Algebra and Coalgebra
meet
Proof Theory

Bern, 27-29 April 2011

"Abstracts"

Schweizerische Mathematische Gesellschaft
Société Mathématique Suisse
Swiss Mathematical Society

UNIVERSITÄT BERN

Foreword

This booklet contains abstracts of the talks presented at ALCOP 2011 (Algebra and Coalgebra meet Proof Theory), held April 27-29, 2011 at the University of Bern, Switzerland. The workshop brings together experts in algebraic logic, coalgebraic logic, and proof theory with the goal of sharing new results and developing mutually beneficial relationships, serving both as the spring meeting of the Swiss Mathematical Society and as a sequel to ALCOP 2010 held at Imperial College London.

I would like to thank the Scientific Committee for their help and encouragement in planning the workshop: Nick Bezhanishvili (Imperial College London, UK), Laura Ciobanu (Fribourg University, Switzerland), Rosalie Iemhoff (Utrecht University, Netherlands), Clemens Kupke (Oxford University, UK), and Alessandra Palmigiano (University of Amsterdam, Netherlands). I am also very grateful to the members of the Organizing Committee for their much appreciated support and expertise: Leonardo Cabrer, Lukas Gerber, and Christoph Röthlisberger. Finally, I would like to thank our sponsors: the Swiss Doctoral Program in Mathematics, the Swiss Academy of Sciences, the Swiss National Science Foundation, the University of Bern, and the EU FP7 Program (Reintegration Grant 230889).

George Metcalfe

Bern, 25 April 2011

Index

Proof systems for Moss’ coalgebraic logic

Marta Bílková

(joint work with Alessandra Palmigiano and Yde Venema)

Department of Logic
Charles University – Prague

marta.bilkova@ff.cuni.cz

Moss’ coalgebraic language, based on a single “cover” modality nabla, provides an expressive language for set coalgebras of weak pullback and inclusion preserving functors. We consider the finitary version of Moss’ language with the nabla modality, its extension with a dual modality delta, and positive fragments of the two languages. We present uniform sound, complete, invertible and cut-free sequent calculi for such languages.

Blurring the line between proof and (probabilistic) computation

Alexandre Borovik

School of Mathematics
University of Manchester

alexandre.borovik@manchester.ac.uk

The talk will describe a peculiar and perhaps unique phenomenon in mathematics: the so-called “black box” probabilistic algorithms of computational group theory which, in their highly structured and sophisticated recursive setup, imitate inductive proofs of the classification of finite simple groups. Moreover, it will be shown how these probabilistic algorithms can be translated into proofs of “asymptotic” results about “sufficiently large” finite simple groups (for example, the celebrated Larsen-Pink Theorem). It appears that the “black box groups” theory is just a facet of a still unexplored area of probabilistic logic and probabilistic proofs.

Craig interpolation in displayable logics

James Brotherston

(joint work with Rajeev Goré)

Deptarment of Computing
Imperial College London

J.Brotherston@imperial.ac.uk

Craig interpolation of a logic is the property that, for any provable entailment $F \vdash G$ between formulas, one can find an "interpolant" formula I such that $F \vdash I$ and $I \vdash G$ are both provable and every nonlogical constant in I occurs in both F and G. This property is well known to be of practical importance in computer science as well as theoretical importance in logic.

Display logic, due to Belnap, is a general consecution framework à la Gentzen whose calculi are characterised by the availability of a "display-equivalence" relation on consecutions. Display-equivalence allows any consecution to be rearranged so that a selected substructure appears alone on the appropriate side of the proof turnstile. Aside from their theoretical elegance, the main appeal of display calculi is their very general cut-elimination theorem which relies on checking eight simple conditions on the proof rules. It has been shown that very many substructural and modal logics can be presented as a cut-free display calculus.

However, in contrast to the situation for sequent calculi, it has been open since their inception whether cut-free display calculi can be used to prove an interpolation result. In this talk we (partially) address that question by showing how to obtain Craig interpolation for a large class of cut-free display calculi.

The talk is based on a paper of the same name to appear at TABLEAUX 2011, a preliminary version of which can be found at:

http://www.doc.ic.ac.uk/ jbrother/TABLEAUX11/interpolation.pdf

Existentially definable sets

Laura Ciobanu

University of Fribourg

laura.ciobanu@unifr.ch

A set S in a free semigroup on generators $\{a, b\}$ is existentially definable if there exists an equation Σ such that S is the solution set of Σ. We will present a few results of Büchi and Senger on existentially definable sets, and show that, for example, the set $S = \{a^n b^n | n = 0, 1, \ldots\}$ is not existentially definable. We will then discuss the same questions in the context of free groups.

Algebras, simulation, and provable ordinals

Peter Hancock

Department of Computing and Information Sciences
University of Strathclyde

hancock@spamcop.net

To show that the provable ordinals of a system such as a type theory are closed under a certain function, one can sometimes show that the type structure is closed under a certain transformer of algebras. My idea is that there is some intriguing 'algebraic' structure implicit, if not buried away in the usual presentations of well-ordering proofs. My talk will try to illustrate this structure by reference to the lower foothills of the Veblen hierarchy.

An algebraic proof of the disjunction property

Rostislav Horčík

Institute of Computer Science
Academy of Sciences of the Czech Republic

horcik@cs.cas.cz

It turns out that the disjunction property (DP) is a sufficient condition for PSPACE-hardness of a substructural logic. By a substructural logic we mean any extension of Full Lambek Calculus. In our talk we will explain why the DP implies PSPACE-hardness. Moreover, we will present an algebraic method for proving the DP for a large class of substructural logics.

Optimal tableau algorithms for coalgebraic logics

Clemens Kupke
(joint work with R. Gore and D. Pattinson)

Department of Computing
Imperial College London

ckupke@doc.ic.ac.uk

Tableau methods provide a versatile tool for automated reasoning in modal and description logics. One drawback of tableau-based decision procedures is, however, that they often fail to meet the known complexity bounds for the logics in question. It has been shown that optimality can be obtained for some logics by using a technique called “global caching”. For example, global caching has been successfully applied in order to devise a tableau algorithm that decides in exponential time whether or not a formula of the description logic ALC is satisfiable with respect to a given finite set of global assumptions (a ‘TBox’ in the terminology of description logics). In my talk I am going to show that global caching is applicable to coalgebraic modal logics such as classical modal logic, graded modal logic, probabilistic modal logic and coalition logic. Furthermore I hope to be able to shed some light on the close connection between tableaux and automata for (coalgebraic) modal logics.

From shallow axioms to cut-free sequent systems

Björn Lellmann

Department of Computing
Imperial College London

b.lellmann10@doc.ic.ac.uk

Many systems of conditional logics or more generally coalgebraic modal logics are characterised syntactically by adding a finite set of shallow axioms (axioms of modal nesting depth one) to a Hilbert-style proof system for the propositional part of the logic. While this allows for relatively easy creations of logics from intuitions, from the perspective of automated reasoning Gentzen- or sequent-systems are preferable. In order to combine the strengths of both approaches we would therefore like to translate the axioms of the Hilbert-system into rules of a (preferably cut-free) sequent system. Unfortunately this translation quite often turns out to be a tedious and non-trivial task. This raises the question whether it is possible to automatise the process of translation in such a way that the resulting sequent system is cut-free and yields a decision procedure of good complexity. Of course the fact that there are undecidable logics axiomatized by axioms of modal nesting depth two suggests a limitation to axioms of nesting depth one. In this talk I will present results of ongoing research, which give a partial positive answer to this question.

Canonical proof nets for propositional classical logic

Richard McKinley

Theoretical Computer Science and Logic
University of Bern

mckinley@iam.unibe.ch

This talk describes my attempts to provide a convincing proof-net counterpart to proofs in the classical sequent calculus: by convincing, I mean that there should be a canonical function from sequent proofs to proof nets, it should be possible to check the correctness of a net in polynomial time, every correct net should be obtainable from a sequent calculus proof, and there should be a cut-elimination procedure which preserves correctness. A calculus of proof nets with all these properties has a strong case for giving the “underlying objects” described by sequent proofs.

Previous attempts to give proof-net-like objects have failed at least one of the above conditions; the calculus (expansion nets) that I will present satisfies all of them, but with respect to a novel one-sided sequent calculus with both additively and multiplicatively formulated disjunction rules; this calculus can be seen as describing a well-behaved “core” of the classical sequent calculus.

Stone type dualities in nominal sets

Daniela Petrisan

(joint work with Jamie Gabbay and Tadeusz Litak)

Department of Computer Science
University of Leicester

petrisan@mcs.le.ac.uk

Algebras over nominal sets model syntax with binding, and coalgebras over nominal sets model behaviour with names, including name-passing and dynamic allocation of names. We generalise a useful tool in coalgebraic logic – Stone type dualities – to the nominal setting:

- We consider distributive lattices and Boolean algebras internal in nominal sets;
- we introduce corresponding notions of nominal topologies; and
- we prove representation theorems.

The proofs are not straightforward, because nominal sets do not allow unrestricted use of Zorn's Lemma and the Axiom of Choice. We obtain our results via a previously developed technique which we used to prove a duality theorem for nominal Boolean algebras equipped with a name-restriction operation that can be thought of as the nominal 'New'-quantifier, and as dynamic allocation of fresh name.

MV-algebras and fuzzy topologies: Stone duality extended

Ciro Russo

Department of Mathematics
University of Salerno – Italy

cirusso@unisa.it

We introduce the concept of *MV-topology*, a generalization of general topology whose main features can be summarized as follows.

- The Boolean algebra $\{0,1\}^X$ of the subsets of the universe is replaced by the MV-algebra $[0,1]^X$ of the fuzzy subsets.
- Classical topological spaces are examples of MV-topological spaces.
- The algebraic structure of the family of open (fuzzy) subsets has a quantale reduct $\langle \Omega, \bigvee, \oplus, \mathbf{0} \rangle$, which replaces the classical sup-lattice $\langle \Omega, \bigvee, \mathbf{0} \rangle$, and an idempotent semiring one $\langle \Omega, \wedge, \odot, \mathbf{1} \rangle$ in place of the classical meet-semilattice $\langle \Omega, \wedge, \mathbf{1} \rangle$. Moreover, the lattice reduct $\langle \Omega, \bigvee, \wedge, \mathbf{0}, \mathbf{1} \rangle$ maintains the property of being a frame.
- The MV-algebraic negation * is, in the aforementioned classes of algebras, an isomorphism between the various structures of open subsets and the corresponding ones of closed subsets.
- A classical topology is canonically associated to each MV-topology. It is called the *shadow topology* and is obtained simply by restricting the family of open subsets to the crisp ones.

We suitably extend the concepts of compactness and separation to MV-topologies. Then — once denoted by $^{\mathrm{MV}}\mathbb{S}\mathrm{tone}$ the category of compact, separated and zero-dimensional MV-topological spaces, with MV-continuous functions, and by $\mathbb{MV}^{\mathrm{ss}}$ the one of semisimple MV-algebras with MV-algebra homomorphisms — we obtain a proper extension of Stone duality:

Theorem 1 *The mappings*

$$\begin{array}{lllllll} \Phi: & \mathbf{T} & \in & ^{\mathrm{MV}}\mathcal{T}\mathrm{op} & \longmapsto & \mathrm{Clop}\mathcal{T} & \in & \mathcal{MV}^{\mathrm{ss}} \\ \Psi: & A & \in & \mathcal{MV}^{\mathrm{ss}} & \longmapsto & \mathrm{Max}A & \in & ^{\mathrm{MV}}\mathcal{T}\mathrm{op} \end{array} \quad (1)$$

define two contravariant functors.

Moreover, they form a duality between $\mathcal{MV}^{\mathrm{ss}}$ *and* $^{\mathrm{MV}}\mathcal{S}\mathrm{tone}$ *whose restriction to Boolean algebras and classical topologies coincide with the classical Stone duality.*

Some algebra for (flat) modal fixpoint logics

Luigi Santocanale

(joint work with Yde Venema)

Laboratoire d'Informatique Fondamentale de Marseille
Centre de Mathématiques et Informatique

luigi.santocanale@cmi.univ-mrs.fr

In this talk I shall first define flat modal fixpoint logics : each such logic is a simple extension of modal logic K and a fragment of the modal μ-calculus. The question we address, and solve, is whether can we find a uniform axiomatization for all these logics – of course we demand these axiomatizations to be complete w.r.t. the standard Kripke semantics.

We shall present some ideas and tools – arising in different areas, algebra, coalgebra, category theory, proof theory – that have shown a key role in answering the previous question: the coalgebric cover modality, exhibiting duality within the syntax, pairs of generalized adjoint functions, constructive (i.e. well behaved) fixpoints, retracts.

Coalgebra and coalgebraic logic

Lutz Schröder

German Research Center for Artificial Intelligence - Bremen
University of Bremen

Lutz.Schroeder@dfki.de

Coalgebra has emerged as a unifying framework for generalized relational structures, seen, e.g., as reactive systems, epistemic structures, or collections of individuals. Examples include Kripke frames, Markov chains, concurrent game structures, preference structures, and many others. In this way, coalgebra provides a generic perspective on core notions such as bisimulation, coinduction, and corecursion. Moreover, it supports generic process calculi and generic logics. The latter can in particular take the shape of modal or hybrid logics. While coalgebraic logic in this sense was originally seen as a dedicated specification language for coalgebra, one can reverse this view and regard coalgebra as a generic semantics for a wide variety of modal and hybrid logics found in the literature. There is a well-developed meta-theory of coalgebraic logic that includes not only expressivity results and sound and complete generic axiomatizations, but also generic algorithms and complexity analyses. Computational coalgebraic logic thus serves as the basis for extensions of description logics and temporal logics with expressive means beyond the relational realm. In the present tutorial, we give an introduction to basic concepts of coalgebra and coalgebraic logic, as well as an outlook on current research in coalgebraic description logics.

On proof by infinite descent

Alex Simpson

Laboratory for Foundations of Computer Science (LFCS)
School of Informatics – University of Edinburgh

Alex.Simpson@ed.ac.uk

Fermat's method of proof by "infinite descent" is a useful proof technique in number theory. But if a number-theoretic proof is to be formalized in a standard logical theory for arithmetic (such as Peano Arithmetic) then the infinite descent argument has to be recast as a proof by induction. The talk will address the question: are all proofs by infinite descent reducible to proofs by induction?

To turn this into a mathematical question, it is first necessary to formalize the notion of proof by infinite descent. Under a naive formulation, the answer to the question is trivially positive. However, in the talk, I will present an interesting and natural combinatorial notion of proof by infinite descent for which the answer is not trivial.

This talk is partly based on joint work with Brotherston (Proc. LICS 2007, J. Logic and Computation 2010). But the talk will differ from this published work, of which no knowledge will be assumed, in focusing on arithmetic. Also, there will be new content.

Hierarchical reasoning in local theory extensions and combinations thereof

Viorica Sofronie-Stokkermans

Max-Planck-Institut für Informatik

sofronie@mpi-inf.mpg.de

Many problems in mathematics and computer science can be reduced to proving the satisfiability of conjunctions of literals in extensions and combinations of theories. It is therefore very important to identify situations where reasoning in complex theories can be done efficiently and accurately. Efficiency can be achieved for instance by:

(1) reducing the search space (preferably without losing completeness);
(2) modularity - i.e. delegating some proof tasks which refer to a specific theory to provers specialized in handling formulae of that theory.

Identifying situations where the search space can be controlled without loss of completeness is of utmost importance, especially in applications where efficient algorithms (in space, but also in time) are essential. To address this problem, very similar ideas occurred in various areas: proof theory, algebra and automated deduction:

1. **Proof theory:** Possibilities of restricting the search space in inference systems without loss of completeness were studied by McAllester and Givan [6] who introduced so-called “local inference systems” which have a certain subformula property which allows to control the search space (and guarantees that validity of ground Horn clauses can be checked in PTIME).
2. **Algebra:** Similar ideas also occurred in algebra; they were used by Skolem [9] to prove that the uniform word problem for lattices is decidable in PTIME and by Evans [4] in the study of classes of algebras with a PTIME decidable word problem, then generalized by Burris [2] who identified a criterion to recognize quasi-varieties for which the uniform word problem is decidable in PTIME.
3. **Automated deduction:** A link between (a certain version of) locality and saturation w.r.t. ordered resolution was established by Basin and Ganzinger [1]. In [5], Ganzinger established a link between the proof theoretic notion of locality and embeddability of partial into total algebras.

In [10], we showed that the notion of locality for Horn clauses can be extended to the more general notion of local extension of a base theory. In this context, as expected, locality allows to reduce the search space. We showed that, even nicer, in local theory extensions hierarchic reasoning is possible (i.e. proof tasks in the extension can be hierarchically reduced in PTIME - and with polynomial growth - to proof tasks w.r.t. the base theory). This allows to give parameterized complexity results for ground satisfiability w.r.t. such extensions. Many theories important for computer science or mathematics fall into this class (typical examples are theories of data structures, theories of free or monotone functions, but also various theories of functions important in mathematical analysis) (cf. [10,7,11,12,8,3]). Since in applications it is often necessary to consider complex extensions, in which various types of functions or data structures need to be taken into account at the same time, we present conditions under which locality is preserved when combining theories, and possibilities of efficient modular reasoning in such theory combinations. We present several examples of application domains where local theory extensions occur in a natural way.

Biblography

[1] D. Basin and H. Ganzinger. Automated complexity analysis based on ordered resolution. *Journal of the ACM*, 48(1):70–109, 2001.

[2] S. Burris. Polynomial time uniform word problems. *Mathematical Logic Quarterly*, 41:173–182, 1995.

[3] W. Damm, C. Ihlemann and V. Sofronie-Stokkermans. PTIME parametric verification of safety properties for reasonable linear hybrid automata. Mathematics in Computer Science. To appear.

[4] T. Evans. The word problem for abstract algebras. *J. London Math. Soc.*, 26:64–71, 1951.

[5] H. Ganzinger. Relating semantic and proof-theoretic concepts for polynomial time decidability of uniform word problems. *Proc. 16th IEEE Symposium on Logic in Computer Science (LICS'01)*, pages 81–92. IEEE Computer Society Press, 2001.

[6] R. Givan and D.A. McAllester. Polynomial-time computation via local inference relations. *ACM Transactions on Computational Logic*, 3(4):521–541, 2002.

[7] C. Ihlemann, S. Jacobs, and V. Sofronie-Stokkermans. On local reasoning in verification. *Proc. of TACAS 2008*, *LNCS 4963*, pp. 265–281. Springer, 2008.

[8] C. Ihlemann and V. Sofronie-Stokkermans. On hierarchical reasoning in combinations of theories. *Automated Reasoning, 5th International Joint Conference, IJCAR 2010*, *LNAI 6173*, pp. 30–45. Springer, 2010.

[9] T. Skolem. Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischen Sätze nebst einem Theoreme über dichte Mengen. *Skrifter utgit av Videnskabsselskapet i Kristiania, I. Matematisk-naturvidenskabelig klasse, 4*, pages 1–36, 1920.

[10] V. Sofronie-Stokkermans. Hierarchic reasoning in local theory extensions. *20th International Conference on Automated Deduction (CADE-20), LNAI 3632*, pages 219–234, 2005. Springer, 2005.

[11] V. Sofronie-Stokkermans. Efficient hierarchical reasoning about functions over numerical domains. In *KI 2008: Advances in Artificial Intelligence, LNAI 5243*, pages 135-143, Springer, 2008.

[12] V. Sofronie-Stokkermans. Locality results for certain extensions of theories with bridging functions. *Automated Deduction - CADE-22, 22nd International Conference on Automated Deduction*, *LNAI 5663*, pp. 67–83. Springer, 2009.

Deductive systems for common knowledge

Thomas Studer

University of Bern

tstuder@iam.unibe.ch

We present a survey of deductive systems for the logic of common knowledge. We study the proof-theoretic properties of those systems including the problem of syntactic cut-elimination. We also address the question of generalizing our results, say to systems for the modal μ-calculus. In the second part of the talk, we introduce a logic of common knowledge with justifications that allow us to express the reason why an agent knows something. Justification logics usually internalize their own notion of proof. We show how this is achieved in the case of common knowledge and we discuss the open question of the relationship between common knowledge with and without justifications.

Relation lifting for endofunctors of preorders, metric spaces, etc

Jiří Velebil

(joint work with Marta Bilkova, Alexander Kurz and Daniela Petrisan)

Czech Technical University in Prague

velebil@math.feld.cvut.cz

For the study of coalgebraic cover modality (Moss' nabla) it is essential that the extension of an endofunctor of sets to the category of relations is an honest functor. One characterisation of functoriality involves weak pullbacks.

We generalise the above result to endofunctors of preorders, metric spaces, etc. The technique we use is category theory enriched in a quantale and the resulting characterisation of functoriality then involves Guitart's exact squares rather than weak pullbacks.

We give examples of endofunctors allowing functorial lift and give a hint how the nabla modality looks like.