

1. Record Nr.	UNISA996587865903316
Autore	Dimitrova Rayna
Titolo	Verification, Model Checking, and Abstract Interpretation : 25th International Conference, VMCAI 2024, London, United Kingdom, January 15-16, 2024, Proceedings, Part I
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-50524-7
Edizione	[1st ed.]
Descrizione fisica	1 online resource (361 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14499
Altri autori (Persone)	LahavOri WolffSebastian
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Invited Keynote Talks -- Two Projects on Human Interaction with AI -- Automating Relational Verification of Infinite-State Programs -- Contents - Part I -- Contents - Part II -- Abstract Interpretation -- Formal Runtime Error Detection During Development in the Automotive Industry -- 1 Introduction -- 2 Background -- 3 Module-Level Abstract Interpretation with Contracts -- 3.1 Generating a Verification Harness -- 3.2 Contracts and Their Effects -- 4 Automatically Inferring Contracts -- 4.1 Contracts from Interface Specifications -- 4.2 Contracts from Abstract Interpretation -- 5 Case Study -- 6 Practical Experiences with Large Systems -- 6.1 Embedded Control Software -- 6.2 Embedded Software Library -- 7 Lessons Learned -- 8 Related Work -- 9 Conclusion -- References -- Abstract Interpretation-Based Feature Importance for Support Vector Machines -- 1 Introduction -- 2 Background -- 3 Methodology -- 3.1 Abstract Feature Importance -- 3.2 Abstracting One-Hot Encoding -- 3.3 Individual Fairness -- 3.4 Searching for Counterexamples -- 4 Experimental Evaluation -- 5 Conclusion -- References -- Generation of Violation Witnesses by Under-Approximating Abstract Interpretation -- 1 Introduction -- 2 Semantics -- 2.1 Notation -- 2.2 Background on Sufficient Preconditions Semantic -- 2.3 User Input -- 2.4 Integer Wrapping -- 3 Powerset Domain -- 3.1 Under-Approximated Powerset

-- 3.2 Case Study: Polyhedra Refinement -- 4 Implementation and Experiments -- 5 Conclusion -- References -- Correctness Witness Validation by Abstract Interpretation -- 1 Introduction -- 2 Preliminaries -- 2.1 Witnesses -- 2.2 Abstract Interpretation -- 3 Initialization-Based Approaches -- 4 Unassuming -- 4.1 Specification -- 4.2 Naïve Definition -- 4.3 Dual-Narrowing -- 5 Unassuming Indirectly -- 5.1 Propagating Unassume -- 6 Evaluation. 6.1 Precision Evaluation -- 6.2 Performance Evaluation -- 7 Related Work -- 8 Conclusion -- References -- Infinite-State Systems -- Project and Conquer: Fast Quantifier Elimination for Checking Petri Net Reachability -- 1 Introduction -- 2 Petri Nets and Polyhedral Abstraction -- 3 Combining Polyhedral Abstraction with Reachability -- 4 Projecting Formulas Using Token Flow Graphs -- 5 Formal Procedure and Proof of Correctness -- 6 Experimental Results -- 7 Discussion and Related Works -- References -- Parameterized Verification of Disjunctive Timed Networks -- 1 Introduction -- 2 Preliminaries -- 2.1 Parameterized Verification Problems -- 2.2 Symbolic Semantics of Timed Automata -- 3 Minimum-Time Reachability Algorithm for DTN- -- 3.1 Symbolic Semantics for DTN- -- 3.2 An Algorithm for Solving Minreach -- 3.3 Verification of DTNs -- 4 Conditions for Decidability with Location Invariants -- 5 Evaluation -- 6 Conclusion -- References -- Resilience and Home-Space for WSTS -- 1 Introduction -- 2 Well-Structured Transition Systems and VASS -- 3 Resilience for WSTS -- 3.1 Case: Safe="3222378 Safe -- 3.2 Case: Safe="3223379 Safe -- 4 State-Resilience -- 4.1 Case: Safe="3222378 Safe -- 4.2 Case: Safe="3223379 Safe -- 5 Resilience for VASS and Variations -- 6 Conclusion and Perspectives -- References -- Model Checking and Synthesis -- Generic Model Checking for Modal Fixpoint Logics in COOL-MC -- 1 Introduction -- 2 Model Checking for the Coalgebraic -Calculus -- 3 Implementation - Model Checking in COOL-MC -- 4 Experimental Evaluation of the Implementation -- 5 Conclusions and Future Work -- References -- Model-Guided Synthesis for LTL over Finite Traces -- 1 Introduction -- 2 Preliminaries -- 2.1 LTL over Finite Traces (LTLf) -- 2.2 Transition-Based DFA -- 2.3 LTLf Realizability, Synthesis, and tdfa Games -- 3 LTLf-to-tdfa via Progression. 4 Guided LTL f Synthesis with Satisfiable Traces -- 4.1 An Example -- 4.2 The Synthesis Algorithm MoGuS -- 4.3 Back to Our Example -- 5 Experimental Evaluation -- 5.1 Experimental Set-Up -- 5.2 Results and Analysis I: Random and Two-player-Games Benchmarks -- 5.3 Results and Analysis II: Ascending Benchmarks -- 6 LTL Synthesis - Related Work -- 7 Concluding Remarks -- References -- Solving Two-Player Games Under Progress Assumptions -- 1 Introduction -- 2 Preliminaries -- 3 Problem Statement -- 4 Strong Transition Fairness Assumptions -- 5 Strong Transition Co-fairness Assumptions -- 6 Group Transition Fairness Assumptions -- 6.1 Live Group Assumptions -- 6.2 Singleton-Source Live Groups -- 6.3 Live Groups in Product Games -- 6.4 A Remark on Co-live Groups -- 7 Persistent Live Group Assumptions -- 7.1 Augmented Reachability Games -- 7.2 Augmented Parity Games -- References -- SAT, SMT, and Automated Reasoning -- Interpolation and Quantifiers in Ortholattices -- 1 Introduction -- 2 Quantified Orthologic: Syntax, Semantics, and a Complete Proof System -- 2.1 Complete Ortholattices -- 2.2 Soundness -- 2.3 Completeness -- 3 No Quantifier Elimination for Orthologic -- 4 Failure of a Refutation-Based Interpolation -- 5 Interpolation for Orthologic Formulas -- 6 Further Related Work -- 7 Conclusion -- References -- Function Synthesis for Maximizing Model Counting -- 1 Introduction -- 2 Problem Statement -- 2.1 Preliminaries -- 2.2 Problem Formulation -- 2.3 Hardness of DQMax#SAT -- 3 Global Method -- 4 Incremental

Method -- 5 Local Method -- 5.1 Reducing Common Dependencies --
5.2 Solving Variables with No Dependencies -- 6 Application to
Software Security -- 6.1 Our Model of Security in Presence of an
Adaptive Adversary -- 6.2 Security as a Rechability Property -- 6.3
Security as a Lack of Leakage Property.
6.4 Some Remarks About the Applications to Security -- 7
Implementation and Experiments -- 8 Related Work -- 9 Conclusions
-- References -- Boosting Constrained Horn Solving by Unsat Core
Learning -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2
Constraint Horn Clauses -- 2.3 Graph Neural Networks -- 3 Abstract
Symbolic Model Checking for CHCs -- 3.1 Satisfiability Checking for
CHCs -- 3.2 CEGAR- And Symbolic Execution-Style Exploration -- 4
Guiding CHC Solvers Using MUSes -- 4.1 Minimal Unsatisfiable Sets --
4.2 MUS-Based Guidance for CHC Solvers -- 5 Design of Model -- 5.1
Encode CHCs to Graph Representation -- 5.2 Model Structure -- 6
Evaluation -- 6.1 Benchmark -- 6.2 Parameters -- 6.3 Experimental
Results -- 7 Related Work -- 8 Conclusion and Future Works --
References -- On the Verification of the Correctness of a Subgraph
Construction Algorithm -- 1 Introduction -- 2 The CP-Algorithm --
2.1 The CP-Algorithm -- Idea of the Correctness Proof -- 3 Modeling
Geometric Graphs -- 3.1 Geometric Axioms -- 3.2 Axiomatizing Graph
Properties -- 3.3 Axioms for Notions Used in the CP-Algorithm -- 3.4
Axioms for Notions Used in the Correctness Proof -- 4 Automated
Reasoning -- 4.1 Analyzing the Axioms -- Decidability -- 4.2
Choosing the Proof Systems -- 4.3 Automated Proof of Properties of
Geometric Graphs -- 4.4 Correctness of the CP-Algorithm: Verifying
Main Steps -- 4.5 Connection Between the Components X and Y -- 4.6
Proof of Properties for the Convex Hull -- 4.7 Constructing a
Counterexample Without Coexistence Property -- 5 Conclusion --
References -- Efficient Local Search for Nonlinear Real Arithmetic -- 1
Introduction -- 1.1 Contributions -- 1.2 Related Work -- 1.3 Structure
of the Paper -- 2 Preliminaries -- 3 Incremental Computation of
Variable Scores -- 4 Relaxation of Equalities -- 5 Implementation.
5.1 Heuristic Moves Selection and Look-Ahead -- 5.2 Implementation
Details -- 6 Evaluation -- 6.1 Overall Result -- 6.2 Comparison with
Other Work on Local Search -- 6.3 Effect of Incremental Computation
of Variable Scores -- 6.4 Effect of Relaxation of Equalities -- 6.5 Other
Techniques -- 7 Conclusion -- References -- Author Index.
