# Preface

This volume presents a set of papers accompanying the lectures of the sixth edition of the International School on Formal Methods for the Design of Computer, Communication and Software Systems (SFM).

This series of schools addresses the use of formal methods in computer science as a prominent approach to the rigorous design of computer, communication and software systems. The main aim of the SFM series is to offer a good spectrum of current research in foundations as well as applications of formal methods, which can be of help for graduate students and young researchers who intend to approach the field.

SFM 2006 was devoted to formal techniques for hardware verification and covered several aspects of the hardware design process, including hardware design languages and simulation, property specification formalisms, automatic test pattern generation, symbolic trajectory evaluation, BDD-based and SAT-based model checking, decision procedures, refinement, theorem proving, and the verification of floating-point units.

The opening paper by Bombieri, Fummi, and Pravadelli provides a general view on simulation-based modeling and verification strategies for developing embedded systems. In particular, the paper is focussed on describing state-of-the art co-simulation approaches and verification strategies based on fault simulation and assertion checking.

The paper by Drechsler and Fey reviews the basic concepts and algorithms for the postproduction test of integrated circuits. Then the authors present an advanced SAT-based tool for automatic test pattern generation.

The paper by Claessen and Roorda concentrates on simulation-based model checking techniques, which do not need to represent the states of the design, but only the values that flow through each signal. In particular, the authors introduce a high-performance simulation-based model checking technique called symbolic trajectory evaluation.

The paper by Cabodi and Murciano overviews binary decision diagrams (BDD) and their application in formal hardware verification. The paper by Gupta, Ganai, and Wang illustrates instead a promising alternative to BDD-based symbolic model checking methods that relies on boolean satisfiability (SAT).

The paper by Cimatti and Sebastiani deals with decision procedures for verification problems that can be represented as satisfiability problems in some decidable fragments of first-order logic. The authors focus on integration techniques for combining technology for propositional satisfiability and solvers able to deal with the theory component.

The paper by Manolios addresses theorem proving systems and show how they can be employed to model and verify hardware using refinement. Theorem

proving is considered also in the closing paper by Harrison, where it is used for the verification of floating-point algorithms.

We believe that this book offers a comprehensive view of what has been done and what is going on worldwide in the field of formal methods for hardware verification. We wish to thank all the lecturers and all the participants for a lively and fruitful school. We also wish to thank the entire staff of the University Residential Center of Bertinoro for the organizational and administrative support.

May 2006

Marco Bernardo and Alessandro Cimatti
SFM 2006 Directors

# Table of Contents

# Hardware Design and Simulation for Verification

Nicola Bombieri, Franco Fummi, Graziano Pravadelli

# Automatic Test Pattern Generation

Rolf Drechsler, Görschwin Fey

# An Introduction to Symbolic Trajectory Evaluation

Koen Claessen, Jan-Willem Roorda

# BDD-Based Hardware Verification

Gianpiero Cabodi, Marco Murciano

# SAT-Based Verification Methods and Applications in Hardware Verification

Aarti Gupta, Malay K. Ganai, Chao Wang

# Building Efficient Decision Procedures on Top of SAT Solvers

Alessandro Cimatti, Roberto Sebastiani

# Refinement and Theorem Proving

Panagiotis Manolios

# Floating-Point Verification using Theorem Proving

John Harrison

# Author Index