Programs from Proofs

University of Bath

September 15 – 16, 2025

Contents

`https://t-powell.github.io/pfp/index.html`

Welcome Address

This one-off workshop aims to bring together researchers from different backgrounds and traditions who share a common interest in the computational content of proofs. A particular focus will be on the application of ideas and techniques from proof theory to systematically extract this content, though the workshop will encompass both theory and application, and will cover research across pure mathematics, logic, theoretical computer science, and computer formalised mathematics.

Organisers
Davide Barbarossa, Thomas Powell

Local support
Ben Langton, Alex Wan

Outline of the workshop

The International Workshop on Programs from Proofs is held on the main campus of the University of Bath from 15th to 16th September 2025. The workshop takes place in person in the Department of Computer Science in the room 1W 2.104. The event is supported by the EPSRC grant Imperative Programs from Proofs and the Department of Computer Science at the University of Bath.

The program includes 12 talks from experts across pure mathematics, logic, theoretical computer science, and computer formalised mathematics and can be found at the back of this booklet, with abstracts for talks following this outline.

The list of participants will be compiled in the final version of this book of abstracts.

Name	Affiliation

Abstracts of Talks

Logical Aspects of Proof Mining and Recent Applications to Optimization, Ergodic Theory and Difference Inclusions

Ulrich Kohlenbach
Department of Mathematics, Technische Universität Darmstadt
kohlenbach@mathematik.tu-darmstadt.de

We discuss some of the logical features of the Proof Mining paradigm focusing on what sets this apart from areas such as computable analysis or program extractions. In the 2nd part of the talk we will mention some recent applications to nonsmooth optimization, ergodic theory and second-order accretive difference inclusions (partly joined work with N. Pischke, S. Saeidi and J. Treusch).

Realizability models for set theory

Laura Fontanella
University Paris Est Créteil
laura.fontanella@u-pec.fr

In the 19th century, mathematicians began to explore fundamental questions about the foundations of mathematics. This inquiry led to the development of formal logic, marked by a particular focus on axiomatic systems, from which set theory emerged as a solid foundation for all mathematics. Around the same time, the concept of computability was investigated in connection with the idea that mathematical proofs should be "computable." This line of inquiry gave rise to Kleene's realizability. In this talk, we will examine how these two research traditions are now converging in the field of classical realizability for set theory. We will explore the construction of models of ZF using lambda-terms and use this technique to investigate the computational content of set theory. We will present the current state of the art alongside several open problems in this area. In particular, we will show that while it is possible to realize even large cardinal axioms, the computational content of the Axiom of Choice remains elusive.

Π-types and Prejudice

Pierre-Marie Pédrot
Inria Rennes-Bretagne-Atlantique

In this talk, we will describe a Dialectica interpretation of Martin-Löf Type Theory in the Diller-Nahm style and in a syntactic way. This model includes all fancy features of dependent types such as dependent elimination and universes. In case the previous sentence made little sense to you, fear not! For the realizability-savvy audience, we will attempt to pedagogically emphasize the specificities of MLTT compared to more traditional post-hoc approaches. As a result, this talk is also a thinly veiled propaganda for dependent type theory. Finally, we will argue that our interpretation corresponds computationally to a generalization of graded types to a very expressive setting where annotations range over complex higher-order objects rather than just elements of a semiring.

Applications of proof mining for program extraction in Lean

Horațiu Cheval
Department of Computer Science, University of Bucharest
horatiu.cheval@unibuc.ro

In this talk, we explore how proof mining, a research program seeking to extract hidden computational content from ineffective mathematical proofs through an analysis guided by proof-theoretical techniques, can be combined with formalized mathematics, using the Lean theorem prover in particular. The main focus will be on implementing term extraction tools based on proof mining methods.

More specifically, the fundamental theoretical results of the field take the form of a series of general metatheorems, beginning with those proved by Kohlenbach in 2005, on the extractability of computable bounds from classes of ineffective proofs. While in practice these serve to guide the analysis and offer a theoretical explanation for the phenomena encountered, their constructive nature means that they can also be seen as providing program extraction algorithms.

We start by presenting a Lean formalization of the logical framework and metatheorems from proof mining. While the current implementation is a deep embedding, thus requiring the input proofs to be written from scratch in our logical system, we aim to develop tools that work natively on Lean proofs, taking advantage of Lean's extensive library of formal proofs, and we discuss some approaches to this end. Beyond automatic term extraction capabilities, we intend these tools to also assist in the analysis of formalized proofs, more closely resembling the day-to-day practice of proof mining. We will also discuss some preliminary investigations in this area.

Oscillations in the Laws of Large Numbers

Morenikeji Neri
Department of Mathematics, Technische Universität Darmstadt
neri@mathematik.tu-darmstadt.de

We introduce the concept of R-learnable rates of uniform convergence, which extend the earlier notion of learnable rates of uniform convergence developed with Powell (Trans. Amer. Math. Soc. Series B, 12:974–1019, 2025). That notion was established as a means of assigning computational interpretations to theorems in probability theory with nonconstructive proofs, and R-learnable rates refine it to capture further quantitative structure. We apply this new concept to analyse the oscillatory behavior of sample means in the Strong Law of Large Numbers and demonstrate how the resulting rates correspond to established quantitative results in ergodic theory. We conclude by highlighting open questions about the computational connections between quantitative notions from proof mining and those arising in ergodic theory.

On proof theoretic and quantitative aspects of stochastic processes

Thomas Powell
Department of Computer Science, University of Bath
trjp20@bath.ac.uk

In the first part of the talk, I give an overview of recent work on applications of proof theory in the theory of martingales and stochastic approximation. This includes a quantitative study of martingale convergence in its various forms, including the Robbins-Siegmund supermartingale convergence theorem, documented in a series of papers joint with Morenikeji Neri and Nicholas Pischke. In the second part, I briefly outline on ongoing project with Ben Langton on formalisation and automated reasoning in optimization.

Non-deterministic and Stochastic Selection Functions

Paulo Oliva
Queen Mary University of London
p.oliva@qmul.ac.uk

Selection functions can serve as a bridge between Proof Theory (interpretation of double negated formulas) and Game Theory (modelling of strategies). Given any monad T and a fixed type R, the type mapping $JTX = (X- > TR)- > TX$ is also a monad [1]. In recent work with Martín Escardó we explored the cases when

(1) T is the finite (non-empty) power-set monad and
(2) T is the distribution monad.

We showed that in the first case (1) the product of selection functions can be used to calculate all optimal plays in a sequential (higher-order) game, while in the second case (2) we can calculate optimal strategies even when playing against irrational (stochastic) players. In proof-theoretic terms (1) has been used to give a Herbrand functional interpretation to countable choice [1], while (2) could prove to be useful in the interpretation of proofs in Probability Theory.

References

[1] M. Escardoó, P. Oliva, The Herbrand Functional Interpretation of the Double Negation Shift, *The Journal of Symbolic Logic* **82**(2), pp. 590–607, 2017.

Proof Theory for Probabilistic Termination

Paolo Pistone
École Normale Supérieure de Lyon
paolo.pistone@ens-lyon.fr

Logic, and especially proof theory, have played an important role for understanding computation and programming. For example, formal proofs are largely employed today to certify sensitive properties of algorithms (will the algorithm meet its own specification in every context? Do two algorithms compute the same function?). However, while such applications of proof theory mostly pertain to deterministic programs, probabilistic programming and statistical inference methods have gained today a prominent position among the programming paradigms. The algorithms arising from such methods are not thought to meet some specification exactly, but only up to some probability, nor to compute some given function precisely, but only to approximate its values in an efficient way. In this talk I will discuss how ideas and methods from logic and proof theory, like the

Curry-Howard correspondence, can be adapted in order to certify properties of probabilistic functional programs. A particular focus will be put on establishing the probability that a program will terminate, as well as the probability that it will meet some target specification.

Classical realizability: characteristic Boolean algebras and nondeterminism

Guillaume Geoffroy

Université Paris Cité

guilaume.geoffroy@irif.fr

In Jean-Louis Krivine's version of realizability, each realizability model contains a "characteristic Boolean algebra". We discuss what is currently known in general about these algebras and what questions remain, as well as the connections between the characteristic Boolean algebra of a particular realizability model and the presence of nondeterminism in the underlying model of computation.

Recent progress in proof mining and probability theory

Nicholas Pischke

Department of Compuer Science, University of Bath

nnp39@bath.ac.uk

On the surface, the theory of probability measures requires the use of proof theoretically strong principles to already develop some of the most basic notions. Contrary to these apparent limitations, an approach for extending the program of proof mining to this area has recently been proposed. This approach, which is fundamentally based on the use of probability contents (i.e., finitely additive [0, 1]-valued functions defined on algebras of sets), has proven to be widely effective based on a range of new case studies presented in the last year. In this talk, we sketch recent theoretical results based on a novel use of the outer measure which augment this previous work by providing a structured approach towards recognizing wide classes of almost-sure statements as actual formal statements in the language of the underlying theory. Concretely, a special case of our results yields a translation that maps any formula "F" to a formula "F a.s" which represents that F holds with probability one. This translation, if chained with the previously developed bound extraction theorems, provides a uniform and systematic view on the computational content of probabilistic statements which moreover reproduces a range of established quantitative variants of well-known notions from probability theory, like almost sure infinitely often and convergence statements. This is joint work with Paulo Oliva and Morenikeji Neri.

On the computational expressivity of type systems with fixed points

Anupam Das
School of Computer Science, University of Birmingham
a.das@bham.ac.uk

We study the computational expressivity of proof systems with fixed point operators, within the 'proofs-as-programs' paradigm. We start with a calculus muLJ that extends intuitionistic logic by least and greatest positive fixed points. Based in the sequent calculus, muLJ admits a standard extension to a 'circular' calculus CmuLJ. Our main result is that, perhaps surprisingly, both muLJ and CmuLJ represent the same first-order functions: those provably total in Pi12-CA0, a subsystem of second-order arithmetic far 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; the latter has been shown to be arithmetically equivalent to Pi12-CA0 by 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 must formalise this argument itself within Pi12-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.

This talk is based on joint work with Gianluca Curzi:

Conference: `https://ieeexplore.ieee.org/document/10175772`
Preprint: `https://arxiv.org/abs/2302.14825`

Dialectica realisers and Hoare Logic

Davide Barbarossa
Department of Computer Science, University of Bath
db2437@bath.ac.uk

I will present in this talk some recent work and work in progress (joint with Thomas Powell) about the structure of Dialectica realisers. In particular, we notice an analogy between a judgment stating the adequacy of a Dialectica realiser and Hoare triples in program logics. We think therefore of Dialectica as a specific program logic system for certain programs, which crucially have both a forward and a backward component. I will show that this perspective is compatible with the addition of a while constructor, which appears natural in the proof mining of classical proofs. Finally, I will address the problem of approaching Dialectica from an imperative paradigm perspective, which seems possible and interesting: for instance, the big-step semantics of (some) forward+backward realisers performs a backpropagation procedure.

Program

	Monday	Tuesday
0900 - 0930	Arrival and welcome	
0930 - 1020	**Kohlenbach**	**Oliva**
1020 - 1050	Coffee and discussion	
1050 - 1140	**Fontanella**	**Pistone**
1140 - 1230	**Pedrot**	**Geoffroy**
1230 - 1410	Lunch	
1410 - 1500	**Cheval**	**Pischke**
1500 - 1550	**Neri**	**Das**
1550 - 1620	Coffee and discussion	
1620 - 1710	**Powell**	**Barbarossa**
1830 -	Workshop dinner	Informal plans