BRICS *Newsletter*

Basic Research in Computer Science No 8, February 1998

In this Issue

Welcome

Welcome to the eighth issue of the BRICS newsletter. Its purpose is to inform you of appointments, publications, courses and other activities within BRICS. Further details can be obtained by contacting the addresses on the back page.

We recently received the good news that the BRICS Research Centre, under the direction of *Glynn Winskel*, is to receive funding for a further five year period, taking BRICS forward until at least the year 2003. Meanwhile the International PhD School gathers strength with increasing numbers of students, associated teachers and researchers. The PhD School, under the direction of *Mogens Nielsen*, like the BRICS Research Centre is funded by the Danish National Research Foundation, on a rolling grant, so far till the year 2000.

This year has seen the start of an important venture, the Thomas B. Thrige's Centre for Quantum Informatics, abbreviated to CKI (standing for the Danish "Center for KvanteInformatik"), under the direction of *Ivan B. Damgård*. See the article on page 14.

The key event of last year's theme *Algorithms in Quantum Information Processing* actually took place early this year, in January (see Page 8). The conference on this topic was an enjoyable, stimulating meeting which managed to assemble most of the world's experts in the area. Even to an outsider to the subject, the meeting gave a fascinating insight into how the often paradoxical phenomena predicted by quantum mechanics have the potential to play a key role in the future of computing and cryptology.

This year's theme is in *Proofs and Complexity*. Its major meeting is a workshop taking place early in August '98.

You'll find a description of these and other recent and future BRICS activities in this newsletter.

Coming Events

For details see the BRICS Activities web page:

www.brics.dk / Activities.

2-Categories and Bicategories

March 4, 11 and 18, 1998, Aarhus. *Anthony J. Power*, LFCS (Laboratory for Foundations of Computer Science), University of Edinburgh, Scotland, UK, will give a mini-course on 2-Categories and Bicategories.

We introduce the notion of 2-category and outline the basic theory of 2-categories. The notion of 2-category arises in the study of programming languages as follows. Given an idealised programming language, its types and constructors generate a category with structure. Its models are given by structure preserving functors from that generic structured category to any other category possessing such structure. The collection of all such structured categories and functors between them form a 2-category, and properties of such 2-categories support programming constructs, for instance making precise the idea of the language generated by syntax.

We study adjunctions within a 2-category, pasting composition, adjunctions between 2-categories, and the various notions of limit in a 2-category. We also give coherence results that allow one to make simplifying assumptions about the various structures, which can otherwise be very complicated. This is all illustrated by a selection of examples arising from programming languages.

Expressiveness and Complexity of Program Logics

April 20–24, 1998, Aarhus. *Igor Walukiewicz*, Department of Informatics, Warsaw University, Poland, will give a mini-course on Expressiveness and Complexity of Program Logics.

We will consider second order theories that have found applications in program verification and other areas of computer science. We will consider first and second order logics over words and trees. We will also discuss temporal logics and the mu-calculus over these structures. Finally we will consider all these logics over traces. We will be interested in the expressive power of these logics and the complexity of the satisfiability and the model checking problems.

Although we will approach the subject from the program verification perspective we hope that especially complexity issues may be of broader interest as the theories we will discuss proved to be a convenient tool for establishing the complexity of many problems in computer science.

Normalisation in Lambda-Calculus and Type Theory

April 29–30, 1998, Aarhus. *Morten H. Sørensen*, DIKU, University of Copenhagen, Denmark will give a mini-course on Normalisation in Lambda-Calculus and Type Theory.

This course presents some recent results about normalisation in lambda-calculus and type-theory. We aim to cover the theory of so-called perpetual reduction strategies (ie, reduction strategies that compute infinite reduction paths from lambda-terms) and techniques to infer strong normalisation (all reduction sequences from all terms eventually terminate) from weak normalisation (all terms have a reduction sequence to normal form) with an application to the so-called The Barendregt-Geuvers-Klop conjecture about pure type systems.

APPSEM Workshop on Normalisation by Evaluation

May 8-9, 1998, Aarhus.

The terms “normalisation by evaluation”, “normalisation by intuitionistic model construction”, “reduction-free normalisation”, and “type-directed partial evaluation” all designate a very concise and elegant specification of normalisation in the lambda-calculus where normalisation steps are carried out in the meta-language. The idea originates in the area of logic and proof theory, and recently, it has surfaced in the area of programming languages. The goal of this workshop is to bring together all people who have discovered and/or worked with normalisation by evaluation.

Organisers

Olivier Danvy (danvy@brics.dk) and *Peter Dybjer* (peterd@cs.chalmers.se).

Advanced Data Structures

Late May 1998, Aarhus. *Arne Andersson*, LTH (Lund Institute of Technology), Sweden, will give a mini-course on Advanced Data Structures.

This course will deal with data structures and algorithms for sorting and searching. An important issue to cover (and to discuss through the course) is: what is a reasonable model of computation for designing fast algorithms? During the course it will be shown that, when viewing data as binary strings stored in memory cells, we can derive very efficient algorithms, both in theory and practice.

The course will be five double lectures, and includes some assignments. We will also try to create some lively, inspiring, discussions.

ICALP ’98 and Satellite Events

July 13–17, 1998, BRICS, Aalborg, will host the 25th International Colloquium on Automata, Languages, and Programming, ICALP ’98.

Invited Speakers

Gilles Brassard	— Quantum information processing
Mark Overmars	— Title to be announced
Leslie G. Valiant	— A neuroidal architecture for cognitive computation
Avi Wigderson	— Can probabilistic algorithms significantly outperform deterministic ones?
Martin Abadi	— Protection in programming-language translations
Andrew Pitts	— Existential types: logical relations and operational equivalence
Thomas A. Henzinger	— Title to be announced
Amir Pnueli	— Algorithmic verification of linear temporal logic specifications

Programme Committee

The colloquium is chaired by *Kim G. Larsen* jointly with *Sven Skyum* and *Glynn Winskel.*

Further information including list of accepted papers with abstracts can be found at: www.cs.auc.dk/icalp98/.

Satellite Events in July

12–13 STTT ’98, Software Tools for Technology Transfer

17–18 INFINITY ’98, 3rd International Workshop on Verification of Infinite State Systems

18 SOAP ’98, Semantics of Objects As Processes

18–19 APPROX ’98, 1st International Workshop on Approximation Algorithms for Combinatorial Optimisation Problems

20–24 Summer School in Cryptology and Data Security, see below.

Summer School in Cryptology and Data Security

July 20–24, 1998, there will in Aarhus be a Summer School in Cryptology and Data Security. The event is organised jointly with TUCS (Finland) and IPA (Holland) as a part of the EEF series of summer schools, supported by the European Union.

A number of leading experts in the field, from academia as well as industry, have been invited to give introductory and advanced lectures on all aspects of modern cryptology including:

- Design and analysis of Classical Crypto Systems, Public key and Signature Systems and Zero-Knowledge Protocols
- Cryptographic Hash Functions
- Computational Number Theory and Cryptology
- Multiparty Computations
- Secret Sharing
- Quantum Cryptography
- Quantum Computing and Cryptology
- Unconditionally secure cryptographic schemes
- Electronic Commerce and Electronic Payment Systems
- Standards in Data Security
- Industrial Applications

Theme on Proofs and Complexity

During the last years the connections between proof theory and theoretical computer science have become more and more intensive in both directions: proof theoretic techniques are central tools in e.g. logic programming, verification of programs, automated theorem proving, studies of resource sensitive reasoning etc. In the other direction questions in complexity theory have stimulated new developments in the study of proofs and proof systems. The theme Proofs and Complexity intends to disseminate technical tools and results of this complexity-oriented approach to proof transformations and proof systems at BRICS. One of the major aims is to create joint research activities between visitors and researchers at BRICS.

A main activity will be the workshop *Proof Theory and Complexity* held August 3–7, 1998, in Aarhus.

Topics of this workshop are:

- Strength (proof-theoretic and mathematical) of subsystems of second-order arithmetic and type theories.
- Type-free applicative systems (explicit mathematics).
- Complexity of Proof Transformations (cut-elimination, normalisation, epsilon-substitution etc.).
- Proofs as Programs.
- Proof Interpretations and their complexity: Realisability and functional interpretations, game theoretic and categorical interpretations.
- Bounded arithmetic and connections to complexity theory (including feasible arithmetic and analysis).

- Proof Complexity of propositional proof systems: resolution, Frege systems, Nullstellensatz proofs etc.

- Interactive and probabilistic proofs.

Program Committee

Carsten Butz	— BRICS
Ulrich Kohlenbach	— BRICS
Jan Krajícek	— Prague, Czech Rep. & Oxford, UK
Grigori Mints	— Stanford, USA
Søren M. Riis	— BRICS
Helmut Schwichtenberg	— Munich, Germany
Anne Troelstra	— Amsterdam, Holland

Organising Committee

Carsten Butz, *Ulrich Kohlenbach* and *Søren M. Riis* all BRICS.

We are in an early stage of inviting speakers.

Solomon Feferman (Stanford) has already accepted. Also *Grigori Mints* and *Helmut Schwichtenberg* have agreed to give talks.

Regularly updated information will be available from a web-page linked to the BRICS Activities web-page.

Besides the workshop there will be several other activities that are related to this year's theme including mini-courses by guests throughout the year.

Reports on Events

Concentration of Measure and Applications to Analysis of Algorithms

5–19 September, 1997, *Devdatt Dubhashi*, SPIC Mathematical Institute, Madras, India, and *Alessandro Panconesi*, BRICS, gave a single introductory lecture followed up by six advanced double lectures on concentration of measure and applications to analysis of algorithms.

The State-Explosion Problem

6–10 October, 1997, *Antti Valmari*, Software Systems Laboratory, Department of Information Technology, Tampere University of Technology, Finland, gave three double lectures on the state-explosion problem.

Systems Programming in Scheme

13–16 October, 1997, *Olin Shivers*, Artificial Intelligence Laboratory, MIT (Massachusetts Institute of Technology), USA, gave three double lectures on systems programming in Scheme.

BRICS PhD Workshop

On October 20–21, 1998, BRICS had a retreat on the theme of "meta-issues" of research and PhD studies in computer science. The agenda included sessions on issues like:

- Research Skills

- Writing Skills (papers and theses)

- Publishing (how to get your paper rejected / accepted)

- Speaking (how to present a paper)

- Responsible Conduct in Research

- Refereeing papers for Journals and Conferences

The retreat was primarily aimed at PhD students, but also the more senior participants found the talks and discussions very valuable. Figure 1 shows the participants in the BRICS PhD workshop.

Figure 1: Participants in the BRICS PhD workshop.

Functional Programming with Effect

24–27 October, 1997, *Andrzej Filinski*, LFCS (Laboratory for Foundations of Computer Science), University of Edinburgh, Scotland, UK, gave two double lectures on functional programming with effects.

65th PSSL

The *65th Peripatetic Seminar on Sheaves and Logic* (PSSL) organised and sponsored by BRICS, was held over the weekend of 1–2 November 1997.

The PSSL is *the* regular seminar in Europe on category theory and related topics. The topics covered by the seminar include applications of category theory in *mathematical logic* (in particular intuitionistic logic), but also on *categorical algebra* and *topology*. One of the major topics is always *topos theory*, a general framework for both logic and topology. Currently, *logic* and *category theory*, in particular applications thereof in mathematics and computer science cover a large part of the intersection of the interests of the participants.

As the name suggests the seminar is organised at various places in Europe, the seminars before took place in Utrecht (The Netherlands) and in Braunschweig (Germany). The next meetings will be in

Birmingham, March 28-29, 1998 (contact: Neil Ghani, Neil.Ghani@cs.bham.ac.uk),

Utrecht, May 30-31, 1998 (contact: Jaap van Oosten, jvoosten@math.ruu.nl),

and in Brno, August 29-30, 1998 (contact: Jiri Rosicky, rosicky@math.muni.cz).

One of the highlights of this PSSL was the talk by *Dimitri Pataraia* (Tbilisi), who presented his recent constructive proof of the fixed-point theorem for DCPO's. Besides this, the meeting was very successful, as all talks very of high quality.

Besides the 7 local participants (which have 4 different nationalities) we had participants coming from England (3), Georgia (2), Germany (2), Holland (1), Scotland (2), and Sweden (1).

Local Organisers

Carsten Butz and *Anders Kock*.

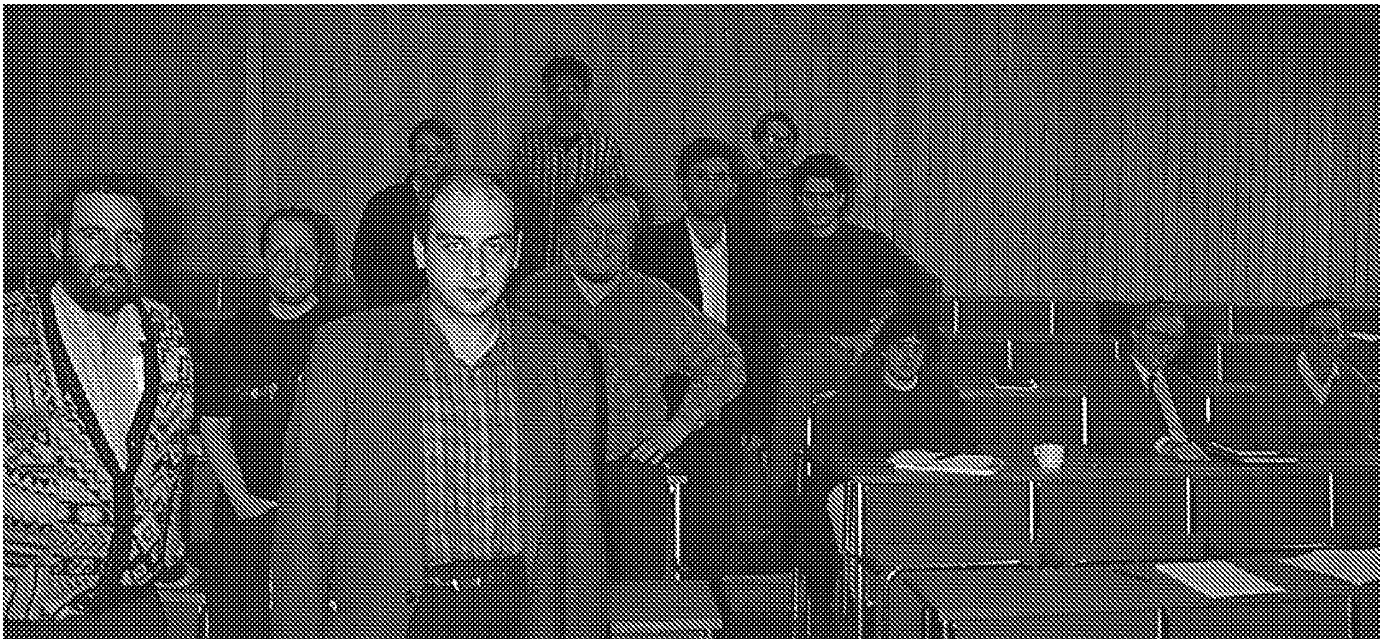

Figure 2: Participants in the 65th PSSL. From the left: *Reinhard Börger*, *Jürgen Koslowski*, *Dimitri Patarai*, *Gian Luca Cattani*, *Jaap van Oosten*, *Sergei Soloviev*, *Mamuka Jibladze*, *Erik Palmgren*, *Marcello Fiore*, *Takis Psarogiannakopoulos*, *Peter T. Johnstone* and *John Power*.

Talks Presented at the Seminar

R. Börger — Tensor products of orthomodular posets and related structures

C. Butz — Remarks on the Structure of finitely presented Heyting algebras

M. Fiore — Towards a categorical theory of binding

M. Jibladze — Cosheaves, coframes, cotoposes - some new facts, some old questions

A. Kock — Extension theory for local groupoids

J. Koslowski — A double category of strategies

E. Palmgren — Constructive nonstandard analysis

D. Pataraia — A constructive proof of the fixed-point theorem for DCPO's

J. Power — Weak higher-dimensional categories

S. Soloviev — Finite completeness theorem for multiplicative intuitionistic linear logic

Pure Type Systems and Applications

7–8 November, 1997, *Gilles Barthe*, Department of Computing Science, Chalmers University of Technology, Gothenburg, Sweden, gave three double lectures and a one hour lecture on pure type systems and applications.

Temporal Data Bases

21–24 November, 1997, *David Toman*, BRICS, gave two double lectures on temporal data bases. Please see also the accompanying lecture notes, LS-97-1, below.

Quantum Computing and Quantum Cryptology

15–17 December, 1997, *Peter Høyer*, Department of Computer Science, University of Odense, Denmark and *Louis Salvail*, BRICS, gave 3 double lectures on quantum computing and quantum

Figure 3: Stairway to Quantum Information Processing. Who is who of the 64 AQIP '98 participants on the picture can be seen under "picure" at the workshop URL below.

cryptology. The min-course was intended for computer scientists with little or no prior knowledge of quantum information processing and served as a warm up for the following AQIP '98 workshop.

Algorithms in Quantum Information Processing, AQIP '98

January 12-16, 1998

Here we bring a report written by one of the participants *André Berthiaume*, CTI (School of Computer Science, Telecommunications & Informations Systems), DePaul University, USA.

AQIP '98, the first workshop on quantum information processing entirely devoted to the computer science and algorithmic aspects of the field, was a resounding success. Organised by BRICS and held in Aarhus the workshop attracted over 60 participants from both Europe and North America. Through 26 scheduled talks, the workshop provided a comprehensive review of the state of the art in quantum information processing from a computer science perspective.

The talks were divided in four categories:

Quantum Algorithms and Complexity: Many talks in this category revolved around the properties of the quantum Fourier transform and its group theoretical implications in quantum algorithmics. Also presented were new fast algorithms for quantum database searching and quantum counting. New complexity results were explored, such as the complexity of counting classes and some limitations on quantum computations, including relations between quantum and classical space-bounded complexity classes.

Quantum Cryptology: An interesting trend in this area is results that involve both classical and quantum aspects of cryptographic protocols. Some examples include: mounting quantum attacks on classical bit commitment schemes, creating a secure quantum bit commitment using physical assumptions and a protocol for oblivious transfer based on the difference of classical information between parties. Other results of a more quantum nature were also presented such as proofs of the security of key distribution and bounds on the capacity of quantum channels.

Quantum Information Theory: Here, the most popular area of research was quantum communication complexity in multiparty function evaluation. Other results in entanglement purification were also presented.

Quantum Error Correction and other issues: Very interesting new results on computing polynomial invariants for quantum codes were presented as well as computation in a noisy environment. These were followed by presentation on reductions between the various types of classical and quantum information.

Figure 4: There were lively discussions on the excursion to the Museum of Prehistory at Moesgård and here Skovmøllen.

The talks generated much discussion that occupied most of the free time between talks. The organising committee planned two outings: an excursion to the Moesgård Museum and a guided tour of the Steno Museum, both fascinating and very appreciated by the participants. A dinner and drinks at the cafeteria of the mathematics department closed the workshop. Incidentally, Danish colleagues have assured the author that it is customary during these dinners to cultivate the creative talents of the participants. Particularly appreciated is singing, especially in foreign tongues and preferably standing on tables.

Figure 5: High spirits at the AQIP '98 workshop dinner. In the foreground from the left: *Louis Salvail* and *Christian Cachin*

Indubitably, AQIP '98 was a success and the participants were unanimous in their appreciation of the strictly computer science formula. Although AQIP '98 was meant as a one time only affair, one can only hope the enthusiasm generated this year will be enough to spark the organisation of future AQIPs.

—— ——

More information on the workshop including abstracts of talks can be found at www.brics.dk/Activities/98/aqip/. Subsequent extended abstract and full version papers will be available.

Visit from Kiel

January 22–23, 1998, Wolfgang Thomas and his group from University of Kiel, Germany paid BRICS a one and a half day visit in return to our visit in Kiel in December 1996 (see newsletter no. 6). They arrived Thursday after lunch, and left again the following day in the afternoon. As in Kiel, there was a dense scientific programme for the visit consisting mainly of a series of informal talks:

Kim G. Larsen — Recent Developments in Automatic Verification of Large Systems

Oliver Matz, Kiel — One Quantifier Will Do in Existential Monadic Second-Order Logic over Pictures

Julian Bradfield, LFCS — The Modal Mu-Calculus Alternation Hierarchy Made Really Easy

Michael I. Schwartzbach — Status of MONA / FIDO, Implementation and Applications

Thomas Wilke, Kiel — Linear Tense Logic and Two-Variable First-Order Logic

Marcin Jurdzinski — Parity Games Are in UP

More than fifteen local participants and guests followed the talks with great interest.

Newly Appointed Researchers, Guests and PhD’s

Andrzej O. Filinski
Andrzej Filinski received his PhD from Carnegie Mellon University in 1996, supervised by John Reynolds and Robert Harper. His thesis, *Controlling Effects*, explored specification and implementation of programmer-definable computational effects in functional languages. Since then, he has been a research fellow at the University of Edinburgh, working on logical frameworks as a tool for formalising and reasoning about programming language semantics. He will be joining BRICS in May 1998.

Julian Bradfield
Julian Bradfield obtained his PhD from Edinburgh in 1991, on the topic of ‘Verifying temporal properties of systems’. Since 1992, he has been a Lecturer in the Department of Computer Science at Edinburgh; from 1997 to 2002 he is also an EPSRC Advanced Research Fellow. His research interests centre around the modal mu-calculus, and include causality and true concurrency, and interactive verification. He will visit BRICS for a year starting from August 1998.

Kevin Compton
University of Michigan, Ann Arbor, Michigan, USA, will start in September 1998 and visit BRICS for one year. Kevin got his PhD in 1980 under the direction of H. J. Keisler at the University of Wisconsin. His research areas deal with applications of logic and combinatorics to computer science, particularly in finite model theory, complexity theory, analysis of algorithms, and database theory. His current research interests include proofs of cryptographic protocols, optimisation and counting complexity, and zero-one laws.

Peter Høyer
Peter is a PhD student at IMADA, Odense University. The topic for his thesis is quantum computation, and his supervisors are Joan Boyar and Gilles Brassard. His other research interests are algorithmics, data structures and complexity theory. He has made regular visits to BRICS where he has collaborated mainly with Ivan B. Damgård and Louis Salvai. He spent the academic year 1996–1997 at Université de Montréal. Currently, he is visiting the group of Richard Hughes at Los Alamos National Laboratory, New Mexico, where he also hopes to get in excellent condition from biking up and down the mountains.

Rasmus Pagh
Rasmus Pagh has just started as a PhD student at the BRICS PhD School under supervision of Peter Bro Miltersen. He has studied for three and a half years at Department of Computer Science, University of Aarhus, before this. His interests are within theoretical computer science in general, and algorithms and complexity theory in particular.

Dissertation Abstracts

The CLP(OIH) Language

by Ole Ildsgaard Hougaard

Many type inference problems are different instances of the same constraint satisfaction problem. That is, there is a class of constraints so that these type inference problems can be reduced to the problem of finding a solution to a set of constraints. Furthermore, there is an efficient constraint solving algorithm which can find this solution in polynomial time.

We have shown this by defining the appropriate constraint domain, devising an efficient constraint satisfaction algorithm, and designing a constraint logic programming language over the constraint domain. We have implemented an interpreter for the language and have thus produced a tool which is well-suited for type inference problems of different kinds.

Among the problems that can be reduced to our constraint domain are the following:

- The simply typed λ-calculus.
- The λ-calculus with subtyping.
- Arbadi and Cardelli's Object calculus.
- Effect systems for control flow analysis.
- Turbo Pascal.

With the added power of the constraint logic programming language, certain type systems with no known efficient algorithm can also be implemented — e.g. the object calculus with self-type.

The programming language thus provides a very easy way of implementing a vast array of different type inference problems.

New in the BRICS Report Series, 1997 and 1998

ISSN 0909-0878

4 Mogens Nielsen and Thomas S. Hune. *Deciding Timed Bisimulation through Open Maps*. February 1998.

3 Christian N. S. Pedersen, Rune B. Lyngsø, and Jotun Hein. *Comparison of Coding DNA*. January 1998. 20 pp.

2 Olivier Danvy. *An Extensional Characterization of Lambda-Lifting and Lambda-Dropping*. January 1998.

1 Olivier Danvy. *A Simple Solution to Type Specialization (Extended Abstract)*. January 1998. 7 pp.

53 Olivier Danvy. *Online Type-Directed Partial Evaluation*. December 1997. 31 pp. Extended version of an article to appear in *Third Fuji International Symposium on Functional and Logic Programming*, FLOPS '98 Proceedings (Kyoto, Japan, April 2–4, 1998).

52 Paola Quaglia. *On the Finitary Characterization of π-Congruences*. December 1997. 59 pp.

51 James McKinna and Robert Pollack. *Some*

Lambda Calculus and Type Theory Formalized. December 1997. 43 pp.

50 Ivan B. Damgård and Birgit Pfitzmann. *Sequential Iteration of Interactive Arguments and an Efficient Zero-Knowledge Argument for NP*. December 1997. 19 pp.

49 Peter D. Mosses. *CASL for ASF+SDF Users*. December 1997. 22 pp. Appears in *ASF+SDF'97, Proceedings of the 2nd International Workshop on the Theory and Practice of Algebraic Specifications, Electronic Workshops in Computing*, http://www.springer.co.uk/ewic/workshops/ASFSDF97. Springer-Verlag, 1997.

48 Peter D. Mosses. *CoFI: The Common Framework Initiative for Algebraic Specification and Development*. December 1997. 24 pp. Appears in Bidoit and Dauchet, editors, *Theory and Practice of Software Development. 7th International Joint Conference CAAP/FASE*, TAPSOFT '97 Proceedings, LNCS 1214, 1997, pages 115–137.

47 Anders B. Sandholm and Michael I. Schwartzbach. *Distributed Safety Controllers for Web Services*. December 1997. 20 pp. To appear in *European Theory and Practice of Software. 1st Joint Conference FoSSaCS/FASE/ESOP/CC/TACAS*, ETAPS '97 Proceedings, LNCS, 1998.

46 Olivier Danvy and Kristoffer H. Rose. *Higher-Order Rewriting and Partial Evaluation*. December 1997. 20 pp. Extended version of paper to appear in *Rewriting Techniques and Applications: 9th International Conference*, RTA '98 Proceedings, LNCS, 1998.

45 Uwe Nestmann. *What Is a 'Good' Encoding of Guarded Choice?* December 1997. 28 pp. Revised and slightly extended version of a paper published in *5th International Workshop on Expressiveness in Concurrency*, EXPRESS '97 Proceedings, volume 7 of Electronic Notes in Theoretical Computer Science, Elsevier Science Publishers.

44 Gudmund Skovbjerg Frandsen. *On the Density of Normal Bases in Finite Field*. December 1997. 14 pp.

43 Vincent Balat and Olivier Danvy. *Strong Normalization by Run-Time Code Generation*. December 1997.

42 Ulrich Kohlenbach. *On the No-Counterexample Interpretation*. December 1997. 26 pp.

41 Jon G. Riecke and Anders B. Sandholm. *A Relational Account of Call-by-Value Sequentiality*. December 1997. 24 pp. Appears in *Twelfth Annual IEEE Symposium on Logic in Computer Science*, LICS '97 Proceedings, pages 258–267.

40 Harry Buhrman, Richard Cleve, and Wim van Dam. *Quantum Entanglement and Communication Complexity*. December 1997. 14 pp.

39 Ian Stark. *Names, Equations, Relations: Practical Ways to Reason about 'new'*. December 1997. ii+33 pp. This supersedes the earlier BRICS Report RS-96-31. It also expands on the paper presented in Groote and Hindley, editors, *Typed Lambda Calculi and Applications: 3rd International Conference*, TLCA '97 Proceedings, LNCS 1210, 1997, pages 336–353.

38 Michał Hańćkowiak, Michał Karoński, and Alessandro Panconesi. *On the Distributed Complexity of Computing Maximal Matchings*. December 1997. 16 pp. To appear in *The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '98.

37 David A. Grable and Alessandro Panconesi. *Fast Distributed Algorithms for Brooks-Vizing Colourings (Extended Abstract)*. December 1997. 20 pp. To appear in *The Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '98.

36 Thomas Troels Hildebrandt, Prakash Panangaden, and Glynn Winskel. *Relational Semantics of Non-Deterministic Dataflow*. December 1997. 21 pp.

35 Gian Luca Cattani, Marcelo P. Fiore, and Glynn Winskel. *A Theory of Recursive Domains with Applications to Concurrency*. December 1997. ii+23 pp.

34 Gian Luca Cattani, Ian Stark, and Glynn Winskel. *Presheaf Models for the π-Calculus*. December 1997. ii+27 pp. Appears in Moggi and Rosolini, editors, *Category Theory and Computer Science: 7th International Conference*, CTCS '97 Proceedings, LNCS 1290, 1997, pages 106–126.

33 Anders Kock and Gonzalo E. Reyes. *A Note on Frame Distributions*. December 1997. 15 pp.

32 Thore Husfeldt and Theis Rauhe. *Hardness Results for Dynamic Problems by Extensions of Fredman and Saks' Chronogram Method*. November 1997. i+13 pp.

31 Klaus Havelund, Arne Skou, Kim G. Larsen, and Kristian Lund. *Formal Modeling and Analysis of an Audio/Video Protocol: An Industrial Case Study Using* UPPAAL. November 1997. 23 pp. To appear in *The 18th IEEE Real-Time Systems Symposium, RTSS '97 Proceedings*.

30 Ulrich Kohlenbach. *Proof Theory and Computational Analysis*. November 1997. 38 pp.

29 Luca Aceto, Augusto Burgueño, and Kim G. Larsen. *Model Checking via Reachability Testing for Timed Automata*. November 1997. 29 pp.

28 Ronald Cramer, Ivan B. Damgård, and Ueli Maurer. *Span Programs and General Secure Multi-Party Computation*. November 1997. 27 pp.

27 Ronald Cramer and Ivan B. Damgård. *Zero-Knowledge Proofs for Finite Field Arithmetic or: Can Zero-Knowledge be for Free?* November 1997. 33 pp.

26 Luca Aceto and Anna Ingólfsdóttir. *A Characterization of Finitary Bisimulation*. October 1997. 9 pp. To appear in *Information Processing Letters*.

BRICS Lecture Series, 1997

ISSN 1395-2048

1 Jan Chomicki and David Toman. *Temporal Logic in Information Systems*. November 1997. viii+42 pp. Full version to appear in: Logics for Database and Information Systems, Chomicki and Saake (eds.), Kluwer Academic Publishers, 1998.

Abstract

Temporal logic is obtained by adding temporal connectives to a logic language. Explicit references to time are hidden inside the temporal connectives. Different variants of temporal logic use different sets of such connectives. In this chapter, we survey the fundamental varieties of temporal logic and describe their applications in information systems.

Several features of temporal logic make it especially attractive as a query and integrity constraint language for temporal databases. First, because the references to time are hidden, queries and integrity constraints are formulated in an abstract, representation-independent way. Second, temporal logic is amenable to efficient implementation. Temporal logic queries can be translated to an algebraic language. Temporal logic constraints can be efficiently enforced using auxiliary stored information. More general languages, with explicit references to time, do not share these properties.

Recent research has proposed various implementation techniques to make temporal logic practically useful in database applications. Also, the relationships between different varieties of temporal logic and between temporal logic and other temporal languages have been clarified. We report on these developments and outline some of the remaining open

research problems.

Contents

BRICS Dissertations Series, 1997

ISSN 1396-7002

3 Thore Husfeldt. *Dynamic Computation*. December 1997. PhD thesis. 90 pp.

News

New Center for Quantum Informatics

On January 1^{st}, 1998, the Thomas B. Thrige "Centre for Quantum Informatics" was established at University of Aarhus. So far, the centre is to exist for a period of three years and is based on a grant from The Thomas B. Thrige Foundation. The official opening takes place at University of Aarhus on 26 March 1998.

Centre Activities

The activities of the centre include a specific project, more general research and educational activities. The aim of the project is to develop technology for quantum encryption, i.e. a technology which in practice can exploit quantum mechanics to develop a verifiably secure encryption system. The time perspective for an operational lab set-up for a system (or alternatively to demonstrate its impossibility)is two years, and, depending on the results, the centre does not anticipate development of a real prototype until after three years.

Concurrently with the project described above, the centre will contribute to the internationally rapidly growing activity within quantum informatics, the purpose of which is to investigate the practical viability of using quantum mechanics as a basis for a whole new calculation paradigm.

Such activities both influence basic research and technology since the ability to prepare microscopical systems in specific states and to control quantum mechanical processes lead to a number of new and interesting opportunities. Among these, we mention the possibility of making particularly faint light sources, developing new storage media and methods, and constructing ultra-sensitive detectors.

Centre Organisation

The centre receives financial support from the Faculty for Natural Sciences at University of Aarhus and from the two research centres Acap (Aarhus Centre of Atomic Physics) and BRICS (Basic Research In Computer Science), which are two of the centres at University of Aarhus to receive financial support from the Danish National Research Foundation. Furthermore, the Engineering College of Aarhus participates in the centre activities to the extent to which it is relevant for the educational activities of the Engineering College.

The centre's research is primarily based on already existing activities at the Institute of Physics and Astronomy, University of Aarhus (Associate professors *Klaus Mølmer* and *Eugene Polzik*) and at the Department of Computer Science, University of Aarhus (Associate professor *Ivan B. Damgård*). Besides these, other senior researchers, post docs and PhD-students will be employed by the centre - the total number of employees is expected to reach 10. On top of this, students will also participate with their exam projects, master theses etc.

In order to promote the application-oriented dimension of the activities, a "club from industry", the CKI-club, will be involved in the centre activities as well. Members of the club are to be companies having (potential) commercial interests in the centre's activities. All company members pay a club fee and are expected to follow up on the centre activities closely and to assist the projects in cases in which they are considered especially qualified. In return, a membership buys a "First Right of Refusal" as regards possible patentable inventions emerging from the centre.

MONA released

We have released MONA, a programming language and tool based on monadic second-order logics WS1S and WS2S. The logic WS1S (Weak Second-order theory of One Successor) expresses limited properties of arithmetic (where "+" is restricted to "+ constant"), and WS2S (Weak Second-order theory of Two Successors) expresses properties about finite, labelled subsets of the infinite, binary tree. MONA is also the name of our tool, which efficiently translates programs to finite-state automata. Mona is being used for applications in hardware verification, temporal logics, program verification, software engineering, and linguistics.

URL

www.brics.dk/˜mona

Contact

Anders Møller, BRICS, amoeller@brics.dk or
Nils Klarlund, AT&T Labs, NJ, USA,
klarlund@research.att.com

Calendar of Events

Date	Event
4–18 Mar ’98	Mini-course on 2-Categories and Bicategories
20–24 Apr ’98	Mini-course on Expressiveness and Complexity of Program Logics
29–30 Apr ’98	Mini-course on Normalization in Lambda-Calculus and Type Theory
8–9 May ’98	APPSEM Workshop on Normalization by Evaluation
Late May ’97	Mini-course on Advanced Data Structures
13–17 Jul ’98	ICALP, 25th International Colloquium on Automata, Languages, and Programming
20–24 Jul ’98	Summer School in Cryptology and Data Security
3–7 Aug ’98	Main event of BRICS theme on Proofs and Complexity.

BRICS Address and World Wide Web

For further information, hard copies of information material and reports of the BRICS Series as well as enrolment into the BRICS newsgroup, please contact **BRICS** at

Telephone:	+45 8942 3360
Telefax:	+45 8942 3255
Internet:	`<BRICS@brics.dk>`

or, in writing, to

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark.

You can get access to information from BRICS through World Wide Web (WWW) and anonymous FTP. To connect to the BRICS WWW entry, open the URL:

```
http://www.brics.dk/
```

The BRICS WWW entry contains updated information about most of the topics covered in the newsletter as well as access to electronic copies of information material and reports of the BRICS Series (look under Publications).

To access the information material and reports of the BRICS Series via anonymous FTP do the following:

```
ftp ftp.brics.dk
get README.
```

BRICS *Newsletter*

ISSN 0909-6043

Editors: Glynn Winskel & Uffe H. Engberg
Lay-out: Uffe H. Engberg
Publisher: BRICS

Print: Departments of Mathematical Sciences
University of Aarhus

© BRICS 1998