1. Record Nr. UNISA996466223503316

Titolo	Hardware and Software: Verification and Testing [[electronic resource]] : 11th International Haifa Verification Conference, HVC 2015, Haifa, Israel, November 17-19, 2015, Proceedings / / edited by Nir Piterman
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-26287-4
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVI, 293 p. 88 illus. in color.)
Collana	Programming and Software Engineering ; ; 9434
Disciplina	005.1
Soggetti	Software engineering Computer logic Programming languages (Electronic computers) Mathematical logic Artificial intelligence Computer communication systems Software Engineering Logics and Meanings of Programs Programming Languages, Compilers, Interpreters Mathematical Logic and Formal Languages Artificial Intelligence Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Invited Talks -- Hybrid Systems -- Between Testing and Verification: Software Model Checking via Systematic Testing -- Fight for the Future of Verification -- Live in it Today -- Between Art and Craft: The Self-conception of a Verification Engineer -- Reasoning About Program Data Structure Shape: From the Heap to Distributed Systems -- Contents -- XSpeed: Accelerating Reachability Analysis on Multi-core Processors -- 1 Introduction -- 2 Preliminaries -- 2.1 Support Functions -- 2.2 Reachability Analysis Using Support Functions -- 3 Parallel State-Space Exploration -- 3.1

Parallel Samplings over Template Directions -- 3.2 Parallel Exploration of Reachable States -- 4 Sampling Support Functions in GPU -- 4.1 CUDA Programming Model -- 4.2 Computing Support Functions of Polytopes in GPU -- 4.3 Computing Support Functions of Hyperbox in GPU -- 5 Experiments -- 5.1 Five Dimensional System -- 5.2 Helicopter Controller -- 6 Conclusion -- References -- Abstraction-Based Parameter Synthesis for Multiaffine Systems -- 1 Introduction -- 2 Preliminaries -- 3 Abstraction of MHA -- 3.1 Pointwise LHA Abstraction -- 3.2 Set-Based LHA Abstraction -- 4 Hierarchical Parameter Search -- 4.1 Computation of Underapproximative Abstractions -- 4.2 Discrete Abstraction of MHA -- 4.3 Parameter Identification -- 5 Evaluation -- 6 Related Work -- 7 Conclusion -- References -- Tools -- Combining Static and Dynamic Analyses for Vulnerability Detection: Illustration on Heartbleed -- 1 Introduction -- 2 The Heartbleed Vulnerability -- 3 Overview of the Flinder-SCA Tool -- 4 Detection of Alarms by Static Analysis -- 5 Simplification of the Program by Slicing -- 6 Confirmation of Alarms by Fuzz Testing -- 7 Tool Demonstration -- 7.1 Static Analysis Step Applied to the Heartbleed Vulnerability.
7.2 Fuzz Testing Step Applied to the Heartbleed Vulnerability -- 8 Discussion -- 9 Conclusion and Future Work -- References -- The Verification Cockpit -- Creating the Dream Playground for Data Analytics over the Verification Process -- 1 Introduction -- 2 Motivation and Goals -- 3 Architecture and Implementation of the Verification Cockpit -- 3.1 Architecture of the Verification Cockpit -- 3.2 The Data Model -- 3.3 Implementation -- 4 Use Examples -- 4.1 Test Submission Dashboards -- 4.2 Coverage Dashboards -- 4.3 Connecting Coverage to the Verification Plan -- 4.4 Template Aware Coverage -- 5 Conclusions -- References -- Verification of Robotics -- Coverage-Driven Verification --- An Approach to Verify Code for Robots that Directly Interact with Humans -- 1 Introduction -- 2 Coverage-Driven Verification -- 2.1 Structure of a CDV Testbench -- 2.2 Test Generator -- 2.3 Driver -- 2.4 Checker -- 2.5 Coverage Collector -- 2.6 CDV Methodology -- 3 CDV Implementation -- 3.1 Case Study: Robot to Human Object Handover Task -- 3.2 Requirements -- 3.3 CDV Testbench Implementation -- 3.4 Test Generator and Driver -- 3.5 Checker -- 3.6 Coverage Collector -- 4 Experiments and Verification Results -- 5 Conclusions -- References -- Symbolic Execution -- PANDA: Simultaneous Predicate Abstraction and Concrete Execution -- 1 Introduction -- 2 Preliminaries -- 3 PANDA Algorithm -- 3.1 Dynamic Pruning and Discovery of Feasible Covering Paths -- 3.2 Soundness and Termination -- 4 Implementation -- 5 Evaluation -- 6 Related Work -- 7 Conclusion -- References -- TSO to SC via Symbolic Execution -- 1 Introduction -- 2 Weak Memory Reorderings -- 3 Processes and Their Parallel Composition -- 4 Symbolic Store-Buffer Graphs -- 5 SC Program Generation -- 6 Experimental Results -- 7 Related Work -- 8 Conclusion -- References.
Parallel Symbolic Execution: Merging In-Flight Requests -- 1 Introduction -- 2 Multi-threaded Symbolic Execution -- 2.1 Symbolic Execution -- 2.2 Single-Threaded Symbolic Execution -- 2.3 Going Multi-Threaded -- 3 Reducing Overall Solver Costs -- 3.1 Batching Solver Requests -- 3.2 Merging and Solving Requests -- 3.3 Merging vs. Caching -- 4 Implementation -- 5 Evaluation -- 5.1 Time Spent by the Solver -- 5.2 Thread-Based Parallel Symbolic Execution -- 5.3 Batching and Merging Parallel Requests -- 5.4 Prototype Limitations -- 5.5 Threats to Validity -- 6 Related Work -- 7 Conclusion -- References -- Model Checking -- Limited Mobility, Eventual Stability -- 1 Introduction -- 1.1 Related Work on Verifying Mobile IP -- 2 The

Formal Framework -- 2.1 Just Discrete Systems -- 2.2 Finitary Abstraction -- 2.3 Partial System Abstraction -- 3 Modelling Mobility -- 3.1 IPv6 Mobility Basics -- 3.2 The System -- 3.3 Properties -- 4 Formal Verification of the System -- 4.1 Proving Eventual Stable Routing -- 4.2 Method I: From Stability to Safety -- 4.3 Method II -- 5 Conclusions -- References -- A New Refinement Strategy for CEGAR-Based Industrial Model Checking -- 1 Introduction -- 2 Preliminaries -- 3 Lazy Abstraction -- 4 Abstraction Refinement -- 4.1 Path Projection -- 5 Implementation and Experimental Results -- 6 Conclusion -- References -- Timed Systems -- Quasi-equal Clock Reduction: Eliminating Assumptions on Networks -- 1 Introduction -- 2 Preliminaries -- 3 Reducing Clocks in Networks of Timed Automata -- 3.1 Algorithm for Transformation of Networks -- 3.2 Transformation of Properties -- 4 Weak Bisimulation -- 5 Experimental Results -- References -- Resource-Parameterized Timing Analysis of Real-Time Systems -- 1 Introduction -- 2 Backgrounds -- 2.1 Related Work -- 3 Resource-Parameterized Timing Analysis -- 3.1 Response Time of Applications.
3.2 Behavior Models of PIM and PSM -- 4 Case Study: Turn Indication Systems -- 4.1 PIM Analysis -- 4.2 PSM Analysis -- 5 Conclusions -- References -- SAT Solving -- SAT-Based Explicit LTL Reasoning -- 1 Introduction -- 2 Preliminaries -- 3 Explicit LTL Reasoning -- 3.1 Temporal Transition System -- 3.2 System Construction -- 3.3 Related Work -- 4 LTL Satisfiability Checking -- 4.1 The Main Algorithm -- 4.2 Heuristics for State Elimination -- 5 Experiments on LTL Satisfiability Checking -- 5.1 Experimental Methodologies -- 5.2 Results -- 6 Concluding Remarks -- References -- Understanding VSIDS Branching Heuristics in Conflict-Driven Clause-Learning SAT Solvers -- 1 Introduction -- 2 Background -- 3 Contribution I and II: Community-Focused Search, Bridge Variables, and VSIDS -- 4 Contribution III: Experimental Evidence Supporting Strong Correlation Between TGC and VSIDS -- 5 Contribution IV: Exponential Moving Average and Multiplicative Decay -- 6 Contribution V: A Faster Branching Heuristic Based on Adaptive Moving Average -- 7 Interpretation of Results -- 8 Related Work -- 9 Conclusions and Future Work -- References -- Multi Domain Verification -- Multi-Domain Verification of Power, Clock and Reset Domains -- Abstract -- 1 Introduction -- 2 Individual Domain Verification -- 2.1 Clock Domain Crossing -- 2.2 Reset Domain Crossing -- 2.3 Power Domain Crossing -- 3 Multi-Domain Verification -- 3.1 Domain Structure Verification -- 3.2 Domain Control Verification -- 3.3 Domain Crossing Verification -- 4 Results -- 5 Conclusion -- References -- Synthesis -- FudgeFactor: Syntax-Guided Synthesis for Accurate RTL Error Localization and Correction -- 1 Introduction -- 2 Related Work -- 3 ``Fudging'' Buggy RTL Circuits -- 3.1 Common Error Library -- 3.2 Error Modeling -- 3.3 Instrumentation of the Buggy Circuit -- 3.4 The 2QBF Problem -- 3.5 Miter Construction.
4 Selecting Areas for ``Fudging'' -- 4.1 SAT-Based Debugger -- 5 Experimental Methodology -- 6 Experimental Results -- 7 Conclusions -- References -- On Switching Aware Synthesis for Combinational Circuits -- 1 Introduction -- 2 Problem Statement -- 3 Input Pairing for and Gates -- 4 Evaluation: Synthetic Boolean Models -- 5 Evaluation: A Mini Instruction Decoder -- 6 Discussion -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Haifa Verification Conference, HVC 2015, held in Haifa, Israel, in November 2015. The 17 revised full papers and 4 invited talks presented were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on hybrid

systems; tools; verification of robotics; symbolic execution; model checking; timed systems; SAT solving; multi domain verification; and synthesis.