

# BRICS *Newsletter*

Basic Research in Computer Science


No 4, February 1996

## In this Issue

<b>Welcome</b>	<b>1</b>
<b>Coming Events</b>	<b>1</b>
Courses . . . . .	1
Summer Student Program . . . . .	1
Verification '96 . . . . .	2
Autumn School . . . . .	2
<b>Reports on Courses</b>	<b>2</b>
Evolving Algebras . . . . .	2
Analysis and Transformation of Set-Theoretic Languages . . . . .	3
Secure Multiparty Computations . . . . .	3
<b>Newly Appointed Researchers, PhDs and Guests</b>	<b>4</b>
<b>New Reports</b>	<b>5</b>
<b>Notes Series</b>	<b>7</b>
<b>Lecture Series</b>	<b>8</b>
<b>News and Technical Contributions</b>	<b>9</b>
The Common Framework Initiative (CFI)	9
ALCOM-IT . . . . .	9
Educational Forum . . . . .	9
UPPAAL (cont.) . . . . .	10
B&O Industrial Collaboration . . . . .	11
<b>Calendar of Events</b>	<b>12</b>
<b>New: BRICS Address and World Wide Web</b>	<b>12</b>

## Welcome


Welcome to the fourth issue of the BRICS newsletter. Its purpose is to inform you of appointments, publications, courses and other ac-

tivities within BRICS. Further details can be obtained by contacting the addresses on the back page. 

## Coming Events

### Courses

For details see the BRICS Activities web page<sup>1</sup>.

- Mini-course on Higher Dimensional Automata by *Vladimiro Sassone*, August 1996.
- Mini-course by *Dexter Kozen*, August 1996. Title to be announced.
- Mini-course on Distributed Logics by *P. S. Thiagarajan*, autumn 1996.
- Lecture course on Stochastic Methods in the Theory of Concurrency by *Prakash Panangaden*, September to December, 1996. 

## BRICS Summer Student Program

A number of summer student positions will be available at BRICS. The positions will be associated to ongoing research activities and the students are expected to spend considerable time working on these. Examples of such activities are the UPPAAL and MONA projects.

<sup>1</sup><http://www.brics.dk/Activities>

The available positions are listed on the Web<sup>2</sup>. Only applications directed to these specific positions will be considered. Applications must be directed to the indicated researchers.

The positions will be offered for a period of one to three months during June, July, and August. BRICS will cover travel expenses and provide approximately US\$1200/month (tax free) to cover living expenses. ☰

## Verification '96

This year's BRICS theme is Verification. The activities will cover verification of computing systems in a broad sense. More specifically, we intend to investigate specification formalisms, proof principles, and technology of automated tools for verification. Events will take place during the autumn of '96.

Guests of the theme include David Basin, Tom Melham, Nils Klarlund, Randy Pollack, Prakash Panangaden and P. S. Thiagarajan.

## Autumn School

In connection with the theme, a one week autumn school will be held starting October 28 covering "Theorem Proving and Model Checking". The contents of the autumn school will be the presentation of a selected set of tools principles (theorem provers, model checkers and combina-

tions) focussing on "Cutting-Edge Applications-Oriented Techniques".

The aim of the autumn school is that the participants leave with:

- an understanding of theorem proving and model checking and their status, based on our choices of concrete tools
- (hands-on) experience with (state of the art) applications of the tools
- a feeling for the advantages and disadvantages of theorem proving vs. model checking
- ideas of possibilities of combining theorem proving and model checking
- possible research projects (short and long term)

We expect 30–40 participants. BRICS grants covering parts of local expenses will be available.

The final call for participation, including a listing of the lecturers and tools, will soon be available on the Verification theme Web page<sup>3</sup>.

David Basin, Allan Cheng, Kim G. Larsen, Tom Melham, and Mogens Nielsen are responsible for the planning. Everybody potentially interested in taking part in the activities is welcome to contact us directly at BRICS@brics.dk. ☰

## Reports on Courses

### Evolving Algebras

Professors *Egon Börger* (Univ. of Pisa) and *Yuri Gurevich* (Univ. of Michigan) visited BRICS during August 1995. From 7–10 August they held an intensive mini-course of 14 double lectures on Evolving Algebras: their framework for mod-

elling algorithms and languages, with links to both Complexity Theory and Semantics. The background and interests of both lecturers fitted particularly well with the BRICS idea of synergy between Algorithms and Complexity Theory, Semantics, and Logic.

The course was attended by 12 PhD students.

<sup>2</sup><http://www.brics.dk/Activities/96/SummerStudent>

<sup>3</sup><http://www.brics.dk/Activities/96/Verification>

Gurevich's lectures on the basic concepts and definitions of evolving algebras were all prepared specially for the course, and supported by a large collection of papers from the literature. Börger's lectures on applications of evolving algebras were based on some of his latest papers.

The supporting material for the course has been collected as printed in the BRICS Notes Series, number NS-95-4 below. Both this foreword and the individual papers can be accessed electronically via the BRICS archives. ☰

## Analysis and Transformation of Set-Theoretic Languages

In the week of 14–18 August *Robert Paige*, Courant Institute, New York University, gave a short course on how types and transformations can be used to integrate algorithm design and analysis, program development, and high level compilation of set theoretic programming languages. Topics: 1. Introduction to SETL and sources of inefficiency; program improvement by finite differencing, 2. Program improvement by real-time simulation of a typed set machine (equipped with high level input/output) on a RAM, 3. Reconstruction and extension of the linear time fragment of Willard's database predicate retrieval theory, 4. Design of a linear time fixed point language; experiments in productivity of algorithm implementation.

The course notes are published as BRICS note NS-95-5 below. ☰

## Secure Multiparty Computations

*Michael Ben-Or*, Hebrew University, Jerusalem, gave a 3 lectures mini-course on Secure Multiparty Computations 24 and 25 August.

The problem of secure multi-party function computation is as follows:  $n$  players wish to evaluate a function  $F(x_1, \dots, x_n)$ , where  $x_i$  is a secret value provided by the  $i$ 'th player. The goal

is to preserve the privacy of the player's inputs and guarantee the correctness of the computation. This problem is trivial if a trusted third party  $T$  is added to the computation. Simply,  $T$  collects all the inputs from the players, computes the function  $F$ , and announces the result. (This is the way we usually have elections, where the voters are the players and the trusted third party is the government). In general, secure multiparty computation is defined as any protocol in an ideal scenario with a 'trusted party', and a real life protocol is defined as secure if it is "equivalent" to a computation in the ideal scenario.

It was shown that whatever can be computed in this ideal scenario can be computed in a secure manner when no such trusted party exists. The course focused on two results. First it was proved that if players always follow the protocol then a  $n/2$ -private protocol exists. That is, any group with less than  $n/2$  members collaborating cannot learn additional information about the input belonging to the remaining players. For the general case where faulty players can collaborate in any way to gather information and disrupt the computation a  $n/3$ -secure protocol was given.

Literature and further information can be found on the Web<sup>4</sup>. ☰


## Quantum Computation

On 11 and 18 December 1995 *Klaus Mølmer*, Institute of Physics, Aarhus University, gave two tutorial seminars on Quantum Mechanics as a warm up to Berthiaume's mini-course in January. The seminars concentrated on aspects of Quantum Mechanics relevant to Computing and Cryptography.

*André Berthiaume*, CWI, Amsterdam visited 21–28 January 1996 and gave a 4 lecture mini-course on quantum computation. Dr. Berthiaume is one of the pioneers in quantum computation and earned the 1996 doctoral prize from the Natural Sciences and Engineering Research Council of

<sup>4</sup><http://www.brics.dk/Activities/95/SecMultComp>

Canada for his thesis on the complexity and stabilisation of quantum computation. The course introduced at a tutorial level the quantum computer and presented some milestone results in quantum complexity theory leading up to Shor's factoring algorithm. Issues pertaining to the con-

struction of a quantum computer were also discussed. The course was well attended by researchers and students from Aarhus and Odense. The course notes are published as BRICS note NS-96-1 below. 

## Newly Appointed Researchers, PhDs and Guests

### *P. S. Thiagarajan*

Prof. P. S. Thiagarajan, School of Mathematics, SPIC Science Foundation, Madras, India, will be associated with BRICS from June 1st 1996 until February 1st 1997. Thiagarajan has a record of close cooperation with BRICS, and has visited previously on a number of occasions. Thiagarajan's research area is the theory of distributed computing. He previously worked within Petri Nets, but his main contributions during the past decade has been in specification logics and semantic models, and he has particularly been a key developer of so-called "distributed logics and models".

### *Prakash Panangaden*

Prof. Prakash Panangaden, McGill University, Montreal, Canada, will in August visit BRICS for a year. Prakash Panangaden's research area is the theory of concurrency, where he has worked on expressiveness, the development of semantics for concurrent programming languages and the relationships between logic and concurrent computation. The main arenas for these studies have been indeterminate dataflow and concurrent constraint programming. More recently he has been looking at the expressive power of rendezvous in synchronous languages, the semantics of typed concurrent languages like CML, the relationship between logical connectives and process combinators and, most recently, stochastic systems.

### *Robert (Randy) Pollack*

Randy Pollack, originally from the US, got his thesis from University of Edinburgh, where he was supervised by Rod Burstall. He developed the LEGO proof development system, support-

ing proof by refinement in the Extended Calculus of Constructions and related logics, and has theoretically explained many of LEGO's features and formalized much of this work in LEGO, including the theory of Pure Type Systems leading to verified typechecking algorithms. He joins BRICS at the end of the year after a Post-Doctoral Fellowship at Chalmers University.

### *Aleksandar Pekec*

Aleksandar Pekec, originally from Croatia, recently finished his PhD thesis at Rutgers University, New Brunswick, NJ, USA, under the supervision of Fred S. Roberts. His main research interests are in the applications of discrete mathematics and has strong interests in analyzing and developing algorithms for solving various combinatorial optimization problems. Pekec will start at BRICS in early August.

### *Kousha Etessami*

Recently Kousha Etessami got his PhD from University of Massachusetts-Amherst, where Neil Immerman was his advisor. Kousha Etessami interests cover Computational and Descriptive Complexity Theory and the related areas of theoretical computer science and logic. From early August Kousha Etessami will take up a position at BRICS after having worked at the DIMACS Centre for a year.

### *Allan Cheng*

Allan Cheng got his MSc from University of Aarhus and has recently handed in his PhD dissertation entitled "Reasoning About Concurrent Computational Systems", under the supervision of Mogens Nielsen. His main interests lie within verification, concurrency, and set constraints. Allan Cheng joined BRICS February 1st.

### Lars A. Arge

Lars Arge has been a PhD student at BRICS under the supervision of Erik Meineche Schmidt, and he just submitted his PhD dissertation "Efficient External-Memory Data Structures and Applications". His area of interest is algorithms and data structures, especially for large-scale applications where I/O communication costs dominate the overall execution time. Lars Arge joined the Centre this month.

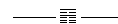
### Dexter Kozen

Dexter Kozen, Joseph Newton Pew, Jr. Prof. of Engineering, Cornell University, Ithaca, NY, USA, will visit BRICS around August. Professor Kozen's research interests include the theory of computational complexity, especially complexity of decision problems in logic and algebra, and logics and semantics of programming languages. His recent work includes new polynomial-time algorithms and deductive systems for type inference and solutions of set constraints; a new algorithm for decomposition of algebraic functions; a new polynomial-time algorithm for resolution of singularities of plane curves; and new polynomial-time algorithms for optimal transmission of encoded video data.

### Vladimiro Sassone

Research Associate Vladimiro Sassone, University of Pisa, Italy, will be visiting BRICS during summer 1996. Sassone has been associated with BRICS until recently, but has now taken up a position at his original university in Pisa. Sassone's

main interests are within theory of computation, in particular concurrency theory. He has recently taken up work on higher dimensional automata.



### Chiara Bodei

Chiara Bodei got her MSc in Computer Science from University of Pisa, with a dissertation titled "Some Relationships among Models for Concurrency" under the supervision of Prof. Pierpaolo Degano. She is now a PhD student at Pisa with her main interests in concurrency and the  $\pi$ -calculus in particular. She is visiting BRICS during spring semester of 1996, supervised by Mogens Nielsen.

### Gian-Luca Cattani

Cattani got his MSc in mathematics from University of Parma, with a dissertation titled "Categorical Models for Linear Logic" under the supervision of Prof. G. Rosolini. He is now writing his PhD dissertation at BRICS on the theme of "Sheaf models for Parallel Computation", supervised by Glynn Winskel.

### Dirk Dussart

Dussart is a graduate student, supported by the Belgian National Fund for Scientific Research (NFWO), at the Katholieke Universiteit Leuven in Belgium. He is mainly interested in partial evaluation, the application of the continuation-passing style transformation, type theory, program analysis logics and inference based program analysis. Dussart will be with BRICS for a year.

## BRICS Report Series for 1996 and 1995

ISSN 0909-0878

- 4 Jørgen H. Andersen, Ed Harcourt, and K. V. S. Prasad. *A Machine Verified Distributed Sorting Algorithm*. February 1996. 21 pp. Abstract appeared in *7th Nordic Workshop on Programming Theory*, NWPT '7 Proceedings, 1995.
- 3 Jaap van Oosten. *The Modified Realizability Topos*. February 1996. 17 pp.
- 2 Allan Cheng and Mogens Nielsen. *Open Maps, Behavioural Equivalences, and Congru-*

*ences*. January 1996. A short version of this paper is to appear in the proceedings of CAAP '96.

- 1 Gerth Støtting Brodal and Thore Husfeldt. *A Communication Complexity Proof that Symmetric Functions have Logarithmic Depth*. January 1996. 3 pp.
- 60 Jørgen H. Andersen, Carsten H. Kristensen, and Arne Skou. *Specification and Automated*

- Verification of Real-Time Behaviour — A Case Study*. December 1995. 24 pp. Appears in *3rd IFAC/IFIP workshop on Algorithms and Architectures for Real-Time Control*, AARTC '95 Proceedings, 1995, pages 613–628.
- 59 Luca Aceto and Anna Ingólfssdóttir. *On the Finitary Bisimulation*. November 1995. 29 pp.
- 58 Nils Klarlund, Madhavan Mukund, and Milind Sohoni. *Determinizing Asynchronous Automata on Infinite Inputs*. November 1995. 32 pp. Appears in *Foundations of Software Technology and Theoretical Computer Science: 15th Conference, FST&TCS '95 Proceedings*, LNCS 1026.
- 57 Jaap van Oosten. *Topological Aspects of Traces*. November 1995. 16 pp.
- 56 Luca Aceto, Wan J. Fokkink, Rob J. van Glabbeek, and Anna Ingólfssdóttir. *Axiomatizing Prefix Iteration with Silent Steps*. November 1995. 25 pp. To appear in *Information and Computation*.
- 55 Mogens Nielsen and Kim Sunesen. *Trace Equivalence - Partially Decidable!* November 1995.
- 54 Nils Klarlund, Mogens Nielsen, and Kim Sunesen. *Using Monadic Second-Order Logic with Finite Domains for Specification and Verification*. November 1995.
- 53 Nils Klarlund, Mogens Nielsen, and Kim Sunesen. *Automated Logical Verification based on Trace Abstractions*. November 1995. 19 pp.
- 52 Antonín Kucera. *Deciding Regularity in Process Algebras*. October 1995. 42 pp.
- 51 Rowan Davies. *A Temporal-Logic Approach to Binding-Time Analysis*. October 1995. 15 pp. To appear in *Eleventh Annual IEEE Symposium on Logic in Computer Science*, LICS '95 Proceedings.
- 50 Dany Breslauer. *On Competitive On-Line Paging with Lookahead*. September 1995. 12 pp. To appear in *13th Symposium on Theoretical Aspects of Computer Science*, STACS '96.
- 49 Mayer Goldberg. *Solving Equations in the  $\lambda$ -Calculus using Syntactic Encapsulation*. September 1995. 13 pp.
- 48 Devdatt P. Dubhashi. *Simple Proofs of Occupancy Tail Bounds*. September 1995. 7 pp. To appear in *Random Structures and Algorithms*.
- 47 Dany Breslauer. *The Suffix Tree of a Tree and Minimizing Sequential Transducers*. September 1995. 15 pp.
- 46 Dany Breslauer, Livio Colussi, and Laura Tonio. *On the Comparison Complexity of the String Prefix-Matching Problem*. August 1995. 39 pp. Appears in Leeuwen, editor, *Algorithms - ESA '94: Second Annual European Symposium proceedings*, LNCS 855, 1994, pages 483–494.
- 45 Gudmund Skovbjerg Frandsen and Sven Skyum. *Dynamic Maintenance of Majority Information in Constant Time per Update*. August 1995. 9 pp.
- 44 Bruno Courcelle and Igor Walukiewicz. *Monadic Second-Order Logic, Graphs and Unfoldings of Transition Systems*. August 1995. 39 pp. Presented at *Annual Conf. of the European Association for Computer Science Logic*, CSL '95.
- 43 Noam Nisan and Avi Wigderson. *Lower Bounds on Arithmetic Circuits via Partial Derivatives (Preliminary Version)*. August 1995. 17 pp. Appears in *36th Annual Conference on Foundations of Computer Science*, FOCS '95, IEEE, 1995, pages 16–25.
- 42 Mayer Goldberg. *An Adequate Left-Associated Binary Numeral System in the  $\lambda$ -Calculus*. August 1995. 16 pp. Accepted for *Journal of Functional Programming*.
- 41 Olivier Danvy, Karoline Malmkjær, and Jens Palsberg. *Eta-Expansion Does The Trick*. August 1995. 23 pp.
- 40 Anna Ingólfssdóttir and Andrea Schalk. *A Fully Abstract Denotational Model for Observational Congruence*. August 1995. 29 pp.

- 39 Allan Cheng. *Petri Nets, Traces, and Local Model Checking*. July 1995. 32 pp. Full version of paper appearing in Alagar and Nivat, editors, *Algebraic Methodology and Software Technology: 4th International Conference*, AMAST '95 Proceedings, LNCS 936, 1995.
- 38 Mayer Goldberg. *Gödelisation in the  $\lambda$ -Calculus*. July 1995. 7 pp. Accepted for *Information Processing Letters*.
- 37 Sten Agerholm and Mike Gordon. *Experiments with ZF Set Theory in HOL and Isabelle*. July 1995. 14 pp. Appears in Schubert, Windley, and Alves-Foss, editors, *Higher Order Logic Theorem Proving and Its Applications: 8th International Workshop Proceedings*, LNCS 971, 1995.
- 36 Sten Agerholm. *Non-primitive Recursive Function Definitions*. July 1995. 15 pp. Appears in Schubert, Windley, and Alves-Foss, editors, *Higher Order Logic Theorem Proving and Its Applications: 8th International Workshop Proceedings*, LNCS 971, 1995.
- 35 Mayer Goldberg. *Constructing Fixed-Point Combinators Using Application Survival*. June 1995. 14 pp.
- 34 Jens Palsberg. *Type Inference with Selftype*. June 1995. 22 pp.
- 33 Jens Palsberg, Mitchell Wand, and Patrick O'Keefe. *Type Inference with Non-structural Subtyping*. June 1995. 22 pp. To appear in *Mathematical Structures in Computer Science*.
- 32 Jens Palsberg. *Efficient Inference of Object Types*. June 1995. 32 pp. To appear in *Information and Computation*. Preliminary version appears in *Ninth Annual IEEE Symposium on Logic in Computer Science*, LICS '94 Proceedings, pages 186–195.
- 31 Jens Palsberg and Peter Ørbæk. *Trust in the  $\lambda$ -calculus*. June 1995. 32 pp. Appears in Mycroft, editor, *Static Analysis: 2nd International Symposium*, SAS '95 Proceedings, 1995, pages 314–330.
- 30 Franck van Breugel. *From Branching to Linear Metric Domains (and back)*. June 1995. 30 pp. Abstract appeared in Engberg, Larsen, and Mosses, editors, *6th Nordic Workshop on Programming Theory*, NWPT '96 Proceedings, 1994, pages 444–447.
- 29 Nils Klarlund. *An  $n \log n$  Algorithm for Online BDD Refinement*. May 1995. 20 pp.
- 28 Luca Aceto and Jan Friso Groote. *A Complete Equational Axiomatization for MPA with String Iteration*. May 1995. 39 pp.
- 27 David Janin and Igor Walukiewicz. *Automata for the  $\mu$ -calculus and Related Results*. May 1995. 11 pp. Appears in *Mathematical Foundations of Computer Science: 20th Int. Symposium*, MFCS '95 Proceedings, LNCS 969, 1995.
- 26 Faith Fich and Peter Bro Miltersen. *Tables should be sorted (on random access machines)*. May 1995. 11 pp. Appears in Akl, Dehne, Sack, and Santoro, editors, *Algorithms and Data Structures: 4th Workshop*, WADS '95 Proceedings, LNCS 955, 1995, pages 482–493.
- 25 Søren B. Lassen. *Basic Action Theory*. May 1995. 47 pp.

## BRICS Notes Series for 1996 and 1995

ISSN 0909-3206

- 1 André Berthiaume. *Quantum Computation. Mini-Course*. January 1996. iv+126 pp.
- 6 Aravind Srinivasan. *The Role of Randomness in Computation*. November 1995. iv+99 pp.
- 5 Robert Paige. *Analysis and Transformation of Set-Theoretic Languages. Mini-Course*. August 1995. iv+157 pp.
- 4 Yuri Gurevich and Egon Börger. *Evolving Algebras. Mini-Course*. July 1995. iv+222 pp.

5 Devdatt P. Dubhashi. *Complexity of Logical Theories*. September 1995. x+46 pp.

**Abstract:**

These are informal lecture notes from the course “Fundamental Results of Complexity Theory” taught at Aarhus University in the winter of 1994. The method of Ehrenfeucht–Fraïssé games is used to give a uniform framework for the analysis of the complexity of logical theories, following the well known monograph of Ferrante and Rackoff. Two examples are given as illustrations: the theory of real addition and the theory of Boolean algebras.

**Contents**

- 1 Introduction
  - 1.1 Models, Languages and Theories
  - 1.2 Decision Problems and their Complexity
  - 1.3 Bibliographical Notes
- 2 Alternation
  - 2.1 Alternating Turing Machines
  - 2.2 Alternating Complexity Classes
  - 2.3 Logical Theories in Alternating Classes
  - 2.4 Bibliographical Notes
- 3 Ehrenfeucht–Fraïssé Games
  - 3.1 Ehrenfeucht–Fraïssé Games and Elementary Equivalence
  - 3.2 Ehrenfeucht–Fraïssé Games and Bounded Structures
  - 3.3 Bibliographical Notes
- 4 Real Addition
  - 4.1 Quantifier–Elimination
  - 4.2 An EF Game
  - 4.3 Lower Bound
  - 4.4 A Research Problem
  - 4.5 Bibliographical Notes
- 5 Boolean Algebras
  - 5.1 The Structure of Boolean Algebras

- 5.2 Decision Procedures
- 5.3 Some Lower Bounds
- 5.4 Extensions
- 5.5 A Research Problem
- 5.6 Bibliographical Notes

4 Dany Breslauer and Devdatt P. Dubhashi. *Combinatorics for Computer Scientists*. August 1995. viii+184 pp.

**Abstract:**

These are informal lecture notes from the course *Combinatorics for Computer Scientists* that was offered at Aarhus University in Spring 1995. The topics covered fall into roughly three parts corresponding to the organisation of these notes:

- Part I: **Enumeration**. The techniques covered here were inclusion–exclusion, Möbius Inversion and Generating functions.
- Part II: **Graph Theory**. This consisted of a fairly standard set of topics in Graph theory including trees, matchings, Euler and Hamilton paths, (vertex and edge) colouring, Ramsey theory, planar graphs.
- Part III: **Linear Algebraic Methods**. In this somewhat novel part, simple linear algebraic methods were applied to combinatorial problems.

**Contents**

- I Enumeration
  - 1 Inclusion–Exclusion
  - 2 Inclusion–Exclusion II
  - 3 Möbius Inversion
  - 4 Möbius Inversion II
  - 5 Generating Functions
  - 6 Generating Functions II
  - 7 Yet more on Generating Functions
  - 8 Probability Generating Functions
  - 9 A Coin Flipping Game



## II Graph Theory

- 10 Basics
- 11 Trees
- 12 Eulerian and Hamiltonian Walks
- 13 Connectivity
- 14 Matching
- 15 Edge Colouring
- 16 Cliques
- 17 Vertex Colouring
- 18 Planar Graphs

## 19 Problems

### III Linear Algebra in Combinatorics

- 20 Invitation to Club Theory
- 21 Some Club Theory Classics
- 22 More Club Theory
- 23 Greedy Algorithms and Matroids
- 24 Probability Spaces with Limited Independence

## News and Technical Contributions

### Common Framework Initiative (CFI)

An open collaborative effort has been initiated: to design a *Common Framework for Algebraic Specification*. The rationale behind this initiative is that the lack of such a framework greatly hinders the dissemination and application of research results in algebraic specification. In particular, the proliferation of specification languages, some differing in only quite minor ways from each other, is a considerable obstacle for the use of algebraic methods in industrial contexts, making it difficult to exploit standard examples, case studies and training material. A common framework with widespread support throughout the research community is urgently needed.

The CFI was started by COMPASS (ESPRIT Basic Research WG 6112), in cooperation with IFIP WG 14.3 (Foundations of Systems Specification), but participation is not confined to members of those groups. Participants include some 30 leading researchers in algebraic specification, with representatives from almost all the European groups working in this area. For further details, see the CFI URL<sup>5</sup>. The coordinator of the Common Framework Initiative is Peter Mosses. ☐

### ALCOM-IT

ALCOM-IT (ALgorithms and COMplexity in Information Technology) is a new project under the ESPRIT Long Term Research programme. ALCOM-IT is a successor of the ALCOM project which was a project under the old Basic Research programme.

The Algorithmics group within BRICS is (still) a partner of ALCOM-IT; there are 11 other partners including many of the best groups in Europe. ☐

### Educational Forum

BRICS has formed a so-called "Educational Forum" with two other European Research Schools in the areas of Basic Research in Computer Science: the Dutch IPA (Institute voor Programmatuurkunde en Algoritmiëk) and the Finnish TUCs (Turku Centre for Computer Science). The aim of the Forum is to cooperate on training of young researchers. One way the Forum will present itself will be through annual meetings of educational character aimed at PhDs and young researchers. The first meeting will be organized by IPA in late 1996 in the area of Embedded Systems. The Educational Forum is chaired by prof. G. Rozenberg, University of Leiden. ☐

---

<sup>5</sup><http://www.brics.dk/Projects/CFI>

## UPPAAL — The Continued Story

by Kim G. Larsen

In BRICS Newsletter no. 3, July 95, I gave the first report on the tool UPPAAL and the collaboration between BRICS and Department of Computing Systems at Uppsala University. Since then the collaboration has continued and exciting new results and applications have been obtained. In particular, a three month visit of Paul Pettersson from Uppsala University proved very productive.

### What is UPPAAL?

First let me recall the essentials of UPPAAL. UPPAAL is a tool suite for automatic verification of invariant and reachability properties of real-time systems modelled as networks of timed automata. More concretely, UPPAAL contains a *graphical user interface* based on Autograph, and a *model-checker* combining on-the-fly verification with a symbolic technique reducing the verification problem to that of solving simple constraint systems. Figure 1 gives an overview of UPPAAL with `atg2ta` being a compiler from the graphical representation (`.atg`) of a real-time system to a textual one (`.ta`); `hs2ta` is a filter that automatically transforms certain hybrid automata (i.e. automata where clocks may have drifting and varying speed); `checkta` performs a number of simple but in practice useful syntactical checks, and `verifyta` is the model-checking module combining on-the-fly verification with constraint solving techniques. To facilitate debugging a diagnostic trace is constructed when verification fails.

### Extensions of UPPAAL

To meet requirements arising from a number of case studies the UPPAAL model and model-checker have been extended with a number of new features. In particular a notion of *commit-*

*ted locations* has been introduced enabling atomic broadcasting in real-time systems to be modelled. Additionally, in order to enable modelling of progress properties UPPAAL has been extended with a notion of *urgent channels*, on which processes should synchronize as soon as possible.

### Philips Audio Control Protocol: An Industrial Case Study

The main UPPAAL event during the autumn of 1995 was the successful verification of the so-called *Philips Audio Control Protocol* extended with handling of bus collision occurring when *two* senders initiate transmission simultaneously. The protocol is used to connect components (e.g. amplifier, tuner, CD-player, etc.) in one of Philips' high-end audio sets in order that they can communicate control messages. In particular, the bus is used to transmit remote-control messages to components without a remote-control receiver (red-eye). During our analysis we not only verified correctness for an error tolerance of up to 5% on the timing, but also detected an error in the version of the protocol that is actually implemented by Philips. This confirms our strong beliefs in the potential benefits of automatic verification.

It should be emphasised that the analysed version is comprehensive compared with previously verified versions (where in all cases bus collision is not considered): for example, the size of node space (i.e. the size of the overall product automaton) of this protocol is around  $10^6$  or  $10^3$  times larger than for the same protocol without bus collision<sup>6</sup> and contains several more clocks, synchronization channels and data variables.

The successful analysis was based on several ingredients. Most important was a two week *workshop meeting* in Aalborg in November with participation of all (seven) UPPAAL contributors<sup>7</sup> as well as David Griffioen from CWI, Amsterdam. David Griffioen had previously collaborated ex-

<sup>6</sup>which can now be verified in 3.6 seconds by UPPAAL.

<sup>7</sup>See BRICS Newsletter no. 3.

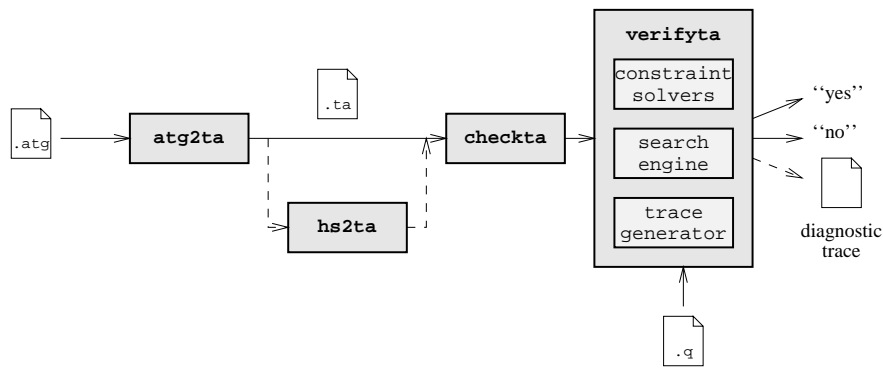


Figure 1: Overview of UPPAAL

tensively with Philips on specifying, modelling and manually analysing the protocol and his deep understanding of the case study combined with the tool insight provided by the UPPAAL team was ideal. Another crucial factor was an installation of UPPAAL on a SGI ONYX machine with very large primary memory (2 Gbytes). The verification time was approximately 15 minutes.

### Other Case Studies

In terms of complexity, Philips Audio Control Protocol with bus collision is the most serious case-study undertaken by UPPAAL so far (or any other automatic tool for verifying real time systems). In addition UPPAAL has been applied to a number of other case-studies and benchmark examples during 1995, including: several versions of Fischer's Protocol, a Steam Generator, A Train Gate Controller, a Manufacturing Plant, a Mine-Pump Controller and a Water Tank. For more information on these, the by now extensive publication list, installation guide, users manual, etc. we refer the reader to UPPAAL's WWW homepage<sup>8</sup>.

### Future Activities

The collaboration with Department of Computer Systems (DoCS), Uppsala University, will continue also in 1996. During the next six months

a BRICS PhD student (Kåre J. Kristoffersen) will visit DoCS and a guest visit of Wang Yi during the summer of 1996 is scheduled. In addition a number of mutual short-term visits will undoubtedly be made. ☐

### Bang & Olufsen: Future Industrial Collaboration

Following the successful application of UPPAAL to the Philips Audio Control Protocol a collaboration has recently been initiated between BRICS and Bang & Olufsen. The overall aim is to obtain mutual insight and experience on the application of formal methods for embedded systems. The working method will be analysis and design of realistic case studies.

In the initial phase, the focus will be made on experiments with automatic verification of real time properties. The case studies are based on the protocols of the existing B&O product BeoLink for control of audio/video devices in multiple rooms. Currently the timing aspects of the protocols at the MAC layer are being analysed. The modelling and verification is carried out by BRICS researchers whereas the company provides the detailed information on cases and their desired properties. Problems/results will be discussed at regular meetings. ☐

<sup>8</sup><http://www.docs.uu.se/docs/rtmv/uppaal>

# Calendar of Events

Date	Event
Jun-Aug 1996	Summer Student Program
Aug 1996	<i>Vladimiro Sassone</i> , University of Pisa; mini-course on Higher Dimensional Automata
Aug 1996	<i>Dexter Kozen</i> , Cornell University, NY; mini-course — title to be announced
Sep–Dec 1996	<i>Prakash Panangaden</i> , McGill University, Montreal; lecture course on Stochastic Methods in the Theory of Concurrency
Autumn 1996	<i>P. S. Thiagarajan</i> , SPIC Science Foundation, Madras; mini-course on Distributed Logics
Autumn 1996	BRICS theme on Verification
Week 44 Oct 1996	Autumn School on Theorem Proving and Model Checking
1997	CSL '97 (Computer Science Logic).

## New: BRICS Address and World Wide Web

Please **note** that the Centre now has got new (and shorter) net addresses! The old ones, however, will continue to be valid.

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, at

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 infor-

mation 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
cd pub/BRICS
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 1996