

André Platzer

Logical Analysis of Hybrid Systems

Proving Theorems for Complex Dynamics

Springer

Contents

1	Introduction	1
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
 Part I Logics and Proof Calculi for Hybrid Systems		31
2	Differential Dynamic Logic \mathbf{dL}	33
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
3	Differential-Algebraic Dynamic Logic DAL	123
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
4	Differential Temporal Dynamic Logic dTL	203
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
	Part II Automated Theorem Proving for Hybrid Systems	231
5	Deduction Modulo Real Algebra and Computer Algebra	233
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
6	Computing Differential Invariants as Fixed Points	253
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
Part III Case Studies and Applications in Hybrid Systems Verification		275
7	European Train Control System	277
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
8	Air Traffic Collision Avoidance	303
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
9	Conclusion	335
Part IV Appendix		339
A	First-Order Logic and Theorem Proving	341
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	Differential Equations	359
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
C	Hybrid Automata	369
C.1	Syntax and Traces of Hybrid Automata	369
C.2	Embedding Hybrid Automata into Hybrid Programs	371
D	KeYmaera Implementation	377
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 Decomposition	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
	References	401
	Index	415
	Operators and Proof Rules	423

List of Figures

1.1	European Train Control System	2
1.2	ETCS: discrete evolution of acceleration a , continuous evolution of velocity v and of position z over time t	3
1.3	Collision avoidance manoeuvres in air traffic control	3
1.4	Hybrid automaton for an (overly) simplified train control system	5
1.5	Hybrid automaton and hybrid program of a simple bouncing ball	7
1.6	Switching between two damped oscillators	8
1.7	Hybrid automaton for switching damped oscillators	9
1.8	Stable trajectory switching between two damped oscillators	9
1.9	Unstable trajectory switching between two damped oscillators	10
1.10	Simple water tank system	11
1.11	Successive state space exploration in finite-state model checking	12
1.12	Failed hybrid automaton decomposition attempt	17
1.13	Successful hybrid program decomposition	18
1.14	Dependencies and suggested reading sequence of chapters and appendices	28
2.1	Hybrid program rendition of hybrid automaton for (overly) simplified train control	36
2.2	Parametric bouncing ball	45
2.3	Parametric bouncing ball (with abbreviations resolved)	46
2.4	Transition semantics of modalities in \mathbf{dL} formulas	52
2.5	Transition semantics and example dynamics of hybrid programs	56
2.6	Continuous flow along differential equation $x' = \theta$ over time	57
2.7	Transition structure and transition example in (overly) simple train control	59
2.8	ETCS train coordination protocol using dynamic movement authorities	61
2.9	ETCS transition structure and various choices of speed regulation for train speed control	63
2.10	Application of simultaneous substitutions	65

2.11	Rule schemata of the free-variable calculus for differential dynamic logic	79
2.12	Correspondence of dynamic proof rules and transition semantics	83
2.13	Simple propositional example proof	87
2.14	Deduction modulo for analysis of MA violation in braking mode	89
2.15	Controllable region of ETCS dynamics	90
2.16	Deduction modulo for analysis of MA-safety in braking mode	90
2.17a	Wrong rearrangement with deduction modulo by invertible quantifiers	91
2.17b	Correct reintroduction order with deduction modulo by invertible quantifiers	91
2.18	Bouncing ball proof (no evolution domain)	95
2.19a	Unsound attempt of induction without universal closure \forall^α	95
2.19b	Correct use of induction with universal closure \forall^α , i.e., $\forall x$	95
2.20	Bouncing ball proof (with evolution domain)	97
2.21	Characterisation of \mathbb{N} as zeros of solutions of differential equations	103
2.22	Fractional encoding principle of \mathbb{R} -Gödel encoding by bit interleaving	105
2.23	FOD definition characterising Gödel encoding of \mathbb{R} -sequences in one real number	106
2.24	Explicit rendition of hybrid program transition semantics in FOD	107
2.25	Evolution domain checks along backwards flow over time	108
3.1	Controllability violated in the presence of disturbance	138
3.2	Differential state flow	143
3.3	Zeno system run	146
3.4	Aircraft dynamics	148
3.5	Reparametrise for differential axiomatisation	149
3.6	Flight manoeuvres for collision avoidance in air traffic control	151
3.7	Flight control with tangential roundabout collision avoidance manoeuvres	152
3.8	Vector field and a solution of a differential equation	153
3.9	Rule schemata of the proof calculus for differential-algebraic dynamic logic	164
3.10	Side deduction for quantifier elimination rules	164
3.11	Nested side deductions and differential variants for progress property	169
3.12	Differential invariants	171
3.13a	Cubic dynamics proof	172
3.13b	Cubic dynamics	172
3.14	Unsound restriction of differential invariance	173
3.15a	Restricting differential invariance	174
3.15b	Linear dynamics	174
3.16	Proof of MA-safety in braking mode with disturbance	176
3.17	Trajectory and evolution of a damped oscillator	177
3.18	Trajectory switching between two damped oscillators	178

3.19	Parametric switched damped oscillator system	178
3.20	Instable trajectory switching between two damped oscillators	179
3.21	Parametric switched damped oscillator proof	180
3.22	Differential variants	182
3.23a	Monotonically decreasing convergent counterexample	184
3.23b	Convergent descent dynamics	184
3.23c	Non-inductive property in convergent descent	184
3.24a	Counterexample of unbounded dynamics without Lipschitz continuity	184
3.24b	Explosive dynamics with limited duration of solutions	184
3.25	Differential induction splitting over disjunctions for negative equations	189
3.26a	Counterexample for disjunctive monotonicity	193
3.26b	Interrupted dynamics	193
3.27	Quadrant sign selection regions of differential invariant	196
3.28	Circular dependencies for differential strengthening	196
3.29	Tangential construction for characteristics of roundabout dynamics	198
4.1	Trace semantics of dTL formulas	214
4.2	ETCS train coordination protocol phases	216
4.3	Rule schemata of the proof calculus for temporal differential dynamic logic	218
4.4	Correspondence of temporal proof rules and trace semantics	219
4.5	Explicit rendition of hybrid program trace semantics in FOD	225
4.6	Transformation rules for alternating temporal path and trace quantifiers	229
5.1	Deductive, real algebraic, computer algebraic prover combination	236
5.2	Tableau procedure for differential dynamic logics	237
5.3	Nondeterminisms in the tableau procedure for differential dynamic logics	237
5.4	Computational distraction in quantifier elimination	240
5.5	Eager and lazy quantifier elimination in proof search space	241
5.6	A large subgoal of first-order real arithmetic during ETCS verification	242
5.7a	Proof strategy priorities	244
5.7b	Iterative background closure (IBC) proof strategy	244
5.8	Iterative background closure (IBC) algorithm schema	245
5.9	General and/or-branching in proof strategies for differential dynamic logics	245
5.10	Iterative inflation order (IIO) algorithm schema	247
6.1	d \mathcal{L} -based verification by symbolic decomposition	257
6.2	Aircraft dynamics	261
6.3	Fixed-point algorithm for differential invariants (<i>Differential Saturation</i>)	262

6.4	Differential dependencies and variable clusters of flight dynamics	264
6.5	Fixed-point algorithm for discrete loop invariants (loop saturation)	266
6.6	Hybrid program rendition of hybrid automaton for simple water tank	267
6.7	Interplay of local and global fixed-point verification loops during symbolic decomposition	268
6.8	Robustness in counterexamples	271
6.9	Flyable aircraft roundabout	272
7.1	ETCS train cooperation protocol phases and dynamic movement authorities	282
7.2	ETCS track profile	283
7.3	Formal model of parametric ETCS cooperation protocol (skeleton)	284
7.4	Transition structure of ETCS skeleton	286
7.5	Controllable region of ETCS	288
7.6	ETCS cooperation protocol refined with parameter constraints	291
7.7	Proof sketch for ETCS safety	292
7.8	Controllability region changes in the presence of disturbance	295
7.9	Proof of ETCS controllability despite disturbance	297
7.10	Parametric ETCS cooperation protocol with disturbances	299
7.11	Parametric ETCS cooperation protocol with disturbances (full in- stantiation)	300
8.1	Evolution of collision avoidance manoeuvres in air traffic control	304
8.2	Non-flyable straight-line manoeuvre with instant turns	305
8.3	Flyable aircraft roundabout	309
8.4	Flight dynamics	309
8.5	Protocol cycle and construction of flyable roundabout manoeuvre	310
8.6	Non-flyable tangential roundabout collision avoidance manoeuvre NTRM	312
8.7	Tangential configuration \mathcal{T}	313
8.8	Flyable aircraft roundabout (multiple aircraft)	314
8.9	Tangential roundabout collision avoidance manoeuvre (four aircraft)	314
8.10	Flyable entry characteristics	316
8.11	Entry separation by bounded nondeterministic overapproximation	320
8.12	Some mutually agreeable negotiation choices for aircraft	323
8.13	Far separation for mutually agreeable negotiation choices	325
8.14a	Exit ray separation	327
8.14b	Incompatible exit rays	327
8.15	Flight control with flyable tangential roundabout collision avoidance	329
8.16	Verification loop for flyable tangential roundabout manoeuvres	330
8.17	Flight control with FTRM (synchronous instantiation)	332
9.1	Topics contributing to the logical analysis of hybrid systems	336
A.1	Rule schemata of the sequent calculus for first-order logic	352
A.2a	Ground proof example	354

A.2b	Free-variable proof example	354
A.3	Wrong proof attempt in first-order logic	355
B.1	Vector field and a solution of a differential equation	360
C.1	Hybrid automaton and corresponding hybrid program	370
C.2a	Hybrid automaton for water tank	373
C.2b	Hybrid program for water tank	373
C.3	Parametric bouncing ball	374
D.1	Architecture and plug-in structure of the KeYmaera prover	378
D.2	Screenshot of the KeYmaera user interface	379
D.3	KeYmaera proof strategy options	380
D.4	Projection of semialgebraic sets and quantifier elimination	384
D.5	Rule schemata of Gröbner calculus rules	389
D.6	Some algebraic varieties generated by one polynomial equation in two variables	391
D.7	Example proof using the real Nullstellensatz	393
D.8	Rule schema of Positivstellensatz calculus rule	395
D.9	Example proof using the Positivstellensatz	395

List of Tables

2.1	Statements and effects of hybrid programs (HPs)	42
2.2	Statements and control structures definable with hybrid programs . .	44
2.3	Operators and meaning in differential dynamic logic (\mathbf{dL}) . . .	47
3.1	Comparison of DAL with DA-programs versus \mathbf{dL} with hybrid programs	127
3.2	Statements and effects of differential-algebraic programs	137
3.3	Classification of differential-algebraic programs and correspondence to dynamical systems	139
3.4	Operators and meaning in differential-algebraic dynamic logic (DAL)	140
3.5	Embedding hybrid programs as DA-programs	147
4.1	Operators and meaning in differential temporal dynamic logic (dTL)	208
5.1	Experimental results for proof strategies (with standalone QE) I . .	249
5.2	Experimental results for proof strategies (with standalone QE) II . .	249
5.3	Experimental results for proof strategies (no standalone QE) I . . .	250
5.4	Experimental results for proof strategies (no standalone QE) II . . .	250
6.1	Experimental results for differential invariants as fixed points	273
7.1	Experimental results for the European Train Control System	300
8.1	Verification loop properties for flyable tangential roundabout manoeuvres	330
8.2	Experimental results for air traffic control (initial timeout = 10s) . .	331
8.3	Experimental results for air traffic control (initial timeout = 4s) . . .	333
A.1	Intuitive meaning of logical operators in first-order logic	343

List of Theorems

L 2.1	Uniqueness	57
L 2.2	Substitution Lemma	70
L 2.3	Substitution property	75
L 2.4	Substitutions preserve validity	76
L 2.5	Quantifier elimination lifting	92
L 2.6	Coincidence lemma	93
T 2.1	Soundness of $\mathbf{d}\mathcal{L}$	98
T 2.2	Incompleteness of $\mathbf{d}\mathcal{L}$	102
T 2.3	Relative completeness of $\mathbf{d}\mathcal{L}$	104
L 2.7	\mathbb{R} -Gödel encoding	105
L 2.8	Hybrid program rendition	106
L 2.9	$\mathbf{d}\mathcal{L}$ Expressibility	108
L 2.10	Derivability of sequents	109
L 2.11	Generalisation	110
P 2.1	Relative completeness of first-order safety	111
P 2.2	Relative completeness of first-order liveness	112
T 2.4	Relatively semidecidable fragment	114
L 2.12	Uniform Skolem symbols	115
P 3.1	Conservative extension	147
L 3.1	Derivation lemma	156
L 3.2	Differential substitution property	158
L 3.3	Differential transformation principle	158
L 3.4	Differential inequality elimination	161
L 3.5	Differential equation normalisation	161
L 3.6	Differential weakening	175
L 3.7	Closure properties of differential invariants	181
T 3.1	Soundness of DAL	185
P 3.2	Open differential induction	188
P 3.3	Differential monotonicity	191
T 3.2	Relative completeness of DAL	193
P 3.4	Equational deductive power	194

T 3.3	Deductive power	194
T 3.4	Safety of tangential roundabout manoeuvre	199
P 3.5	External separation of roundabout manoeuvres	200
P 4.1	Conservative temporal extension	215
L 4.1	Trace relation	215
T 4.1	Soundness of dTL	221
T 4.2	Incompleteness of dTL	223
T 4.3	Relative completeness of dTL	224
L 4.2	Hybrid program trace rendition	225
L 4.3	dTL Expressibility	225
P 4.2	Local soundness for temporal quantifier alternation	229
P 6.1	Principle of differential induction	260
P 6.2	Differential saturation	262
P 6.3	Loop saturation	265
T 6.1	Soundness of fixed-point verification algorithm	269
L 7.1	Principle of separation by movement authorities	282
P 7.1	Controllability	288
P 7.2	RBC preserves train controllability	289
P 7.3	Reactivity of ETCS	290
P 7.4	Reactivity constraint	290
P 7.5	Safety of ETCS	291
P 7.6	Liveness of ETCS	293
T 7.1	Correctness of ETCS cooperation protocol	294
P 7.7	Controllability despite disturbance	296
P 7.8	Reactivity constraint despite disturbance	298
P 7.9	Safety despite disturbance	298
T 8.1	Safety property of flyable tangential roundabouts	331
T A.1	Soundness of FOL	356
T A.2	Completeness of FOL	356
T B.1	Existence theorem of Peano	363
T B.2	Uniqueness theorem of Picard-Lindelöf	364
P B.1	Continuation of solutions	365
P B.2	Linear systems with constant coefficients	365
P C.1	Hybrid automata embedding	371
T D.1	Tarski-Seidenberg principle	383
T D.2	Semialgebraic sets	383
T D.3	Hilbert's basis theorem	388
P D.1	Soundness of Gröbner basis rules	390
T D.4	Hilbert's Nullstellensatz	391
T D.5	Real Nullstellensatz for real-closed fields	392
T D.6	Positivstellensatz for real-closed fields	394