BRICS Newsletter

Basic Research in Computer Science — No 7, September 1997

In this Issue

Welcome

Welcome to the seventh 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.

This year has seen the start of an important venture, the BRICS International PhD School, under the direction of *Mogens Nielsen*. The school, like the BRICS Research Centre funded by the Danish National Research Foundation, is an experiment in Danish postgraduate education, aiming at establishing an international graduate school in computer science around BRICS and its activities. One of the more concrete aims is to supplement the twenty or so Danish PhD students of BRICS with a corresponding number from abroad. As a result of the first (electronic) call for applications from foreign students for admission and grants starting August 1997, 5 new students were selected from a total of 62 applications.

Due to a combination of circumstances this year's theme, *Algorithms in Quantum Information Processing*, will take place early in the new year, concentrated in January 1998! We have been very fortunate in that several internationally known experts in the field have been kind enough to join the program committee to help in planning the scientific content of the event.

In the following you will find a brief description of some recent and future BRICS activities. Please pay attention to the call for applications for a number of BRICS research positions starting in 1998!

Coming Events

For details see the BRICS Activities web page:

www.brics.dk / Activities.

The State-Explosion Problem

October 6, 8 and 10, 1997, *Antti Valmari*, Software Systems Laboratory, Department of Information Technology, Tampere University of Technology, Finland, will give a mini-course on the state-explosion problem.

State space methods are one of the most important approaches to computer-aided analysis and verification of the behaviour of concurrent systems. In their basic form, they consist of enumerating and analysing the set of the states the system can ever reach. Unfortunately, the number of states of even a relatively small system is often far greater than can be handled in a realistic computer. The goal of this mini-course is to analyse this "state explosion problem" from several directions. Many advanced state space methods alleviate the problem by using a subset or an abstraction of the set of states. Unfortunately, their use tends to restrict the set of analysis or verification questions that can be answered, making it impossible to discuss the methods without some taxonomy of the questions. Therefore, the course contains a lengthy discussion on alternative ways of stating analysis and verification questions, and algorithms for answering them. After that, many advanced state space methods are briefly described. The state explosion problem is also investigated from the computational complexity point of view.

Systems Programming in Scheme

October 13–17, 1997, *Olin Shivers*, Artificial Intelligence Laboratory, MIT (Massachusetts Institute of Technology), USA, will give a mini-course on systems programming in Scheme.

Functional programming languages are not only useful for teaching and theorem proving—they have many benefits for programming systems applications and scripting. Over the last five years, Olin Shivers has tried to support this thesis by designing and implementing `scsh`, a Scheme programming environment that is designed for Unix systems programming.

The mini-course will cover topics drawn from experience using `scsh` as a systems-programming tool: 1) Embedding domain-specific "little languages" within Scheme; 2) Automatic management of OS resources in a functional language; 3) Using Scheme as a high-level scripting tool; 4) Writing systems-level code in Scheme, such as extensible Web servers.

Functional Programming with Effects

October 24–27, 1997, *Andrzej Filinski*, LFCS (Laboratory for Foundations of Computer Science), University of Edinburgh, Scotland, UK, will give a mini-course on functional programming with effects.

Over the last few years, the theory and practice of functional programming have been significantly influenced by the concept of computational monads. Perhaps most importantly, monads provide a uniform mathematical framework for defining the semantics of "computational effects" such as mutable state or exceptions in ML-like languages. Equally notable, monads can be used as a convenient structuring technique for expressing imperative concepts in purely functional languages such as Haskell. So far, however, these two application areas have seen little overlap; the main goal of this mini-course is therefore to explore some consequences of a cross-fertilisation.

The course will start with a general introduction to monads, their use in denotational semantics, and techniques for reasoning about languages defined in terms of monads. Most of these con-

cepts and techniques generalise naturally to a more syntactic setting, allowing us to specify declaratively a wide range of new computational effects, such as nondeterministic choice, within a functional language itself. In particular, we will consider "monadic reflection", a generalisation of Wadler's monad comprehensions, which will allow us to write programs using the newly-defined effects, with the same conciseness and convenience as we expect from "built-in" effects in ML-like languages.

We will then see how a surprising semantic result—the existence of a "universal" monadic effect—allows us to uniformly implement monadic reflection in terms of two primitive effects: mutable state and first-class continuations, as found in Scheme or SML/NJ. This technique gives us the best of both worlds: uniform, declarative specifications of new computational effects, combined with the full programming environment and efficiency of an existing production-quality language implementation.

The course will be largely self-contained, requiring only familiarity with basic concepts of denotational semantics and a working knowledge of ML or Scheme.

PSSL, the 56th Peripatetic Seminar on Sheaves and Logic

The 65th Peripatetic Seminar on Sheaves and Logic will take place in Aarhus over the weekend 1–2 November 1997. The seminar invites contributions related to category theory, mathematical logic (in particular, intuitionistic logic), categorical algebra, topology and, for example, topos theory. Of interest as well are applications of the above subjects, for example in computer science.

As the title of the seminar suggests, the seminar (founded by Dana Scott in the seventies) is held two or three times a year at different places in Europe. It is *the* European seminar on category theory and applications thereof.

The local organisers of the 65th seminar are *Carsten Butz* (BRICS) and *Anders Kock* (Department of Mathematics, Aarhus). The Seminar is partly sponsored by BRICS and the Department of Mathematics, Aarhus. For more information contact Carsten Butz (butz@brics.dk), or visit the WWW-page of the seminar at www.brics.dk/Activities/97/PSSL65/.

Pure Type Systems and Applications

November 13–18, 1997, *Gilles Barthe*, Department of Computing Science, Chalmers University of Technology, Gothenburg, Sweden, will give a mini-course on pure type systems and applications.

Pure type systems (PTSs) were introduced in the late 80's by Barendregt, Berardi and Terlouw as a framework to define and study typed lambda calculi. The framework motivates its uses and applications (e.g. in theorem proving and programming languages), and reflections upon its shortcomings will be presented. Finally, it is the hope to conclude with some recent developments in the field.

Temporal Data Bases

In November, *David Toman*, BRICS, will give a mini-course of 3 to 6 lectures on temporal data bases.

Time is ubiquitous in information systems. Almost every enterprise faces the problem of its data becoming out of date. However, such data is often valuable, so it should be archived and some means to access it should be provided. Also, some data may be inherently historical, e.g., medical, cadastral, or judicial records. Temporal databases provide a uniform and systematic way of dealing with historical data.

In our presentation we concentrate on possible ways of extending the standard relational model with new a-priori interpreted data types in a

clean and natural way. In the context of *temporal databases* we are mostly interested in the type of linearly ordered set of *time instants* that represents the flow of time. We discuss the necessary extensions to the original model needed to accommodate the new functionality. While we mainly concentrate on single data type—linear order for representing time—the general techniques can be extended to other interpreted domains of data.

We also give an overview of the developments in the area of temporal databases with an emphasis on relating the various proposed models to our precise abstract model based on logic. ▤

BRICS Theme on Algorithms in Quantum Information Processing

There have long been plans to have a BRICS 1997 theme in some form of algorithmics. The plans for this are now being finalised. Due to a combination of circumstances the theme will take place early in the new year, concentrated in January 1998!

We have been very fortunate in that several internationally known experts in the field have been kind enough to join the program committee to help in planning the scientific content of the event.

The Background

The last few years, we have seen a rapidly growing interest in quantum computing, quantum cryptography and quantum information theory. A large number of conferences and workshops are devoted to these subjects. Typically, these events are somewhat specialised and include to a significant extent quantum physics and contributions from quantum physicists.

While such events are clearly important, e.g. in order to disseminate the necessary physics background in the computer science community, we feel that there is also a need for an event that is devoted entirely to the computer science and

Figure 1: The ICALP '98 Poster.

algorithmic side of the field. We also feel that it is natural to cover the entire field of quantum information processing, that is, to include quantum computing, quantum cryptography and quantum information theory.

One specific reason for organising such an event at the BRICS research centre is that BRICS has recently started research activities in the area in cooperation with the Physics Institute at the University of Aarhus, covering both the theoretical and experimental side.

Format of the Event

A number of researchers in the area will be invited to visit BRICS for as much of January 98 as they wish. Week 3, i.e. January 12–16, will be the focal point of the event. During that week, a program with various talks will be scheduled and announced publically. We expect that the opportunity to interact informally and do joint work is

one important reason for participating, and we will leave ample time in the program for this.

Organising Committee

Joan Boyar (Odense University, Denmark) and from BRICS: *Ivan Damgård*, *Gudmund S. Frandsen* and *Erik M. Schmidt*.

Program Committee

Charles Bennett — T. J. Watson Res. Cent., USA
André Berthiaume — DePaul University, USA
Richard E. Cleve — Univ. of Calgary, Canada
Ivan Damgård (chair) — BRICS
Lov Grover — Lucent Technologies, USA
Peter Høyer — Odense University, Denmark
Louis Salvail — BRICS
Umesh Vazirani — Univ. of Calif., Berkeley, USA

Contents

We will attempt to cover the entire field of quantum information processing, including quantum computing, quantum cryptography, quantum information theory, and related subjects from computer science. The fact that we will try to take a computer science point of view does (of course) not exclude subjects that relate to physics, but it does exclude subjects such as specific physical realizations of quantum cryptography and quantum computers.

ICALP '98, 25th International Colloquium on Automata, Languages, and Programming

July 13–17, 1998, BRICS, Aalborg, will host the 25th International Colloquium on Automata, Languages, and Programming, ICALP '98. Chaired by *Kim G. Larsen* jointly with *Sven Skyum* and *Glynn Winskel*. Further information can be found at: www.cs.auc.dk/icalp98/.

Reports on Events

Algebraic Theory of Automata, Temporal Logic and Expressiveness

April 29 and 30, 1997, *Denis Thérien*, School of Computer Science, McGill University, Canada, gave two double lectures covering the following topics: algebraic theory of automata, decomposition of finite semigroups, logical description of $*$-free languages and regular languages and boolean circuits.

Information Theoretic Security in Cryptography

May 1–2, 1997, *Ueli Maurer*, Department of Computer Science, ETH (The Swiss Federal Institute of Technology), Zürich, Switzerland, gave 3 lectures on Information Theoretic Security in Cryptography.

Combinatorial Optimisation Meeting

The first BRICS Combinatorial Optimisation Meeting was held in Aarhus on May 5–6, 1997. The meeting was a clear success with almost 40 participants and 10 excellent talks that generated interesting discussions.

The meeting started with five talks devoted to some standard combinatorial optimisation topics. The speakers were Jens Clausen (now at DTU, the Technical Univ. of Denmark), Tibor Jordán (Odense Univ., Denmark), David Pisinger (Univ. of Copenhagen, Denmark), Michael M. Sørensen (The Aarhus School of Business, Denmark) and the featured speaker of the meeting, *Martin Grötschel* from Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB), Germany. The day ended with a dinner for participants followed by beers downtown (for those who were ready for the Monday night action).

The talks on the second day of the meeting were mostly geared towards combinatorial optimisation problems arising in (more or less) related areas such as graph theory, computational biology, probabilistic logic and cryptography. The speakers were Jørgen Bang-Jensen (Odense University), Rune B. Lyngsø and Christian N. S. Pedersen (both BRICS), Erling D. Andersen (Dept. of Management, Odense University), Kim A. Andersen (Theoretical Statistics and Operations Research, University of Aarhus), and Michael Fellows (University of Victoria, Canada). The titles and the abstracts of all the talks are available via www.brics.dk/Activities/97/CombOpt/.

Aleksandar (Sasa) Pekec organised the meeting.

See you next year at the second annual BRICS Combinatorial Optimisation Meeting.

xBIFF Soccer-team

Figure 2: The xBiff Soccer-team. In the background from the left: *Christian N. S. Pedersen*, *Aleksandar (Sasa) Pekec*, *Jesper G. Henriksen*, *Peter Ørbæk*, *Thomas S. Hune*; middle: *Mads Kyed*, *Jakob Pagter*, *Gian Luca Cattani*, *Jakob Fredslund*; foreground *Rune B. Lyngsø* (Goalkeeper).

In the spring this year BRICS PhD students and associated took the initiative to form a football team (*the Great xBIFF Soccer-team*) and signed up for a season in the J league (a Jutland tournament for companies).

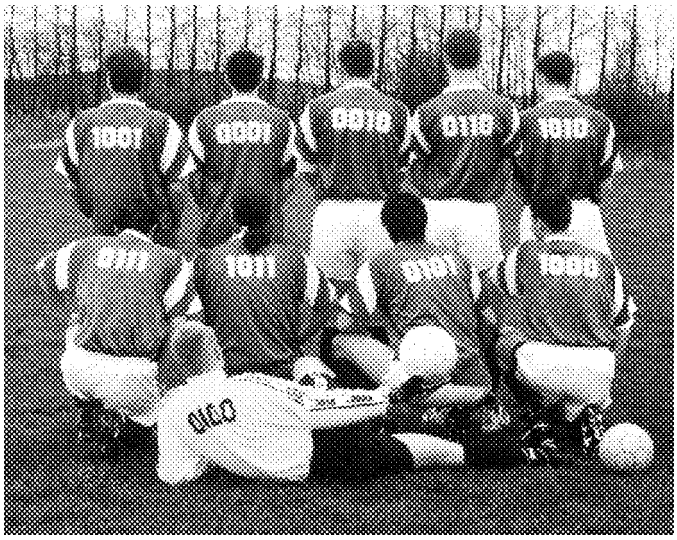

Figure 3: The players' numbers reveal the origins of the players.

Despite extensive training and excellent play unfortunate circumstances prevented the team from obtaining more than 15 points in their 14 matches. The team management is thus constantly on the look-out for new talents among the newly admitted PhD students to ensure an even better outcome next year.

First Order Logic with Dependent Sorts, Simulation, and Higher Dimensional Categories

May 20 and 22, *Michael Makkai*, McGill University, Canada, gave two double lectures on first order logic with dependent sorts, simulation, and higher dimensional categories.

Inductive Logic Programming

May 20–23, 1997, *Nada Lavrac*, Department of Intelligent Systems, Jozef Stefan Institute, Ljubljana, Slovenija, and *Peter Flach*, Infolab, Department of Management Information Science, Tilburg University, Holland, gave three double lectures on inductive logic programming.

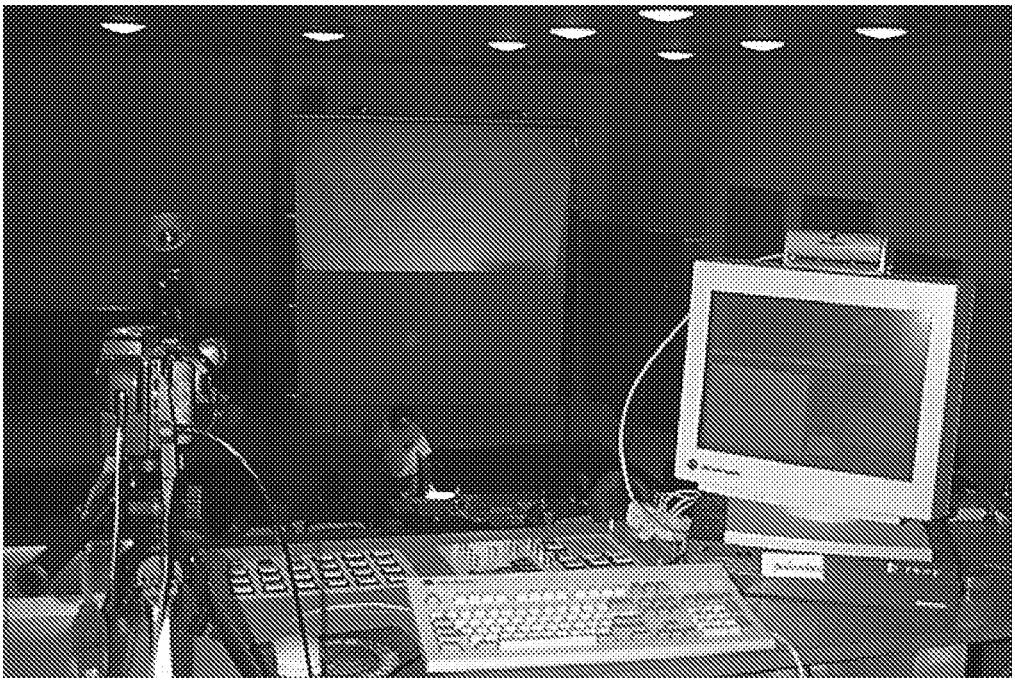

Figure 4: The CPM '97 Symposium was transmitted via M-bone.

Reduction-Free Normalisation

On June 3 and 4, 1997, *Philip Scott*, Department of Mathematics, University of Ottawa, Canada, gave two double lectures on reduction-free normalisation.

8th Annual Symposium on Combinatorial Pattern Matching, CPM '97

June 30 – July 2, 1997

We bring a report here written by one of the participants Professor *Amihood Amir*, Department of Mathematics and Computer Science, Bar-Ilan University, Israel.

CPM is one of my favorite conferences. It is a symposium where I know practically all the attendees and understand all the talks (a rarer and rarer trait in today's conferences scene). In addition to the usual pleasurable anticipation, I was particularly looking forward to visiting Denmark for the first time.

My first meeting with Denmark was Copenhagen airport. Walking from the international airport to the domestic side, I was struck with the special lanes for bicycles and with the bicycles everywhere. I was utterly amazed at the fact that people can leave bicycles outside, guarded solely by a flimsy lock, and find them intact upon their return. I was sure that here I see the achievement of the acme of human moral evolution. I was ready to sing the praises of the Danish people who scaled such ethical heights!

My poetic mood was somewhat dashed when I entered the domestic terminal and saw the mass smoking taking place under the "no smoking" signs. I sighed and concluded that human moral perfection has not been attained yet...

I spent Sunday afternoon (June 29) with a good friend from Georgia Tech, Prof. Leo Mark, who was on Sabbatical at Aalborg. Leo drove all the way to Aarhus airport to pick me up and I spent a wonderful evening with his family. It was very pleasant to experience Danish hospitality and daily living style, something one does not generally get a chance to experience in a professional conference. An added advantage of the trip to Aalborg and back was that I could get a

first hand impression of the towering mountains and deep ravines of Denmark...

Danish hospitality was apparent at the symposium as well. The organisers, and especially Christian Storm Pedersen took great pains to make everyone comfortable. Christian was even in touch with the Chief Rabbi of Denmark, in order to organise kosher food for the participants that required it. Everyone was well fed.

The conference had two social events, the conference dinner and an excursion to the Steno Museum. The dinner was not only an occasion to socialise with old and new friends, but also an opportunity to celebrate Maxime Crochemore's birthday. Max is one of the founding fathers of CPM and a world leader in pattern matching. His many friends and colleagues took the opportunity to congratulate him. The excursion was also quite successful. Scientists are always happy to wander around in a science museum and fondly recall all the science that they had forgotten.

The reader may be wondering at this point if the entire symposium was one great party. Scientifically the conference was challenging and interesting. Twenty submitted papers were presented and two invited lectures. The papers were selected after a thorough, careful, and at some (rare) occasions, heated review process. I believe the results speak for themselves.

Pattern matching is maturing into an interesting and important field. The conference drew 73 registered participants, which is quite a large number for symposiums of this sort. Participants came from Brazil, Canada, Chile, the Czech Republic, Denmark, Finland, France, Germany, Hungary, Israel, Italy, Japan, Korea, New Zealand, Norway, Poland, Sweden, the USA and the United Kingdom.

I was particularly interested with the work on compressed matching, searching for templates in compressed images without decompressing. It is a topic that becomes more important with the explosive growth of multi-media and compressed image data. (Of course the best papers were those that referenced my work...)

The conference ended with lunch on July 2. After tearful goodbyes some of us took advantage of the wonderful sunny afternoon to visit Den Gamle By. We were quite impressed and would recommend future events at Aarhus to make the excursion there. It is a uniquely Danish attraction and we are sure all visitors will enjoy it.

All in all we had a fruitful and enjoyable conference and we thank the organisers and program committee for a successful event. ▩

Annual Conference of the European Association for Computer Science Logic, CSL '97

August 23–29, 1997

Here we bring a report written by one of the participants *Antonín Kučera*, Masaryk University, Brno, Czech Republic.

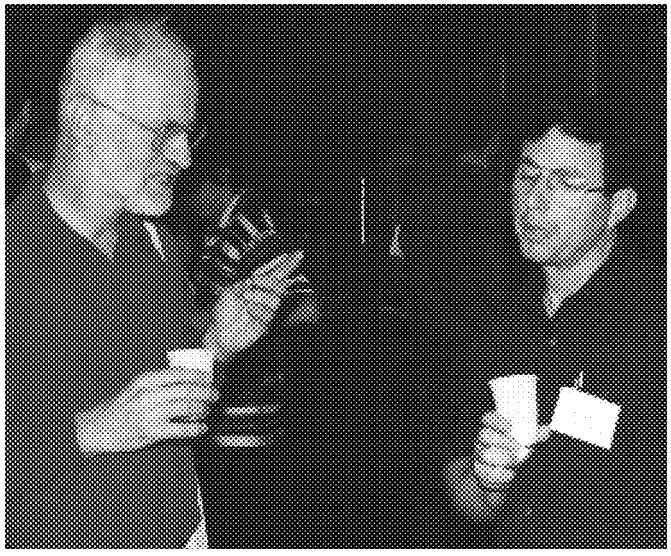

Figure 5: From the left: *Egon Börger* (resigning president of the European Association for Computer Science Logic, EACSL) in discussion with *Neil Immerman* (invited speaker).

This year, the conference was preceded by tutorials on games in computer science logic.

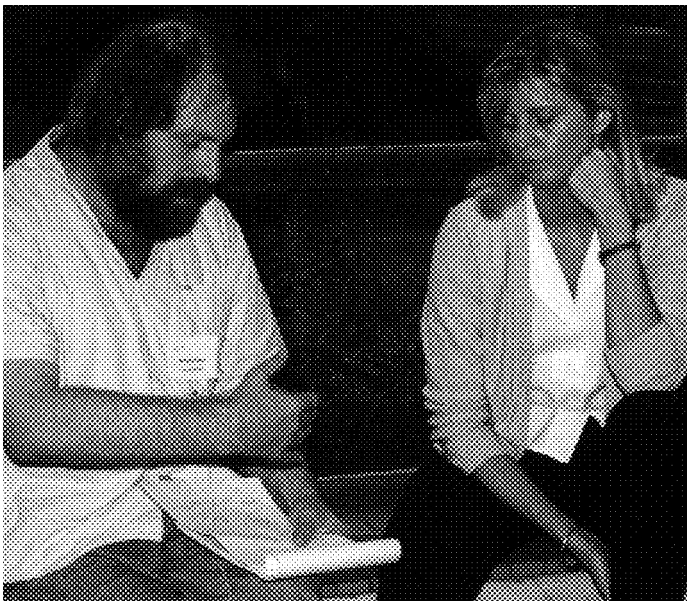

Figure 6: Many used the breaks for scientific discussions, here: *Wolfgang Degen* and *Sabine Broda*.

The lectures were given by Samson Abramsky (Game Semantics), E. Allen Emerson (Games, μ-calculus, and Program Verification), and by Wolfgang Thomas and Igor Walukiewicz (Determinacy, the Rabin Theorem and its Extensions). To give a measure of their success, it suffices to mention that the tutorials were attended by more than 70 participants, who could enjoy the excellent programme.

The CSL conference started on Monday, August 25. The scientific programme consisted of eight invited talks and 31 contributed talks selected out of 92 submitted papers. It was divided into eight sessions with an invited talk at the beginning. The invited speakers were:

Samuel R. Buss — Resolution, The Pigeonhole Principle and Proof Complexity

Hubert Comon — Higher-Order Matching and Tree Automata

Thierry Coquand — Formal Topology and Inductive Definitions

Martin Hyland — Constructing Categories of Abstract Games

Neil Immerman —Descriptive Complexity and Model Checking

Nils Klarlund —Mona & Fido: The Logic / Automaton Connection in Practice

Yiannis N. Moschovakis — Concurrent Recursion

Leszek Pacholski —Complexity of Type Inference

The conference was well-attended—112 registered participants from 17 countries. Preliminary proceedings with pre-reviewed contributed papers were available at the conference. Final proceedings will be published by Springer in the LNCS series.

Figure 7: Entering the Museum of Prehistory at Moesgaard: *Egon Börger*, *Mogens Nielsen*, *Karen K. Møller* and *Yiannis N. Moschovakis* (invited speaker).

In addition to its doubtless scientific value, the conference was particularly pleasant because of its friendly atmosphere and hospitality of hosts. Karen K. Møller and Mogens Nielsen did an excellent job as local guides, and their additional comments during the visit in the Museum of Prehistory at Moesgaard (a culture-historical museum) sometimes attracted more attention than the speech of a professional guide. The excursion also included a visit to The Old Town, an open-air museum with 75 half-timbered houses, rebuilt along cobbled streets and fitted with all the workshops and furnishings of a Danish market town.

Another opportunity to become familiar with some specific Danish habits was offered during

Figure 8: There was also time for conviviality during breaks: *Ina Schiering*, *Igor Walukiewicz* (tutorial speaker), *Anthony J. Power* and wife *Mei Chi Shum*, *Marcin Jurdziński* and *David Janin*.

the Conference Banquet. All participants were provided with a list of songs (to sing!) and this performance was really appreciated by all of them, especially in the moment when everybody stood on the table.

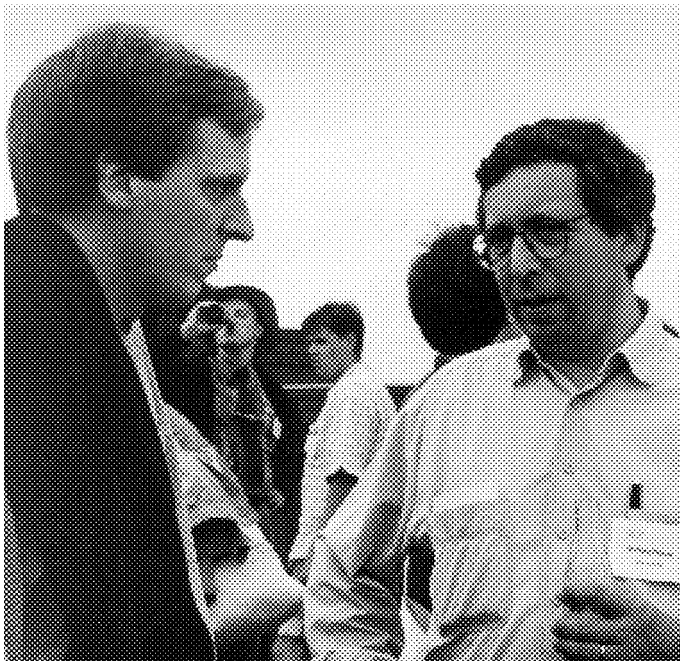

Figure 9: *Ulrich Kohlenbach* in discussion with *Wolfgang Thomas* (chair of the prog. committee) during the excursion.

To sum up, CSL'97 was a very successful meeting. The program committee (chaired by Wolfgang Thomas) did an excellent work—the set of invited talks splendidly demonstrated various ways of applying logic to computer science, and the selected contributed papers were of a high quality as well. The work of the organising committee, composed of Gian Luca Cattani, Uffe H. Engberg, Karen K. Møller, and Mogens Nielsen (chair) substantially contributed to this success—the conference ran smoothly and all 'local' people were willing to help anybody with any problem.

The next CSL conference will be held in Brno, Czech Republic, and it will be federated with MFCS '98 conference.

Concentration of Measure and Applications to Analysis of Algorithms

September 5–19, *Devdatt Dubhashi*, SPIC Mathematical Institute, Madras, India, and *Alessandro Panconesi*, BRICS, gave 6 double lectures on concentration of measure and applications to analysis of algorithms.

Newly Appointed Researchers, Guests and PhD's

Ole Høgh Jensen
Ole H. Jensen joined BRICS in Aalborg in August 1997. He got an MSc from Aalborg in 1993, and has carried out work for a PhD thesis at Edinburgh and Cambridge Universities. His interests are semantics of concurrent and distributed systems, and his thesis work has focused on Milner's action calculi, a unifying framework for various computational calculi, for which he has made advances towards a general theory of operational equivalence.

Søren Møller Riis
Søren M. Riis got his PhD from University of Oxford 1993. His thesis *Independence in Bounded Arithmetic* applied techniques like forcing known from set theory. The field of Bounded Arithmetic provides a natural interface between Fragments of Number Theory, Mathematical Logic and the Theory of the Complexity of Computations. Søren visited BRICS during 1994. In 1995 he visited Jerusalem and spent the remaining time in Leeds . Before joining BRICS in August 1997, Søren has visited Lund, Copenhagen, Dimacs New Jersey (twice) and Kent State University. Current interests include applying techniques from Algebra and Representation theory to solve problems in Complexity Theory. He has recently worked on the decidability and undecidability of Laws in Dynamical Systems.

Louis Salvail
The research interests of Louis Salvail lie within quantum cryptography, classical cryptography, quantum information theory and quantum computation. He obtained his PhD in quantum cryptography in 1997 from the University of Montréal supervised by Claude Crépeau and Gilles Brassard. Current interests include secure and practical implementations of quantum crypto systems.

Peter Selinger
Peter Selinger received his PhD in 1997 from the University of Pennsylvania, and he is now an Assistant Professor of Mathematics at the University of Michigan. His research interests include the semantics of concurrent and distributed computation, and he is currently working on categorical models of asynchronous communication in networks of communicating processes. Peter will visit us at BRICS for six months starting in January, 1998.

Paola Quaglia
Paola Quaglia's research interests are in the area of semantics for concurrency, in particular of semantics for synchronous and asynchronous mobile process calculi, and for probabilistic and stochastic distributed systems. Paola got her PhD in Computer Science from Pisa University in 1996, defending the thesis *The π-calculus with explicit substitutions*, supervised by Ugo Montanari. She was an Associate Researcher at the Computer Laboratory of Cambridge University from October 1996 to May 1997, before joining BRICS in June 1997 as a TMR research fellow.

Carsten Weise
Carsten Weise got his PhD from Aachen University of Technology (RWTH Aachen) in 1996. The thesis was entitled *Decision Algorithms for Equivalences in Real Time Process Algebras with a Dense Time Domain* and was supervised by Bernhard Steffen and Jürgen Merkwitz. Among his current interests are formal methods for hybrid systems and tools aiding in the application of the methods. Carsten visited Aalborg University for six weeks in 1994 and joined BRICS in Aalborg again in a position starting September 1997.

BRICS is also happy to welcome the following newly admitted PhD students.

Mikkel Christiansen
Mikkel Christiansen recently graduated from Aalborg University with an MSc thesis on automated trace analysis of distributed systems. The aim of his PhD study is to extend this work to real-time systems and also to develop a prototype tool for real time trace analysis. Supervisor: Arne Skou

Niels Damgaard
Niels Damgaard is a PhD student at BRICS since August 1997. He studied four years at DAIMI, the Department of Computer Science at the University of Aarhus. Niels hasn't settled on a specific main area of research yet but he is mainly concerned with compilers, data structures, algorithmics and cryptography. Preliminary supervisor: Michael I. Schwartzbach.

Daniel Damian
Daniel Damian graduated in July 1997 from the Faculty of Mathematics and Computer Science at the University of Craiova, Rumania. His previous work focused on implementation of logic programming and algorithms. The main lines of studies followed in Craiova were semantics for logic programming, complexity of algorithms and programming languages. Preliminary supervisor: Peter B. Miltersen.

Stefan Dziembowski
Stefan Dziembowski graduated from Warsaw University, Poland, and worked there for one year as a teaching assistant. His MSc thesis written under the guidance of Damian Niwiński concerned fixpoint database queries. Stefan's fields of interest also include theory of automata on infinite objects, μ-calculus and monadic second-order logic. He already visited BRICS as a summer student in 1996. Preliminary supervisor: Glynn Winskel.

Bernd Grobauer
Bernd Grobauer graduated this summer from the Munich University of Technology, Germany, with an MSc thesis titled *A Verified Unification Algorithm for Higher-Order Patterns*, written under guidance of Tobias Nipkow. During 1996 he was a visiting scholar at the Laboratory of Formal Methods at the catholic university of Rio de Janeiro. His main area of interest is formal methods. Preliminary supervisor: Olivier Danvy.

Mikkel Jensen
Mikkel Jensen is a newly accepted PhD student under the supervision of Jan Depenau and Brian Mayoh. His main research interest lies in the field of AI, particularly neural networks, genetic algorithms and combinations of these. He also has an interest in complexity theory.

Gabriel Juhás
Gabriel Juhás is a PhD student at the Slovak Academy of Sciences. He obtained his MSc (Mgr.) from the Faculty of Mathematics and Physics, Comenius University of Bratislava, Slovakia, in 1993, with a master thesis on structural analysis of Petri Nets. His research interests are within concurrency theory. In particular, he is working on an algebraic generalisation of Petri nets. During his stay he will work on his PhD thesis on these topics. He should finish his PhD study in Spring 1998. Gabriel Juhás is visiting BRICS from August to December 1997 under the supervision of Mogens Nielsen.

Marcin Jurdziński
Marcin Jurdziński recently graduated from Warsaw University, Poland, with an MSc thesis on the complexity of model checking for the μ-calculus under the guidance of Damian Niwiński. His interests include verification of finite state concurrent systems, complexity theory and finite model theory. Marcin visited BRICS for six months last year on a Polish-Danish exchange grant. Preliminary supervisor: Mogens Nielsen.

Dirk Lenzkes
Dirk Lenzkes recently graduated from Aachen University of Technology (RWTH Aachen), Germany with his MSc thesis on verification of real-time systems. This is also the research topic he is working on while visiting BRICS. He has published two papers on timed bisimulation and on modal hybrid systems with his thesis supervisor Carsten Weise. Dirk is visiting BRICS September and October 1997.

Marijana Lomić
Marijana Lomić's main fields of interest are databases, database design and structure. She graduated from the University of Novi Sad, Yugoslavia and since then has taken postgraduate studies there. Preliminary supervisor: Ivan B. Damgård.

Lasse Reichstein Nielsen
Lasse R. Nielsen has just started as a PhD student at the BRICS PhD School. He has studied for five years at DAIMI before this, where he acquired his interest in the theoretical aspects of computer science, in particular formal systems and methods used for modelling programming languages and their semantics. Supervisor: Olivier Danvy.

Flemming Friche Rodler
Flemming F. Rodler has just started his PhD studies at DAIMI under supervision of Brian H. Mayoh. He has been studying for five years including a one year visit at Technical University of Vienna. Flemming is mainly interested in wavelet analysis and how it can be applied in computer science, especially in the analysis and transformation of sound and images.

Dissertation Abstracts

Dynamic Computation

by Thore Husfeldt

Chapter 1 contains a brief introduction and motivation of dynamic computations, and illustrates the main computational models used throughout the thesis, the random access machine and the *cell probe model* introduced by Fredman.

Chapter 2 paves the road to proving lower bounds for several dynamic problems. In particular, the chapter identifies a number of key problems which are hard for dynamic computations, and to which many other dynamic problems can be reduced. The main contribution of this chapter can be summarised in two results. The first shows that the signed prefix sum problem, which has already been heavily exploited for proving lower bounds on dynamic algorithms and data structures, remains hard even when we provide some amount of nondeterminism to the query algorithms. The second result studies the amount of extra information that can be provided to the query algorithm without affecting the lower bound. Some applications of these results are contained in this chapter; in addition, they are heavily developed for the lower bound proofs in the remainder of the thesis.

Chapter 3 investigates the dynamic complexity of the symmetric Boolean functions, and provides upper and lower bounds. These results establish links between parallel complexity (namely, Boolean circuit complexity) and dynamic complexity. In particular, it is shown that the circuit depth of any symmetric function and the dynamic prefix problem for the same function depend on the same combinatorial properties. The connection between these two different modes and models of computation is shown to be very strong in that the trade-off between circuit size and circuit depth is similar to the trade-off between update and query time.

Chapter 4 considers dynamic graph problems. In particular, it presents the fastest known algorithm for dynamic reachability on planar acyclic digraphs with one source and one sink (known as planar *st-graphs*). Previous partial solutions to this problem were known. In the second part of the chapter, the techniques for lower bounds of chapter 2 are further exploited to yield new hardness results for a number of graph problems, including reachability problems in planar graphs and grid graphs, dynamic upward planarity testing and monotone point location.

Chapter 5 turns to strings, and focuses on the problem of maintaining a string of parentheses, known as the dynamic membership problem for the Dyck languages. Parentheses are inserted and removed dynamically, while the algorithm has to check whether the string is properly balanced. It is shown that this problem can be solved in polylogarithmic time per operation. The lower bound techniques from the thesis are again used to prove the hardness of this problem.

New in the BRICS Report Series, 1997

ISSN 0909-0878

25 David A. Mix Barrington, Chi-Jen Lu, Peter Bro Miltersen, and Sven Skyum. *Searching Constant Width Mazes Captures the AC^0 Hierarchy*. September 1997. 20 pp.

24 Søren B. Lassen. *Relational Reasoning about Contexts*. September 1997. 45 pp. To appear as a chapter in the book *Higher Order Operational Techniques in Semantics*, eds. Andrew D. Gordon and Andrew M. Pitts, Cambridge University Press.

23 Ulrich Kohlenbach. *On the Arithmetical Content of Restricted Forms of Comprehension, Choice and General Uniform Boundedness*. August 1997. 35 pp.

22 Carsten Butz. *Syntax and Semantics of the logic $\mathcal{L}^{\lambda}_{\omega\omega}$*. July 1997. 14 pp.

21 Steve Awodey and Carsten Butz. *Topological Completeness for Higher-Order Logic*. July 1997. 19 pp.

20 Carsten Butz and Peter T. Johnstone. *Classifying Toposes for First Order Theories*. July 1997. 34 pp.

19 Andrew D. Gordon, Paul D. Hankin, and Søren B. Lassen. *Compilation and Equivalence of Imperative Objects*. July 1997. iv+64 pp. Appears also as Tech. Rep. 429, Univ. of Cambridge Comp. Lab., June 1997. To appear in *Foundations of Soft. Tech., and Th. Comp. Sci.: 17th Conference*, FCT&TCS '97 Proceedings, LNCS, 1997.

18 Robert Pollack. *How to Believe a Machine-Checked Proof*. July 1997. 18 pp. To appear as a chapter in the book *Twenty Five Years of Constructive Type Theory*, eds. Smith and Sambin, Oxford University Press.

17 Peter Bro Miltersen. *Error Correcting Codes, Perfect Hashing Circuits, and Deterministic Dynamic Dictionaries*. June 1997. 10 pp.

16 Noga Alon, Martin Dietzfelbinger, Peter Bro Miltersen, Erez Petrank, and Gábor Tardos. *Linear Hashing*. June 1997. 22 pp. A preliminary version appeared with the title *Is Linear Hashing Good?* in *The 29th Annual ACM Symp. on Theory of Comp.*, STOC '97, pages 465–474.

15 Pierre-Louis Curien, Gordon Plotkin, and Glynn Winskel. *Bistructures, Bidomains and Linear Logic*. June 1997. 41 pp.

14 Arne Andersson, Peter Bro Miltersen, Søren Riis, and Mikkel Thorup. *Dictionaries on AC^0 RAMs: Query Time $\Theta(\sqrt{\log n/\log\log n})$ is Necessary and Sufficient*. June 1997. 18 pp. Appears in *37th Annual Symp. on Found. of Comp. Sci., FOCS '96 Proceedings*, pages 441–450.

13 Jørgen H. Andersen and Kim G. Larsen. *Compositional Safety Logics*. June 1997. 16 pp.

12 Andrej Brodnik, Peter Bro Miltersen, and J. Ian Munro. *Trans-Dichotomous Algorithms without Multiplication — some Upper and Lower Bounds*. May 1997. 19 pp. Appears in Dehne, Rau-Chaulin, Sack and Tamassio, editors, *Algorithms and Data Structures: 5th International Workshop*, WADS '97 Proceedings, LNCS 1272, 1997, pages 426–439.

11 Kārlis Čerāns, Jens Chr. Godskesen, and Kim G. Larsen. *Timed Modal Specification — Theory and Tools*. April 1997. 32 pp.

10 Thomas Troels Hildebrandt and Vladimiro Sassone. *Transition Systems with Independence and Multi-Arcs*. April 1997. 20 pp. Appears in Peled, Pratt and Holzmann, editors, *DIMACS Workshop on Partial Order Methods in Verification*, POMIV '96, pages 273–288.

New in the BRICS Notes Series, 1997

ISSN 0909-3206

1 Mogens Nielsen and Wolfgang Thomas, editors. *Preliminary Proceedings of the Annual Conference of the European Association for Computer Science Logic, CSL '97* (Aarhus, Denmark, August 23–29, 1997), August 1997. vi+432 pp.

BRICS Dissertations Series, 1997

ISSN 1396-7002

2 Peter Ørbæk. *Trust and Dependence Analysis.* July 1997. PhD thesis. x+175 pp.

1 Gerth Stølting Brodal. *Worst Case Efficient Data Structures.* January 1997. PhD thesis. x+121 pp.

News

Research Positions at BRICS Research Centre and International PhD School

There are several research positions at BRICS starting next year, 1998. Applications by researchers are welcome in theoretical computer science and related areas, especially, but not exclusively, within the following areas:

- Semantics of Computation,
- Logic,
- Algorithms and Datastructures,
- Complexity Theory,
- Data Security,
- Programming Languages,
- Distributed Computing,
- Verification.

Openings, while likely to start as postdoctoral positions generally for 1-2 years, have the possibility of extension to longer-term positions.

BRICS is funded by the Danish National Research Foundation and consists of the BRICS Research Centre and the BRICS Int. PhD School.
The Research Centre (Director Glynn Winskel) is a joint venture between the theoretical-computer-science groups at the universities of Aarhus and Aalborg, Denmark.
The PhD School (Director Mogens Nielsen) is based in the Computer Science Department at the University of Aarhus.

The BRICS Research Centre is based on a commitment to develop theoretical computer science and related mathematics, using a combination of long-term efforts and a number of short-term, intensive programmes, within carefully chosen scientific themes. The BRICS International PhD School offers a full PhD programme in computer science, including a wide range of courses, summer schools etc., and a number of PhD grants for Danish as well as foreign students. At present BRICS comprises around 25 researchers and a similar number of PhD students.

Further information on BRICS can be accessed by opening the URL below. The BRICS WWW entry contains information about activities, courses, PhD grants and researchers as well as access to electronic copies of information material and reports of the BRICS Series.

How to apply

Applications for positions should preferably be sent by e-mail (`BRICS@brics.dk`) and include: a) curriculum vitae and b) two or three names of referees for recommendations with the referees' regular mail addresses and, if possible, e-mail addresses, as well as c) an URL to your WWW home directory if available. The various parts of the application (application letter, CV, etc.) can be sent by e-mail as e.g. uuencoded PDF, PostScript, clear ASCII text or if it causes trouble, just as an URL in which case we will try to load the files.

Calendar of Events

Date	Event
6–10 Oct '97	Mini-course on The State-Explosion Problem
13–17 Oct '97	Mini-course on Systems Programming in Scheme
24–27 Nov '97	Mini-course on Functional Programming with Effect
1–2 Nov '97	PSSL, 56th Peripatetic Seminar on Sheaves and Logic
13–18 Nov '97	Mini-course on Pure Type Systems and Applications
Nov '97	Mini-course on Temporal Data Bases
12–16 Jan '98	Main event of BRICS theme on Algorithms in Quantum Information Processing
13–17 Jul '98	ICALP, 25th International Colloquium on Automata, Languages, and Programming.

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