

## REPORT ON BCTCS 2010

### The 26th British Colloquium for Theoretical Computer Science

6–9 April 2010, University of Edinburgh

Julian Bradfield and Mary Cryan

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

BCTCS 2010 was hosted by the University of Edinburgh, and held at the Informatics Forum during 6–9 April 2010. The event attracted just over a hundred participants, and featured an interesting and wide-ranging programme of six invited talks and forty-nine contributed talks; the majority of the contributed talks were given by PhD students.

The meeting began on Tuesday afternoon with Kim Larsen’s invited talk - *Verifying LEGO: Validation and Synthesis of Embedded Software*, a practical talk describing the success of the fifteen-year UPPAAL project in verification, with applications ranging from walking robots through installation of wind turbines to ventilation in Danish pig farms. As this was an accessible topic, we opened this talk to the general public via the *Edinburgh International Science Festival*, which was running in April 2010. So it was a well-attended talk with plenty of questions afterwards. The talk was followed by the welcome reception for BCTCS, which took place in the *InSpace* laboratory on the ground floor of the Informatics Forum.

Wednesday’s programme started with the invited talk by Gil Kalai, our LMS Discrete Mathematics invited speaker. Best-known for his past work on the diameter of multidimensional polytopes, at BCTCS he spoke about more recent work – giving a detailed survey about *Analysis and Probability of Boolean Functions*. Built around the concepts of Influence (of a variable, on its function) and Noise-sensitivity, the talk was a good combination of basic material accessible to all, and more advanced recent developments. To follow Gil’s talk, Oded Lachish spoke on property testing in parallel with Wei Chen’s talk on games, binary trees and cyclotomic polynomials, before we all broke for coffee (and our first experience of excellent pastries and fruit from Green’s Deli). The morning continued with a group of pattern-matching and string talks in one room, and a parallel session on Bisimulation and Scheduling. Then we broke, and headed upstairs for the lunch buffet.

The afternoon program for Wednesday started with the invited talk by Catuscia Palamidessi on *Information-Theoretic Approaches to Information Flow*. This

talk explained how the leakage of information is a security problem, and how such leakage has been quantified in classical information theoretic terms. Then Catuscia explained how this analysis does not properly deal with many types of attack, and proposed techniques to correct this. There followed two contributed talks on the theme of distributed information.

Later that afternoon, the main afternoon sessions took place; one session mainly on Verification and Model Checking, with no fewer than three Swansea talks (two about railways), and a parallel session with some very nice talks on Graph Theory and Graph Algorithms.

After the talks many of the attenders took up the organizers' suggestion of visiting one of the local pubs.

The first talk on Thursday was Ulrike Sattler's invited talk on *Automated Reasoning for Ontology Engineering*. This was an extremely clear, well-explained and accessible talk, with examples drawn from applications. Later that morning, the main sessions for Thursday morning were on Logic and Automata in one room, and on Algorithms for Counting and Sampling (including some new results on approximating the Tutte polynomial by Mark Jerrum) in the other.

After lunch, Thursday's afternoon session started with a lively and interactive presentation on *Algorithms meet Art, Puzzles, and Magic* by invited speaker Erik Demaine. The talk was extremely broad and accessible to all, covering Origami, Geometric Games, Algorithms, and a really entertaining video. Due to the breadth of the topics, Erik's talk had been advertised widely through the Informatics department at Edinburgh, so there was a packed hall for the talk, and many questions for Erik to answer afterwards.

Thursday afternoon's parallel sessions were on Applied Algorithms and Semantics respectively.

After the sessions for Thursday were finished, the more involved members of BCTCS headed for the BCTCS Annual General Meeting. This meeting mainly discussed finances, and elected new officers for those whose terms had expired – including BCTCS's first student representative from overseas. Achim Jung reported on arrangements for BCTCS 27 in Birmingham, and Ian Pratt-Hartmann offered to host BCTCS 28 in Manchester.

Later that evening the Colloquium dinner took place in Howies on Waterloo Place, Edinburgh. We had an excellent choice of dishes including the obligatory haggis in a starter. After the meal Faron Moller, president of the BCTCS, took to the floor to make a speech. He talked about the history of BCTCS meetings in the past, and some of the highlights of this year's BCTCS in Edinburgh. Also he gave some time to reflect on Robin Milner's contributions to the Theoretical Computer Science community, before giving a toast to his memory. Following the dinner, the group dispersed into the many nearby pubs and clubs.

The final day of BCTCS was Friday, and we started with an excellent invited

talk by Johan Håstad on *Approximation Resistance* predicates. He gave a broad survey of results (and discussed his frustration with having to assume the Unique Games Conjecture) on the computational hardness of approximating such problems.

The program for Friday concluded with two parallel sessions, one on Algorithms and Games, and another session on General Algorithms. Some excellent talks in each session had interested parties jumping rooms.

We concluded the Colloquium with lunch, and the departure of the participants.

Abstracts for the talks are provided below; further details are available via the BCTCS 2010 website at <http://www.bctcs.ac.uk/BCTCS2010/>. The financial support of the Engineering and Physical Sciences Research Council (EPSRC), the London Mathematical Society (LMS) and the Scottish Informatics and Computer Science Alliance (SICSA) is gratefully acknowledged. The organizers also thank the local staff and students who were part of the team: Bahareh Afshari, Marjorie Dunlop, Julian Gutierrez, Avril Heron, Monika Lekuse, Magdalena Mazurczak, Carrie McNamee, Grant Passmore, Sarah Reay.

BCTCS 2011 will be hosted by the University of Birmingham from 18–21 April 2011. Researchers and PhD students wishing to contribute talks concerning any aspect of theoretical computer science are warmly welcomed to do so. Further details are available from the BCTCS website at <http://www.bctcs.ac.uk/>

## Invited Talks at BCTCS 2010

**Erik Demaine**, MIT

*Algorithms Meet Art, Puzzles, and Magic*

When I was six years old, my father Martin Demaine and I designed and made puzzles as the Erik and Dad Puzzle Company, which distributed to toy stores across Canada. So began our journey into the interactions between algorithms and the arts (here, puzzle design). More and more, we find that our mathematical research and artistic projects converge, with the artistic side inspiring the mathematical side and vice versa. Mathematics itself is an art form, and through other media such as sculpture, puzzles, and magic, the beauty of mathematics can be brought to a wider audience. These artistic endeavors also provide us with deeper insights into the underlying mathematics, by providing physical realizations of objects under consideration, by pointing to interesting special cases and directions to explore, and by suggesting new problems to solve (such as the metapuzzle of how to solve a puzzle). This talk will give several examples in each category, from how our first font design led to a universality result in hinged dissections, to how

studying curved creases in origami led to sculptures at MoMA. The audience will be expected to participate in some live magic demonstrations.

**Johan Håstad**, KTH Stockholm

*Approximation Resistance*

Consider 3SAT, the problem of satisfying a number of clauses each being the disjunction of exactly three literals. This is one of the basic NP-complete problems. Its maximization companion Max-3SAT, which asks to satisfy as many clauses as possible, is easily seen to be NP-hard to solve exactly but turns out to remain NP-hard in much weaker, approximate, forms. Given a satisfiable instance with  $m$  clauses and  $\varepsilon > 0$ , it is NP-hard to find an assignment that satisfies  $(7/8 + \varepsilon)m$  clauses. As a random assignment satisfies  $7m/8$  clauses this result can be interpreted as saying that efficient computation cannot do anything useful for Max-3SAT.

We say that a predicate  $P$  is “approximation resistant” if, for the problem above with the predicate  $P$  taking the role of “disjunction of three literals”, it is computationally hard to find an assignment that does better than a random assignment even when (almost) all constraints can be satisfied simultaneously. In this talk, we will survey many of the results relating to approximation resistance giving both positive and negative results as well as some indication of the proof-techniques involved.

**Gil Kalai**, Hebrew University of Jerusalem

*Analysis and Probability of Boolean Functions*

Boolean functions (under various names) are important in combinatorics, probability theory, computer science, game theory, and other areas. In this talk I will discuss a few results and some problems concerning analysis and probability of Boolean functions. In the (self-contained and friendly for students) lecture I will describe first a few notions: (1) Influence: The definition and properties of the influence of a variable on a Boolean function. (This is related to the power of a voter for an election rule; the effect of malicious processors in a collective coin flipping.) (2) Noise-sensitivity: How sensitive is a Boolean function to noise? (This is related to how likely it is that errors in counting the votes will change the outcomes of an election.) (3) The Fourier Walsh expansion.

Next I will briefly describe a few results: the existence of influential variable (KKL), the tradeoff between total influence and noise sensitivity (BKS) and the majority is stablest (MOO).

Next, two conjectures will be presented: the first on the relation between expectation threshold and the actual threshold (with Jeff Kahn); and the second about the noise stability conjecture for monotone threshold circuits and the reverse Boppana-Håstad conjecture (with Itai Benjamini and Oded Schramm).

Finally, two extensions will be mentioned: (a) Maps from  $\Sigma_n$  to  $\Sigma$  where  $\Sigma$  is a larger alphabet and their thresholds (with Elchanan Mossel); and (b) maps from  $\{0, 1\}^{mn}$  to  $\{0, 1\}^m$  in the context of judgement aggregation (with Muli Safra and Moshe Tennenholtz).

**Kim Larsen**, Aalborg

*Verifying LEGO: Validation and Synthesis of Embedded Software*

Embedded systems are to be found almost everywhere in today's society. Intelligence in the form of software and hardware is introduced into all kinds of products and sectors with the objective of enhancing their functionality. Examples include consumer electronics (e.g. MP3 players, audio/video systems), transport systems (e.g. ABS in cars, control software in high speed trains), medical devices (intelligent pens for treating diabetes), and many others.

As indicated by the examples above, embedded software are often applied in highly safety critical applications. The increased complexity of embedded systems challenges the methods used for designing and realising embedded systems, in order that they are bug-free, correct, predictable and fault-tolerant. In addition, embedded systems are often used in situations where timing guarantees (e.g. the release of an airbag in a car must happen within a few milliseconds after impact regardless) as well as bounds on usages of resources (memory, power, bandwidth) are crucial properties, making this effort even more difficult.

In the talk we will introduce the real-time validation tool UPPAAL and demonstrate on a number of embedded system examples, realised in LEGO Mindstorm, how UPPAAL enables us to find and correct bugs as well as to optimize resource consumption.

**Catuscia Palamidessi**, INRIA/École Polytechnique

*Information-Theoretic approaches to Information Flow*

In recent years, there has been a growing interest in considering the quantitative aspects of Information Flow, partly because often the a priori knowledge of the secret information can be represented by a probability distribution, and partly because the mechanisms to protect the information may use randomization to obfuscate the relation between the secrets and the observables. Among the quantitative approaches to Information Flow, the most prominent is the one based on Information Theory, which interprets a system producing information leakage as a (noisy) channel between the secrets (input) and the observables (output), and the leakage itself as the difference between the Shannon entropies of the input before and after the output (Mutual Information). This approach however suffers from two shortcomings: (1) The Shannon entropy is not the most suitable measure in case of the typical attacks in security (in particular, the one-try attacks), and (2) the analogy with the (simple) channel collapses in case of an interactive system.

In this talk we discuss these issues and propose some solutions.

**Ulrike Sattler**, Manchester University

*Automated Reasoning for Ontology Engineering*

In the last decade, “ontologies” are being developed as logical theories capturing domain knowledge, and used in a variety of applications, most prominently in clinical and life sciences. They are used to design and maintain terminologies, to base information systems on, and to provide flexible access to data. Description Logics, i.e., decidable fragments of first order logic, are used as the basis for ontology languages such as OWL, and the standardisation of these ontology languages has led to an increasing number of applications and tool developments, and to an increased interest in automated reasoning services.

I will briefly introduce OWL and describe its relationship with other logics, and then describe some of the recent developments in automated reasoning for ontology engineering. On the one hand, progress was made regarding standard reasoning tasks: e.g., we have seen the development of new reasoning techniques to cope with extremely large, modestly complex theories and to answer queries against databases w.r.t. ontologies. On the other hand, the “serious” usage of ontologies requires ever more and powerful non-standard reasoning services such as the extraction of modules or the explanation of entailments from an ontology.

I will assume a basic knowledge of first order or modal logic, and hope to provide an interesting overview of this lively area of logic- based knowledge representation.

## **Contributed Talks at BCTCS 2010**

**Anna Adamaszek**, DIMAP, Warwick University, A.M.Adamaszek@warwick.ac.uk

*Large-girth roots of graphs:* If  $H$  is a graph, its  $r$ -th power  $G = H^r$  is the graph on the same vertex set such that two distinct vertices are adjacent in  $G$  if their distance in  $H$  is at most  $r$ . We also call  $H$  the  $r$ -th root of  $G$ .

We study the problem of recognizing graph powers and computing roots of graphs. We provide a polynomial time recognition algorithm for  $r$ -th powers of graphs of girth (the length of the shortest cycle) at least  $2r + 3$ , thus improving a bound conjectured by Farzad et al. (STACS 2009). Our algorithm also finds all  $r$ -th roots of a given graph that have girth at least  $2r + 3$  and no degree one vertices, which is a step towards a recent conjecture of Levenshtein that such root should be unique.

On the negative side, we prove that recognition becomes an NP-complete problem when the bound on girth is about twice smaller. Similar results have so far only been attempted for  $r = 2, 3$ .

It is a joint work with Michał Adamaszek.

**Djihed Affi**, University of Manchester, djihed@cs.man.ac.uk

*Using Automated Reasoning Tools in the Simulation of Evolvable System:* We consider the modelling of systems that can adapt their behaviour at runtime in response to external

and internal stimuli. A logical framework for such evolvable systems is introduced in (IGPL 17:6 631-696 2009). In this framework, an evolvable system is modelled as a tree of components. Each component is modelled as a first order logic theory with constraints, actions and a state modelled as ground atoms. A component may be standalone or may be formed by a special supervisor/supervisee pairing. In this pair, the supervisee has access to the supervisor's theory and so it can trigger an evolution by altering its sub-components, its constraints or its state, or it can also replace.

A simulator tool for this framework is under development. The simulator accepts a logical specification and executes a sequence of instructions (program). During execution, the component's theories must remain internally consistent. Actions pre-conditions must be met before firing actions. constraints or components must not render the component's state conflicting.

In this talk I will present my work in using current automated theorem provers to simulate fairly complex specifications. Practical issues such as theory conversions and the use of caching techniques to speed up performance will be described.

**Golnaz Badkobeh**, King's College London, [golnaz.badkobeh@kcl.ac.uk](mailto:golnaz.badkobeh@kcl.ac.uk)

*An infinite Binary word containing only three distinct squares*: A square in a word is composed of two adjacent occurrences of a nonempty word. This note gives a simple proof and a straight construction of the existence of an infinite binary word that contains only three squares. No infinite binary word can contain fewer squares. The only factors of exponent larger than two that our infinite binary contains are two cubes which are not avoidable.

**Keywords**: combinatorics on words, repetitions, word morphisms.

**Michael J. Banks**, University of York, [mbanks@cs.york.ac.uk](mailto:mbanks@cs.york.ac.uk)

*Multi-User Systems in the Unifying Theories of Programming*: Hoare and He's Unifying Theories of Programming (UTP) is a framework for giving a denotational semantics to various programming paradigms and features of programming languages. In the UTP, a system is expressed as a predicate which describes the behaviour of the system that is visible to the environment. We focus on the question: how can the UTP be used to reason about systems that interact with multiple users?

This talk presents a new approach for modelling multi-user systems in the UTP. It is assumed that users operate in isolation and that each user only has direct knowledge of its own interactions with the system. Following this approach, we can identify what information a user of a system can deduce about the activities of other users and the behaviour of the system as a whole.

To illustrate the practical significance of this approach, we will cover an important topic in computer security — the regulation of “information flow” from systems to users — and define conditions in the UTP ensuring that a system does not leak confidential information to untrusted users.

**Martin Birks**, University of Leicester, [mb259@mcs.le.ac.uk](mailto:mb259@mcs.le.ac.uk)

*Temperature Aware Online Scheduling with a Low Cooling Factor*: With the speed of processors increasing, along with the number of cores on each chip, the temperatures gener-

ated by computers are increasing. Reliability of components can be reduced by running at high temperatures and exceeding certain temperature limits can often result in immediate failure. This, coupled with the high cost of cooling, has meant that temperature is fast becoming a bottleneck for the speed of computers. Until recently, research in this area has concentrated on hardware, but algorithms can also be used to manage temperature.

Online algorithms are algorithms that can't predict the future. A processor is inherently online as future jobs that may arrive will be difficult to predict as they depend on many variables such as human user inputs. In our case we will need to schedule unit length jobs arriving to a processor which have hard deadlines. In addition to this, each job will generate a (possibly) different amount of heat depending on how CPU intensive it is. The objective of an algorithm will be to maximise the throughput of jobs, without violating the systems Temperature Threshold. We analyse a large class of algorithms using a simplified cooling model, where at every step the temperature of a system is reduced by a cooling factor  $R$ . We show that this whole class of algorithms is optimal for deterministic algorithms with  $1 < R \leq 2$ .

**Christopher Broadbent**, Oxford University, [chrbr@comlab.ox.ac.uk](mailto:chrbr@comlab.ox.ac.uk)

*Some results concerning first-order logic and collapsible pushdown graphs.:* A higher-order pushdown automaton is an abstract machine equipped with a stack that itself contains nested stacks of stacks. It is known that the transition graphs of such devices have decidable MSO theories. Collapsible pushdown automata were introduced by Hague *et al.* (LICS 2008) and extend higher-order stacks with *links* that point between elements residing in the stack. They have shown that the transition graphs of collapsible pushdown automata have decidable mu-calculus theories but undecidable MSO theories. This left open the question as to whether first-order logic was decidable on such graphs.

Kartzow addressed this question in recent work (STACS 2010) in which he showed that order-2 collapsible pushdown graphs together with a reachability binary predicate are tree-automatic and consequently have decidable first-order theories. We will present some undecidability results showing that this cannot be fully extended to order-3 if reachability is retained and that moreover first-order logic is undecidable at order-4 even without reachability. We will also mention some work in progress that is attempting to show decidability for plain order-3 graphs.

**Supaporn Chairungsee**, King's College London,  
[supaporn.chairungsee@kcl.ac.uk](mailto:supaporn.chairungsee@kcl.ac.uk)

*Efficient computation of minimal absent words:* DNA sequence computation is a basic precondition for studying and analysing biological molecules. Having complete genome sequences allows to look for similarities and differences between genomes to make evolutionary and functional inferences. An absent (forbidden) word is a word that does not occur in a given genome; it is minimal if all its proper factors are factors of the given genome.

The problem of finding absent words has been recently addressed and there is only one algorithm for finding shortest absent words. However, this algorithm does not have



any specification of a length estimate. Recently, there is a new solution that computes a larger set of minimal absent words but this solution does not runs in a linear-time.

We present an efficient method for computing absent words of DNA sequence using a Suffix Trie of bounded length factors. This method outputs the whole set of absent words. Our technique provides a linear-time algorithm and uses less memory than previous solution.

**Keywords:** minimal absent words, absent words, forbidden words, DNA sequence, suffix trie.

**Prasad Chebolu**, University of Liverpool, [prasadc@liverpool.ac.uk](mailto:prasadc@liverpool.ac.uk)

*The Complexity of Approximately Counting Stable Matchings:* We investigate the complexity of *approximately counting* stable matchings in the special settings of the  $k$ -attribute model, where the preference lists are determined by dot products of “preference vectors” with “attribute vectors”, or by Euclidean distances between “preference points” and “attribute points”. It is known that counting the number of stable matchings in the general case is #P-complete. Counting the number of stable matchings is reducible to counting the number of downsets in a (related) partial order and is interreducible, in an approximation-preserving sense, to a class of problems that includes counting the number of independent sets in a bipartite graph (#BIS). The existence of a fully-polynomial randomized approximation scheme for this class of problems remains an open question. We show this approximation-preserving interreducibility remains even in the restricted  $k$ -attribute setting when  $k \geq 3$  for dot product and  $k \geq 2$  for Euclidean distance. Finally, we show it is easy to count the number of stable matchings in the 1-attribute dot-product setting.

**Wei Chen**, School of Computer Science, University of Nottingham,  
[wzc@cs.nott.ac.uk](mailto:wzc@cs.nott.ac.uk)

*From Seven-trees-in-one to Cyclotomics:* The well-known type isomorphism between seven-tuples of complete binary trees and binary trees, known as seven-trees-in-one, raises the question of whether for a given number  $n$  it is possible to construct an “interesting” type  $T$  such that  $n$   $T$ s are one, i.e.  $T^n \cong T$ . We show that the answer is yes; moreover, we show that any such isomorphism is generated by a so-called “cyclotomic” polynomial.

Seven-trees-in-one is also embodied in the “nuclear pennies game” posted by Piponi. Inspired by the relation between cyclotomic polynomials and seven-trees-in-one, we introduce a class of one-player games, described as follows.

Suppose there is an unbounded one-dimensional board on which a checker is placed. An instance of the class of games is specified by a finite set of integers  $R$ . If there is a checker at position  $i$ , one can replace it by adding one checker at each position in the set  $A = \{i + k \mid k \in R\}$ . Also, if there is at least one checker at each position in  $A$ , a checker from each of these positions can be removed and replaced by a checker at position  $i$ . The aim to move the initial checker  $m$  positions, for some  $m$  at least 1.

We are currently constructing a precise characterisation of the combination of number  $m$  (at least 1) and set  $R$  for which it is possible to move a checker  $m$  squares and, in the case that it is possible, we are developing an algorithm to solve the problem. At this stage

in our research, we have such a characterisation for a large class of games and we hope to have a complete characterisation soon.

Joint work with Roland Backhouse.

**Lorenzo Clemente**, Edinburgh University, L.Clemente@sms.ed.ac.uk

*Multipebble Simulation Preorders for Alternating Büchi Automata*: Language-inclusion, i.e., containment, is an important problem in automata theory: It's PSPACE-complete, thus it is natural to look for efficient under-approximations to it. One such approximation is given by *simulation preorders*. Intuitively, while in containment the whole word is known in advance, in simulation the word is revealed one letter at a time. Simulations *desiderata* are: 1) sufficient for containment, 2) suitable for state-space reduction of automata, i.e., quotienting under the induced equivalence should preserve the language of the automaton, and 3) polynomial-time computable. A thorough study of simulations for nondeterministic automata has been done by Etessami et al. [1]; Fritz and Wilke [2] extend their findings to alternating automata. Additionally, Etessami [3] studies *multipebble* simulations for nondeterministic automata: Using more pebbles gives coarser simulations, at the cost of being more expensive to compute. (Usual simulations correspond to 1 pebble in the language of [3].) Thus, multipebble simulations results in tighter under-approximations to containment, and they yield smaller quotients.

We extend the theory of multipebble simulations from nondeterministic to *alternating* automata. We generalize both [2] to multiple-pebbles, and [3] to alternation, proving that our multipebble simulations satisfy 1)-3) above. The most technically difficult result to prove is 2).

Joint work with Richard Mayr.

**Raphaël Clifford**, Department of Computer Science, University of Bristol, clifford@cs.bris.ac.uk

*From coding theory to efficient pattern matching*: Pattern matching is one of the basic tasks of modern computer systems. Simple and fast solutions have been known for exact matching, for example, since the 1970s and so it is perhaps somewhat surprising to discover that even small variants still raise novel and exciting challenges. A particular difficulty is caused by the introduction of promiscuously matching, wildcard or don't care symbols, especially where inexact matches are permissible. We will give an overview of the history of this problem area, briefly exploring the new techniques that have been developed and setting out those questions which have yet to be resolved.

**Andrew Collins**, University of Liverpool, acollins@liv.ac.uk

*Asynchronous rendezvous with local information*: We study efficient rendezvous of two anonymous agents located in a discrete Euclidean 2D-space represented by a two dimensional grid with integer coordinates. This model is equivalent to a standard geometric model in which the agents have limited visibility allowing them to observe one another at a close (e.g., unit) range. It is assumed here that each agent is aware of its own initial integer coordinates, however, the agents are not aware of positions of one another. We present an efficient explicit construction of space-covering sequences embedded into a discrete 2D-space that allow two robots located at distance  $d$  to meet after adopting a

trajectory of length  $O(d^{2+\epsilon})$ , for any constant  $\epsilon > 0$ . This upper bound is complemented by a simple lower bound argument preventing two robots from meeting each other along a route of length  $o(d^2)$ , in the worst case. We also show how to adopt our rendezvous algorithm to efficient gathering of a larger number of agents in 2D-space.

Joint work with Jurek Czyzowicz, Leszek Gasieniec, and Arnaud Labourel

**Páidí Creed**, Royal Holloway, University of London, [paidi@cs.rhul.ac.uk](mailto:paidi@cs.rhul.ac.uk)

*A Galois connection for the Valued Constraint Satisfaction Problem:*

A constraint in classical CSP is a pair  $(\sigma, \rho)$  where  $\sigma$  is a list of variables, from a set  $V$ , called the scope and  $\rho$  is a relation, over a domain  $D$ , whose arity is the size of the scope.

A key tool in the analysis of the complexity of constraint languages is the Galois connection  $\text{Pol} - \text{Inv}$ , between clones of operations and the sets of constraints expressible over a fixed constraint language.

The Valued Constraint Satisfaction Problem (VCSP) is a natural and useful extension to CSP that replaces the relation  $\rho$  in a constraint with a function which maps all possible tuples of domain elements to costs in some set (usually the positive rationals with infinity). Taking the solution to a VCSP instance as being an assignment with minimum cost, we can model many optimisation problems in this framework.

In 2006, Cohen et al showed that VCSP expressibility is precisely characterised by objects they called fractional polymorphisms. We will show how the set of fractional polymorphisms of a valued constraint language can be embedded in a natural structure we call a weighted clone, and define a Galois connection between weighted clones and sets of cost functions. We hope that this result will prove a useful tool in the search for tractable valued constraint languages.

Joint work with Dave Cohen, Martin Cooper, Peter Jeavons, and Standa Živný.

**Konrad Dabrowski**, DIMAP, University of Warwick, UK,

[K.K.Dabrowski@warwick.ac.uk](mailto:K.K.Dabrowski@warwick.ac.uk)

*Parametrised complexity and the independent set problem.:* Like many graph-theoretic problems, the MAXIMAL INDEPENDENT SET problem is NP-complete in general. However, all is not lost. Sometimes we know more information about the structure of the graphs we're looking at. We introduce a parameter which encodes some of this information. Often we can construct algorithms where the "non-polynomial behaviour" is somehow restricted by this parameter, in which case we say the algorithm is FIXED-PARAMETER TRACTABLE.

This talk gives a quick introduction to parametrised complexity. It describes some techniques that are useful when looking for independent sets. In particular, it gives an outline of some fixed-parameter algorithms for some particular classes of graphs.

(This is joint work with Vadim Lozin, Haiko Müller and Dieter Rautenbach.)

**Richard Dobson**, King's College London, [richard.dobson@kcl.ac.uk](mailto:richard.dobson@kcl.ac.uk)

*Low Energy Scheduling with Non-Uniform Multiprocessor Systems:* In recent times the demand for low energy scheduling has increased phenomenally; this is due to a number of reasons one of which is the rise of the smart phone, which needs to provide high

performance whilst maximising battery life. The goals of minimising processor energy consumption whilst maximising performance are conflicting as  $\text{Power} = \text{Speed}^\alpha$  where  $\alpha$  is a constant which differs between processors but is typically between 2 and 3.

Extensive research has taken place which looks at ways to slow down the processor whilst still achieving a predefined quality of service. One of the most compelling solutions presented by Albers and Fujiwara tries to minimise the sum of the Flow (the difference between a job being released and the current time) of all jobs whilst also trying to minimise energy consumed. These two objectives are then combined into one value of  $\sum \text{Flow} + \text{Energy}$  which is then minimised, this provides a good balance between performance and energy saving. This method has been applied to the uniform multiprocessor architectures (such as multi-core processors) and has been proven to have the potential to save large amounts of energy; although there has been little research which applies this to the non-uniform multiprocessor environment.

There is an increasing need to understand how we can utilise non-uniform multiprocessors systems as they have the potential to be even more energy efficient than their uniform multiprocessor counterparts, if harnessed correctly. We look at the best ways to utilise multiple non uniform processor systems through optimal processor selection and low energy scheduling using  $\sum \text{Flow} + \text{Energy}$  as the objective function.

**Charilaos Efthymiou**, University of Warwick, [charis@dcs.warwick.ac.uk](mailto:charis@dcs.warwick.ac.uk)

*Deterministic Counting of Graph Colourings Using Sequences of Subgraphs*: In this paper we propose a deterministic algorithm for approximate counting the  $k$ -colourings of a graph  $G$ . We consider two categories of graphs. The first one is the sparse random graphs  $G_{n,d/n}$ , where each edge is chosen independently with probability  $d/n$  and  $d$  is fixed. The second one is a family we call *locally  $\alpha$ -dense graphs* of bounded maximum degree  $\Delta$ . A graph  $G = (V, E)$  in this family has following property: For all  $\{u, v\} \in E$  the number of vertices which are adjacent to  $v$  but not adjacent to  $u$  are at most  $(1 - \alpha)\Delta$ , where  $\alpha \in [0, 1]$  is a parameter of the model.

Our algorithm computes in polynomial time a  $(1 \pm n^{-\Omega(1)})$ -approximation of the logarithm of the number of  $k$ -colourings of  $G_{n,d/n}$  for  $k \geq 2.1d$  with high probability. Also, for  $G$  a locally  $\alpha$ -dense graph of *bounded* maximum degree  $\Delta$  it computes in polynomial time a  $(1 \pm (\log n)^{-\Omega(1)})$ -approximation of the logarithm of the number of  $k$ -colourings, for  $k > (2 - \alpha)\Delta$ . Restricting the treewidth of the neighbourhoods in  $G$  we get improved approximation.

Our algorithm is related to the algorithms of A. Bandyopadhyay et al. in SODA '06, and A. Montanari et al. in SODA '06. However, we use correlation decay properties for the *Gibbs distribution* in a completely different manner. I.e. given the graph  $G = (V, E)$ , we alter the graph structure in some specific region  $\Lambda \subseteq V$  (by deleting edges between vertices of  $\Lambda$ ) and then we show that the effect of this change on the marginals of Gibbs distribution, diminishes as we move away from  $\Lambda$ . Our approach is novel and suggests a new context for the study of deterministic counting algorithms.

**Denham Coates-Evelyn**, Logic Code Generator Ltd  
73A Oldfied Road, Harlesden

London, U.K. NW10 9UT, denhamevelyn@googlemail.com

*An in-place optimal k-way merge-sort with  $O(N)$  data moves:* We show that for optimum k-way merge of k sorted lists, each consisting of  $m_j$  data values the number of comparisons is  $\sum_{j=1}^k m_j = n \log_2(k) - (k-1)$ , when  $n = km$ , and the number of data moves is  $n$  with  $O(n)$  additional memory. We use the principles of (1) Block partitioning, (2) Data Encoding, (3) the Encoded Binary Selection Tree and (4) the Internal Buffer to develop an optimum algorithm that merges k sorted lists in-place. For block size  $\nu = \sqrt{m}$ , our algorithm does no more than  $\{(n-k-2) + \nu(2k-1)\} \log_2(k) + \{(\nu(k-1) - k) \log_2(\nu) + k - 2\}$  comparisons and  $4n + 8(k(\nu-1) - \nu)$  moves.

We use our basic k-way merge to implement an in-place merge-sort of N values with the use of no more than  $N \log_2(N) - N\lambda + N\{\frac{\lambda}{k} + 1 + \log_2(k)\} + O(\log_2(N))$  comparisons and  $2N(\lambda + 4)$  data moves. Where  $\lambda = \log_2(N) / \log_2(k)$ . We use additional constant memory to reduce the number of data moves to no more than  $2N(\lambda + 2)$ . By setting  $k = N^\epsilon$ , where  $0 < \epsilon < 1$ , we improve the number of data moves to no more than  $6N\epsilon + o(N)$  moves while maintaining about the same number of comparisons.

We consider our results to be the best for in-place sort with optimum comparisons and  $O(N)$  data moves so far to those given in the literatures. Our algorithm is a generalisation of that given in

[www.dcs.kcl.ac.uk/technical-reports/papers/TR-04-05.pdf](http://www.dcs.kcl.ac.uk/technical-reports/papers/TR-04-05.pdf).

Key Terms: Binary numbers, Binary selection tree, Block partition, Internal buffer, Internal merge, k-way merge, In-place and stable merge, Operational cost, Operational complexity analysis.

**John Faben**, QMUL, [j.faben@qmul.ac.uk](mailto:j.faben@qmul.ac.uk)

*The complexity of counting H-colourings modulo 2, when H is a tree:* The H-colouring, or Graph Homomorphism problem is a natural generalisation of the problem of graph colouring. It has been established by Hell and Nesetril that dichotomy theorems exist for the decision version of H-colouring: an H-colouring problem is either NP-complete or in P; and for the counting version of the H-colouring problem (by Dyer and Greenhill): an H colouring problem is either #P-complete or in FP.

Modular counting classes, and specifically parity P (counting the number of solutions to NP problems modulo 2) were introduced by Valiant in the late seventies, and there has been recent work showing some interesting hardness results for modular classes. We look at the problem of counting H-colourings modulo 2, and conjecture a complexity dichotomy for this problem - we prove that the dichotomy holds in the case where we require H to be a tree.

**Vashti Galpin**, LFCS, School of Informatics, University of Edinburgh,  
[Vashti.Galpin@ed.ac.uk](mailto:Vashti.Galpin@ed.ac.uk)

*Bisimulations for biology:* In recent year, process algebras have been used to model biological systems. The main methods of analysis applied to these models are stochastic simulation and deterministic evaluation via ordinary differential equations, as both can be

achieved without the overhead of transition system construction and the attendant state space explosion problem when considering large molecular counts.

The stochastic process algebra Bio-PEPA, developed specifically for systems biology, permits concentrations to be discretised and for molecular counts to be stratified, effectively reducing the number of states and hence offering access to transition-system-based analysis techniques such as those based on continuous time Markov chains. Additionally, this allows for the definition of semantic equivalences in the process algebra tradition.

In this presentation, different approaches to developing equivalences for biological modelling will be described, together with the progress that has been made in each approach. Additionally, applicability of these equivalences beyond Bio-PEPA will be discussed.

**Neelam Gohar**, University of Liverpool, UK, [neego@liv.ac.uk](mailto:neego@liv.ac.uk)

*Tactical and Manipulative dynamics*: Social choice theory investigates many kinds of multiperson decision-making problems. The unifying element in Social choice studies is the desire to understand “preference aggregation,” the way that individual different preferences combine into a policy. Voting provide a broad framework for preference aggregation. One key problem voting schemes are confronted with is that of manipulation where a voter lies about their preferences in the hope of improving the election’s outcome. We analyze the sequences of votes that may result from various voters performing “tactical voting” in unweighted setting and “manipulative voting dynamics” in weighted votes setting. We show that the process of making tactical vote and manipulative vote terminates at some point. We study the number of steps required to reach a state where no voter has incentive to migrate. For manipulative dynamics the only restriction is that a voter migrates to a new winner with increased support than the previous winner. We consider the voting protocols that can be manipulated in polynomial time like plurality, borda and Copeland.

**David Hopkins**, University of Oxford, [david.hopkins@st-hughs.ox.ac.uk](mailto:david.hopkins@st-hughs.ox.ac.uk)

*Game Semantics and Symbolic Execution*: Game semantic models of programming languages are often fully abstract yet concrete. This concrete nature lends itself well to model checking. In some cases, the strategy denotation of a term can be represented as an automaton, and observational equivalence of programs is reduced to language equivalence of the corresponding automata. When modelling the automata explicitly, however, we inevitably run into the state-space explosion problem. In recent years, some progress has been made on addressing this by combining general model checking techniques, such as on-the-fly model checking or CEGAR, with the game semantic approach. We present our work on using symbolic execution with the game semantic approach. We attempt to build up symbolic expressions in a way which reflects the symmetry of the games model and allows us to reduce program equivalence to a satisfiability problem.

**Markus Jalsenius**, University of Bristol, [m.jalsenius@bristol.ac.uk](mailto:m.jalsenius@bristol.ac.uk)

*Flood-It: The Colourful Game of Board Domination*: This talk is about the popular one player combinatorial game known as Flood-It. The player is given an  $n \times n$  board of tiles where each tile is allocated one of  $c$  colours. The goal is to make the colours of all tiles

equal via the shortest possible sequence of flooding operations. A flooding operation consists of the player choosing a colour  $k$ , which then changes the colour of all the tiles in the monochromatic region connected to the top left tile to  $k$ . After this operation has been performed, neighbouring regions which are already of the chosen colour  $k$  will then also become connected, thereby extending the monochromatic region of the board.

Various interesting facts about Flood-It will be presented. For example, we will see that finding an optimal solution is NP-hard if the number of colours is at least three, we will take a look at greedy approaches and give some approximation results and examples of “most difficult” boards. We will also consider random boards and analyse the complexity of the game when the player can perform flooding operations from any position on the board.

For those interested in playing the game, publicly available versions, including our own implementation, can be found linked from <http://floodit.cs.bris.ac.uk>.

Joint work with David Arthur, Raphael Clifford, Ashley Montanaro and Benjamin Sach.

**Phillip James**, Swansea University, [cspj@swansea.ac.uk](mailto:cspj@swansea.ac.uk)

*Verification of train control systems: Reducing the complexity:* In this talk, we present results on the successful application of various SAT-based model checking techniques to verify train control systems. We use propositional logic to model control systems and finite automaton to model the execution of such control systems. We report on slicing, a method which has been applied to reduce the complexity of the verification process, namely through state space reduction. We also review some current work to reduce the state space further, via the extraction of functional dependencies. Finally, we comment on results obtained when verifying real world train control systems.

**Mark Jerrum**, Queen Mary, University of London, [m.jerrum@qmul.ac.uk](mailto:m.jerrum@qmul.ac.uk)

*Approximating the Tutte polynomial: another status report:* The Tutte polynomial of a graph  $G$  is a two-variable polynomial  $T(G; x, y)$ , which encodes much information about  $G$ . The number of spanning trees in  $G$ , the number of acyclic orientations of  $G$ , and the partition function of the  $q$ -state Potts model are all specialisations of the Tutte polynomial. The phrase “mapping the Tutte plane” is shorthand for determining, for each pair  $(x, y)$ , the computational complexity of the map  $G \mapsto T(G; x, y)$ . For exact computation, this mapping was done in detail by Jaeger, Vertigan and Welsh two decades ago. For approximate computation (within specified relative error), the picture is still incomplete. I gave a talk in Edinburgh in 2006 with almost the same title. However, there has been substantial progress in the meantime, and almost all the material will be post-2006 (by a considerable margin).

This is joint work with Leslie Ann Goldberg (Liverpool).

**Karim Kanso**, Swansea University, [cskarim@swan.ac.uk](mailto:cskarim@swan.ac.uk)

*Model Checking from a Type Theoretic Platform:* Theorem proving can be a complicated task; tools have been developed

to reduce the complexity, so that the user can focus on a simplified core proof.

This project is concerned with the theorem prover and dependently typed programming language, Agda. The problem of simplifying Agda proofs by applying existing theorem provers is explored. An outline of a generic connection is presented. Briefly this entails defining what it means for a formula (i.e. propositional, LTL, CTL) to hold w.r.t. a model, defining a decision procedure and proving its correctness in Agda. As a case study of the above mechanism, the model checking theory is presented.

**Christian Kissig**, University of Leicester, [christian@mcs.le.ac.uk](mailto:christian@mcs.le.ac.uk)

*Trace Semantics for Coalgebras*: Coalgebras for a functor  $T$  in the category  $\text{Set}$  of sets and functions generalise state-based and possibly non-terminating transition systems. Their semantics in the final  $T$ -coalgebra defines  $T$ -behaviour which identifies precisely  $T$ -bisimilar states.

Previous work on generic trace theory has shown that structuring additionally in a  $\text{Set}$ -monad  $B$  introduces branching which subsumes non-determinism, probabilism and graded branching. We call coalgebras with branching type  $B$  and transition type  $T$   $(B,T)$ -coalgebras.

Semantics by  $BT$ -behaviour turns out to be unsuitable for  $(B,T)$ -coalgebras. Jacobs et al defined an alternative semantics by lifting into the Kleisli-category. The so obtained semantics is known as trace semantics. We distinguish semantics in finite and infinite traces. Jacobs gave a uniform definition for the first, but for the latter only in the case of non-deterministic branching.

In this talk we present infinite trace semantics generic for a large class of branching and transition types. We characterise the codomain of infinite trace semantics as Cauchy converging sequences. The characterisation is based on a stratified axiomatisation of infinite traces from  $T$ -behaviour and a span which describes whether the continuation in a trace is plausible. Infinite trace semantics is not unique.

**Oliver Kullmann**, Computer Science, Swansea University,  
[O.Kullmann@Swansea.ac.uk](mailto:O.Kullmann@Swansea.ac.uk)

*Green-Tao numbers and SAT*: The field of Ramsey theory offers great opportunities for improving our understanding of SAT solving: try solving the many divers problem instances arising when computing (concrete) Ramsey-type numbers, and understand/improve what's happening.

Van der Waerden numbers are obtained when seeking the smallest  $n$  such that partitioning the first  $n$  number into a given number of parts is guaranteed to produce an arithmetic progression of a given length. We have introduced *Green-Tao numbers*, defined analogously to van der Waerden numbers, but using the first  $n$  *prime numbers* instead of the first  $n$  natural numbers. The existence of these numbers is guaranteed by the Green-Tao theorem (which runs under the slogan "there are arithmetic progressions of arbitrary size in the primes"). In my talk I want to report on our first findings regarding these Green-Tao numbers, what these findings might have to offer to mathematics (in the future), and



what the whole undertaking of computing Ramsey-type numbers quite likely can offer for the SAT community.

**Oded Lachish**, University of Warwick, `oded@dcs.warwick.ac.uk`

*Two-phase algorithms for the parametric shortest path problem:* A *parametric weighted graph* is a graph whose edges are labeled with continuous real functions of a single common variable. For any instantiation of the variable, one obtains a standard edge-weighted graph. Parametric weighted graph problems are generalizations of weighted graph problems, and arise in various natural scenarios. Parametric weighted graph algorithms consist of two phases. A *preprocessing phase* whose input is a parametric weighted graph, and whose output is a data structure, the advice, that is later used by the *instantiation phase*, where a specific value for the variable is given. The instantiation phase outputs the solution to the (standard) weighted graph problem that arises from the instantiation. The goal is to have the running time of the instantiation phase supersede the running time of any algorithm that solves the weighted graph problem from scratch, by taking advantage of the advice. We construct several parametric algorithms for the shortest path problem.

**Iain Lane**, University of Nottingham, `ial@cs.nott.ac.uk`

*Presheaf models of local state:* Local state is a computational effect in which computations may create and refer to mutable reference cells. This effect is employed extensively when specifying imperative computations. These are what we wish to understand.

Current approaches to specifying imperative computations include monads in Haskell, uniqueness types in clean, and the Ynot system developed by Morrisett et al. at Harvard.

In this talk, I will describe work undertaken jointly with Thorsten Altenkirch to give a model of local state, which has an implementation in the dependently typed functional programming language Agda. This model is based on the concept of *presheaves* from category theory, and builds on previous work on functional specifications conceived by Swierstra. We also build on work by Plotkin and Power.

By giving a specification of computations involving local state, we are able to capture and describe how programs interact with their environment. A key property of such programs is *monotonicity* of resources — once a reference cell is allocated, it can never be deallocated. In this way, our model is reminiscent of Haskell's ST monad.

I will open by discussing the context in which the work is undertaken, before moving on to the model's implementation and why we think it is correct. Finally I will discuss where we want to go in the future.

**Andy Lawrence**, Swansea University, `csal@swansea.ac.uk`

*Verification of Railway Interlockings in SCADE:* This MRes (Master of Research) Logic and Computation project is concerned with the correctness of railway interlockings, carried out in collaboration with the company Invensys Rail. More specifically, the aim of the project is to investigate the modelling and model checking capabilities of the SCADE suite from Esterel Technologies and find out how they can be applied to interlockings. By looking at case studies conducted in previous MRes projects at Swansea I will be able to make comparisons between the previous techniques applied and the techniques used in the SCADE suite.

**David Manlove**, University of Glasgow, davidm@dcs.gla.ac.uk

*Optimising paired and pooled kidney exchanges:* Recent changes in legislation in the UK have allowed a patient who requires a kidney transplant, and who has a willing but incompatible donor, to be involved in a “pairwise kidney exchange” with another patient-donor pair in a similar position. “Pooled donations” extend this concept to three or more couples in a cyclic manner. NHS Blood and Transplant (NHSBT) run the National Matching Scheme for Paired Donation (NMSPD), which finds pairwise and 3-way exchanges (the latter being pooled exchanges involving three couples) at regular intervals. This matching scheme is based on optimising firstly the number of transplants, and subject to this, the total weight of the transplants, based on a scoring system that incorporates a number of factors including sensitivity, HLA compatibility, age and geographic location.

In this talk we describe three computational techniques that we have used in order to construct optimal exchanges for quarterly matching runs of the NMSPD between July 2008 and April 2010. The first two of these involve polynomial-time algorithms, based on weighted matching in graphs, to find an optimal set of exchanges and are implemented in C++. The third technique deals with an NP-hard optimisation problem, and uses integer linear programming, implemented in Matlab. We present a summary of the results that we obtained for the matching runs, as applied to anonymous data supplied by NHSBT.

This is joint work with Péter Biró and Kirstin MacDonald.

**Antony McCabe**, University of Liverpool, a.mccabe@liv.ac.uk

*Examining Frugality in Simple Procurement Auctions:* (Joint work with Professor Leslie Ann Goldberg and Professor Paul W. Goldberg.)

In this setting, we have a single buyer, who wishes to procure at least an integer quantity  $Q$  of some homogenous commodity from a number of sellers by auction. We aim to measure the ‘frugality’ of truthful mechanisms, which means comparing the price paid by a truthful mechanism to some ‘benchmark’ considered to be a reasonable lower-bound. For a mechanism to be truthful it must conduct the auction in a way that means sellers will never benefit by declaring some value which is not their true valuation.

We show that, even where every seller has a quantity of exactly 1 or 2, the well-known, truthful, VCG mechanism may overpay by a factor of  $Q$  (relative to the benchmark). We propose an alternative truthful mechanism, using scaling to create virtual bids, that reduces this worst-case to  $3\sqrt{Q}$ , and show that any virtual-bid scaling mechanism of this type must overpay by at least a factor of  $\sqrt{Q}$ . We also consider the more general case, where sellers may have quantity  $\{1, \dots, Q\}$ , and show a lower-bound that is close to  $Q$  for similar scaling mechanisms in this setting.

**Ashley Montanaro**, University of Bristol, montanar@cs.bris.ac.uk

*Quantum search with advice:* One of the most famous results in the field of quantum computation is Grover’s algorithm, which shows that quantum computers can search an unstructured list for a special “marked” item more efficiently than classical computers. However, in realistic search problems, there is often some prior information (“advice”) about the location of the marked item. This can be used to guide the search process, and sometimes obtain much better performance than naive unstructured quantum search.

In this talk, I will discuss new quantum algorithms that take advantage of such advice, given in the form of a probability distribution. The algorithms can achieve significant speed-ups over any possible classical algorithm. In some cases, exponential or even super-exponential speed-ups (on average) can be achieved.

This talk is based on the paper [arXiv:0908.3066](https://arxiv.org/abs/0908.3066).

**Thomas Nickson**, University of Liverpool, [tnickson@liverpool.ac.uk](mailto:tnickson@liverpool.ac.uk)

*Geometric Computations by a Graph Dynamical System on a Square Grid:* This talk will present a number of geometric problems for networks of finite automata. Network topology is a graph that is a subset of  $Z^2$ . It is shown that in this model it is possible to reason, in a distributed way, about the underlying properties of the graph. We describe an algorithm for the election of nodes that represent the 'center of gravity' of these graphs, as well as an algorithm for partitioning. Two methods of geometric computation are proposed, one, defines the automata's final state by the difference between activation signals, the other, defines it through message passing. The algorithms are finally analysed with respects to a variety of constraints possible within the model including the size of the alphabet and the synchronicity of the automata.

**Fredrik Nordvall Forsberg**, Swansea University, [csfnf@swansea.ac.uk](mailto:csfnf@swansea.ac.uk)

*Inductive-inductive definitions:* Induction is a powerful and important principle of definition, perhaps especially so in dependent type theory and constructive mathematics. However, many rather natural constructions cannot be introduced by ordinary inductive definitions alone, such as lists of a certain length or universes in type theory. This leads us to consider variants such as indexed inductive definitions, where a family of sets is simultaneously inductively defined, or inductive-recursive definitions, where a set  $U$  is inductively defined together with a recursive function  $T : U \rightarrow D$  for some fixed (large) type  $D$ .

In this talk, we will introduce yet another variant, called *induction-induction*, which generalises indexed inductive definitions. Induction-induction gives the possibility to simultaneously introduce a set  $A$  together with an  $A$ -indexed set  $B$ , i.e. for every  $a : A$ ,  $B(a)$  is a set. Both  $A$  and  $B(a)$  are inductively defined, and the constructors for  $A$  can also refer to  $B$  and vice versa.

Instances of induction-induction have implicitly been used by several researchers (Dybjer, Danielsson, Chapman) to model type theory inside type theory, and inductive-inductive definitions are available in the proof assistant/ programming language Agda, but without justification of the principle.

**Liam O'Reilly**, Swansea University, [csliam@swansea.ac.uk](mailto:csliam@swansea.ac.uk)

*Compositional Based Reasoning in CSP-CASL:* Specification languages, like programming languages, need hierarchy in order to make system descriptions comprehensible by offering modularity. In our talk we address the question of how to utilize such structural information in proofs.

Here, we enrich the specification language CSP-CASL by the institution independent structuring mechanisms of CASL. CSP-CASL provides an integrated view on processes and data, as needed for the description of distributed computer applications such as flight

booking systems, web services and electronic payment systems. In a second step, we exploit the structure information available to ease reasoning.

**Daniel Paulusma**, Durham University, [daniel.paulusma@durham.ac.uk](mailto:daniel.paulusma@durham.ac.uk)

*The k-in-a-path problem for claw-free graphs*: Testing whether there is an induced path in a graph spanning  $k$  given vertices is NP-complete in general graphs, already when  $k = 3$ . We show how to solve this problem in polynomial time on claw-free graphs, when  $k$  is a fixed integer not part of the input. When  $k$  is part of the input, we show that this problem is NP-complete, even for the class of line graphs, which form a subclass of the class of claw-free graphs.

(joint work with Jiří Fiala, Marcin Kamiński and Bernard Lidický)

**Alexandru Popa**, University of Bristol, [popa@cs.bris.ac.uk](mailto:popa@cs.bris.ac.uk)

*Permuted Common Supersequence*: The Shortest Common Supersequence (SCS) is a well studied problem having a wide range of applications. In this talk we first introduce a new problem closely related to the SCS, denoted as the PCS problem. Given a set  $L$  of  $k$  strings,  $s_1, s_2, \dots, s_k$ , and a text  $t$ , the goal is to find a permutation  $\pi(t)$  of the text  $t$ , such that as many input strings of the set  $L$  are subsequences of  $\pi(t)$ . We first show hardness results for the problem in its most general setting and for several restricted variants: when all the strings are of length 2 and when the alphabet is binary. Moreover, we present approximation algorithms for two variants of the PCS problem, the first is a  $2/(1 + \Omega(1/\sqrt{\Delta}))$  approximation algorithm for the case where all input strings are of length 2, where  $\Delta$  is the number of occurrences of the most frequent character. Then, for PCS instances such that each character of  $t$  is unique, we present a simple randomized approximation algorithm that achieves a constant approximation ratio when the length of the longest string in  $L$  is fixed. In the second part of this talk, we present approximation algorithms for several restricted variants of the SCS problem.

**Christopher M. Poskitt**, The University of York, [cposkitt@cs.york.ac.uk](mailto:cposkitt@cs.york.ac.uk)

*Towards a Hoare Calculus for Graph Programs*: Graph programs, comprised of graph transformation rules and simple control constructs directing their nondeterministic application, allow programmers to solve graph problems at a high level of abstraction, freeing them from the difficulties of low level data structures. Whereas the state of a “classic” program is the value of all program variables at a specific time, the state of a graph program is the graph on which the rules are operating. We present a preliminary system of proof rules for verifying the partial correctness of graph programs, discuss the use of the rules and their properties, and highlight challenges such as choosing an appropriate formalism for specifying graph properties.

**Radhakrishnan DelhiBabu**, Anna University, [rdelhibabu@gmail.com](mailto:rdelhibabu@gmail.com)

*Updating Logical Database*: We live in a constantly changing world and consequence our belief and knowledge on the state of the world change over time. This notion of change manifests itself in application such as database updates etc. This raises two major questions to be answered: *when are we sure that we carry out change rationally?* and *How this can be implemented for a specific application* so far, these question have been dealt

with separately: various philosophical works on belief dynamics giving the postulates to satisfied by a rational changes through view deletion [1,2].

In this presentation I provide as assessment as to what Jack Minker [3] has been achieved since the field started as a distinct discipline and also my contribution of work how knowledge base dynamics can provide an axiomatic characterization for view insertion in to database.

[1] Aravindan C and Dung,P.M, *Dynamics of Belief: Epistemology,Abduction and Database Updates*, Dissertation No.CS-95-2(AIT,Bangkok)

[2] Aravindan C and Baumgartner P, Theorem Proving for View Deletion in Databases, *Journal of Symbolic Computation* 29, 200, pp. 119–147.

[3] Jack Minker, Logic and Database: a 20 year Retrospective Updated in Honor of Ray Reiter, *Logic Foundations for Cognitive Agents*, 1999, pp. 234–275.

**Stephan Reiff-Marganiec**, University of Leicester, srm13@le.ac.uk

*Selecting the Right Service at the Right Time*: Service oriented computing allows to dynamically bind to service, which might be part of a workflow, as and when they are required. One crucial problem arising is that of identifying the right service given a user's current context and the context of the services – needless to say that the environment is highly dynamic in that context changes and service might become un(available). There are two general choices available when selecting services: one can make a decision for a specific service in isolation trying to achieve a local optimum or one can instantiate the whole workflow aiming to gain a global optimum.

In this talk we will review these two options and consider their drawbacks and benefits in terms of their complexity as well as practicality. We will present a proposed new approach that aims to fill a middle ground.

**Benjamin Sach**, University of Bristol, ben@cs.bris.ac.uk

*Pattern matching algorithms for streaming data*: Many sophisticated methods have been developed for pattern matching under a variety of measures of distance over recent years. However, almost without exception these have been analysed in models of computation where it is assumed that all of the data can be accessed at any time. We consider the problem of pattern matching in streaming data where symbols arrive one at a time and at great speed. Here, not only is there a restriction on the storage space available but we also require any new matches that are found to be reported as soon as they occur. We will discuss recent results and the degree to which the gap between the running time of the best online and offline algorithms can be closed.

**Rafiq Saleh**, University of Liverpool, R.A.Saleh@liv.ac.uk

*On descriptive complexity of knot properties*: We investigate the descriptive complexity of knot problems and show lower and upper bounds for the planarity problem of knot diagrams represented by Gauss words.

We study these problems in the context of automata models over an infinite alphabet and by their expressibility in first order logic and its extensions. In particular we show that planarity of unsigned Gauss words is recognisable by 2-way co-nondeterministic register automata over an infinite alphabet. Although this result is incomparable with the result

of B.Courcelle on MSO definability of planarity of Gauss words, it tightens the known bounds in terms of register automata model.

**Iain Stewart**, Durham University, [i.a.stewart@durham.ac.uk](mailto:i.a.stewart@durham.ac.uk)

*A general algorithm for detecting faults under the comparison diagnosis model:* We develop a widely applicable algorithm to solve the fault diagnosis problem in certain distributed-memory multiprocessor systems in which there are a limited number of faulty processors. In particular, we prove that if the underlying graph forming the interconnection network has connectivity no less than its diagnosability  $\delta$  and can be partitioned into enough connected components of large enough size then given a syndrome of test results under the comparison diagnosis model resulting from some set of faulty nodes of size at most  $\delta$ , we can find the actual set of faulty nodes with time complexity  $O(\Delta N)$ , where  $\Delta$  is the maximal degree of any node of the graph and  $N$  is the number of nodes.

**Rick Thomas**, University of Leicester, [rmt@mcs.le.ac.uk](mailto:rmt@mcs.le.ac.uk)

*Word problems of groups and complexity classes:* There are several intriguing links between group theory and formal language theory. One such connection is the consideration of which groups  $G$  have a word problem lying in a particular class  $\mathcal{F}$  of formal languages.

A slightly surprising feature is that we can find examples of naturally occurring classes of languages  $\mathcal{F}_1$  and  $\mathcal{F}_2$  such that  $\mathcal{F}_1 \subset \mathcal{F}_2$  but such that the classes of groups whose word problems lie in  $\mathcal{F}_1$  and  $\mathcal{F}_2$  coincide. One such case is where  $\mathcal{F}_1$  is the class of deterministic context-free languages and  $\mathcal{F}_2$  is the class of context-free languages; this follows from the beautiful result of Muller and Schupp which says that a finitely generated group has a context-free or deterministic context-free word problem if and only if it has a free subgroup of finite index. Indeed, by a result of Autebert, Boasson and Sénizergues, this is still the case if we replace the class of deterministic context-free languages by the class of NTS languages

The point here is that there are some significant restrictions imposed on a language by insisting that it is the word problem of a group; a consequence of this is the type of situation described above. The aim of this talk is to describe some sufficient conditions on the classes  $\mathcal{F}_1$  and  $\mathcal{F}_2$  to ensure that this situation does not occur, i.e. that there really are groups whose word problem lies in  $\mathcal{F}_2$  but not in  $\mathcal{F}_1$ . In our case the families  $\mathcal{F}_1$  and  $\mathcal{F}_2$  will be space complexity classes and the groups we construct will all have decidable word problem. This is joint work with Steve Lakin.

**German Tischler**, King's College London, [german.tischler@kcl.ac.uk](mailto:german.tischler@kcl.ac.uk)

*Linear Time Computation of Longest Previous non-overlapping Factors:* The Longest Previous non-overlapping Factor table (LPnF) stores for each position of a string the maximal length of factors occurring both there and in the preceding part of the string. The notion is a slight variant of the Longest Previous Factor (LPF) table described before and used for text compression. The LPnF table is an essential element for the design of efficient algorithms on strings as it is related to a certain type of Ziv-Lempel factorisation used for this purpose. We show how to compute the LPnF table in linear time from the suffix array of the string when it is drawn from an integer alphabet. The algorithm

is a non-immediate extension of the LPF computation and it does not require any other sophisticated data structure than the suffix array of the input string.

**Anthony Widjaja To**, University of Edinburgh, [anthony.w.to@ed.ac.uk](mailto:anthony.w.to@ed.ac.uk)

*Parikh Images of Regular Languages: Complexity and Applications:* We show that the Parikh image of the language of an NFA with  $n$  states over an alphabet of size  $k$  can be described as a finite union of linear sets with at most  $k$  generators and total size polynomial for all fixed  $k \geq 1$ . Previously, it was not known whether the number of generators could be made independent of  $n$ , and best upper bounds on the total size were exponential in  $n$ . Furthermore, we give an polynomial algorithm for performing such a translation for all fixed  $k \geq 1$ . Our proof exploits a previously unknown connection to the theory of convex sets, and establishes a normal form theorem for semilinear sets, which is of independent interests. To complement these results, we show that our upper bounds are tight and that the results cannot be extended to context-free languages. We give four applications: (1) a new polynomial fragment of integer programming, (2) precise complexity of membership for Parikh images of NFAs, (3) an answer to an open question about polynomial PAC-learnability of semilinear sets, and (4) an optimal algorithm for LTL model checking over discrete-timed reversal-bounded counter systems.

**Carmine Ventre**, University of Liverpool, [carmine.ventre@gmail.com](mailto:carmine.ventre@gmail.com)

*Ranking Games that have Competitiveness-based Strategies:* In this talk we consider — from the perspective of efficient computation— a type of competition that is widespread throughout the plant and animal kingdoms, higher education, politics and artificial contests. In this setting, an agent gains utility from his relative performance (on some measurable criterion) against other agents, as opposed to his absolute performance. Each strategy corresponds to a level of competitiveness, and incurs an upfront cost that is higher for more competitive strategies. We study the Nash equilibria of these games, and polynomial-time algorithms for computing them. For games in which there is no tie between agents' levels of competitiveness we give a polynomial-time algorithm for computing an exact equilibrium in the 2-player case, and a characterization of Nash equilibria that shows an interesting parallel between these games and unrestricted 2-player games in normal form. When ties are allowed, via a reduction from these games to a subclass of anonymous games, we give polynomial-time approximation schemes for two special cases: constant-sized set of strategies, and constant number of players. The latter result is improved to a fully polynomial-time approximation scheme when the constant number of players only compete to win the game, i.e. to be ranked first.

This is a joint work with Leslie Ann Goldberg, Paul W. Goldberg and Piotr Krysta.

**Pim van 't Hof**, Durham University, [pim.vanthof@dur.ac.uk](mailto:pim.vanthof@dur.ac.uk)

*On graph contractions and induced minors:* The INDUCED MINOR CONTAINMENT problem takes as input two graphs  $G$  and  $H$ , and asks whether  $G$  has  $H$  as an induced minor. We show that this problem is fixed parameter tractable in  $|V(H)|$  if  $G$  belongs to any minor-closed graph class and  $H$  is a planar graph. For a fixed graph  $H$ , the  $H$ -CONTRACTIBILITY problem is to decide whether a graph can be contracted to  $H$ . The computational complexity classification of this problem is still open. So far,  $H$  has a dominating vertex in all

cases known to be polynomially solvable, whereas  $H$  does not have such a vertex in all cases known to be NP-complete. Here, we present a class of graphs  $H$  with a dominating vertex for which  $H$ -CONTRACTIBILITY is NP-complete. We also present a new class of graphs  $H$  for which  $H$ -CONTRACTIBILITY is solvable in polynomial time. Finally, we study the  $(H, v)$ -CONTRACTIBILITY problem, where  $v$  is a vertex of  $H$ . The input of this problem is a graph  $G$  and an integer  $k$ , and the question is whether  $G$  is  $H$ -contractible such that the “bag” of  $G$  corresponding to  $v$  contains at least  $k$  vertices. We show that this problem is NP-complete whenever  $H$  is connected and  $v$  is not a dominating vertex of  $H$ .

*Joint work with Marcin Kamiński, Daniël Paulusma, Dimitrios M. Thilikos and Stefan Szeider.*

**Standa Živný**, University of Oxford, [standa.zivny@comlab.ox.ac.uk](mailto:standa.zivny@comlab.ox.ac.uk)

*Generalising Bisubmodularity to Domains of Arbitrary Size:* Submodular functions play a key role in combinatorial optimisation and in the study of Valued Constraint Satisfaction Problems. Bisubmodular functions are an important extension of submodular functions to domains of size 3. We generalise bisubmodular functions to domains of arbitrary size. Over a domain of size  $k + 1$ , these functions are called *k-submodular*. We prove that that for any  $k \geq 1$  the minimisation problem for locally-defined  $k$ -submodular functions is solvable in polynomial time, but any extension is NP-hard. Our results provide a new maximal tractable class of VCSPs over domains of arbitrary size.

Joint work with Martin Cooper (University of Toulouse).