CIRM Conference 2319

Type Theory, Constructive Mathematics and Geometric Logic

1 – 5 May 2023

Abstracts

Sergei Artemov

Serial Properties and the Provability of Consistency

For Hilbert, the consistency of a formalized theory T is an infinite collection of claims "D does not contain a contradiction" with a parameter D ranging over derivations in T. Proving the consistency of T in a theory S, therefore, amounts to finding a finite proof in S of this infinite collection of claims.

The natural approach "first convert the consistency property of T to a single formula Con(T) and then test whether S proves Con(T)," is a priori inconclusive. Indeed, if S does not prove Con(T) then we can only claim that no finite fragment of S proves the consistency of T. The latter is weaker than the unprovability of consistency by means of S = PA, ZF, etc., since these theories are not finitely axiomatizable.

Hilbert himself viewed consistency proof as a pair containing

(i) an operation (which we suggest calling "selector") that given a derivation D produces evidence that D does not contain a contradiction and

(ii) a conventional proof (which we call "verifier") that the selector works for all inputs D.

We prove the consistency of PA in PA in the Hilbert format. Similar self-consistency proofs appear to work for all extensions of PA and ZF. These findings demolish the well-known "Unprovability of Consistency" paradigm and remove a major obstacle for Hilbert's consistency program.

Matthias Baaz

Constructivity within classical logic

In this lecture we describe a simple translation which describes constructive behaviour of quantifiers within classical logic. The soundness and completeness of this translation is based on the soundness and completeness of resolution calculus.

Ulrich Berger

Program Extraction for Higher-Order Logic

In Constructive Mathematics objects proven to exist can be constructed, proven disjunctions can be effectively decided, and proofs of implications or universally quantified statements give rise to (algorithms for) computable functions.

In other words, proofs in Constructive Mathematics have computational content.

The computational content of a proof can be viewed as a program that solves the problem expressed by the proven statement. Hence, one arrives at the notion of program extraction from proofs which is also known as the proofs-as-programs paradigm or the Curry-Howard correspondence. Technically, program extraction can be based on various forms of Kleene's realizability or Goedel's functional interpretation. Notable implementations of program extraction can be found in the type-theoretic systems Nuprl (Constable, 1986), Coq (Coquand, Huet, 1988), Agda (http://wiki.portal.chalmers.se/agda/), and the Minlog system (Schwichtenberg, LNAI 3600, 2006). The latter is based on intuitionistic finite type arithmetic with inductive and coinductive definitions .

This talk addresses two challenges one faces when pursuing program extraction:

(1) The formal system (which programs are to be extracted from) should be flexible and expressive enough to naturally capture relevant mathematical theories with interesting (from a programmer's point of view) computational content.

(2) Extracted programs should be free of garbage, that is, they should only compute and depend on data that are of interest to the user and necessary for the computation. For example, a recursive program on natural numbers should have as input only a natural number but not the proof that the recursion terminates.

(1) is addressed in Nuprl, Coq and Agda as these systems have great expressive power.

(2) is partly addressed in type theory through the concept of proof irrelevance.

However, through proof irrelevance garbage is not avoided but only compressed to one point. In contrast, the Minlog system and also the system IFP (Tsuiki, B.: Intuitionistic Fixed Point Logic, APAL 172 (3), 2021) truly avoid garbage.

In (Hou, B., MSCS 27 (8), 2017) a realizability interpretation of Church's Simple Type Theory, a formalization of higher-order logic, is given which addresses (1) but not (2). In this talk I will describe a refinement of this interpretation which is garbage free and hence addresses (1) and (2) simultaneously.

Ingo Blechschmidt
New modal operators for constructive mathematics

Let A be a commutative ring. Does it have a maximal ideal? Classically, Zorn's lemma would allow us to concoct such an ideal. Constructively, no such ideal needs to exist. However, even though no maximal ideal might exist in the standard domain of discourse, a maximal ideal always exists *somewhere*. This is because every ring is countable *somewhere*, and *everywhere*, countable rings have maximal ideals. Concrete computational consequences follow from this phantomic variant of existence.
The talk will introduce the modal operators "somewhere" and "everywhere", referring to the multiverse of parametrized mathematics, the multitude of computational forcing extensions. Just like the well-known double negation operator, they are (mostly) trivial from a classical point of view. Their purpose is to
(a) put established results in constructive algebra and constructive combinatorics into perspective,
(b) construct an origin story for certain inductive definitions and
(c) form a unified framework for certain techniques for extracting programs from classical proofs.
Our proposal is inspired by the study of the set-theoretic multiverse, but focuses less on exploring the range of set/topos-theoretic possibility and more on concrete applications in constructive mathematics. As guiding examples, we will examine algebraic closures of fields, Noetherian conditions on rings and the foundations of well-quasi orders such as Dickson's Lemma.
(joint work with Alexander Oldenziel)

Felix Cherubini, Thierry Coquand, Matthias Hutzler
A Foundation for Synthetic Algebraic Geometry

Algebraic geometry is the study of solutions of non-linear equations using methods from geometry. The basic objects in this classical theory are called affine schemes, where, informally, an affine scheme corresponds to a solution set of polynomial equations. We use homotopy type theory together with some axioms modeled by the Zariski-topos, to have an intuitive theory, where affine schemes are solution sets of polynomial equations. To get an analogue of the most important classical tool, cohomology of schemes, we use higher types (in the homotopy theoretic sense).

Anupam Das
Computational expressivity of (circular) proofs with fixed points

We study the computational expressivity of proof systems with fixed point operators, within the `proofs-as-programs' paradigm. We start with a calculus μLJ (due to Clairambault) that extends intuitionistic logic by least and greatest positive fixed points. Based in the sequent calculus, μLJ admits a standard extension to a `circular' calculus CμLJ.
Our main result is that, perhaps surprisingly, both μLJ and CμLJ represent the same first-order functions: those provably total in Π12-CA0, a subsystem of second-order arithmetic beyond the `big five' of reverse mathematics and one of the strongest theories for which we have an ordinal analysis (due to Rathjen). This solves various questions in the literature on the computational strength of (circular) proof systems with fixed points.
For the lower bound we give a realisability interpretation from an extension of Peano Arithmetic by fixed points that has been shown to be arithmetically equivalent to Π12-CA0 (due to Möllerfeld). For the upper bound we construct a novel computability model in order to give a totality argument for circular proofs with fixed points. In fact we formalise this argument itself within Π12-CA0 in order to obtain the tight bounds we are after.
Along the way we develop some novel reverse mathematics for the Knaster-Tarski fixed point theorem.
(j.w.w. Gianluca Curzi)

Tom de Jong, Fredrik Nordvall Forsberg
The set-theoretic and type-theoretic ordinals are the same

In constructive set theory, an ordinal is a hereditarily transitive set. In homotopy type theory, an ordinal is a type with a transitive, wellfounded, and extensional binary relation. These approaches to ordinals might seem quite different, but we show that the two definitions are equivalent if we use (a higher-inductive refinement of) Aczel's interpretation of constructive set theory into type theory. We also show how the notion of a type-theoretic ordinal can be generalised to capture all sets in Aczel's interpretation, and not just the ordinals. This leads to a natural class of ordered structures which contains the type-theoretic ordinals, and realizes the higher inductive interpretation of set theory in homotopy type theory.
This is joint work with Nicolai Kraus and Chuangjie Xu, and will appear at LICS this year. Preprint: https://arxiv.org/abs/2301.10696

Martin Escardó

Ordinals in HoTT/UF

We will discuss new and old facts about ordinals in HoTT/UF, in particular about the large ordinal of small ordinals.

Simon Henry

On Compact Haussdorf locales in (presheaf) toposes

(Joint work with Christopher Townsend) Informally, Compact Hausdorff locales can be thought of as being "dual" to sets through open-proper duality. I'll report on two new results that exhibit this dual behaviour in a more concrete way: The first one says that compact Hausdorf locales in a presheaf topos can be described very simply as just covariant functors from the indexing category to the category of compact Hausdroff spaces, the second one that compacts Hausdorff locales in an arbitrary Grothendieck topos are classified by a localic groupoid.

Joost J. Joosten

Formalised provability in constructive arithmetic

Provability logics describe the structural behaviour of what theories can prove about a specific formalised provability predicate. For a large class of classical theories that contain arithmetic the propositional modal provability logic is the same: Gödel-Löb's logic GL. Two classes of theories have resisted to having their corresponding provability logics revealed: weak arithmetics below Elementary Arithmetic on the one hand and constructive theories containing arithmetic on the other hand. Recently, Mojtaba Mojtahedi published a proof establishing an axiomatisation of the provability logic of Heyting Arithmetic (HA) and a proof that the thus axiomatised logic is decidable. In this talk we briefly comment on what makes the constructive setting so much more complex. Next we consider a simple fragment from joint work with Ana Borges, Dick de Jongh and Albert Visser: the strictly positive provability logic of HA where no nestings of implications are allowed. The fragment is much simpler than the full logic and even allows for a decidable generalisation to the quantified strictly positive provability logic of HA. The latter results should be contrasted with Vardanyan's theorem to the effect that the full quantified provability logic of Peano Arithmetic is Pi^0_2-complete.

Peter Lumsdaine

The cumulative hierarchy in type theory

TBA

Samuele Maschio

Implicative algebras, supercompactness and assemblies

Implicative algebras were introduced by A. Miquel to provide a common foundation for forcing and realizability interpretation of logical operators. In particular, every locale is an implicative algebra. In this talk we will show how some topological notions such as some kinds of compactness and connectedness can be generalized to implicative algebras and the role they play in relation with assemblies which can be defined from implicative triposes. Since, as shown by Miquel, every tripos over Set is isomorphic to one arising from an implicative algebra, such correspondence between topological notions and properties of assemblies can be applied to a very wide class of triposes including those arising from different variants of realizability.
This is a joint work with Davide Trotta.

Dale Miller

From axioms to synthetic inference rules via focusing

Gentzen's sequent calculus can be given additional structure via focusing. We illustrate how that additional structure can be used to construct synthetic inference rules. In particular, bipolar formulas (a slight generalization of geometric formulas) can be converted to such synthetic rules once polarity is assigned to the atomic formulas and some logical connectives. Since there is some flexibility in the assignment of polarity, a given formula might yield several different synthetic rules. It is also the case that cut-elimination immediately holds for these new inference rules. Such conversion of bipolar axioms to inference rules can be done in classical and intuitionistic logics.
This talk is based in part on a paper in the Annals of Pure and Applied Logic co-authored with Sonia Marin, Elaine Pimentel, and Marco Volpe (2022).

Takako Nemoto

On the decomposition of WKL!!

Constructive reverse mathematics aims to decompose mathematical theorems into choice principles and logical principles.
In this talk, we decompose a version of weak Koenig's lemma with a uniqueness condition called WKL!!.

Sara Negri

Gödel, Barr, and modal embeddings

Motivated by the idea that intuitionism expresses a modal notion of provability, Gödel defined in 1933 a translation of intuitionistic logic Int into the modal logic S4. He stated without proof the soundness of the translation and only conjectured its faithfulness. It took some years before McKinsey and Tarski proved the conjecture indirectly using algebraic semantics and completeness of S4 with respect to closure algebras and of intuitionistic logic with respect to Heyting algebras.

The result was later extended in various directions, most notably to embedding results for intermediate logics in modal logics between S4 and S5 by Dummett and Lemmon, and to the embeddings of Int into the provability logics GL and Grz of Gödel-Löb and of Grzegorczyk.

Unlike the proofs of soundness, the syntactical proofs of faithfulness of these embeddings are not entirely straightforward, as witnessed in section 9.2 of [4] for the relatively simple case of the embedding of Int into S4. In our earlier work we based our approach to such faithfulness results on the formulation of a cut-free sequent system for the logic that is the target of the embedding and offered a modular treatment by the use of labelled sequent calculi for intermediate logics into their modal companions [1, 2] and for infinitary logics [5].

It turned out, however, that Gödel's so far unknown work of 1941 in his book manuscript "Resultate Grundlagen" contains a proof of faithfulness of the translation of intuitionistic into modal logic [3]. The proof is purely syntactic and gives a converse to his translation of 1933 through a propositional version of Barr's theorem. Besides providing the topological semantics of modal logic, later used by McKinsey and Tarski to prove the same embedding result by semantic means, he obtained many other-at the time new-results by the topological semantics, among them that there is an infinity of inequivalent propositions in one variable in intuitionistic logic.

[1] Dyckhoff, R. and S. Negri. Proof analysis in intermediate propositional logics. Archive for Mathematical Logic, vol. 51, pp. 71–92, 2012.

[2] Dyckhoff, R. and S. Negri. A cut-free sequent system for Grzegorczyk logic with an application to the Gödel-McKinsey-Tarski embedding. Journal of Logic and Computation, vol. 26, pp. 169–187, 2016.

[3] Negri, S. and J. von Plato. Translation from modal to intuitionistic logic: Gödel's proof of his 1933 conjecture, ms.

[4] Troelstra, A. and H. Schwichtenberg. Basic Proof Theory. 2nd ed, Cambridge, 2000.

[5] Tesi, M. and S. Negri. Infinitary modal logic and the Gödel-McKinsey-Tarski embedding. Submitted.

Ming Ng

Foundations in Non-Archimedean & Arithmetic Geometry: Topology vs. Set Theory

In classical point-set topology, one defines a space by taking a set of elements before defining the topology on it in the usual way. By contrast, in locale theory, the basic unit for defining a space is not the underlying set of points but the opens. Topos theory extends this perspective, and says: a space is a universe whose points correspond to models of a geometric theory.

The differences between these perspectives brings into focus two key foundational questions: (i) What is the role of set theory in topology? (ii) What are the consequences of working classically, rather than intuitionistically?

This talk will discuss a couple of illustrating examples from recent work. The first example involves using point-free techniques to sharpen a foundational result in Berkovich geometry, showing that algebraic hypotheses imposed by the classical mathematician (e.g. requiring that the base field K be non-trivially valued) are sometimes in fact point-set hypotheses, and are thus inessential to the underlying mathematics. The second example, from joint work with Steve Vickers, involves classifying the places of Q via geometric logic. The big surprise is that, working geometrically, one discovers that the Archimedean place corresponds to a blurred unit interval — by contrast, the Archimedean place has always been classically regarded as a singleton (by number theorists). Aside from raising urgent questions for the foundations of arithmetic geometry, this result also illustrates an interesting moral: sometimes, working classically results in a serious loss of information that is only visible when looked at from the intuitionistic perspective.

Nicola Olivetti

A taste of Intuitionistic Modal Logic: normal and non-normal modalities

Modal extensions of intuitionistic logic have a long history going back to the work by Fitch in the 40'. Two traditions are now consolidated, called respectively Intuitionistic Modal Logic and Constructive Modal logic. In the former tradition originated by Fischer-Servi and then systematized by Simpson, the basic system is IK, whereas in the tradition of constructive modal logics the two basic systems are Wijesekera' systems WK and the system CK by Bellin et als. Constructive modal logic are non-normal modal logics. In the classical setting, non-normal modal logics have been studied for a long time for several purposes. The observation that constructive modal logics are non-normal and the interest in non-normal modalities in itself leads to the question: which are the intuitionistic analog of classical non-normal modal logic?

It turns out that the framework of intuitionistic non-normal modal logic is richer than the classical one. Similarly to classical non-normal modal logics, all systems of non-normal intuitionistic modal logic are characterized by a simple neighbourhood semantics. Moreover the neighbourhood semantics helps to understand also Constructive modal logics CK and WK, as it covers also these systems. The interest of the neighbourhood semantics for constructive modal logic can also be justified from a proof-theoretical perspective, as it witnessed by some unprovability calculi for these logics. In these calculi, each derivation precisely corresponds to one neighbourhood countermodel. This fact confirms the usefulness and the naturalness of neighbourhood semantics for analysing intuitionistic modal logics. [Joint work with Tiziano Dalmonte and Charles Grellois.]

Iosif Petrakis

From algebras of complemented subsets to swap algebras

Following [1], an equality and an inequality on a set X induce the positive notions of disjoint subsets and of complemented subsets of X. Complemented subsets are easier to handle than plain subsets, as their partial, characteristic functions are constructively defined and their complement, formed by swapping its components, behaves like the classical complement of a subset. Complemented subsets are crucial to the constructive reconstruction of the classical Daniell approach to measure theory. We explain why the pair of notions (complemented subsets, Boolean-valued partial functions) is the constructive analogue to the classical pair (subsets, Boolean-valued total functions). Following [2, 3], we introduce swap algebras of type (I) and (II) as an abstract version of Bishop's algebras of complemented subsets of type (I) and (II), respectively, and swap rings as an abstract version of the Boolean-valued partial functions on a set. We present several results indicating that the theory of swap algebras and swap rings is a generalisation of the theory of Boolean algebras and Boolean rings.

[1] E. Bishop, D. Bridges, Constructive Analysis, Springer-Verlag, 1985.

[2] I. Petrakis, D. Wessel: Algebras of complemented subsets, in U. Berger et.al. (Eds): Revolutions and Revelations in Computability, LNCS 13359, Springer, 2022, 246–258.

[3] I. Petrakis, D. Wessel: Complemented subsets and boolean-valued, partial functions, submitted to Computability, 2023.

Thomas Powell

Recursive inequalities in applied proof theory

Applied proof theory is an area of research that uses ideas and techniques from proof theory to produce new results in "mainstream" mathematics and computer science. While the field has historical roots in Hilbert's program, where it aligns with the much broader effort to give a computational meaning to mathematical proofs, its emergence as a powerful area of applied logic only started in the early 2000s with the research of Kohlenbach and his collaborators. This talk aims to accomplish two things. Firstly, I seek to give a brief overview of the main ideas behind applied proof theory without assuming any prior background in the area. Secondly, within this context, I want to present some recent results which have focused on abstract convergence properties of sequences of real numbers that satisfy certain recursive inequalities. I argue that recursive inequalities present us with a unifying framework for viewing many convergence proofs in the literature, and propose what I believe to be some fascinating possibilities for future work, involving stochastic convergence, computer formalized mathematics and automated reasoning.

Luigi Santocanale

Lifting structure(s) from the base to the total category of a predoctrine

A handy way of constructing new categories from a give category one is to consider the total SQ (or Grothendieck) category of a functor Q : C -> Pos (where Pos is the category of posets and order preserving functions). There is a canonical functor SQ -> C, we describe a general methodology to lift structure from C to SQ. The methodology applies to functors, monoidal (possibly closed) structures monads, algebras and coalgebras, monads, etc.

We give an exact description of what it means that C being a SMCC, SQ is also a SMCC, and the canonical functor preserves all the structure. In particular, it turns out that if Q is monoidal and factors through the category of complete lattice and sup-preserving functions, then SQ is always monoidal closed and the canonical functor preserves all this structure. We shall discuss on how this applies to various categories, such as the category of totality spaces and Schalk/de Paiva categories Q-Sets.

Andrew Swan

Oracle Modalities

Following up on Hyland's embedding of Turing degrees in the lattice of subtoposes of the effective topos, I give a formulation of Turing reducibility in terms of the Rijke-Shulman-Spitter notion of topological modality in homotopy type theory. This new formulation gives a promising new connection between computability theory, via Turing degrees and homotopy theory via homotopy type theory and higher modalities. In particular we can define the "homotopy group" of a Turing degree as an instance of a more general definition in modalities and use the HoTT approach to group theory to give a proof that two Turing degrees are equal as soon as they have isomorphic homotopy groups.

Steve Vickers

Dependent type theory of point-free topological spaces

In any elementary topos E, internal point-free spaces expressed in various forms (frames, formal topologies, propositional geometric theories ...) are equivalent to localic geometric morphisms to E. Moreover, this extends to sites and bounded geometric morphisms - which we call "bundles". Thus we may say internal generalized spaces in E are equivalent to bundles over E.

If E itself is a classifying topos S[T], then for each of its points (models of T) we have a space, the fibre. A point at stage F is a geometric morphism F -> E, equivalent to a model of T in F, and the bundle can be pulled back along it. Thus we get the bundle idea of an assignment of fibres to points. This then suggests a dependent type theory, type = (bounded S-)topos, element = point, dependent type = bundle.

Categorically much of this is banal. But it becomes more significant when we understand it logically: S[T] comprises what can be constructed geometrically out of the generic model of T, and an internal space is the *generic* construction point |-> fibre, specific instances being got by substitution. The type theory comes naturally if we can limit ourselves to geometric constructions, and topology will be intrinsic to it - "continuity = geometricity".

What is this dependent type theory of spaces? It does not drop cleanly out of the usual models of type-theory, as it has a number of unfamiliar properties. It cannot have function types or Π-types, so maps must be an explicit part of the machinery, not just elements of function type. The 2-cells (specialization order, homomorphisms between models) are important and not necessarily invertible, so the usual notion of identity type is inadequate. Universes exist, but of many kinds - eg universes of sets and of Stone spaces.

I shall present some of the mathematics that makes this work, and some of the issues that need to be addressed in making a decent type theory.

Background: Vickers "Generalized point-free space, pointwise", arXiv:2206.01113

Chuangjie Xu

From Double-Negation Translation of Proofs to Static Analysis of Code

Double-negation translations are a powerful approach for embedding classical logic into intuitionistic logic. The idea is to insert double negations into a classically valid formula to make the resulting formula intuitionistically valid. Such translations can be generalized by replacing double negation with a nucleus, an endofunction on formulas satisfying certain conditions.

This talk will explore how these proof translations can become term translations for Gödel's System T parametrized with a nucleus for types under the proofs-as-programs correspondence. By working with different nuclei, we can use the translations to reveal various properties of T-definable functionals, including majorizability, continuity, and bar recursion.

Moreover, we will demonstrate that this technique can be generalized further into a generic interpreter and applied to sophisticated programming languages. Specifically, we will show that a few static analysis tools for finding program bugs, such as taint analysis and symbolic execution, are instances of such a generic interpreter and thus are variants of Gentzen's double-negation translation.

Ihsen Yengui

The Gröbner Ring Conjecture

We discuss the problem of constructing Gröbner bases over valuation rings.