

1. Record Nr.	UNISA996495571003316
Autore	Seidl Helmut
Titolo	Theoretical aspects of computing - ICTAC 2022 : 19th International Colloquium, Tbilisi, Georgia, September 27-29, 2022, proceedings // Helmut Seidl, Zhiming Liu, and Corina S. Pasareanu
Pubbl/distr/stampa	Cham, Switzerland : , : Springer International Publishing, , [2022] ©2022
ISBN	3-031-17715-0
Descrizione fisica	1 online resource (494 pages)
Collana	Lecture Notes in Computer Science
Disciplina	004
Soggetti	Computer science Computer science - Social aspects
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- On Safety, Assurance and Reliability: A Software Engineering Perspective (Abstract of Invited Talk) -- Contents -- VeriMon: A Formally Verified Monitoring Tool -- 1 Introduction -- 2 Evolution -- 3 Future Directions -- 4 Discussion -- References -- Generalized Test Tables: A Domain-Specific Specification Language for Automated Production Systems -- 1 Introduction -- 2 The Domain of Automated Production Systems -- 3 Generalized Test Tables -- 4 Relational Test Tables -- 5 Conclusion -- References -- Reachability Games and Parity Games -- 1 Introduction -- 2 Games on Graphs -- 3 Reachability Games and Attractors -- 4 Optimal Strategies for Reachability Games -- 5 Parity Games -- 6 Zielonka's Algorithm for Parity Games -- 7 Lehtinen's Algorithm for Parity Games -- 8 Conclusion -- References -- Human-Cyber-Physical Automata and Their Synthesis -- 1 The Basic Model of HCPA -- 2 Synthesis of HCPS -- 3 Concluding Remarks -- References -- A PO Characterisation of Reconfiguration -- 1 Introduction -- 2 Labelled Partial Order Computations in a Nutshell -- 3 Preliminaries -- 3.1 Partial Orders and Labeled Partial Orders -- 3.2 Channelled Transition Systems (CTS) -- 3.3 Petri Nets with Inhibitor Arcs (PTI-nets) -- 4 LPO Semantics -- 4.1 Channelled Transition Systems (CTS) -- 4.2 Petri Nets with Inhibitor Arcs (PTI-nets) -- 5 Partial Order with Glue -- 5.1 Glue Computations

for CTSs -- 5.2 Glue Computations for PTI-nets -- 6 Separating Choice and Forced Interleaving -- 6.1 Choice vs Reconfiguration-Forced Interleaving in CTSs -- 6.2 Choice vs Interleaving in PTI-nets -- 7 Concluding Remarks -- References -- Structural Rules and Algebraic Properties of Intersection Types -- 1 Introduction -- 2 Type Systems -- 3 Term Expansion -- 4 Conclusions -- References -- Quantitative Weak Linearisation -- 1 Introduction. 2 Terms and Reductions -- 3 Types -- 4 Weak-Linearisation for Strongly Normalising Terms -- 5 A Characterisation of Weak-Linear Terms -- 6 Related Works and Discussions -- 7 Conclusions and Future Work -- References -- On the Formalization and Computational Complexity of Resilience Problems for Cyber-Physical Systems -- 1 Introduction -- 1.1 Related Work -- 2 Motivating Example Involving Drones -- 3 Timed Multiset Rewriting -- 4 Timed MSR for Resilient Systems -- 5 Verification Problems -- 6 Computational Complexity Results -- 7 Conclusions -- References -- Spatial and Timing Properties in Highway Traffic -- 1 Introduction -- 2 Preliminaries -- 2.1 Abstract Model of Motorway Traffic -- 2.2 Evolution of a Traffic Snapshot -- 2.3 MLSL with Scopes -- 2.4 State-Clock Logic -- 2.5 First-Order Theory of Real-Closed Fields -- 3 Timed MLSL -- 4 Semi-decision Procedure for TMLSL -- 5 Conclusion -- References -- Denotational and Algebraic Semantics for the CaIT Calculus -- 1 Introduction -- 2 The CaIT Calculus -- 2.1 Syntax -- 2.2 Guided Choice -- 3 Denotational Semantics -- 3.1 Semantic Model -- 3.2 Healthiness Conditions -- 3.3 Denotational Semantics of Basic Commands -- 3.4 Denotational Semantics of Guarded Choice -- 3.5 Parallel Composition -- 3.6 Channel Restriction -- 4 Algebraic Semantics -- 4.1 Algebraic Laws of Basic Commands -- 4.2 Algebraic Laws of Parallel Composition -- 5 Conclusion and Future Work -- References -- Reconciling Communication Delays and Negation -- 1 Introduction -- 2 Background -- 2.1 Continuous Queries over Datastreams in Temporal Datalog -- 2.2 Hypothetical Answers to Continuous Queries -- 2.3 Operational Semantics -- 2.4 Adding Negation -- 3 Declarative Semantics of Negation with Delays -- 4 Operational Semantics of Negation with Delays -- 4.1 The Evidence Lattice -- 4.2 The Negation Update Operator. 4.3 Soundness and Completeness -- 5 Computing the Operational Semantics -- 6 Related Work and Discussion -- References -- A Combinatorial Study of Async/Await Processes -- 1 Introduction -- 2 Async/Await Concurrency -- 3 Partial Order Decomposition and the Counting Problem -- 4 Chord Processes, Interval Orders and Related Families -- 5 Uniform Random Generation: Experimental Study -- 6 Conclusion and Future Work -- References -- Unsatisfiability of Comparison-Based Non-malleability for Commitments -- 1 Introduction -- 2 Comparison-Based Non-malleability -- 2.1 (Un)satisfiability of the Comparison-Based Definition -- 3 Conclusions -- References -- Alternating Automatic Register Machines -- 1 Introduction -- 2 Preliminaries -- 3 Alternating Automatic Register Machines -- 4 Polynomial-Size Padded Alternating Automatic Register Machine -- References -- Functional Choreographic Programming -- 1 Introduction -- 2 The Choreographic -calculus -- 2.1 Syntax -- 2.2 Typing -- 3 Semantics of Chor -- 4 Illustrative Examples -- 4.1 Secure Communication -- 4.2 EAP -- 5 Related Work -- 6 Conclusion and Future Work -- A Single Sign-on Authentication -- B Full Definitions and Proofs -- C Proof of Theorem 1 -- D Proof of Theorem 2 -- References -- A Model Checking Based Approach to Detect Safety-Critical Adversarial Examples on Autonomous Driving Systems -- 1 Introduction -- 2 Preliminaries -- 2.1 Model Checking with UPPAAL --

2.2 Adversarial Examples Generation Algorithm -- 3 The Safety-Critical Adversarial Examples -- 4 Modelling the System and Detecting the SCAEs -- 4.1 Abstract Model of ADS in UPPAAL -- 4.2 Locating the Target and Timing -- 5 Experimental Evaluation -- 5.1 Experimental Setup -- 5.2 Selection of Traffic Map -- 5.3 Quantitative Performance -- 5.4 Analysis of the Experiment -- 6 Conclusion -- References.

Ground Confluence and Strong Commutation Modulo Alpha-Equivalence in Nominal Rewriting -- 1 Introduction -- 2 Nominal Rewriting Systems with Atom-Variables -- 2.1 Preliminaries -- 2.2 Ground Nominal Terms -- 2.3 Nominal Term Expressions -- 2.4 Nominal Rewriting Systems with Atom-Variables -- 2.5 Overlaps -- 2.6 Parallel Reduction -- 3 Confluence Criteria by Strong Commutation -- 3.1 Proof Method for Confluence by Strong Commutation -- 3.2 Confluence Properties in Nominal Rewriting -- 3.3 A Sufficient Condition for Church-Rosser Modulo α -equivalence -- 4 Conclusion -- References -- Local XOR Unification: Definitions, Algorithms and Application to Cryptography -- 1 Introduction -- 2 Preliminaries -- 3 Local XOR Unification -- 3.1 f -rooted Local Unification -- 3.2 α -rooted Local Unification -- 4 Solving f -rooted Local Unification -- 4.1 Overview -- 4.2 Algorithm for Solving f -rooted Local Unification -- 5 Solving α -rooted Local Unification -- 5.1 Overview -- 5.2 Handling Variables -- 5.3 Applying Inference Rules -- 5.4 α -rooted Local Unification Procedure -- 6 Conclusion -- References -- A Matching Logic Foundation for Alk -- 1 Introduction -- 2 A Taste of Alk -- 3 Matching Logic Semantics of the Alk Language -- 3.1 A Short Introduction to Matching Logic -- 3.2 Alk Semantics in Matching Logic Terms -- 4 Behavioral Properties of Algorithms as ML Patterns -- 5 Implementation of the Verification Process -- 5.1 Deriving Reachability Patterns from Annotations -- 5.2 Proving Reachability Patterns by Symbolic Execution -- 5.3 Implementation -- 6 Related Work -- 7 Conclusion -- References -- A Type System with Subtyping for WebAssembly's Stack Polymorphism -- 1 Introduction -- 2 A Small Fragment of Wasm -- 3 Type System Dir with "Direct" Sequential Composition -- 4 Type System Sub with Qualifiers and Subtyping -- 5 Typed Big-Step Semantics Based on Sub.

6 An Improvement over Sub -- 7 Conclusions and Future Work -- References -- A Verified Implementation of B+-Trees in Isabelle/HOL -- 1 Introduction -- 2 Contributions -- 2.1 Related Work -- 3 B+-trees and Approach -- 3.1 Notation -- 3.2 Definitions -- 3.3 Implementation Definitions -- 3.4 Node Internal Navigation -- 4 Set Operations -- 4.1 Functional Point Query -- 4.2 Imperative Point Query -- 4.3 Insertion and Deletion -- 5 Range Operations -- 5.1 Iterators -- 5.2 Range Queries -- 6 Conclusion -- 6.1 Evaluation -- 6.2 Outlook -- References -- Active Learning for Deterministic Bottom-Up Nominal Tree Automata -- 1 Introduction -- 2 Preliminaries -- 2.1 Nominal Set -- 2.2 Data Tree -- 3 Deterministic Bottom-Up Nominal Tree Automata -- 4 Myhill-Nerode Theorem -- 5 Observation Table -- 6 Learning Algorithm -- 7 Example -- 8 Conclusion -- References -- Towards a User Interface Description Language Based on Bigraphs -- 1 Introduction -- 2 UIDLs -- 3 Bigraphs -- 3.1 Structural Aspect and Rewriting Rules -- 3.2 Bigraphical Reactive Systems (BRS) -- 4 Representation of Mechanisms with Bigraphs -- 4.1 Representation of the Scene Graph -- 4.2 GUI Interactions -- 4.3 Bigraphs Expressiveness -- 5 Bigraphs Verification -- 5.1 Predicats -- 5.2 Properties Verification on UI -- 6 Related and Future Work -- References -- A Specification Logic for Programs in the Probabilistic Guarded Command Language -- 1 Introduction -- 2 State of the Art -- 3 Preliminaries -- 4 pGCL: A Probabilistic Guarded Command Language -- 5 Probabilistic Dynamic

Logic -- 6 The P-Box Modality and Logical Connectives -- 7
Expectations for Program Constructs -- 8 Purely Probabilistic and
Deterministic Programs -- 9 Program Analysis with pDL -- 9.1 Monty
Hall Game -- 9.2 Convergence of a Bernoulli Random Variable -- 10
Conclusion -- References.
Card-Minimal Protocols for Symmetric Boolean Functions of More than
Seven Inputs.
