
Contents



I	Need and Tools to Verify Critical Cyber-Physical Systems	1
1	Critical Embedded Software: Control Software Development and V&V	3
2	Formal Methods: Different Approaches for Verification	7
2.1	Semantics and Properties	7
2.2	A Formal Verification Methods Overview	11
2.3	Deductive Methods	19
2.4	SMT-based Model-checking	21
2.5	Abstract Interpretation (of Collecting Semantics)	23
2.6	Need for Inductive Invariants	29
3	Control Systems	31
3.1	Controllers' Development Process	31
3.2	A Simple Linear System: Spring-mass Damper	35
II	Invariant Synthesis: Convex-optimization Based Abstract Interpretation	41
4	Definitions–Background	43
4.1	Discrete Dynamical Systems	43
4.2	Elements of (Applied) Convex Optimization	54
5	Invariants Synthesis via Convex Optimization: Postfixpoint Computation as Semialgebraic Constraints	64
5.1	Invariants, Lyapunov Functions, and Convex Optimization	64
5.2	Quadratic Invariants	68
5.3	Piecewise Quadratic Invariants	76
5.4	k -inductive Quadratic Invariants	87

5.5	Polynomial Invariants	95
5.6	Image Measure Method	103
5.7	Related Works	108
6	Template-based Analyses and Min-policy Iteration	111
6.1	Template-based Abstract Domains	111
6.2	Template Abstraction Fixpoint as an Optimization Problem	112
6.3	SOS-relaxed Semantics	114
6.4	Example	122
6.5	Related Works	124
III	System-level Analysis at Model and Code Level	127
7	System-level Properties as Numerical Invariants	129
7.1	Open-loop and Closed-loop Stability	130
7.2	Robustness with Vector Margin	139
7.3	Related Work	145
8	Validation of System-level Properties at Code Level	147
8.1	Axiomatic Semantics of Control Properties through Synchronous Observers and Hoare Triples	147
8.2	Generating Annotations: A Strongest Postcondition Propagation Algorithm	155
8.3	Discharging Proof Objectives using PVS	159
IV	Numerical Issues	165
9	Floating-point Semantics of Analyzed Programs	167
9.1	Floating-point Semantics	167
9.2	Revisiting Inductiveness Constraints	170
9.3	Bound Floating-point Errors: Taylor-based Abstractions aka Zonotopic Abstract Domains	173
9.4	Related Works	190
10	Convex Optimization and Numerical Issues	191
10.1	Convex Optimization Algorithms	191
10.2	Guaranteed Feasible Solutions with Floats	196
	Bibliography	201
	Index	217
	Acknowledgments	220