BRICS Newsletter

Basic Research in Computer Science

No 9, September 1998

In this Issue

Welcome

Welcome to the ninth 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.

BRICS has had a busy summer, with an exciting range of activities. They began with the first APPSEM workshop in May, for which Olivier Danvy was a chief organiser; it was due to be held at Aarhus under the auspices of BRICS but because of widespread strikes in Denmark had to be moved to Göteborg at the last minute. In June, Peter D. Mosses arranged possibly the first of a series of short workshops on Applications of Formal Methods, aimed mainly at Danish attendees. The exciting list of invited speakers and satellite meetings helped attract a large attendance to ICALP '98 in Aalborg, organised by BRICS with Kim Guldstrand Larsen as programme chair and Sven Skyum and Glynn Winskel as vice chairs. Another enjoyable event, also in July, was the summer school on Cryptography and Data Security, arranged by Ivan B. Damgård. Lars Arge and Jeffrey S. Vitter held a meeting on Massive Datasets. The workshop PTAC (Proof Theory and Complexity), organised by Carsten Butz, Ulrich Kohlenbach and Søren Riis, capped the end of the summer. It attracted many big names of the field and gave a fascinating and broad view of the state of the art in Mathematical Logic.

Glynn Winskel is going ahead with plans for a May summer school on Semantics of Computation, based around lectures from some of the chapters from the Handbook of Logic and Computer Science.

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.

Which π-Calculus are we Talking About?

Late October, 1998, Aarhus. *Paola Quaglia*, BRICS, will give a mini-course of 4 double lectures on the π-calculus and related calculi.

The π-calculus is considered to be the prototypical calculus for the description of distributed systems with a dynamically changing interconnection topology. It was introduced by R. Milner, J. Parrow, and D. Walker in 1989, and over since it has proliferated in a family of calculi slightly departing from the original one in their view about interaction.

This will be a self-contained course, meant to be a very basic introduction to π-calculus and π-calculi. We will present late and barbed semantics, and touch on polyadicity, asynchrony, and their encodings.

Biological Concepts for Adaptive and Distributed Algorithms

November 9, 10, 11, 16, 17, 1998, Aarhus. *Thiemo Krink*, BRICS, will give a mini-course of 5 double lectures on biological concepts for adaptive and distributed algorithms.

Biological ideas can serve as sophisticated models for problem-solving strategies and the design and management of complex computing systems. This potential, found in biological systems, arises from Nature's characteristic capability of parallel processing, self-organisation, efficiency and robustness, i.e., effective behaviour under unpredictably changing conditions. Interestingly, there are various analogies between complex systems in computer science and biology, as for instance competition for resources, division of labour or concurrency. However, apart from evolutionary computing and artificial neural networks, there are surprisingly few studies into potential applications of other biological ideas that might be useful to IT problems and questions.

In this mini-course we will discuss various aspects of biology, which could be used for novel adaptive and distributed algorithms and introduce some existing biological models already used in in artificial intelligence (AI) and artificial life (ALife). The aim of the course is to raise interest for these (yet) unused biological ideas and to point at problems related to their identification and application in computer science.

In particular, we will discuss:

- Introduction and overview (including general introduction and motivation, organisation and origin of life, and methods for identification of significant processes)
- Emergent properties and self-organisation (including concept of emergent properties, ALife, chaos theory, and virtual robotics)
- Adaptive and distributed information processing (including concepts and models of evolution and genetics)
- Means of interaction (including perception, communication, synchronisation, and decision making)
- Models for complex interactions in natural and artificial systems (including optimal foraging theory, game theory, coevolution, and organisation of social systems)

Information about the speaker

Thiemo Krink is currently enrolled as a research assistant professor (Forskningsadjunkt) at the BRICS PhD school. He was trained as a computer scientist at the Universities of Erlangen-Nürnberg and Hamburg (Germany), with special focus on computer simulation, AI and object-oriented programming. Within these areas he had specific interests in interdisciplinary research, which were stimulated by his medicine studies and his free lance activity as a business consultant. As an MSc student, he conducted two interdisciplinary projects on modelling of animal behaviour in collaboration with the biologist prof. Fritz Vollrath at Oxford. In 1994, he received his MSc degree in computer science and continued his research at the Department of Zoology, Aarhus, where he was conferred his PhD degree (biology) in 1997. Most of his papers and conference talks were focused on the design and application of virtual robots for biological research. Apart from his own activity as a scientific author, his research has been published by public media such as newspapers (e.g., Berlingske Tidende), journals (New Scientist), books (R. Dawkins: Climbing Mount Improbable) and TV (e.g. Scientific American Frontiers). His current research interests are in the fields of (i) applications of biological concepts for computational ideas and (ii) theoretical biology concerning general models for coevolution and behavioural ecology.

A Formal Calculus for Distributed Agents

Late November, 1998, Aarhus. *Matthew Hennessy*, School of Cognitive and Computing Sciences, University of Sussex, UK, will give a mini-course on a formal calculus for distributed agents.

The lectures will examine a formal language for describing widely distributed open systems where mobile agents can move from site to site seeking resources and effecting computations. We will principally be concerned with type systems for such agents which guarantee no misuse of local resources, even in the presence of agents which may harbour malicious intentions.

The language, Dpi, is obtained by adding to the the π-calculus new constructs for located processes and process migration. The type system is based on the notion of a location type, which describes the set of resources (channels) available to an agent at a location. Resources are themselves equipped with capabilities, and thus an agent may be given permission to send data along a channel at a particular location without being granted permission to read data along the same channel.

In the presence of potentially malicious agents we show that the integrity of local resources can still be maintained by incorporating various forms of type checking into the runtime semantics.

Mobile Agents in Practise

January, 1999, Aarhus. *Vladimiro Sassone*, Dept. Computer Science, Queen Mary and Westfield College, University of London, UK, will give a mini-course on Mobile Agents in practise.

The lectures will provide an overview of some of the existing mobile agents programming systems, illustrating their designs, features, and some implementation issues. We might also focus on few formal calculi to serve as common languages to describe and compare things at an essential level and, possibly, provide inspiration for future developments.

For further information on the lecturer, please refer to his profile on page 16.

Modelling and Verifying Authentication Protocols

January–February, 1999, Aarhus. *Sanjiva Prasad*, IIT (Indian Institute of Technology), Delhi, India, will give a mini-course on modelling and verifying authentication protocols.

With the growth of the internet, and communication between distributed sites, *security* and *privacy* are “hot” topics. A class of protocols, called authentication protocols, are used to establish (with cryptography) secure communication channels between distributed agents. We will study *some* approaches to specifying and modelling such protocols, and to establish their correctness, assuming perfect cryptography. The focus of our treatment will be on process calculus approaches and general theorem-proving techniques, as opposed to belief logics and logic programming approaches. A working knowledge of the π-calculus will be assumed.

For further information on the lecturer, please refer to his profile on page 16.

Summer School in Semantics

The European Educational Forum (EEF) is a joint initiative of the three research schools BRICS (Basic Research in Computer Science) in Denmark, IPA (Institute for Programming Research and Algorithmics) in the Netherlands, and TUCS (Turku centre for Computer Science) in Finland.

The EEF organises summer schools on foundations of Computer Science, each covering parts of the Handbook of Logic in Computer Science (Oxford University Press), the relevant chapters being part of the course material. There are student grants available.

As part of this programme Glynn Winskel is organising a Summer School on Semantics, based principally on part 3 of the Handbook. The Summer School will take place here in Aarhus over a week in May 1999 (the precise time is to be fixed shortly).

So far the following lectures are planned:

Carl Gunter	— Semantics of Types
Achim Jung	— Domain Theory
Luke Ong	— Correspondence between Operational and Denotational Semantics
Bob Tennent	— Denotational Semantics

There are likely to be supplementary lectures on Category Theory.

Each lecturer is to teach for 5–6 hours based on the topic of their chapter in the Handbook—a proportion of this time could be spent supervising students through exercises. Lecturers are under no obligation to stick religiously to the Handbook material, and might prefer to use it more as a starting point from which to look at new developments.

Reports on Events

2-Categories and Bicategories

March 4–18, 1998, *Anthony J. Power*, LFCS (Laboratory for Foundations of Computer Science), University of Edinburgh, Scotland, UK, gave three double lectures on 2-Categories and Bicategories. The course notes are available as BRICS Note [NS-98-7] below.

Expressiveness and Complexity of Program Logics

April 23–27, 1998, *Igor Walukiewicz*, Department of Informatics, Warsaw University, gave three double lectures on Expressiveness and Complexity of Program Logics.

Normalisation in Lambda-Calculus and Type Theory

April 29–30, 1998, *Morten H. Sørensen*, DIKU, University of Copenhagen, Denmark, gave three double lectures on Normalisation in Lambda-Calculus and Type Theory.

Advanced Data Structures

May 26–June 3, 1998, *Arne Andersson*, LTH (Lund Institute of Technology), Sweden, gave five double lectures on Advanced Data Structures with an initial special guest lecture of *Stefan Nilsson*, Technical University, Helsingfors, Finland, on Efficient Data Structures with Bit Fiddling.

APPSEM Workshop on Normalisation by Evaluation

The first APPSEM Workshop on Normalisation by Evaluation, NBE '98, took place on May 8 and 9, 1998 in Chalmers, Sweden.

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 NBE '98 was to bring together all people who have discovered and / or worked with normalisation by evaluation. And this very international workshop certainly succeeded in that respect: most talks culminated with the same normalisation function, starting from proof theory (Ulrich Berger, Matthias Eberl, Helmut Schwichtenberg), type theory (Peter Dybjer), category theory (John Reynolds, Thomas Streicher), logic (Thorsten Altenkirch), and partial evaluation (Olivier Danvy). The presentations were both recapitulative (Peter Hancock) and prospective (Andrzej Filinski, Eugenio Moggi, Torben Mogensen, Kristoffer Rose, Zhe Yang).

For the record, NBE '98 was scheduled to take place in Aarhus. Because of the strike in Denmark, however, on May 4, we boldly relocated the workshop to Göteborg, and thanks to Janne Christensen at BRICS and Marie Larsson at Chalmers, things worked out. As for the scientific momentum, it was such that we only lost three participants from abroad (Japan, Israel, and France).

Further information on APPSEM: www.md.chalmers.se/Cs/Research/Semantics/APPSEM and NBE'98: www.brics.dk/~nbe98. Preliminary proceedings: [NS-98-1] below.

Organisers: Olivier Danvy and Peter Dybjer.

AFM '98, Workshop on Applicability of Formal Methods

Aarhus, June 2, 1998

The aim of the workshop was to gather together some of the leading Danish researchers working on formal methods and tools. The invited speakers presented their favourite methods / tools, giving a summary of industrial usage: experience, prospects. Some of the presentations included demonstrations of tools.

The methods and tools presented included Design / CPN, Mona, RAISE, UPPAAL, VDM, and visualSTATE. The invited speakers were Henrik R. Andersen (Computer Systems Section, DTU, Technical University of Denmark), Dines Bjørner (Software Systems Section, DTU), Kurt Jensen (DAIMI, University of Aarhus) Peter Gorm Larsen (IFAD, Odense), Kim G. Larsen (BRICS) and Michael I. Schwartzbach (BRICS).

The workshop concluded with an open discussion of the prospects for increasing the use of formal methods and related tools in software engineering, and of ways of improving dissemination and awareness of Danish work in this area, both within the research community and for potential industrial users.

52 registered to the workshop.

The proceedings of the workshop are available as BRICS Note [NS-98-2] below.

ICALP '98

by Manfred Kudlek[1]

ICALP '98, the 25th in this series of conferences on Theoretical Computer Science, took place at Aalborg, for the second time in Denmark, from July 13 to 17, 1998. It was the Silver Jubilee of *ICALP*.

The conference site was the Aalborg Congress and Culture Centre, a modern and very convenient place for conferences, situated near Main

[1] Some tables of statistical nature have been removed from the report.

Railway Station, and 10 minutes walk from the town centre.

ICALP '98 was organised by EATCS, BRICS and the Department of Computer Science at Aalborg University.

The organising committee consisted of Helle Andersen, Hans Hüttel, Ole Høgh Jensen, Kim Guldstrand Larsen (Chair), Lene Mogensen, and Arne Skou.

ICALP '98 was supported by Bosch Telecom, Beologic VisualSTATE, Department of Computer Science at Aalborg University, BRICS, ERCIM, and the City of Aalborg.

ICALP '98 was attended by 220 participants from 29 countries, most of them from Denmark, Germany, USA, and France. The following table is presenting their numbers.

DK	45	CDN	3	J	3	TJ	2
D	35	S	7	P	3	A	1
USA	23	PL	5	AUS	2	IS	1
F	17	B	4	CH	2	LT	1
I	13	CZ	4	H	2	N	1
GB	12	E	4	IND	2	RC	1
IL	11	NL	4	RUS	2	SK	1

There were also 4 satellite workshops, namely

- Software Tools for Technology Transfer, STTT '98 (July 12 with 8 submissions, and 22 participants),
- Infinity '98 (July 18 with 3 invited talks and 5 submissions, and 27 participants),
- Semantics of Objects as Processes, SOAP '98 (July 18 with 7 submissions, and 24 participants),
- APPROX '98 (July 18–19 with 3 invited talks and 14 submissions, demos, and 34 participants),
- a Summer School in Cryptology and Data Security (July 20-24),
- as well as tool exhibitions (July 13–14 : APICES, UPPAAL, XTL, C-Mix, CVT).

Including the satellite workshops there were 227 participants in total.

The scientific program consisted of 8 invited lectures, a special lecture, and 70 contributions selected from 176 (originally 182 because 6 were withdrawn) submitted papers from 38 countries. It covered the following fields :

Algorithms

Approximation

Automata

Automata and BSP

Complexity

Computational Geometry

Formal Languages

Networks and Routing

Quantum Computing and Computational Biology

Zero-knowledge

Semantics

Automata and Temporal Logic

Concurrency

Infinite State Systems

Pi-Calculus

Programming Languages and Types

Real Time

Rewriting

Semantics

Theorem Proving

Verification

The 8 invited lectures as well as the special lecture were given in plenary sessions. 69 of the 70 submitted papers (the talk by Alexandre Tiskin was cancelled) were presented in two parallel sessions, the second time on ICALP. Sessions A (Semantics) were in Musiksalen, plenary sessions and sessions B (Algorithmics) in Radiosalen.

Submitted / Accepted	S	A
Algorithmics		
Algorithms and Data Structures	36	18
Complexity	24	11
Languages and Automata	17	6
Semantics		
Logic and Verification	36	15
Concurrency	28	12
Semantics	25	5
Programming Languages and Types	10	3

The conference was opened on Monday morning by Kim Larsen, presenting information on the organisation of ICALP '98, and on BRICS which was founded in 1994 at Aarhus and Aalborg.

The first invited talk by Amir Pnueli (coauthors Yonit Kesten, Li-on Raviv) on *'Algorithmic Verification of Linear Temporal Logic Specifications'* was an excellent introduction into methodology and techniques of a framework for model checking in linear-time temporal logic.

Mark Overmars with the second one, *'Geometric Algorithms for Robotic Manipulation'*, presented another good talk on fixturing (*'How many fingers to hold a beer bottle fixed ?'*) and orienting parts. He started with *'Hoping to manage better with slides than on my first talk ?'*

Avi Wigderson presented an excellent third invited talk *'Do Probabilistic Outperform Deterministic Ones ?'* on computational Pseudo-randoms, also putting questions from time to time.

Also Andrew Pitts with *'Existential Types : Logical Relations and Operational Equivalence'* gave an excellent fourth invited lecture, starting with *'I am for the first time on ICALP'*, demonstrating with a gymnastic position he always sees ICALP lecturers in the Bulletin, and also asking for a third projector.

Another excellent invited lecture was presented by Thomas Henzinger with the fifth one *'Model Checking Game Properties of Multi-agent Systems'*, and two messages *Kripke structures are poor models* and *linear/branching time temporal logic is too restrictive*, introducing *alternating transition structures* and *alternating temporal logics*.

Leslie Valiant gave a good sixth one with *'A Neuroidal Architecture for Cognitive Computation'*, unifying the formalism of reasoning and learning.

The seventh invited lecture *'New Horizons in Quantum Information Processing'* by Gilles Brassard was another excellent presentation on the present status of Quantum Computing, especially on quantum bank notes, quantum cryptography, and quantum teleportation, showing that quantum beats deterministic and probabilistic. He finished with *'The quantum taketh away and the quantum giveth back'*.

In the eighth one, *'Protection in Programming-Language Translations'*, Martín Abadi discussed translations of Java classes and implementations of private channels with cryptographic methods. He started with Jorge Luis Borges's book *La muerte y la brújula*, the foreseeing of a murder by a logician.

With the Gödel price lecture *'A Brief Survey on Operator-based Complexity Theory'* Seinosuke Toda gave an excellent presentation of his results on an interesting alternative approach to Complexity Theory.

Only some personal impressions on the submitted papers can be given here.

Dietrich Kuske showed interesting results on existentially first-order definable languages and their relations to NP.

Sławomir Lasota, with the best student paper in semantics, gave a very good presentation *'Partial-congruence Factorisation of Bisimilarity Induced by Open Maps'*. He started with two semantics of his title, and showed an interesting new approach.

Alain Finkel gave a good presentation on interesting results between decidability and undecidability for reset nets, mentioning *'I have a proof of 20 pages (after my talk is only lunch !)'*, *'Yesterday I had 50 slides trying to compress'*, and *'To finish my conclusion I have 2 minutes'*.

Chi-Jen Lu had a good presentation with the best student paper in algorithmics, *'Improved Pseudorandom Generators for Combinatorial Rectangles'*.

Paolo Baldan showed interesting relations between traces and graph processes, and John Power with a blackboard talk told us *'At this point most of you are anyway lost, don't worry, only 5 minutes'*.

In the *bird session* (for the T-shirts or pullovers) Arto Lepistö showed new results on the behaviour of infinite words, and Jean-Éric Pin had an excellent presentation on relations between *non-commutative algebra, finite model theory, structural complexity*, and *topology*. It was his 10^{th} full ICALP paper with which he earned the golden EATCS button. the golden EATCS button.

Giovanni Manzini presented interesting results on the *entropy of cellular automata*, and Daria Walukiewicz gave a nice talk on rewriting with associative and commutative symbols. As her brother Igor Walukiewicz also gave a talk this was the first time on ICALP's that there were talks by sister and brother.

Moshe Vardi had an excellent presentation on the *μ-calculus*, with reasoning about the past. Wojciech Plandowski showed interesting results on word equations, and Alain Tapp gave a good talk on quantum counting.

John Michael Robson with *'The most topical talk of the conference'*, using also both hands, presented nice results on queue machines and *Palindromedaries* like *damejer nis berg $ greb sin rejemad*.

During the breaks coffee, tea, water, and cakes were served. Lunch was served in 2 rooms of the restaurant of Aalborg Congress and Culture Centre.

The conference proceedings, edited by Kim Guldstrand Larsen, Sven Skyum, and Glynn Winskel, containing all invited lectures and all contributions, although the invited lectures of Mark Overmars, Avi Wigderson, Thomas Henzinger and Gilles Brassard, only as abstracts, have been published as Springer LNCS 1443.

The proceedings of APPROX '98, edited by Klaus Jansen, and José Rolim, have been published as Springer LNCS 1444.

Telnet, with 9 work stations, was available during the entire conference.

There was the book exhibition by Springer as usual, and also such by VSP, and Cambridge University Press.

The social program started on Sunday evening with registration and the World Football Champion final match TV show on a large screen in the room 'Det lille Teater' (the French team won against the team of Brazil). There was free beer, cola, and chips.

On Monday evening there was a reception in Nordjyllands Kunstmuseum, a modern building designed by Alvar Aalto (his only building in Denmark). There we listened to speeches by Sven Caspersen, the University President, on the university and science in Aalborg, and by Mrs. Aase Bak, the Curator of the museum, on the museum, and on Ingvar Cronhammer and his art (e.g. the *Ballroom*) After a guided tour (in two groups) through the museum we got snacks and white wine. The reception ended well after 20 h.

Figure 1: Demonstrations in the "telnet corner" during breaks.

On Tuesday evening the Gödel price for 1998 was presented by Emo Welzl to Seinosuke Toda for his work on *Operator-based Complexity Theory*, and the awards for the best student papers by Kim Larsen to Chi-Jen Lu in algorithmics, and to Sławomir Lasota in semantics.

After that there was a special celebration of 25 ICALP's by Josep Díaz and this report's author who showed slides from all the 24 previous ICALP's.

Following was the traditional EATCS General Assembly. The author of this report presented silver EATCS buttons to the three editors of the proceedings (Kim Larsen, Sven Skyum, Glynn Winskel, to Torben Hagerup for having reached 5 full papers on ICALP's, and a golden EATCS button to Jean-Éric Pin as the first author having reached 10 full papers. Another button goes to Michael Rabin for 5 full papers too (due to a mistake he didn't get it in 1997).

Because of late time some topics had again to be postponed to the Conference dinner.

On Wednesday afternoon we first went by bus to the town centre to visit the Monastery of the Holy Spirit, a complex from 1431, being Denmark's oldest social welfare station.

After proceeding with a short sightseeing through the town by bus we went to Thingbæk Kalkminer (chalk mines) where we walked in the underground to admire some 100 sculptures in gypsum being mostly originals from which bronze figures have been cast, e.g. a Cimbrian bull at Aalborg. Listening to Aalborg Jægerklub Blæsergruppe we got red wine with blackberry.

After another short bus trip, we walked through the woods of the Rold Skov National Park, climbing through the trunks of a yew tree for good health, meeting robbers and getting champagne on the way.
Finally, we arrived at Rold Storkro where we had the Conference Dinner.

In a special performance Kim Larsen also proved that ICALP '98 beated ICALP '82 in showing that the conference bags were bigger at Aalborg. After that he distributed, in the name of Grzegorz Rozenberg who, unfortunately, couldn't come, presents (a little bottle of Aquavit or a booklet on Vikings) to all those having at hand the latest EATCS Bulletin, or having contributed to the last 3 issues (but the list of contributors was missing).

Josep Díaz gave presents to the organisers of ICALP '98 and to Wilfried Brauer.

Later on some groups inspired by Kim Larsen who distributed copies of songs from ICALP '82 at Aarhus, started to sing, the Danish and Polish group finally standing on their chairs, Jacques Sakarovitch for the French, and Klaus-Jörn Lange for the Germans.

Soon after that the Rebild Spillemændene (Rebild fiddlers), with dance group, presented us Danish folklore music for dancing, and quite a number of us had to join.

Just after the last talk on Thursday afternoon there was a local football match among two groups of participants from Aalborg and some from other countries.

Figure 2: *Mike Paterson* in sword fight with local inhabitants.

Following that there was a bus excursion to Lindholm Høje, a Viking burial ground in a suburb of Aalborg. After visiting also the Viking museum there we got a Viking meal (roasted pork) with mjød (actually 2/3 beer and 1/3 mead) from a Viking group. Some of us (as Mike Paterson and the author of this report) also had a sword fight with one of these vikings. Fortunately, we survived.

Weather was fresh, with showers and highest temperatures between 15° and 20°C .

Unfortunately, all those nice things like Algorithms, the biggest Computability in Town, Automata, Languages, Complexity, Semantics, etc. were not offered in Jomfru Ane Gade, the main restaurant street in Aalborg, as indicated on the front page of the ICALP program.

Thus, ICALP '98 was again successful, in a relaxed atmosphere, well organised and on a high level.

Next ICALP, the 26^{th}, will be held at Praha (*Czechia*) from July 11–15, 1999. Again, it will be organised with satellite workshops.

Semantics of Objects As Processes, SOAP '98

July 18, 1998, this informal workshop with selected contributions on *(clean) semantics for objects as processes* was held in Aalborg Congress and

Culture Centre as a post-satellite of ICALP ’98.

With the growing popularity of languages like C++ and Java, the past decade has seen a flurry of interest within the programming language research community for providing a firm semantic basis for object-oriented constructs. Recently, there has been growing interest in studying the behavioural properties of object-oriented programs using concepts and ideas from the world of concurrent process calculi, in particular calculi with some notion of mobility. Not only do such calculi, as the well-known π-calculus by Milner and others, have features like references and scoping in common with object-oriented languages; they also provide one with a rich vocabulary of reasoning techniques firmly grounded in structural operational semantics.

The aim of the SOAP workshop has been to bring together researchers working mainly in this area, but in related fields as well, where other process models or calculi are used as a basis for the semantics of objects. Among the submissions, the following six were selected by the programme committee (Martín Abadi, Hans Hüttel, Josva Kleist, and Uwe Nestmann) and presented at the meeting, which attracted more than 30 researchers to participate:

Carlos Herrero — Object-Oriented Parallel Label-Selective λ-calculus
Lucia Pomello — Observation equivalences for type and implementation inheritances
António Ravara — Towards an Algebra of Dynamic Object Types
Paul Hankin — A Concurrent Object Calculus: Summary of the Operational Semantics
Silvano Dal-Zilio — Quiet and Bouncing Objects: Two Migration Abstractions in a Simple Distributed Blue Calculus
Josva Kleist — Surrogates in Øjeblik: Towards Migration in Obliq

Local organisers of the workshop were Hans Hüttel and Uwe Nestmann.

Summer School ’98 in Cryptology and Data Security

Chronicle by *Jose Manuel Fernandez*, Montreal University, Canada.

The Summer School ’98 in Cryptology and Data Security organised by BRICS and paid for by the generous European Commission, was celebrated in Aarhus, Denmark on July 20–24, 1998. The speakers, all of them leading experts in their field, spoke and explained the basics and some of the deeper concepts and techniques relating to modern Cryptology today. Some 130 participants from four continents and 27 countries attended the summer school, including undergraduate and graduate students as well as industry professionals.

The consensus seemed unanimous in praising the organisation of the summer school for choosing speakers of such high quality, and at the same time achieving a difficult balance of theoretical and practical aspects in covering the most important and relevant areas of the field. The overall quality of the presentations, as well as the availability of the speakers to field questions during and after the presentations, made the school a rotund success.

Figure 3: *Ivan B. Damgård* in discussion with *Bart Preneel*.

The conference debuted with a welcoming reception on Sunday. On Wednesday, the social program resumed with an organised visit to the

Figure 4: Summer School participants on their "arduous" trek through the woods.

Moesgaard museum of Danish Pre-History and Medieval History. The attendees were educated by the museum guides on the peculiarities of Viking life in Denmark. Many attendees and particularly some of the new foreign students in BRICS, were glad to realize that some of the more "interesting" customs are not as much in use nowadays, such as the one involving foreign slaves (students) being "voluntold" to accompany their masters (directors) into Valhalla.

Figure 5: Students exchanging ideas during the welcoming reception.

After the visit and an arduous trek through the woods, during which we were repeatedly attacked by hordes of horse-mounted Vikings (participating at a nearby re-enactment festival), most of the group made it to the beach. Such arduous efforts were dully compensated by the refreshments which awaited for us there, provided by the organisers. Two valiant male members of the group volunteered to perform an interesting scientific experiment: the measurement of sea water temperature in inches...

Later that evening, the conference dinner was celebrated at the Mathematics cafeteria, with Professor Peter Landrock acting as toastmaster and master of ceremonies. Professor Ivan Damgård started to warm up the evening with his fiddle, playing some traditional Danish tunes, a Polka, and a very technically demanding piece of his own composition, "The Mouse Trap", to which the crowd went wild. After the suitable amount of food and refreshments was imbibed, a singing match ensued between the different cultural groups represented, carefully orchestrated by Professor Landrock. Songs were "sung" in Polish, Dutch, German, Swedish, Danish, Spanish, and English. It was deemed necessary, for better sonority it is presumed, that the last song be sung from higher ground. Fortunately and miraculously, no furniture was damaged. It is also quite fortunate that the perspectives for improvement in the industry job market in Cryptology will help in keeping those present at the dinner far away from the musical scene.

Figure 6: PTAC '98 participants in the Botanical Gardens on their way to the Old Town.

Cryptologists are compulsive gamblers and like to take risks, and this conference was an excellent proof of this fact. David Chaum gambled 100 Kroner, hoping that nobody in the audience could identify the three cryptographers in the "Dining Cryptographers' Problem" cartoon, which was part of his presentation. Bart Preneel, on trying to make a point about the power of birthday attacks, promised to pay 20 Kroner if THREE people in the audience had their birthday in the same day. Needless to say, both of them lost their wagers, but as good gamblers, they both paid up their dues.

The second and last excursion of the conference, on Thursday, was to Den Gamble By. Much to the surprise of many participants, this was not some sort of casino (keeping in tone with the conference), but a charming open air historic museum of old Danish houses. The visit was followed by a finger-food reception in one of the old houses.

However, not everything was fun and games. The presentations by the speakers motivated some fruitful informal talks amongst the attendees, from which some new directions of research have been suggested, such as:

- The application of Borel Space representations to Zero-Knowledge Protocols, and more generally to Multi-Party Secure Computations,
- How to build scalable 1-qubit quantum computers, and
- the Dancing Cryptographers' Problem, a more generalised and up-to date version of the Dining Cryptographers' Problem (to be submitted to the next EuroCrypt or Crypto).

In summary, the summer school was an exemplary success of organisation, both in content and in its logistic and social aspects. It was also a success of participation and collegiality, as it provided a stimulating environment of interaction among experts, students and professionals interested and / or already working in the field of Cryptology. 𝌆

Proof Theory and Complexity, PTAC '98

Here we bring a report written by one of the participants *Jeremy Avigad*, Department of Philosophy, Carnegie Mellon University, Pittsburgh, USA.

Figure 7: *Gaisi Takeuti* and *Solomon Feferman*.

Figure 8: *Sasha Razborov* and *Vladimir Orevkov*.

PTAC ’98, the BRICS workshop on Proof Theory and Complexity, was held in Aarhus on August 3–7, and drew more than 60 participants from around the globe. The program contained 26 talks and brought together a mix of logicians with a wide range of interests. These included the following:

- Proof Theory: that is, the study of the proof-theoretic and computational strength of classical theories of mathematics. This includes theories of second-order arithmetic, explicit mathematics, and set theory, and the various proof theoretic tools that are used to analyse them.

- Constructive Mathematics and Computability: this includes various forms of constructive logic, the semantics thereof, and applications to computer science. In particular, a number of talks addressed the problem of finding natural frameworks for polynomial-time computability.

- Bounded arithmetic and proof complexity: this includes weak fragments of arithmetic, lower bounds on the complexity of proofs in various proof systems, and relationships to computational complexity.

Figure 9: *Roy Dyckhoff* and *Helmut Schwichtenberg*.

Figure 10: *Anita Feferman* and “her group” listening to the Old Town guide.

This mixture proved to be an exciting and stimulating one for all involved, and participants were

Figure 11: Participants in workshop on Massive Data Sets. Back row from the left: *Andreas Crauser*, *Jeffrey S. Vitter*, *Gerth Brodal*, *Lars Arge*, *Erik Meineche Schmidt*. Front row from the left: *Roberto Grossi*, *Paolo Franciosa*, *Octavian Procopiuc*, *Jan Vahrenhold*.

able to share insights from their various fields of expertise during question periods and breaks. A biographical talk on Alfred Tarski, given by Anita Feferman, helped all present to locate important logical developments in interesting personal and historical contexts.

Of course, the social side to the gathering can't be ignored. On Wednesday afternoon, visitors to the conference enjoyed an excursion to the old town, Den Gamle By. And at the conference dinner on the second to last day, they were treated to a rousing rendition of "Een Triomfantelijk Lied van de Zilvervloot," and were inspired to augment "Famous Men of Science" with a few new verses.

Many participants have expressed the hope that there will be future PTAC meetings, held at other sites. Indeed, the conference's success, with its particular affiliation of disciplines, suggest that such gatherings have much to contribute to logic and computer science.

More information on the workshop including abstracts of talks can be found at www.brics.dk/PTAC98/. Proceedings with full version papers will be published as a special issue of "Annals of Pure and Applied Logic".

BRICS workshop on Massive Data Sets

In the week of August 3–7, 1998, BRICS hosted an informal workshop around the theme "Theory and practice of algorithms for problems involving massive data sets". Apart from local BRICS researchers and researchers from Danish universities, the workshop had participants from several European universities (MPI, Müenster, Florence, Rome) and from the leading US university in the area (Duke).

The workshop activities were initiated Monday afternoon with a two lecture survey of the area given by Jeffrey S. Vitter from Duke University. Jeff Vitter is well regarded as an expert and world leader in the area of algorithms for problems involving massive data sets (also called *external-memory algorithms* or *I/O-algorithms*). In the late 1980s he was one of the founders of the area. Jeff's participation in the workshop was part of a 4 week visit to BRICS.

Tuesday morning was devoted to four short talks on practical implementation aspects of algorithms for massive data sets. Octavian (Tavi) Procopiuc (Duke) talked about "I/O-efficient algorithms for batched searching problems with applications to spatial data", Jan

Figure 12: From left: *Josef Tapken* (sitting), *Carsten Weise* and *Josva Kleist*.

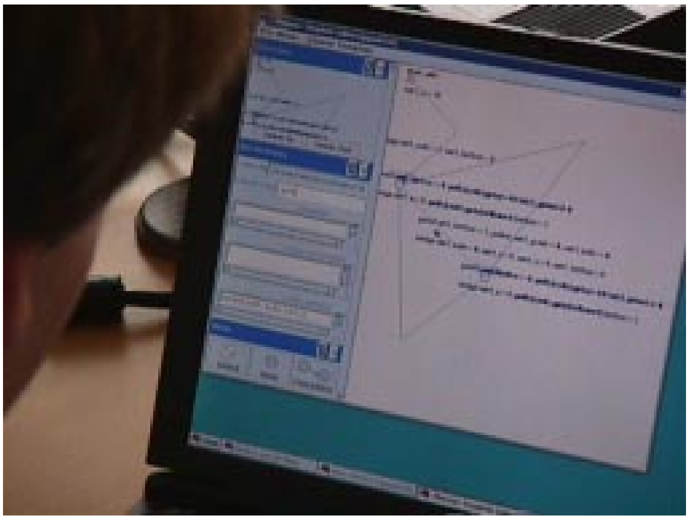


Figure 13: UPPAAL trying to recognise the internal format of MOBY.

Vahrenhold (Müenster) about "Efficient bulk operations on dynamic R-trees", Andreas Crauser (MPI, Saarbrücken) presented "LEDA-SM: A library towards secondary memory computation", and Roberto Grossi (Florence) gave "Some remarks on the block size in external memory experiments". In the afternoon the discussion of ideas and results continued in several small research groups.

On Wednesday morning two longer talks on some very recent theoretical results were given. Lars Arge (Duke) talked about "I/O-efficient point location in planar monotone subdivisions" and Gerth Brodal (MPI/BRICS) presented "Level-balanced B-trees". The afternoon, as well as Thursday, was again spent in small (and very productive) research groups. Somehow time was also found to research the night-life of Aarhus.

Altogether the workshop was a great success; existing research collaboration between BRICS, other European, and US researchers were further developed and new collaboration was initiated. A few exciting new theoretical results were also obtained (—stay tuned for bestselling BRICS research reports). In the early summer of 1999 the workshop will probably be followed up by a BRICS mini-course on external-memory algorithms given by Lars Arge and Jeff Vitter.

Introduction to Evolutionary Computation

September 14–23, 1998, *Zbigniew Michalewicz*, University of North Carolina at Charlotte, USA, gave 4 introductory double lectures on evolutionary computation.

Mini-Workshop on Verification of Hybrid Systems

September 21–22, 1998, *Ernst Rüdiger Olderog*, *Josef Tapken* and *Henning Dierks* from University of Oldenburg, Germany, visited BRICS in Aalborg. Together with Kim G. Larsen and his group they organised an informal workshop on the theme of Verification of Hybrid Systems, with special emphasis on PLC's and TA's (Programmable Logic Controlers and Timed Automata). The speakers and talks were:

K. Larsen	— Overview of BRICS@Aalborg, Status of UPPAAL
A. Skou	— Case Studies in UPPAAL
H. Dierks	— PLC-automata: concepts and results
J. Tapken	— Tool support for PLC-automata
K. Larsen, G. Behrmann	— The VVS project: Verification of Large and Hierarchical systems

C. Weise	— The VHS project Verification of Hybrid systems
H. Dierks	— Model-Checking via Translation into Timed Automata
J. Tapken	— Model-Checking of DC Properties
E. R. Olderog	— Design of Real Time Systems
C. Weise, K. Larsen	— Datastructures for Real Time Verification

The 10 talks were accompanied with discussions and tool demonstrations.

Newly Appointed Researchers, Guests and PhDs

Gerth Stølting Brodal

Gerth Stølting Brodal received his PhD from the University of Aarhus in 1997, supervised by Erik Meineche Schmidt. His thesis, *Worst Case Efficient Data Structures*, considered a worst-case efficient technique for making ephemeral data structures partial persistent and the implementation of priority queues and dictionaries. From February 1997 to July 1998 he held a post-doc position in Kurt Mehlhorn's group at the Max-Planck-Institute for Computer Science in Saarbrücken, Germany. He joined BRICS in August 1998.

Jan Camenisch

Jan Camenisch received his PhD from ETH Zürich in 1998 under the supervision of Ueli Maurer. His current research interests include cryptographic proof systems, cryptographic protocols such as digital payment-systems, and group-oriented signature schemes. He joined BRICS in June 1998 as a post-doc.

Daniel Fridlender

Daniel Fridlender, originally from Argentina, received his PhD in 1997 from Göteborg University, where he was supervised by Thierry Coquand. His interests include type theory, functional programming, program correctness, constructive mathematics, and machine assisted program and proof construction. His thesis, *Higman's Lemma in Type Theory*, explores the possibilities of a particular formulation of type theory. Daniel spent last year in Stockholm working as a consultant for industry, doing formal verification of safety requirements of railways interlocking systems. He joined BRICS on September 1st.

Thiemo Krink

Thiemo Krink was trained as a computer scientist at the Universities of Erlangen and Hamburg, Germany. As an MSc student, he participated in interdisciplinary projects on object-oriented modelling of animal behaviour in collaboration with biologists at Oxford. He continued his research at the Institute of Biological Science at Aarhus, where he received his PhD degree in 1997. His current interests are focused on applications of biological concepts for adaptive and distributed computing. His one-year visit at BRICS started August 1st, 1998.

Sanjiva Prasad

Sanjiva Prasad received his PhD from SUNY, Stony Brook in 1991. His thesis, *Towards a symmetric integration of concurrent and functional programming* explored issues in the design of higher-order mobile concurrent programming languages. He worked at Odyssey Research Associates, Ithaca, from 1990–92, and then at ECRC, Munich from 1992–94 working on the Facile project, based on his thesis work. Since 1994 he has been an assistant professor at IIT Delhi. His research interests are typed programming languages for mobile, distributed computing; operational concurrency theory; and formal methods for specification and verification. He will be visiting BRICS from August 1998 to April 1999.

Vladimiro Sassone

Vladimiro Sassone received his PhD from Università di Pisa, Italy, in 1994. Since then he has been associate researcher at BRICS, assistant professor at Pisa, and lecturer at QMW College, University of London. He is now is back in Aarhus on his way to start as associate professor at Università di Catania, Italy.

His research activity focused mainly on the semantics of concurrency, one of his favourite themes therein being the study of abstract models. His interests include semantics, formal methods, type theory, logics and, generally speaking, foundations of computer science. He is currently very interested in mobility, higher order concurrency, and theories of types for processes.

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

Mario José Cáccamo
In 1995, Mario graduated in computer science from Universidad Nacional del Sur, Argentina. Last March, he got his MSc degree from State University of Campinas, Brazil. His MSc dissertation was focused on the use of finite-state automata to implement NLP. His interests include semantics of programming languages and type theory. Preliminary supervisor: Glynn Winskel.

Federico Crazzolara
Federico Crazzolara graduated from the University of Pisa, Italy. His MSc thesis, written under the guidance of Roberto Giacobazzi, is concerned with the use of quasi-metric spaces as domains for abstract interpretation and program analysis. His main interests include semantics of computation, concurrency theory, and program analysis. Preliminary supervisor: Olivier Danvy.

Stefan Dantchev
Stefan Dantchev graduated in 1994 from the Department of Mathematics and Computer Science at Sofia University, Bulgaria. His MSc thesis, written under the supervision of Valentin Brimkov, treated the computational complexity of some integer programming problems with real coefficients. Stefan worked at the Bulgarian Academy of Sciences for two years as a research assistant. His fields of interest include combinatorial algorithms and complexity theory. Preliminary supervisor: Erik Meineche Schmidt.

Martin Drozda
Martin Drozda obtained his MSc in 1995 from the Slovak University of Technology where he studied at the Department of Electrical Engineering and Information Technologies. Since 1997, he has been a PhD student at the Slovak Academy of Sciences, Institute of Control Theory and Robotics. He is visiting BRICS since April 1998 where he is staying on a scholarship awarded by the Danish Research Academy. Martin's supervisor is Mogens Nielsen. His main research interest is modelling of Discrete Event Systems.

Riko Jacob
Riko Jacob graduated in September 97 from the University of Würzburg, Germany. Before coming to Århus, he stayed for one year at the Los Alamos National Laboratory in New Mexico, USA in a traffic-simulation project called TRANSIMS. He worked as a research assistant on routing models and algorithms. His areas of interest are complexity theory, (graph and approximation) algorithms, and combinatorial optimisation.

Oliver Möller
Oliver Möller is one of the fresh PhD students at BRICS who started this September. He completed his diploma in Ulm, Germany, after working some weeks at the SRI. Topics of interest are computational logic and automated deduction, though this is not completely fixed. Current philosophy: You never can tell, unless something told you. His supervisor is Michael I. Schwartzbach.

Anders Møller
Anders has studied four years at the Department of Computer Science, University of Aarhus and spent two months at AT&T Labs Research. He is currently working on the MONA project, the BigWig project, and a project in collaboration with AT&T. Main interests include programming languages, logic and verification. Supervisor: Michael I. Schwartzbach.

Morten Rhiger
Morten Rhiger graduated from the University of Aarhus in January 1998 after which he spent five months at Hanyang University, Seoul, South Korea. His interests are in the theory of pro-

gramming languages, most notably the fields of program transformations, analyses and optimisations, semantics and implementations. Preliminary supervisor: Oliver Danvy

Frank D. Valencia
Frank D. Valencia is a PhD student at BRICS since August 1998. He has a BSc degree from the Pontificia Universidad Javeriana Cali, Colombia. Frank Valencia has published works on calculus for Concurrent Constraint Objects and Constraint Satisfaction Problems (CSP). He has been a member of research team AVISPA since 1995. AVISPA is supported in part by the Colombian research funding agency (COLCIENCIAS). The aim of the group is to develop models for an integration of Object Oriented and Concurrent Constraint Programming into a Visual Language, so as to have a programming environment sustained in a rich semantics that eases the task of developing computer music application. Frank Valencia hasn't settled on a specific main area of research yet but he is mainly interested in semantics of computation. His current advisor is Mogens Nielsen.

Dissertation Abstracts

Reasoning about Reactive Systems

by Kim Sunesen

The main concern of this thesis is the formal reasoning about reactive systems, that is, systems that repeatedly act and react in interaction with their environment without necessarily terminating. When describing such systems the focus is not on what is computed but rather on the interaction capabilities over time. Moreover, reactive systems are usually highly concurrent, typically spatially distributed, and often nondeterministic. Such systems include telecommunication protocols, telephone switches, air-traffic controllers, circuits, and many more. The goal of formal reasoning is to achieve systems with provably correct behaviour. The task of formal reasoning is to specify systems and properties of systems as mathematical objects and to supply methodologies and techniques supporting formal proofs of properties of these. Numerous semantic formalisms such as synchronisation trees, event structures, transition systems, temporal logics, Petri nets, and process algebras, to mention a few, have been proposed for the specification of reactive systems. In particular, formalisms vary in the sort of reasoning methodologies they support and encourage. Some methods have little practical pertinence, others have more. Some methods are decidable, others are not. Hence, numerous methods for reasoning about systems have been proposed; ranging from manual methods for the analysis of the most simple isolated aspects of systems to automatic methods for the synthesis of complex systems from succinct logical specifications.

In this thesis, we first consider the automated verification of safety properties of finite systems. We propose a practical framework for integrating the behavioural reasoning about distributed reactive systems with model-checking methods. We devise a small self-contained theory of distributed reactive systems including standard concepts like implementation, abstraction, and proof methods for compositional reasoning. The proof methods are based on trace abstractions that relate the behaviours of the program with the specification. Our main goal is to show that the methods are useful in practice. Hence, the use of the proof methods must be supported by a decision procedure which will answer questions about the system, such as "Does trace abstraction R show that program P implements S?" and "Do the trace abstractions between the subsystems combine to a trace abstraction between the compound systems?" Therefore, we show that trace abstractions and the proof methods can be expressed in a decidable Monadic Second-Order Logic (M2L) on words. Trace abstractions offer an alternative to refinement mappings when working with behavioural specifications, and we show that trace abstraction can aid in encompassing combinatorial blow-ups and in performing non-trivial decompositional reasoning. To demonstrate the practical pertinence of the approach, we give a self-contained, introductory account of the method applied to an RPC-memory specification problem proposed by Broy and Lamport. The purely behavioural descriptions which we formulate from the informal specifications are written in the high-level symbolic language FIDO, a syntactic extension of M2L. Our solution involves FIDO-formulas more than 10 pages long. They are translated into M2L-formulas of length more than 100 pages which are decided automatically within minutes. Hence, our work shows that complex behaviours of reactive systems can be formulated and reasoned about without explicit state-based programming, and moreover that within FIDO, temporal properties can be stated succinctly while enjoying automated analysis and verification.

Next, we consider the theoretical borderline of decidability of behavioural equivalences for infinite-state systems. We provide a systematic study of the decidability of non-interleaving linear-time behavioural equivalences for infinite-state systems defined by CCS and TCSP style process description languages. We compare standard language equivalence with two generalisations based on the predominant approaches for capturing non-interleaving behaviour: pomsets representing global causal dependency, and locality representing spatial distribution of events. Beginning with the process calculus of Basic Parallel Processes (BPP) obtained as a minimal concurrent extension of finite processes, we systematically investigate extensions towards full CCS and TCSP. The highlights are as follows. For BPP, the two notions of non-interleaving equivalences coincide, and we show that they are decidable, contrasting a result by Hirshfeld that standard interleaving language equivalence is undecidable. Also, for finite-state systems non-interleaving equivalences are computationally in general at least as hard as interleaving equivalences, whereas the result shows that when moving to infinite-state systems, this situation can change dramatically. We examine subclasses obtained by adding different means for communication, and discover a significant difference between the two non-interleaving equivalences. We show that for a non-trivial class of processes between BPP and TCSP not only are the two equivalences different, but one (locality) is decidable whereas the other (pomset) is not. Hence, the result shows that whether a non-interleaving equivalence is based on global causal dependency between events or whether it is based on spatial distribution of events can have an impact on decidability. It is well-known that TCSP is Turing powerful even without the renaming and hiding combinators. We show that if either renaming or hiding is added to the already mentioned class of processes between BPP and TCSP, then also the locality based equivalence becomes undecidable. Furthermore, we investigate tau-forgetting versions of the two non-interleaving equivalences, and show that for BPP they are decidable. These results are to the best of our knowledge the first examples of natural τ-forgetting behavioural equivalence which are decidable for the full class of BPP processes.

Finally, we address the issue of synthesising distributed systems—modelled as elementary net systems—from purely sequential behaviours represented by synchronisation trees. Based on the notion of regions, Ehrenfeucht and Rozenberg have characterised the transition systems that correspond to the behaviour of elementary net systems. Building upon their results, we characterise the synchronisation trees that correspond to the behaviour of active elementary net systems, that is, those in which each condition can always cease to hold. Moreover, we show that the identified class of synchronisation trees is definable in a monadic second order logic over infinite trees. Hence, our work provides a theoretical foundation for smoothly combining techniques for the synthesis of nets from transition systems with the synthesis of synchronisation trees from logical specifications. In particular, we discuss how this leads to an automata theoretic approach to the synthesis of elementary net systems which combines with standard automata based decision procedures. In working out our main results, we show a number of fundamental relationships between regions, zig-zag morphisms and bisimulation which might also be of independent interest.

New in the BRICS Report Series, 1998

ISSN 0909-0878

22 Gian Luca Cattani, John Power, and Glynn Winskel. *A Categorical Axiomatics for Bisimulation*. September 1998. ii+21 pp. Appears in Sangiorgi and de Simone, editors, *Concurrency Theory: 9th International Conference*, CONCUR '98 Proceedings, LNCS 1466, 1998, pages 581–596.

21 John Power, Gian Luca Cattani, and Glynn Winskel. *A Representation Result for Free Cocompletions*. September 1998. 16 pp.

20 Søren Riis and Meera Sitharam. *Uniformly Generated Submodules of Permutation Modules*. September 1998. 35 pp.

19 Søren Riis and Meera Sitharam. *Generating Hard Tautologies Using Predicate Logic and the Symmetric Group*. September 1998. 13 pp.

18 Ulrich Kohlenbach. *Things that can and things that can't be done in PRA*. September 1998. 24 pp.

17 Roberto Bruni, José Meseguer, Ugo Montanari, and Vladimiro Sassone. *A Comparison of Petri Net Semantics under the Collective Token Philosophy*. September 1998. 20 pp. To appear in *4th Asian Computing Science Conference*, ASIAN '98 Proceedings, LNCS, 1998.

16 Stephen Alstrup, Thore Husfeldt, and Theis Rauhe. *Marked Ancestor Problems*. September 1998.

15 Jung-taek Kim, Kwangkeun Yi, and Olivier Danvy. *Assessing the Overhead of ML Exceptions by Selective CPS Transformation*. September 1998. 31 pp. To appear in the proceedings of the *1998 ACM SIGPLAN Workshop on ML*, Baltimore, Maryland, September 26, 1998.

14 Sandeep Sen. *The Hardness of Speeding-up Knapsack*. August 1998. 6 pp.

13 Olivier Danvy and Morten Rhiger. *Compiling Actions by Partial Evaluation, Revisited*. June 1998. 25 pp.

12 Olivier Danvy. *Functional Unparsing*. May 1998. 7 pp. This report supersedes the earlier report BRICS RS-98-5. Extended version of an article to appear in *Journal of Functional Programming*.

11 Gudmund Skovbjerg Frandsen, Johan P. Hansen, and Peter Bro Miltersen. *Lower Bounds for Dynamic Algebraic Problems*. May 1998. 30 pp.

10 Jakob Pagter and Theis Rauhe. *Optimal Time-Space Trade-Offs for Sorting*. May 1998. 12 pp.

9 Zhe Yang. *Encoding Types in ML-like Languages (Preliminary Version)*. April 1998. 32 pp.

8 P. S. Thiagarajan and Jesper G. Henriksen. *Distributed Versions of Linear Time Temporal Logic: A Trace Perspective*. April 1998. 49 pp. To appear in *3rd Advanced Course on Petri Nets*, ACPN '96 Proceedings, LNCS, 1998.

7 Stephen Alstrup, Thore Husfeldt, and Theis Rauhe. *Marked Ancestor Problems (Preliminary Version)*. April 1998. 36 pp.

6 Kim Sunesen. *Further Results on Partial Order Equivalences on Infinite Systems*. March 1998. 48 pp.

5 Olivier Danvy. *Formatting Strings in ML*. March 1998. 3 pp. This report is superseded by the later report BRICS RS-98-12.

New in the BRICS Notes Series, 1998

ISSN 0909-3206

7 John Power. *2-Categories*. August 1998. 18 pp.

6 Carsten Butz, Ulrich Kohlenbach, Søren Riis, and Glynn Winskel, editors. *Abstracts of the Workshop on Proof Theory and Complexity, PTAC '98*, (Aarhus, Denmark, August 3–7, 1998), July 1998. vi+16 pp.

5 Hans Hüttel and Uwe Nestmann, editors. *Proceedings of the Workshop on Semantics of Objects as Processes, SOAP '98*, (Aalborg, Denmark, July 18, 1998), June 1998. 50 pp.

4 Tiziana Margaria and Bernhard Steffen, editors. *Proceedings of the International Workshop on Software Tools for Technology Transfer, STTT '98*, (Aalborg, Denmark, July 12–13, 1998), June 1998. 86 pp.

3 Nils Klarlund and Anders Møller. MONA *Version 1.2 — User Manual*. June 1998. 60 pp.

2 Peter D. Mosses and Uffe H. Engberg, editors. *Proceedings of the Workshop on Applicability of Formal Methods, AFM '98*, (Aarhus, Denmark, June 2, 1998), June 1998. 94 pp.

1 Olivier Danvy and Peter Dybjer, editors. *Preliminary Proceedings of the 1998 APPSEM Workshop on Normalization by Evaluation, NBE '98*, (Gothenburg, Sweden, May 8–9, 1998), May 1998.

BRICS Lecture Series, 1998

ISSN 1395-2048

1 Ulrich Kohlenbach. *Proof Interpretations*. June 1998.

Abstract

These lecture notes are a polished version of notes from a BRICS PhD course given in the spring term 1998.

Their purpose is to give an introduction to two major proof theoretic techniques: functional interpretation and (modified) realizability. We focus on the possible use of these methods to extract programs, bounds and other effective data from given proofs.

Both methods are developed in the framework of intuitionistic arithmetic in higher types.

We also discuss applications to systems based on classical logic. We show that the combination of functional interpretation with the so-called negative translation, which allows to embed various classical theories into their intuitionistic counterparts, can be used to unwind non-constructive proofs.

Instead of combining functional interpretation with negative translation one can also use in some circumstances a combination of modified realizability with negative translation if one inserts the so-called A-translation (due to H. Friedman) as an intermediate step.

Contents

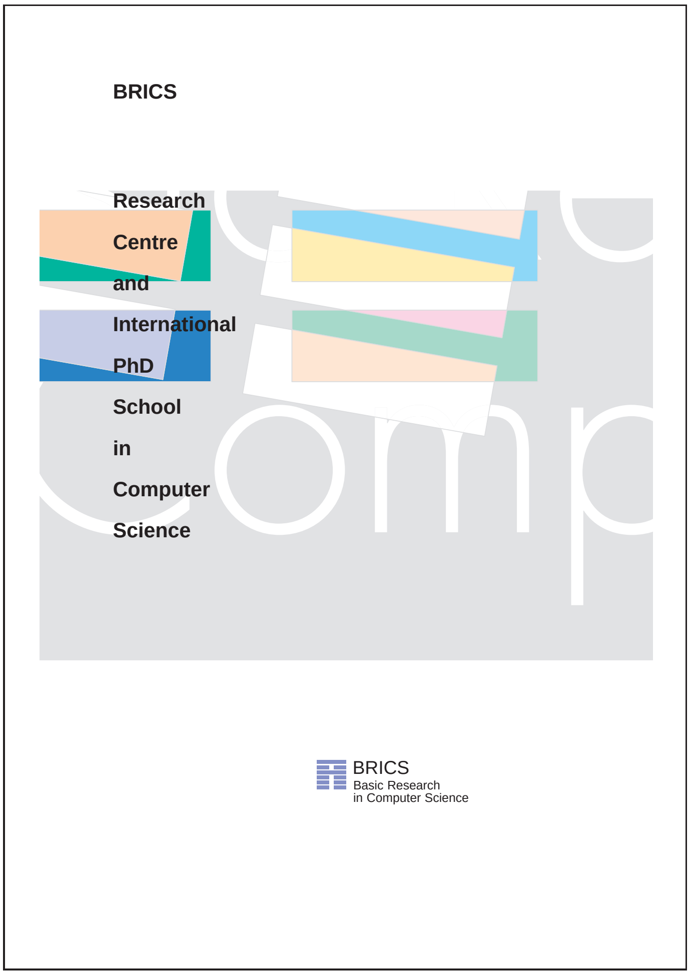
News

Folder with BRICS Profile

In June 1998 BRICS issued an 8 pages full colour folder containing information on BRICS and its PhD school in particular.

The contents is

- Staff and Management
- General description of the Research Centre and the PhD School
- PhD Studies
- PhD Admission
- Co-operation and Activities
- Environment



BRICS

Research Centre and International PhD School in Computer Science

BRICS
Basic Research
in Computer Science

Figure 15: The new BRICS folder.

Hardcopies can be obtained by contacting BRICS at the address on the back side of this newsletter. PDF versions are available at www.brics.dk/IM/98/Profile/.

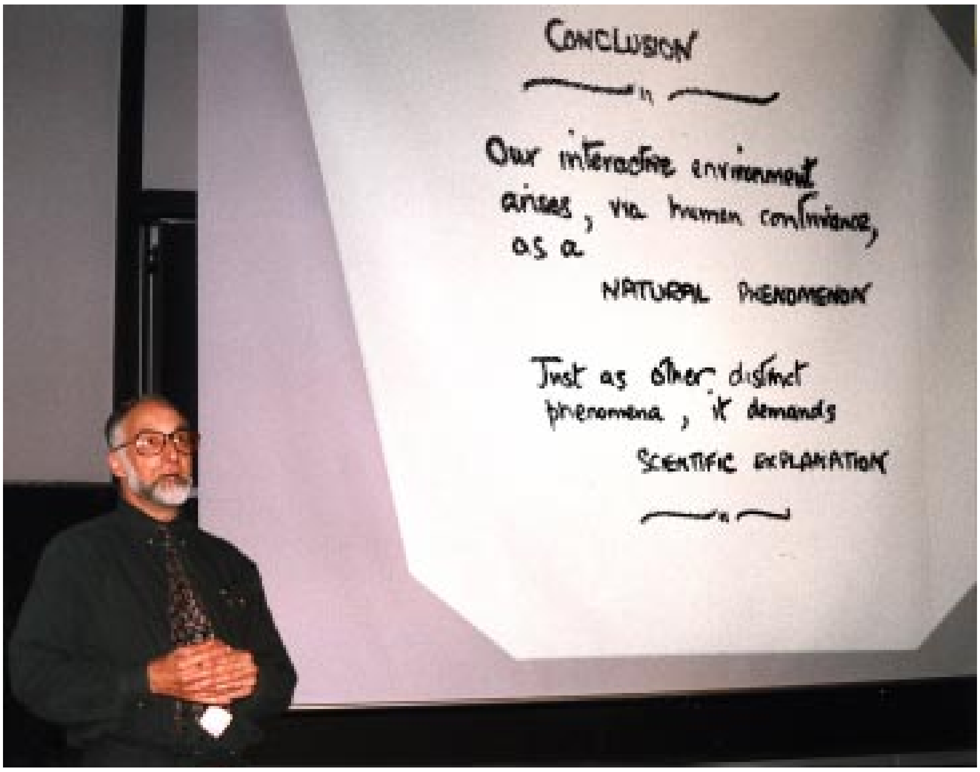
Professor Robin Milner Honorary Doctorate

The University of Aarhus has conferred its first honorary doctorate in computer science. In connection with the University's 70th Anniversary on September 11 this year, honorary doctorates for each of the five faculties were conferred, and for The Faculty of Science, the choice fell on Professor *Arthur John Robin Gorell Milner* from the Computer Laboratory at Cambridge University, England. And we could not have wished for a better choice!

First and foremost, Robin Milner is a highly respected and more than worthy representative for the field of computer science, well known for his innovative ideas and achievements in several different subjects. His contributions range from theory of programming, semantics, types, concurrency, logic and automated theorem proving, and his breakthrough ideas have started entire research areas. Milner has been honoured with several scientific awards, including the Turing award in 1992, considered the most prestigious in computer science.

Secondly, Milner and University of Aarhus have enjoyed a long-standing friendship, dating back to 1979, when Milner was a guest professor in Aarhus. During this period, Milner wrote his pioneering book on CCS, based on a graduate course at the Department of Computer Science.

The event was celebrated in different ways. On September 8, *Vladimiro Sassone* hosted a seminar, *Robin Milner—a Pioneer in Computer Science*, during which some of Milner's most important contributions to computer science were presented by:



CONCLUSION

Our interactive environment arises, via human connivance, as a NATURAL PHENOMENON

Just as other distinct phenomena, it demands SCIENTIFIC EXPLANATION

Figure 14: Robin Milner concluding his talk: *Computing and Communication—What's the Difference?*

Glynn Winskel — Contributions to Full Abstraction,
Olivier Danvy — ML and its Type System,
Paola Quaglia — Mobile Computing and the π-Calculus,

respectively.

On September 10 Milner himself gave a lecture, with the title *Computing and Communication—What's the Difference?*. The lecture and the subsequent reception was extremely well-attended, and, as always, Milner gave an inspiring and thought-provoking lecture, emphasising the scientific foundations of computer science, and, in particular, the challenges to be met by research as information technology moves towards *global computation*.

Through the years, many of us have been inspired by Robin's thoughts and views on computer science, directly or indirectly. Computer Science at the University of Aarhus is greatly indebted to Robin for many things—and proud to have him as our first honorary doctor.

<bigwig>

by Michael I. Schwartzbach

Interactive web services are offered by seemingly everyone these days, including your bank, public transportation services, news agencies, and in fact most larger businesses and organisations.

A few years ago one could establish a respectable "net-presence" by simply publishing a snazzy homepage with attractive graphics and some informative text. Starting with larger organisations this trend migrated downwards fueled by the advent of web-authoring tools and affordable web-hosting services. Now, a fancy homepage is within reach of even the most modest of budgets.

But a homepage that just passively displays information actually makes very little use of the capabilities of the web. Larger organisations have gone further by incorporating business transactions into their homepages. On the web you can access your bank accounts, buy train tickets, subscribe to customised news bulletins, and much more.

One would expect that this trend should similarly migrate downwards to smaller organisations and even to dedicated individuals. But such a development is likely to come to a grinding halt, since interactive web services are much harder to produce. They involve a host of technologies like HTML-forms, CGI-scripts, Javascript, Java, and plugins, and they must solve hard-core computer science problems such as concurrency control, cryptology, and database access.

Today, highly specialised programmers earn exorbitant salaries by constructing interactive web services. So did HTML-designers a few years ago, but they became less essential with the availability of graphical point-and-click HTML-editors that made everybody an instant web-author. It is unlikely, however, that original interactive web services can be produced by similar means, since they involve essential aspects of programming.

The <bigwig> project aims to make the production of original interactive web services as easy as simple programming. This will bring the technology within reach of smaller organisations and dedicated individuals. Anyone with even rudimentary programming skills should be able to construct simple services using the <bigwig> tool, which also scales to the production of quite sophisticated and professional services.

The basic concept is the <bigwig> programming language which allows the specification of an entire interactive web service in a single coherent formalism that is then compiled into a conglomerate of lower-level technologies. The <bigwig> compiler will potentially use all existing web-technologies as target code and automatically handle their intricate connections.

The <bigwig> Project

The <bigwig> project is an intellectual descendant of the Mawl project from Lucent Bell Labs with whom we continue to have an informal collaboration. Mawl introduced the fundamental ideas as early as 1995 and seemed to offer a useful tool at the right time, but even so it failed to gain popular acceptance. We believe a significant reason for this is that it simply did not solve enough of the hard problems that are involved in interactive web services.

The <bigwig> project is a completely new design and implementation of a similar tool with vastly expanded ambitions. A toy version of the proposed language, called WIG, was introduced as the compiler project in a Fall ’97 compiler course. Simultaneously, we outlined a design for the real language. In the Spring ’98 term some 25 compiler-graduates enrolled in the course “WIG Projects” where they designed and implemented eight different extensions of the basic WIG language, each focusing on different aspects. The project groups were all very successful and produced a wealth of good ideas, clever designs, and hard-earned experiences.

On this basis BRICS has formed the <bigwig> project which will design, implement, evaluate, and distribute a combined tool. We have made a complete redesign and are rewriting all the code from scratch (“make one to throw away” is a good principle). A version 0.9 will be available in the beginning of October 1998 for (internal) evaluation purposes. Extensive web-based documentation will be produced during the fall. The project is scheduled to deliver a version 1.0 of the <bigwig> tool in June 1999. This will be freely available in an open source distribution for both UNIX and WinNT.

The project team consists of myself, one full-time PhD-student, one part-time PhD-student, four MSc-students, three permanent student programmers, and a varying number of temporary student programmers and volunteers. Visit our homepage at www.brics.dk/bigwig to see how we are doing.

Figure 16: BigWig programmer *Claus Brabrand* demonstrating a BigWig Service (a chat room) and the underlying source code.

Domain-Specific Languages

The <bigwig> language is also an exercise in domain-specific language design, which is an emerging trend in software engineering. The idea is to express the analysis of a particular problem domain through the design of a programming language tailored to solving problems within that domain. There are many established examples of domain-specific languages, such as LaTeX, flex, and yacc. The novelty is to use such techniques for solving traditional software engineering task, where one would previously construct some collection of (class) libraries within a general-purpose language.

There are many advantages to a domain-specific language. A superficial one is nicer syntax, in that one is not restricted to a fixed notation for invoking library routines. A much deeper advantage is that the compiler may exploit domain-specific knowledge for analysis and optimisations. The disadvantages of domain-specific languages are equally clear. First of all, they are presumably more expensive to develop, even though that may gradually change. Secondly, they introduce new syntax to learn and remember.

The <bigwig> language is really a collection of tiny domain-specific languages focusing on different aspects of interactive web services. To minimise the syntactic burdens, these contributing languages are held together by a C-like skeleton language. Thus, <bigwig> has the look and feel of C-programs with special data- and control-structures.

The <bigwig> Design

A service consists of some global data and a number of named sessions. Global data includes database relations, HTML documents, and ordinary values. Clients around the web may invoke an arbitrary numbers of threads of each session kind. Thus, a web service is a highly dynamic and concurrent system. Each thread executes sequentially until termination, interrupted by interaction with its client.

Global data is accessible from all threads, but may be protected by the programmer in many ways. Local data is declared within the scope of a session and is allocated for each thread. In between these levels, it is possible to declare user data which is allocated for each userid. Each client is assigned a unique userid, which is stored in a browser cookie for future visits. Any thread may access the relevant user data by assuming the appropriate userid. The archetypical use of this mechanism is to implement a shopping basket for web customers, but it has many other applications as well. All kinds of data may be declared for all available data types.

A service executes a dynamically varying number of threads. To provide a means of controlling the concurrent behaviour, a thread may synchronise with a central controller that enforces the global behaviour to conform to a regular language accepted by a finite-state automaton. This is a very general control mechanism that may be specialised to all known synchronisation primitives. The controlling automaton is not given directly, but is computed (by the MONA system) from a collection of individual concurrency constraints phrased in first-order logic. Extensions with counters and negated alphabet symbols add expressiveness beyond regular languages.

A thread communicates with its client by displaying a document and receiving values that are entered in HTML form input fields. When a form is submitted, the client impatiently awaits an answer. If this is not forthcoming within 8 seconds, the system automatically displays a temporary message which is redisplayed every 5 seconds until the answer is shown. The contents of this message may be continually changed by the service.

HTML documents are first-class values that may be computed and stored in variables. A document may contain named gaps that are placeholders for either HTML fragments or attributes in tags. Such gaps may at runtime be plugged with concrete values. Since those values may themselves contain further gaps, this is a highly dynamic mechanism for building documents. The documents are represented in a very compressed format, and the plug operations takes constant time only. A flow-sensitive type checker ensures that documents are used in a consistent manner.

A session can browse other sites or services. This gives back raw HTML documents that possibly need some analysis afterwards. For this purpose, a pattern match primitive allows an HTML value with gaps to be used as a pattern for cutting out relevant parts.

A standard service executes with hardly any security. Higher levels of security may be requested, such that all communications are digitally signed or encrypted using using 512 bit RSA and DES3 (kindly provided by Cryptomathic). The required protocols are implemented using a combination of Java, Javascript, and native plugins.

The familiar struct and array datastructures are replaced with tuples and relations which allow for a simple construction of small relational databases. These are efficiently implemented and should be sufficient for databases no bigger than a few MBs (of which there are quite a lot). A relation may be declared to be external, which will automatically handle the connection to some external server. An external relation is accessed with (a subset of) the syntax for internal relations, which is then translated into SQL.

An important mechanism for gluing these components together is a fully general hygienic macro mechanism that allows `<bigwig>` programmers to extend the language by adding arbitrary new productions to it grammar. All nonterminals are potential arguments and result types for such macros that, unlike C-front macros, are soundly implemented with full alpha-conversions. Also, error messages remain sensible, since they are threaded back through macro expansion. This allows the definition of Very Domain-Specific Languages that contain specialised constructions for building chat rooms, shopping centers, and much more. Macros are also used to wrap concurrency constraints and other primitives in layers of user-friendly syntax.

Implementation Status

Version 0.9 of `<bigwig>` will be available for internal evaluation in the beginning of October. Most features are implemented fully, so the tool is already quite usable. If you want to try it out, then contact us for more information. The documentation is very rough as yet, but this has a high priority in the next few months. We currently support all kinds of UNIX, but will start porting the system to WinNT next spring.

Continuation of Algorithms in Quantum Information Processing, AQIP

by Ivan B. Damgård

In January 1998, BRICS organised an event we called the Algorithms in Quantum Information Processing (AQIP) workshop. This was part of the 97 BRICS theme which was algorithms in general. AQIP was a new type of event in this field, in that it seems to have been the first major workshop that focused on the computer science and algorithmic aspects of the area—in contrast to other events which have been as much physics conferences as computer science ones. Maybe it was more luck than anything else, but this seemed to be the right idea at the right time: it was surprisingly easy to gather an impressive list of invited speakers, and the attendance by far exceeded our expectations (details on AQIP '98 can still be found at the BRICS web site). It says something about the intensity of the event that the conference concluded with a more or less improvised talk, showing two results that were respectively 2 weeks and 2 days old!

All of us involved in AQIP '98 were happy about the way it went, so we were of course pleased to find out that many other people in the field also liked the idea. In fact there was general agreement that there was a need for a new workshop of the same type. As a result of these discussions, there will be an AQIP '99, which will take place in January 1999 at DePaul University in Chicago. Andre Berthiaume, who many of us will remember from a great mini course he gave at BRICS in 96, is the program chair, and more details can be found at www.cs.depaul.edu/AQIP99.

Of course, us here at BRICS cannot help feeling that the baby that was born here in 1998 is now growing up and seems to be strong and healthy. We wish AQIP lots of luck in the future!

IFIP WG1.3

IFIP WG1.3 is a working group on Foundations of System Specification under the IFIP Technical Committee on Foundations of Computer Science, TC1. The declared *aims* of WG1.3 are to support and promote the systematic development of the fundamental mathematical theory of systems specification, and to investigate the theory of formal models for systems specification, development, transformation and verification. The *scope* is theoretical aspects of the specification and development of computing systems that are based on algebraic and logical concepts and can be studied systematically within a theory of systems specification.

See the IFIP WG1.3 web, IFIP-WG1.3 www.brics.dk/~pdm/IFIP-WG1.3/, for further details. Peter D. Mosses was recently appointed Chairman of WG1.3.

CASL

CoFI, The Common Framework Initiative for algebraic specification and development, has now completed the design of CASL, intended as a *common* language for formal specification of functional requirements and modular software design. CASL is to support interoperability of prototyping and verification tools, and it should subsume many previous algebraic specification languages. It caters for partial functions, subsorts, first-order logic axioms, structured and architectural specifications, and distributed libraries. Higher-order features and other advanced constructs are to be included in CASL extensions. CASL is a central element of the proposed Common Framework; other elements include tools, methodology, and support for specification and development using particular software paradigms.

See the CoFI web pages, www.brics.dk/Projects/CoFI/, for further details. Peter D. Mosses has been the overall coordinator of CoFI since its start in 1995.

Calendar of Events

Date	Event
Late Oct ’98	Mini-course: Which π-Calculus are we Talking About?
9–17 Nov ’98	Mini-course on Biological Concepts for Adaptive and Distributed Algorithms
Late Nov ’98	Mini-course on A Formal Calculus for Distributed Agents
Jan ’99	Mini-course on Mobile Agents in Practise
Jan / Feb ’99	Mini-course on Modelling and Verifying Authentication Protocols
May ’99	Summer School in Semantics

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:

`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