

Preface

This volume contains the proceedings of TFM2009, the *Second International FME Conference on Teaching Formal Methods*, organized by the Subgroup of Education of the Formal Methods Europe (FME) association. The conference took place as part of the first Formal Methods Week (FMWeek), held in Eindhoven, The Netherlands, in November 2009.

TFM2009 was a one-day forum in which to explore the successes and failures of Formal Methods (FM) education, and to promote cooperative projects to further education and training in FMs. The organizers gathered lecturers, teachers, and industrial partners to discuss their experience, present their pedagogical methodologies, and explore best practices.

Interest in formal method teaching is growing. TFM2009 followed in a series of events on teaching formal methods which includes two BCS-FACS TFM workshops (Oxford in 2003, and London in 2006), the TFM2004 conference (Ghent, 2004, with proceedings published as Springer LNCS Volume 3294), the FM-Ed 2006 workshop (Hamilton, co-located with FM2006), FORMED (Budapest, at ETAPS 2008), and FMET 2008 (Kitakyushu, co-located with ICFEM 2008).

Formal methods have an important role to play in the development of complex computing systems—a role acknowledged in industrial standards such as IEC 61508 and ISO/IEC 15408, and in the increasing use of precise modelling notations, semantic markup languages, and model-driven techniques. There is a growing need for software engineers who can work effectively with simple, mathematical abstractions, and with practical notions of inference and proof.

Original contributions were solicited providing insight, opinions, and suggestions for courses of action regarding the teaching FMs, including but not limited to the following aspects: experiences of teaching FMs, both successful and unsuccessful; educational resources including the use of books, case studies and the internet; the education of weak and mathphobic students; the integration, or otherwise, of FMs into the curriculum, including contributions to the definition of a Formal Methods Body of Knowledge (FMBoK); the advantages of FM-trained graduates in the workplace; changing attitudes towards FMs in students, academic staff and practitioners; the necessary mathematical background.

There were 19 submissions, each being reviewed by at least 4 programme committee members. 10 papers were accepted, some of which were subject to a round of shepherding before completion. Two of the accepted papers addressed the conference theme of ‘widening access to FMs’ in terms of reaching students with limited enthusiasm for FMs as an end in themselves: Catano and Rueda describe two courses taught in Columbia—one on JML and one on B—that venture into the ‘unconquered territory’ of conventional software companies, and Ölveczky discusses an approach based on rewriting logic using the Maude tool. Two more papers address ‘widening access’ in a different dimension, extending that access beyond traditional university education: Ferreira *et al.* describe the

MathIS project that aims to reinvigorate high-school mathematics teaching, and Ishikawa *et al.* present some of their experiences with the TopSE programme of education for professional software engineers in Japan.

The next two papers describe synergistic combinations of similar FMs: Tarkan and Sazawal on using Alloy as a tool in the teaching of Z, and Poll on the combination of the JML specification language and the ESC/Java verification tool. Two more papers describe teaching approaches based on the integration of complementary FMs: Hallerstede and Leuschel on integrating model-checking with formal proof, and Ahrendt *et al.* on integrating formal and informal approaches to verification. Finally, the last two papers illustrate the typical evolution of an education programme in FMs: from graduate-level courses in new fields, as discussed by Kofroň *et al.*, in which the state of the art is rapidly evolving and the only materials available are primary sources, through a decade or two of development, to more mainstream undergraduate courses in more mature fields, in which secondary sources such as the textbook described by Aceto *et al.* may be used.

The programme commenced with an invited talk by Jeff Kramer on abstraction and modelling, arguing that these two crucial skills for software engineers are complementary partners. The conference closed with a panel discussion on the idea of building a *Guide to the Formal Methods Body of Knowledge* (FMBoK), inspired by similar efforts for software engineering (SWEBoK) and for project management (PMBoK); such a resource would provide guidance to teachers, managers, and developers on what should be expected from a comprehensive, balanced programme of education in FMs.

During the electronic programme committee meeting, there was a spirited discussion about the intent and extent of events of this kind; we feel this discussion is worth summarizing here. We are convinced that the papers included in this volume will be useful to those teaching formal methods: reporting on experiences; describing approaches that worked, and those that didn't; identifying common issues, to increase our understanding of which aspects are generic and which specific to a particular context; and generally providing inspiration for others. Nevertheless, it will be clear to readers that the papers do not present detailed qualitative or quantitative data collected during robust, repeatable, scientific experiments; the authors, the programme committee, and the intended audience may be leading researchers in formal methods, but they are by and large mere practitioners in pedagogy. Formal assessments of the efficacy of particular approaches to teaching formal methods would be valuable in informing our teaching, but they are very difficult to conduct—we leave this as a challenge for future events.

The conference was managed, and these proceedings were prepared, using the EasyChair conference management system (<http://www.easychair.org/>), whose valuable service we are happy to acknowledge.

August 2009

Jeremy Gibbons
José Oliveira

Acknowledgements

We are very grateful to the members of the programme committee and their additional referees for their care and diligence in reviewing the submitted papers. We are also grateful to Tijn Borghuis and Erik de Vink, FMWeek coordinators, for their help and support, and to the sponsoring institutions.

Organization

TFM 2009 was organized by the Subgroup of Education of the Formal Methods Europe (FME) association, in close collaboration with the organization of the *Formal Methods Week (FMWeek)*.

Programme Committee

Izzat Alsmadi	(North Dakota State University, USA)
Dines Bjørner	(IIMM Institute, Denmark)
Eerke Boiten	(University of Kent, UK)
Raymond Boute	(Ghent University, Belgium)
Andrew Butterfield	(Trinity College Dublin, Ireland)
Jim Davies	(University of Oxford, UK)
David Duce	(Oxford Brookes University, UK)
John Fitzgerald	(University of Newcastle upon Tyne, UK)
Jeremy Gibbons	(University of Oxford, UK)
Randolph Johnson	(National Security Agency, USA)
Mícheál Mac an Airchinnigh	(Trinity College Dublin, Ireland)
Dino Mandrioli	(Politecnico di Milano, Italy)
José Oliveira	(University of Minho, Portugal)
Kees Pronk	(Delft University of Technology, Netherlands)
Bernhard Schätz	(Technische Universität München, Germany)
Wolfgang Schreiner	(Johannes Kepler University Linz, Austria)
Simão Sousa	(Universidade da Beira Interior, Portugal)
Kenji Taguchi	(National Institute of Informatics, Japan)
Jeannette Wing	(Carnegie-Mellon University, USA)

Referees

Besides the members of the programme committee, the following external referees contributed to the paper reviewing process:

André Brito Passos	David Pereira	Ian Bayley
Clare Martin	Fuyuki Ishikawa	Radu Calinescu
Cyrille Artho	Henrique Costa	

Sponsoring Institutions

Formal Methods Europe Association (FME)
Software Improvement Group (SIG), Amsterdam, Netherlands

Table of Contents

Preface	V
Abstraction and Modelling: A Complementary Partnership	1
<i>Jeffrey Kramer</i>	
Teaching Formal Methods for the Unconquered Territory	2
<i>Nestor Catano, Camilo Rueda</i>	
Teaching Formal Methods Based on Rewriting Logic and Maude	20
<i>Peter Csaba Ölveczky</i>	
Which Mathematics for the Information Society?	39
<i>João F. Ferreira, Alexandra Mendes, Roland Backhouse, Luís S. Barbosa</i>	
What Top-Level Software Engineers Tackle after Learning Formal Methods: Experiences from the Top SE Project	59
<i>Fuyuki Ishikawa, Kenji Taguchi, Nobukazu Yoshioka, Shinichi Honiden</i>	
Chief Chefs of Z to Alloy	74
<i>Sureyya Tarkan, Vibha Sazawal</i>	
Teaching Program Specification and Verification Using JML and ESC/Java2	94
<i>Erik Poll</i>	
How to Explain Mistakes	107
<i>Stefan Hallerstede and Michael Leuschel</i>	
Integrated and Tool-Supported Teaching of Testing, Debugging, and Verification	127
<i>Wolfgang Ahrendt, Richard Bubel, Reiner Hähnle</i>	
On Teaching Formal Methods: Behavior Models and Code Analysis	146
<i>Jan Kofroň, Pavel Parížek, Ondřej Šerý</i>	
Teaching Concurrency: Theory in Practice	160
<i>Luca Aceto, Anna Ingolfsdottir, Kim G. Larsen, Jiří Srba</i>	
Author Index	179