

# Mathematical Foundations Seminars

Seminar series of the Mathematical Foundations group at the University of Bath.

Organisers: [Willem Heijltjes](#) and [Giulio Guerrieri](#)  
Email us to suggest speakers

**Tuesdays 13:15 - 15:05 in 6E 2.5**

Seminars are open to all.

---

## Upcoming seminars

**8th October**

**Giulio Guerrieri (University of Bath)**

**Factorization and Normalization, Essentially** (joint work with **Beniamino Accattoli** and **Claudia Faggian**)

Lambda-calculi come with no fixed evaluation strategy. Different strategies may then be considered, and it is important that they satisfy some abstract rewriting property, such as factorization or normalization theorems. In this paper we provide simple proof techniques for these theorems. Our starting point is a revisit of Takahashi's technique to prove factorization for head reduction. Our technique is both simpler and more powerful, as it works in cases where Takahashi's does not. We then pair factorization with two other abstract properties, defining essential systems, and show that normalization follows. Concretely, we apply the technique to four case studies, two classic ones, head and the leftmost-outermost reductions, and two less classic ones, non-deterministic weak call-by-value and least-level reductions.

This work will appear at APLAS 2019.

---

## Past seminars

**2019**

**30th July (room 1W 2.03)**

**Ugo Dal Lago (Università di Bologna, Italy)**

**Differential Logical Relations** (joint work with **Francesco Gavazzo** and **Akira Yoshimizu**)

We introduce a new form of logical relation which, in the spirit of metric relations, assigns each pair of programs a quantity measuring their distance, rather than a boolean value standing for their being equivalent (or not). The novelty of differential logical relations consists in measuring the distance between terms not (necessarily) by a numerical value, but by a mathematical object which somehow reflects the interactive complexity, i.e. the type, of the compared terms. We exemplify this concept in the simply-typed lambda-calculus, and show a form of soundness theorem. We also see how ordinary logical relations and metric relations can be seen as instances of differential logical relations. Finally, we show that differential logical relations can be organised in a cartesian closed category, contrarily to metric relations, which are well-known not to have such a structure, but only that of a monoidal closed category. We conclude the talk by hinting at other forms of differential program semantics, which are being studied as part of the DIAPASoN research project.

This work appeared at ICALP 2019 ([link to the paper](#)).

---

**Informal Workshop Micro Structures and Deduction (Micro-SD)**

----- **Program** -----

### Wednesday 29 May (Room 3W 3.7)

1:15 Adam Lassiter (Bath): Coalescence Proof Search for Classical Logic  
2:00 Michelangelo Meozi (Bath): Expansion Tree Proofs with Unification  
2:45 --- Coffee break ---  
3:15 Chris Barrett (Bath): A Subatomic Proof System for Decision Trees  
4:15 --- End ---

### Monday 3 June (Room 8W 1.33)

1:15 Delia Kesner (Paris 7): Principles of Quantitative Types for Higher-Order Languages  
2:15 David Sherratt (Jena): The Spinal Atomic Lambda-Calculus  
2:45 --- Coffee break ---  
3:15 Giulio Guerrieri (Bath): Standardization via Linear Logic for Call-by-Name, Call-by-Value and Choice Effects  
4:00 Benjamin Ralph (INRIA Paris): Towards a Combinatorial Proof Theory  
4:45 --- End ---

### ----- Abstracts -----

#### Adam Lassiter (University of Bath)

##### *Coalescence Proof Search for Classical Logic*

Coalescence is a highly efficient proof search method for additive linear logic, the logic of categorical sum and product. For a proof of a sequent over two formulas  $A$  and  $B$ , it is a linear algorithm on the 2-dimensional product space  $|A| \times |B|$  over the subformulas  $|A|$  of  $A$  and the subformulas  $|B|$  of  $B$ . By design, the algorithm has no need for backtracking, and has built-in sharing (or memoization).

In this talk, I discuss how to adapt this method for classical logic. The starting point is the observation that a classical formula  $A$  can be proved by  $n$ -dimensional coalescence - that is, there is some  $n$  such that  $A$  can be proved by coalescence over the space  $|A| \times |A| \times \dots \times |A|$  (with  $n$  copies of  $|A|$ ).

Whether this algorithm is efficient depends on the growth of  $n$ . In a naive approach, this growth is far worse than expected. I will then discuss some natural ways of optimizing the algorithm.

-----

#### Michelangelo Meozi (University of Bath)

##### *Expansion Tree Proofs with Unification*

Expansion tree proofs are a representation of proofs in first-order classical logic that is focused on the witnessing terms to existential quantifiers, factoring out both propositional proof content (which is decidable) and the bureaucracy of sequent calculus. They are based on Herbrand's theorem, and have a natural game-semantic interpretation. There is also an interesting connection with learning algorithms.

Herbrand's theorem, however, makes no mention of explicit witnesses. In line with this, Hughes, Heijltjes, and Strassburger have recently given proof formalisms for fragments of first-order linear logic that omit witnessing terms, and instead reconstruct these by unification.

In this talk, I will apply this idea to expansion tree proofs, yielding a variant that omits witnessing terms, and discuss algorithms to reconstruct these.

-----

#### Chris Barrett (University of Bath)

##### *A Subatomic Proof System for Decision Trees*

Recently, several proof systems have been developed in a very principled and regular way according to a methodology called 'subatomic'. The main idea is to consider atoms as non-commutative self-dual connectives representing a superposition of truth values. This way, non-linear inference rules, such as contraction and cut, become linear and obey a unique scheme. Normalisation is, therefore, at the same time, simplified and generalised. The contribution of this talk is that, surprisingly, by completing in the most natural way the standard subatomic proof system for propositional classical logic, we obtain a new proof system for a conservative extension of propositional classical logic and of binary decision trees. Cut elimination for this system becomes an almost trivial variation of the already known (and also trivial) 'experiment method', which is essentially a truth tabling operation that generates canonical analytic proofs.

-----

**Delia Kesner (Université de Paris, IRIF, CNRS)**

### *Principles of Quantitative Types for Higher-Order Languages*

Quantitative techniques are emerging in different areas of computer science (model checking, logic, automata theory, etc) to face the challenge of today's resource aware computation.

In this talk we discuss quantitative types, a.k.a. non-idempotent (intersection/union) types, which provide a natural tool to reason about resource consumption. Quantitative types are applicable to a wide range of powerful models of computation, including pure functional programming, pattern matching, control operators and infinitary computations.

We provide a clean theoretical understanding of the use of resources, and survey some recent semantical and operational results in the domain.

-----

**David Sherratt (University of Jena)**

### *The Spinal Atomic Lambda-Calculus*

We introduce a variant of Gundersen, Heijltjes, and Parigot's atomic lambda-calculus. This typeable calculus with explicit sharing extends the Curry-Howard interpretation of open deduction already established by the previous calculus. This expanded interpretation allows us to follow a duplication strategy stronger than full laziness, in the sense that we duplicate less and share more of a term. This new ability is strongly connected to interpreting the scopes of abstractions, which is strongly related to the open deduction system in turn. We establish the good operational behaviour of the language by means of some fundamental properties such as confluence and preservation of strong normalisation. We finally discuss the possible benefits of this calculus, which may lead to some remarkable breakthroughs.

-----

**Giulio Guerrieri (University of Bath)**

### *Standardization via Linear Logic for Call-by-Name, Call-by-Value and Choice Effects*

Linear Logic (LL) has proved powerful in providing insights and tools to analyze computational and denotational properties of programming languages. When considering the lambda-calculus, LL provides a common setting where both call-by-name (CbN) and call-by-value (CbV) evaluation mechanisms can be interpreted via Girard's translations. The bang calculus internalizes the insights coming from LL proof-nets into an untyped lambda-like syntax which subsumes both CbN and CbV. In a different sense, the idea of a system which subsumes both CbN and CbV had been already advocated and developed by Levy, via the Call-By-Push-Value paradigm; and indeed, the bang calculus can be seen as an untyped version of Levy's one. This approach has been mainly exploited semantically. Moreover, the Call-by-Push Value paradigm, as well as related polarized calculi, admits LL-based models featuring non-trivial computational effects such as non-deterministic or probabilistic computations.

We show that the bang calculus provides a powerful methodology to study syntactical properties of CbN and CbV, and their extension to calculi with a choice effect (such as probabilistic, non-deterministic, or quantum). In particular, we have a uniform method to study the fundamental syntactical results for CbN and CbV lambda-calculi: confluence, standardization and normalization, and their extension to calculi with effects. Our approach allows us not only to revisit some well-known results, but also to discover new ones, namely in studying calculi with effects.

-----

**Benjamin Ralph (Inria Paris Saclay)**

### *Towards a Combinatorial Proof Theory*

Combinatorial proofs have been introduced by Hughes to give a "syntax-free" presentations for proofs in classical propositional logic. In a nutshell, a classical combinatorial proof consists of two parts: (i) a linear part, and (ii) a skew fibration. The linear part encodes a proof in multiplicative linear logic (MLL), whose conclusion is given represented in a cograph, while the skew fibration maps this linear cograph to the cograph of the conclusion of the whole proof. In deep inference, this skew fibration corresponds exactly to a contraction-weakening derivation. Applying certain restrictions to these two rules leads to substructural logics and substructural proof theory. These proof theoretic restrictions correspond precisely to set-theoretic and graph-theoretic restrictions on the skew fibration, allowing us to characterise proof systems by their graph homomorphism class.

-----

**21st May (room 1W 3.107)**

**Cristina Matache (University of Oxford)**

**A Sound and Complete Logic for Algebraic Effects** (joint work with Sam Staton)

I will talk about definitions of program equivalence, for a language with algebraic effects in the style of Plotkin and Power. Program equivalence is a long-standing problem in computer science, made more difficult by the presence of higher-order functions and algebraic effects. In this talk I will present a logic whose formulas represent properties of effectful programs. The satisfaction relation of the logic induces a notion of program equivalence. Notably, the induced equivalence coincides with contextual equivalence (which equates programs with the same observable behaviour) and also with an applicative bisimilarity.

This is joint work with Sam Staton which appeared at FOSSACS 2019. ([link to the article](#))

[pdf](#)

**16th April**

**Alessio Santamaria (University of Bath)**

**Towards a Godement Calculus for Dinatural Transformations**

Dinatural transformations, which have been used to interpret the second-order lambda calculus [1] as well as derivations in intuitionistic logic [2] and multiplicative linear logic [3], fail to compose in general; this has been known since they were discovered by Dubuc and Street in 1970 [4]. Many ad hoc solutions to this remarkable shortcoming have been found, but a general theory of compositionality was missing. The results Guy and I obtained during my PhD and that I'll show in the talk are the following:

1. Acyclicity of certain graphs associated to dinatural transformations is a sufficient and essentially necessary condition for two dinatural transformations to compose;
2. This yields to the definition of a category whose objects are mixed-variant functors and morphisms are partially dinatural transformations;

3. A new definition of horizontal composition for dinatural transformations embodying substitution of functors into transformations and vice-versa, intuitively reflected from the string-diagram point of view by substitution of graphs into graphs.

This work represents the first, fundamental steps towards a Godement-like calculus of dinatural transformations as sought—but never achieved—by Kelly in [5], with the intention then to apply it to describe coherence problems abstractly [6]. We have not managed to get such a complete calculus yet, but we are “well on our way” on the path paved by Kelly himself in [5] when he was assessing the simpler case of a many-variable fully covariant functorial calculus. What we have not done yet will be the subject of future work.

[pdf](#)

[1] Bainbridge, E.S., Freyd, P.J., Scedrov, A. and Scott, P.J., 1990. Functorial polymorphism. *Theoretical Computer Science* [Online], 70(1), pp.35–64. Available from: [https://doi.org/10.1016/0304-3975\(90\)90151-7](https://doi.org/10.1016/0304-3975(90)90151-7).

[2] Girard, J.-Y., Scedrov, A. and Scott, P.J., 1992. Normal Forms and Cut-Free Proofs as Natural Transformations. In: N.M. Yiannis, ed. *Logic from Computer Science*, [Online]. Mathematical Sciences Research Institute Publications. Springer, New York, NY, pp.217–241. Available from: [https://doi.org/10.1007/978-1-4612-2822-6\\_8](https://doi.org/10.1007/978-1-4612-2822-6_8).

[3] Blute, R., 1993. Linear logic, coherence and dinaturality. *Theoretical Computer Science* [Online], 115(1), pp.3–41. Available from: [https://doi.org/10.1016/0304-3975\(93\)90053-V](https://doi.org/10.1016/0304-3975(93)90053-V).

[4] Dubuc, E. and Street, R., 1970. Dinatural transformations. In: S. Mac Lane, H. Applegate, M. Barr, B. Day, E. Dubuc, A.P. Phreilambud, R. Street, M. Tierney and S. Swierczkowski, eds. *Reports of the Midwest Category Seminar IV*, [Online]. Lecture Notes in Mathematics. Springer, Berlin, Heidelberg, pp.126–137. Available from: <https://doi.org/10.1007/BFb0060443>.

[5] Kelly, G.M., 1972. Many-variable functorial calculus. I. In: G.M. Kelly, M. Laplaza, G. Lewis and S. Mac Lane, eds. *Coherence in Categories*, [Online]. Lecture Notes in Mathematics. Springer, Berlin, Heidelberg, pp. 66–105. Available from: <https://doi.org/10.1007/BFb0059556>.

[6] Kelly, G.M., 1972. An abstract approach to coherence. In: G.M. Kelly, M. Laplaza, G. Lewis and S. Mac Lane, eds. *Coherence in Categories*, [Online]. Lecture Notes in Mathematics. Springer, Berlin, Heidelberg, pp. 106–147. Available from: <https://doi.org/10.1007/BFb0059557>.

**19th March**

**Nicolas Wu (University of Bristol)**  
**The Scope of Algebraic Effect Handlers**

Algebraic effect handlers are a methodology for dealing with effectful programs in a modular way. They build on the free monad for a functor as means of describing a syntax tree. An interpretation of syntax is provided by a handler, which folds over the structure with an algebra. Handlers themselves are not always algebraic operations, which can lead to surprising properties of programs written in this style. This talk presents scoped algebraic effect handlers, which allow a certain class of handlers to be expressed algebraically.

**12th March**

**Luc Pellissier (Université Paris Diderot)**  
**Fibrations, approximations and intersection type systems** (joint work with **Damiano Mazza** and **Pierre Vial**)

We present calculi (intuitionistic or classical) in a bioperadic setting, and, following Melliès and Zeilberger (2015), represent type systems as morphisms of such structure.

Programs in such calculi can be approximated arbitrarily well by linear programs, that use their argument exactly once. In this work, we show that such linear approximations give rise, through an adapted

Grothendieck construction, to intersection type systems for any logical system that can be embed meaningfully into linear logic.

We recover in this way all well-known intersection type systems, capturing different notions of normalization for various languages, and give a blueprint to compute new ones.

[pdf](#)

## 26th February

**Willem Heijltjes (University of Bath)**

**Intuitionistic Proofs without Syntax** (joint work with **Dominic Hughes** and **Lutz Straßburger**)

Hughes's Combinatorial Proofs are an intriguing, purely graphical notion of proof for propositional classical logic. Here, we answer the question: what is their intuitionistic counterpart? Our result, Intuitionistic Combinatorial Proofs (ICPs), are a concrete geometric semantics of intuitionistic proof that reveal many interesting connections: to game semantics, deep inference, supercombinator reduction, and more.

The technical development starts with a graphical representation of formulas, in the style of arenas in game semantics, and co-graphs and coherence spaces in classical and linear logic. Unlike game semantics, where arenas are most often tree-like, our arenas are DAG-like.

ICPs, like their classical counterparts, are then composed of two fragments: a linear fragment called an "arena net", and a contraction-weakening fragment called a "skew fibration". An arena net is a proof net in intuitionistic multiplicative linear logic (IMLL), but over an arena rather than a formula. A skew fibration is a particular graph homomorphism between the arena net and the arena for the conclusion formula of the proof.

In contrast with linear logic, where linear/non-linear factorization is at the formula level through the bang operator, ICPs factor at the level of proofs, like Herbrand's Theorem for first-order classical logic, and like proof stratification in deep inference. An ICP can be viewed as a Hyland-Ong strategy with additional sharing.

ICPs abstract fully and faithfully over all non-duplicating permutations of the sequent calculus, a result we call "Polynomial Full Completeness" that is analogous to the Hughes and Heijltjes's recent "Local Canonicity" result for MALL. By contrast, lambda-calculus and game semantics incur an exponential blowup. This manifests in ICPs as a natural form of sharing, induced by the DAG-form of arenas.

We give a simple and direct normalization relation that arises naturally from the semantics. It relates to closed reduction in lambda-calculus (a redex may only reduce if it contains no free variables) and supercombinator reduction (as used in the implementation of Haskell), techniques originally devised for reasons of efficiency. Intriguingly, the sharing in ICPs need not be unfolded during normalization, and instead the shared subterm is evaluated first, similarly to call-by-need reduction.

[pdf](#)

## 12th February

**David Sherratt (University of Bath)**

**Exploring the limits of full laziness**

For my PhD I introduce a variant of Gundersen, Heijltjes, and Parigot's atomic lambda calculus. This typeable calculus with explicit sharing extends the Curry-Howard interpretation of open deduction already established by the previous calculus. This expanded interpretation allows us to follow a duplication strategy stronger than full laziness, in the sense that we duplicate less and share more of a term. We call this optimal laziness, and explain the different levels of laziness and how they relate to implementations, including optimal graph reduction in the style of Lamping.

[pdf](#)

**15th January**

**Andrea Aler Tubella (University Paris Diderot)**  
**Decomposing proof systems with contraction**

We present a general normalisation theory for logics with contraction. We show that in a wide variety of proof systems fulfilling some general conditions we can separate every proof into two phases: a linear phase followed by a phase made up only of contractions. By combining these results together with splitting, a generalised cut-elimination theory for linear proof systems, we are therefore presenting a modular normalisation theory encompassing many existing logics.

**2018**

**20th November**

**Giulio Guerrieri (University of Bologna)**  
**Types of Fireballs**

The good properties of Plotkin's call-by-value lambda-calculus crucially rely on the restriction to weak evaluation and closed terms. Open call-by-value is the more general setting where evaluation is weak but terms may be open. Such an extension is delicate and the literature contains a number of proposals. Recently, we provided operational and implementative studies of these proposals, showing that they are equivalent with respect to termination, and also at the level of time cost models. This paper explores the denotational semantics of open call-by-value, adapting de Carvalho's analysis of call-by-name via multi types (aka non-idempotent intersection types). Our type system characterises normalisation and thus provides an adequate relational semantics. Moreover, type derivations carry quantitative information about the cost of evaluation: their size bounds the number of evaluation steps and the size of the normal form, and we also characterise derivations giving exact bounds. The study crucially relies on a new, refined presentation of the fireball calculus, the simplest proposal for open call-by-value, that is more apt to denotational investigations.

[pdf](#)

**30th October**

**Georg Moser (University of Innsbruck)**  
**Epsilon Calculus and Herbrand Complexity (the case with equality)**

Hilbert's epsilon calculus is based on an extension of the language of predicate logic by a term-forming operator  $\varepsilon_{x}$ . Two fundamental results about the epsilon calculus, the first and second epsilon theorem, play a role similar to that which cut-elimination or decomposition techniques in other logical formalisms. In particular, Herbrand's Theorem is a consequence of the epsilon theorems. In the talk I will present the epsilon theorems and present new results (for the case with equality) on the complexity of the elimination procedure underlying their proof, as well as the length of Herbrand disjunctions of existential theorems obtained by this elimination procedure.

**13 June**

**James Davenport (University of Bath)**  
**Category Theory of Computer Algebra**

Computer algebra systems started off manipulating polynomials over the integers, or groups of permutations. As they moved into greater ranges of data structures, the need for underpinning theory became felt, and Scratchpad II (later Axiom) was the first system to use Universal Algebra and Category Theory for this. These days, other systems such as Sage and Magma also do this. This Talk explains how Axiom's category structure works, and some of the challenges posed by constructivity.

**22 May**

**Fabio Zanasi (University College of London)**

**Algebraic methods for network diagrams and component-based systems**

Diagrammatic languages are used in diverse fields of science to specify and study systems based on interacting components. Graphics outperforms textual information in highlighting connectivity and resource-exchange between parts of a system. This makes diagrammatic languages particularly effective in the analysis of subtle interactions as those found in cyber-physical, concurrent and quantum systems.

In recent years "algebraic network theory" emerged in theoretical computer science as a unifying mathematical framework in which diagrammatic languages are given a completely formal status and are studied using the compositional methods of algebraic program semantics. Nowadays the algebraic approach finds application in fields as diverse as quantum theory, linguistics, Bayesian probability, concurrency theory and the analysis of signal processing, electrical and digital circuits.

In this talk I give a general overview of the approach, focussing on signal processing theory as case study. Towards the end I will touch on some current research threads, including structural operational semantics for string diagrams, diagram rewriting implementation, and diagrammatic reasoning in Bayesian inference.

**15 May**

**Joe Paulus (University of Bath)**

**Deep Inference Intersection Types**

In this talk we investigate typing the basic calculus, a linear calculus with explicit sharing. We do this in open deduction formalism which is a combination of the sequent calculus and natural deduction. In the process we made the key innovation of multiset derivations in open deduction.

**8 May**

**James Laird (University of Bath)**

**Genericity Meets Dinaturality: The Semantics of Bounded Quantification**

Bounded quantification (exemplified by the typing system  $F_{\text{sub}}$ ) combines parametric polymorphism with subtyping, increasing its capacity to capture genericity and modularity of code by representing phenomena such as inheritance.

We describe a denotational semantics for bounded quantification, specifically:

- A general construction of a model of  $F_{\text{sub}}$  from a model of System F (the second order lambda-calculus) which has certain dinaturality properties. (A "converse" to the observation of Cardelli et. al. that instantiation of bounded quantifiers should be dinatural in subtype coercions.)
- A category of polymorphic games with the required dinaturality properties.
- A game semantics based on the above, for a programming language in which programs are stateful objects with bounded polymorphic types. In this model, full abstraction holds for "concretely bounded" types, but fails in general, arguably pointing to a gap in the expressiveness of existing typing systems for bounded polymorphism.

**20 March**



**Zak Tonks (University of Bath)**

**Fast Matrix Inversion in Computer Algebra**

James R. Bunch and John E. Hopcroft improved upon Strassen's (1969) method for matrix inversion via fast matrix multiplication in 1974. Bunch–Hopcroft handled the case in which principal submatrices are singular, and presented a modification for providing LU factorisation via this scheme. Such fast matrix multiplication techniques based on Strassen's method recurse via 7 multiplications on submatrices instead of the naive 8, and such methods achieve a worst case complexity of  $O(n^{\log_2 7})$  where  $\log_2 7 \approx 2.81$ .

However, Bunch–Hopcroft's method assumes that the input matrix is over a field — in particular the recursive nature of the algorithm requires that certain elements and sub-determinants are invertible. But this is not always true of a ring, and in doing Computer Algebra we are most interested in rings of polynomials. In this presentation a fraction free formulation of the algorithm is presented that is most suitable for (dense) matrices of sparse polynomials, where the intention is that such a method should be more efficient than interpolation methods in this case. In such a way, it is attempted to provide for these matrix inversion methods what Bareiss–Dodgson did for Gaussian Elimination.

**9 January**

**Vladimir Dotsenko (Trinity College Dublin)**

**Pre-Lie Algebras and F-manifolds**

The geometric notion of an F-manifold was introduced by Hertling and Manin as a natural generalisation of the celebrated notion of a Frobenius manifold. Pointwise, the structure of an F-manifold leads to an algebraic structure on tangent spaces that is a weakened version of a Poisson algebra, that is a commutative associative product and a Lie bracket that are compatible in some way that is slightly weaker than the Leibniz identity for Poisson algebras. Poisson algebras can be thought of as "infinitesimal associative algebras". The slogan of this talk is that "F-manifold algebras are infinitesimal pre-Lie algebras", relating them to a remarkable algebraic structure discovered independently by Gerstenhaber, Koszul and Vinberg in the 1960s. I shall outline the proof, which relies on a mixture of theory of rewriting systems and homotopical algebra.

**2017**

**28 November**

**Nobuko Yoshida (Imperial College of London)**

**Linear Logic and Session Types**

In this talk, we first outline recent activities in our mobility group in

Department of Computing, Imperial College London. Then we talk about the following work on Linear Logic and Session Types.

Linear logic has long been heralded as a potential model for concurrency: from Girard's original paper, to Abramsky's computational interpretation, reiterated by Bellin and Scott. More recently, an interpretation for intuitionistic linear logic has been given by Caires and Pfenning where propositions are viewed as session types - a well established typing discipline for concurrency - proofs as processes and proof reduction as inter-process communication.

In this talk we will detail how several generalisations and extensions of this interpretation arguably form a basis for a logical foundation that captures several interesting features of message-passing concurrent computation. Specifically, we will detail how the basic interpretation can be extended to richer typed settings such as polymorphism and dependent type theories

and how to account for a meaningful notion of typed process equivalence that gives meaning to both proof conversions and type isomorphisms.

**21 November**

**Hugo Paquet (University of Cambridge)**  
**Probabilistic Concurrent Game Semantics**

Game semantics has been very successful at modelling the language PCF and various extensions. In particular, there is a fully abstract games model (Danos-Harmer 2002) for Probabilistic Algol, an extension of PCF with probability and ground references. But it proved difficult to study Probabilistic PCF itself, without references, in this context.

I will show how concurrent games, based on event structures, provide a new framework for probabilistic game semantics. In this setting we can express "probabilistic innocence", the property characterising Probabilistic PCF programs. We will see that concurrent games also allow us to also interpret a concurrent version of Probabilistic PCF, in which some programs can be evaluated in parallel. Finally, I will talk about a new direction in probabilistic game semantics, aiming at supporting languages with continuous probability distributions.

**7 November**

**Pawel Sobocinski (University of Southampton)**  
**Graphical Linear Algebra**

Graphical linear algebra is a string diagrammatic alternative to the usual mathematical treatment of linear algebra (vector spaces, matrices and all that). Like process algebra, it is both a specification language and an implementation language, giving a new way "operational" way to approach this classical and uniquely important mathematical subject. The language enjoys a sound and complete axiomatisation (called the theory of Interacting Hopf Algebras), making it an attractive alternative calculus in which one can perform elementary computations of linear algebra.

Finally, string diagrams—like classical syntax—can be equipped with an operational semantics, becoming an extension Shannon's signal flow graphs, connecting process algebraic notions with classical control and systems theory.

**31 October**

**Lutz Straßburger (INRIA Saclay - Ile de France)**  
**Combinatorial Flows**

In this talk I will introduce combinatorial flows as a generalization of Hughes' combinatorial proofs. I will show how they can cover cut and substitution as methods of proof compression, and how cut and substitution are eliminated. Finally, I will show how proofs in syntactic formalisms like deep inference or sequent calculus are translated into combinatorial flows and vice versa.

**7 June**

**Pierre Clairambault (ENS de Lyon)**  
**A compositional account of Herbrand's theorem via concurrent games**

Herbrand's theorem, often regarded as a cornerstone of proof theory, exposes some of the constructive content of classical logic. In its simplest form, it reduces the validity of a first-order purely existential formula  $\exists x. \phi(x)$  (with  $\phi$  quantifier-free) to that of a finite disjunction  $\phi(t_1) \vee \dots \vee \phi(t_n)$ . More generally, it gives an education of first-order

validity to propositional validity, by understanding the structure of the assignment of first-order terms to existential quantifiers, and the causal dependency between quantifiers.

In this talk, I will show that Herbrand's theorem in its general form can be elegantly stated as a theorem in the framework of concurrent games. The causal structure of concurrent strategies, paired with annotations by first-order terms, is used to specify the dependency between quantifiers. Furthermore concurrent strategies can be composed, yielding a compositional proof of Herbrand's theorem, simply by interpreting classical sequent proofs in a well-chosen denotational model. I assume no prior knowledge of Herbrand's theorem or concurrent games.

This is joint work with Aurore Alcolei, Martin Hyland and Glynn Winskel.

**6 June**

**John Gowers (University of Bath)**  
**Sequoidal Categories and Transfinite Games: A Coalgebraic Approach to Stateful Objects in Game Semantics**

The non-commutative sequoid operator on games was introduced to capture algebraically the presence of state in history-sensitive strategies in game semantics, by imposing a causality relation on the tensor product of games. Coalgebras for the functor  $A \_$  - i.e., morphisms from  $S$  to  $A \_ S$  - may be viewed as state transformers: if  $A \_$  has a final coalgebra,  $!A$ , then the anamorphism of such a state transformer encapsulates its explicit state, so that it is shared only between successive invocations.

When we use this construction to model stateful objects in game semantics, we are using two properties of the game  $!A$ : firstly, that it is the final coalgebra for the functor  $A \_$  (so that we may use it to encapsulate state) and secondly, that it is a model for the exponential from linear logic (specifically, it is the cofree commutative comonoid over  $A$ ). I will investigate the underlying reasons why the same object carries both structures by using the notion of a sequoidal category, which generalizes and formalizes the sequoid operator from games, and discussing what extra conditions we need to place on it in order to guarantee that the final coalgebra for  $A \_$  has the same carrier as the cofree commutative comonoid over  $A$ .

I will give two different situations in which we can make this conclusion. The first is based upon the Melliès-Tabareau-Tasson formula for the cofree commutative comonoid in the situation where it can be constructed as a sequential limit of symmetrized tensor powers. The second approach adds the extra axiom that a certain isomorphism from  $!(A \times B)$  to  $!A \ !B$  is an isomorphism. This second condition always holds in the case that  $!A$  is a bifree algebra for  $A \_$ , but in general it is necessary to impose it, as we establish by giving an example of a sequoidally decomposable category of games in which plays will be allowed to have transfinite length. In this category, the final coalgebra for the functor  $A \_$  is not the cofree commutative comonoid over  $A$ : we illustrate this by explicitly contrasting the final sequence for the functor  $A \_$  with the chain of symmetric tensor powers used in the construction by Melliès, Tabareau and Tasson.

**23 May**

**John Power (University of Bath)**  
**One-dimensional generalisations of the notion of category**

A few weeks ago, I gave a seminar on joint work with Richard Garner that was based upon categories enriched in bicategories. However, I only outlined a definition and only briefly mentioned the context in which they arise. So I plan to give an expository talk outlining a few of the one-dimensional generalisations of the notion of category that have been studied over the past sixty years, with an idea of how they arose and how they relate to each other.

**16 May**

**Alessio Guglielmi (University of Bath)**  
**Sabbatical Report**

In the past year we have obtained several results in deep inference, helped by a productive sabbatical for me. In my opinion, it is time to make an effort and push deep inference into the mainstream.

In fact, I just found out that, contrary to what I have been thinking so far, deep inference has dramatic, positive consequences on the complexity of proofs above propositional logic. Another reason is that we have now a theory of normalisation that is more powerful and is conceptually clearer than the traditional one.

I will give a high-level presentation of the main results of the past year, which are: 1) subatomic logic and a common structure behind normalisation procedures; 2) elimination of cycles and its impact on substitution theory; 3) a generalised understanding of quantification and its impact on the complexity of proofs.

There are opportunities for several projects that extend or apply those results, in particular on cyclic proofs, process algebras, the epsilon calculus, the Curry-Howard isomorphism (on which I recently changed my mind a bit), and more. It would be helpful for me to get feedback on what the best strategy for future grant applications could be.

I have been told by many experienced colleagues that what is needed now, in order to make deep inference popular, is a textbook. I am convinced that this is necessary and I believe that the best way is to found the new theory starting from the notion of atomic flow. I will tell you what I think the atomic flows can and should do in terms of foundations, but I need your help to approach them from the categorical point of view. (A categorical understanding of atomic flows is necessary because they basically are string diagrams, which are seemingly becoming the foundation for quantum theories, which in turn might benefit from the compression and computation properties of deep inference.)

## 2 May

**John Power (University of Bath)**

### **From finitary monads to Lawvere theories: Cauchy completions (joint with Richard Garner)**

The two main category theoretic formulations of universal algebra are Lawvere theories and finitary (= filtered-colimit preserving) monads on  $\mathbf{Set}$ . The usual way in which to construct a Lawvere theory from a finitary monad  $T$  is by considering the opposite of the restriction of the Kleisli category  $\mathbf{Kl}(T)$  to finite sets or equivalently natural numbers. Richard Garner recently found a different formulation of this, using the notion of Cauchy completion of a finitary monad qua monoid, i.e., qua one-object  $V$ -category, in  $V$ , where  $V$  is the monoidal category  $[\mathbf{Set}_f, \mathbf{Set}]$ , equivalently the monoidal category  $[\mathbf{Set}, \mathbf{Set}]$  of filtered-colimit preserving functors from  $\mathbf{Set}$  to  $\mathbf{Set}$ .

Both finitary monads (easily) and Lawvere theories (with more effort) extend from  $\mathbf{Set}$  to arbitrary locally finitely presentable categories. So last year in Sydney, Richard and I explored the extension of his construction via Cauchy completions. That works most naturally if one does it in a unified way, i.e., not for one locally finitely presentable category at a time, but for all simultaneously, using the notion of  $W$ -category for a bicategory  $W$ .

I shall talk about as much of this as we can reasonably handle: it is work in progress, so I have not fully grasped it myself yet, and there is much to absorb, e.g. the concepts of Cauchy completion and categories enriched in bicategories. The emphasis will very likely be on Richard's work rather than the work we did jointly.

## 28 March

**John Power (University of Bath)**

### **Logic programming: laxness and saturation (joint with Ekaterina Komendantskaya)**

A propositional logic program  $P$  may be identified with a  $(\mathbf{Pf} \ \mathbf{Pf})$ -coalgebra on the set of atomic propositions in the program. The corresponding  $C(\mathbf{Pf} \ \mathbf{Pf})$ -coalgebra, where  $C(\mathbf{Pf} \ \mathbf{Pf})$  is the cofree comonad on  $\mathbf{Pf} \ \mathbf{Pf}$ , describes derivations by resolution. That

correspondence has been developed to model first-order programs in two ways, with lax semantics and saturated semantics, based on locally ordered categories and right Kan extensions respectively. We unify the two approaches, exhibiting them as complementary rather than competing, reflecting the theorem-proving and proof-search aspects of logic programming.

While maintaining that unity, we further refine lax semantics to give finitary models of logic programs with existential variables, and to develop a precise semantic relationship between variables in logic programming and worlds in local state.

**7 March**

**Nicolai Vorobjov (University of Bath)  
Lindemann's Theorem and Schanuel's Conjecture**

Schanuel's conjecture is the central, yet unsettled, proposition in transcendental number theory. Most of the known results (like famous Lindemann-Weierstrass theorem) and other conjectures in this theory follow from Schanuel. The conjecture turned out to be useful in model theory/analytic geometry, for example Macintyre and Wilkie proved Tarski's conjecture on decidability of the theory of the reals with exponentiation, assuming Schanuel. Recently I studied, with C. Riener, the structure of irreducible components of real exponential sets, using Schanuel. In this talk I will remind the basics of transcendental numbers, formulate the conjecture and some of its consequences.

**28 February**

**John Power (University of Bath)  
Clubs, enrichment and weak n categories: a progress report**

In the early 1960's, Jean Benabou proposed the notion of bicategory: a bicategory bears the same relationship to a 2-category as a monoidal category bears to a strict monoidal category, a monoidal category being a one-object bicategory and a strict monoidal category being a one-object 2-category.

It is not difficult to generalise the notion of 2-category to one of n-category for arbitrary n, but generalising the notion of bicategory has been a focus of research in both category theory and algebraic topology since the late 1980's, and it remains so now. Here, I report on progress that Soichiro Fujii, Thomas Cottrell and I have made over the past few months, as we have gradually come to understand and, to some extent, reorganise the approach taken by Michael Batanin in Australia and Tom Leinster in Scotland.

Our work is not yet complete, but we believe it explicates at least part of the underlying structure more clearly than hitherto done by using an enriched category theoretic perspective

**21 February**

**Marco Solieri (University of Bath)  
The good, the bad and the ugly  
Sharing, superposition and expansion in lambda terms and proof nets**

Models of efficient implementation and fine semantics of higher order programming languages both need to include a formal account of duplication. Once deconstructed, duplication can then be:

- \* avoided - as in the static normalisation of proof nets given by Girard's geometry of interaction (GoI);
- \* anticipated - as in the linearisation of lambda terms given by Taylor-Ehrhard-Regnier expansion;
- \* postponed - as in the optimal implementation of the lambda calculus given by Lamping's sharing graphs (SG).

How the GoI and the Taylor expansion are related? Is the optimal implementation efficient? In this talk I will survey two of the contributions I obtained in my doctoral investigations, and sketch some the directions of my current or prospective interest.

I will first introduce the geometry of resource interaction, a Gol for the resource lambda calculus, that is the linear and non-deterministic variation of the ordinary one being the domain of Taylor expansion. The algebraic structure which implements computation on paths within a term/proof correspond essentially to the multiplicative portion of the latter, enriched with a superposition operator. An expanded version of Girard's execution formula can then be easily formulated and shown to be invariant under reduction for ground-typed closed terms.

Secondly, I will recall that the only general (i.e. not empirical) result about the complexity of SG is restricted to two variants of linear logic proof-nets, ELL and LLL, which characterise two time complexity classes, respectively elementary and polynomial. In these cases, Baillot and Dal Lago have shown exploiting a Gol-like approach that the complexity of SG remains in such complexity classes. In the same setting, and together with Guerrini, I obtained a direct cost comparison between SG and the proof net reduction by purely syntactical means. A simulation between the two reductions allows to establish that a stronger bound: a quadratic function.

## 7 February

### **Noam Zeilberger (University of Birmingham)** **A Categorical Perspective on Type Refinement Systems**

A "type refinement system" is a type system built on top of a typed programming language, as an extra layer of typing. Type refinement systems in this sense have become increasingly popular, as a lightweight mechanism for improving the correctness of programs. In the talk, I will give an introduction to a categorical perspective on type refinement systems that I have been developing in collaboration with Paul-André Melliès, based on the simple idea of modelling a type refinement system as an "erasure" functor from a category of typing derivations to a category of terms. Some questions one can consider from this perspective include:

- \* What does it mean for a program to have more than one type? What does it mean for a typing judgment to have more than one derivation?
- \* How should we understand the so-called "subsumption rule"?
- \* If functors are type refinement systems, what does it mean for a functor to be a Grothendieck (bi)fibration?

A particular class of type refinement systems that are especially natural from this perspective are ones coming from a strict monoidal closed functor that is simultaneously a bifibration. I will give some examples illustrating how such type refinement systems can be used to give an axiomatic account of some phenomena from the semantics of separation logic and lambda calculus.

## 24 January

### **Koko Muroya (University of Birmingham)** **Dynamic Geometry of Interaction machine: call-by-need graph rewriter**

Girard's Geometry of Interaction (Gol), that is semantics of Linear Logic proofs, has been applied to program semantics in mainly two styles. One style yields graph rewriting systems for the lambda-calculus in which Gol gives an invariant of rewriting. The other style produces abstract machines that pass a token on a fixed graph along a path indicated by Gol. These styles of Gol in program semantics handle duplication of computation differently with linear logic as a back end, and consequently can be efficient in different ways.

The graph-rewriting Gol achieves time efficiency by copying subgraphs, whereas the token-passing Gol is space efficient by repeating moves of a token in a fixed (sub)graph. Aiming at exploring this spectrum of space and time efficiency, we introduce an abstract machine called Dynamic Gol Machine (DGoIM). It combines graph rewriting with token passing using a history of token passing.

We prove that the DGoIM can implement the call-by-need evaluation by interleaving token passing with as much graph rewriting as possible. Finally, we explore the tradeoffs of space and time cost in the DGoIM, by comparing it with a variant of Danvy et al.'s call-by-

need storeless abstract machine.

The quantitative analysis confirms that these two machines have the same space efficiency (up to constant factors) and the DGoIM is more time efficient than the storeless abstract machine.

**2016**

**19 December**

**Thomas Strum (CNRS, France and MPI for Informatics, Germany)**  
**Beautiful Decision Methods and Adventurous Heuristics for Solving Problems over the Reals**

Effective quantifier elimination procedures for first-order theories provide a powerful tool for generically solving a wide range of problems based on logical specifications. In contrast to general first-order provers, quantifier elimination procedures are based on a fixed set of admissible logical symbols with an implicitly fixed semantics. This admits the use of subalgorithms from symbolic computation. We are going to start with traditional quantifier elimination applied to verification and simple problems from the life sciences. Beyond quantifier elimination we are going to discuss recent results on an incomplete decision procedure for the existential fragment of the reals, which has been successfully applied to the analysis of reaction systems in chemistry and in the life sciences, which scales to models currently used in systems biology. We might mention our open-source computer logic software Redlog, where our methods are implemented ([www.redlog.eu](http://www.redlog.eu)).

**29 November**

**James Brotherston (University College London)**  
**Biabduction (and Related Problems) in Array Separation Logic**

I describe array separation logic (ASL), a variant of separation logic in which the data structures are either pointers or arrays. This logic can be used, e.g., to give memory safety proofs of imperative array programs.

The key to automatically inferring specifications is the so-called "*biabduction*" problem, given formulas  $A$  and  $B$ , find formulas  $X$  and  $Y$  such that

$A * X \models B * Y$

(and such that  $A * X$  is also satisfiable), where  $*$  is the well-known "separating conjunction" of separation logic. We give an NP decision procedure for this problem that produces solutions of reasonable quality, and we also show that the problem of finding a consistent solution is NP-hard.

Along the way, we study satisfiability and entailment in our logic, giving decision procedures and complexity bounds for both problems.

This is joint work with Nikos Gorogiannis (*Middlesex*) and Max Kanovich (*UCL*). A paper describing the work is available at <https://arxiv.org/abs/1607.01993>.

**22 November**

**Thomas Cottrell (University of Bath)**  
**Operads, generalised operads, and weak n-categories**

Operads are tools for defining algebraic structures in terms of the operations they have. In this talk, I will describe the classical case of operads, in which each operation has a natural number of inputs, called its arity. I will then explain how to generalise this definition to allow for operads with more complex shapes of inputs. Finally, I will show how these generalised operads can be used to define weak n-categories, a very general type of higher-dimensional category.

**15 November**

**Soichiro Fujii (The University of Tokyo)**  
**Generalized Global States**

From the outset, the global state has been among the leading examples in the algebraic approach to computational effects. Indeed, the approach itself started from the recognition that the global state admits a computationally natural presentation in terms of operations and equations.

In this talk, I attempt to shed new light on the global states by introducing a new class of computational effects which I tentatively call 'generalized global states'. First, I explain that the now standard presentation of the global state monad on Set (in terms of the update and lookup operations) is a particular instance of a much more general phenomenon, whose first appearance essentially dates back to Lawvere's thesis. Second, I present a unified operational semantics for generalized global states and state a relationship to Plotkin and Power's operational semantics based on effect values.

**1 November**

**Martín Escardó (University of Birmingham)**  
**Continuity in type theory**

The formulation in Martin-Loef type theory of a Brouwerian continuity principle, saying that all functions  $(N \rightarrow N) \rightarrow N$  are continuous, via the so-called Curry-Howard interpretation of logic, turns out to be inconsistent. It becomes consistent under the univalent interpretation of logic, which is similar to that of topos logic. In particular, the notion of existence is interpreted as something strictly weaker than that Martin-Loef's Sigma type, but stronger than its classical manifestation as the negation of a universal quantifier. In fact, the original paper by Howard already points out that there are two natural constructive notions of existence (a weak and a strong one).

**25 October**

**Pedro Henrique Carrasqueira (CLE, University of Campinas, Brazil)**  
**Some introductory remarks to paraconsistency and logics of formal inconsistency**

A logic is paraconsistent if inconsistencies do not imply triviality in it. Paraconsistent logics are thus suited for reasoning in the presence of ineliminable inconsistencies, and they produce non-trivial but inconsistent theories. There are two main philosophical traditions of studies of inconsistency and paraconsistent logic. One of them advocates for the position known as *dialetheism*: that some contradictions are true, or, equivalently (given classical negation), that some propositions are both true and false. There is, however, another, somewhat earlier tradition, which takes a very different approach to the matter of inconsistency. This tradition assumes, instead, paraconsistency to be a common trait of logics that are in some sense appropriate for situations of imperfect rationality or imperfect information. In particular, their research focuses on logics in which the presence of disagreement or misinformation can be expressed by a formal language itself. Collectively, the various logics developed by this tradition and having such a property are known as *logics of formal inconsistency*. In my talk I shall briefly discuss the main differences that keep apart these two traditions of paraconsistency, with special attention to the different theoretical and practical problems they aim to solve. Then I shall focus on logics of formal inconsistency, taking the logic called *mbC* as my main example of the kind of behavior such logics exhibit. I shall end with some remarks on the ongoing research in this tradition of paraconsistency, as well as on its possible further developments.

**4 October**

**David Sherratt (University of Bath)**  
**Towards an atomic abstract machine**

The atomic lambda-calculus is known for its efficiency when evaluating terms; it is naturally fully lazy. Abstract machines are used to administer evaluation strategies. In this talk, I will discuss the idea of building an



atomic abstract machine, implementing the evaluation strategy for the atomic lambda-calculus, with the intent of developing a fully lazy abstract machine and proving it to be effective.

**Alessio Santamaria (University of Bath)**

**Looking for a categorical notion of substitution of atomic flows**

In this talk I present the work I have done in my first year: trying to give a categorical understanding of atomic flows in order to study their algebra - in the technical sense of the term, that is the operations we can do with them. Apart from plugging together and juxtaposing two flows, Guglielmi et al. proposed in an unpublished manuscript a notion of substitution of a flow inside a connected component of another, an operation which would generalise the usual notion of substitution of a formula inside the occurrences of an atom in another formula to that of substitution of a derivation inside the occurrences of an atom in another derivation. Categorically speaking, it seems that their idea can be formalised in terms of horizontal composition of families of morphisms, with which we interpret atomic flows. I will show how we generalised the well known definition of horizontal composition of natural transformations for a larger class of families of morphisms, namely extranatural transformations, in a meaningful way and what we have in mind to do for families of morphisms which are obtained by composing natural and extranatural transformations, but themselves are neither of them.

**12 May**

**Giulio Manzonetto (Université Paris XIII)**

**New Results on Morris's Observational Theory --- The Benefits of Separating the Inseparable**

We study the theory of contextual equivalence in the untyped lambda-calculus, generated by taking the normal forms as observables. Introduced by Morris in 1968, this is the original extensional lambda theory  $H+$  of observational equivalence. On the syntactic side, we show that this lambda-theory validates the omega-rule, thus settling a long-standing open problem. On the semantic side, we provide sufficient and necessary conditions for relational graph models to be fully abstract for  $H+$ . We show that a relational graph model captures Morris's observational pre-order exactly when it is extensional and lambda-König. Intuitively, a model is lambda-König when every lambda-definable tree has an infinite path which is witnessed by some element of the model.

**27 April**

**Pino Rosolini (University of Genoa)**

**Frames from topology, algebraically**

We describe a connection between frames and algebras for the double exponential monad on the Sierpinski space. Instrumental for the presentation is Dana Scott's category  $Equ$  of equilogical spaces. We present a subcategory of  $Equ$ , closed under the double exponential monad, on which the category of algebras is equivalent to that of frames (and frame homomorphisms). I hope to connect this with Taylor's work on Abstract Stone Duality.

This is joint work with Giulia Frosoni and Alessio Santamaria.

**20 April**

**Jamie Vicary (University of Oxford)**

**Geometrical Proofs for Linear Logic**

Linear logic is a fundamental way to reason about resources that cannot be duplicated or deleted. In this talk, I will present a new approach to the proof theory of linear logic, in which proofs are represented as surfaces embedded in 3-dimensional space. Proof equivalence then has a simple definition: two proofs are logically equivalent just when their surfaces are geometrically equivalent. The technical basis for the work comes from higher category theory, and I will give a simple and accessible introduction to this.

19 April

**Paul Harrenstein (University of Oxford)**  
**Expressiveness and Nash Equilibrium in Iterated Boolean Games**

We introduce and investigate a novel notion of expressiveness for temporal logics that is based on game theoretic properties of multi-agent systems. We focus on iterated Boolean games, where each player has a goal, represented using (a fragment of) Linear Temporal Logic (LTL). This goal captures the player's preferences: the models of the goal represent system behaviours that would satisfy the player. Moreover each player is assumed to act strategically, taking into account the goals of the other players, in order to bring about computations satisfying their goal. In this setting, we apply the standard game-theoretic concept of Nash equilibria: the Nash equilibria of an iterated Boolean game can be understood as a (possibly empty) set of computations, each computation representing one way the system could evolve if players chose strategies in Nash equilibrium. Such an equilibrium set of computations can be understood as expressing a temporal property—which may or may not be expressible within a particular LTL fragment. The new notion of expressiveness that we study is then as follows: what LTL properties are characterised by the Nash equilibria of games in which agent goals are expressed in fragments of LTL? We formally define and investigate this notion of expressiveness and some related issues, for a range of LTL fragments.

12 April

**Harry Gunn (University of Bath, Masters Student)**  
**Nature-based Cryptography**

This is a review of several papers by G. Grigoriev and V. Shpilrain on a novel approach to public key cryptography. These authors write:

"We use various laws of classical physics to offer several solutions of Yao's millionaires' problem without using any one-way functions. We also describe several informationally secure public key encryption protocols, i.e., protocols secure against passive computationally unbounded adversary. This introduces a new paradigm of decoy-based cryptography, as opposed to "traditional" complexity-based cryptography. In particular, our protocols do not employ any one-way functions."

5 April

**Sam Staton (University of Oxford)**  
**Semantics for probabilistic programming**

I'll talk about the semantics of probabilistic programming languages. This is an old subject, but recently probabilistic programming has attracted a lot of interest as a method of statistical modelling, through languages like Anglican and Church. These raise some new problems, such as how to combine continuous distributions with higher types. I'll describe our work on operational semantics and denotational semantics (based on sheaves and measurable spaces).

15 March

**John Power (University of Bath)**  
**Category theoretic semantics for theorem proving in logic programming: embracing the laxness**  
**(joint with Ekaterina Komendantskaya)**

A propositional logic program  $P$  may be identified with a  $P_f P_f$ -coalgebra on the set of atomic propositions in the program. The corresponding  $C(P_f P_f)$ -coalgebra, where  $C(P_f P_f)$  is the cofree comonad on  $P_f P_f$  describes derivations by resolution. Using lax semantics, that correspondence may be extended to a class of first-order logic programs without existential variables. The resulting extension captures proofs by term-matching resolution in logic programming. Refining the lax approach, we further extend it to arbitrary logic programs.

**8 March**

**John Gowers (University of Bath)  
Games with ordinal sequences of moves**

I shall present a modification of the Abramsky-Jagadeesan games model to allow sequences of moves indexed by transfinite ordinals. The motivation for this construction is work arising from work by Laird and Churchill in [1,2] concerning the sequoid operator. In [2], the authors construct an exponential in the category of games that is a cofree commutative comonoid for the 'tensor on the left' functor and a final coalgebra for the 'sequoid on the left' functor. In the category of finite games and strategies, this exponential can be constructed from the sequoid functor as the limit of a diagram indexed by the ordinal  $\omega$ . If we try to extend this result to the 'sequoidal categories' introduced in [1], then we find that this construction does not always produce a final coalgebra, but that for natural categories of games a similar construction using a higher ordinal will work. If the lengths of plays in an ordinal game can be bounded by a limit ordinal  $\kappa$  then we may construct the final coalgebra for the sequoid using a suitable diagram indexed by  $\kappa$ . Conversely, if a game contains plays greater than an ordinal  $\kappa$  then the limit of the natural diagram indexed by  $\kappa$  does not have the natural structure of a coalgebra.

There is a sizeable body of research in the field of games with plays indexed by transfinite ordinals (sometimes called 'long games'). In [3], Itay Neeman presents results concerning whether or not such games are determined. More recently, Laird has applied a similar model to the study of unbounded determinism in [4]. The construction given in this talk is a straightforward extension of the games model outlined in [1,5]. A nice feature of the construction is that it includes as special cases both the 'games with winning condition on infinite plays', given in [5], and the pure finite games introduced by Blatt in [6].

After shifting focus from finite to infinite ordinals, it becomes convenient to treat plays (ordinal sequences of moves), rather than moves, as primitive, and one possible formulation is to define a game to be a sheaf of sets on some given ordinal  $\kappa$ , where the ordinal  $b < \kappa$  is sent to the set of legal plays of length  $b$ . In contrast to the Abramsky-Jagadeesan model, in which moves are designated as Player-moves or Opponent-moves, we have a function that designates plays as Player-plays or Opponent-plays. If a play is indexed by a limit ordinal, then it has no last move, so this distinction is important. For example, in the case of games played over the ordinal  $\omega + 1$ , we are free to specify whether a play of length  $\omega$  should belong to Player or to Opponent, and this corresponds exactly to choosing a set of infinite plays that are Player-winning, as in [5].

I shall outline the motivation and construction for games played over transfinite ordinals, and shall discuss briefly some tentative questions about links to ordinals occurring elsewhere in the theory - in particular, game-value ordinals for winning positions and consistency-strength ordinals in proof theory.

[1]: Martin Churchill, James Laird and Guy McCusker. Imperative programs as proofs via game semantics. LICS 2011: 65-74, June 2011

[2]: James Laird. A Categorical Semantics of Higher Order Store, CTCS 2002. Proceedings of CTCS '02, Elsevier, 2002

[3]: Itay Neeman. The Determinacy of Long Games. De Gruyter Series in Logic and its Applications, 1972

[4]: James Laird. Sequential Algorithms for Unbounded Nondeterminism. MFPS XXXI: 271-287, 2015

[5]: Samson Abramsky, Radha Jagadeesan. Games and full completeness for multiplicative linear logic. Journal of Symbolic Logic 59 (02): 543-574, 1994

[6]: A. Blass. A game semantics for linear logic. Annals of Pure and Applied Logic, 56(1-3): 183 - 220, 1992

**1 March**

**Willem Heijltjes (University of Bath)**  
**Proof Nets and Complexity**

In this talk I will give an overview of some recent and some very recent developments in linear logic proof nets.

**2015**

**8 December**

**Giuseppe Primiero (Middlesex University)**  
**SecureND: Natural Deduction for Secure Trust**

Applications in computational domains complement verified knowledge with information sharing processes. From a logical viewpoint, formulating assertion operations in terms of a trust function is challenging, both conceptually and technically. In this talk we overview SecureND, a natural deduction calculus for knowledge derivation under trust. Its design is motivated by the problem of trust transitivity. We present also its implementation as the Coq protocol SecureNDC, to deal with trusted sources in software management systems. We conclude with an overview of current and future extensions of our language.

**1 December**

**Andrea Aler Tubella (University of Bath)**  
**A generalised cut-elimination procedure through subatomic logic**

Through subatomic logic we are able to present sufficient conditions for a proof system to enjoy cut-elimination. In this talk I will present subatomic logic, how it enables us to present proof systems that have single (linear) rule scheme and a recent result: we can generalise the splitting procedure for cut-elimination to any proof system whose rules and connectives have certain properties.

**17 & 24 November**

**John Power (University of Bath)**  
**Lawvere Theories**

I plan to give two talks about Lawvere theories. These are not for experts but rather to give the details. Lawvere introduced the notion in his PhD thesis in 1963, providing not only a category theoretic account of universal algebra but one that is also presentation-independent. Remarkably, his definition was embraced, albeit with a caveat and in different terms, by universal algebraists but not by category theorists. The latter, from 1966, generally preferred to model universal algebra owing to a little more generality but at a very considerable cost. Computer scientists were then influenced to adopt monads, but much could and has been gained by recasting some of the latter's concerns in terms of Lawvere theories. Ultimately, I think Lawvere theories are a superior approach, but benefit very much from the relationship with monads, and I duly plan to explain it.

**27 October**

**Guillaume Munch-Maccagnoni (University of Cambridge)**  
**Polarised realizability structures, models, and depolarisation**

Polarisation describes the presence of an evaluation order, and is characterised denotationally by a non-associativity of compositions. We recently proposed a polarised, Curry-style approach to the  $\lambda$ -calculus with extensional sums, in correspondence with polarised intuitionistic logic. We suggested that associativity of composition in this context should not be seen as a syntactic axiom, but as an emergent property akin to termination. Traditionally, issues with sums in denotational semantics have rather been considered to be with extensionality than with the associativity. This will be explained in an introductory fashion in a first part.

In a second part, I will more formally relate the termination in the  $\lambda$ -calculus with sums to depolarisation, i.e. associativity of composition, or more familiarly the fact that the order of evaluation does not matter. First, a general setting of polarised realizability structures for polarised calculi with or without control operators is developed. Then, a general technique to build observational models from these structures is explained. Finally, under broad conditions, the observational models that the non-associative syntactic structure gives rise to satisfy the associativity of composition (and are therefore cartesian closed categories with binary co-products). I will sketch an analogy between intuitionistic depolarisation and parametricity.

**20 October**

**Matthijs Vákár (University of Oxford)**  
**Game Semantics for Dependent Types**

Game semantics can act as a unifying semantic framework, providing compelling models for a strikingly wide range of programming languages, type theories and logics. A notable exception has been dependent type theory, which had so far defied a game theoretic description. We present a proposal to fill this gap in the form of a new categorical model of dependent type theory, based on a category of games and history-free winning strategies. We model dependent type theory with  $1$ -,  $\Sigma$ -,  $\Pi$ - and intensional  $\text{Id}$ -types as well as finite inductive type families (which act as ground types, like calendars). We discuss the place of the  $\text{Id}$ -types in the intensionality spectrum as well as the strong completeness properties the model satisfies.

Most of the talk should be understandable without prior knowledge of game semantics and dependent type theory.

**15 October**

**Ugo dal Lago (Università di Bologna)**  
**Higher-Order Probabilistic Computation: Calculi, Observational Equivalence, and Implicit Complexity**

Probabilistic models are more and more pervasive in computer science, and randomized algorithms are the ones offering the best performances in many domains. Higher-order probabilistic computation – in which a probabilistic function may be passed as a parameter and returned as a result – is on the other hand a relatively underdeveloped field, which is however receiving more and more attention. We give a survey of what is known about probabilistic  $\lambda$ -calculi, later focusing on some of our recent results on implicit complexity and on inductive and coinductive techniques for program equivalence. Finally, we hint at how all this could be useful when structuring proofs of security for cryptographic primitives, but also when expressing probabilistic models in the context of machine learning.

**10 June**

**Willem Heijltjes (University of Bath)**  
**Complexity Bounds for Sum-Product Logic via Additive Proof Nets and Petri Nets**

This is joint work with Dominic Hughes. We investigate efficient algorithms for the additive fragment of linear logic. This logic is an internal language for categories with finite sums and products, and describes concurrent two-player games of finite choice. In the context of session types, typing disciplines for communication along channels, the logic describes the communication of finite choice along a single channel.

We give a simple linear time correctness criterion for unit-free propositional additive proof nets via a natural construction on Petri nets. This is an essential ingredient to linear time complexity of the combinatorial proofs for classical logic by Dominic Hughes.

For full propositional additive linear logic, including the units, we give a proof search algorithm that is linear-time in the product of the source and target formula, and an algorithm for proof net correctness that is of

the same time complexity. We prove that proof search in first-order additive linear logic is NP-complete.

**2 June**

**Anupam Das (ENS Lyon)**

**A complete axiomatisation of MSOL on infinite trees.**

We show that an adaptation of Peano's axioms for second-order arithmetic to the language of monadic second-order logic (MSOL) completely axiomatises the associated theory (SkS) over infinite trees. This continues a line of work begun by Büchi and Siefkes with axiomatisations of MSOL over various classes of linear orders. Our proof formalises, in the axiomatisation, a translation of MSO formulas to alternating parity tree automata. The main ingredient is the formalised proof of positional determinacy for the corresponding parity games which, as usual, allows us to complement automata and to deal with the negation of MSO formulas. The Comprehension Scheme of MSOL is used to obtain uniform winning strategies, whereas most usual proofs of positional determinacy rely on instances of the Axiom of Choice or transfinite induction. (Consequently we obtain an alternative decision procedure for MSOL over infinite trees, via proof search, that remains entirely internal to the language.)

This talk is based on joint work with Colin Riba that will be presented at LICS '15.

**12 May**

**Georg Struth (University of Sheffield)**

**Completeness Theorems for Bi-Kleene Algebras and Series-Parallel Rational Pomset Languages**

Pomsets form a standard model of true concurrency. In this lecture I present a completeness result for a class of pomset languages, which generalises the regular languages to the realm of concurrency. More precisely I show that the congruence on series-parallel rational pomset expressions generated by series-parallel rational pomset language identity is axiomatised by the axioms of Kleene algebra plus those of commutative Kleene algebra. A decision procedure is extracted from this proof. On the way to this result, series-parallel rational pomset languages are proved to be closed under the operations of co-Heyting algebras and homomorphisms. These results form a significant step towards a decision procedure for the equational theory of concurrent Kleene algebras, which have recently been proposed for concurrency verification (joint work with Michael Laurence).

**5 May**

**James Brotherston (University College London)**

**Parametric completeness for separation theories (via hybrid logic).**

In this talk, we consider the logical gap between the following two concepts:

(1) provability in a propositional axiomatisation of separation logic, which is usually given by the bunched logic BBI; and

(2) validity in an intended class of models of separation logic, as commonly considered in its program verification applications. Such intended classes are usually specified by a collection of algebraic axioms describing specific model properties, which we call a separation theory.

Here, we show first that several typical properties of separation theories are in fact not definable in BBI. Then, we show that these properties become definable in a natural hybrid extension of BBI, obtained by adding a theory of naming to BBI in the same way that hybrid logic extends normal modal logic. Finally, we show how to build an axiomatic proof system for our hybrid logic in such a way that adding any axiom of a certain form yields a sound and complete proof system with respect to the models satisfying those axioms. In particular, this yields sound and

complete proof systems for any separation theory from our considered class (which, to the best of our knowledge, includes all those appearing in the literature).

This is joint work with Jules Villard, now at Facebook.

**28 April**

**Guilhem Jaber (Queen Mary)**

**Reasoning on Equivalence of Stateful Programs with Operational Game Semantics**

Contextual equivalence of programs written in a functional language with references (i.e. local mutable states) is a notoriously hard problem, specially with higher-order references (i.e. references which can store functions). In the last twenty years, different techniques have been introduced to that purpose: Kripke Logical Relations, Bisimulations and Algorithmic Game Semantics.

In this talk, we will see how to use operational game semantics, namely the trace semantics for a language with references introduced by Laird, to build a new technique, Kripke Open Bisimulations, to reason on equivalence of programs, taking the best of the previous methods. This technique is simple enough to be mostly automatized: it becomes possible to model-check equivalence of programs.

If time permits, we will see how to extend this technique to polymorphism.







