

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

C. Neville Dean Raymond T. Boute (Eds.)

Teaching Formal Methods

CoLogNET/FME Symposium, TFM 2004
Ghent, Belgium, November 18-19, 2004
Proceedings



Springer

Volume Editors

C. Neville Dean
Anglia Polytechnic University
East Rd, Cambridge, CB1 1PT, UK
E-mail: c.n.dean@apu.ac.uk

Raymond T. Boute
INTEC, Ghent University
Sint-Pietersnieuwstraat 41, B-9000 Ghent, Belgium
E-mail: raymond.boute@intec.UGent.be

Library of Congress Control Number: 2004113937

CR Subject Classification (1998): D.2, F.3, F.2, F.4, D.1, E.1, K.3

ISSN 0302-9743
ISBN 3-540-23611-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11339786 06/3142 5 4 3 2 1 0

Preface

“Professional engineers can often be distinguished from other designers by the engineers’ ability to use mathematical models to describe and analyze their products.”¹

This observation by Parnas describes the de facto professional standards in all classical engineering disciplines (civil, mechanical, electrical, etc.). Unfortunately, it is in sharp contrast with current (industrial) practice in software design, where mathematical models are hardly used at all, even by those who, in Holloway’s words² “aspire to be engineers.” The rare exceptions are certain critical applications, where mathematical techniques are used under the general name formal methods.

Yet, the same characteristics that make formal methods a necessity in critical applications make them also advantageous in everyday software design at various levels from design efficiency to software quality.

Why, then, is education failing with respect to formal methods?

- failing to convince students, academics and practitioners alike that formal methods are truly pragmatic;
- failing to overcome a phobia of formality and mathematics;
- failing to provide students with the basic skills and understanding required to adopt a more mathematical and logical approach to software development.

Until education takes these failings seriously, formal methods will be an obscure byway in software engineering, which in turn will remain severely impoverished as a result.

These proceedings record the papers presented at the Symposium on Teaching formal methods (TFM 2004) held at the University of Ghent in Belgium, 18–19 November 2004. This symposium served as a forum to explore the failures and successes of formal methods education, to consider how the failings might be resolved, to learn from the successes, and to promote cooperative projects to further the teaching and learning of formal methods (FMs). The symposium was instrumental in bringing together

- formal methods educators, both actual and potential;
- other computer science and software engineering educators;
- industrial practitioners and project managers;
- technical and scientific publishers.

¹ David L. Parnas, “Predicate Logic for Software Engineering”, *IEEE Trans. SWE* 19, 9, pp. 856–862 (Sept. 1993)

² Michael Holloway, “Why Engineers Should Consider Formal Methods”, *Proc. 16th. Digital Avionics Systems Conference* (Oct. 1997), <http://techreports.larc.nasa.gov/ltrs/PDF/1997/mtg/NASA-97-16dasc-cmh.pdf>

The response to the Call for Papers was very encouraging, and it was possible to select a number of high-quality contributions.

The conference was also blessed with three excellent invited speakers: David Gries from Cornell University, Leslie Lamport from Microsoft Corporation, and Peter Pepper from the Technische Universität Berlin.

September 2004

Neville Dean
Raymond Boute

Program Committee

The following people were members of the TFM 2004 program committee and reviewed papers for the symposium:

Neville Dean (*Program Chair*), Anglia Polytechnic University, UK
Vicki Almstrum, University of Texas at Austin, USA
Roland Backhouse, University of Nottingham, UK
Wolfgang Grieskamp, Microsoft Research, USA
Henri Habrias, Université de Nantes, France
Andrew Martin, University of Oxford, UK
José Oliveira, Universidade do Minho, Braga, Portugal
Elvinia Riccobene, Università di Catania, Italy

External Referees

The program committee members are grateful to the following people who assisted them in the reviewing of papers:

Bernhard Aichernig, UNU-IIST, Macao, SAR China
Franco Barbanera, Università di Catania, Italy
L. Soares Barbosa, Universidade do Minho, Braga, Portugal
Giampaolo Bella, Università di Catania, Italy
Egon Boerger, Università di Pisa, Italy
Giuseppe Difazio, Università di Catania, Italy
Angelo Gargantini, Università di Catania, Italy
Jeremy Gibbons, Oxford University Computing Laboratory, UK
Yuri Gurevich, Microsoft Research, Redmond, USA
Marc Guyomard, ENSAT, Université de Rennes, France
John Jacky, University of Washington, Seattle, USA
Steve McKeever, Oxford University Computing Laboratory, UK
Giuseppe Pappalardo, Università di Catania, Italy
J. Sousa Pinto, Universidade do Minho, Braga, Portugal
Pascal Poizat, Université d'Evry, France
Patrizia Scandurra, Università di Catania, Italy
S. Melo de Sousa, Universidade da Beira Interior, Portugal
Nikolai Tillmann, Microsoft Research, Redmond, USA
Guy Vidal-Naquet, Ecole Supérieure d'Electricité, Paris, France

Support

Financial support from the following was instrumental in making the symposium possible:

CoLogNET

Fonds voor Wetenschappelijk Onderzoek (FWO) Vlaanderen

Organization

Many thanks must also go to Prof. Jean-François Raskin (Local Organization Chairman) and Bernadette Becue (Financial Administration INTEC) for their roles in organizing and running the symposium.

Finally, thanks are due to Dines Bjørner for instigating the symposium and for his help.

Table of Contents

A Beginner's Course on Reasoning About Imperative Programs	1
<i>Kung-Kiu Lau</i>	
Designing Algorithms in High School Mathematics	17
<i>Sylvia da Rosa</i>	
Motivating Study of Formal Methods in the Classroom	32
<i>Joy N. Reed, Jane E. Sinclair</i>	
Formal Systems, Not Methods	47
<i>Martin Loomes, Bruce Christianson, Neil Davey</i>	
A Practice-Oriented Course on the Principles of Computation, Programming, and System Design and Analysis	65
<i>Egon Börger</i>	
Teaching How to Derive Correct Concurrent Programs from State-Based Specifications and Code Patterns	85
<i>Manuel Carro, Julio Mariño, Ángel Herranz, Juan José Moreno-Navarro</i>	
Specification-Driven Design with Eiffel and Agents for Teaching Lightweight Formal Methods	107
<i>Richard F. Paige, Jonathan S. Ostroff</i>	
Integrating Formal Specification and Software Verification and Validation	124
<i>Roger Duke, Tim Miller, Paul Strooper</i>	
Distributed Teaching of Formal Methods	140
<i>Peter Pepper</i>	
An Undergraduate Course on Protocol Engineering – How to Teach Formal Methods Without Scaring Students	153
<i>Manuel J. Fernández-Iglesias, Martín Llamas-Nistal</i>	
Linking Paradigms, Semi-formal and Formal Notations	166
<i>Henri Habrias, Sébastien Faucou</i>	
Teaching Formal Methods in Context	185
<i>Jim Davies, Andrew Simpson, Andrew Martin</i>	
Embedding Formal Development in Software Engineering	203
<i>Ken Robinson</i>	

Advertising Formal Methods and Organizing Their Teaching: <i>Yes, but ...</i>	214
<i>Dino Mandrioli</i>	
Retrospect and Prospect of Formal Methods Education in China	225
<i>Baowen Xu, Yingzhou Zhang, Yanhui Li</i>	
A Survey of Formal Methods Courses in European Higher Education	235
<i>The FME Subgroup on Education (Convenor: J.N. Oliveira)</i>	
Author Index	249