

Scalable Techniques For Formal Verification

[DOWNLOAD HERE](#)

1; Scalable Techniques for Formal Verification; 1 1.1; Preface; 7 1.2; Contents; 11 1.3; 1 Introduction; 15 1.4; Part I Preliminaries; 20 1.4.1; 2 Overview of Formal Verification; 21 1.4.1.1; 2.1 Theorem Proving; 21 1.4.1.2; 2.2 Temporal Logic and Model Checking; 24 1.4.1.3; 2.3 Program Logics, Axiomatic Semantics, and Verification Conditions; 29 1.4.1.4; 2.4 Bibliographic Notes; 34 1.4.2; 3 Introduction to ACL2; 36 1.4.2.1; 3.1 Basic Logic of ACL2; 36 1.4.2.2; 3.2 Ground Zero Theory; 38 1.4.2.2.1; 3.2.1 Terms, Formulas, Functions, and Predicates; 41 1.4.2.2.2; 3.2.2 Ordinals and Well-Founded Induction; 43 1.4.2.3; 3.3 Extension Principles; 46 1.4.2.3.1; 3.3.1 Definitional Principle; 47 1.4.2.3.2; 3.3.2 Encapsulation Principle; 51 1.4.2.3.3; 3.3.3 Defchoose Principle; 53 1.4.2.4; 3.4 The Theorem Prover; 55 1.4.2.5; 3.5 Structuring Mechanisms; 56 1.4.2.6; 3.6 Evaluators; 57 1.4.2.7; 3.7 The ACL2 Programming Environment; 58 1.4.2.8; 3.8 Bibliographic Notes; 59 1.5; Part II Sequential Program Verification; 61 1.5.1; 4 Sequential Programs; 62 1.5.1.1; 4.1 Modeling Sequential Programs; 62 1.5.1.2; 4.2 Proof Styles; 64 1.5.1.2.1; 4.2.1 Stepwise Invariants; 64 1.5.1.2.2; 4.2.2 Clock Functions; 65 1.5.1.3; 4.3 Comparison of Proof Styles; 66 1.5.1.4; 4.4 Verifying Program Components and Generalized Proof Obligations; 68 1.5.1.5; 4.5 Discussion; 71 1.5.1.5.1; 4.5.1 Overspecification; 71 1.5.1.5.2; 4.5.2 Forced Homogeneity; 72 1.5.1.6; 4.6 Summary; 73 1.5.1.7; 4.7 Bibliographic Notes; 73 1.5.2; 5 Operational Semantics and Assertion Reasoning; 74 1.5.2.1; 5.1 Cutpoints, Assertions, and VCG Guarantees; 74 1.5.2.2; 5.2 VCG Guarantees and Symbolic Simulation; 77 1.5.2.3; 5.3 Composing Correctness Statements; 79 1.5.2.4; 5.4 Applications; 81 1.5.2.4.1; 5.4.1 Fibonacci Implementation on TINY; 82 1.5.2.4.2; 5.4.2 Recursive Factorial Implementation on the JVM; 84 1.5.2.4.3; 5.4.3 CBC-Mode Encryption and Decryption; 84 1.5.2.5; 5.5 Comparison with Related Approaches; 85 1.5.2.6; 5.6 Summary; 87 1.5.2.7; 5.7 Bibliographic Notes; 87 1.5.3; 6 Connecting Different Proof Styles; 89 1.5.3.1; 6.1 Soundness of Proof Styles; 90 1.5.3.2; 6.2 Completeness; 92 1.5.3.3; 6.3 Remarks on Mechanization; 96 1.5.3.4; 6.4 Discussion; 96 1.5.3.5; 6.5 Summary and Conclusion; 98 1.5.3.6; 6.6 Bibliographic Notes; 99 1.6; Part III Verification of Reactive Systems; 101 1.6.1; 7 Reactive Systems; 102 1.6.1.1; 7.1 Modeling Reactive Systems; 103 1.6.1.2; 7.2 Stuttering Trace Containment; 104 1.6.1.3; 7.3 Fairness Constraints; 106 1.6.1.4; 7.4 Discussion; 110 1.6.1.5; 7.5

Summary;113 1.6.1.6;7.6 Bibliographic Notes;114 1.6.2;8 Verifying Concurrent Protocols Using Refinements;115 1.6.2.1;8.1 Reduction via Stepwise Refinement;116 1.6.2.2;8.2 Reduction to Single-Step Theorems;116 1.6.2.3;8.3 Equivalences and Auxiliary Variables;120 1.6.2.4;8.4 Examples;122 1.6.2.4.1;8.4.1 An ESI Cache Coherence Protocol;122 1.6.2.4.2;8.4.2 An Implementation of the Bakery Algorithm;125 1.6.2.4.3;8.4.3 A Concurrent Deque Implementation;130 1.6.2.5;8.5 Summary;135 1.6.2.6;8.6 Bibliographic Notes;135 1.6.3;9 Pipelined Machines;137 1.6.3.1;9.1 Simulation Correspondence, Pipelines, and Flushing Proofs;137 1.6.3.2;9.2 Reducing Flushing Proofs to Refinements;140 1.6.3.3;9.3 A New Proof Rule;142 1.6.3.4;9.4 Example;143 1.6.3.5;9.5 Advanced Features;147 1.6.3.5.1;9.5.1 Stalls;147 1.6.3.5.2;9.5.2 Interrupts;147 1.6.3.5.3;9.5.3 Out-of-Order Execution;148 1.6.3.5.4;9.5.4 Out-of-Order and Multiple Instruction Completion;148 1.6.3.6;9.6 Summary;149 1.6.3.7;9.7 Bibliographic Notes;150 1.7;Part IV Invariant Proving;152 1.7.1;10 Invariant Proving;153 1.7.1.1;10.1 Predicate Abstractions;155 1.7.1.2;10.2 Discussion;157 1.7.1.3;10.3 An Illustrative Example;158 1.7.1.4;10.4 Summary;160 1.7.1.5;10.5 Bibliographic Notes;161 1.7.2;11 Predicate Abstraction via Rewriting;162 1.7.2.1;11.1 Features and Optimizations;166 1.7.2.1.1;11.1.1 User-Guided Abstraction;167 1.7.2.1.2;11.1.2 Assume Guarantee Reasoning;167 1.7.2.2;11.2 Reachability Analysis;16 EAN/ISBN : 9781441959980 Publisher(s): Springer, Berlin, Springer Science & Business Media Discussed keywords: Skalierung Format: ePub/PDF Author(s): Ray, Sandip

[DOWNLOAD HERE](#)

Similar manuals: