

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Technical Context . . . . .	4
1.1.1	Hybrid Systems . . . . .	4
1.1.2	Model Checking . . . . .	12
1.1.3	Deductive Verification . . . . .	14
1.1.4	Compositional Verification . . . . .	16
1.1.5	Lifting Quantifier Elimination . . . . .	19
1.1.6	Differential Induction and Differential Strengthening . . . . .	20
1.2	Related Work . . . . .	21
1.3	Contributions . . . . .	25
1.4	Structure of This Book . . . . .	25
	<b>Part I Logics and Proof Calculi for Hybrid Systems</b>	<b>31</b>
<b>2</b>	<b>Differential Dynamic Logic <math>\mathbf{dL}</math></b>	<b>33</b>
2.1	Introduction . . . . .	34
2.1.1	Structure of This Chapter . . . . .	35
2.2	Syntax . . . . .	35
2.2.1	Terms . . . . .	37
2.2.2	Hybrid Programs . . . . .	41
2.2.3	Formulas . . . . .	47
2.3	Semantics . . . . .	49
2.3.1	Valuation of Terms . . . . .	50
2.3.2	Valuation of Formulas . . . . .	51
2.3.3	Transition Semantics of Hybrid Programs . . . . .	54
2.4	Collision Avoidance in Train Control . . . . .	61
2.5	Proof Calculus . . . . .	64
2.5.1	Substitution . . . . .	65
2.5.2	Proof Rules . . . . .	76

2.5.3	Deduction Modulo with Invertible Quantifiers and Real Quantifier Elimination . . . . .	88
2.5.3.1	Lifting Quantifier Elimination by Invertible Quantifier Rules . . . . .	88
2.5.3.2	Admissibility in Invertible Quantifier Rules . . . . .	91
2.5.3.3	Quantifier Elimination and Modalities . . . . .	93
2.5.3.4	Global Invertible Quantifier Rules . . . . .	93
2.5.4	Verification Example . . . . .	94
2.6	Soundness . . . . .	97
2.7	Completeness . . . . .	101
2.7.1	Incompleteness . . . . .	102
2.7.2	Relative Completeness . . . . .	103
2.7.3	Characterising Real Gödel Encodings . . . . .	105
2.7.4	Expressibility and Rendition of Hybrid Program Semantics . . . . .	106
2.7.5	Relative Completeness of First-Order Assertions . . . . .	109
2.7.6	Relative Completeness of the Differential Logic Calculus . . . . .	113
2.8	Relatively Semidecidable Fragments . . . . .	114
2.9	Train Control Verification . . . . .	118
2.9.1	Finding Inductive Candidates . . . . .	118
2.9.2	Inductive Verification . . . . .	119
2.9.3	Parameter Constraint Discovery . . . . .	120
2.10	Summary . . . . .	122
<b>3</b>	<b>Differential-Algebraic Dynamic Logic DAL</b>	<b>123</b>
3.1	Introduction . . . . .	124
3.1.1	Related Work . . . . .	128
3.1.2	Structure of This Chapter . . . . .	130
3.2	Syntax . . . . .	130
3.2.1	Terms . . . . .	132
3.2.2	Differential-Algebraic Programs . . . . .	132
3.2.3	Formulas . . . . .	139
3.3	Semantics . . . . .	141
3.3.1	Transition Semantics of Differential-Algebraic Programs . . . . .	141
3.3.2	Valuation of Formulas . . . . .	145
3.3.3	Time Anomalies . . . . .	145
3.3.4	Conservative Extension . . . . .	147
3.4	Collision Avoidance in Air Traffic Control . . . . .	148
3.4.1	Flight Dynamics . . . . .	148
3.4.2	Differential Axiomatisation . . . . .	149
3.4.3	Aircraft Collision Avoidance Manoeuvres . . . . .	150
3.4.4	Tangential Roundabout Manoeuvre . . . . .	151
3.5	Proof Calculus . . . . .	152
3.5.1	Motivation . . . . .	153
3.5.2	Derivations and Differentiation . . . . .	154
3.5.3	Differential Reduction and Differential Elimination . . . . .	160

3.5.4	Proof Rules . . . . .	162
3.5.5	Deduction Modulo by Side Deduction . . . . .	168
3.5.6	Differential Induction with Differential Invariants . . . . .	170
3.5.7	Differential Induction with Differential Variants . . . . .	181
3.6	Soundness . . . . .	185
3.7	Restricting Differential Invariants . . . . .	188
3.8	Differential Monotonicity Relaxations . . . . .	189
3.9	Relative Completeness . . . . .	193
3.10	Deductive Strength of Differential Induction . . . . .	194
3.11	Air Traffic Control Verification . . . . .	197
3.11.1	Characterisation of Safe Roundabout Dynamics . . . . .	197
3.11.2	Tangential Entry Procedures . . . . .	200
3.11.3	Discussion . . . . .	201
3.12	Summary . . . . .	201
<b>4</b>	<b>Differential Temporal Dynamic Logic dTL</b>	<b>203</b>
4.1	Introduction . . . . .	204
4.1.1	Related Work . . . . .	205
4.1.2	Structure of This Chapter . . . . .	206
4.2	Syntax . . . . .	206
4.2.1	Hybrid Programs . . . . .	207
4.2.2	State and Trace Formulas . . . . .	207
4.3	Semantics . . . . .	210
4.3.1	Trace Semantics of Hybrid Programs . . . . .	210
4.3.2	Valuation of State and Trace Formulas . . . . .	213
4.3.3	Conservative Temporal Extension . . . . .	215
4.4	Safety Invariants in Train Control . . . . .	216
4.5	Proof Calculus . . . . .	217
4.5.1	Proof Rules . . . . .	218
4.5.2	Verification Example . . . . .	221
4.6	Soundness . . . . .	221
4.7	Completeness . . . . .	223
4.7.1	Incompleteness . . . . .	223
4.7.2	Relative Completeness . . . . .	224
4.7.3	Expressibility and Rendition of Hybrid Trace Semantics . . . . .	225
4.7.4	Modular Relative Completeness Proof . . . . .	226
4.8	Verification of Train Control Safety Invariants . . . . .	227
4.9	Liveness by Quantifier Alternation . . . . .	228
4.10	Summary . . . . .	230
	<b>Part II Automated Theorem Proving for Hybrid Systems</b>	<b>231</b>
<b>5</b>	<b>Deduction Modulo Real Algebra and Computer Algebra</b>	<b>233</b>
5.1	Introduction . . . . .	234

5.1.1	Related Work . . . . .	234
5.1.2	Structure of This Chapter . . . . .	235
5.2	Tableau Procedures Modulo . . . . .	235
5.3	Nondeterminisms in Tableau Modulo . . . . .	238
5.3.1	Nondeterminisms in Branch Selection . . . . .	238
5.3.2	Nondeterminisms in Formula Selection . . . . .	239
5.3.3	Nondeterminisms in Mode Selection . . . . .	240
5.4	Iterative Background Closure . . . . .	243
5.5	Iterative Inflation . . . . .	246
5.6	Experimental Results . . . . .	248
5.7	Summary . . . . .	251
<b>6</b>	<b>Computing Differential Invariants as Fixed Points</b>	<b>253</b>
6.1	Introduction . . . . .	254
6.1.1	Related Work . . . . .	255
6.1.2	Structure of This Chapter . . . . .	256
6.2	Inductive Verification by Combining Local Fixed Points . . . . .	256
6.2.1	Verification by Symbolic Decomposition . . . . .	257
6.2.2	Discrete and Differential Induction, Differential Invariants . . . . .	258
6.2.3	Flight Dynamics in Air Traffic Control . . . . .	260
6.2.4	Local Fixed-Point Computation for Differential Invariants . . . . .	262
6.2.5	Dependency-Directed Induction Candidates . . . . .	263
6.2.6	Global Fixed-Point Computation for Loop Invariants . . . . .	265
6.2.7	Interplay of Local and Global Fixed-Point Loops . . . . .	268
6.3	Soundness . . . . .	269
6.4	Optimisations . . . . .	271
6.4.1	Sound Interleaving with Numerical Simulation . . . . .	271
6.4.2	Optimisations for the Verification Algorithm . . . . .	272
6.5	Experimental Results . . . . .	272
6.6	Summary . . . . .	273
<b>Part III Case Studies and Applications in Hybrid Systems Verification</b>		<b>275</b>

<b>7</b>	<b>European Train Control System</b>	<b>277</b>
7.1	Introduction . . . . .	278
7.1.1	Related Work . . . . .	280
7.1.2	Structure of This Chapter . . . . .	281
7.2	Parametric European Train Control System . . . . .	281
7.2.1	Overview of the ETCS Cooperation Protocol . . . . .	281
7.2.2	Formal Model of Fully Parametric ETCS . . . . .	284
7.3	Parametric Verification of Train Control . . . . .	286
7.3.1	Controllability Discovery . . . . .	287
7.3.2	Iterative Control Refinement . . . . .	288

7.3.3	Safety Verification . . . . .	291
7.3.4	Liveness Verification . . . . .	293
7.3.5	Full Correctness of ETCS . . . . .	294
7.4	Disturbance and the European Train Control System . . . . .	295
7.4.1	Controllability Discovery . . . . .	296
7.4.2	Iterative Control Refinement . . . . .	298
7.4.3	Safety Verification . . . . .	298
7.5	Experimental Results . . . . .	299
7.6	Summary . . . . .	301
<b>8</b>	<b>Air Traffic Collision Avoidance</b>	<b>303</b>
8.1	Introduction . . . . .	304
8.1.1	Related Work . . . . .	307
8.1.2	Structure of This Chapter . . . . .	308
8.2	Curved Flight in Roundabout Manoeuvres . . . . .	309
8.2.1	Flight Dynamics . . . . .	309
8.2.2	Roundabout Manoeuvre Overview . . . . .	310
8.2.3	Compositional Verification Plan . . . . .	311
8.2.4	Tangential Roundabout Manoeuvre Cycles . . . . .	312
8.2.5	Bounded Control Choices . . . . .	315
8.2.6	Flyable Entry Procedures . . . . .	315
8.2.7	Bounded Entry Duration . . . . .	318
8.2.8	Safe Entry Separation . . . . .	319
8.3	Synchronisation of Roundabout Manoeuvres . . . . .	322
8.3.1	Successful Negotiation . . . . .	322
8.3.2	Safe Exit Separation . . . . .	326
8.4	Compositional Verification . . . . .	328
8.5	Flyable Tangential Roundabout Manoeuvre . . . . .	329
8.6	Experimental Results . . . . .	331
8.7	Summary . . . . .	333
<b>9</b>	<b>Conclusion</b>	<b>335</b>

## Part IV Appendix 339

<b>A</b>	<b>First-Order Logic and Theorem Proving</b>	<b>341</b>
A.1	Overview . . . . .	341
A.2	Syntax . . . . .	346
A.2.1	Terms . . . . .	346
A.2.2	Formulas . . . . .	347
A.3	Semantics . . . . .	348
A.3.1	Valuation of Terms . . . . .	349
A.3.2	Valuation of Formulas . . . . .	349
A.4	Proof Calculus . . . . .	350
A.4.1	Proof Rules . . . . .	351

A.4.2	Proof Example: Ground Proving Versus Free-Variable Proving	354
A.5	Soundness . . . . .	356
A.6	Completeness . . . . .	356
A.7	Computability Theory and Decidability . . . . .	357
<b>B</b>	<b>Differential Equations</b>	<b>359</b>
B.1	Ordinary Differential Equations . . . . .	359
B.2	Existence Theorems . . . . .	363
B.3	Existence and Uniqueness Theorems . . . . .	364
B.4	Linear Differential Equations with Constant Coefficients . . . . .	365
<b>C</b>	<b>Hybrid Automata</b>	<b>369</b>
C.1	Syntax and Traces of Hybrid Automata . . . . .	369
C.2	Embedding Hybrid Automata into Hybrid Programs . . . . .	371
<b>D</b>	<b>KeYmaera Implementation</b>	<b>377</b>
D.1	KeYmaera: A Hybrid Theorem Prover for Hybrid Systems . . . . .	377
D.1.1	Structure of This Appendix . . . . .	379
D.2	Computational Back-ends for Real Arithmetic . . . . .	380
D.2.1	Real-Closed Fields . . . . .	381
D.2.2	Semialgebraic Geometry and Cylindrical Algebraic Decom- position . . . . .	383
D.2.3	Nullstellensatz and Gröbner Bases . . . . .	386
D.2.4	Real Nullstellensatz . . . . .	392
D.2.5	Positivstellensatz and Semidefinite Programming . . . . .	394
D.3	Discussion . . . . .	396
D.4	Performance Measurements . . . . .	399
	<b>References</b>	<b>401</b>
	<b>Index</b>	<b>415</b>
	<b>Operators and Proof Rules</b>	<b>423</b>



<http://www.springer.com/978-3-642-14508-7>

Logical Analysis of Hybrid Systems  
Proving Theorems for Complex Dynamics

Platzer, A.

2010, XXX, 426 p., Hardcover

ISBN: 978-3-642-14508-7