geq r}$ will be used to express the intensity of a wish, while the operator $CP_{\geq r}$ will express subjective conditional probability. The syntax of the proposed language will be introduced and the corresponding semantics will be given. We will also consider the possibility of formulating WOOP/MCII principles in the form of axioms, as well as the soundness, completeness, and decidability of the system.

References

- [1] Gollwitzer, P. M. *Implementation intentions: Strong effects of simple plans*, American psychologist, 1999.
- [2] Ognjanović, Z., Ikodinović, N. A LOGIC WITH HIGHER ORDER CONDITIONAL PROBABILITIES, Publications de l'Institut Mathematique, 2007.
- [3] Oettingen, G., Pak, H. J., Schnetter, K. *Self-regulation of goal-setting: Turning free fantasies about the future into binding goals*, Journal of personality and social psychology, 2001.
- [4] Rašković, M., Marković, Z., Ognjanović, Z. *A logic with approximate conditional probabilities that can model default reasoning*, International Journal of Approximate Reasoning, 2008.
- [5] Sailer, P., Wieber, F., Pröpster, K., Stoewer, S., Nischk, D., Volk, F., Odenwald, M. *A brief intervention to improve exercising in patients with schizophrenia: a controlled pilot study with mental contrasting and implementation intentions (MCII)*, BMC psychiatry, 2015.

Rebasing Social Choice Functions

Marcel Maretić

*Faculty of Organization and Informatics
University of Zagreb*

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