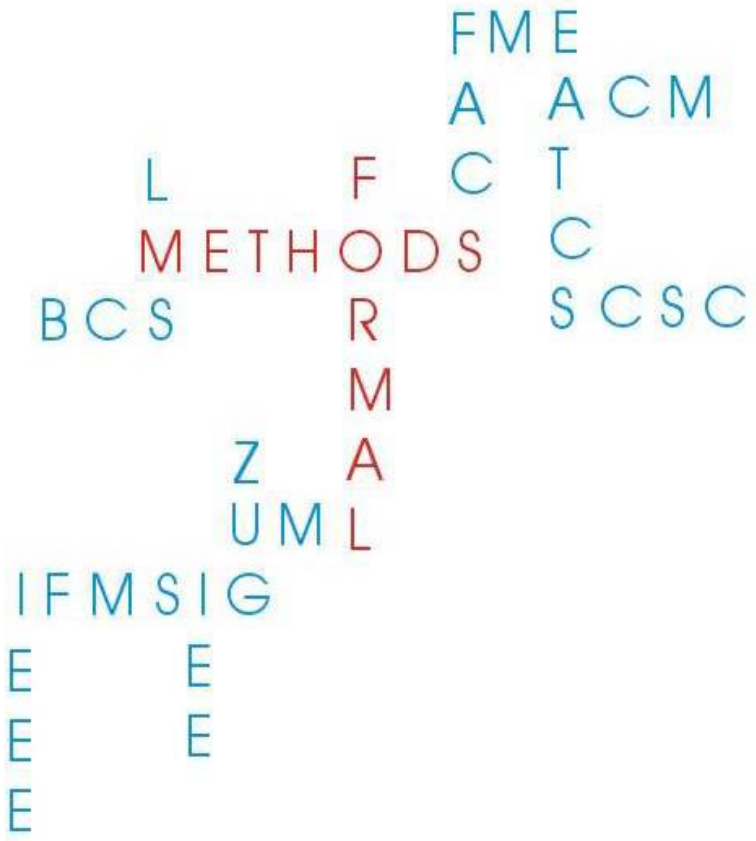
FACS FACTS



About FACS FACTS

FACS FACTS (ISSN: 0950-1231) is the newsletter of the BCS Specialist Group on Formal Aspects of Computing Science (FACS). *FACS FACTS* is distributed in electronic form to all FACS members.

Submissions to FACS FACTS are always welcome. Please visit the newsletter area of the BCS FACS website (for further details see http://www.bcs.org/category/12461).

Back issues of *FACS FACTS* are available for download from: http://www.bcs.org/content/conWebDoc/33135

The FACS FACTS Team

Contributors to this Issue

Jonathan Bowen, Eerke Boiten, Richard Bornat, Tim Denvir, Margaret West.

BCS-FACS websites

BCS: http://www.bcs-facs.org

LinkedIn: http://www.linkedin.com/groups?gid=2427579

Facebook: http://www.facebook.com/pages/BCS-FACS/120243984688255

Wikipedia: http://en.wikipedia.org/wiki/BCS-FACS

If you have any questions about BCS-FACS, please send these to Paul Boca: paul.boca@gmail.com

Editorial

Welcome to Issue 2016-1 of *FACS FACTS*.

We note with sadness the death of Professor Barry Cooper of Leeds University on 26th October 2015. Although primarily a mathematician, Barry Cooper will have become well known to computer scientists with his extremely energetic championing of the Alan Turing Centenary Year (2012) over a period of some five years. Indeed, Barry's own area of academic research started from the structure theory of Turing degrees, and in 2013 his edited volume, *Alan Turing: His Work and Impact*, with Jan van Leeuwen, won an Association of American Publishers award. So one might say that Barry Cooper's work was around the fuzzy borders between mathematics and computer science. An obituary for him can be found on the web site of the LMS, of which Barry was a member from 1974: http://newsletter.lms.ac.uk/barry-cooper-1943-2015/

The FACS AGM was held in the Headquarters of the BCS in London on 7th December 2015. The Chair's report to the AGM by Jonathan Bowen is reproduced below. The AGM was followed by the Peter Landin Annual Semantics Seminar, given by Jan Peleska, on Semantic Families for Cyber-Physical Systems. A short report of his talk can be found herein.

This issue also contains reports on other events. Jonathan Bowen reports on the ProCos 2015 Workshop. Eerke Boiten writes on the 2105 Refinement Workshop. Margaret West reports on the FACS meeting held on 16th September given by Ian Hayes from the University of Queensland, currently visiting the University of Newcastle: Separating the concerns of rely and guarantee in reasoning about concurrent programs. Finally, Richard Bornat reports on the joint LMS-FACS meeting: The Mathematics of Program Construction given by Roland Backhouse.

We note some forthcoming events: a FACS evening seminar on 17th May, FM 2016 and iFM 2016.

We announce two books on Carl Adam Petri and Petri Nets, by Einar Smith and Wolfgang Reisig.

Lastly, we offer some links to recorded seminars by Leslie Lamport and Donald Knuth which may be of interest to FACS readers.

Most FACS seminars take place in the offices of the British Computer Society in the Davidson Building, Southampton Street. These excellent facilities are conveniently situated in Central London close to Covent Garden and we would like to thank the BCS for making these available to us.

BCS-FACS 2015 AGM

BCS London Offices, 5 Southampton Street, London WC2E 7HA

Monday 7th December 2015

Chair's Report

First let me apologise for not being present at the BCS-FACS AGM, due to a work commitment abroad. Thank you to FACS treasurer (and treasure!) Prof. Jawed Siddiqi for presenting this report in my absence.

During 9-10 March 2015, we held a major two-day international ProCoS Workshop on *Provably Correct Systems* at the BCS London offices with sponsorship from LERO - the Irish Software Research Centre. This was well attended by delegates and speakers from four continents, including Prof. Sir Tony Hoare, Prof. Dines Bjørner (from Denmark), and others who were members of or influenced by the ESPRIT ProCoS projects of the early 1990s, around 25 years ago. The event was co-chaired by me, Jonathan Bowen, together with Prof. Mike Hinchey (University of Limerick, Ireland, and FACS committee member) and Prof. Dr Ernst-Rüdiger Olderog (University of Oldenburg, Germany). A post-proceedings is planned, to be published by Springer.

The group also supported the BCS-FACS Refinement Workshop on 22 June 2015, co-located with the FM 2015 Symposium in Oslo, Norway. Thank you to FACS committee member Eerke Boiten for his involvement in organizing this event. On 16 September 2015, Prof Ian Hayes of the University of Queensland in Australia, gave a FACS evening seminar at the BCS London offices on "Separating the Concerns of Rely and Guarantee in Reasoning about Concurrent Programs", during his visit to Newcastle University. Thank you to Prof. Cliff Jones for suggesting and chairing this event. On 3 November 2015, Prof. Roland Backhouse of the University of Nottingham presented a joint BCS-FACS/LMS evening seminar on "The Mathematics of Program Construction" at

the London Mathematical Society headquarters in Russell Square. Thank you to FACS committee member John Cooke for organizing this event as usual.

Finally, I give a special thank you to FACS secretary Paul Boca for yet again organizing the Annual Peter Landin Semantics Seminar later today. This is to be delivered by Prof. Jan Peleska of the University of Bremen (Germany) on "Semantic Families for Cyber Physical Systems". Thanks also go to FACS committee member Prof. John Fitzgerald and Formal Methods Europe for sponsorship of the event in assisting with European travel costs. We continue our long association with Formal Methods Europe through an FME meeting at the BCS London offices during the afternoon, following this AGM.

BCS-FACS depends on members proposing events, especially evening seminars. I know that a few ideas are in the offing and can be discussed at this AGM. Currently 2016 is wide open for possible FACS events and I would encourage you to make suggestions and offer help in organizing meetings. We are entirely dependent on members volunteering in this regard, although there is good support from the BCS with an effectively free venue at the BCS London offices for FACS meetings. I as chair can also offer support and advice in organizing a meeting if you have not done one before. It is a good learning experience and you get a free dinner with the speaker for your efforts and travel expenses if you chair the meeting as well. We try to have a maximum of one meeting per month (January to June and September to October, since we normally have the joint LMS event in November and the Landin Seminar in December). I look forward to hearing your ideas and suggestions, especially if you can volunteer to organize or even give an evening seminar in 2016.

I would also like to thank FACS committee members Tim Denvir and Brian Monahan for their work on co-editing the *FACS FACTS* newsletter. I know from experience what a mammoth effort this is for little or no reward, but it is wonderful to have it as a record of FACS activities and interests. Volunteers to write reports on talks, trip reports, book reviews, short technical submissions,

or anything of potential interest to FACS members are greatly appreciated at any time. Submission of photographs (with captions!) is also encouraged.

I hope you enjoy the rest of the day. Happy Christmas to you all, apologies I cannot be with you today, and I look forward to seeing you again in 2016, hopefully at a FACS event!

Jonathan Bowen

Chair, BCS-FACS

Forthcoming Events

There is a forthcoming Formal Aspects of Computing Science (FACS) Group event:

Date	Details
17 May 2016	**Title:** *Model-Based Testing: There is Nothing More Practical than a Good Theory*; BCS FACS – evening seminar with Dr. Jan Tretmans, Senior Research Fellow, TNO - Embedded Systems Innovation, Eindhoven, NL, and Radboud University, Nijmegen, NL **Venue:** BCS, London **Details:** http://www.bcs.org/content/ConWebDoc/55737 **Abstract:** We build ever larger and more complex software systems. Systematic testing plays an important role in assessing the quality of such systems. The effort for testing, however, turns out to grow even faster than the size and complexity of the systems under test themselves. One of the promising testing technologies to detect more bugs faster and cheaper is model-based testing. Model-based testing starts with an abstract model of the system's behaviour. This model constitutes a precise and concise specification of what the system shall do, and, consequently, is a good basis for the algorithmic generation of test cases and the analysis of test results. Model-based testing enables the next step in test automation by combining automatic test generation with test execution, and providing more,

longer, and more diversified test cases with less effort.

The presentation aims at covering the chain from theoretical concepts, via algorithms and tools, to industrial applications of model-based testing. Starting point is the 'ioco'-testing theory for labelled transition systems, to which concepts from process algebra, the theory of testing equivalences, symbolic transition systems, algebraic data types, satisfaction-modulo-theories tools, and equational reasoning are added. We show how these theories have led to the development of the model-based testing tool 'TorXakis'.

On the one hand, TorXakis provides provably sound and exhaustive (in the limit) test generation from models. These models combine state-based control flow and complex data definitions, they deal with uncertainty through nondeterminism, they support compositionality by providing combinators for alternative, concurrent, sequential, exceptional, and interrupting behaviours, and they support abstraction and under-specification. On the other hand, TorXakis has shown practical usability in academia, both in research and in education, as well as in industrial applications, ranging from smart-card software to large, systems-of-systems kind of applications. So, for model-based testing there is nothing more practical than a good theory.

(See: Forthcoming Events for up-to-date information.)

Other forthcoming events:

Date	Details
7-11 November 2016	**Title:** FM 2016: 21st International Symposium on Formal Methods **Venue**: Limassol, Cyprus **Details:** http://fm2016.cs.ucy.ac.cy FM 2016 is the latest in a series of symposia organized by Formal Methods Europe, an independent association that encourages the use of, and research on, formal methods for the engineering of computer-based systems and software. The symposia have been notably successful in bringing together researchers and industrial users around a programme of original papers on research and industrial experience, workshops, tutorials, reports on tools, projects, and ongoing doctoral work.
1-3 June 2016	**Title:** iFM 2016: Integrated Formal Methods **Venue:** Reykjavik, Iceland **Details:** http://en.ru.is/ifm/
4-5 June 2016	UTP 2016: 6th International Symposium on Unifying Theories of Programming **Details:** http://utp2016.ecnu.edu.cn/

Reports of Events

FACS-FME Peter Landin Annual Semantics Seminar

Semantic Families for Cyber-Physical Systems (CPS)

7 December 2015

BCS HQ, London

Jan Peleska
(University of Bremen;
Verified Systems International GmbH)

Reported by: Tim Denvir

Abstract

In this seminar talk we discuss a potential change of paradigm in the field of semantics, with a focus on behavioural modelling formalisms applicable to cyber physical systems (CPS), systems of systems, or complex distributed, reactive systems in general. The well-established semantic models for these application domains, such as Kripke structures, labelled transition systems, or finite state machines and their denotational or axiomatic counterparts, are reviewed in the light of today's practical challenges. To name just a few of them: how do these familiar approaches cope with large numbers of replicated components, the dynamicity of system configurations, evolution of contractual behaviour, and presentation of emergent properties? From the perspective of today's distributed collaborative development and verification projects another challenge arises: how can artefacts (models, code, verification results, ...) obtained "locally" in a semantic framework specialised for a system component be translated into another framework used, for example, to model and verify emergent behaviour of the complete CPS?

The challenges and potential solutions are illustrated using examples from testing theories for and bounded model checking of CPS. It is shown how the objective to obtain bounded results (identification of finite test sequences,

verification of behaviour for a bounded number of transitions in the vicinity of a given state) facilitates the elaboration of solutions to the identified problems. Moreover, we advocate the identification of semantic families, each family well-optimised to model the behaviour of a specific class of applications, and mechanisms to navigate between different families, while being able to translate theories and verification results between families. It is pointed out that the means to set up such a collection of semantic families and navigation mechanisms have been established long ago and have matured to very powerful tools. To name two prominent examples, Goguen's and Burstall's theory of institutions (the informal term "family" used above roughly corresponds to an institution), as well as the Unifying Theories of Programming are suitable vehicles for such an undertaking.

Introductions

Jawed Siddiqi reminded us of the contributions Peter Landin had made to the study of semantics and John Fitzgerald introduced the speaker.

Talk

Jan Peleska recalled Tony Hoare's approach to formalising concurrent systems. No single formalism is adequate for modelling CPS. We need multiple formalisms, used by different teams within the development or modelling effort. The question is, how does one do reification (or proofs) in the presence of multiple formalisms?

Dynamic reconfiguration is another potential difficulty: maybe a semantics for Object Oriented systems can provide a way forward, or can we find something simpler?

Cyber-Physical Systems are typically systems of collaborating computational elements controlling physical entities. Such systems can have large numbers of replicated components; can the knowledge of this duplication lead to some optimisation in the use of V&V methods?

Jan Peleska took two examples of multiple formalisms in CPS modelling. The first was: Testing Theories and Collaborative Tool environments. The application scenario was an on-board speed controller for a train. The CPS

consists of several components. Some components are modelled by Finite State Machines (FSMs) and others are modelled by SysML state machines with Kripke semantics.

The speed controller comprises an emergency brake control with discrete input, a discrete state and discrete output, interfacing with more analogue sensors with a computer controller. Complete test suites can be defined with respect to a fault model (M, $<$, Dom), where:

- M is a reference model
- $<$ is a conformance relation
- Dom is a fault domain.

For FSMs many complete test strategies exist, for deterministic or non-deterministic, completely defined or incomplete FSMs.

The on-board main controller in this example system has large (analogue) input domains such as speed, and a discrete internal state and discrete output domains. He introduced the idea of Testing Theory Translation between different semantic domains with their conformance relations. Here the two semantic domains are FSMs and Kripke structures, with signatures Sig1 and Sig2. One creates a model map T from a sub-domain of Sig1 to Sig2 and a Test Case map T* from test cases of Sig2 to test cases of Sig1. Then a two-part Satisfaction Condition is defined: Condition 1 being that the model map is compatible with the conformance relations and Condition 2 being that the Model Map and Test Case Map preserve the Pass relationship. These Satisfaction Conditions can be usefully represented by commuting diagrams and relational composition. These constructions then led on to two theorems on the preservation of properties (namely completeness, i.e. sound and exhaustive) over Testing Theory Translation. They are:

Theorem 1:

> Suppose (T, T*) exist and fulfil the satisfaction condition. Then every complete (sound, exhaustive) testing theory established in Sig2 induces a likewise complete (sound, exhaustive) testing theory on Sig1 .

Theorem 2:

> Every complete (sound, exhaustive) FSM testing theory formalising
>
> - language equivalence or
> - language containment
>
> induces a complete (sound, exhaustive) equivalence class partition testing theory with analogous conformance relations for Kripke structures with infinite input domains, bounded non-determinism, and finite internal state and finite outputs.

The proofs of the two theorems were straightforward, that of Theorem 1 by diagram chasing. The Test Case Map corresponds to sentence translation map in Goguen and Burstall's Theory of Institutions.

These constructions and arguments are all about mapping infinite-state complex models to simpler finite ones; not all of them can.

Jan Peleska's second example comprised the verification of an additional, "emergent" property of the system. FSM I/O events can be mapped to CSP channel events. FSM parallel composition by intersection is similar to synchronous channel communication of CSP processes. CSP failure models can be represented by normalised transition graphs. Jan Peleska proposed an underpinning of this approach using He and Hoare's UTP (Unified Theories of Programming), with Galois connections.

Jan Peleska's slides can be found here:

http://www.bcs.org/upload/pdf/peleska-peter-landin-seminar-2015.pdf

BCS-FACS - ProCoS Workshop on Provably Correct Systems

Monday 9 March - Tuesday 10 March 2015

BCS, The Davidson Building, 5 Southampton Street, London WC2E 7HA

Reported by: Jonathan P. Bowen, Chair of BCS-FACS

Co-chairs:

Prof. Jonathan Bowen, Birmingham City University, UK

Prof. Mike Hinchey, LERO, University of Limerick, Republic of Ireland

Prof. Dr Ernst-Rüdiger Olderog, Carl von Ossietzky Universität Oldenburg, Germany

The years 2014 and 2015 have marked 25 years and 20 years, respectively, since the start and end of the European ESPRIT ProCoS projects on Provably Correct Systems, inspired by the CLInc project in the US. The ProCoS I/II projects [1-3] and the associated ProCoS-US initiative ran from 1989-1995, followed by the ProCoS-WG Working Group of 25 partners [4]. The projects aimed to perform research in the fundamental technical aspects of a development process for critical embedded systems, from the original capture of requirements all the way down to the computers and special purpose hardware on which the programs run. The projects were significant in their contributions to provably correct systems, and led directly to a better general understanding of the relationship between a range of theories, and how their combination can be used in the planning and development of critical software tasks. This event marked these 20th and 25th anniversaries of ProCoS to look back at its achievements and to identify key research contributing to the next generation of provably correct systems, with invited talks by leading international computer science researchers, many directly involved with the original ProCoS projects.

The ProCoS Workshop included 38 attendees and 25 talks from presenters who travelled from four continents. The event was recorded by Geoff Sharman with the help of Xiaohong Chen, a PhD student at Birmingham City University. A dinner was held on the first evening, sponsored by Lero, at which Prof. Dr Hans

Langmaack of the University of Kiel, Germany, gave an after-dinner speech. It is intended to produce a post-proceedings of papers associated with selected presentations, to be published by Springer in due course.

References

1. Dines Bjørner, C.A.R. Hoare, Jonathan P. Bowen, He Jifeng, Hans Langmaack, Ernst-Rüdiger Olderog, Ursula Martin, Victoria Stavridou, Fleming Nielson, Hanne Riis Nielson, Howard Barringer, Doug Edwards, Hans Henrik Løvengreen, Anders P. Ravn, and Hans Rischel, A ProCoS Project Description: ESPRIT BRA 3104. Bulletin of the European Association for Theoretical Computer Science (EATCS), 39:60-73, October 1989.
2. Jonathan P. Bowen, Martin Fränzle, Ernst-Rüdiger Olderog and Anders P. Ravn, Developing Correct Systems. Proc. 5th Euromicro Workshop on Real-Time Systems, Oulu, Finland, 22-24 June 1993. IEEE Computer Society Press, pages 176-187, 1993.
3. Jonathan P. Bowen, C.A.R. Hoare, Hans Langmaack, Ernst-Rüdiger Olderog and Anders P. Ravn, A ProCoS II Project Final Report: ESPRIT Basic Research project 7071. Bulletin of the European Association for Theoretical Computer Science (EATCS), 59:76-99, June 1996.
4. Jonathan P. Bowen, C.A.R. Hoare, Hans Langmaack, Ernst-Rüdiger Olderog and Anders P. Ravn, A ProCoS-WG Working Group Final Report: ESPRIT Working Group 8694. Bulletin of the European Association for Theoretical Computer Science (EATCS), 64:63-72, February 1998.

Programme

The following presentations were given by former members of the ProCoS projects and Working Group was well as those influenced by ProCoS-related research. The first day was largely by members of ProCoS and the second day mostly by those influenced by ProCoS.

Monday 9 March 2015 ("Whence")

Session 1 (Introduction) - Chair: Prof. Dr Ernst-Rüdiger Olderog, Carl von Ossietzky Universität Oldenburg, Germany

How it all Began: As seen from Denmark – Prof. Dines Bjørner, Technical University of Denmark, Denmark

Provably Correct Systems: Whence and whither? – Prof. Jonathan P. Bowen, Birmingham City University, UK

Algebraic Proof of Consistency of Operational and Verification Semantics – Prof. Sir Tony Hoare, Microsoft Research Cambridge, UK

Session 2 (Hybrid systems) – Chair: Prof. Jonathan Bowen, Birmingham City University, UK

Hybrid Systems from the ProCoS Gas Burner to Highway Traffic – Prof. Anders P. Ravn, Aalborg University, Denmark

Engineering Arithmetic Constraint Solvers for Automatic Analysis of Hybrid Discrete-continuous Systems – Prof. Dr Martin Fränzle, Carl von Ossietzky Universität Oldenburg, Germany

Hybrid Relation Calculus – Prof. Jifeng He and Prof. Huibiao Zhu, East China Normal University, Shanghai, China

Session 3 (Reasoning, Analysis & Refinement) – Chair: Prof. Mike Hinchey, LERO, University of Limerick, Republic of Ireland

Reasoning Abstractly about Concurrency – Prof. Cliff Jones, Newcastle University, UK

From ProCoS to Space and Mind-models – Prof. Dr Bettina Buth, HAW Hamburg, Germany

Refinement Algebra and Applications – Prof. Augusto Sampaio, Universidade Federal de Pernambuco, Brazil

Space for Traffic Manoeuvres – Prof. Dr Ernst-Rüdiger Olderog, Carl von Ossietzky Universität Oldenburg, Germany

Session 4 (Mechanization) – Chair: Prof. Dr Debora Weber-Wulff, Hochschule für Technik und Wirtschaft Berlin, Germany

Model Checking Duration Calculus: The DCVALID story – Dr Paritosh Pandya, Tata Institute of Fundamental Research, Mumbai, India

Automatic Verification of Infinite-state Systems – Prof. Dr Markus Müller-Olm, Westfälische Wilhelms-Universität Münster, Germany

Commercial Use of the ACL2 System – Prof. Warren Hunt, The University of Texas at Austin, USA

Managing Large Terms Representing Realistic Machine States – Prof. J Strother Moore, The University of Texas at Austin, USA

Tuesday 10 March 2015 ("Whither")

Session 1 (Assertions & Testing) – Chair: Prof. Michael R. Hansen, Technical University of Denmark, Denmark

Run-time Assertion Checking of Data- and Protocol-oriented Properties of Java Programs – Prof. Frank de Boer, CWI, Netherlands

Assertions for Hardware – Prof. Wayne Luk, Imperial College London, UK

Combining Testing and Verification – Prof. Dr Heike Wehrheim, University of Paderborn, Germany

Session 2 (Proof) – Chair: Dr Hans Rischel, Technical University of Denmark, Denmark

Proof with Event-B/Rodin – Prof. Michael Butler, University of Southampton, UK

Are We There Yet? Twenty years of industrial theorem proving with SPARK – Dr Rod Chapman, Protean Code Ltd, UK

What have we Learned about Proof? – Prof. Ursula Martin, University of Oxford, UK

Session 3 (Models & ATP) – Chair: Dr Huibiao Zhu

Model-checking Extended Linear Duration Invariants – Prof. Naijun Zhan, Institute of Software, Chinese Academy of Sciences, China (representing Prof. Zhou Chaochen)

A Model of Cyber-physical Component Systems – Prof. Zhiming Liu, Birmingham City University, UK

Advances in Connection-based Automated Theorem Proving – Prof. Dr Wolfgang Bibel, Darmstadt University of Technology, Germany and Prof. Dr Jens Otten, Potsdam University, Germany

Session 4 (Correctness) – Chair: Prof. Jim Woodcock, University of York, UK

Synthesis of Provably Correct Systems – Prof. Dr Bernd Finkbeiner, Saarland University, Germany

Linearizability and Correctness for Weak Memory Models – Prof. John Derrick, University of Sheffield, UK

Photographs

Group photograph of former ProCoS members at the ProCoS Workshop

Back row (left to right): Martin Fränzle, Hans Rischel, Michael Hansen, Hans Løvengreen, Hans Langmaack, Augusto Sampiao, Markus Müller-Olm, Paritosh Pandya

Front row (left to right): Debora Weber-Wulff, Bettina Buth, Jonathan Bowen, Ernst-Rüdiger Olderog

Audience at the ProCoS Workshop on the first day

Prof. Dr Dines Bjørner, Technical University of Denmark

Prof. Jonathan Bowen, Birmingham City University

Prof. Sir Tony Hoare, Microsoft Research Cambridge

Prof. Sir Tony Hoare and Prof. Dr Ernst-Rüdiger Olderog (co-chair)

Prof. Anders P. Ravn, Aalborg University

Prof. Dr Martin Fränzle, Carl von Ossietzky Universität Oldenburg

Audience at the ProCoS workshop during Martin Fränzle's talk

Prof. Huibiao Zhu (presenting for Prof. Jifeng He), East China Normal University

Prof. Cliff Jones, Newcastle University

Prof. Dr Bettina Buth, HAW Hamburg

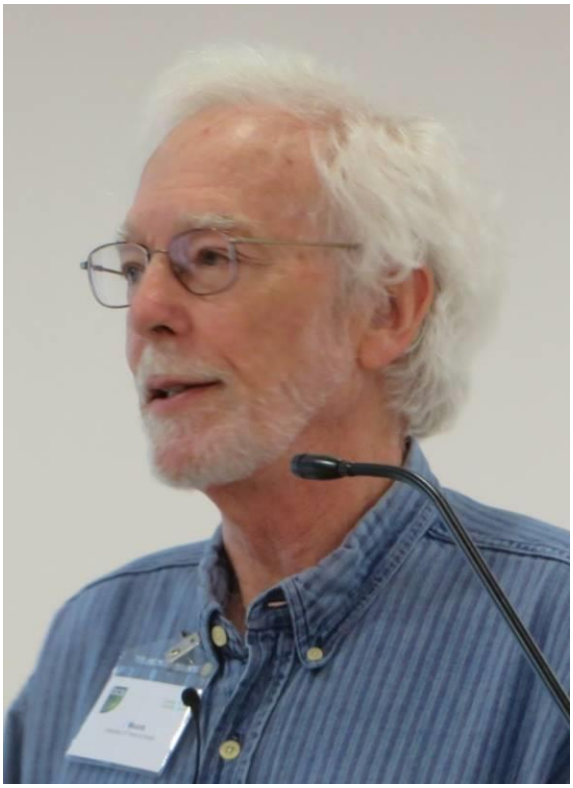
Prof. Augusto Sampaio, Universidade Federal de Pernambuco

Prof. Dr Ernst-Rüdiger Olderog, Carl von Ossietzky Universität Oldenburg

Dr Paritosh Pandya, Tata Institute of Fundamental Research

Prof. Dr Markus Müller-Olm, Westfälische Wilhelms-Universität Münster

Prof. Warren Hunt, The University of Texas at Austin



Prof. J Strother Moore, The University of Texas at Austin

The ProCoS Workshop drinks reception at the BCS offices on the evening of the first day

Geoff Sharman, Prof. Mike Hinchey (Lero), and Prof. Dr Ernst-Rüdiger Olderog at the drinks reception

The ProCoS Workshop dinner on the evening of the first day (sponsored by Lero)

The ProCoS Workshop audience during Frank de Boer's talk at the start of the second day

Prof. Frank de Boer, CWI

Prof. Wayne Luk, Imperial College London

Prof. Dr Heike Wehrheim, University of Paderborn

Prof. Michael Butler, University of Southampton

Dr Rod Chapman, Protean Code Ltd

Prof. Ursula Martin, University of Oxford

Prof. Naijun Zhan, Institute of Software, Chinese Academy of Sciences (representing Prof. Zhou Chaochen)

Prof. Zhiming Liu, Birmingham City University

Prof. Dr Jens Otten, Potsdam University

Prof. Dr Bernd Finkbeiner, Saarland University

Prof. John Derrick, University of Sheffield

Sponsored by Lero **(The Irish Software Research Centre)**

17th BCS-FACS Refinement Workshop

Monday 22 June 2015
Department of Informatics, University of Oslo
Reported by Eerke Boiten
University of Kent

The 17th BCS-FACS 2015 Refinement Workshop was held on 22 June 2015 in Oslo, as a satellite workshop of the FM conference. Some thirty attendees enjoyed the following series of both technical and more discursive talks.

"SCJ-Circus: a refinement-oriented formal notation for Safety-Critical Java" - Alvaro Miyazawa and Ana Cavalcanti.

"Denotational Semantics of Channel Mobility" - Gerard Ekembe Ngondi and Jim Woodcock.

"A Theory of Service Dependency" - Luigia Petre and Mats Neovius "Formal refinement of extended state machines" - Thomas Fayolle, Marc Frappier, Frederic Gervais and Regine Laleau.

"Program Derivation by Correctness Enhancements" - Nafi Diallo, Wided Ghardallou, Jules Desharnais and Ali Mili.

"Reversible Computing and Refinement" - Frank Zeyda, Steve Dunne and Bill Stoddart.

"Linking linearizability and contextual trace refinement" - Lindsay Groves and Brijesh Dongol.

"A logic for n-dimensional hierarchical refinement" - Alexandre Madeira, Manuel A. Martins and Luis Barbosa.

"Programming language features for refinement" - Rustan Leino and Jason Koenig.

"Big Data refinement" - Eerke Boiten.

Most talks led to lively and interesting discussions. Proceedings are due to appear in EPTCS before the end of 2015.

FACS Meeting: Separating the concerns of rely and guarantee in reasoning about concurrent programs

Ian J. Hayes
The University of Queensland, currently visiting Newcastle University

Wednesday16th September 2015
BCS Headquarters Southampton Street London

Reported by Margaret West
University of Huddersfield

The speaker briefly introduced the concepts of Hoare logic and refinement in terms of **pre** and **post** conditions **p, q** which have to be satisfied by program statement **s.** However when concurrency is involved there are problems in coping with interference of shared variables and an augmented – 5-tuple – version of the Hoare triple is then utilised involving rely **r** and guarantee **g** :

{p, r} s {g, q}

Rely **r** represents an **assumption** – about the environment of the program statement **s** and guarantee **g** represents constraints on the effects of s on the environment. An example was provided to illustrate – viz the "Sieve of Eratosthenes" which requires that all primes are identified up to some maximum value.

The next part of the talk concerned the separation of concerns of rely and guarantee. In the first place the notion of **guarantee** was developed using **weak** (aka **strict)** conjunction – where if two processes are weakly conjoined then they only succeed (and do not abort) if both succeed. **Rely** was then developed using **rely quotient** (an analogous notion to arithmetic division).

The properties of both weak conjunction and rely quotient were provided and subsequently applied to the Prime sieve. The approach developed in the talk was found to be more conducive to analysis (with nice algebraic rules) and made for simpler proofs of Laws e.g. Parallel-Introduction.

After the talk we then repaired to an eating establishment in Covent Garden where we were apparently guaranteed at least one course before the Northerners among us caught their trains from Kings Cross. The conversations between diners during the following couple of hours were then interleaved by the regular sounding of the restaurant fire alarm.

Unfortunately, due to the parallel and competing requirements of many diners, the service was slow and those of us who were relying on catching our late trains became very anxious. In the end I (at least) managed to catch mine and ended up comfortably established in my carriage after a successful and interesting evening.

The slides are available: http://www.bcs.org/upload/pdf/ihayes-160915.pdf

Photographs by Jonathan Bowen (Chair of BCS-FACS)

The coffee break before the talk
Left to right (foreground): Steve Dunne, Michael Jackson, Ian Hayes, Tony Hoare

Cliff Jones introduces the talk to an attentive audience (Tony Hoare)

Ian Hayes starts his talk on “Separating the concerns of reply and guarantee in reasoning about concurrent programs”

LMS-FACS seminar: The Mathematics of Program Construction

Professor Roland Backhouse
(University of Nottingham)
Tuesday 3rd November 2015
London Mathematical Society, De Morgan House, Russell Square, London
Reported by Richard Bornat
University of Middlesex

Roland Backhouse (Nottingham) gave a talk on **The Mathematics of Program Construction**. It was strongly in the Eindhoven tradition established by Dijkstra: programming is, or should be, a matter of calculation from a mathematical statement of purpose, using well-understood mathematical principles.

Backhouse's talk focussed on Galois connections and fixed points. This, I believe, went well beyond Dijkstra, who dealt mostly with the predicate calculus. But it was grounded in the tradition because it showed how well-known algorithms could be connected back to well-known mathematics. It gave us programmers -- most of the audience -- glimpses of the mathematical beauty which hides behind our algorithmic artefacts.

The talk was overwhelmingly convincing, but (esprit d'escalier, walking back to Kings Cross) I wonder. Until major surprising new algorithms are discovered in this way, it seems to be a sophisticated and beautiful form of verification of algorithms that already exist. I don't say 'no more than': it's too powerful for that, and it does allow us to see general forms, and thus connections between algorithms that we wouldn't suspect. And it is so, so beautiful. But construction=calculation? On the stairway, I wasn't convinced. But I shall buy his book in the hope that I'm wrong.

(Postscript: Esprit d'escalier afflicts smart-arses on the way out. I showed the note above to the speaker, who told me that, had he time at the end of his talk,

he would have talked about a novel algorithm that has indeed been discovered in this way. I look forward to being gladly humbled; I've learnt, once again, never to mock a mathematician. Poets are dangerous too ...)

Book Announcements

Author	Wolfgang Reisig
Title	Understanding Petri Nets
Publisher	Springer
ISBN	978-3-642-33277-7
	978-3-642-33278-4 (eBook)
Date	2013

This is a translation from the author's original work, Petrinetze, published by Springer in 2010. Both books have the subtitle, Modeling Techniques, Analysis Techniques, Case Studies. Carl Adam Petri himself has provided a Foreword. The book contains some twenty examples and case studies from distributed and dynamic systems, including a vending machine, mutual exclusion and crosstalk algorithms, message-based mutex and synchronisation in acyclic networks. This is a comprehensive tutorial of both the theory and application of Petri Nets; Part I covers Modelling Techniques, Part II Analysis Methods and Part III Case Studies. Closing Remarks form Part IV, Conclusion.

A flyer contains high praise for Wolfgang Reisig's book from the great and the good: from Carl Adam Petri himself (on the original German text); from David Harel; Schahram Dustdar; Dines Bjørner; Wil van der Aalst; Rocco de Nicola; Cliff Jones; Gul Agha; Reinhard Wilhelm; Dimitris Karagiannis; Frank Lehmann; Joost-Pieter Katoen; Manfred Broy; Holger Hermanns; Grzegorz Rozenberg; Rob van Glabbeek.

Author	Einar Smith
Title	Carl Adam Petri: Life and Science
Publisher	Springer
ISBN	978-3-662-48092-2
	978-3-662-48093-9 (eBook)
Date	2015

This book is another translation from its author's original German: *Carl Adam Petri: Eine Biographie*, again published by Springer in 2014. While this is a

biography of Petri, it focusses on the history of his scientific thought and research, and about 50% of the material in the book is, one could say, technical. Some of the chapter headings reveal this: Thesis on Automata; GMD: the Home of Petri Nets; Net Foldings, Morphisms and Topology; Non-Sequential Processes and Concurrency Theory; Communication Disciplines; Theory of Measurement. These are interleaved with other chapters which are more of what one would expect in a biography: Infancy and Youth; University, Academe, Family; The Maturing Years; The Prosperity Years; etc. Thus this book gives an insight into the thought processes and development of Petri the scientist, as well as some intriguing revelations of his character. For this reason, Einar Smith's book will, I believe, appeal to a range of computer scientist readers.

In 1944 Petri, drafted into Military service, was captured and taken to a prisoner of war camp in England. Einar Smith writes: "During his 4-year captivity, Petri was treated very decently by the British, for which he was always very grateful. The camp had a library, provided by anonymous benefactors... He was allowed to work as a land surveyor, and contribute to the planning of a new suburb of Walsall in the West Midlands... in 1948 he was allowed to graduate in the final secondary school exams in Birmingham, originally intended as second-chance education for British adults.", which British readers in particular may be interested, and perhaps pleased, to read.

I must admit to having an interest in these two books, in that I helped with their final rendering into English.

Reports by Tim Denvir

Some Interesting Links

Some links which may be of interest to FACS:

Leslie Lamport, Second Heidelberg Laureate Forum Lecture; *How to write a 21st century proof*: http://www.heidelberg-laureate-forum.org/blog/video/lecture-tuesday-september-23-2014-leslie-lamport/ Lamport's Abstract reads: *Mathematicians have made a lot of progress in the last 350 years, but not in writing proofs. The proofs they write today are just like the ones written by Newton. This makes it all too easy to prove things that aren't true. I'll describe a better way that I've been using for about 25 years.* Looking at his slides while listening to the lecture requires manual intervention. Lamport's delivery is somewhat slow, not a complaint I often have. He takes twenty minutes to reach his main thesis, that of using hypertext to structure proofs. But it is good to see someone attempting to analyse proof techniques from the point of view of effective communication from the giver of the proof to its receiver. He refers to a favourite "theorem" of mine, Lewis Carroll's spoof proof that all triangles are isosceles.

Donald Knuth's 21st "Annual Christmas Tree Lecture"; an annual lecture given by Knuth vaguely on the subject of Trees. This one is titled *Universal Comma-free Codes*. It seems he has given such a lecture for the last 21 years: https://m.youtube.com/watch?v=48iJx8FVuis Reactions to this are mixed, some criticising his lecturing style, which is certainly less dynamic than Leslie Lamport's, others full of reverential praise. This web page has links to many other lectures on YouTube, from Stanford University and elsewhere.

These were found in *Hacker News* https://news.ycombinator.com/ a forum for general programming/SW engineering but which has occasional links to formal topics.

Thanks to Roger Carsley and Bill Pearson for pointing us to these links.

Tim Denvir

FACS Committee

Formal Aspects of Computing Science Specialist Group

Jonathan Bowen
Chairman
ZUG Liaison

Jawed Siddiqi
FACS Treasurer

Paul Boca
FACS Secretary

Roger Carsley
Minutes Secretary

John Cooke
BCS Liaison
Publications

John Fitzgerald
FME Liaison

Margaret West
BCS Women Liaison

Rob Hierons
Chair, Formal Methods and Testing Subgroup

John Derrick
Chair, Refinement Subgroup

Eerke Boiten
CryptoForma Liaison

Tim Denvir
Co-Editor, FACS FACTS

Brian Monahan
Co-Editor, FACS FACTS

FACS is always interested to hear from its members and keen to recruit additional helpers. Presently we have vacancies for officers to help with fund raising, to liaise with other specialist groups such as the Requirements Engineering group and the European Association for Theoretical Computer Science (EATCS), and to maintain the FACS website. If you are able to help, please contact the FACS Chair, Professor Jonathan Bowen at the contact points below:

BCS-FACS

c/o Professor Jonathan Bowen (Chair)
London South Bank University

Email jonathan.bowen@lsbu.ac.uk

Web www.bcs-facs.org

You can also contact the other Committee members via this email address.

Please feel free to discuss any ideas you have for FACS or voice any opinions openly on the FACS mailing list <FACS@jiscmail.ac.uk>. You can also use this list to pose questions and to make contact with other members working in your area. Note: only FACS members can post to the list; archives are accessible to everyone at http://www.jiscmail.ac.uk/lists/facs.html.