Report on BCTCS & AlgoUK 2020

The 36th British Colloquium for Theoretical Computer Science colocated with the 4th AlgoUK Workshop

6–8 April 2020, Swansea University

Ulrich Berger and Faron Moller

The British Colloquium for Theoretical Computer Science (BCTCS) is an annual forum in which researchers in Theoretical Computer Science can meet, present research findings, and discuss developments in the field. It also provides a welcoming environment for PhD students to gain experience in presenting their work to a broader audience, and to benefit from contact with established researchers.

AlgoUK is an EPSRC-funded research network for Algorithms and Complexity in the UK. The key aim of the network is to facilitate multi-faceted interactions within the UK's algorithmic research community and to promote interdisciplinary cooperation between these researchers and those in industry and other STEM (Science, Technology, Engineering, Mathematics) subjects. The founding research groups are at Durham, King's College London, Leicester, Liverpool, Royal Holloway and Warwick, but the network is open to all who wish to engage with it.

The joint BCTCS & AlgoUK 2020 event was hosted by Swansea University and held from 6th to 8th April, 2020. Unfortunately, due to the COVID-19 pandemic, it was impossible to host this as a physical meeting in Swansea. Instead, the whole event was run on-line using the Zoom virtual conference software. This turned out to be surprisingly effective, attracting over 220 distinct participants with close to 100 attending the Keynote Lectures. The event featured an interesting and wide-ranging programme of 10 invited talks and 25 contributed talks.

The meeting started on Monday afternoon with an AlgoUK Session on Railway Verification. With the scene set by the opening invited lecture by Simon Chadwick from Siemens Rail Automation UK, three of Europe's leading railway verification groups presented the state-of-the-art in railway verification from their respective countries: Professor Anne Haxthausen (Denmark); Professor Jan Peleska (Bremen, Germany); and Professor Bas Luttik (Eindhoven, The Netherlands). The meeting continued on Tuesday morning with an AlgoUK Session on Algorithmics which featured four more invited talks. Professor Kristina Vusković (Leeds) spoke on induced disjoint paths in restricted graphs; Dr Patrik Totzke (Liverpool) spoke on games on infinite graphs; Professor Edith Elkind (Oxford) spoke on hedonistic diversity games; and Dr MS Ramanujan (Warwick) spoke on lossy kernelization.

The meeting then continued with parallel sessions of contributed talks interspersed with two further invited talks: one by Professor David Manlove (Glasgow) on stable matchings; and the annual LMS Keynote Lecture on Discrete Mathematics delivered by Professor Robert Constable (Cornell) on implementing intuitionistic mathematics. Professor Constable delivered his lecture jointly with Dr Mark Bickford (Cornell).

BCTCS 2021 will be hosted by the University of Liverpool. Researchers and PhD students wishing to contribute talks concerning any aspect of Theoretical Computer Science are cordially invited to do so. Further details are available from the BCTCS website at `www.bctcs.ac.uk`.

Invited Talks

Robert Constable (Cornell University)
LMS Keynote Lecture in Discrete Maths
Implementing elements of intuitionistic mathematics in Nuprl

There is no way to implement all of intuitionistic real analysis or even formalize it. Brouwer, the primary creator of intuitionistic mathematics, knew this and said that a construction of the continuum is inconceivable. We will explain in this lecture why that is so. This is not the case for the Bishop and Bridges account of constructive analysis. Mark Bickford has implemented significant parts of constructive analysis in Nuprl. It might be possible to implement the entire book. Bishop's comment on Brouwer's view is priceless, and perhaps not well known. The lecture will use Bishop's written remark as motivation and then discuss how we are implementing elements of intuitionistic mathematics in Nuprl.

David Manlove (University of Glasgow)
Assigning junior doctors to hospitals – what makes it so hard?

In many countries, junior doctors are assigned to hospitals via a centralised matching process. Algorithms take as input the preferences of doctors over hospitals and vice versa, as well as quotas of hospitals (the numbers of doctors that each hospital has room for). The algorithms typically produce stable matchings of doctors to hospitals, which guarantee that no doctor and hospital would rather be assigned to one another than to remain with their existing assignee/s (if any). The underlying computational problem has been well studied in its classical form, and fast algorithms are known for finding stable matchings. In this talk we focus on extensions of the classical problem of assigning junior doctors to hospitals that are motivated by practical applications, each of which leads to an NP-hard problem. Variants that we consider include, for example: (i) trading off size with stability, where we seek larger matchings that minimise instability; (ii) allowing ties in the preference lists; (iii) allowing couples to apply jointly to pairs of hospitals that are typically

geographically close; and (iv) allowing hospitals to have lower quotas as well as upper quotas. In each case we motivate and define the problem, survey existing algorithmic results and outline some open cases.

AlgoUK Talks on Railway Verification

Simon Chadwick (Siemens Rail Automation UK)
Formal Verification: The Journey from Theory towards Practice

This presentation will look at the steps we have taken towards practical verification of railway signalling interlocking logic using formal verification. The theory is well demonstrated, and we have been working on some steps towards a system for use by railway signalling engineers. The issues we consider include: how to convey understanding about formal verification – what is checked, what is not checked; how to express safety properties; how to capture railway geography; how to provide a user interface; how to present the results; and how formal verification fits within the overall process for interlocking data.

Anne Haxthausen (Technical University of Denmark)
The RobustRailS Verification Method for Railway Interlocking Systems

In this talk, we present a method and an associated toolchain for the formal verification of the new Danish railway interlocking systems that are compatible with the European Train Control System (ERTMS/ETCS) Level 2. We have made a generic and reconfigurable model of the system behaviour and generic safety properties. To verify the safety of an interlocking system, first a domain-specific description of interlocking configuration data is constructed and validated. Then the generic model and safety properties are automatically instantiated with the well-formed description of interlocking configuration data. This instantiation produces a model instance in the form of a Kripke structure, and concrete safety properties expressed as invariants. Finally, using a combination of SMT-based bounded model checking (BMC) and inductive reasoning, it is verified that the generated model instance satisfies the generated safety properties. Using this method, it has been possible to verify the safety properties for model instances corresponding to railway networks of industrial size.

Bas Luttik (Eindhoven University of Technology)
Supporting Railway Infrastructure Managers with Formal Models and Analyses

In this talk, I will discuss our recent experiences with using the mCRL2 toolset – which has a process-algebra based modelling language, a modal mu-calculus-based property language, and an explicit-state model checker – to support two major innovation activities from railway infrastructure managers.

First, there is the EULYNX initiative of the European railway infrastructure managers. The aim of EULYNX is to standardise the interfaces between the interlocking and field elements (signals, points, level crossings); these interface standards are modelled in SysML. In a project funded by the Dutch and German railway infrastructure managers we are translating the SysML models to mCRL2 not only to formally assess the quality of the standard by model checking, but also to facilitate using them for model-based testing of compliance to the standard of delivered components.

Second, in collaboration with the Dutch railway infrastructure manager ProRail we have formally modelled and analysed the ERTMS Hybrid Level 3 principles. These principles facilitate subdividing track sections into virtual subsections, in order to allow multiple trains simultaneously on the same track section, thus increasing capacity. We have plans to support ProRail developers in their further elaboration of the design and implementation of ERTMS Hybrid Level 3.

Jan Peleska (Bremen University)
Advances in Railway Control Systems Architectures and Related Challenges for Verification and Validation

This presentation is about Formal Methods and their practical application in the railway control systems domain. As a staring point, we discuss a new "flavour" of distributed interlocking systems, where the proper interlocking logic is allocated on cloud computers using conventional (i.e. commercial off-the-shelf) multi-core hardware and operating systems. The servers in the cloud communicate with intelligent track elements over internet connections. Interlocking logic may even be geographically distributed on more than one server farm, introducing a new dimension of fault tolerance. This technology has been announced in 2018 by Siemens Mobility, and a first application is expected to become operative this year. We sketch how this architecture results in obvious reliability and availability improvements, but at the same time creates new challenges for comprehensive formal verification of safety properties. At the same time, novel requirements of European railways concerning the autonomous control of rolling stock increase the verification load and its complexity in a significant way. The overall verification challenges may be structured into (a) data validation, (b) safety-related verification of dynamic behaviour, (c) verification of hardware/software integration, and (d) runtime verification. We describe where Formal Methods are already applied today in a successful way and focus on some more specific verification problems requiring further research effort. The material presented here is based on a collaboration between Siemens and Verified Systems International, a company specialised on verification and validation of safety-critical systems.

AlgoUK Talks on Algorithmics

Edith Elkind (Oxford University)
Hedonistic diversity games

We consider a setting where players belong to two types (men and women, vegetarians and carnivores, junior and senior researchers) and need to split into groups, with each player having preferences over the proportion of the two player types in his or her group. We study the problem of finding a stable partition, for several game-theoretic notions of stability; while some of the problems we consider turn out to be polynomial-time solvable, others are NP-hard, in which case we also explore their parameterized complexity.

MS Ramanujan (Warwick University)
Lossy Kernelization

Polynomial-time preprocessing is one of the most widely used methods for tackling NP-hardness in practice, and in the area of kernelization, one has a robust mathematical framework to design and analyze preprocessing algorithms for decision problems. However, the standard notion of a kernelization algorithm does not combine well with approximation algorithms and heuristics, and Lokshtanov et al. (2017) introduced a notion of "approximate kernelization" to overcome this barrier. In this talk, we will discuss the framework and review some recent results on approximate kernels.

Patrick Totzke (University of Liverpool)
Playing with counters: how to solve games on infinite arenas

I will talk about perfect information zero-sum games played on graphs, which are ubiquitous in formal verification of reactive systems. For instance, solving (i.e., determining the winner of) parity games is equivalent to model checking for modal μ-calculus formulæ, which in turn subsumes both LTL and CTL specifications. LetâĂŹs ignore for now that the complexity of solving parity games remains unknown and instead be greedy and look into more expressive types of games. Moving from finite graphs to infinite ones and introducing randomization allows to study interesting interplay between the structure of the graphs, the complexities of winning strategies, and the decidability/complexity of game solving. It turns out that many interesting generalizations effectively reduce to solving so-called energy games, in which one of the two players simply wants to keep a discrete âĂIJenergyâĂİ level nonnegative. In this talk I recall historical and recent results on such games played on infinite graphs and point to open problems in the area.

Kristina Vušković (University of Leeds)
The induced disjoint paths problem on (theta, wheel)-free graphs

A hole in a graph is a chordless cycle of length at least 4. A theta is a graph

formed by three internally vertex-disjoint paths of length at least 2 between the same pair of distinct vertices. A wheel is a graph formed by a hole and a node that has at least 3 neighbors in the hole. In joint work with Trotignon and Radovanović we obtain a decomposition theorem for the class of graphs that do not contain as an induced subgraph a theta or a wheel, using clique cutsets and 2-joins. In this talk we show how this decomposition theorem can be used to solve the induced disjoint paths and related problems on this class.

Contributed Talks

Duncan Adamson (University of Liverpool)
Multidimensional Necklaces: Enumeration, Generation, Ranking and Unranking.

Crystals are highly structured periodic structures, defined by a 3-dimensional unit cell which periodically tiles an infinite 3-dimensional space. This tiling allows for many functionally identical unit cells, most obviously those that are the same up to translation. To explore the space of possible unit cells within a discrete unit space it is necessary to capture these symmetries. In one dimension, these symmetries can be easily captured by representing the unit cell as a necklace, which is the lexicographically minimal representation of a cyclic string. Motivated by the applications on crystals, we study the generalisation of necklaces to higher dimensions. This talk will focus on the generalisation of several key results on one-dimensional necklaces to the multi-dimensional case. These are the classical problem of enumeration, algorithms for the efficient generation of all necklaces, and polynomial-time algorithms for the two inverse operations of ranking and unranking of necklaces.

Ahmed Bhayat (University of Manchester)
Recent Developments in Higher-Order Theorem Proving

Higher-order logic is the natural language for many areas of mathematics. As such, it would be useful to have strong automation for higher-order reasoning. Unfortunately, automation for higher-order logic has lagged behind that for first-order logic. The Vampire theorem prover, developed in Manchester, along with other leading first-order theorem provers are based on the superposition calculus. Superposition is essentially a brute-force search through the set of all conclusions from given axioms. However, it adds powerful simplification techniques that allow the deletion of redundant conclusion thus keeping the search space manageable. For many years it was an open question whether superposition could be extended to higher-order logic. In this presentation, I provide details on recent research extending superposition to higher-order logic. This has been done in two ways, one of which has been implemented in Vampire.

Alex V Berka (Isynchronise)
The alpha-ram family: bit-level models for parallelism and concurrency

There are no bit-level machine models for parallelism and concurrency, amongst the standard formal models of computation, that permit computer simulations in tractable amounts of time and space, for the investigation of not just trivial programming constructs, but also more complex high-level programs. Such a machine would provide a basis for investigating processes running on a basic device rather than in a formalism abstracted from hardware, without introducing biases from the particulars of higher-level architectures. The α-ram family of deterministic machines provides not only simple semantics and neutral machine platforms for language design, but also opportunities for developing specialized and more general-purpose architectures. Physical constraints can be incrementally introduced into the design process in a least restrictive order, thereby reducing bias towards pre-conceived architectural types.

Adam /'O Conghaile (Cambridge University)
Game comonads and generalised quantifiers

Game comonads, introduced for the pebble game by Abramsky, Dawar and Wang (2017), and expanded to EF and bisimulation games by Abramsky and Shah (2018), offer a compositional perspective on the vast landscape of Spoiler-Duplicator games used in finite model theory and descriptive complexity. These constructions exhibit surprising connections between games and elegantly link the games in question with well-known algorithms for constraint satisfaction and graph isomorphism, and related combinatorial parameters such as tree-width. In my talk, I will review this new direction in finite model theory and sketch some upcoming work by me and Anuj Dawar on a new family of game comonads which extends these surprising connections to logics with generalised quantifiers, formally linking work of Hella (1990) and Hairgora & Luosto (2014) and introducing a new family of generalised tree-width parameters.

Frances Cooper (University of Glasgow)
Algorithms for new types of fair stable matchings

We study the problem of finding "fair" stable matchings in the Stable Marriage problem with Incomplete Lists (SMI). For an instance I of SMI there may be many stable matchings, providing significantly different outcomes for the sets of men and women. We introduce two new notions of fairness in SMI. Firstly, a regret-equal stable matching minimises the difference in ranks of a worst-off man and a worst-off woman, among all stable matchings. Secondly, a min-regret sum stable matching minimises the sum of ranks of a worst-off man and a worst-off woman, among all stable matchings. We present two new efficient algorithms to

find stable matchings of these types. Additionally, we discuss experiments that compare several types of fair optimal stable matchings and show that our algorithm to find a regret-equal stable matching produces matchings is competitive with respect to other fairness objectives.

Tonicha Crook (Swansea University)
The degree of non-computability of Nash equilibria in multiplayer games

Is there an algorithm that takes a game in normal form as input, and outputs a Nash equilibrium? If the payoffs are integers, the answer is yes, and a lot of work has been done on its computational complexity. If the payoffs are permitted to be real numbers, the answer is no, for continuity reasons. It is worthwhile to investigate the precise degree of non-computability (the Weihrauch degree), since knowing the degree entails what other approaches are available (eg, is there a randomized algorithm with positive success change?). The two player case has already been fully classified, but the multiplayer case remains open and is addressed here. Our approach involves classifying the degree of finding roots of polynomials, and lifting this to systems of polynomial inequalities via cylindrical algebraic decomposition. This is joint work with Arno Pauly.

Matthew England (Coventry University)
Machine Learning to Steer Symbolic Computation from its Worst Case Complexity

Machine Learning (ML) refers to algorithms that use statistical techniques to give computers the ability to learn from data. ML has been successfully applied in a wide variety of domains over the last decade. Our hypothesis is that ML could be used to improve the implementation of symbolic computation algorithms: to steer them away from their worst case complexity results. We report the results of EPSRC Project EP/R019622/1 which has considered the problem of selecting the variable ordering for a cylindrical algebraic decomposition (CAD). CAD is a key algorithm in real algebraic geometry and computational logic, used e.g. for quantifier elimination. We have experimented with different ML models, implemented techniques for feature generation from polynomial sets, proposed an improved measure of accuracy for such problems and used this to improve cross-validation hyper-parameter selection.

Arved Friedemann (Swansea University)
Functional Solving Engines

Solving is a reoccuring problem in computer science, which is why there are strong off the shelf universal solving engines like SAT, SMT or even FOL solvers. The problem with these solving engines is however, that they are quite hard to use. They lack proper embeddings into programming languages and their expres-

sive power does not suffice to express general recursion. There are languages with solving capabilities like PROLOG or Curry, but their solving engines are rudimentary when compared to state-of-the-art SMT solvers. This research aims to create a programming language with SAT-like solving capabilities. A formalism is introduced that could furthermore be used to perform complexity analysis on solvers, or that might even be used to automatically synthesize a solving engine.

Andrej Ivaskovic (Cambridge University)
Graded monads in program analysis

Functions with side-effects (e.g. mutable state, exceptions) introduce difficulties in reasoning about program semantics. Functional programmers are well acquainted with representing effectful computation as pure code that uses monads. Wadler and Thiemann have shown that there is a correspondence between monads and effect systems, a kind of static analysis used for computational effects. More recent research has looked into applications of the more general concept of graded monads. In this talk I will introduce graded monads and focus on how they are convenient for representing different kinds of static analysis. A part of this talk will be based on my recent work with Alan Mycroft and Dominic Orchard.

Tom de Jong (University of Birmingham)
Constructive domain theory in Univalent Foundations

Voevodsky's Univalent Foundations (UF), otherwise known as Homotopy Type Theory, is a modern foundation for mathematics, based on Martin-Löf Type Theory. By default, it is a constructive system and without adding resizing axioms, it is predicative. In this talk we will explain how to develop basic domain theory constructively and predicatively in UF. In particular, we will show how to define the Scott model of the programming language PCF and prove fundamental properties such as soundness and computational adequacy. We will highlight (1) our constructive treatment, (2) important features of UF and (3) predicativity concerns. To illustrate (1): we use the Escardó-Knapp lifting monad to constructively account for the non-termination in PCF. A prime example of (2) in our development is the propositional truncation. If time permits, we will report on ongoing work, such as our treatment of continuous and algebraic domains.

Noleen Köhler (University of Leeds)
Property Testing of NP-hard Problems

Property testers are probabilistic algorithms that aim for constant running time while providing accuracy guarantees and hence are highly relevant for solving hard problems for very large instances approximately as encountered in big-data applications. In this talk we consider the bounded-degree model of property testing. While there are NP-hard problems that are known to have no constant query

complexity testers (3-Sat, 3-colourability) there is a class of NP-hard problems, for which constant query complexity property testers exist. This follows from a result of Newman and Sohler (2013) which implies that on bounded-degree planar graphs all problems are testable of which several are NP-hard (e.g. Hamiltonicity). We recently discovered that for Hamiltonicity and dominating set there is no constant query complexity tester, using the property testing equivalent of polynomial reductions, namely local reductions. In general however it is not clear, how NP-hardness relates to property testing in the bounded-degree model.

Oliver Kullmann (Swansea University)
Classifying all minimally unsatisfiable 2-CNFs up to isomorphism

The SAT problem for 2-CNFs is a well-known special case where an NP-complete problem can be solved in linear time. We are interested in minimally unsatisfiable 2-CNFs (2-MUs), and we present a complete classification up to isomorphism (renaming of variables, and flipping of literals) of all 2-MUs. The bulk of the work is in establishing a link to weak double cycles (WDCs) as a nice class of digraphs: the implication digraphs of 2-MUs in the main cases are WDCs, and WDCs have exactly one skew-symmetry (which transforms a digraph into a 2-CNF) for those implication digraphs. Thus the isomorphism problem for 2-MUs reduces to the isomorphism problem of WDCs, which are essentially one big cycle of small cycles, and thus their isomorphisms are understood via the symmetries of the cycle (the Dihedral group).

Edwin Lock (Oxford University)
Translating into and from the Product-Mix Auction bidding language

In the Product-Mix Auction proposed by Paul Klemperer, bidders express their strong substitutes buying preferences using a novel bidding language by submitting a list of positive and negative 'dot bids'. While it has been shown that every strong substitutes buying preferences can be uniquely expressed using positive and negative bids, there exists no mechanism in the literature that assists the bidders in compiling their bid lists. Assuming access to a demand correspondence oracle, we provide an algorithm that computes the unique list of bids corresponding to a bidder's buying preferences. In the special case where buying preferences can be expressed using positive bids only, we have an efficient algorithm that learns the bids in linear time. We also show super-polynomial lower bounds on the query complexity of computing the unique list of bids in the general case where bids may be positive and negative.

Diptapriyo Majumdar (Royal Holloway University of London)
Parameterized Pre-coloring Extension and List Coloring Problems

Graph Coloring is a well studied NP-Complete problem in Theoretical Computer

Science. In this talk, we will discuss parameterized complexity approaches to Pre-coloring Extension and List Coloring problems. Golovach, Paulusma, and Song (2014) asked to determine the parameterized complexity of the following problems parameterized by k: (1) Given a graph G, a clique modulator (a set of vertices whose removal results in a clique) D of size at most k, and a list $L(v)$ of colors for every vertex v of G, decide whether G has a proper list colouring; (2) Given a graph G, a clique modulator D of size k, and a pre-coloring $\lambda_P : X \to Q$ for $X \subseteq V(G)$ decide whether λ_P can be extended to a proper coloring of G using colors from Q. For Problem 1, we design a $O(2^k)$-time randomized algorithm, and for Problem 2, we obtain a kernel with at most $3k$ vertices. Banik et al. (2019) proved the following problem is fixed-parameter tractable and asked whether it admits a polynomial kernel: Given a graph G, an integer k, and a list $L(v)$ of exactly $(n-k)$ colors for every vertex v of G, decide whether there is a proper list coloring for G. We obtain a kernel with $O(k^2)$ vertices and colors and a compression to a variation of this problem with $O(k)$ vertices and $O(k^2)$ colors. This talk is based on joint work with Gregory Gutin, Sebastian Ordyniak, and Magnus Wahlstrom.

Francisco J. Marmolejo-Cossío (Oxford University)
Fairness and Efficiency in DAG-based Cryptocurrencies

Bitcoin is a decentralised digital currency that serves as an alternative to existing transaction systems based on an external central authority for security. Although Bitcoin has many desirable properties, one of its fundamental shortcomings is its inability to process transactions at high rates. To address this challenge, many subsequent protocols either modify the rules of block acceptance and reward, or alter the graphical structure of the public ledger to a directed acyclic graph (DAG). We introduce a general framework for ledger growth in a large class of DAG-based implementations. By assuming honest miner behaviour, we explore how different DAG-based protocols perform in terms of fairness (whether the block reward of a miner is proportional to their hash power) as well as efficiency (what proportion of transactions a ledger validates after over time). Our results demonstrate fundamental structural limits on how well DAG-based ledger protocols cope with a high transaction load.

Michael McKay (University of Glasgow)
Stable Roommates with triple rooms under B- and W-preferences

In this talk we consider two possible formalisations of the three-dimensional Stable Roommates problem (3D-SR). In both, players specify preference lists over their peers, and the task is to partition the players into sets of size 3 based on their preferences. We consider two methods of generalising preference lists over individuals into preferences over sets. The first (second) method, B-preferences

(W-preferences) is based on the âĂŸbestâĂŹ (âĂŸworstâĂŹ) player in a set. The decision problem in each case asks whether we can partition the players into sets of three, such that no three players would prefer to be in a set together than remain in their current triples. We name the corresponding two problems 3D-SR-B and 3D-SR-W respectively, and we show that each problem is NP-complete. This contrasts with the known polynomial-time solvability of the problems (known as Hedonic Games) if we allow coalition sets of any size.

Peter Mosses (Swansea University)
Towards semantics online

At BCTCS 2006, I suggested the creation of an online repository of semantic definitions. The main idea was to define individual abstract constructs independently, and to specify programming languages by translation to combinations of abstract constructs. Since 2011, the PLanCompS project (plancomps.org) has been developing a component-based framework for semantics. A beta-release of a semantics repository is available (plancomps.github.io/CBS-beta), together with Haskell-based tools (hackage.haskell.org/package/funcons-tools/docs/Funcons-Tools) for executing abstract constructs (and hence programs via translation). Cliff Jones has also developed a digital library of historical semantic descriptions (plancomps.org/-semantic-descriptions-library). In this talk, I will present the foundations of component-based semantics, and look at how far the PLanCompS project has come towards establishing semantics online.

Arno Pauly (Swansea University)
From finite memory determinacy to Nash equilibria

Two-player win/lose games played on finite graphs are a central tool for verification. A common question is whether a winning strategy can be implemented by a finite automaton. As we consider quantitative objections and heterogeneous systems, we would want to consider multiplayer multi-objective games, and now have Nash equilibria realized by finite automata. I will present some transfer results that show under what conditions finite memory determinacy of the two-player win/lose case yields finite memory Nash equilibria of the multiplayer multi-outcome case. This is joint work with Stephane Le Roux.

Olga Petrovska (Swansea University)
Intuitionistic Fixed Point Logic and Program Extraction

In this talk I will present Intuitionistic Fixed Point logic (IFP) and its extensions that lie in the foundation of a new approach to program extraction. After discussing some examples, I will outline the main challenges of the soundness proof, which come from the optimisations required to include a fair amount of classical logic and to obtain garbage-free programs.

William Pettersson (University of Glasgow)
Preprocessing theory and practice in stable matching problems

Stable matching problems arise when agents with preferences must be matched in pairs, while avoiding having any pair of agents not currently matched together but who would prefer to be matched together to their current partners. Where agents can have incomplete preferences, with ties, finding a largest stable matching is NP hard, but such matchings are required in real-world applications. Preprocessing is the removal of entries from preferences of agents that don't affect any stable matching, which in turn reduces the time required to find largest stable matchings. We present new theory that allows the removal of more such entries, and then extend our new work to more general settings where agents may have integral capacities. We also present new algorithms that take advantage of this new theory, and perform computational experiments that show considerable improvements.

Tobias Rosenberger (Swansea University)
Unbabel your tools: Leveraging SPASS for UML

We present our progress towards fully automated symbolic reasoning about UML state machines. We do this in the context of institution theory and the Heterogeneous Framework (Hets), which allow the principled reuse of results and tools between different logics. In particular, we integrate a language for simple UML state machines into Hets and show how Hets can be used to apply the automated theorem prover SPASS to state machine properties. This is part of a larger effort to provide institution based tool-support and integrated semantics for UML diagrams.

Anton Setzer (Swansea University)
Did Erik Palmgren Solve a Revised Hilbert's Program?

This talk is dedicated to the memory of Erik Palmgren (1963-2019). We revisit the article by Palmgren giving an embedding of iterated inductive definitions into Martin-Löf Type Theory, and explain in what sense it provides an early substantial solution to a revised Hilbert's program. Palmgren's result didn't provide a sharp lower bound. We present a restricted version of Martin-Löf Type Theory with W-type and one universe, for which the embedding of Palmgren works as well and for which Palmgren's lower bound is sharp. We give a proof sketch for the sharpness of this bound.

Pavel Vesely (Warwick University)
Tight Lower Bound for Comparison-Based Quantile Summaries

Quantiles, such as the median or percentiles, provide concise and useful information about the distribution of a collection of items, drawn from a totally ordered universe. We study data structures, called quantile summaries, which keep track

of all quantiles, up to an error of at most ε. That is, an ε-approximate quantile summary first processes a stream of items and then, given any quantile query $0 \leq \phi \leq 1$, returns an item from the stream, which is a ϕ'-quantile for some $\phi' = \phi \pm \varepsilon$. We focus on comparison-based quantile summaries that can only compare two items and are otherwise completely oblivious of the universe. The best such deterministic quantile summary to date, due to Greenwald and Khanna (2001), stores at most $(1/\varepsilon \cdot \log \varepsilon N)$ items, where N is the number of items in the stream. We prove that this space bound is optimal by showing a matching lower bound.

Aled Walters (Swansea University)
Model-Based Testing of ETCS RBCs

The European Train Control System (ETCS) is a state-of-the-art railway control system, based on the communication between trains and interlockings via a Radio Block Centre (RBC). We are investigating the use of model-based testing in performing the quality control of RBC implementations in development. Using a formal model of ETCS based on a real-world implementation of a RBC, we can establish whether the comparison of a proven safety-verified model can in turn offer the same assurances to the real-world implementation under test, or whether issues in the implementation can be detected before heavy testing. The required elements necessary for an abstract yet sufficiently accurate model are key, and further models could be improved with additional details, or by using alternative modelling tools, while we aim to examine the advantages of using a formal proof alongside testing. In this talk we will discuss an instantiation of an ETCS model in Real-Time Maude based on data from industry implementation, and a comparison between its outcomes and that of industrial simulations. There will also be a brief look at possible tools to be implemented for the modelling, and an outlook for the project going forward. The research is done in collaboration with our Industry partner Siemens Rail Automation UK, and the talk is based on joint work with Markus Roggenbach and Monika Seisenberger.

Daniel Ward-Williams (Swansea University)
Exploring search characteristics of numeral system encodings

While we know numeral systems such as decimal and binary very well, there is a plethora of alternative ways to encode numbers. We look at some unusual systems and see what they have to offer as search space encodings. Characteristics such as range of value representability and unusual arithmetic laws are reviewed. Results from use in genetic algorithm encoding are discussed.