Computer Aided Verification

5th International Conference, CAV '93
Elounda, Greece, June 28-July 1, 1993
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest
Preface

This volume contains the proceedings of the Fifth Conference on Computer-Aided Verification (CAV'93), held in Elounda, Crete, Greece, from June 28 to July 1, 1993.

The objective of the CAV conferences is to bring together researchers and practitioners interested in the development and use of methods, tools and theories for the computer-aided verification of concurrent systems. The conferences provide an opportunity for comparing various verification methods and tools that can be used to assist the applications designer. Emphasis is placed on new research results and the application of existing methods to real verification problems.

Of the 84 submitted papers, 37 were accepted for presentation. Invited talks were given by B. Brayton (UC Berkeley), M. Gordon (Cambridge University), and P. Varaiya (UC Berkeley). The first day of the conference was dedicated to tutorials on real-time formalisms by R. Alur (AT&T Bell Laboratories), D. Dill (Stanford University), T. Henzinger (Cornell University), and partial order verification methods by P. Wolper (University of Liege). Besides the areas of real-time verification (which this year included results about the new formalism of hybrid systems) partial order methods and hardware verification where the conference has been traditionally strong in the past, there were some new themes which emerged in this year's conference. These themes are of vital importance for advancing the state-of-the-art in computer-aided verification and include the combination of model-checking with theorem proving techniques, and the exploitation of symmetry in verification methodologies. There were sessions devoted to hardware verification, theorem proving, real-time formalisms, process algebras and calculi, partial order methods, the exploitation of symmetry, and other verification methods and tools.

Financial support is provided among others by the Institute of Computer Science, FORTH, the University of Crete, and mainly by the Commission of the European Communities, Directorate-General XIII, ESPRIT program. Many research projects funded by ESPRIT Basic Research contributed a large number of high-quality papers to this conference.

The Program Committee was very active in reviewing and shaping the final program. The Steering Committee, consisting of E.M. Clarke (Carnegie Mellon University), R.P. Kurshan (AT&T Bell Laboratories), A. Pnueli (Weizmann Institute), and J. Sifakis (VERIMAG), took part in the reviewing process as well and offered council at appropriate moments. This year, the Program Committee members were: R. Alur (AT&T Bell Labs), G. Bochmann (U. Montreal), R. Brayton (UC Berkeley), E. Brinksma (U. Twente), R. Cleaveland (North Carolina State U.), W. Damm (Oldenburg U.), R. de Simone (INRIA), D. Dill (Stanford U.), A. Emerson (UT Austin), O. Grumberg (Technion), N. Halbwachs (VERIMAG), H. Hiraishi (Kyoto Sangyo U.), G. Holzmann (AT&T Bell Labs), K. Larsen (Aalborg U.), P. Loewenstein (Sun), L. Paulson (Cambridge
VI

U.), D.K. Probst (Concordia U.), A. Sangiovanni-Vincentelli (UC Berkeley), B. Steffen (TU Aachen), C. Stirling (Edinburgh U.), P. Wolper (U. Liege) and T. Yoneda (Tokyo Inst. of Tech.).

Costas Courcoubetis is General and Program Chair. MITOS SA is responsible for the local arrangements, registration, and the treasurer functions. Liana Kefalaki is the Conference Secretary and Magda Hadzaki is the assistant to the Program Chair. P. Godefroid (Liege U.) assisted in the preparation of the tutorial on partial order verification methods. R. Schapire (AT&T Bell Labs) provided his program for compiling the electronic scorecards of the reviewers to produce the final reports.


Heraklion, May 1993

Costas Courcoubetis
Table of Contents

Invited Lecture: Logic Synthesis and Design Verification  
R. Brayton (UC Berkeley) .............................................. 1

Session 1: Hardware Verification with BDDs  
Efficient Verification with BDDs Using Implicitly Conjoined Invariants  
A. Hu and D. Dill (Stanford U.)  ........................................... 3

Parametric Circuit Representation Using Inductive Boolean Functions  
A. Gupta and A. Fisher (Carnegie Mellon U.) ............................................. 15

An Iterative Approach to Language Containment  
F. Balin and A. Sangiovanni-Vincenelli (UC Berkeley)  .............................................. 29

BDD-Based Debugging of Designs Using Language Containment and Fair CTL  
R. Hojati and R. Brayton (UC Berkeley),  
R. Kurshan (AT&T Bell Labs) ............................................. 41

Session 2: Methods and Tools  
Reliable Hashing Without Collision Detection  
P. Wolper and D. Leroy (U. Liege) ........................................... 59

A Tool for Symbolic Program Verification and Abstraction  
S. Graf and C. Loiseaux (VERIMAG) ........................................... 71

Symbolic Equivalence Checking  
J.-C. Fernandez, A. Kerbrat and L. Mounier (VERIMAG) ........................................... 85

A Decision Algorithm for Full Propositional Temporal Logic  
Y. Kesten (Weizmann Inst.), Z. Manna and McGuire (Stanford U.),  
A. Pnueli (Weizmann Inst.) ........................................... 97

Reachability and Recurrence in Extended Finite State Machines: Modular Vector Addition Systems  
A. Krishnakumar (AT&T Bell Labs) ........................................... 110

Automatic Generation of Network Invariants for the Verification of Iterative Sequential Systems  
J.-K. Rho and F. Somenzi (U. Colorado) ........................................... 123

A Graphical Interval Logic Toolset for Verifying Concurrent Systems  
G. Kutty, Y. Ramakrishna, L. Moser, L. Dillon,  
and P. Melliar-Smith (UC Santa Barbara) ........................................... 138

Session 3: Theorem Proving 1  
Combining Model Checking and Theorem Proving to Verify Parallel Processes  
H. Hungar (U. Oldenburg) ........................................... 154

Verification of a Multiplier: 64 Bits and Beyond  
R. Kurshan (AT&T Bell Labs) and L. Lamport (Digital Equipm. Corp.) ........................................... 166
Invited Lecture: Protocol Design for an Automated Highway System
P. Varaiya (UC Berkeley) .......................................................... 180

Session 4: Analysis of Real-Time Systems 1
Computing Accumulated Delays in Real-Time Systems
R. Alur (AT&T Bell Labs), C. Courcoubetis (U. Crete and ICS, FORTH)
and T. Henzinger (Cornell U.) .................................................. 181
Reachability Analysis of Planar Multi-Linear Systems
O. Maler (VERIMAG) and A. Pnueli (Weizmann Inst.) ....................... 194
An Efficient Algorithm for Minimizing Real-Time Transition Systems
M. Yannakakis and D. Lee (AT&T Bell Labs) .................................. 210
Verification of Timing Properties of VHDL
C. Courcoubetis (U. Crete and ICS, FORTH), W. Damm and
B. Josko (U. Oldenburg) .......................................................... 225
Alternating RQ Timed Automata
W. Lam and R. Brayton (UC Berkeley) ......................................... 237
Timed Modal Specification - Theory and Tools
K. Čerăns (Chalmers U. of Tech.), J. Godskesen
and K. Larsen (Aalborg U.) .................................................... 253

Session 5: Theorem Proving 2
A Mechanically Verified Application for a Mechanically Verified Environment
M. Wilding (Comp. Logic Inc. and UT Austin) .................................. 268
Verification of Real-Time Systems Using PVS
N. Shankar (SRI Int.) ................................................................. 280
The Formal Verification of an Algorithm for Interactive Consistency Under a
Hybrid Fault Model
P. Lincoln and J. Rushby (SRI Int.) ............................................. 292
Computer-Assisted Simulation Proofs
J. Søgaard-Andersen (Denmark Tech. U.), S. Garland,
J. Guttag, N. Lynch and A. Pogosyants (MIT) ................................ 305

Invited Lecture: A Verifier and Timing Analyser for Simple Imperative
Programs
M. Gordon (Cambridge U.) .......................................................... 320

Session 6: Analysis of Real-Time Systems 2
Efficient Verification of Parallel Real-Time Systems
T. Yoneda and A. Shibayama (Tokyo Tech. Inst.),
B.-H. Schlingloff (TU Muenchen) and E. Clarke (Carnegie Mellon U.) .... 321
Delay Analysis in Synchronous Programs
N. Halbwachs (IMAG and Stanford U.) ........................................ 333
Verifying Quantitative Real-Time Properties of Synchronous Programs
M. Jourdan, F. Maraninchi and A. Olivero (VERIMAG) ..................... 347
Session 7: Process Algebras and Calculi

A Modal Logic for Message Passing Processes
M. Hennessy and X. Liu (U. Sussex) ........................................ 359

Functionality Decomposition by Compositional Correctness Preserving Transformation
E. Brinksma, R. Langerak and P. Broekroelofs (U. Twente) .............. 371

On Model-Checking for Fragments of μ-Calculus
E. Emerson (UT Austin), C. Jutla (IBM) and A. Sistla (U. Illinois) .......... 385

Session 8: Partial Orders

On-The-Fly Verification with Stubborn Sets
A. Valmari (Tampere U. and TRC Finland) .................................. 397

All from One, One for All: On Model Checking Using Representatives
D. Peled (AT&T Bell Labs) ......................................................... 409

Verifying Timed Behavior Automata with Input/Output Critical Races
D. Probst and H. Li (Concordia U.) ........................................... 424

Refining Dependencies Improves Partial-Order Verification Methods
P. Godefroid and D. Pirottin (U. Liege) ........................................ 438

Session 9: Exploiting Symmetry

Exploiting Symmetry in Temporal Logic Model Checking
E. Clarke (Carnegie Mellon U.), T. Filkorn (SIEMENS),
S. Jha (Carnegie Mellon U.) .................................................... 450

Symmetry and Model Checking
E. Emerson (UT Austin) and A. Sistla (U. Illinois) ......................... 463

Generation of Reduced Models for Checking Fragments of CTL
D. Dams (Eindhoven U.), O. Grumberg (AT&T Bell Labs),
R. Gerth (Eindhoven U.) .......................................................... 479

A Structural Linearization Principle for Processes
R. Kurshan and M. Merritt (AT&T Bell Labs), A. Orda (Technion)
and S. Sachs (UC Berkeley) ..................................................... 491