Lecture Notes in Computer Science 4710

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Chris W. George Zhiming Liu
Jim Woodcock (Eds.)

Domain Modeling and the Duration Calculus

International Training School
Shanghai, China, September 17-21, 2007
Advanced Lectures

Springer

Volume Editors

Chris W. George
Zhiming Liu
United Nations University
International Institute for Software Technology
P.O.Box 3058, Macau SAR, China
E-mail:{cwg, z.liu}@iist.unu.edu

Jim Woodcock
University of York
Department of Computer Science
Heslington, York YO10 5DD, UK
E-mail: jim@cs.york.ac.uk

Library of Congress Control Number: Applied for

CR Subject Classification (1998): F.3, D.2.11, D.2.4, D.2.2, F.2.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-74963-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74963-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12124022 06/3180 5 4 3 2 1 0

Preface

This volume contains a record of the lectures given at the *ICTAC Training School on Domain Modelling and Duration Calculus*, held during the 17th–21st September 2007 in Shanghai. The *School* was organised by East China Normal University, UNU-IIST, and the University of York as part of the celebrations of the 70th birthdays of Dines Bjørner and Zhou Chaochen. There were two associated events:

- *Essays in Honour of Dines Bjørner and Zhou Chaochen on the Occasion of their 70th Birthdays*. Papers presented at a Symposium held in Macao on 24th & 25th September 2007. LNCS volume 4700. Springer 2007.
- *Proceedings of the International Colloquium on Theoretical Aspects of Computing*. Held in Macao during 26th–28th September 2007. LNCS volume 4711. Springer 2007.

The *school* is aimed at postgraduate students, researchers, academics, and industrial software engineers who are interested in the state of the art in these topics. No previous knowledge of the topics involved is assumed. Two of the courses are in the area of domain engineering (and in formal, abstract modelling in general) and two are in the area of duration calculus; the fifth links the two areas. The five courses are taught by experts in these fields from Europe and Asia.

We are happy to acknowledge sponsorship from the following organisations:

- China International Talent Exchange Foundation
- East China Normal University
- United Nations University International Institute for Software Technology
- University of York

The proceedings were managed and assembled using the EasyChair conference management system.

Contributors

Alan Burns is a professor of computer science at the University of York. His research interests are in real-time systems, including the assessment of real-time programming languages, distributed operating systems, the formal specification of scheduling algorithms and implementation strategies, and the design of dependable user interfaces to real-time applications.

Dang Van Hung is a research fellow of UNU-IIST. He received a doctoral-level degree in computer science in 1988 from the Computer and Automation Research

Institute, Hungarian Academy of Sciences. His research interests include formal techniques of programming, concurrent and distributed computing, and design techniques for real-time systems.

Chris George is the Associate Director of the United Nations International Institute for Software Technology (UNU-IIST) in Macao. He is one of the main contributors to RAISE, particularly the RAISE method, and that remains his main research interest. Before coming to UNU-IIST he worked for companies in the UK and Denmark.

Michael Reichhardt Hansen is an associate professor at the Technical University of Denmark. His research interests include duration calculus, interval logic, and formal methods. He is one of the authors of the book *Duration Calculus* with Zhou Chaochen.

Cliff Jones was a professor at the University of Manchester, worked in industry at Harlequin for a period, and is now a professor of computing science at Newcastle University. He is Editor-in-Chief of the *Formal Aspects of Computing Journal*. He undertook the DPhil at Oxford University Computing Laboratory under Prof. Sir Tony Hoare frs, awarded in 1981. He worked with Dines Bjørner and others on the Vienna Development Method (VDM) at IBM in Vienna. He is a Fellow of the Royal Academy of Engineering.

Lecture Courses

Course 1: Delivering Real-Time Behaviour. This series of lectures is given by Alan Burns, and it focuses on how to engineer systems so that they can meet their timing requirements. Four separate, but related, issues are addressed.

1. A time band model that caters for the broad set of granularities found in a typical complex system.
2. The delay and deadline statements that allow timing requirements to be specified.
3. Scheduling analysis that enables a set of concurrent deadlines to be verified.
4. Timing analysis that enables sequential code to be inspected to determine its worst case behaviour.

These four topics—together with a number of other techniques and tools described in the course—allow real-time behaviour to be delivered.

Course 2: Applicative Modelling with RAISE. This course—given by Chris George—provides an introduction to the RAISE Specification Language and to the RAISE method. The course concentrates on the applicative style of RAISE, the style most commonly used initially in development. It also describes two examples. The first is a simple communication system that allows the transmission of messages with the possibility of higher priority messages overtaking others. The example illustrates the use of abstract initial specification to capture

vital properties, and of more detailed concrete specification to describe a model having those properties. The second example is a control system of a lift and illustrates the use of model checking to gain confidence in a RAISE model.

Course 3: A Theory of Duration Calculus with Application. This course is given jointly by Dang Van Hung and Michael Hansen. It presents selected central elements in the theory of the *duration calculus* and gives examples of applications. The lectures cover syntax, semantics, and a proof system for the basic logic. Results on decidability, undecidability, and model-checking are also presented. Some extensions of the basic calculus are described; in particular, hybrid duration calculus and duration calculus with iterations. The concepts are illustrated by a case study: the bi-phase mark protocol. References are provided for further study.

Course 4: Understanding Programming Language Concepts via Operational Semantics. Cliff Jones's lectures cover five topics.

1. **History of Verification.** This is based on his *Annals of the History of Computing* paper [Jon03]; this lecture adds more on semantics.
2. **Rely/Guarantee Method.** The most accessible reference for this is [Jon96] but the origins lie a long way back [Jon81,Jon83a,Jon83b] (see the extensive list of publications on various forms of rely/guarantee conditions at `homepages.cs.ncl.ac.uk/cliff.jones/home.formal`).
3. **Deriving Specifications.** This lecture is described in the accompanying *Festschrift* volume [JHJ07]; there is an earlier conference paper [HJJ03]).
4. **Semantics of Programming Languages.** This lecture is published in this volume. Chris George covers the idea of abstract modelling in general; Cliff Jones focuses on the application of this idea to programming languages.
5. **Soundness of Rely/Guarantee Proof Rules.** This final lecture justifies a set of proof rules like those introduced in Lecture 2 based on a semantics like that in Lecture 4. The proof is published in [CJ07]. This material links to "Refining Atomicity" [JLRW05,BJ05,Jon05,Jon07].

July 2007 J. C. P. W.

References

[BJ05] Burton, J.I., Jones, C.B.: Investigating atomicity and observability. Journal of Universal Computer Science 11(5), 661–686 (2005)

[CJ07] Coleman, J.W., Jones, C.B.: Guaranteeing the soundness of rely/guarantee rules (revised). Journal of Logic and Computation (in press, 2007)

[HJJ03] Hayes, I., Jackson, M., Jones, C.: Determining the specification of a control system from that of its environment. In: Araki, K., Gnesi, S., Mandrioli, D. (eds.) FME 2003. LNCS, vol. 2805, pp. 154–169. Springer, Heidelberg (2003)

[Jon81] Jones, C.B.: Development Methods for Computer Programs including a Notion of Interference. PhD thesis, Oxford University, June 1981 Printed as: Programming Research Group, Technical Monograph 25 (1981)

[Jon83a] Jones, C.B.: Specification and design of (parallel) programs. In: Proceedings of IFIP 1983, pp. 321–332. North-Holland, Amsterdam (1983)

[Jon83b] Jones, C.B.: Tentative steps toward a development method for interfering programs. ACM Transactions on Programming Languages and Systems 5(4), 596–619 (1983)

[Jon96] Jones, C.B.: Accommodating interference in the formal design of concurrent object-based programs. Formal Methods in System Design 8(2), 105–122 (1996)

[Jon01] Jones, C.B.: On the search for tractable ways of reasoning about programs. Technical Report CS-TR-740, Newcastle University, Superceded by (2001)

[Jon03] Jones, C.B.: The early search for tractable ways of reasoning about programs. IEEE, Annals of the History of Computing 25(2), 26–49 (2003)

[Jon05] Jones, C.B.: An approach to splitting atoms safely. In: Electronic Notes in Theoretical Computer Science, MFPS XXI, 21st Annual Conference of Mathematical Foundations of Programming Semantics, pp. 35–52 (2005)

[Jon07] Jones, C.B.: Splitting atoms safely. Theoretical Computer Science 357, 109–119 (2007)

[JHJ07] Jones, C., Hayes, I., Jackson, M.A.: Specifying systems that connect to the physical world. In: Essays in Honour of Dines Bjørner and Zhou Chaochen on the Occasion of the 70th Birthdays. Papers presented at a Symposium held in Macao on 24th & 25th September 2007. LNCS, vol. 4700, Springer, Heidelberg (2007)

[JLRW05] Jones, C.B., Lomet, D., Romanovsky, A., Weikum, G.: The atomicity manifesto (2005)

Coordinating Committee

Chris George	UNU-IIST
He Jifeng	East China Normal University
Zhiming Liu	UNU-IIST
Geguang Pu	East China Normal University
Jim Woodcock	University of York
Yong Zhou	East China Normal University

Table of Contents