Report on BCTCS18.
7-10 April 2002
HP Laboratories Bristol.

Chris Tofts

1 The Conference

This years *British Colloquim on Theoretical Conputer Science*, was held at HP Laboratories Bristol http://www.hpl.hp.com/bristol/index.html. There were 7 invited presentations and 26 contributed presentations the abstracts of which are presented below. PhD student attendance at the meeting was supported by a combination of EPSRC and HP funding. The London Mathematical Society supported the travel of
Prof. Paul Spirakis.

2 Invited Talks

Engineering with Randomness
Neil Davies, Degree2 Innovations.

The Internet is beginning to mature, but to create services requires new solutions to the management of the network. To make money services need to be reliable, predictable and, most importantly, deliverable. Interestingly we have found that re-engineering the behaviour of network components to behave consistently with mathematical assumptions, offers a whole approach to achieving these aims. In this talk I will outline the way in which designing and building network equipment that behaves explicitly randomly offers a practical solution.

Complexity as Expressive Power
Anuj Dawar, Cambridge University.

One of the achievements of descriptive complexity theory is to characterise computational complexity in terms of the expressive power of languages. So, we can understand the limitations of a language in terms of time and space complexity. However, logical languages also imposc other limitations, in terms of their ability to distinguish structures (or descriptions of structures). The interaction between these two kinds of limitations have given rise to some of the most interesting questions and results of descriptive complexity theory - such as whether there is a language for isomorphism-invariant polynomial time; finite variable equivalence and bisimulation-invariant complexity. In this talk, I will examine this interaction through a survey of some such results and questions.

An Extended Analytic Methodology for Arbitrary Queueing Networks
Demetres Kouvatsos, Bradford University.

The performance modelling and quantitative analysis of heterogeneous telecommunication systems, such as terrestrial and mobile networks, constitute a rapidly growing research area due to their ever expanding usage and the multiplicity of their component parts together with the complexity of their functioning. Inherent problems and open issues associated these systems, such as traffic characterisation of multiple packet classes under congestion control schemes, blocking mechanisms and buffer management policies, need to be addressed further and resolved before a global integrated broadband network infrastructure can be established. Queueing network models (QNMs) are widely recognised as powerful and realistic tools for the performance monitoring and prediction of these discrete flow systems. However, analytic algorithms for QNMs are often hindered by the generation of large state spaces requiring further approximations and a considerable (or, even prohibitive) amount of computation.

The talk will focus on the characterisation of an extended maximum entropy (ME) product-form approximation, subject to appropriate flow formulae and queueing theoretic constraints, leading to the development of a universal queue-by-queue decomposition algorithm for the stochastic analysis of arbitrary open QNMs with non-exponential inter arrival and service times, mixed (priority and non-priority) classes of jobs, repetitive service (RSB) blocking and complete (CBS) and partial (PBS) buffer sharing schemes. Consequently, explicit performance expressions for individual finite capacity station queues with a sequence of class buffer thresholds are presented, as cost-effective building blocks in the solution process. Highlights of ME applications will be included relating to the congestion control of multi-buffered ATM switch architectures and the performance modelling of a wireless GSM/GPRS cell.

A Tail of a Dog
Brian McBride, HP Labs Bristol.

The widespread adoption of the web led, in the later half of the 90's to a number of disparate efforts to provide metadata describing the resources available on it. These efforts coalesced into a common language known as the Resource Description Framework (RDF).

This talk will describe the RDF data model and difficulties arising from the first attempt at its formalization. It will describe how a new working group has applied model theory to clarify the semantics of the language. It will conclude by identifying other areas of web architecture which could also from formalization.

Bigraphical Reactive Systems
Robin Milner, Cambridge University.

Forty years ago, Carl-Adam Petri devised the first substantial model of concurrent computation, and it was a graphical model. Since then there has been a steady flow of models and calculi in which the spatial metaphor is never far away; we often use terms like linkage, location, mobility, and so on.

The flow is increasing, with the challenge to understand mobility, security, and other properties of virtual and real networks. We shall soon have as many calculi as programming languages. I believe that the only way to achieve some unity is to represent **connectivity** and **locality** graphically, in an unconstrained form upon which different specific calculi can impose finer or stricter structure.

In the talk I shall describe **bigraphs**, which arise from the pi calculus, the ambient calculus and action calculi; they treat connectivity and locality orthogonally ("where you are does not affect who you can talk to"). I shall show with examples how the model specialises to familiar calculi. I shall also explain how the general theory of bigraphs uniformly yields labelled transition systems for which many behavioural relations –like

bisimilarity– are necessarily congruential. So bigraphs not only give a **framework** for a variety of models, but also provide a **core theory** which they can all use.

The talk will not presuppose any knowledge of calculi for concurrency.

Algorithmic aspects of game theory - Paul Spirakis, CTI Greece.

We discuss here recent results and some open problems in the fascinating crossing of game theoretic ideas with algorithms and complexity. In particular , we will try to exemplify a novel and timely genre of algorithmic problems in which the measure to be investigated is the cost of lack of coordination , due to the fact that competing computing entities act selfishly and spontaneously. This "cost of anarchy" tries to capture a phenomenon that reminds the cases of lack of information (in on line algorithms) or the lack of computational resources (as in the case of approximation algorithms). The notions of equilibriums (especially Nash equlibriums) , their worst case, and the notion of mechanisms (that can affect the game in a way in favour of the system) will be also discussed.

Computable and hierarchical models of physical systems
John Tucker, Swansea University

Many models of physical systems are algorithms, commonly derived from differential equations. These algorithms compute on discrete and, in particular, continuous data. This lecture will consider two theoretical questions about models of spatially extended dynamically systems.

1. What makes a dynamical system computable?
2. What role do levels of abstraction play in computationally modelling physical systems?

I will use the theory of synchronous concurrent algorithms to explore answers to these questions. A synchronous concurrent algorithm (SCA) is

a network of processing units operating in time and synchronized by a global clock. There are many examples of SCAs among algorithmic models of a system: cellular automata, neural nets, lattice models, some finite differences and element models etc.

The computability question involves my research with J I Zucker into the theory of computation on real numbers and its application to SCAs. The

hierarchy question involves my research with A V Holden and M J Poole into hybrid multilevel SCAs and its applications to modelling the whole

heart.

3 Contributed Talks

Linear Logic: from Stochastic Analysis to Software Testing
Manuela L. Bujorianu with Marius Bujorianu, Stirling University

In this talk we continue the research presented at the last edition of BCTCS. We have presented a linear logical framework, which provides a constructive logical foundation for Pure and Applied Mathematics, particularly to Stochastic Analysis. In this work we extend the framework to provide a logical foundation to Software Testing. The phase semantics of Linear Logic is interpreted in terms of testing activities and logical operations provide in this way tests operators. Connections with our our previous work in formal testing in a categorical logic setting are also sketched.

Run of Squares in Fibonacci Strings
Emmanouil Christodoulakis, King's College London.

A (finite) Fibonacci string F_n is defined as follows: $F_0 3Db$, $F_1 3Da$ and for every integer $n > 3D2, F_n 3DF_{n-1}F_{n-2}$. For $n > 3D1$, the length of F_n is denoted by $f_n 3D|F_n|$. The infinite Fibonacci string F is the string which contains

every $F_n, n > 3D1$, as a prefix. We specify all the squares of F_n in an appropriate encoding. This encoding is made possible by the fact that the squares of F_n occur consecutively, in "runs", the number of which is $\Theta(f_n)$. Suppose that F contains a set of $h > 0$ consecutive squares all of length $2p$. We say that $R(i,p,h)$ is a run of squares of length h, where i denotes the starting position of the first square. We then count the number of distinct squares $D(n)3D2(F_{n-2} - 1)$ $(n > 3D5)$ and repeated squares $R(n)3D(4/5)nF_n - (2/5)(n+6)F_{n-1} - 4F_{n-2} + n + 1$ $(n > 3D3)$.

Embeddings of Metrics on Strings and Permutations
Graham Cormode, Warwick University

Sequences represent a large class of fundamental objects in Computer Science — sets, strings, vectors and permutations are considered to be sequences. Distances between sequences measure their similarity, and computations based on distances are ubiquitous: either to compute the distance, or to use distance computation as part of a more complex problem. A very specific approach to solving questions of sequence distance is taken: sequences are embedded into other distance measures, so that distance in the new space approximates the original distance. This allows the solution of a variety of problems including:

- Fast computation of short 'sketches' in a variety of computing models, which allow sequences to be compared in constant time and space irrespective of the size of the original sequences.
- Approximate nearest neighbor and clustering problems, significantly faster than the naive exact solutions.
- Algorithms to find approximate occurences of pattern sequences in long text sequences in near linear time.
- Efficient communication schemes to approximate the distance between, and exchange, sequences in close to the optimal amount of communication.

Solutions are given for these problems for a variety of distances, including distances inspired by biological problems for permutations and powerful editing distances for strings.

A maximum performance specification, but no numbers. Formal Methods in Practice
Kerstin Eder, Bristol University

There still appears to be a wide gulf between theory and practice of formal methods. This talk presents one successful project where theory met a practical application in pipelined microprocessor design.

Getting the interlock logic that controls the pipeline flow of a pipelined design, e.g. a microprocessor, right first time is an important prerequisite for maximising pipeline throughput. Performance bugs in this area are often due to unnecessary pipeline stalls. Unnecessary pipeline stalls can only be eliminated when they can be distinguished from those stalls which are necessary to preserve functional correctness.

I will show how a maximum pipeline performance specification can be derived from a complete functional specification of the pipeline control logic. The specifications can be developed early in the design process and can support several design stages, including testing, property checking and even code generation.

Links Between Belief Revision and Abduction
Corinna Elsenbroich, King's College London

In the AGM theory of belief change there are three basic kinds of belief change: expansion, contraction and revision. For each of them rationality postulates (the AGM postulates) are proposed to constrain change-operators. In the investigations on abductive reasoning only expansion is considered. Some authors, such as R. Wassermann, suggest close links between belief expansion and abductive expansion so that postulates similar to the AGM postulates are used to constrain an abductive operator. However, the investigation of abductive reasoning found in the literature only considers expansion. In this work, we show that connections between abduction and revision are far more intimate and that we have to extend our concept of abduction to include the mechanisms of abductive revision and contraction. The motivation behind this is that a properly applicable abduction algorithm will be useful to resolve problems in database maintenance.

More specifically, the well known problem of updating through views in

relational databases. When updating through a view, the new information has to be mapped back to the base relations that define the view. This poses two main problems:

1. If a tuple is inserted through a view, and some columns of the base relations are not used in the view's definition, the information in the new tuple will not be sufficient to fill in the gaps in the base relations. Abduction can help to fill these gaps using predefined abduction rules and a set of possible entries into gaps.

2. Insertions through a view might cause inconsistencies in the base relations used in the view's definition. A revision or contraction abduction on the base can restore consistency.

Ordered Tree Logics
Ulle Endriss, King's College London

We introduce a family of modal logics with models that correspond to ordered trees. An ordered tree is a tree for which the children of each node are ordered. Branching may be finite or infinite and the orders declared over sibling nodes may be discrete, dense, or general linear orders. Our logics provide modal operators working both along the branches of a tree and along the order declared over the children of a node.

Such a logic can be useful to describe the temporal behaviour of a complex system consisting of several subsystems. In that sense, ordered tree logics are generalisations of propositional linear temporal logics. The additional modal operators allow us to "zoom" into a particular state and describe the temporal behaviour of the associated subsystem in more detail, without affecting, for example, the validity of next-operators referring to events on the main time line.

To prove decidability, we have investigated techniques to establish bounded finite model properties (fmp) for ordered tree logics. (A logic has the bounded fmp iff every satisfiable formula is also satisfiable in a model of bounded size, where the maximal size is a function of the length of the formula in question.)

Formalising Design Patterns using Algebraic Methods: A Case Study of the Iterator Pattern
Saad Al-Foudari, Newcastle University

Design patterns are outlines for tried and tested solutions for recurring problems in software development. They are becoming increasingly important for the design of reliable computing systems and provide an invaluable means of cataloguing proven solutions. One of the main problems with using design patterns at present is the informal way in which they are documented and the lack of any framework in which to reason about them. In this talk, we will consider using algebraic methods and support tools to formalise and reason about design patterns. Using the well-known iterator pattern as a case study, we consider how an abstract algebraic specification can be formulated which captures the key properties of the iterator pattern without losing its generality. We illustrate how concrete instances of the pattern can be shown to be correct with respect to this abstract specification using the Maude rewriting tool. We then consider a possible refinement of the iterator pattern which allows elements to be filtered out according to a given property. We show formally that this refinement is correct with respect to our abstract iterator specification.

Computational Behaviour of Spatio-Temporal Logics
David Gabelaia, King's College London

The presentation is meant to display a research area currently active at King's College London, Group of Logic and Computation. We present several combined systems which can be seen as a formal representation of a dynamic development of spatial data. We use temporal logics over various linear orders to represent the time dimension, while for the spatial representation RCC-8 or modal spatial logics are considered. Combinations of spatial and temporal languages allow us to develop numerous expressive formalisms which can be used as reasoning tools in KR or AI. Some of these formalisms have been proved decidable. In various cases upper bounds for complexity of satisfiability problem are known. The presentation will exhibit the present tasks and important remaining questions we are investigating in this area.

Algorithms for Guiding Clausal Temporal Resolution
M. Carmen Fernandez Gago, Liverpool University

Temporal logic is a variety of non-classical logic used in a range of areas within Computer Science and Artificial Intelligence. Consequently, different proof methods have been developed, implemented and applied. Our approach is based upon resolution. The resolution method is characterised for the translation into a normal form, classical resolution on formulae that occur at the same moment in time (step resolution) and temporal resolution between states. Although the clausal temporal resolution method has been proved, proved correct and implemented it sometimes generates an unneccesarily set of formulas that may be irrelevant to the refutation. Also, the temporal resolution operation requires the search for a set of clauses satisfying a specified condition. As the search for such a candidates is the most expensive part of the method, but it is likely to be required, our intention is to guide the search and, if possible, avoid all unnecessary step resolution. In this sense we propose one algorithm to guide the search and in cases where further searchs are needed, we propose a second algorithm based on the first one, which allows us to re-use infromation from the original searchs.

Towards a concise proof of the 4-colour problem of planar maps Alan Gibbons and Paul Sant, King's College London.

Extant proofs of the 4-colour theorem of planar maps are very long and rely upon computer time for checking certain details. We seek a concise proof independant of electronic computation. In this talk we present details of ongoing research in which we relate the 4-colour problem to one of so-called rotations in binary trees. The combinatorics developed so far are independentally interesting. This work, along with a missing proof of a intuitve lemma concerned with rotation distances between binary trees, would provide the concise proof of the 4-colour theorem that we seek. We describe circumstantial evidence for the validity of the lemma.

Game Semantics for Region Analysis Will Greenland, Oxford University

Region Analysis is a tool for program analysis which allows static (compile-time) determination of safe memory reclamation. As such, it offers a useful alternative to garbage collection, particularly in settings where space is at a premium, and when memory usage needs to be tightly controlled.

One obstacle to the study and implementation of Region Analysis is the complexity which results from the augmentation of any semantics with the store operations needed to model memory use. We seek to overcome this difficulty by proposing a game semantics for a region-annotated language, with the aim of providing correctness proofs for that language which also offer insights into the general behaviour of region-based memory systems.

Adding a Temporal Dimension to First-order Tableaux Roman Kontchakov, King's College London.

First-order temporal logic (FOTL) as well as various seemingly weak fragments of it are known to be undecidable and mostly not even recursively axiomatizable. Recently, however, Hodkinson, Wolter and Zakharyaschev have introduced the monodic fragment of FOTL (in which temporal operators may be applied only to formulas with not more than one free variable). The whole monodic fragment can be represented as a finite Hilbert-style axiomatic system. Moreover, it contains a number of decidable but yet expressive fragments (like the monodic guarded fragment, the monodic two-variable fragment, the monodic monadic fragment.) The decision procedures provided for these fragments are of model-theoretic character. A proof-theoretic (and possibly implementable) analysis of the decision problem for those fragments is missing so far. In this paper we are concerned with the following problem: Given a tableau-based decision procedure for some fragment F of first-order logic, how and under which conditions can this procedure be combined with Wolper's tableau procedure for propositional temporal logic, such that we obtain a tableau-based decision procedure for the monodic fragment of the temporal extension of F?

Approximate String Matching with Gaps for Musical Melodic Recognition
Masahiro Kurokawa, King's College London

This talk focuses on a set of string pattern matching problems that arise in musical analysis, and especially in musical information retrieval. A musical score can be viewed (at one level) as a string: at a very rudimentary level, the alphabet could simply be the set of notes in the chromatic or diatonic notation, or the set of intervals that appear between notes (e.g. pitch may be represented as MIDI numbers and pitch intervals as number of semitones). An important example of flexibility required in score searching arises from the nature of polyphonic music. Within a certain time span, each of the simultaneously performed voices in a musical composition does not, typically, contain the same number of notes. So 'melodic events' occurring in one voice may be separated from their neighbours in a score by intervening events in other voices. Since we cannot generally rely on voice information being present in the score we need to allow for temporal 'gaps' between events in the matched pattern. Typically, the magnitude of such a gap will be a parameter set by the user. In our mathematical treatment the allowance for gaps in the query and the score being searched is represented by the constant alpha. The gaps can be bounded or unbounded. We have designed efficient algorithms and implemented them with music pieces.

On Definability of Parametric Families of Labelled Transition Systems
Ranko Lazic, Warwick University

Logical relations and bisimulation can be used to define when a family of labelled transition systems (LTSs) is parametric. Intuitively, such a family corresponds to a parametrically polymorphic nondeterministic program. We present a result which states that, under certain restrictions on types, a parametric family of LTSs is definable by a symbolic LTS.

Validation of Partially Occluded Images
Manal Mohamed, King's College London.

In this paper we describe an implementation of the on-line validation algorithm for the analysis of occluded images, which was developed by Iliopoulos and Simpson. The algorithm operates on images represented in one dimension as strings and assumes objects within images are of the same length. We also investigate the decomposition of a given image into the set of (perhaps partially occluded) objects occurring in it.

Lower Bounds for Equivalence Checking One-Counter Automata
Faron Moller(Swansea University), Petr Jancar, Antonin Kucera and Zdenek Sawa.

We present a technique for proving DP-hardness of equivalence-checking problems on one-counter automata. To this end, we show a reduction from the DP-complete Sat-Unsat problem to the truth problem for a fragment of (Presburger) arithmetic. The fragment used is suited for transforming to simulation-like equivalences on one-counter automata. In this way we show that the membership problem for any relation subsuming bisimilarity and subsumed by simulation preorder is DP-hard (even) for one-counter nets (where the counter cannot be tested for zero). We also show DP-hardness for deciding simulation between one-counter automata and finite-state systems (in both directions).

A constructive refinement method for process algebras
Friedger Mueffke, Bristol University

Process algebras allow to reason about communicating systems in a formal way. Their strength lies in the ability to abstract from selected actions such that a relation between two systems can be established. Thereby, it is possible to verify that an implementation of a system satisfies its specification. However, it is often desirable to design a system from top to bottom in a way that provides a formal proof of the correctness of the implementation of the system. In software engineering the B method was developed to achieve such a verified design method. It uses abstract systems as the high level description and a general substitution language to stepwise refine the specification.

I'm currently working on integrating parts of the B method with process algebra to obtain a formal refinement methodology for the design of communication protocols. A process algebra based on CSP is extended by broadcast communication and a temporal logic that allows to reason about the action history of processes. Using this extension it is possible to model specifications in a similar way to abstract systems.

In the talk I will show how the extension simplifies the specification of communication protocols and how parts of the specification can be stepwise substituted until one has obtained a refined description of the system in classical process algebra. This implementation will satisfy the same properties as the specification and an additional verification is not necessary anymore.

Resolution for Interacting Logics of Knowledge and Time
Claudia Nalon, Liverpool University

We propose a new normal form for a temporal logics of knowledge, which simplifies the resolution calculus for this logic. Clauses in this normal form are classified according to the context (epistemic or temporal) to which they refer to. A set of resolution rules are then applied (repeatedly) to each context until a contradiction is found or no new clauses can be generated. We show that this proof method is sound, complete and terminating. We also consider particular interactions between knowledge and time, and show how the resolution method can be extended to deal with them.

Reasoning About Mobile Distributed Applications
Andrew Phillips, Imperial College London.

The Internet has grown substantially in recent years, and an increasing number of applications are now being developed to exploit this distributed infrastructure. Mobility is an important paradigm for such applications, where mobile code is supplied on demand and mobile components move freely within a given network. However, mobile distributed applications are notoriously difficult to develop. Not only do they involve complex parallel interactions between multiple components, but they must also satisfy strict requirements for security, reliability and correctness. It can be argued that a rigorous means of reasoning about mobile distributed computation is essential to the development of such applications.

This presentation introduces a new model for mobile distributed computation, the deltapi-calculus, and shows how it can be used to specify simple mobile distributed applications, in order to reason about their security and correctness properties. It also investigates the feasibility of developing a programming language and runtime system based on the deltapi model, as a means of bridging the gap between application specification and implementation.

Optimised Predecessor Data Structures for Internal Memory
Naila Rahman, Richard Cole and Rajeev Raman, King's College London.

We demonstrate the importance of reducing misses in the translation-lookaside buffer (TLB) for obtaining good performance on modern computer architectures. We focus on data structures for the dynamic predecessor problem: to maintain a set S of keys from a totally ordered universe under insertions, deletions and predecessor queries. We give two general techniques for simultaneously reducing cache and TLB misses: simulating 3-level hierarchical memory algorithms and cache-oblivious algorithms. We give preliminary experimental results which demonstrate that data structures based on these ideas outperform data structures which are based on minimising cache misses alone, namely B-tree variants.

Policies for Call Processing
Stephan Reiff-Marganiec, University of Stirling

Policies are governing choices in the behaviour of a system. They have been used extensively for system management issues such as access control. We consider policies in the context of call control. They have not been considered much in this context, despite their potential.

The talk will focus on several aspects of our work. We consider the concept of call control and distinguish it from system management. Some example

policies lead to a discussion as to which concerns can be governed by policies in the call control context.

We discuss notations to express policies, which range from special purpose languages to logics, and identify the properties we require from a policy description language.

To conclude, we indicate with the example of SIP (Session Initiation Protocol) how a realistic system can incorporate these concepts.

Fixed-Point Logics with Nondeterministic Choice
David Richerby, Cambridge University.

We consider the extension of first-order logic with an inductive operator **nio** due to Arvind and Biswas. At each stage in forming the fixed point of a formula, a single tuple is nondeterministically chosen and added to the relation which has been constructed so far.

Arvind and Biswas gave only informal semantics for their logic; we provide the first formal semantics. A difficulty that arises is that nondeterministic formulae may denote a set of relations, each one depending on a sequence of choices. Conventionally, satisfaction is defined for formulae denoting a single relation but, given a set of relations, there are many possible definitions of satisfaction. We separate the semantics of a logic into its denotational element, which assigns to each formula a set of relations, and a satisfaction relation, which provides a means of combining the relations in a formula's denotation into a single one.

By using an appropriate satisfaction relation, essentially any computational complexity class defined in terms of nondeterministic Turing machines operating within polynomial time bounds can be expressed in terms of nondeterministic fixed-point formulae.

Robust Spatial Data Processing
Anthony Roy and John Stell, Leeds University

Spatial data is of practical importance in areas such as geographic information systems. Models for representing spatial data have traditionally been based on continuous Euclidean space, but are accompanied by various robustness issues. For example, rounding errors on input data may mean the difference between a point being inside or being outside the convex hull of a set of points. Ideally it makes sense to work with a discrete model of space, thus avoiding such robustness issues (all working being done using integer arithmetic).

We survey the most prominent approaches to a discrete representation of space, comparing the underlying representation of space, and how regions are then defined. We also look at the kinds of operations and relations that can be defined on such regions.

We investigate a geometric theory of discrete space which is both robust, and captures the topology of Euclidean space. The underlying structure of the theory is a cell complex, which can be thought of as a partition of Euclidean space into cells of different dimensions. We show that such a complex (shown by Kovalevsky to be a topological space) has an oriented matroid structure. We also discuss operations such as convex hull and delaunay triangulation in terms of the oriented matroid structure.

Bounded Model Checking using Fixpoints
Daniel Sheridan, York University

Bounded model checking is a technique for encoding LTL model checking problems into Boolean satisfiability, exploiting off-the-shelf SAT solvers. With recent developments in SAT technology, bounded model checking can be significantly faster than conventional model checking techniques. The fixpoint characterisations of temporal logic operators form the basis of other model checking techniques such as symbolic model checking. By converting the LTL specification into the normal form SNF, we are able to exploit the fixpoint characterisations to produce a smaller and more easily solved encoding for bounded model checking. We also show an extension to SNF which can result in further benefits and give a number of examples using the model checker NuSMV.

Automatic and hyperbolic monoids
Rick Thomas(Liecester University),Michael Hoffmann, Dietrich Kuske and Friedrich Otto

There has been much interest over the years in automatic and hyperbolic groups. These share the property that their multiplication can be described in terms of computing devices. The theory of automatic groups has now been extended to automatic monoids. In this talk we will introduce these classes and we will also consider hyperbolic, asynchronously automatic, and rational monoids. We will survey (without any proofs) some of what is known about these classes, such as their closure properties and the complexity of the word problem. We will also describe the relationship between these various classes.

On Reduction Semantics for the Push and Pull Ambient Calculus
Maria Grazia Vigliotti, Imperial College London

Honda and Yoshida showed how to obtain a meaniful equivalence on processes in the asynchronous pi-calculus using equational theories identifying insensitive processes. We apply their approach to a dialect of Cardelli and Gordon's Ambient Calculus. The version we propose here is the Push and Pull Ambient Calculus, where the operational semantics is no longer defined in terms of ambients entering and exiting other ambients but in terms of being pulled and being pushed away by another ambient. Like the standard Ambient Calculus, this dialect has the computational power of the asynchronous pi-calculus.

Integer Factorisation: Current Status and Future Developments
Song Y Yan, Aston University

Integer factorisation is a hard problem in both mathematics and computer science. In fact, the most popular and widely used cryptographic system RSA is based its security on the computational infeasibility of factoring large integers, typically with more than 200 digits. In this talk, I will first give an overview of the most popular classical factoring algorithms in use, such as the continued fraction method (CFRAC), the multiple-polynomial quadratic sieve (MPQS), the elliptic curve method (ECM) and the number field sieve (NFS). Then I will discuss the prospectives and future developments of new factoring algorithms. More specifically, I will present a mathematical analysis of the problems in the quantum factoring algorithm. The implication of the progress in factoring is unfortunate (it is fortunate for cryptographers but unfortunate for mathematicians) that the cryptographic systems based on integer factorisation will be still secure at least at present or in the foreseeable future.

Acknowledgements

BCTCS18 would like to acknowledge the generous support by EPSRC, HP and the LMS. For other details of the meeting see **http://www-uk.hpl.hp.com/BCTCS18/**