Preface

This volume contains the revised version of papers presented at VMCAI 2002, the Third International Workshop on Verification, Model Checking, and Abstract Interpretation, Venice (Italy), January 21-22, 2002.

The main goal of the workshop was to give an overview of the main directions decisive for the growth and cross-fertilization of major research activities in program analysis and verification.

The VMCAI series was started in 1997 with the aim of gathering researchers interested in investigating similarities and differences among these three research methodologies, that may be summarized as follows:

- program verification aims at proving that programs meet their specifications, i.e., that the actual program behavior corresponds to the desired one.
- model checking is a specific approach to the verification of temporal properties of reactive and concurrent systems, which has been very successful in the area of finite-state programs.
- abstract interpretation is a method for designing and comparing semantics of program, expressing various types of program properties; in particular, it has been successfully used to infer run-time program properties that can be valuable in optimizing programs.

The program committee selected 22 papers out of 41 submissions on the basis of at least 3 reviews. The principal selection criteria were relevance, quality, and clarity. The resulting volume offers the reader an interesting perspective of the current research trends in the area. In particular, the papers contribute to the following topics: Security and Protocols, Timed Systems and Games, Static Analysis, Optimizations, Types and Verification, and Temporal Logics and Systems.

The quality of the papers, the interesting discussions at the workshop, and the friendly atmosphere enjoyed by all participants in Venice, encouraged us in the project of making VMCAI an annual privileged forum for researchers in the area.

Special thanks are due to the institutions that sponsored the event: the Computer Science Department of the University Ca’ Foscari, the European Association for Programming Languages and Systems (EAPLS), the MIUR Project “Interpretazione Astratta, Type Systems e Analisi Control-Flow” and the MIUR Project “Metodi Formali per la Sicurezza - MEFISTO”. We are especially grateful to C. Braghin for her helpful support in organizing the workshop.

March 2002

Agostino Cortesi
Program Committee Chair

Agostino Cortesi  Univ. Ca’ Foscari - Venezia (Italy)

Program Committee

Annalisa Bossi  Univ. Ca’ Foscari
Dennis Dams  Bell Labs and TU Eindhoven
Javier Esparza  TU Munchen
Chris Hankin  Imperial College
Joxan Jaffar  NU Singapore
Thomas Jensen  Irisa Rennes
Cosimo Laneve  Univ. di Bologna
Baudouin Le Charlier  UC Louvain La Neuve
Michael Leuschel  Univ. of Southampton
Giorgio Levi  Univ. di Pisa
Torben Mogensen  DIKU, Copenhagen
Supratik Mukhopadhyay  Univ. of Pennsylvania
Thomas Reps  Univ. of Wisconsin
Hanne Riis Nielson  TU of Denmark
David Schmidt  Kansas State University
Pascal Van Hentenryck  Brown University

Additional Referees

Busi Nadia  Levi Francesca  Scozzari Francesca
Charatonik Witold  Levin Vladimir  Sharygina Natasha
Thao Dang  Lovengreen Hans Henrik  Sokolsky Oleg
Di Piero Alessandra  Maggiolo Schettini Andrea  Steffen Martin
Elphick Daniel  Maija Patrick  Sun Hongyan
Faella Marco  Martinelli Fabio  Taguchi Kenji
Ferrari Gianluigi  Murano Aniello  Thiagarajan P.S.
Giacobazzi Roberto  Namjoshi Kedar  Tronci Enrico
Godefroid Patrice  Ngan Chinh Wei  Varea Mauricio
Gori Roberta  Pinna Michele  Voicu Razvan
Hansen Michael R.  Ravi Kavita  Xiaoqun Du
Hansen Rene Rydhof  Roychoudhury Abhik  Zavattaro Gianluigi
Kho Siu Chong  Sacerdoti Coen Claudio
### Table of Contents

#### Security and Protocols

- Combining Abstract Interpretation and Model Checking for Analysing Security Properties of Java Bytecode
  
  *Cinzia Bernardeschi, Nicoletta De Francesco*
  
  1

- Proofs Methods for Bisimulation Based Information Flow Security
  
  *Riccardo Focardi, Carla Piazza, Sabina Rossi*
  
  16

- A Formal Correspondence between Offensive and Defensive JavaCard Virtual Machines
  
  *Gilles Barthe, GUillaume Dufay, Line Jakubiec, Simão Melo de Sousa*
  
  32

- Analyzing Cryptographic Protocols in a Reactive Framework
  
  *R.K. Shyamasundar*
  
  46

#### Timed Systems and Games

- An Abstract Schema for Equivalence-Checking Games
  
  *Li Tan*
  
  65

- Synchronous Closing of Timed SDL Systems for Model Checking
  
  *Natalia Sidoroea, Martin Steffen*
  
  79

- Automata-Theoretic Decision of Timed Games
  
  *Marco Fuella, Salvatore La Torre, Aniello Murano*
  
  94

#### Static Analysis

- Compositional Termination Analysis of Symbolic Forward Analysis
  
  *Witold Charatonik, Supratik Mukhopadhyay, Andreas Podelski*
  
  109

- Combining Norms to Prove Termination
  
  *Samir Genaim, Michael Codish, John Gallagher, Vitaly Lagoon*
  
  126

- Static Monotonicity Analysis for $\lambda$-definable Functions over Lattices
  
  *Andrzej S. Murawski, Kwangkeun Yi*
  
  139

- A Refinement of the Escape Property
  
  *Patricia M. Hill, Fausto Spoto*
  
  154
Optimizations

Storage Size Reduction by In-place Mapping of Arrays ................. 167
   Remko Tronçon, Maurice Bruynooghe, Gerda Janssens,
   Francky Catthoor

Verifying BDD Algorithms through Monadic Interpretation .............. 182
   Sava Krstić, John Matthews

Improving the Encoding of LTL Model Checking into SAT ............... 196
   Alessandro Cimatti, Marco Pistore, Marco Roveri, Roberto Sebastiani

Types and Verification

Automatic Verification of Probabilistic Free Choice .................. 208
   Lenore Zuck, Amir Pnueli, Yonit Kesten

An Experiment in Type Inference and Verification by Abstract
   Interpretation .................................................. 225
   Roberta Gori, Giorgio Levi

Weak Muller Acceptance Conditions for Tree Automata ................. 240
   Salvatore La Torre, Aniello Murano, Maryherita Napoli

A Fully Abstract Model for Higher-Order Mobile Ambients ............ 255
   Mario Coppo, Mariangiola Dezani-Ciancaglini

Temporal Logics and Systems

A Simulation Preorder for Abstraction of Reactive Systems .......... 272
   Ferucio Laurentiu Tiplea, Aurora Tiplea

Approximating ATL' in ATL ..................................... 289
   Aidan Harding, Mark Ryan, Pierre-Yves Schobbens

Model Checking Modal Transition Systems Using Kripke Structures .... 302
   Michael Huth

Parameterized Verification of a Cache Coherence Protocol:
   Safety and Liveness ........................................ 317
   Kai Baukus, Yassine Lakhnech, Karsten Stahl

Author Index ...................................................... 331