13$^{\text{TH}}$ INTERNATIONAL CONFERENCE

Logic and Applications

LAP 2024

September 23 - 27, 2024
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 13th International Conference on Logic and Applications - LAP 2024, held as a hybrid meeting hosted by the Inter University Center Dubrovnik, Croatia, September 23 - 27, 2024.

LaTeX book of abstracts preparation and typesetting:

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

LAP 2024 Web site: `https://lap.math.hr/LAP2024/` Maintained by Marko Horvat, University of Zagreb, and Simona Prokić, University of Novi Sad.

Contents

Logicism and the Philosophy of Mathematics

Tin Adlešić [1]

[1] *University of Zagreb, Faculty of Chemical Engineering and Technology*
Trg Marka Marulića 19

E-mail: [1]tadelsic@fkit.unizg.hr

Keywords:
Logicism, Philosophy of Mathematics, Mathematical Logic

Logicism is a philosophical standpoint that mathematics can be reduced to logic. It came into prominence in the works of Gottlob Frege and was later significantly modified by Bertrand Russell. Russell's version of logicism can be best seen in *Principia Mathematica*, written in collaboration with Alfred Whitehead. Even though *Principia Mathematica* was very influential, it did not provide a satisfactory defense of logicism. At the end of the 20th century, a modern version of logicism emerged, called *neologicism*.

In this talk, we will give a short historical survey of logicism and put forward a new view on its role in the philosophy of mathematics.

References

[1] Frege, G. *Begriffsschrift, a formula language, modeled upon that of arithmetic.* in van Heijenoort (ed.): *From Frege to Gödel: A source book in mathematical logic 1897–1931*, pp. 1–82. Harvard University Press, 1967.

[2] Frege, G. *Osnove aritmetike i drugi spisi.* Kruzak, 1995.

[3] Hale, B. and Wright, C. *Logicism in the Twenty-first Century.* in Shapiro (ed.): *The Oxford Handbook of Philosophy of Mathematics and Logic*, pp. 166–202. Oxford University Press, 2005.

[4] Whitehead, A. and Russell, B. *Principia Mathematica.* Cambridge University Press, 1910, 1912, 1913.

Semicomputable irreducible continua

Tea Arvaj[1]**, Zvonko Iljazović**[2]

[1] *University of Zagreb, Faculty of Electrical Engineering and Computing*
Unska 3, Zagreb
[2] *University of Zagreb, Faculty of Science, Department of Mathematics*
Bijenička cesta 30, Zagreb
E-mail: [1]`tarvaj@fer.hr`, [2]`zilj@math.hr`

Keywords:
Computable metric space, computable set, semicomputable set, irreducible continuum.

A topological pair (A, B) of space A and its subspace B is said to have computable type if, whenever $f : A \to X$ is an embedding of A in a computable metric space such that $f(A)$ and $f(B)$ are semicomputable, then $f(A)$ is computable.

It is known that $([0, 1], \{0, 1\})$ has computable type. In other words, an arc together with its endpoints has computable type.

However, it is known that a more general result holds:
if K is a continuum chainable from a to b, then $(K, \{a, b\})$ has computable type. That a continuum (i.e. a connected and compact metric space) K is chainable from a to b means that for every $\varepsilon > 0$ there exist finitely many open sets $C_0, \ldots, C_n$ in K whose diameters are less than ε, which cover K, such that $a \in C_0$, $b \in C_n$, and $C_i \cap C_j = \emptyset$ iff $|i - j| > 1$.

If A is an arc with endpoints a and b, then A is a continuum chainable from a to b. On the other hand, a continuum K chainable from a to b need not be an arc (for example topologist's sine curve).

In this talk we examine more general spaces, namely irreducible continua. A continuum K is irreducible between a and b, where $a, b \in K$, if there exist no proper sobcontinua of K that contain both a and b.

We have the following result.

Theorem 1. *Let K be a continuum irreducible between a and b. Then the pair $(K, \{a, b\})$ has computable type.*

It is known that every computable set contains a dense subset of computable points. So a question naturally arises: if K is a semicomputable continuum irreducible between a and b, where a and b are not necesserily computable (then

K is also not necessarily computable), does K contain at least one computable point.

Answer to that question is affirmative in the case when K is an arc, which is shown in [4].

We show that the previuos result also holds for irreducible continua, with an additional assumption that the continuum K can be shown as a union of its three proper subcontinua such that no two of them cover K. Furthermore, in that case K not only contains a computable point, but contains a computably enumerable subset with non-empty interior in K.

References

[1] D.E. Amir and M. Hoyrup. "Strong computable type". In: *Comput.* 12 (2022), pp. 227–269.

[2] C.O. Christenson and W.L. Voxman. *Aspects of Topology.* Marcel Dekker, Inc., New York, 1977.

[3] E. Č ičković, Z. Iljazović, and L. Validžić. "Chainable and circularly chainable semicomputable sets in computable topological spaces". In: *Archive for Mathematical Logic* 58 (2019), pp. 885–897.

[4] Z. Iljazović. "Chainable and Circularly Chainable Co-c.e. Sets in Computable Metric Spaces". In: *Journal of Universal Computer Science* 15.6 (2009), pp. 1206–1235.

Time-Bounded Resilience: Formalization, Computational Complexity and Implementation

Tajana Ban Kirigin[1], Jesse Comer[2], Max Kanovich[3] Andre Scedrov[2], Carolyn Talcott[4]

[1] *University of Rijeka, Faculty of Mathematics, Rijeka, Croatia*

[2] *University of Pennsylvania, Philadelphia, PA, USA*

[3] *University College London, London, UK*

[4] *SRI International, Menlo Park, CA, USA*

Keywords: Resilience, Computational Complexity, Cyber-Physical Systems, Multiset Rewriting

Most research on formal system design has focused on optimizing various measures of *efficiency*. However, not enough attention has been paid to the design of systems optimizing *resilience*, that is, the ability of systems to adapt to unexpected changes or adversarial disruptions. In our previous work [1], we formalized the intuitive notion of resilience as a property of cyber-physical systems. We used a multiset rewriting language with explicit time that is suitable for the specification and verification of various goal-oriented systems.

A primary challenge in [1] was to formalize the disruptions against which systems must be resilient. This was accomplished by separating the system from the environment and distinguishing between rules applied by the system and rules imposed on the system, such as changes in conditions, regulations, or mission objectives. Although the related verification problems are undecidable in general, it was shown that these problems are PSPACE-complete for the class of *balanced* systems, in which facts are of bounded size, and the rewrite rules do not change the configuration size.

In this work, we consider the *time-bounded* version of the resilience problems, with the intuition that a resilient system can fulfil its tasks within the given time bounds. Time-bounded resilience is motivated by bounded model checking and automated experiments, which can help system designers verify properties and find counterexamples where their specifications do not satisfy time-bounded resilience. Moreover, bounded versions of resilience problems arise naturally when the missions of the systems being modeled are necessarily bounded at some level.

In particular, we focus on progressing planning scenarios, where, only a bounded number of rules can be applied in a single time step. We study the computational complexity of *time-bounded* resilience problems for the class of η-simple progressing planning scenarios (PPS), for which it is simple to check whether a system configuration is critical. We show that, in the time-bounded model with n (potentially adversarially chosen) updates, the corresponding time-bounded resilience problem for the class of η-simple PPSs is complete for the $\Sigma_{2n+1}^{\mathsf{P}}$ class of the polynomial hierarchy, PH [2]. To support the formal models and complexity results, we perform automated experiments for time-bounded verification using the rewriting logic tool Maude.

References

[1] M. A. Alturki, T. Ban Kirigin, M. Kanovich, V. Nigam, A. Scedrov, and C. Talcott. On the formalization and computational complexity of resilience problems for cyber-physical systems. In *Theoretical Aspects of Computing–ICTAC 2022: 19th International Colloquium, Tbilisi, Georgia, September 27–29, 2022, Proceedings*, pages 96–113. Springer, 2022.

[2] T. Ban Kirigin, J. Comer, M. Kanovich, A. Scedrov, and C. Talcott. Time-Bounded Resilience. In *15th International Workshop on Rewriting Logic and its Applications (WRLA)*, Luxembourg, April 6-7, 2024, Springer Lecture Notes in Computer Science, to appear.

[3] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Timed multiset rewriting and the verification of time-sensitive distributed systems. In *14th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS)*, 2016.

[4] M. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, and C. Talcott. On the complexity of verification of time-sensitive distributed systems. In D. Dougherty, J. Meseguer, S. A. Mödersheim, and P. Rowe, eds., *Protocols, Strands, and Logic.* Springer LNCS Volume 13066, Springer-Verlag, pp. 251 - 275. First Online 19 November 2021.

On feasibility in non-standard Heyting arithmetic

Péter Battyányi [1]

[1] *University of Debrecen, Faculty of Informatics, Department of Computer Science*
Kassai út 26., 4028 Debrecen, Hungary
E-mail: [1]battyanyi.peter@inf.unideb.hu

Keywords:
Heyting arithmetic, non-standard arithmetic, realizability, feasibility

As early as in 1934, Skolem [8] proved that, if we add the axioms $\underline{n} < c$ ($n \in \mathbb{N}$) to first-order arithmetic, in other words, if we demand the existence of an infinite number, then the resulting theory is consistent [4, 5]. We examine Heyting arithmetic [3, 9], that is, first-order arithmetic with intuitionistic predicate logic, augmented with these axioms of non-standardness together with a predicate expressing the property of being feasible. We define feasibility following [2]: the property of feasibility is a downward closed property, where 0 is feasible, and, for all primitive recursive functions, if the arguments are feasible, then the result should be feasible. Furthermore, the infinite number c is not feasible.

The overspill principle, due to Robinson, for non-standard Peano arithmetic states that we are not able to define a proper cut of a model of Peano arithmetic with an arithmetic formula [5]. In our case, we prove that F, however, defines the proper cut of standard elements. Of course, F does not belong to the original language. A theory admits the disjunction property, if, whenever $A \vee B$ is derivable for the closed formula $A \vee B$, then either A or B is derivable. Similarly, we say that for a theory the existential property fulfills, if, whenever $\exists x A(x)$ is derivable for the closed formula $\exists x A(x)$, then $A(t)$ is derivable for some closed term t. Constructive, non-standard theories may refute both properties [1, 7]. One of the reasons is that they usually require the fulfillment of axioms other than the ones considered in this paper, for example transfer principles [1]. However, we have deliberately chosen the simplest axioms that could possibly be more defendable from a constructive standpoint. As a result of this, our theory preserves both the disjunction and the existential properties. Formally, the notion of a feasible term can be defined as follows:

1. $F(0)$,
2. $\forall x \forall y (F(x) \wedge y < x \supset F(y))$,

3. $\forall x(F(x) \supset x < c)$,
4. $\forall x_1 ... \forall x_n(F(x_1) \wedge ... \wedge F(x_n) \supset F(g(x_1, ..., x_n)))$, for each symbol g standing for a primitive recursive function.

Furthermore, we accomplish slight modifications to the predicate calculus of intuitionistic first-order logic to facilitate the treatment of feasibility in our theory. Basically, we state that all of our newly introduced terms should be feasible. Then we consider the following version of induction

$$A(0) \wedge \forall^f x(A(x) \supset A(Sx)) \supset \forall^f x A(x) \quad (Ind^f),$$

where $A(x)$ does not contain F and the notation $\forall^f x A(x)$ stands for $\forall x(F(x) \supset A(x))$. If $\vdash$ denotes provability in our newly obtained theorem, then we can state the following results:

Theorem 1 *Let* $\vdash F(t)$ *for a closed term* t*. Then there exists an* n *such that* $\vdash t = \underline{n}$*.*

The proof of the theorem follows a realisability technique due to Kleene [6].

As a consequence of the Theorem, we obtain the disjunction and existential properties.

Corollary 2 *Let* A *be a closed formula such that* $\vdash A$*. Then the following assertions are valid.*

1. *If* $A = (B \vee C)$ *then either* $\vdash B$ *or* $\vdash C$*.*
2. *If* $A = \exists x C(x)$ *then* $\vdash C(\underline{k})$ *for some number* k*.*

In the talk, we are going to give a brief exposure of the results and the background notions together with some possible further implications and future directions.

References

[1] Avigad, J., Helzner, J., *Transfer principles in nonstandard intuitionistic arithmetic.* Archive for Mathematical Logic 41 (6), 581–602 (2002)

[2] Dragalin, A. G., *Explicit algebraic models for constructive and classical theories with non-standard elements.* Studia Logica, 55 (1), 33–61 (1995)

[3] Dragalin, A. G., *Mathematical Intuitionism. Introduction to Proof Theory.* Translations of AMS, 67, American Mathematical Society, Providence, Rhode Island (1988)

[4] Hájek, P., Pudlák, P., *Metamathematics of First-Order Arithmetic.* Springer-Verlag, Berlin Heidelberg (1993)

[5] Kaye, R., *Models of Peano Arithmetic.* Clarendon Press, Oxford (1991)

[6] Kleene, S. C., *Introduction to Metamathematics.* North Holand, Amsterdam (1952)

[7] Palmgren, E., *A note on mathematics of infinity.* The Journal of Symbolic Logic, 58 (4), 1195–1200 (1993)

[8] Skolem, Th. A., *Über die Nichtcharakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vielen Aussagen mit ausschliesslich Zahlvariablen.* Fundamenta Mathematicae, 23, 150–161 (1934)

[9] Troelstra, A. S., van Dalen, D., *Constructivism in Mathematics.* Vol. I.-II. North-Holland, Amsterdam (1988)

Puzzles in parameterized realizability

Andrej Bauer

University of Ljubljana, Slovenia
https://www.andrej.com/

The author and James Hanson formulated a variant of realizability, called parameterized realizability, which they used to construct a topos in which the object of Dedekind reals is countable. Many facts are known about the topos, but many more remain unanswered. In this talk we shall review the current status of our knowledge. Parameterized realizability seems to be resilient against the usual battery of computability-theoretic arguments involving the Recursion theorem and diagonalization. Even such basic questions as validity of the Lesser principle of omniscience (every infinite binary sequence contains a 1 or is constantly 0) is unknown, as well as that of the statement "all functions are continuous". One gets the feeling that sufficiently ingenious modifications of known techniques ought to work, but the author has only been able to find ones that tricked him into holding false beliefs.

Probabilized Unranked Sequent Calculus

Merium Bishara[1], Lia Kurtanidze[2], Mikheil Rukhaia[3], Lali Tibua[3]

[1] *International Black Sea University*

2, David Agmashenebeli Alley 13 km, 0131 Tbilisi, Georgia

[2] *Georgian National University SEU*

9, Tsinandali Str., 0144 Tbilisi, Georgia

[3] *Institute of Applied Mathematics, Tbilisi State University*

11, University Str., 0186 Tbilisi, Georgia

E-mail: [1] 22100636@ibsu.edu.ge, [2] l.kurtanidze@seu.edu.ge,
[3] mrukhaia@logic.at, ltibua@viam.tsu.ge

Keywords:
sequence variables, probabilistic primitives, sequent calculus.

Since the early days of Artificial Intelligence (AI) logical and probabilistic methods have been independently used in order to solve tasks that require some sorts of "intelligence". Probability theory deals with the challenges posed by uncertainty, while logic is more often used for reasoning with perfect knowledge. Considerable efforts have been devoted to combining logical and probabilistic methods in a single framework, which influenced the development of several formalisms and programming tools. Among others, the most prominent ones include Independent Choice Logic (ICL) [13], Markov Logic Networks (MLN) [14], Bayesian Logic Programs [9], P-log [2], ProbLog [7], and Probabilistic Soft Logic (PSL) [1]. These languages and formalisms have been successfully applied to many domains.

All probabilistic logic formalisms studied so far are either propositional, or permit only individual variables, i.e., variables that can be instantiated by a single term. On the other hand, theories and systems that use not only individual variables but also sequence variables (these variables can be replaced by arbitrary finite, possibly empty, sequences of terms) have emerged. Recently, the usefulness of sequence variables and unranked symbols (function and/or predicate symbols without fixed arity) has been shown in several formalisms and illustrated in practical applications related to XML [5], knowledge representation [8, 6], automated reasoning [12], and rule-based programming [11], just to name a few. There are systems for programming with sequence variables. Probably the most prominent one is Mathematica [15], with a powerful rule-based programming language that uses (essentially first order, equational) unranked matching with sequence variables [4]. The unranked term is a first-order term, where the same function symbol can occur in different places with different number of arguments. Unranked function symbols and sequence variables bring a great deal of expressiveness in this language, permitting writing a short, concise, readable code.

We make one step forward in hybridizing logical and probabilistic methods, and present probabilized first-order sequent calculus with sequence variables and unranked function symbols. In such formalism, sequence variables, unranked terms and probabilistic primitives are available together. We probabilize the Gentzen-style inference system **G**, given in [10], in a similar way, as Marija Boričić probabilized classical propositional sequent calculus in [3]. We show that the new system keeps properties like soundness and completeness.

The inference system **G** is an extension of the standard first-order **LK** calculus with the additional $\forall$ and $\exists$ quantifier rules over sequence variables. The language defines unranked forumale using flexible arity predicate symbols where quantification is allowed over both – individual (usual first-order) and sequence variables.

In our presentation we formally define the notions of unranked term, unranked formula, sequent and the probabilized sequent, which is an expression $\Gamma \vdash_a^b \Delta$, for an interval $[a, b] \subseteq [0, 1]$, with the intended meaning that the probability of derivability of $\Gamma \vdash \Delta$ (or of validity of the unranked formula $\bigwedge \Gamma \rightarrow \bigvee \Delta$) is in the interval $[a, b]$. If there is a case when $a > b$ or $a, b \notin [0, 1]$, then we write $\Gamma \vdash^{\emptyset} \Delta$ and treat it as a contradiction. Next, we define the inference rules, give an example derivation and discuss the properties of the calculus.

Acknowledgment

This work was supported by Shota Rustaveli National Science Foundation of Georgia under the grant №FR-22-4254.

References

[1] Stephen H Bach, Matthias Broecheler, Bert Huang, and Lise Getoor. Hinge-loss markov random fields and probabilistic soft logic. *Journal of Machine Learning Research*, 18:1–67, 2017.

[2] Chitta Baral, Michael Gelfond, and Nelson Rushton. Probabilistic reasoning with answer sets. *Theory and Practice of Logic Programming*, 9(1):57–144, 2009.

[3] Marija Boričić. Sequent calculus for classical logic probabilized. *Archive for Mathematical Logic*, 58:119–136, 2019.

[4] Bruno Buchberger. Mathematica as a rewrite language. In Tetsuo Ida, Atsushi Ohori, and Masato Takeich, editors, *Functional and Logic Programming - 2nd Fuji International Workshop, FLOPS 1996, Shonan Village, Japan, June 4-6, 1996. Proceedings*, Lecture Notes in Computer Science, pages 1–13. Springer, 1996.

[5] Jorge Coelho and Mário Florido. XCentric: logic programming for XML processing. In Irini Fundulaki and Neoklis Polyzotis, editors, *9th ACM International Workshop on Web Information and Data Management (WIDM 2007), Lisbon, Portugal, November 9, 2007*, pages 1–8. ACM, 2007.

[6] Common Logic Working Group. Common Logic Working Group Documents: Common Logic Standard. http://common-logic.org/, 2007.

[7] Luc De Raedt and Angelika Kimmig. Probabilistic (logic) programming concepts. *Machine Learning*, 100(1):5–47, 2015.

[8] Michael R. Genesereth. Knowledge Interchange Format, draft proposed American National Standard (dpANS). Technical Report NCITS.T2/98-004, Stanford University, 1998. Available from http://logic.stanford.edu/kif/dpans.html.

[9] Kristian Kersting and Luc De Raedt. Bayesian logic programming: theory and tool. In L. Getoor and B. Taskar, editors, *Introduction to Statistical Relational Learning*, chapter 10. MIT press, 2007.

[10] Temur Kutsia and Bruno Buchberger. Predicate logic with sequence variables and sequence function symbols. In *International Conference on Mathematical Knowledge Management*, pages 205–219. Springer, 2004.

[11] Mircea Marin and Temur Kutsia. Foundations of the rule-based system ρLog. *Journal of Applied Non-Classical Logics*, 16(1-2):151–168, 2006.

[12] Lawrence C. Paulson. Isabelle: The next 700 theorem provers. In *Logic and Computer Science*, pages 361–386. Academic Press, 1990.

[13] David Poole. Abducing through negation as failure: Stable models within the independent choice logic. *The Journal of Logic Programming*, 44(1-3):5–35, 2000.

[14] Matthew Richardson and Pedro Domingos. Markov logic networks. *Machine learning*, 62(1-2):107–136, 2006.

[15] Stephen Wolfram. *The Mathematica Book*. Wolfram Media, 5th edition, 2003.

Measuring Node Integration in Directed Graphs and the Applications

Sanda Bujačić Babić, Tajana Ban Kirigin

Faculty of Mathematics, University of Rijeka
R. Matejčić 2, 51000 Rijeka, Croatia
E-mail: bank@uniri.hr, sbujacic@uniri.hr

Keywords:
complex networks; directed graphs; centrality measures; key nodes.

In the era of big data, enormous amounts of data are collected and analysed to gain important information and make decisions in a variety of application areas. Graphs are recognised as an excellent tool for visualising the information structure of many data systems.

When analysing the structure and behaviour of complex networks, centrality measures help to determine and evaluate the role and importance of individual nodes in the graph and provide information about various network properties such as connectivity, survivability and robustness. There is no unanimity on the criteria for defining the concept of centrality. Different centralities emphasise different aspects of the importance of nodes in directed and undirected graphs.

As part of our research in NLP, we found that the available standard centrality measures were not suitable for detecting a high degree of node integration in the graph representations of certain syntactic-semantic lexical structures. This motivated the definition of Semi-Local Integration Measure of Node Importance (SLI) [1], a centrality measure that evaluated the level of node integration in undirected and weighted complex networks. The tailor-made SLI measure proved to be very valuable for NLP analysis [2], but also showed high potential for other applications, particularly for identifying well-integrated nodes within friend-of-a-friend types of networks, where SLI centrality provides a more nuanced differentiation of the importance of nodes compared to standard centrality measures.

Recently, we focused on applications modeled by directed and weighted networks, taking into account the directionality of links, which adds a more elaborate perspective on the importance of nodes within the network. This led us to propose the directed version of our SLI centrality, the Semi-Local Integration Measure for Directed Graphs (DSLI) [3]. This novel centrality measure evaluates the integration of nodes within the local cluster based on link presence, direction, its strength, organisation and optimisation of inbound and outbound interconnectivity, and redundancy within the local subnetwork.

There is a variety of applications that rely on directed graph models to address specific issues, from managing transportation networks, organizing distribution and delivery, and studying biological networks, to organizing the Internet. Since centrality measures are involved in the detection of key nodes in complex networks, they are a valuable tool within the robust complex network framework. For example, by identifying critical nodes and understanding the flow of information in the task of improving cybersecurity, security experts can detect, analyse, and mitigate various structural threats within the network. This approach not only strengthens immediate security measures but also contributes to long-term resilience to evolving threats.

Acknowledgment

This work has been supported by the University of Rijeka under the project *Mathematical Modelling in NLP* (uniri-iskusni-prirod-23-150).

References

[1] T. Ban Kirigin, S. Bujačić Babić, B. Perak.
Semi-Local Integration Measure of Node Importance, Mathematics, 10(3):405, 2022.

[2] T. Ban Kirigin, S. Bujačić Babić, B. Perak.
Graph-Based Taxonomic Semantic Class Labeling, Future Internet, 14(12):383, 2022.

[3] T. Ban Kirigin, S. Bujačić Babić.
Semi-Local Integration Measure for Directed Graphs, Mathematics, 12, 1087, 2024.

Computable metric bases

Konrad Burnik [*] Zvonko Iljazović [†] Lucija Validžić [‡]

If (X, d) is a metric space and $x_0, \ldots, x_n$ is a finite sequence in X such that for all $a, b \in X$ the equalities $d(a, x_0) = d(b, x_0), \ldots, d(a, x_n) = d(b, x_n)$ imply $a = b$, then we say that $x_0, \ldots, x_n$ is a metric basis for (X, d). We investigate computable metric spaces (X, d, α) and metric bases $x_0, \ldots, x_n$ for (X, d) such that $x_0, \ldots, x_n$ are computable points in (X, d, α). In particular, we are interested in the case when (X, d) has a one-point metric basis x_0 and we investigate conditions under which such an x_0 has to be computable. In view of this, it turns out that effective compactness of the ambient space plays an important role.

We have the following two results.

Theorem 1 *Let (X, d, α) be an effectively compact computable metric space such that (X, d) has finitely many connected components. If x_0 is metric basis for (X, d), then x_0 is a computable point in (X, d, α).*

Theorem 2 *Let (X, d, α) be a computable metric space which has the effective covering property and compact closed balls. Suppose (X, d) is homeomorphic to $[0, +\infty\rangle$. If x_0 is a metric basis for (X, d), then x_0 is a computable point in (X, d, α).*

References

[1] Z. Iljazović. Co-c.e. spheres and cells in computable metric spaces. *Logical Methods in Computer Science*, 7(3:05):1–21, 2011.

[2] Z. Iljazović and L. Validžić. Maximal computability structures. *Bulletin of Symbolic Logic*, 22(4):445–468, 2016.

[3] R.A. Melter and I. Tomescu. Metric bases in digital geometry. *Computer Vision, Graphics, and Image Processing*, 25:113–121, 1984.

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

[*] Xebia Data, email: kburnik@gmail.com

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

[‡] University of Zagreb, email: lucija.validzic@math.hr

[5] E. Čičković, Z. Iljazović, and L. Validžić. Chainable and circularly chainable semicomputable sets in computable topological spaces. *Archive for Mathematical Logic*, 58:885–897, 2019.

Approximating semicomputable graphs in computable metric spaces

Vedran Čačić[1], **Matea Čelar**[2], **Marko Horvat**[3], **Zvonko Iljazović**[4]

[1,2,3,4]*Department of Mathematics, University of Zagreb Faculty of Science*
Bijenička 30, Zagreb, Croatia
E-mail: [1]`veky@math.hr`, [2]`matea.celar@math.hr`, [3]`mhorvat@math.hr`, [4]`zilj@math.hr`

Keywords:
computable analysis, computable metric space, semicomputable set, generalized graph, computable approximation

We study generalized topological graphs, which are obtained by gluing rays and arcs together at their endpoints. We prove that every semicomputable generalized graph in a computable metric space can be approximated, with arbitrary precision, by a computable subgraph with computable endpoints.

References

[AH23] Djamel Eddine Amir and Mathieu Hoyrup. Strong computable type. *Computability*, 12(3):227–269, 2023.

[Ilj20] Zvonko Iljazović. Computability of graphs. *Math. Log. Q.*, 66(1):51–64, 2020.

[IP18] Zvonko Iljazović and Bojan Pažek. Computable intersection points. *Computability*, 7:57–99, 2018.

[IV17] Zvonko Iljazović and Lucija Validžić. Computable neighbourhoods of points in semicomputable manifolds. *Annals of Pure and Applied Logic*, 168(4):840–859, 2017.

A certified algorithm for stratification

Vedran Čačić[1], **Marko Doko**[2]

[1] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, Zagreb, Croatia
[2] *Heriot–Watt University*
Edinburgh, United Kingdom
E-mail: [1]`veky@math.hr`, [2]`M.Doko@hw.ac.uk`

Keywords:
New Foundations with Urelements,
Coq proof assistant,
certified programming with dependent types.

Quine's theory of New Foundations, enriched by Jensen's Urelements, promises to be a fertile ground for developing new methods of doing mathematics collaboratively by humans and computers, since it combines human-like intuition of set theory with computer-like rigidity of type theory. The main tool for achieving this is defining new concepts as sets, using abstraction terms over stratified formulas. However, the need to iterate this construction necessitates characterizing the stratification of formulas extended with abstraction terms.

There are three common approaches to this: the new terms can be *eliminated* (reverting to basic formulas), *typed* (treating them as new variables with special stratification conditions), or *named* (extending the signature with new constant and function symbols). Two years ago, an idea emerged to harmonize these three approaches, demonstrating that they lead to equivalent notions of stratification in the extended language. Today, we have completed the first step by developing a certified algorithm for stratification (based on [1]) and proved that (with an interesting exception involving constant terms) eliminating abstraction terms results in the same stratified formulas as typing them.

Acknowledgment

This work was done while the first author was on sabbatical leave. I thank Department of Mathematics for granting me a semester free of teaching, and Heriot–Watt University for the warm welcome and hospitality.

References

[1] Adlešić, T., Čačić, V., *A Modern Rigorous Approach to Stratification in NF/NFU*, Logica Universalis, 2022., 10.1007/s11787-022-00310-y

Formal Certification of Synthesized Sorting Algorithms

Isabela Drămnesc[1], Tudor Jebelean[2], Sorin Stratulat[3]

[1] *Department of Computer Science, West University of Timisoara, Romania*
[2] *ICAM, West University of Timisoara, Romania*
RISC, Johannes Kepler University, Linz, Austria
[3] *Université de Lorraine, CNRS, LORIA, Metz, F-57000, France*
E-mail: [1] `Isabela.Dramnesc@e-uvt.ro`,
[2] `Tudor.Jebelean@e-uvt.ro`,
[3] `sorin.stratulat@univ-lorraine.fr`

Keywords:
formal certification, sorting algorithms, natural style proofs, *Theorema*, skeptical proofs, Coq

Today, we assist to a growing complexity of software that increases the difficulty to develop reliable applications. On the other hand, faulty software can dangerously lead to destructive results. Software written for controlling robots is an example of critical applications that need to be certified that nothing bad can happen. Even for simple operations that can be encountered every-day, the certification process may be non-trivial. Data sorting is such an operation, with practical applications for spreadsheet users, the storage and analysis of data related to the environment and climat change, etc.

In this talk, we give an overview of some computer-based experiments of formal certification of various sorting algorithms by using mechanized reasoning tools such as the *Theorema* [1, 2, 8] and Coq [7] proof systems. The sorting algorithms that we consider process a multiset of naturals such that its elements become increasingly ordered. They are: *Quick–Sort*, *Patience–Sort*, *Min–Sort*, *Max–Sort*, *Min–Max–Sort*, and *Bubble-Sort*. They have been synthesized in recent work [3, 4] using the *Theorema* prover, then certified with *Theorema* and Coq in [5, 6].

We explain how to construct the appropriate underlying theory, define the sorting algorithms in a functional style, run on examples and discuss the proofs of their correctness and of the required lemmas. Since the certification was performed in parallel, both in *Theorema* and Coq, we also take advantage to compare their characteristics and performances.

In *Theorema*, the underlying theory uses multisets in order to express the fact that the input and the output have the same elements. The proofs are built almost completely automatically, and presented in a (natural) style close to the proofs produced by humans. The proofs are non-trivial and require explicit induction reasoning that uses generalized induction schemes based on a well-founded ordering on lists defined by the strict inclusion of multisets. On the other hand, the background theory, the algorithms, and the proof rules are composed by the user without any restrictions – thus the proofs are error prone.

In Coq, the specification of sorting algorithms uses a multiset representation based on lists and a permutation relation. The proofs are highly interactive, based on scripts built by humans, which require more additional lemmas and proof effort. On the other hand, the algorithm definitions and the proofs are absolutely rigurous as Coq cannot accept elements that are not theoretically correct.

Our experiments contribute to a better understanding and estimation of the complexity of such certification tasks, and to create a basis for further increase of the level of automation in the two systems and for their possible integration.

Acknowledgments

This work is co-funded by the European Union, Erasmus+ project AiRobo: Artificial Intelligence based Robotics, 2023-1-RO01-KA220-HED-000152418.

References

[1] B. Buchberger, T. Jebelean, F. Kriftner, M. Marin, E. Tomuta, and D. Vasaru. A survey on the Theorema project. In *In International Symposium on Symbolic and Algebraic Computation*, pages 384–391. ACM Press, 1997.

[2] B. Buchberger, T. Jebelean, T. Kutsia, A. Maletzky, and W. Windsteiger. Theorema 2.0: Computer-Assisted Natural-Style Mathematics. *Journal of Formalized Reasoning*, 9(1):149–185, 2016.

[3] I. Dramnesc and T. Jebelean. Mechanical Verification of Insert-Sort and Merge-Sort Using Multisets in Theorema. In *SISY 2023*, pages 55–60. IEEE, 2023.

[4] I. Dramnesc, T. Jebelean, and S. Stratulat. Mechanical synthesis of sorting algorithms for binary trees by logic and combinatorial techniques. *Journal of Symbolic Computation*, 90:3–41, 2019.

[5] I. Dramnesc, T. Jebelean, and S. Stratulat. Certification of Sorting Algorithms Using Theorema and Coq. In *SCSS 2024*. Submitted, 2024.

[6] I. Dramnesc, T. Jebelean, and S. Stratulat. Certification of tail recursive Bubble–Sort in Theorema and Coq. In N. Bjorner, M. Heule, and

A. Voronkov, editors, *LPAR 2024 Complementary Volume*, volume 18 of *Kalpa Publications in Computing*, pages 53–68. EasyChair, 2024.

[7] The Coq development team. *The Coq Reference Manual.* INRIA, 2020.

[8] W. Windsteiger. Theorema 2.0: A system for mathematical theory exploration. In *ICMS'2014*, volume 8592 of *LNCS*, pages 49–52, 2014.

Fuzzy Pattern Calculus

Besik Dundua

Kutaisi International University

Akhalgazrdoba Ave. Lane 5/7, Kutaisi, 4600 Georgia

E-mail: bdundua@gmail.com

Keywords:
lambda calculus, pattern calculus, matching, rewriting.

Pattern calculus [2] extends the λ-calculus [1] with pattern matching capabilities. Instead of abstracting from a variable, they permit abstractions from a pattern: a λ-term which specifies the form of the argument. The more flexible the patterns are, the more powerful the calculus is. Patterns are the most expressive ones: They can be instantiated, generated, and reduced. Pattern calculus is expressive, but there is also a price to pay for that: Confluence is lost and various restrictions have to be imposed to recover it.

Fuzzy similarity relations are reflexive, symmetric, and transitive fuzzy relations. Similarity-based matching and unification has been quite intensively investigated, as a core computational method for approximate reasoning and declarative programming. In this talk we propose extension of pattern calculus with fuzzy similarity relations.

Reduction in pure pattern calculus is parameterized by crisp pattern matching. We replace it by similarity based pattern matching to obtain the calculus that supports approximate reduction. That means, for a term $(\lambda_V P.M)N$, if P matches to N with substitution σ and degree d, then $(\lambda_V P.M)N$ reduces to $M\sigma$ with degree d. Certainly, such a reduction is not generally confluent. We discuss restrictions that guarantee confluence of the fuzzy pattern calculus.

Acknowledgment

This work was supported by Shota Rustaveli National Science Foundation of Georgia under the project FR-21-7973.

References

[1] Hendrik Pieter Barendregt, Wil Dekkers, and Richard Statman. *Lambda calculus with types.* Cambridge University Press, 2013.

[2] Barry Jay. *Pattern Calculus: Computing with Functions and Structures.* Springer Science & Business Media, 2009.

Proofs-as-programs: from logic to AI

Silvia Ghilezan

University of Novi Sad

Mathematical Institute of the Serbian Academy of Sciences and Arts

The proofs-as-programs correspondence, also known as, the Curry-Howard correspondence and the formulae-as-type is a foundational concept that connects logic and computation. This correspondence establishes a deep connection between logical reasoning and computational processes. The origins of this idea can be traced back to the relationship between intuitionistic logic, lambda calculus and combinatory. Nowadays it is at the heart of formal verification of mathematical proofs. Extensions to various logical and computational frameworks highlights its versatility and broad applicability across different domains of mathematics and computer science.

In this talk, we give an overview of this correspondence in different frameworks of computation and communication in distributed systems. The focus is on recent results which lead to safe orchestrations of federated (machine) learning algorithms.

Acknowledgment

Funded by the European Union (TaRDIS, 101093006). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] C. A. R. Hoare, Communicating Sequential Processes, Prentice Hall International, (1985) 2004

[2] W. A. Howard, The formulae-as-types notion of construction, in J. P. Seldin and J. R. Hindley (eds), *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pp 479–490, Academic Press, (1969) 1980

[3] I. Prokić, S. G., S. Kašterovic ć, M. Popovic, M. Popovic, I. Kaštelan, Correct orchestration of Federated Learning generic algorithms: formalisa-

tion and verification in CSP *ECBS 2023 - Engineering of Computer-Based Systems*, Lecture Notes in Computer Science 14390, pp 274–288 (2023)

[4] M. H. B. Sörensen, P. Urzyczyn, Lectures on the Curry-Howard isomorphism, MIT Press, 2002

Effective analogue of an ultraproduct of structures

Valentina Harizanov

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

Keywords:
Computable structure, cohesive set, ultraproduct, partial computable function, effective product, decidable structure.

We study an effective analogue of the ultraproduct construction for computable structures. A structure A is computable (constructive) if its domain is a computable set and its relations and functions are uniformly computable or, equivalently, the atomic diagram of A is computable. We consider computability-theoretic product construction for an infinite uniformly computable sequence of structures, where the role of an ultrafilter is played by a cohesive set. A cohesive set is an infinite set of natural numbers that cannot be split into two infinite subsets by any computably enumerable set. There are continuum many cohesive sets, and some are the complements of computably enumerable sets, which are known as maximal sets. For the effective product we consider only partial computable functions. Hence, the elements of the product are the equivalence classes of certain partial computable functions, which in the case of a co-maximal set can be replaced by (total) computable functions.

In particular, we study effective powers of a single computable structure. Unlike many classical ultrapowers, effective powers are countable structures and can be isomorphic to the original structure. We investigate the isomorphism types of cohesive powers and their properties when they are not isomorphic to the original structure. It is possible for isomorphic computable structures to have non-elementarily equivalent effective powers over a fixed cohesive set.

In general, effective powers preserve the first-order properties expressed only by sentences of lower levels of quantifier complexity. Additional decidability in the computable structure plays a significant role in increasing satisfiability of sentences in its effective power. For example, a structure A is called decidable (strongly constructive) if its elementary diagram is computable. For a decidable structure, the effective power is elementarily equivalent to the structure.

We will present some of our recent collaborative results on effective powers for various structures [3, 4]. Although effective powers arose naturally in the relatively recent study of the automorphisms of the lattice of computably enumerable vector spaces initiated by R. Dimitrov (see [2]), the original inspiration for effective powers dates back to Skolem's 1934 construction of a countable non-standard model of arithmetic (see [1]).

Acknowledgment

This work has been supported by FRG NSF grant DMS-215209.

References

[1] R.D. Dimitrov and V. Harizanov, *Countable nonstandard models: following Skolem's approach*, in: Handbook of the History and Philosophy of Mathematical Practice, B. Sriraman, ed., Springer, 2024, pp. 1989–2009.

[2] R.D. Dimitrov and V. Harizanov, *Orbits of maximal vector spaces*, Algebra and Logic 54 (2016), pp. 440–477 (English translation).

[3] R. Dimitrov, V. Harizanov, A. Morozov, P. Shafer, A.A. Soskova and S.V. Vatev, *On cohesive powers of linear orders*, Journal of Symbolic Logic 88 (2023), pp. 947–1004.

[4] V. Harizanov and K. Srinivasan, *Cohesive powers of structures*, to appear in Archive for Mathematical Logic

Interpolation Properties of Proofs with Cuts

Anela Lolić [1]

[1] *Kurt Gödel Society, Institute of Logic and Computation, TU Wien*
Favoritenstrasse 9, 1040 Vienna, Austria
E-mail: [1] anela@logic.at

Keywords:
interpolation properties, cut-elimination.

Ever since Craig's seminal result on interpolation [2], interpolation has been recognized as important property of logical systems. In essence, *Craig interpolation* states that a logic L has the interpolation property if whenever $A \to B$ holds in L, the information from A that is relevant to derive B is a formula I in the common language of A and B, i.e. both $A \to I$ and $I \to B$ hold in L. It demonstrates that only contradictory formulas A and valid formulas B admit the validity of $A \to B$ if A and B do not have anything in common.

As it is often the case in proof theory, also Craig interpolation can be seen as an instance of a more general principle, in this case *Maehara's lemma* [4], which establishes an interpolant on any partition of the end-sequent of a cut-free proof. It is one of the most significant properties of cut-free **LK**-derivations that they allow a direct construction of interpolants by Maehara's lemma, thereby limiting the interpolant's complexity in terms of proof complexity.

Maehara's Lemma.

Let $\Gamma \vdash \Delta$ be **LK**-provable, and (Γ_1, Γ_2) and (Δ_1, Δ_2) arbitrary partitions of Γ and Δ, denoted as $[\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2\}]$. Then there exists a formula I, called the interpolant of the partition, s.t.

1. $\Gamma_1 \vdash \Delta_1, I$ and $I, \Gamma_2 \vdash \Delta_2$ are both **LK**-provable.

2. I contains only free variables and individual and predicate constants apart from $\top$ that occur in $\Gamma_1 \cup \Delta_1$ and $\Gamma_2 \cup \Delta_2$.

In classical logic, cut-free proofs can always be obtained from proofs with cuts by Gentzen's cut-elimination theorem [3], hence interpolants based on Maehara's lemma can always be constructed. But what happens if cuts are not eliminated prior to applying Maehara's lemma? In this work we focus on this question and identify cut-formulas that admit the extraction of interpolants from proofs based on a variant of Maehara's lemma. Consider for instance proofs that contain atomic cut-formulas only [1]:

Lemma.

Let φ be an **LK**-proof of the form

$$\frac{\begin{array}{c}(\varphi_1)\\ \Gamma \vdash \Delta, F\end{array} \qquad \begin{array}{c}(\varphi_2)\\ F, \Pi \vdash \Lambda\end{array}}{\Gamma, \Pi \vdash \Delta, \Lambda}\ cut$$

where F is an atomic formula, φ_1 and φ_2 cut-free. Let $X = [\{\Gamma_1, \Pi_1; \Delta_1, \Lambda_1\}, \{\Gamma_2, \Pi_2; \Delta_2, \Lambda_2\}]$ be a partition of the end-sequent $S:\ \Gamma, \Pi \vdash \Delta, \Lambda$. Then there exists an interpolant I of S w.r.t. X s.t. either $I = I^1 \wedge I^2$ or $I = I^1 \vee I^2$, where I^1 is an interpolant of $\Gamma \vdash \Delta, F$ and I^2 is an interpolant of $F, \Pi \vdash \Lambda$.

Proof.

1. F occurs only as a predicate symbol in $\Gamma_2, \Pi_2, \Delta_2, \Lambda_2$. Define the partitions $X_1 = [\{\Gamma_1; \Delta_1\}, \{\Gamma_2; \Delta_2, F\}]$ of $\Gamma \vdash \Delta, F$, and $X_2 = [\{\Pi_1; \Lambda_1\}, \{F, \Pi_2; \Lambda_2\}]$ of $F, \Pi \vdash \Lambda$. By Craig's interpolation theorem there are interpolation derivations ψ'_1 w.r.t. X_1 and ψ'_2 w.r.t. X_2 s.t. $\psi'_1 =$

$$\frac{\begin{array}{c}(\chi_{1,1})\\ \Gamma_1 \vdash \Delta_1, I^1\end{array} \qquad \begin{array}{c}(\chi_{1,2})\\ I^1, \Gamma_2 \vdash \Delta_2, F\end{array}}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2, F}\ cut$$

   s.t. the predicate symbols of I^1 are in the intersection of the predicate symbols in the sequents $\Gamma_1 \vdash \Delta_1$ and $\Gamma_2 \vdash \Delta_2, F$, and, as F occurs in $\Gamma_2, \Pi_2, \Delta_2, \Lambda_2$ we have that the predicate symbols of I^1 are in the intersection of the predicate symbols in the sequents $\Gamma_1 \vdash \Delta_1$ and $\Gamma_2 \vdash \Delta_2$. $\psi'_2 =$

$$\frac{\begin{array}{c}(\chi_{2,1})\\ \Pi_1 \vdash \Lambda_1, I^2\end{array} \qquad \begin{array}{c}(\chi_{2,2})\\ I^2, F, \Pi_2 \vdash \Lambda_2\end{array}}{\Pi_1, \Pi_2, F \vdash \Lambda_1, \Lambda_2}\ cut$$

   s.t. the predicate symbols of I^2 are in the intersection of the predicate symbols in the sequents $\Pi_1 \vdash \Lambda_1$ and $F, \Pi_2 \vdash \Lambda_2$, and, as F occurs in $\Gamma_2, \Pi_2, \Delta_2, \Lambda_2$ we have that the predicate symbols of I^2 are in the intersection of the predicate symbols in the sequents $\Pi_1 \vdash \Lambda_1$ and $\Pi_2 \vdash \Lambda_2$. Now we define an interpolation derivation ψ for S w.r.t. X:

$$\frac{\dfrac{\begin{array}{c}(\chi_{1,1})\\ \Gamma_1 \vdash \Delta_1, I^1\end{array} \qquad \begin{array}{c}(\chi_{2,1})\\ \Pi_1 \vdash \Lambda_1, I^2\end{array}}{\Gamma_1, \Pi_1 \vdash \Delta_1, \Lambda_1, I^1 \wedge I^2}\ \wedge_r \qquad \dfrac{\dfrac{\begin{array}{c}(\chi_{1,2})\\ I^1, \Gamma_2 \vdash \Delta_2, F\end{array} \qquad \begin{array}{c}(\chi_{2,2})\\ I^2, F, \Pi_2 \vdash \Lambda_2\end{array}}{I^1, I^2, \Gamma_2, \Pi_2 \vdash \Delta_2, \Lambda_2}\ cut}{I^1 \wedge I^2, \Gamma_2, \Pi_2 \vdash \Delta_2, \Lambda_2}\ \wedge_l}{\Gamma_1, \Gamma_2, \Pi_1, \Pi_2 \vdash \Delta_1, \Delta_2, \Lambda_1, \Lambda_2}\ cut$$

By construction the predicate symbols in $I^1 \wedge I^2$ are a subset of the predicate symbols in $\Gamma_1, \Pi_1, \vdash \Delta_1, \Lambda_1$ and $\Gamma_2, \Pi_2 \vdash \Delta_2, \Lambda_2$.

2. F occurs only as a predicate symbol in $\Gamma_1, \Pi_1, \Delta_1, \Lambda_1$. Similar to the construction above, except that the interpolant is $I^1 \vee I^2$.

3. F does not occur in $\Gamma, \Pi, \Delta, \Lambda$. Then both cases above work, as neither I^1 nor I^2 contains F, thus $I^1 \wedge I^2$ and $I^1 \vee I^2$ do not contain F.

In the construction above we only considered interpolants s.t. their predicate symbols are in the common language of the formulas in the end-sequent. It can however be shown that from this form of interpolants full interpolants (containing only free variables and individual and predicate constants in the common language) can be obtained.

It is easy to show that a similar result as in the lemma above can be obtained for cut-formulas containing only one predicate symbol, and we conjecture that these results can be obtained even for more complex cut-formulas. It is an open question where the limits of these methods are.

Acknowledgment

The research reported in the paper is partly supported by FWF project I 5848, and an APART-MINT fellowship of the Austrian Academy of Sciences, and based on joint work (to be published) with Matthias Baaz, Simon Corbard, and Alexander Leitsch.

References

[1] Baaz, M., and Leitsch, A., *Methods of Cut-elimination.* Springer Science & Business Media, 2011.

[2] Craig, W., *Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory.* The Journal of Symbolic Logic, 22(03):269–285, 1957.

[3] Gentzen, G., *Untersuchungen über das logische Schließen.* Mathematische Zeitschrift, 39:176–210,405–431, 1934-35.

[4] Takeuti, G., *Proof theory.* North-Holland/American Elsevier, 1975.

Storytelling and extensions

Matej Mihelčić [1,2], Adrian Satja Kurdija[3]

[1] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, Zagreb, Croatia
[2] *Department of Electronics, Ruđer Bošković Institute, Zagreb*
Bijenička cesta 54, Zagreb, Croatia
[3] *Faculty of Electrical Engineering and Computing, University of Zagreb*
Unska 3, Zagreb, Croatia
E-mail: [1] matmih@math.hr, [2] adrian.kurdija@fer.hr

Keywords:
storytelling, redescription mining, complexity, data mining.

Storytelling [1] is an extension of a task of redescrption mining [2] with a goal of relating disjoint subsets of entities contained in the data. Each subset of entities can be associated with one query that describes it. Thus, we have q_{start} describing the first subset and q_{end} describing the second subset, $supp(q_{start}) \cap supp(q_{end}) = \emptyset$. The story is constructed by finding a sequence of redescriptions, of a predefined accuracy, that form a path from the starting query describing the first subset of entities to the final query describing the second subset of entities. Neighboring redescriptions in a sequence share one query and must have the Jaccard index larger than some predefined threshold ε. For example $q_{start} \rightarrow q_2 \rightarrow q_3 \rightarrow q_{end}$ is a sequence of queries that corresponds to a story $R_1 = (q_{start}, q_2),\ R_2 = (q_2, q_3),\ R_3 = (q_3, q_{end}),\ J(R_i) \geq \varepsilon, \forall i$ and $supp(q_{start}) \cap supp(q_{end}) = \emptyset$.

Storytelling has applications in biology, where one might need to relate sets of genes expressed in one experiment to another set implicated in a different pathway, understand the evolution or properties of disjoint sets of bacteria or species etc.

We will present the original formulation of the storytelling problem, including the sole algorithm for storytelling. Next, we will propose the natural extension of a problem to multiple views. Here, the data contains at least two disjoint sets of attributes describing the same set of entities. These can, for example, describe different properties of entities (genetic tests, phenotypic properties, medical measurements etc.). Attributes are grouped into views (W_i), each containing a set of related measurements. Here, all redescriptions are of a form $R_i = (q_1, q_2, \dots, q_{|\mathcal{W}|})$, where attributes forming q_1 come from the first view W_1, the attributes forming q_2 from the second view W_2 etc. Stories are again defined as sequences of redescriptions. One example of such a sequence can be $R_1 = (q_{1,start}, q_{2,1}, \ldots, q_{|\mathcal{W}|,1}), R_2 = (q_{1,3}, q_{2,1}, \ldots, q_{|\mathcal{W}|,2}), R_3 = (q_{1,3}, q_{2,2}, \ldots, q_{|\mathcal{W}|,3}), \ldots, R_n = (q_{1,end}, q_{2,s}, \ldots, q_{|\mathcal{W}|,p})$, where $J(R_i) \geq \varepsilon, \forall i$, $supp(q_{1,start}) \cap supp(q_{1,end}) = \emptyset$. Each neighboring pair of redescriptions shares a query from at least one view. Note that q_{start} and q_{end} can generally be constructed using attributes from different views. For example, one can search for stories between subsets described by $q_{1,start}$ and $q_{2,end}$ etc. Finally, we will show that a restricted 2-view variant, where redescription queries can only contain disjunction logical operator is $\mathcal{NP} - hard$ and the corresponding decision formulation is $\mathcal{NP} - complete$.

Literatura

[1] Deept Kumar, Naren Ramakrishnan, Richard F. Helm i Malcolm Potts. "Algorithms for storytelling". *Proceedings of the Twelfth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Philadelphia, PA, USA, August 20-23, 2006.* ACM, 2006., str. 604–610. DOI: 10.1145/1150402.1150475.

[2] Naren Ramakrishnan, Deept Kumar, Bud Mishra, Malcolm Potts i Richard F. Helm. "Turning cartwheels: An alternating algorithm for mining redescriptions". *Proc. KDD'04.* ACM Press, 2004., str. 266–275.

Learning machines build self-confirming beliefs

Duško Pavlović

Machine-learned language models have transformed everyday life: they steer us when we study, drive, manage money. They have the potential to transform our civilization. But they hallucinate. Their realities are virtual. It turns out that, after they become capable of recognizing hallucinations and dreaming safely, as humans tend to be, the language-learning machines proceed to generate broader systems of false beliefs and self-confirming theories, as humans tend to do. The talk is based on the general logical construction from [2] in the learning framework of [1, Ch. 4].

Unfortunately, the author had to cancel attendance, due to an unexpected duty.

References

[1] Dusko Pavlovic. Language processing in humans and computers. CoRR, arxiv.org/abs/2405.14233, May 2024.

[2] Dusko Pavlovic and Temra Pavlovic. From Gödel's Incompleteness Theorem to the completeness of bot beliefs. In H.H. Hansen et al, editor, Logic, Langugage, Information, and Computation, volume 13923 of Lecture Notes in Computer Science. Springer, 2023. `arxiv.org/abs/2303.14338`.

Locality-based moral planning with LTL values

Adrian Satja Kurdija[1], Matej Mihelčić[2,3]

[1] *Faculty of Electrical Engineering and Computing, University of Zagreb*
Unska 3, Zagreb, Croatia
[2] *Department of Mathematics, Faculty of Science, University of Zagreb*
Bijenička cesta 30, Zagreb, Croatia
[3] *Department of Electronics, Ruđer Bošković Institute*
Bijenička cesta 54, Zagreb, Croatia
E-mail: [1] adrian.kurdija@fer.hr, [2] matmih@math.hr

Keywords:
Automated planning, linear temporal logic, robotics.

A framework for logic-based ethical planning with intended application to robotics was introduced by [2] in 2022. There, several planning tasks have shown to be intractable (PSPACE-complete). Using additional assumptions at the cost of generality, we define a constrained version of the CONFLICT problem that is polynomially solvable and present the algorithm to solve it.

Here, we briefly describe the relevant part of the framework [2] and our proposed contribution.

The world is described by atomic propositions $Prop = \{p_1, \ldots, p_n\}$ and their truth values (states) $s \in 2^{Prop}$. Each action $a \in Act$ can change values of some propositions according to the preconditions $\gamma^+, \gamma^- : Act \times Prop \to \mathcal{L}_{PL}$, where $\mathcal{L}_{PL}$ is the set of well-formed propositional logic formulas over *Prop*. After action a, proposition p becomes true if $\gamma^+(a,p)$ is true, and false if $\gamma^-(a,p)$ is true. If neither or both of them are true, the truth value of p will not change after action a. The described rules (action theory) allow us to calculate a history $H(\pi, s_0, \gamma)$ as the sequence of states generated by an action plan $\pi = (a_1, \ldots, a_k)$ from an initial state s_0 under action theory γ. A set of moral values Ω consists of linear temporal logic (LTL) formulas [3] that describe temporal properties of atomic propositions (evaluated under some history H) using operators such as negation $(\neg\phi)$, conjuction $(\phi_1 \wedge \phi_2)$, "next" $(X\phi)$, "until" $(\phi_1 \mathsf{U} \phi_2)$, "henceforth" $(G\phi)$, and "eventually" $(F\phi)$. For a given moral problem $M = (\Omega, \gamma, s_0)$, the CONFLICT problem asks if there is an action plan π such that the history $H(\pi, s_0, \gamma)$ satisfies all values from Ω. In [2], CONFLICT is shown to be PSPACE-complete using reduction from the propositional STRIPS planning problem called PLANSAT [1].

Our contribution lies in restricting CONFLICT to a polynomially solvable variant using additional assumptions that reduce its generality without sacrificing too much of its practical use. Motivated from various real-world examples, we assume that most propositions (all except for a constant number of them) are *localized* in the following sense: there is an ordering $Loc = (p_1, \ldots, p_n)$ of the localized propositions such that each action a depends on, and changes, only the propositions p_i from an interval $i \in [l(a), r(a)]$ of constant length $(r(a) - l(a) + 1 \leq L)$. In addition, there is a constant number of *global* propositions $Glob = \{q_1, \ldots, q_M\}$ for which there are no such constraints: any action can use or change their truth values. We additionally assume that the local ordering of propositions constrains the temporal order of actions: there is a constant K such that if $r(a) + K < r(b)$, then action a cannot be performed after action b. Finally, the value set Ω contains only the formulas of the form p, Fp, Gp, or FGp, where p is an atomic proposition or its negation. In other words, each goal dictates that some p must be currently/eventually/always/finally satisfied.

Under these assumptions, CONFLICT can be solved in polynomial time. Roughly, the algorithm is based on a breath-first search on a graph where each vertex corresponds to a *substate*, i.e., a truth assignment for an interval of $L+K$ consecutive propositions from *Loc* and all propositions from *Glob*. An edge can "move right", i.e., increase the substate position by 1 if the values from Ω concerning the proposition that gets removed from the substate are satisfied. Other edges correspond to actions that change the values of the substate propositions. The computational complexity is polynomial in the size of *Prop*, *Act*, and Ω, but contains the constant factor 4^{K+L+M}.

References

[1] Tom Bylander. "The computational complexity of propositional STRIPS planning". *Artificial Intelligence* 69.1 (1994.), str. 165–204. ISSN: 0004-3702. DOI: https://doi.org/10.1016/0004-3702(94)90081-7. URL: https://www.sciencedirect.com/science/article/pii/0004370294900817.

[2] Umberto Grandi i dr. "Logic-based ethical planning". *International Conference of the Italian Association for Artificial Intelligence*. Springer. 2022., str. 198–211.

[3] Amir Pnueli. "The temporal logic of programs". *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*. 1977., str. 46–57. DOI: 10.1109/SFCS.1977.32.

Aspects of Non-Associative Linear Logic

Andre Scedrov

University of Pennsylvania

Adding subexponentials to linear logic enhances its power as a logical framework, which has been extensively used in the specification of proof systems and programming languages. Originally, subexponentials were introduced in classical, linear, affine or relevant settings. Later, this framework was enhanced so to allow for commutativity as well. In [1], we closed the cycle by considering associativity. We formulated the resulting intuitionistic, two-sided system and showed that it admits the (multi)cut. In the talk we emphasize two new undecidability results that strengthen the undecidability results for fragments/variations of the system, given in [1]. If time permits we also discuss a classical, one-sided multi-succedent classical analogue of our intuitionistic system, presented in [2], following the exponential-free calculi of Buszkowski, and of de Groote and Lamarche. As in linear logic, a large fragment of our intuitionistic calculus is shown to embed conservatively into the classical version. It should be noted that such conservativity results are quite unusual, as they do not hold for traditional, richer logics which enjoy more structural rules for arbitrary formulae. This is joint work with Eben Blaisdell, Max Kanovich, Stepan L. Kuznetsov, and Elaine Pimentel.

References

[1] Blaisdell, E., Kanovich, M., Kuznetsov, S.L., Pimentel, E., Scedrov, A. (2022). Non-associative, Non-commutative Multi-modal Linear Logic. In: Blanchette, J., Kovács, L., Pattinson, D. (eds), Automated Reasoning. IJCAR 2022. Lecture Notes in Computer Science, vol. 13385, pp. 449–467, Springer, Cham. First Online: 01 August 2022. `https://doi.org/10.1007/978-3-031-10769-6_27`

[2] Blaisdell, E., Kanovich, M., Kuznetsov, S.L., Pimentel, E., Scedrov, A. (2023). Explorations in Subexponential Non-associative Non-commutative Linear Logic. In: M.Moortgat and M. Sadrzadeh, eds., Proceedings Modalities in substructural logics: Applications at the interfaces of logic, language and computation. Electronic Proceedings in Theoretical Computer Science EPTCS 381, pp. 4 - 19. Published: 7th August 2023. `https://doi.org/10.4204/EPTCS.381.3`

General frames for interpretability logic IL

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, interpretabiliy logic, Veltman semantics, general frames, strong completeness.

Interpretability logic **IL** extends provability logic **GL** with a new binary operator $\rhd$. One of the most notable semantics for **IL** is Veltman semantics (see [3]), which extends Kripke frames with a family of relations $\{S_w : w \in W\}$ satisfying some properties.

It is known that the logic **IL** is complete, but not strongly complete with respect to Veltman semantics. Similarly as the analogous problem for **GL**, this problem is due to Löb's axiom, $\Box(\Box\varphi \to \varphi) \to \Box\varphi$, and the fact that it defines a class of transitive and inversely well-founded frames.

In this talk, we will define a new class of frames, in which we replace the problematic property with irreflexivity, thus defining a new class of quasi-Veltman frames. Using this new class of frames we define the class of general frames, similarly as with classical modal logics (see e.g. [1]) and we prove that the logic **IL** is strongly complete with respect to the class of general frames.

References

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

[2] G. Japaridze, D. de Jongh. *The Logic of Provability*, Handbook of Proof Theory, Elsevier, Amsterdam, 1998.

[3] F. Veltman, D. de Jongh, *Provability logics for relative interpretability*, Mathematical Logic, Springer, 1990.

[4] A. Visser, *Preliminary notes on interpretability logic*, Logic Group Preprint Series No. 29, 1988.

Is there mathematical concepts that are real?

Zvonimir Šikić

According to [3], C. F. Gauss said: If $e^{i\pi} = -1$ was not immediately apparent to a student upon being told it, that student would never become a first-class mathematician. We will explore the arguments that support Gauss's claim in order to prove that there are no mathematical concepts that are real in Steiner's sense.

We conform to the position that concept exists if it satisfies the W. O. Quine's condition: Fs exist if $\exists xFx$ is a theorem of a true theory; cf. [8]. But M. Steiner claims in [10] that it is possible for Fs to satisfy this condition without being real. His inspiration is P. Bridgman's definition of physical reality: Something is physically real if it is connected with physical phenomena independent of those phenomena which entered its definition; cf. [1] p.56.

There is something profoundly right in the idea that the real is that which has properties transcending those which enter its definition and Steiner's aim is to show that mathematical entities can occasionally be said to be real in exactly the same sense.

Quine's condition is applicable to the existence of mathematical entities: scientific theories are committed to the existence of mathematical entities, and since we regard some of them as true, we must regard mathematical entities as existent. However, according to Steiner, this is not an argument for the reality of mathematical entities.

To demonstrate the reality of an entity in the natural sciences one typically shows that the entity is indispensable in explaining some new phenomenon. In this way the entity acquires new and independent descriptions. Steiner applies the same idea in mathematics.

For example, π is real because we have at least two independent descriptions for π. Geometric, $\pi = \frac{C}{2r}$ and analytic, $\pi = \frac{\ln(-1)}{i}$. In the first case π is derived from the formula for the circumference of a circle C with radius r. In the second case π is derived from the special case of Euler's formula, $e^{pii} = -1$.

We know by deductive proof that the descriptions are coreferential (unlike the situation in the physical sciences where this is demonstrated empirically). But then, how can provably coreferential descriptions be regarded as independent? Steiner's answer is to distinguish between two kinds of proof of coreference in mathematics: those which are nonexplanatory and merely demonstrate the coreference, and those which explain it. Descriptions are independent if the proofs of their coreferentiality are nonexplanatory.

We show that the "independence of the descriptions of two mathematical entities" is not additionally explained by the "absence of explanatory proofs of their coreference", so we will stick with "independence" as a less vague criterion.

After a detailed analysis of the "reality status" of π, in the previously described context, we conclude that π is not real in Steiner's sense. As a matter of fact, it is difficult to prove for any mathematical concept that it is real in Steiner's sense. Namely, it is not enough to formulate two descriptions of a concept and find a proof of their coreference which keeps the descriptions independent. It should be proved that all proofs of their coreference are such.

But mathematical theories are deeply connected and in the entire history of mathematics, mathematicians are constantly striving to discover these connections. For example, it is typical for mathematicians to persistently search for new proofs of old theorems in order to discover these intertheoretical dependencies.

Hence, our hypothesis is that no mathematical concept is real in Steiner's sense.

References

[1] Bridgman P. W. The logic of modern physics, Macmillan, 1958.

[2] Bürgi, J. Arithmetische und Geometrische Progreß-Tabulen, Prag, 1620.

[3] Derbyshire, J. Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics, Joseph Henry Press, 2003.

[4] Mercator, N., Pitt, M., Godbid, W. Logarithmo-technia sive Methodus construendi logarithmos nova, accurata, & facilis, London, 1667.

[5] Napier, J. Mirifici Logarithmorum Canonis descriptio, Edinburgh, 1619.

[6] Nagel, E. The Structure of Science: Problems in the Logic of Scientific Explanation, Harcourt, 1961.

[7] Newton, I. De analysi per aequationes numero terminorum infinitas, sent by Dr. Barrow to Mr. Collins in a letter dated July 31. 1669.

[8] Quine, W.O. On What There Is, The Review of Metaphysics 2 (5), 21-38, 1948.

[9] Steiner, M. Mathematical explanation, Philosophical Studies 34 (2), 135 – 151, 1978.

[10] Steiner, M. Mathematical Realism, Nous 17 (3), 383-395, 1983.

[11] Šikić, Z. Differential and integral calculus (in Croatian), Profil, 2008.

Threat models and moving target defense for the CoAP messaging protocol

Carolyn Talcott

Networked applications based on Internet of Things provide many services–some convenience, some safety critical (smart buildings, manufacturing, electrical grid, medical devices, ...). Network elements are often resource limited (memory, energy, bandwidth). The CoAP messaging protocol is an http-like protocol designed for use by resource limited devices. To study the vulnerabilities of CoAP and possible mitigations we formalized the CoAP specification RFC7252 in the Maude rewriting logic system. Protocol dialects are light weight moving target defense wrappers that provide additional security guarantees for communication. In this talk we will introduce CoAP, present a dialecting transform for CoAP message, and analyze its properties under different threat models. We will also summarize case studies demonstrating CoAP vulnerabilities and strange effects an attacker can achieve.

Brouwer-Weyl Continuum Through 3D Glasses: Geometry, Computation, General Relativity

Vladimir Tasić

University of New Brunswick, Fredericton, Canada

Keywords:

Brouwer, Weyl, continuum, Laguerre geometry, deSitter space, causal curves

Since at least the 1980s there has been growing interest in the hypothesis that conepts of computability are (or should be) dependent on physics. In the first part of this talk I review some of the fascinating arguments that appear to be at odds with one another more often than one would like.

The guiding idea is that theoretical computational devices like Turing machines ought to be viewed as realized (or realizable) in a particular physical setting. E.g., Turing machines seem to conceptually "live" in the world of classical mechanics. What is meant by "physical setting", however, is in fact a mathematical model of the physical world. Hence it seems more accurate to say that in works on a "physical Church-Turing Thesis", computability is considered in the framework of a *theory* within mathematical physics: classical mechanics, general relativity, or quantum theory, as the case may be.

Although literature on quantum computing features periodic announcements of purported violations of the Church-Turing Thesis, perhaps the most radical expression of the thesis that computability is dependent on physics comes from general relativity. In the somewhat exotic Malament-Hogarth spacetimes a Turing machine can travel along a trajectory that has infinite proper time and, it is argued, can send a signal to an observer in whose frame the machine's trajectory has finite time. The observer would thus have at their disposal an infinite-time Turing machine. Therefore, Hogarth argues [3], "the Church-Turing Thesis is like the outmoded claim: 'Euclidean geometry is the true geometry.'"

The arguments mentioned above proceed in the broader mathematical context of classical analysis, as does most of mathematical physics. In particular, the spacetime continuum is a manifold consisting of points with coordinates in $\mathbb{R}$. In the second part of the talk I would like to add to the overall confusion by showing how the Brouwer-Weyl continuum, or an analogous concept in several dimensions, itself relates to a spacetime familiar from mathematical physics — deSitter spacetime — as well as to order structures introduced in Dana Scott's work on the theory of computation.

According to Brouwer (and, for a time, Weyl), the continuum should be regarded as the collection of 'sequences of nested intervals whose measure converges to zero.' [5]. A higher-dimensional analog would be nested sequences of spheres with radii converging to zero. Classical geometry, going back to Laguerre and Lie, encodes the space of *oriented spheres* in $\mathbb{R}^n$ as points in $\mathbb{R}^{n+1}$: $(\mathbf{x}, r)$ with $\mathbf{x} \in \mathbb{R}^n$ being the centre and $r \in \mathbb{R}$ the oriented radius [1]. In this cyclographic representation the space of spheres has the structure of Minkowski space $\mathbb{R}^{1,n}$ with the usual pseudometric.

In this representation, for $r_1, r_2 > 0$, $||\mathbf{x}_1 - \mathbf{x}_2|| \leq r_1 - r_2$ iff the sphere $(\mathbf{x}_2, r_2)$ is contained in the sphere $(\mathbf{x}_1, r_1)$ [2]. In the terminology of special relativity, sphere inclusion corresponds to events that are related in the causal order. The concept of a nested sequence of spheres thus corresponds to a time-oriented causal sequence of events in Minkowski space.

Restricting to positive radii does not correspond to the full Minkowski space. To deal with this, we consider a different representation, in terms of Lie cycles. For a sphere $(\mathbf{x}, r)$, with $r > 0$, consider the vector $(y_0, \ldots, y_{n+1}) \in \mathbb{R}^{1,n+2}$ given by

$$\begin{aligned} y_0 &= -\frac{1}{2}\Big(\frac{||\mathbf{x}||^2 + 1}{r} - r\Big) \\ (y_1, \ldots, y_n) &= -\frac{1}{r}\mathbf{x} \\ y_{n+1} &= -\frac{1}{2}\Big(\frac{||\mathbf{x}||^2 - 1}{r} - r\Big) \end{aligned}$$

Then $-y_0^2 + \sum_{k=1}^{n+1} y_k^2 = 1$, and inducing the metric on this hyperboloid from $\mathbb{R}^{1,n+2}$ one gets the deSitter metric on the space of spheres

$$ds^2 = \frac{1}{r^2}(-dr^2 + d\mathbf{x}^2).$$

Substitution $r = e^{\mp t}$ yields the deSitter metric $ds^2 = -dt^2 + e^{\pm 2t} d\mathbf{x}^2$ in flat slicing coordinates of the "expanding" (resp. "contracting") part.

Thus, surprisingly, a detour through classical geometries relates the "higher-dimensional continuum" to a well known object in general relativity. Nested sequences of spheres correspond to "time"-oriented causal sequences. Such sequences, without additional qualifications, could be finite; this is not what Brouwer and Weyl had in mind. A more precise analog would be *inextendible* "time"-oriented causal sequences (by analogy of inextendible causal curves): there is no sphere that is contained in all spheres in the nested sequence.

These meditations suffer from a fatal flaw: they invoke the classical analysis that underpins the definition of deSitter space or Lorenzian manifolds in general. Although theorems in general relativity show that the manifold topology (under some assumptions) can be recovered from the space of timelike curves, this requires a notion of smoothness. It may be possible to formulate these ideas in a way that does not presuppose a concept of smoothness. Notably, Martin and Panangaden [4] introduce the category of globally hyperbolic posets, which includes causal orders on globally hyperbolic spacetimes such as deSitter. This category is equivalent to the category of interval domains, introduced by Scott in his pioneering work on the theory of computation and semantics of programming languages.

The upshot of the argument in [4] is that manifold topology (if not geometry) of a globally hyperbolic spacetime can be recovered from a countable dense subset of the associated interval domain of the causal order. The spacetime itself (if we start from one) is homeomorphic to the set of maximal elements in the interval domain, with Scott topology. If no manifold is given from the start, but only a countable dense poset — e.g., spheres with rational centres and rational radii — one can take an ideal completion of the basis of intervals in the poset. The set of maximal elements of the completion, with Scott topology, is the "manifold", topologically; but there is no metric. (This is the fundamental problem of the causal set program.)

Despite interesting and surprising (at least to me) connections with different fields of mathematics, it is not clear whether such an operation, even if successful, would lead to a satisfactory model of the intuitionist continuum in higher dimensions. Automorphisms of the causal order of the Minkowski space $\mathbb{R}^{1,n}$ for $n > 1$ are precisely the Lorenz transformations, by a famous theorem of Alexandrov and Zeeman. In this sense, the structure of the continuum as a set of nested sequences of intervals (which would correspond to $n = 1$) seems to be fundamentally different from a higher-dimensional analog: the Alexandrov-Zeeman theorem does not hold for $n = 1$, as there are nonlinear bijections $\mathbb{R} \to \mathbb{R}$ that preserve interval order.

References

[1] Benz, W. *Classical Geometries in Modern Contexts.* Birkhäuser: 2005.

[2] Brightwell, G., Winkler, P. 'Sphere Orders.' *Order* **6** (1989) 235–240.

[3] Hogarth, M. 'Non-Turing Computers are the New Non-Euclidean Geometries.' *International Journal of Unconventional Computation* **5**(4) (2009) 277–291.

[4] Martin, K., Panangaden, P. 'Domain Theory and General Relativity.' In: Coecke, B. (ed) *New Structures for Physics.* Lecture Notes in Physics, vol 813. Springer: 2010.

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

Interpreting Sequent Calculus Proofs as Functions

Henry Towsner [1]

[1] *University of Pennsylvania*
David Rittenhouse Laboratories, 209 South 33rd Street, Philadelphia, PA 19104-6395
E-mail: [1]htowsner@gmail.com

Keywords:
Cut Elimination, Ordinal Analysis

Many natural functions on proofs—in particular, the cut-elimination operations—can be viewed as continuous functions on proofs[2]. We show how these functions can be written as ill-founded proof-trees in a suitable version of the sequent calculus.

For instance, consider the $\wedge$-inversion operation which inverts a proof of $\phi \wedge \psi$ to a proof of ϕ—that is, the function that transforms a proof of $\Rightarrow \Gamma$ to a proof of $\Rightarrow (\Gamma \setminus \{\phi \wedge \psi\}), \phi$. (We focus on a one-sided sequent calculus for notational convenience.) It can be represented, in our version of the sequent calculus, by a proof of the sequent

$$\Rightarrow [\phi \wedge \psi]^{\langle\rangle}, \phi$$

where the "tagged sequent" $[\phi \wedge \psi]^{\langle\rangle}$ indicates that this is a function which expects to take as input a proof, begins reading that proof from the conclusion (the position $\langle\rangle$), and that the function will modify the conclusion of its input as expected, removing $\phi \wedge \psi$ and adding ϕ. (Note that the tag $\cdot^{\langle\rangle}$ serves two purposes—it indicates that we should view the tagged sequent as being negated, and also tells us which part of the input proof our function depends on.)

The crucial technical tool is the "Read rule". Viewed from the bottom to the top, we can think of this rule as describing the process "read the input proof at some position ϵ and branch based on what rule we see there". For a theory $\mathfrak{T}$, this rule is:

$$\frac{\Rightarrow \Sigma, \Gamma(\mathcal{R}) \setminus \Gamma_0, \{[\Gamma_0]^{\epsilon\iota} \mid \iota \text{ is a premise of } \mathcal{R}\} \qquad (\mathcal{R} \in \mathfrak{T})}{\Rightarrow \Sigma, \Gamma(\epsilon) \setminus \Gamma_0, [\Gamma_0]^{\epsilon}} \text{Read}^{\mathfrak{T}}$$

where ϵ is some position in an input proof (that is, a finite path starting at the root and leading, through the premises of rules in $\mathfrak{T}$, to a position in the proof), $\Gamma(\epsilon) \Rightarrow \Sigma(\epsilon)$ is the premise sequent of the top-most rule in ϵ, and $\Gamma(\mathcal{R}) \Rightarrow \Sigma(\mathcal{R})$ is the conclusion of $\mathcal{R}$.

With careful reading, this rule says exactly what it ought to. The conclusion tells us we have obtained a function which takes as an input a proof d for which ϵ describes a valid path from the root, and depends only on the part of the proof above ϵ. In order to produce such a function, we need a case telling us what to do for each possible rule that could appear at position ϵ; in the case where we see the rule $\mathcal{R}$, we are permitted to use as inputs the proofs above $\epsilon\iota$ for every premise ι of $\mathcal{R}$.

These functions are naturally ill-founded, but it makes sense to impose a different sort of well-foundedness condition, namely that they map well-founded proofs to well-founded proofs.

This is a general scheme which we can use to replace introduction rules: instead of proving ϕ in any sort of direct way, we can use the rule

$$\frac{\Rightarrow \Sigma, [\neg\phi]^{\langle\rangle}}{\Rightarrow \Sigma, \phi}$$

This rule says "in order to prove ϕ, it suffices to have a function which removes $\neg\phi$ from a proof".

This is particularly useful in the context of second order arithmetic. Buchholz gave an ordinal analysis of the theory of Π^1_1-comprehension[1, 3] using the Ω rule:

$$\frac{\Rightarrow \Sigma, \Gamma \qquad \text{(a branch for each proof of } \Rightarrow \Gamma, \neg\phi(X))}{\Rightarrow \Sigma, \exists^2 X\, \phi(X)}\ \Omega$$

This rule justifies introducing $\exists^2 X\, \phi(X)$ with the *graph* of a function transforming proofs of $\Rightarrow \Sigma, \neg\phi(X)$ into proofs of $\Rightarrow \Sigma$.

Using the Read rule, we can instead justify $\exists^2 X\, \phi(X)$ using the *algorithm* for this function, represented as an ill-founded sequent calculus proof. Using this method, we are able to give an ordinal analysis for full second-order arithmetic.

Acknowledgment

The research reported in the paper is partly supported by NSF grant DMS-2054379.

References

[1] Buchholz, W. "Eine Erweiterung der Schnitteliminationsmethode Habilitationsschrift, Universität München", 1977.

[2] Mints, G.E. "Finite investigations of transfinite derivations", *Journal of Soviet Mathematics 10.4 (Oct 1978), pp. 548–596.*

[3] Buchholz, W. and Schütte, K. Proof theory of impredicative subsystems of analysis*. Vol. 2. Studies in Proof Theory, 1988.*

Discovering Aristotle's Syllogistic via indirect proofs: a metatheoretical account

Karol Wapniarski [1], Mariusz Urbański [2]

[1,2] *Adam Mickiewicz University, Poznań, Poland*

E-mail: [1] `wapniarski.karol@gmail.com`, [2] `murbansk@amu.edu.pl`

Keywords:
Aristotle, Syllogistic, syllogistic reduction, indirect proof, Dictum de omni et nullo.

1 Introduction

The history of the search for a minimal set of inference rules for syllogistic reasoning starts already with Aristotle. One of the metatheorems he proves in *Prior Analytics*, later referred to as the *Dictum de omni et nullo*, states that all syllogistic deductions (resp. moods) can ultimately be reduced to the two universal deductions in the First Figure: *Barbara* and *Celarent* [3] (we follow the mnemonic names as given in [3]). The purpose of our talk is to present different possible minimal sets of inference rules necessary to prove all the twenty-four valid Aristotelian syllogistic moods using the indirect-proof method, thus giving a novel matatheoretical view of Syllogistic.

In the talk, we shall first present all the alternative direct proofs which are possible for each mood and which are not present in Aristotle. This will give us an opportunity to combine them with the other results at the end. Then, we shall consider what is the greatest reduction one can achieve when proving the syllogisms indirectly, that is, by showing that assuming the conclusion of a syllogism to be false leads to a contradiction between the negated conclusion and one of the syllogism's premises [2]. The question we shall answer is whether, when proved indirectly, syllogisms behave the same way and, consequently, whether Aristotle was right and his reduction holds for indirect proofs as well.

2 Our method

Aristotle uses the indirect-proof method only to prove moods which are not provable directly, that is: *Baroco* and *Bocardo* (for example in 27a36-b1) [1]. To answer our research question, we shall in turn use the indirect-proof method to prove each syllogistic mood in every possible way. An example syllogistic mood used to demonstrate the indirect-proof method working will be *Cesaro*. The four different sets of single-premise inference rules we shall consider are the ones containing:

1. Subalternation and conversion,
2. Conversion-only,
3. Subalternation-only,
4. No single-premise inference rule (null-set).

The results for each set will then be shown as a 24x24 Chart containing every possible pair of moods, with the cases in which one mood can be proved by another being marked in color (all the Charts are presented in [4]).

Considering the Charts, we shall make some claims regarding both the differences in the results between our different sets of single-premise inference rules and the results of the subalternation and conversion set, as it will prove to be the most interesting one.

3 Results

Our claims for the subalternation and conversion set will be that the syllogisms can be divided into groups based on the fact that they can prove and be proved by the same set of moods. Three main groups are the C Group, containing *Celarent*, *Cesare*, *Camestres*, and *Camenes*; the D Group, containing *Darii*, *Disamis*, *Datisi*, and *Dimaris*; and the F Group, containing *Ferio*, *Festino*, *Ferison*, and *Fresison*. Apart from those, we will identify minor groups containing two or three syllogisms and show various relationships between those groups.

Regarding the differences between sets, we will show that in the null-set and subalternation-only scenarios, neither the First nor the Second or the Third Syllogistic Figure is enough to prove all the moods by itself (i.e. **Aristotelian reduction does not hold**). In the case of conversion and conversion with subalternation scenarios, Aristotle's reduction to *Celarent* and *Barbara* will be shown to hold. However, in the conversion-only scenario, there shall be no substantial difference between taking *Celarent* and any other mood from the C or F Group (described in the previous paragraph). In the conversion with subalternation scenario, in turn, *Barbara* and *Calarent* can be replaced by *Baroco* and any other syllogism from the F Group.

4 Direct plus indirect

Finally, we shall combine the results obtained in previous Section with all the possible direct-proof cases shown before and thus consider all the possible proof cases one can have in Syllogistic. In this scenario, we will show that an even greater amount of moods can be grouped together according to the reductions one can make by the use of them. If we are to next reduce the Chart (i.e. leave only one representative mood of each group), we shall obtain four different possible reduction behaviors: the *Barbara*-*Baroco*-*Bocardo* Group, the C, D, and F Groups further grouped together, the Subalternated (S) Group, and the *Celaront*-*Cesaro*-*Darapti* (SII) Group, essentially dividing all the moods into four different sets, different from the usual Syllogistic Figures:

	B Group	C, D, F Group	S Group	SII Group
B Group				
C, D, F Group				
S Group				
SII Group				

Table 1: Final reduction

In this scenario, as the last two of the identified Groups can be reduced to the first two, the ultimately irreducible moods (i.e. the counterpart of Aristotelian *Dictum*) need not to be *Barbara* and *Celarent*, but can be any pair combining one mood from the B Group and one mood from the combined C, D, F Group. In this way, we can see that when the indirect-proof methot is applied to its' full extent, the metatheoretical structure of Syllogistic can be completely reorganized and proves to be different from the one proposed by Aristotle.

References

[1] Aristotle, *Prior Analytics* (R. S. Hackett, Trans.), 1989.

[2] Dyckhoff, R. *Indirect Proof and Inversions of Syllogisms*. The Bulletin of Symbolic Logic, 25(2): 196–207, 2019. `doi:10.1017/bsl.2018.59`.

[3] Smith, R., *Aristotle's Logic*, The Stanford Encyclopedia of Philosophy, First published Sat Mar 18, 2000; substantive revision Tue Nov 22, 2022, Edward N. Zalta and Uri Nodelman (eds.). `https://plato.stanford.edu/archives/win2022/entries/aristotle-logic/`.

[4] Wapniarski, K., Urbański, M., *Aristotelian Syllogistic more apagogico demonstrata: identifying minimal sets of inference rules for indirectly proving all the syllogistic moods*, 2024. [Manuscript submitted for publication in *Logica Universalis*]

Understanding the computation at the core of exchange on a trading venue

Dragiša Žunić

Institute for Artificial Intelligence R&D of Serbia
Fruškogorska 1, 21000 Novi Sad, Serbia
E-mail: dragisa.zunic@ivi.ac.rs

Keywords:

market design, market microstructure, linear logic, logical frameworks, core of exchange, regulatory compliance, symbolic ai

Trading venues, commonly known as financial exchanges, are a cornerstone system of finance and represent platforms where buyers and sellers come together to trade various financial instruments (stocks, bonds, commodities, currencies, derivatives, etc.). The computational core of exchange manages the interaction between buy and sell orders.

The challenge in designing the exchange core that guides the interaction of supply and demand lies in ensuring it meets various criteria, including regulatory requirements. This becomes a challenge for industry, especially since this is a system with infinite state space.

We present the sequential core, where orders are matched and processed in one-by-one fashion, which is still in use in modern electronic markets (somewhat surprising as the nature of exchange-on-a-trading-venue is rather parallel and even concurrent). This research is presented in [1] as a formalization in a Concurrent Logical Framework, CLF [2].

Using this formalization we were able to prove two standard properties of a market operating under these rules. First, we demonstrated that at any given state, the bid price is always lower than the ask price, ensuring the market is never in a locked or crossed state. Secondly, we proved that trades always occur at either the bid price (best available offer to buy) or the ask price (best available offer to sell).

We will discuss approaches towards designing a new model, from the ground up, that better aligns with the nature of the exchange-on-a-trading-venue operation. Perhaps we can also obtain a preliminary understanding of the decentralized market model (important for DeFi).

Since we address a possible innovation on the side of finance (the domain of fundamental market design and continuous double auctions), a closely related economics research can be found in [3, 4]. Another related work on applications of logic-based formal methods in fixing the electronic markets is [5].

This talk is in good part based on [1], a joint research with Iliano Cervesato, Giselle Reis and Sharjeel Khan.

References

[1] I. Cervesato, G. Reis, S. Khan and D. Žunić, *Formalization of Automated Trading Systems in a Concurrent Linear Framework*, In Proceedings of Linearity & TLLA, Oxford, UK, 2018. EPTCS 292(1):1–14 (2019). `https://doi.org/10.4204/EPTCS.292.1`

[2] I. Cervesato, K. Watkins, F. Pfenning and D. Walker, *A Concurrent Logical Framework I: Judgements and Properties*. Technical Report CMU-CS-02-101, CMU, 2003.

[3] E. Budish, P. Crampton and J. Shim: *The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response*, Quarterly Journal of Economics 130(4):1547–1621 (2015).

[4] M. Aquilina, E. Budish and P. O'Neill, *Quantifying the High-Frequency Trading "Arms Race"*, The Quarterly Journal of Economics, 137(1):493–564 (2022).

[5] D. Ignatovich and G. O. Passmore, *Case Study: 2015 SEC Fine Against UBS ATS*, Aesthetic Integration (now Imandra), Ltd., Technical Whitepaper, 2015.