CIBD 2024

Workshop on Theory and Applications of Craig Interpolation and Beth Definability

Amsterdam, The Netherlands
April 22-23, 2024

Book of Abstracts

Balder ten Cate · Patrick Koopmann · Christoph Wernhard · Frank Wolter
(Eds.)

Organizers

Balder ten Cate	University of Amsterdam, The Netherlands
Patrick Koopmann	Vrije Universiteit Amsterdam, The Netherlands
Christoph Wernhard	University of Potsdam, Germany
Frank Wolter	University of Liverpool, UK

Preface

This volume contains the abstracts of the presentations at the first *Workshop on Theory and Applications of Craig Interpolation and Beth Definability (CIBD 2024)*, held April 22–23, 2024, in Amsterdam, the Netherlands. The particular aim of the workshop was to bring together experts from different research communities – such as proof theory, model theory, proof complexity, verification, database theory, knowledge representation, automated reasoning, automata theory, philosophy, and linguistics – in order to discuss and disseminate recent and ongoing research pertaining to Craig interpolation and Beth definability. The program of CIBD 2024 was centered around six invited talks by leading researchers presenting recent work:

- Michael Benedikt: *Nested Relations, Beth's theorem, and Gaifman Coordinitisation*
- Rahaleh Jalali: *Is Every Interpolation Procedure Complete?*
- Jean Christoph Jung: *Living without Beth and Craig: Interpolant and Definition Existence in Decidable Fragments of First-Order Logic*
- George Metcalfe: *Uniform Interpolation: An Algebraic Perspective*
- Thomas Place: *The Separation Problem in Automata Theory*
- Philipp Rümmer: *Craig Interpolation in SMT: A Survey*

These invited talks were complemented by nine contributed presentations, based on the submissions for an open call for contributions.

We would like to thank all those involved for their high-quality contributions – in particular, the invited speakers, the authors of submitted contributions, the participants, and also the supportive administrations at University of Amsterdam and University of Potsdam.

The workshop was supported by a grant from the Evert Willem Beth Foundation and funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 457292495.

April 2024

Balder ten Cate
Patrick Koopmann
Christoph Wernhard
Frank Wolter

Contents

Invited Talks

Contributed Presentations

Nested Relations, Beth's theorem, and Gaifman Coordinitisation

Michael Benedikt

University of Oxford, UK

Nested relations are a data model built up from atomic scalar types by tuple-formers and set-formers. In database terms, one can have tables where the cells can contain tables. There is a standard language for transforming nested relations, the Nested Relational Calculus (NRC), said to be an analog of first order logic for nested relations. We find that there is a close connection between NRC and the Delta Zero formulas of set theory. In fact, our main results allow one to take any Delta Zero specification that defines a function from nested relations to nested relations and "compile it" into an NRC query.

One argument that one can perform this compilation goes via a variation of an unpublished result in model theory of Gaifman, dubbed "Gaifman's Coordinitisation theorem" by Hodges. We also have an effective/proof-theoretic version of this argument, using a variation of Craig Interpolation.

The talk will briefly review the connection between database query synthesis and effective Beth Definability results in the context of relational databases, and then discuss how the approach extends to nested relations. No database background will be required.

This is joint work with C. Pradic and C. Wernhard, appearing in POPL 2021 and PODS 2023. See: https://arxiv.org/abs/2212.03085

Is Every Interpolation Procedure Complete?

Raheleh Jalali

Czech Academy of Sciences, Czech Republic

Craig interpolation is a fundamental property of logic. The question of which interpolants can be obtained from an interpolation algorithm is of profound importance. Motivated by this question, we initiate the study of completeness properties of interpolation algorithms. Suppose a calculus G for propositional logic (for instance the propositional **LK**) and an interpolation procedure $\mathcal{I}$ (for example, the Maehara-style interpolation procedure) are given. We are interested in the power of the interpolation procedure with respect to the calculus. Stating the problem precisely: Let C be a (semantically possible) interpolant for a given tautology $A \to B$. Does there exist a proof π of $A \to B$ in G such that $\mathcal{I}(\pi)$ is logically equivalent to C? A positive answer to this question allows us to call the interpolation procedure $\mathcal{I}$ *complete* for G. If we take G to be the cut-free propositional **LK**, then the standard Maehara-style interpolation (call it M) fails to provide a positive answer to the question. Similarly, for propositional resolution and the standard algorithm to find the interpolant. However, if we take G to be the propositional **LK** with atomic cuts, then M is complete for G. This shows that to construct any possible interpolant via the Maehara-style interpolation procedure, using the cut rule is inevitable. What if we move to the realm of first-order logic? Then, obviously, M is incomplete for the cut-free first-order **LK**. Interestingly though, M for first-order **LK** with atomic cuts is also incomplete. This talk is based on a joint work with Stefan Hetzl.

Living without Beth and Craig: Interpolant and Definition Existence in Decidable Fragments of First-Order Logic

Jean Christoph Jung

TU Dortmund University, Germany

In logics enjoying the Craig interpolation property (CIP), an interpolant for two formulae φ, φ' exists iff $\varphi \to \varphi'$ is a tautology. Moreover, the proof of the CIP can often be modified to actually construct such an interpolant. Similarly, in logics enjoying the closely related projective Beth definability property (PDBP), an explicit definition of a relation exists iff a certain formula describes its implicit definability is valid. Thus, in logics enjoying CIP/PDBP, interpolant existence and explicit definition existence are reducible to validity.

In this talk, we will show recent progress on interpolant existence and explicit definition existence in logics lacking CIP and PDBP. We will cover both classical decidable fragments of first-order logics, namely the guarded and two-variable fragments, and certain extensions of modal and description logics, which are especially relevant in a knowledge representation context. In a nutshell, we show that in all these logics, the existence problems are decidable but by one exponent harder than validity.

This is joint work with Alessandro Artale, Andrea Mazzullo, Ana Ozaki, and Frank Wolter.

Uniform Interpolation: An Algebraic Perspective

George Metcalfe

University of Bern, Switzerland

Uniform interpolation, a more demanding version of Craig interpolation, is a property of consequence in logical systems that has intriguing connections to concepts from proof theory, universal algebra, and model theory. Notably, this property was established for intuitionistic propositional logic by Pitts via a proof-theoretic argument, and subsequently used by Ghilardi and Zawadowski to prove that the first-order theory of Heyting algebras has a model completion.

In the first part of the talk, I will explain how the well-known relationship between deductive interpolation and the algebraic property of amalgamation extends to an algebraic account of uniform deductive interpolation in terms of properties of compact congruences on free and finitely presented algebras. In particular, I will show that the missing extra ingredient for right uniform deductive interpolation corresponds to coherence, a widely-studied (e.g., for sheaves, rings, groups, and semigroups) algebraic property that was formulated in a model-theoretic setting by Wheeler in the 1970s.

In the second part of the talk, I will focus on failures of coherence (and hence uniform deductive interpolation), beginning with the case of the modal logic K — which does admit implicative uniform interpolation — then generalising to obtain a general criterion for failure that applies to broad families of modal and substructural logics. Time permitting, I will also explore the relationship of uniform deductive interpolation to the existence of model completions for corresponding first-order theories.

The Separation Problem in Automata Theory

Thomas Place

LaBRI, Bordeaux University, France

An important question within automata theory revolves around precisely understanding the natural classes of regular languages. Typically, we are intersted in the classes that can be defined by refining the common definitions of the regular languages, such as regular expressions, automata, monadic second-order logic, or finite monoids. However, the notion of "understanding a class" lacks precision as an objective. A standard approach to formalizing this goal is to seek an algorithm that decides membership for the investigated class: given a regular language as input, decide whether it belongs to the class. Rather than the procedure itself, the motivation is that obtaining such an algorithm requires a deep understanding of the class.

In the talk, I will survey this research area and offer an overview of the most significant related questions. In particular, I will discuss another more general decision problem called separation: given two regular languages L_1 and L_2, as input, decide whether there exists a third language that belongs to the investigated class, includes L_1, and is disjoint from L_2. Separation admits several natural formulations. In particular, it can be reframed as an interpolation problem: given two regular languages L_1 and L_2, as input, decide whether there exists a third language that belongs to the investigated class, includes L_1, and is included in L_2. The problem has garnered a lot of attention in automata theory for two primary reasons. Firstly, despite being more demanding, separation proves to be more rewarding than membership concerning the aforementioned objective of "understanding classes." Secondly, separation turned out to be a key ingredient for solving the most challenging membership questions.

This is joint work with Marc Zeitoun.

Craig Interpolation in SMT: A Survey

Philipp Rümmer

University of Regensburg, Germany

Due to the use and importance of Craig interpolation for verification, there are today various SMT solvers and theorem provers implementing interpolation procedures for propositional logic, first-order logic, or the theories commonly implemented in SMT solvers. In addition to the different logics and theories considered, those interpolation procedures also vary in terms of the supported kind of interpolation, and in terms of the guarantees they provide on generated interpolants. This talk will attempt to survey the methods designed and implemented in this context, and propose some dimensions along which those methods can be categorised. Along the way, some of the challenges related to Craig interpolation recognised in the verification field will be explained.

Towards Model Theory of Ordered Logics: Expressivity and Interpolation

Bartosz Bednarczyk[1,2]

[1] Computational Logic Group, Technische Universität Dresden, Germany
[2] Institute of Computer Science, University of Wrocław, Poland

We consider the family of guarded and unguarded ordered logics, that constitute a recently rediscovered family of decidable fragments of first-order logic (FO), in which the order of quantification of variables coincides with the order in which those variables appear as arguments of predicates. While the complexities of their satisfiability problems are now well-established, their model theory, however, is poorly understood. The research on this topic was initialized in in our MFCS 2022 paper [1] and the purpose of this talk is to present the main results obtained in that work.

We start by providing suitable notions of bisimulation for ordered logics. These bisimulations are then employed to compare the relative expressive power of ordered logics, and to characterise various ordered logics as bisimulation-invariant fragments of FO a la van Benthem. Having a suitable notion of bisimulation at hand, we also study the Craig Interpolation Property (CIP). We refute yet another claim from the infamous work by Purdy, by showing that the fluted and forward fragments do not enjoy CIP. We complement this result by showing that the ordered fragment and the guarded ordered logics enjoy CIP. These positive results rely on novel and quite general model constructions.

References

[1] Bartosz Bednarczyk and Reijo Jaakkola. Towards a Model Theory of Ordered Logics: Expressivity and Interpolation. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 15:1–15:14, 2022.

Split Interpolations

Quentin Blomet[1,2]

[1] École Normale Supérieure, France
[2] University of Greifswald, Germany

Which choice of truth tables and consequence relation for two logics **X** and **Y** guarantees that the following interpolation property holds true: If a formula A is classically satisfiable, a formula B is classically falsifiable, and A classically entails B, then there is a formula C sharing all its atoms with both A and B, such that A entails C in the logic **X** and C entails B in the logic **Y**? We answer this question for any two propositional logics based on the same three-valued Boolean normal monotonic scheme for the connectives and two (possibly identical) monotonic consequence relations. Since the resulting logics will be subclassical, any positive answer to the question must be seen as a particular fine-tuning of Craig's interpolation theorem.

Interpolation Properties for Array Theories: Positive and Negative Results

Silvio Ghilardi

Dipartimento di Matematica
Università degli Studi di Milano
Milano, Italy
silvio.ghilardi@unimi.it

In this talk, we shall first review basic correspondences [2] between syntactic interpolation properties of a first order theory (quantifier-free interpolation property, general quantifier-free interpolation property, uniform quantifier-free interpolation property) and semantic properties related to the class of its models (amalgamation, strong amalgamation, model completability).

Then we shall analyze these notions for variants of McCarthy extensional theory of arrays [5]. Whereas the basic theory does not have quantifier-free interpolation property, such property can be restored by adding it an extra symbol `diff` skolemizing the extensionality axiom [1]. General quantifier-free interpolation property also holds for this theory but not uniform quantifier-free interpolation property, as it can be shown by a counterexample.

Since the semantic content of `diff` operation is rather underspecified, we strenghten the theory by asking $\texttt{diff}(a, b)$ to return the maximum index where two arrays a,b differ [3] (`diff` returns 0 if they are equal). We also add to a unary 'length' operation. We so end up in a theory [4] still having quantifier-free interpolation, as witnessed by a hierarchic polynomial reduction to general interpolation for linear arithmetics. General quantifier free interpolation property may fail, but can be re-gained by introducing some constant arrays in the language.

The second part of this talk comes from joint work with A. Gianola, D. Kapur, C. Naso [4]. The first part of the talk reviews old joint work with R. Bruttomesso and S. Ranise [1, 2] and adds to such old work some recent achievements.

References

[1] Roberto Bruttomesso, Silvio Ghilardi, and Silvio Ranise. Quantifier-free interpolation of a theory of arrays. *Log. Methods Comput. Sci.*, 8(2), 2012.

[2] Roberto Bruttomesso, Silvio Ghilardi, and Silvio Ranise. Quantifier-free interpolation in combinations of equality interpolating theories. *ACM Trans. Comput. Log.*, 15(1):5:1–5:34, 2014.

[3] Silvio Ghilardi, Alessandro Gianola, and Deepak Kapur. Interpolation and amalgamation for arrays with maxdiff. In Stefan Kiefer and Christine Tasson, editors, *Foundations of Software Science and Computation Structures - 24th International Conference, FOSSACS 2021*, volume 12650 of *Lecture Notes in Computer Science*, pages 268–288. Springer, 2021.

[4] Silvio Ghilardi, Alessandro Gianola, Deepak Kapur, and Chiara Naso. Interpolation results for arrays with length and maxdiff. *ACM Trans. Comput. Log.*, 24(4):28:1–28:33, 2023.

[5] John McCarthy. Towards a Mathematical Science of Computation. In *IFIP Congress*, pages 21–28, 1962.

Uniform Interpolants and Bisimulation Quantifiers: Verified Constructions via Proof Systems

Iris van der Giessen*

University of Birmingham, Birmingham, UK
i.vandergiessen@bham.ac.uk

Uniform interpolation is a strong form of Craig interpolation, which says that propositional quantifiers can be defined inside the logic. Existing methods to prove uniform interpolation in propositional and modal logics can be divided, roughly, into two directions: one is syntactic and provides constructions of uniform interpolants via a well-behaved proof system for the logic (see e.g. [6]), the other is semantic and uses Kripke models to establish the existence of bisimulation quantifiers (see e.g. [3]).

I would like to discuss two current lines of research that evolve from these approaches.

1. The first line of research aims to formalize the proof-theoretic methods in Coq. It requires mechanising the interpolant construction ánd mechanising the syntactic proof that proves the correctness of the construction. This allows for automated and verified constructions of uniform interpolants (e.g. [2, 1]).

2. The second line of research provides a close connection between proof-theoretic and semantic approaches. Starting from a proof-theoretic construction, the aim is to provide a semantic correctness proof. In this way, the proof theory is used to explicitly construct bisimulation quantifiers (e.g. [4, 5]). Compared to current semantic methods, this, at least in theory, provides better bounds on the complexity of computing bisimulation quantifiers.

This talk is based on collaborations with Raheleh Jalali, Roman Kuznets, Hugo Férée, Sam van Gool, and Ian Shillito.

References

[1] Hugo Férée, Iris van der Giessen, Sam van Gool, and Ian Shillito. Mechanised uniform interpolation for modal logics K, GL and iSL, 2024. Preprint arXiv 2402.10494.

[2] Hugo Férée and Sam van Gool. Formalizing and computing propositional quantifiers. In *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2023, page 148–158. Association for Computing Machinery, 2023.

[3] Silvio Ghilardi and Marek Zawadowski. *Sheaves, Games, and Model Completions. A Categorical Approach to Nonclassical Propositional Logics*, volume 14 of *Trends in Logic Series*. Kluwer, 01 2002.

[4] Iris van der Giessen, Raheleh Jalali, and Roman Kuznets. Uniform interpolation via nested sequents. In Alexandra Silva, Renata Wassermann, and Ruy de Queiroz, editors, *Logic, Language, Information, and Computation, WoLLIC 2021*, volume 13038 of *LNCS*, pages 337–354, Cham, 2021. Springer International Publishing.

[5] Iris van der Giessen, Raheleh Jalali, and Roman Kuznets. Extensions of K5: Proof theory and uniform Lyndon interpolation. In Revantha Ramanayake and Josef Urban, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, pages 263–282, Cham, 2023. Springer Nature Switzerland.

[6] Andrew M. Pitts. On an interpretation of second order quantification in first order intuitionistic propositional logic. *The Journal of Symbolic Logic*, 57(1):33–52, 1992.

*This work was partially supported by a UKRI Future Leaders Fellowship, 'Structure vs Invariant in Proofs', project reference MR/S035540/1.

First Order Interpolation via Polyadic Spaces

Sam van Gool*

IRIF, Université Paris Cité, Paris, France

Interpolation theorems can often be proved, for propositional logics, by showing an amalgamation property for the corresponding class of algebraic structures. This methodology was used, for example, to identify the seven logics between intuitionistic and classical propositional logic that have interpolation [4]. Combining some ideas from [6] and [3], we show that a similar method can be used to prove interpolation for certain first order logics. To do so, we develop a Stone-type duality between intuitionistic hyperdoctrines, which are an 'algebraic' counterpart of first order intuitionistic logic, and a subclass of 'polyadic spaces'. We further show that the same proof goes through in a non-zero-dimensional setting, and deduce an analogue of Beth definability theorem. We may also comment on an open problem, for which we hoped that this method might be of help: whether or not predicate Gödel logic has interpolation (see e.g. [1]).

References

[1] Matthias Baaz, Mai Gehrke, and Sam van Gool. An interpolant in predicate Gödel logic. Preprint (2018). https://arxiv.org/pdf/1803.03003.pdf

[2] Sam van Gool and Jérémie Marquès. On duality and model theory for polyadic spaces. *Ann. Pure and Appl. Logic* **175** 103388 (2024). https://doi.org/10.1016/j.apal.2023.103388

[3] André Joyal. Polyadic spaces and elementary theories. *Notices of the AMS* 18.3 (1971), p. 563. https://www.ams.org/journals/notices/197104/197104FullIssue.pdf

[4] Larisa L. Maksimova. Interpolation Properties of Superintuitionistic Logics. *Studia Logica* **38** 419–428 (1979). https://link.springer.com/article/10.1007/BF00370479

[5] Jérémie Marquès. Categorical logic from the perspective of duality and compact ordered spaces. PhD Thesis, Université Nice Côte d'Azur (2023). https://jeremie-marques.name/papers/thesis.pdf

[6] Andrew M. Pitts. An application of open maps to categorical logic. *Journal of Pure and Applied Algebra* **29** 313-326 (1983).

*This abstract draws from recently published joint work with Jérémie Marquès [2], see also [5].

Synthesizing Strongly Equivalent Logic Programs: Beth Definability for Answer Set Programs via Craig Interpolation in First-Order Logic

Jan Heuer and Christoph Wernhard

University of Potsdam, Germany
jan.heuer,christoph.wernhard@uni-potsdam.de

We show a sensible form of projective Beth definability for the nonmonotonic framework of answer set programming under the stable model semantics [1]. In particular, it takes generalization of strong equivalence of logic programs [4] into account, a standard criterion to justify replacement of rules in a program while preserving its overall semantics. It is well known (e.g., [5, 2]) that strong equivalence of logic programs can be encoded as classical first-order equivalence, where each program predicate corresponds to two classical predicates, representing, intuitively, a logic with two possible worlds. As we show here, a classical formula that encodes a program can also be *decoded*, with the result program determined up to strong equivalence. Now Craig interpolation can be applied to two encoded programs, yielding after a simple postprocessing step an encoded program whose predicates are common to the two given programs. This variation of Craig interpolation then justifies projective Beth definability for logic programs: For given programs P, Q and vocabulary V (a set of predicates), the existence of a program R in V such that $P \cup R$ and $P \cup Q$ are strongly equivalent can be expressed as a classical first-order entailment. Effectivity, i.e., *construction* of R, is inherited from Craig interpolation applied to the two sides of the classical entailment, followed by the postprocessing and decoding. This is even practically implemented via Craig interpolation with first-order ATP systems [6, 7]. Craig-*Lyndon* interpolation as basis enhances control on the positions of predicate occurrences in the rules of R, e.g., head, body, positive or negated. For a full exposition see [3].

Acknowledgments. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 457292495.

References

[1] Michael Gelfond and Vladimir Lifschitz. The stable model semantics for logic programming. In *ICLP/SLP 1988*, pages 1070–1080, Cambridge, MA, 1988. MIT Press.

[2] Jan Heuer. Automated verification of equivalence properties in advanced logic programs. In *WLP 2023*, 2023. https://dbs.informatik.uni-halle.de/wlp2023/.

[3] Jan Heuer and Christoph Wernhard. Synthesizing strongly equivalent logic programs: Beth definability for answer set programs via Craig interpolation in first-order logic. In *IJCAR 2024*, LNCS (LNAI). Springer, 2024. To appear, preprint https://arxiv.org/abs/2402.07696.

[4] Vladimir Lifschitz, David Pearce, and Agustín Valverde. Strongly equivalent logic programs. *ACM Trans. Comp. Log.*, 2(4):526–541, 2001.

[5] Fangzhen Lin. Reducing strong equivalence of logic programs to entailment in classical propositional logic. In *KR-02*, pages 170–176. Morgan Kaufmann, 2002.

[6] Christoph Wernhard. Craig interpolation with clausal first-order tableaux. *J. Autom. Reasoning*, 65(5):647–690, 2021.

[7] Christoph Wernhard. Range-restricted and Horn interpolation through clausal tableaux. In *TABLEAUX 2023*, volume 14278 of *LNCS (LNAI)*, pages 3–23. Springer, 2023.

Uniform Guarded Fragments: Interpolation and Complexity

Reijo Jaakkola

Tampere University, Finland

The guarded fragment (GF) is a fragment of the first-order logic (FO) which generalizes the standard modal logic in a very natural way. GF behaves well both computationally and model-theoretically. In particular, it is decidable, it has a (generalized) treemodel property and it satisfies various preservation theorems. A well-known downside of the GF is that it does not enjoy the Craig interpolation property (CIP). This is somewhat surprising given that various modal logics are known to enjoy CIP.

The uniform one-dimensional fragment (UF1) — which was introduced in [1] — is a very natural polyadic extension of the two-variable fragment of FO. Roughly speaking, UF1 is obtained from FO by requiring that each maximal existential (or universal) block of quantifiers leaves at most one variable free and that when forming boolean combinations of formulas with more than one free variable, the formulas need to have exactly the same set of free variables. Formulas satisfying the first restriction are called one-dimensional, while formulas satisfying the second restriction are called uniform.

It was proved in [2] that the two-variable fragment of GF has CIP. Given that UF1 is a natural extension of the two-variable FO and that the two-variable GF has CIP, one might conjecture that also the guarded UF1 has CIP. As proved in [3], this turns out to be indeed the case. The main purpose of this talk is to sketch the proof of this result and to present simple examples which demonstrate that neither the one-dimensionality restriction nor the uniformity restriction can be relaxed. Since various modal logics can be embedded into the uniform one-dimensional GF, these results demonstrate that one-dimensionality and uniformity can be used to explain why GF does not have CIP while various modal logics do have it. Time permitting, we will also discuss issues related to the computational complexities of these fragments.

References

[1] Lauri Hella and Antti Kuusisto. One-dimensional fragment of first-order logic. In *Advances in Modal Logic*, 2014.

[2] Eva Hoogland and Maarten Marx. Interpolation and definability in guarded fragments. *Studia Logica*, 70(3):373–409, 2002.

[3] Reijo Jaakkola. Uniform guarded fragments. In *Foundations of Software Science and Computation Structures*, pages 409–427. Springer, 2022.

Craig-Lyndon interpolation as cut-introduction

Alexis Saurin

IRIF, CNRS, Université Paris Cité & INRIA
alexis.saurin@irif.fr

After Craig's seminal results on interpolation theorem [1], a number and variety of proof-techniques, be they semantical or proof-theoretical, have been designed to prove interpolation theorems. Among them, The proof-theoretic method due to Shoji Maheara [3] is notable due to its wide applicability to a range of logics admitting cut-free complete proof systems.

We reconsider Maehara's method and show how, by a close inspection of the proof, one can extract a "proof-relevant" interpolation for first-order linear-logic stated (in the one-sided sequent calculus) as follows, where $\mathcal{L}(\Gamma)$ denotes the set of relation symbols occurring in Γ:

Theorem 1. *Let Γ, Δ be lists of first-order* LL *formulas and $\pi \vdash \Gamma, \Delta$ be cut-free. There exists (i) a* LL *formula C such that $\mathcal{L}(C) \subseteq \mathcal{L}(\Gamma) \cap \mathcal{L}(\Delta)$ and (ii) two cut-free proofs π_1, π_2 of $\vdash \Gamma, C$ and $\vdash C^{\perp}, \Delta$ respectively such that*

$$\dfrac{\dfrac{\pi_1}{\vdash \Gamma, C} \quad \dfrac{\pi_2}{\vdash C^{\perp}, \Delta}}{\vdash \Gamma, \Delta}\ cut \quad \longrightarrow^{\star}_{\mathsf{cut}} \ \pi.$$

This theorem[1] states that if is possible to find an interpolant through which not only the logical entailment, but actually the logical arguments themselves, can be factored. Strickingly, this proof-relevant result is *almost* contained in most of the standard proof-theory textbooks (See references proof-theory books by Girard, Schütte, Takeuti or Troelstra & Schwichtenger for instance) – by this we mean that it is sufficient to write the proofs slightly more explicitly, taking care of the relations between the original cut-free proof and the interpolated proofs which are provided by the induction hypothesis – but none of them draw the point that interpolation can be achieved without changing the logical content of the proofs[2].

We then show that this can be decomposed in two phases: (i) a bottom-up phase which decorates the sequents with a splitting structure, until each axiom is equipped with such a splitting followed by (ii) a top-down phase which solves the interpolation problem, *synthesizing the interpolant by introducing cuts*. This reformulation allows to make explicit that the interpolation process can in fact be recasted as a cut-introduction process.

Depending on time remaining, we will then discuss various extensions of this approach: (i) first by considering extensions of the approach to other logical settings (classical and intuitionistic logics, or to the μ-calculus) and (ii) second by analyzing the computational content of our result and relating it with Čubrić' results for the simply typed λ-calculus.

References

[1] William Craig, *Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory*, ***Journal of Symbolic Logic***, vol. 22(3) (1957), pp. 269–285.

[2] Djordje Čubrić, *Results in categorical proof theory*, ***PhD thesis, McGill University***, 1993.

[3] Shoji Maehara, *On the interpolation theorem of Craig*, ***Sûgaku***, vol 12(4) 1960.

[1] Details are provided in an extended version [5].

[2] To the best of our knowledge, the only reference which made this connection between interpolation and cut-elimination is Čubrić PhD [2] and his subsequent paper which refined Prawitz' proof-theoretic proof of interpolation in natural deduction [4], for propositional minimal logic and expressing this in the λ-calculus.

[4] Dag Prawitz, ***Natural Deduction: A Proof-Theoretical Study***, Dover Publications, Mineola, N.Y., 1965.

[5] Alexis Saurin, ***Interpolation as cut introduction***, draft, 2024, www.irif.fr/_media/users/saurin/pub/interpolation_as_cut_introduction.pdf

Latticed Craig Interpolation with an Application to Probabilistic Verification

Mingqi Yang[1], Kevin Batz[2], Mingshuai Chen[1], Joost-Pieter Katoen[2], Zhiang Wu[3], and Jianwei Yin[1]

[1] Zhejiang University, Hangzhou, China
{mingqiyang,m.chen,zjuyjw}@zju.edu.cn
[2] RWTH Aachen University, Aachen, Germany
{kevin.batz,katoen}@cs.rwth-aachen.de
[3] University of Waterloo, Waterloo, Canada

Due to its inherent capability of local and modular reasoning, *Craig interpolation* serves as a pivotal tool in multiple formal verification techniques, e.g., model checking, theorem proving, and abstract interpretation. In model checking, for instance, the study of interpolation was pioneered by McMillan who proposed to augment SAT-based model checking with the ability to overapproximate the reachable state space via Craig interpolants, thus facilitating *unbounded* symbolic model checking [2]. In particular, Craig interpolation has proved useful in discovering *loop invariants* that are essential to program verification.

As an emerging paradigm, *probabilistic programming* – which describes stochastic models as executable and inferrable computer programs – has undergone a recent surge of interest due to prominent applications in, e.g., cryptography, approximate computing, machine learning, statistical data analysis, and beyond. Unlike verification of deterministic programs against *qualitative* properties, reasoning about probabilistic programs requires addressing various *quantities* such as expected values, assertion-violation probabilities, high-order moments, and expected runtimes. Computing these quantities amounts to inferring the quantitative (least) fixed point $\mathsf{lfp}\ \Phi$ of some monotonic operator Φ capturing the semantics of a possibly unbounded loopy program, which is in general highly intractable.

In this work, we are primarily concerned with the question: *Is Craig interpolation applicable to the automatic, quantitative verification of (infinite-state) probabilistic programs with potentially unbounded loops?* Our preliminary results indicate an affirmative answer:

- *Quantitative Craig interpolants.* We propose a quantitative version of Craig interpolants by extending predicates to expectations (expected values), which can be used to discover quantitative loop invariants that suffice to establish upper bounds on $\mathsf{lfp}\ \Phi$;
- *Latticed Craig interpolation.* We present latticed Craig interpolation by exploiting quantitative interpolants over complete lattices, which conservatively extends both McMillan's interpolation-based SAT model checking [2] (to the *quantitative* setting) and Batz et al.'s latticed bounded model checking [1] (to the *unbounded* case);
- *Soundness and Completeness.* We show that our latticed interpolation procedure is *sound* and establish sufficient conditions under which it is further *complete*.
- *Synthesizing quantitative interpolants.* We (semi-)automated our verification procedure by employing a counterexample-guided inductive synthesis framework to automatically generate quantitative interpolants. Our implementation shows promise: It finds invariants for non-trivial infinite-state programs with unbounded loops.

References

[1] K. Batz, M. Chen, B. L. Kaminski, J.-P. Katoen, C. Matheja, and P. Schröer. Latticed k-induction with an application to probabilistic programs. In *CAV (I)*, LNCS 12760, pages 524–549, 2021.

[2] K. L. McMillan. Interpolation and SAT-based model checking. In *CAV*, LNCS 2725, pages 1–13, 2003.