

Contents

| | | |
|----------|---|-----------|
| 1 | Cyber-Physical Systems: Overview | 1 |
| 1.1 | Introduction | 1 |
| 1.1.1 | Cyber-Physical Systems Analysis by Example | 2 |
| 1.1.2 | Application Domains | 2 |
| 1.1.3 | Significance | 3 |
| 1.1.4 | The Importance of Safety | 4 |
| 1.2 | Hybrid Systems versus Cyber-Physical Systems | 5 |
| 1.3 | Multi-dynamical Systems | 7 |
| 1.4 | How to Learn about Cyber-Physical Systems | 9 |
| 1.5 | Computational Thinking for Cyber-Physical Systems | 11 |
| 1.6 | Learning Objectives | 12 |
| 1.7 | Structure of This Textbook | 14 |
| 1.8 | Summary | 18 |
| | References | 18 |
| | Part I Elementary Cyber-Physical Systems | 23 |
| 2 | Differential Equations & Domains | 25 |
| 2.1 | Introduction | 25 |
| 2.2 | Differential Equations as Models of Continuous Physical Processes | 26 |
| 2.3 | The Meaning of Differential Equations | 29 |
| 2.4 | A Tiny Compendium of Differential Equation Examples | 31 |
| 2.5 | Domains of Differential Equations | 37 |
| 2.6 | Syntax of Continuous Programs | 39 |
| 2.6.1 | Continuous Programs | 39 |
| 2.6.2 | Terms | 40 |
| 2.6.3 | First-order Formulas | 41 |
| 2.7 | Semantics of Continuous Programs | 42 |
| 2.7.1 | Terms | 43 |

| | | |
|----------|--|-----------|
| 2.7.2 | First-order Formulas | 45 |
| 2.7.3 | Continuous Programs | 49 |
| 2.8 | Summary | 50 |
| 2.9 | Appendix | 50 |
| 2.9.1 | Existence Theorems | 51 |
| 2.9.2 | Uniqueness Theorems | 52 |
| 2.9.3 | Linear Differential Equations with Constant Coefficients . . | 53 |
| 2.9.4 | Continuation and Continuous Dependency | 55 |
| | Exercises | 56 |
| | References | 59 |
| 3 | Choice & Control | 61 |
| 3.1 | Introduction | 61 |
| 3.2 | A Gradual Introduction to Hybrid Programs | 63 |
| 3.2.1 | Discrete Change in Programs | 64 |
| 3.2.2 | Compositions of Programs | 64 |
| 3.2.3 | Decisions in Hybrid Programs | 66 |
| 3.2.4 | Choices in Hybrid Programs | 67 |
| 3.2.5 | Tests in Hybrid Programs | 69 |
| 3.2.6 | Repetitions in Hybrid Programs | 71 |
| 3.3 | Hybrid Programs | 73 |
| 3.3.1 | Syntax | 73 |
| 3.3.2 | Semantics | 74 |
| 3.4 | Hybrid Program Design | 78 |
| 3.4.1 | To Brake, or not to Brake, That is the Question | 79 |
| 3.4.2 | A Matter of Choice | 81 |
| 3.5 | Summary | 82 |
| 3.6 | Appendix: Modeling the Motion of a Robot Around the Bend | 83 |
| | Exercises | 85 |
| | References | 89 |
| 4 | Safety & Contracts | 93 |
| 4.1 | Introduction | 93 |
| 4.2 | A Gradual Introduction to CPS Contracts | 95 |
| 4.2.1 | The Adventures of Quantum the Bouncing Ball | 96 |
| 4.2.2 | How Quantum Discovered a Crack in the Fabric of Time . . | 99 |
| 4.2.3 | How Quantum Learned to Deflate | 101 |
| 4.2.4 | Postcondition Contracts for CPS | 102 |
| 4.2.5 | Precondition Contracts for CPS | 104 |
| 4.3 | Logical Formulas for Hybrid Programs | 104 |
| 4.4 | Differential Dynamic Logic | 108 |
| 4.4.1 | Syntax | 108 |
| 4.4.2 | Semantics | 110 |
| 4.5 | CPS Contracts in Logic | 113 |
| 4.6 | Identifying Requirements of a CPS | 116 |

| | | |
|----------|--|------------|
| 4.7 | Summary | 121 |
| 4.8 | Appendix | 121 |
| 4.8.1 | Intermediate Conditions for a Proof of Sequential Compositions | 122 |
| 4.8.2 | A Proof of Choice | 124 |
| 4.8.3 | A Proof of Tests | 125 |
| | Exercises | 127 |
| | References | 131 |
| 5 | Dynamical Systems & Dynamic Axioms | 135 |
| 5.1 | Introduction | 135 |
| 5.2 | Intermediate Conditions for CPS | 138 |
| 5.3 | Dynamic Axioms for Dynamical Systems | 140 |
| 5.3.1 | Nondeterministic Choices | 140 |
| 5.3.2 | Soundness of Axioms | 143 |
| 5.3.3 | Assignments | 144 |
| 5.3.4 | Differential Equations | 145 |
| 5.3.5 | Tests | 149 |
| 5.3.6 | Sequential Compositions | 150 |
| 5.3.7 | Loops | 153 |
| 5.3.8 | Diamonds | 154 |
| 5.4 | A Proof of a Short Bouncing Ball | 155 |
| 5.5 | Summary | 157 |
| 5.6 | Appendix | 158 |
| 5.6.1 | Modal Modus Ponens has Implications on Boxes | 158 |
| 5.6.2 | Vacuous State Change If Nothing Relevant Ever Changes | 159 |
| 5.6.3 | Gödel Generalizes Validities into Boxes | 160 |
| 5.6.4 | Monotonicity of Postconditions | 161 |
| 5.6.5 | Of Free and Bound Variables | 162 |
| 5.6.6 | Free and Bound Variable Analysis | 163 |
| | Exercises | 166 |
| | References | 169 |
| 6 | Truth & Proof | 171 |
| 6.1 | Introduction | 171 |
| 6.2 | Truth and Proof | 173 |
| 6.2.1 | Sequents | 175 |
| 6.2.2 | Proofs | 177 |
| 6.2.3 | Propositional Proof Rules | 178 |
| 6.2.4 | Soundness of Proof Rules | 183 |
| 6.2.5 | Proofs with Dynamics | 185 |
| 6.2.6 | Quantifier Proof Rules | 188 |
| 6.3 | Derived Proof Rules | 190 |
| 6.4 | A Sequent Proof for the Single-Hop Bouncing Ball | 191 |
| 6.5 | Real Arithmetic | 193 |

| | | |
|----------|---|------------|
| 6.5.1 | Real Quantifier Elimination | 194 |
| 6.5.2 | Instantiating Real Arithmetic Quantifiers | 198 |
| 6.5.3 | Weakening Real Arithmetic by Removing Assumptions | 199 |
| 6.5.4 | Structural Proof Rules in Sequent Calculus | 200 |
| 6.5.5 | Substituting Equations Into Formulas | 201 |
| 6.5.6 | Abbreviating Terms to Reduce Complexity | 202 |
| 6.5.7 | Creatively Cutting Real Arithmetic to Transform Questions | 203 |
| 6.6 | Summary | 204 |
| | Exercises | 204 |
| | References | 207 |
| 7 | Control Loops & Invariants | 211 |
| 7.1 | Introduction | 211 |
| 7.2 | Control Loops | 213 |
| 7.3 | Induction for Loops | 215 |
| 7.3.1 | Induction Axioms for Loops | 215 |
| 7.3.2 | Induction Rule for Loops | 217 |
| 7.3.3 | Loop Invariants | 220 |
| 7.3.4 | Contextual Soundness Requirements | 223 |
| 7.4 | A Proof of a Happily Repetitive Bouncing Ball | 225 |
| 7.5 | Splitting Postconditions into Separate Cases | 230 |
| 7.6 | Summary | 232 |
| 7.7 | Appendix | 233 |
| 7.7.1 | Loops of Proofs | 233 |
| 7.7.2 | Breaking Loops of Proofs | 235 |
| 7.7.3 | Invariant Proofs of Loops | 238 |
| 7.7.4 | Alternative Forms of the Induction Axiom | 239 |
| | Exercises | 241 |
| | References | 243 |
| 8 | Events & Responses | 245 |
| 8.1 | Introduction | 245 |
| 8.2 | The Need for Control | 247 |
| 8.2.1 | Events in Control | 248 |
| 8.2.2 | Event Detection | 250 |
| 8.2.3 | Dividing Up the World | 255 |
| 8.2.4 | Event Firing | 259 |
| 8.2.5 | Event-Triggered Verification | 260 |
| 8.2.6 | Event-Triggered Control Paradigm | 261 |
| 8.2.7 | Physics versus Control Distinctions | 262 |
| 8.3 | Summary | 263 |
| | Exercises | 264 |
| | References | 265 |

| | |
|---|------------|
| 9 Reactions & Delays | 267 |
| 9.1 Introduction | 267 |
| 9.2 Delays in Control | 269 |
| 9.2.1 The Impact of Delays on Event Detection | 272 |
| 9.2.2 Model-predictive Control Basics | 273 |
| 9.2.3 Design-by-Invariant | 274 |
| 9.2.4 Sequencing and Prioritizing Reactions | 276 |
| 9.2.5 Time-triggered Verification | 279 |
| 9.3 Summary | 280 |
| Exercises | 282 |
| References | 284 |

Part II Differential Equations Analysis **285**

| | |
|---|------------|
| 10 Differential Equations & Differential Invariants | 287 |
| 10.1 Introduction | 287 |
| 10.2 A Gradual Introduction to Differential Invariants | 289 |
| 10.2.1 Global Descriptive Power of Local Differential Equations | 290 |
| 10.2.2 Intuition for Differential Invariants | 291 |
| 10.2.3 Deriving Differential Invariants | 293 |
| 10.3 Differentials | 295 |
| 10.3.1 Syntax | 295 |
| 10.3.2 Semantics of Differential Symbols | 296 |
| 10.3.3 Semantics of Differential Terms | 299 |
| 10.3.4 Derivation Lemma with Equations of Differentials | 301 |
| 10.3.5 Differential Lemma | 303 |
| 10.3.6 Differential Invariant Term Axiom | 304 |
| 10.3.7 Differential Substitution Lemmas | 306 |
| 10.4 Differential Invariant Terms | 308 |
| 10.5 A Differential Invariant Proof by Generalization | 309 |
| 10.6 Example Proofs | 310 |
| 10.7 Summary | 313 |
| 10.8 Appendix | 314 |
| 10.8.1 Differential Equations vs. Loops | 314 |
| 10.8.2 Differential Invariant Terms and Invariant Functions | 316 |
| Exercises | 319 |
| References | 320 |

| | |
|--|------------|
| 11 Differential Equations & Proofs | 323 |
| 11.1 Introduction | 323 |
| 11.2 Recap: Ingredients for Differential Equation Proofs | 325 |
| 11.3 Differential Weakening | 327 |
| 11.4 Operators in Differential Invariants | 329 |
| 11.4.1 Equational Differential Invariants | 329 |

| | | |
|-----------|---|------------|
| 11.4.2 | Differential Invariant Proof Rule | 331 |
| 11.4.3 | Differential Invariant Inequalities | 333 |
| 11.4.4 | Disequational Differential Invariants | 335 |
| 11.4.5 | Conjunctive Differential Invariants | 336 |
| 11.4.6 | Disjunctive Differential Invariants | 338 |
| 11.5 | Differential Invariants | 340 |
| 11.6 | Example Proofs | 342 |
| 11.7 | Assuming Invariants | 343 |
| 11.8 | Differential Cuts | 347 |
| 11.9 | Differential Weakening Again | 350 |
| 11.10 | Differential Invariants for Solvable Differential Equations | 351 |
| 11.11 | Summary | 353 |
| 11.12 | Appendix: Proving Aerodynamic Bouncing Balls | 354 |
| | Exercises | 358 |
| | References | 360 |
| 12 | Ghosts & Differential Ghosts | 363 |
| 12.1 | Introduction | 363 |
| 12.2 | Recap | 366 |
| 12.3 | A Gradual Introduction to Ghost Variables | 366 |
| 12.3.1 | Discrete Ghosts | 366 |
| 12.3.2 | Proving Bouncing Balls with Sneaky Solutions | 368 |
| 12.3.3 | Differential Ghosts of Time | 374 |
| 12.3.4 | Constructing Differential Ghosts | 375 |
| 12.4 | Differential Ghosts | 378 |
| 12.5 | Substitute Ghosts | 383 |
| 12.6 | Limit Velocity of an Aerodynamic Ball | 384 |
| 12.7 | Axiomatic Ghosts | 387 |
| 12.8 | Summary | 389 |
| 12.9 | Appendix | 389 |
| 12.9.1 | Arithmetic Ghosts | 389 |
| 12.9.2 | Nondeterministic Assignments & Ghosts of Choice | 390 |
| 12.9.3 | Differential-algebraic Ghosts | 392 |
| | Exercises | 394 |
| | References | 395 |
| 13 | Differential Invariants & Proof Theory | 397 |
| 13.1 | Introduction | 397 |
| 13.2 | Recap | 400 |
| 13.3 | Comparative Deductive Study: Relativity Theory for Proofs | 401 |
| 13.4 | Equivalences of Differential Invariants | 402 |
| 13.5 | Differential Invariants & Arithmetic | 403 |
| 13.6 | Differential Invariant Equations | 405 |
| 13.7 | Equational Incompleteness | 407 |
| 13.8 | Strict Differential Invariant Inequalities | 410 |

13.9 Differential Invariant Equations as Differential Invariant Inequalities 412
 13.10 Differential Invariant Atoms 413
 13.11 Summary 414
 13.12 Appendix: Curves Playing with Norms and Degrees 414
 Exercises 416
 References 416

Part III Adversarial Cyber-Physical Systems 419

14 Hybrid Systems & Games 421
 14.1 Introduction 421
 14.2 A Gradual Introduction to Hybrid Games 425
 14.2.1 Choices & Nondeterminism 425
 14.2.2 Control & Dual Control 426
 14.2.3 Demon’s Derived Controls 427
 14.3 Syntax of Differential Game Logic 428
 14.3.1 Hybrid Games 428
 14.3.2 Differential Game Logic Formulas 432
 14.3.3 Examples 433
 14.4 An Informal Operational Game Tree Semantics 439
 14.5 Summary 443
 Exercises 444
 References 447

15 Winning Strategies & Regions 449
 15.1 Introduction 449
 15.2 Semantics of Differential Game Logic 451
 15.2.1 Limits of Reachability Relations 451
 15.2.2 Set-valued Semantics of Differential Game Logic Formulas 452
 15.2.3 Winning Region Semantics of Hybrid Games 453
 15.3 Semantics of Repetition in Hybrid Games 458
 15.3.1 Repetitions with Advance Notice 458
 15.3.2 Repetitions as Infinite Iterations 460
 15.3.3 Inflationary Semantics of Repetition 465
 15.3.4 Characterizing Winning Repetitions Implicitly 468
 15.4 Semantics of Hybrid Games 473
 15.5 Summary 476
 Exercises 476
 References 478

16 Winning & Proving Hybrid Games 479
 16.1 Introduction 479
 16.2 Semantical Considerations 481
 16.2.1 Recap: Semantics of Hybrid Games 481
 16.2.2 Monotonicity 483

| | | |
|----------------|---|------------|
| 16.2.3 | Determinacy | 484 |
| 16.3 | Dynamic Axioms for Hybrid Games | 485 |
| 16.3.1 | Determinacy | 486 |
| 16.3.2 | Monotonicity | 486 |
| 16.3.3 | Assignments | 488 |
| 16.3.4 | Differential Equations | 488 |
| 16.3.5 | Challenge Games | 489 |
| 16.3.6 | Choice Games | 490 |
| 16.3.7 | Sequential Games | 491 |
| 16.3.8 | Dual Games | 492 |
| 16.3.9 | Repetition Games | 494 |
| 16.3.10 | Proof Rules for Repetition Games | 496 |
| 16.4 | Example Proofs | 497 |
| 16.5 | Axiomatization | 500 |
| 16.5.1 | Soundness | 501 |
| 16.5.2 | Completeness | 503 |
| 16.6 | There and Back Again Game | 505 |
| 16.7 | Summary | 506 |
| | Exercises | 506 |
| | References | 508 |
| 17 | Game Proofs & Separations | 511 |
| 17.1 | Introduction | 511 |
| 17.2 | Recap: Hybrid Games | 512 |
| 17.3 | Separating Axioms | 513 |
| 17.4 | Repetitive Diamonds – Convergence vs. Iteration | 518 |
| 17.5 | Summary | 522 |
| 17.6 | Appendix: Relating Differential Game Logic and Differential Dynamic Logic | 522 |
| | Exercises | 524 |
| | References | 524 |
| Part IV | Comprehensive CPS Correctness | 525 |
| 18 | Axioms & Uniform Substitutions | 527 |
| 18.1 | Introduction | 527 |
| 18.2 | Axioms versus Axiom Schemata | 530 |
| 18.3 | What Axioms Want | 532 |
| 18.4 | Differential Dynamic Logic with Interpretations | 535 |
| 18.4.1 | Syntax | 535 |
| 18.4.2 | Semantics | 536 |
| 18.5 | Uniform Substitution | 538 |
| 18.5.1 | Uniform Substitution Rule | 539 |
| 18.5.2 | Examples | 541 |

| | | |
|-----------|--|------------|
| 18.5.3 | Uniform Substitution Application | 543 |
| 18.5.4 | Uniform Substitution Lemmas | 547 |
| 18.5.5 | Soundness | 548 |
| 18.6 | Axiomatic Proof Calculus for dL | 550 |
| 18.7 | Differential Axioms | 550 |
| 18.8 | Summary | 552 |
| | Exercises | 553 |
| | References | 554 |
| 19 | Verified Models & Verified Runtime Validation | 557 |
| 19.1 | Introduction | 557 |
| 19.2 | Fundamental Challenges with Inevitable Models | 560 |
| 19.3 | Runtime Monitors | 562 |
| 19.4 | Model Compliance | 564 |
| 19.5 | Provably Correct Monitor Synthesis | 568 |
| 19.5.1 | Logical State Relations | 569 |
| 19.5.2 | Model Monitors | 570 |
| 19.5.3 | Correct-by-Construction Synthesis | 571 |
| 19.6 | Summary | 573 |
| | Exercises | 574 |
| | References | 574 |
| 20 | Virtual Substitution & Real Equations | 577 |
| 20.1 | Introduction | 577 |
| 20.2 | Framing the Miracle | 580 |
| 20.3 | Quantifier Elimination | 583 |
| 20.3.1 | Homomorphic Normalization for Quantifier Elimination | 585 |
| 20.3.2 | Substitution Base | 587 |
| 20.3.3 | Term Substitutions for Linear Equations | 589 |
| 20.4 | Square Root $\sqrt{\cdot}$ Virtual Substitutions for Quadratics | 591 |
| 20.4.1 | Square Root Algebra | 593 |
| 20.4.2 | Virtual Substitutions of Square Roots | 595 |
| 20.5 | Optimizations | 599 |
| 20.6 | Summary | 600 |
| 20.7 | Appendix: Real Algebraic Geometry | 601 |
| | Exercises | 601 |
| | References | 603 |
| 21 | Virtual Substitution & Real Arithmetic | 607 |
| 21.1 | Introduction | 607 |
| 21.2 | Recap: Square Root $\sqrt{\cdot}$ Virtual Substitutions for Quadratics | 609 |
| 21.3 | Infinity ∞ Virtual Substitution | 609 |
| 21.4 | Infinitesimal ε Virtual Substitution | 614 |
| 21.5 | Quantifier Elimination by Virtual Substitution for Quadratics | 619 |
| 21.6 | Optimizations | 623 |

| | |
|---|------------|
| 21.7 Summary | 624 |
| 21.8 Appendix: Semialgebraic Geometry | 625 |
| Exercises | 626 |
| References | 627 |
| Index | 629 |
| Operators & Axioms | 635 |

List of Figures

| | | |
|------|--|----|
| 1.1 | Airplane example: Which control decisions are safe for aircraft collision avoidance? | 2 |
| 1.2 | Multi-dynamical systems aspects of CPS | 7 |
| 1.3 | Dependencies and suggested reading sequences of the chapters . . . | 17 |
| 2.1 | Vector field with one solution of a differential equation | 27 |
| 2.2 | Vector field with one solution of accelerated straight-line motion . | 28 |
| 2.3 | Discretizations of differential equations with a discretization time step | 29 |
| 2.4 | Differential equation solution condition | 30 |
| 2.5 | Constant differential equation | 31 |
| 2.6 | Linear differential equation | 31 |
| 2.7 | A solution of the rotational differential equations | 34 |
| 2.8 | Another solution of the rotational differential equations with initial values 1 | 34 |
| 2.9 | A faster solution of the rotational differential equations with initial values 1 | 35 |
| 2.10 | A solution of the time square oscillator and the damped oscillator . | 36 |
| 2.11 | System $x' = f(x) \& Q$ follows the differential equation $x' = f(x)$ for any duration but cannot leave evolution domain Q | 39 |
| 2.12 | Illustration of the dynamics of continuous programs | 50 |
| 3.1 | An illustration of the behavior of an instantaneous discrete change . | 64 |
| 3.2 | Fixed acceleration, velocity, and position change over time | 65 |
| 3.3 | Acceleration, velocity, and position change over time | 66 |
| 3.4 | Transition semantics and example dynamics of hybrid programs . . | 76 |
| 3.5 | Nested transition semantics pattern for $(\alpha; \beta)^*$ | 78 |
| 3.6 | Nested transition semantics pattern for $(\alpha \cup \beta)^*$ | 79 |
| 3.7 | Transition structure of the acceleration/braking example | 80 |
| 3.8 | Illustration of a Dubins path consisting of a sequence of lines and maximally curved circle segments | 83 |

| | | |
|------|--|-----|
| 3.9 | Illustration of the Dubins dynamics of a point (x,y) moving into direction (v,w) along a dashed curve with angular velocity ω . . . | 84 |
| 3.10 | Hybrid automaton for a car that can accelerate or brake | 88 |
| 4.1 | Sample trajectory of a bouncing ball | 96 |
| 4.2 | Sample trajectory of a bouncing ball with a crack in the floor . . . | 99 |
| 4.3 | Sample trajectory of a bouncing ball over its hybrid time domain . | 100 |
| 4.4 | Hybrid time domain for the sample trajectory of a bouncing ball . . | 101 |
| 4.5 | Sample trajectory of a bouncing ball that ultimately lies down flat . | 102 |
| 4.6 | Transition semantics of modalities in dL formulas | 112 |
| 4.7 | Sample trajectory of a bouncing ball in an anti-gravity field | 116 |
| 4.8 | Sample trajectory of a bouncing ball with anti-damping | 118 |
| 4.9 | Sample trajectory of a bouncing ball with upwards initial velocity . | 118 |
| 4.10 | Sample trajectory of a bouncing ball dribbling with fast initial velocity | 119 |
| 5.1 | Sample trajectory of a single-hop bouncing ball | 138 |
| 5.2 | Intermediate conditions for sequential compositions | 140 |
| 5.3 | Illustration of dynamic axiom for sequential compositions | 152 |
| 5.4 | Summary of sound differential dynamic logic axioms from this chapter | 158 |
| 5.5 | Additional axioms and proof rules for hybrid systems | 169 |
| 6.1 | Propositional proof rules of sequent calculus | 178 |
| 6.2 | A simple propositional example proof in sequent calculus | 182 |
| 6.3 | A simple dynamics example proof in sequent calculus | 187 |
| 6.4 | Quantifier sequent calculus proof rules | 188 |
| 6.5 | Proof rules of the dL sequent calculus considered in this chapter . . | 205 |
| 7.1 | Successively using induction axiom I at each state reached after running iterations of α^* | 218 |
| 7.2 | Sequent calculus proof shape for bouncing ball | 226 |
| 7.3 | Sequent calculus proof for bouncing ball with split | 231 |
| 7.4 | Summary of proof rules for loops, generalization, monotonicity, and splitting boxes | 232 |
| 7.5 | Loops of proofs: iterating and splitting the box | 234 |
| 7.6 | Loops of proofs: iterating & generalizing the box | 236 |
| 7.7 | Loops of proofs: intermediate generalizations | 238 |
| 7.8 | Derivation of backwards unwinding axiom from alternative induction axiom | 240 |
| 8.1 | Sample trajectory of a bouncing ball bouncing freely | 248 |
| 8.2 | Sample trajectory of a ping pong ball | 249 |
| 8.3 | Sample trajectory of a ping pong ball which misses one event . . . | 250 |
| 8.4 | Sample trajectory of a ping pong ball, sometimes actuating early, sometimes late | 252 |

| | | |
|-------|--|-----|
| 8.5 | Sample trajectory of a ping pong ball with the controller firing multiple times for the same event | 258 |
| 8.6 | Sample trajectory of a ping pong ball with the controller firing multiple times for the same event on the event boundary | 258 |
| 9.1 | Sample trajectory of a ping pong ball, sometimes actuating early, sometimes late | 270 |
| 9.2 | Sample trajectory of a time-triggered ping pong ball missing the first event | 272 |
| 9.3 | Sample trajectory of a time-triggered ping pong ball missing different events with different sampling periods | 274 |
| 9.4 | Sample trajectory of a time-triggered ping pong ball failing to control on the ground | 276 |
| 9.5 | Sample trajectory of a time-triggered ping pong ball stuck on the ground | 277 |
| 10.1 | Vector field and one solution of a differential equation that does not enter the unsafe regions | 292 |
| 10.2 | One scenario for the rotational dynamics and relationship of a direction vector to the radius and angle | 293 |
| 10.3 | Differential invariant remains true in the direction of the dynamics . | 294 |
| 10.4 | Semantics of differential symbol x' along differential equation . . . | 299 |
| 10.5 | Differential form semantics of differentials: their value depends on the point as well as on the direction of the vector field at that point . | 301 |
| 10.6 | Differential invariant (illustrated in thick red) of the indicated dynamics | 311 |
| 10.7 | Two differential invariants of the indicated dynamics | 312 |
| 10.8 | Two differential invariants of the indicated dynamics for the Motzkin polynomial | 312 |
| 10.9 | Axioms for differential invariant terms of differential equations without solutions | 314 |
| 11.1 | Illustration for differential weakening axiom DW | 328 |
| 11.2 | Equal rate of change from equal initial value (drawn slightly apart for visualization) | 330 |
| 11.3 | Differential invariant for safety | 332 |
| 11.4 | Less or equal rate of change from less or equal initial value | 333 |
| 11.5 | Cubic dynamics proof | 334 |
| 11.6 | Cubic dynamics | 334 |
| 11.7 | Less or equal rate of change from lesser initial value | 335 |
| 11.8a | Unsound attempt of using disequalities | 336 |
| 11.8b | Linear evolution | 336 |
| 11.9 | Different rate of change from different initial value do not prove anything | 336 |
| 11.10 | Soundness proof for conjunctive differential invariant axiom | 337 |

| | | |
|-------|---|-----|
| 11.11 | Differential invariant proof for bouncing ball in gravity | 338 |
| 11.12 | Soundness proof for disjunctive differential invariant axiom | 339 |
| 11.13 | Damped oscillator time trajectory and invariant in phase space | 343 |
| 11.14 | Illustration of the Dubins dynamics of a point (x, y) moving into direction (v, w) along a dashed curve with angular velocity ω | 343 |
| 11.15 | If the solution of the differential equation can never leave region C and enter the red region $\neg C$, then this unreachable region $\neg C$ can be cut out of the state space without changing the dynamics of the system. | 348 |
| 11.16 | Trajectory with vector field and evolution of an increasingly damped oscillator | 348 |
| 11.17 | Differential cut proof for the increasingly damped oscillator | 349 |
| 11.18 | If the solution of the differential equation can never leave region D and enter the region $\neg D$, then this unreachable region $\neg D$ can also be cut out of the state space without changing the dynamics of the system. | 350 |
| 11.19 | Axioms and proof rules for differential invariants and differential cuts of differential equations | 353 |
| 12.1 | Exponential decay along $x' = -x$ always makes matters worse for $x > 0$ | 376 |
| 12.2 | Differential ghost y as counterweight for exponential decay along $x' = -x$ | 378 |
| 12.3 | Explosive differential ghosts that do not exist long enough would unsoundly limit the duration of solutions | 379 |
| 12.4 | Differential ghost y to balance for exponential growth along $x' = x$ | 381 |
| 12.5 | Differential ghost y as counterweight for square resistance along $x' = -x^2$ | 383 |
| 12.6 | Velocity of aerodynamic ball approaches limit velocity | 386 |
| 12.7 | Dubins aircraft dynamics illustration | 387 |
| 12.8 | Reparametrize for differential axiomatization | 388 |
| 12.9 | Axioms and proof rules for ghosts and differential ghosts | 389 |
| 12.10 | Axioms for nondeterministic assignments | 391 |
| 13.1 | Equivalent solutions with quite different differential structure | 405 |
| 13.2 | Differential invariance chart | 414 |
| 13.3 | Illustration of p -norm inclusions | 416 |
| 14.1 | Turning hybrid game α into the dual hybrid game α^d corresponds to turning a chessboard around by 180° so that the players control the choices in α^d that the opponent has in α | 427 |
| 14.2 | Angel and Demon accelerating or braking by a and d , respectively, the cart at position x that is moving with velocity x | 431 |
| 14.3 | Velocities and accelerations of two robots on a one-dimensional planet | 435 |

| | | |
|-------|--|-----|
| 14.4 | Goalie in robot soccer moves and, if within radius 1, can capture the ball | 438 |
| 14.5 | Operational game semantics for hybrid games of dGL | 440 |
| 14.6 | The filibuster game formula looks like it might be non-determined and not have a truth-value | 442 |
| 15.1 | Illustration of denotational semantics of hybrid games as Angel's winning regions | 456 |
| 15.2 | Illustration of denotational semantics of hybrid games as Demon's winning regions | 457 |
| 15.3 | Monotonicity: it is easier to win into larger sets of winning states $Y \supseteq X$ | 457 |
| 15.4 | Game trees for $x = 1 \wedge a = 1 \rightarrow \langle (x := a; a := 0) \cap x := 0 \rangle^* x \neq 1$ | 459 |
| 15.5 | Iteration $\zeta_\alpha^n(X)$ of $\zeta_\alpha(\cdot)$ from winning condition X | 461 |
| 15.6 | Winning regions $\zeta_\alpha(Z)$ of sets $Z \subseteq \zeta_{\alpha^*}(X)$ are already included in $\zeta_{\alpha^*}(X)$ since $\zeta_\alpha(Z)$ is just one more round away from Z | 463 |
| 15.7 | Iteration $\zeta_\alpha^{\omega+1}(X)$ of $\zeta_\alpha(\cdot)$ from winning condition $X = [0, 1)$ stops when applying $\zeta_\alpha(\cdot)$ to the ω th infinite iteration $\zeta_\alpha^\omega(X)$ | 464 |
| 15.8 | Illustration of infinitely many ordinals up to ω^ω | 465 |
| 15.9 | Transfinite iteration $\zeta_\alpha^\infty(X)$ of $\zeta_\alpha(\cdot)$ from winning condition X results in winning region $\zeta_{\alpha^*}(X)$ of repetition. | 466 |
| 15.10 | Illustration of denotational semantics of winning region of hybrid game repetitions | 472 |
| 16.1 | Proof of the two robot dance | 499 |
| 16.2 | Differential game logic axiomatization | 500 |
| 16.3 | “There and back again game” | 505 |
| 16.4 | Differential game logic derived axioms for box modalities | 507 |
| 16.5 | Differential game logic derived axioms for Demon's controls | 507 |
| 16.6 | More hybrid system axioms, some of which are sound for hybrid games | 508 |
| 17.1 | Differential game logic axiomatization | 514 |
| 17.2 | Separating axioms sound for hybrid systems but not for hybrid games | 515 |
| 17.3 | dGL Angel proof for non-game system Example 17.1 $x \geq 0 \rightarrow \langle (x := x - 1)^* \rangle 0 \leq x < 1$ | 520 |
| 17.4 | dGL Angel proof for choice game Example 17.2 $x = 1 \wedge a = 1 \rightarrow \langle (x := a; a := 0 \cap x := 0)^* \rangle x \neq 1$ | 521 |
| 17.5 | dGL Angel proof for 2-Nim-type game Example 17.3 $x \geq 0 \rightarrow \langle (x := x - 1 \cap x := x - 2)^* \rangle 0 \leq x < 2$ | 521 |
| 17.6 | dGL Angel proof for hybrid game Example 17.4 $\langle (x := 1; x' = 1^d \cup x := x - 1)^* \rangle 0 \leq x < 1$ | 522 |
| 18.1 | Recursive application of uniform substitution σ | 544 |
| 18.2 | Differential dynamic logic axioms and proof rules | 549 |
| 18.3 | Differential equation axioms and differential axioms | 551 |

| | | |
|------|--|-----|
| 19.1 | ModelPlex monitors sit in between controller and actuator to check controller's decisions for compliance with the model based on sensor data with veto leading to a safe fallback action | 563 |
| 19.2 | Use of ModelPlex monitors along a system run | 564 |
| 19.3 | Sample run of a bouncing ball (plotted as height over time) that ultimately lies down flat | 566 |
| 20.1 | The geometric counterpart of quantifier elimination for $\exists y$ is projection onto the x axis | 585 |
| 20.2 | Roots of different quadratic functions p | 591 |
| 20.3 | Polynomial equations describe (real) affine (algebraic) varieties . . | 602 |
| 21.1 | Illustration of the value of different quadratic functions p where $p_{\bar{x}}^{-\infty} \equiv true$ | 612 |
| 21.2 | Illustration of the sign after the second root for quadratic functions p | 617 |
| 21.3 | Illustration of roots e and infinitesimal offsets $e + \varepsilon$ checked by virtual substitution | 621 |
| 21.4 | Systems of polynomial inequalities describe semialgebraic sets . . | 626 |

List of Tables

| | | |
|------|---|-----|
| 2.1 | Operators and meaning in first-order logic of real arithmetic (FOL) . . . | 51 |
| 3.1 | Statements and effects of hybrid programs (HPs) | 82 |
| 3.2 | Classification of hybrid programs and correspondence to dynamical systems | 87 |
| 4.1 | Operators and (informal) meaning in differential dynamic logic (dL) | 121 |
| 10.1 | Correspondence map between loops and differential equations . . . | 316 |
| 14.1 | Operators and (informal) meaning in differential game logic (dGL) . | 443 |
| 14.2 | Statements and effects of hybrid games (HGs) | 443 |
| 20.1 | Overview of decidability notions (e.g. for the validity problem) . . . | 581 |
| 20.2 | The miracle of reals: Overview of validity problems of first-order logics | 582 |

List of Theorems

| | | |
|--------|--|-----|
| T 2.1 | Peano's existence theorem | 51 |
| T 2.2 | Picard-Lindelöf's uniqueness theorem | 53 |
| P 2.1 | Linear differential equations with constant coefficients | 53 |
| P 2.2 | Continuation of solutions | 55 |
| P 2.3 | Lipschitz estimation | 56 |
| L 5.1 | [U] axiom of nondeterministic choice | 142 |
| L 5.2 | [:=] assignment axiom | 145 |
| L 5.3 | ['] solution axiom | 146 |
| L 5.4 | ['] solution with domains axiom | 147 |
| L 5.5 | [?] test axiom | 149 |
| L 5.6 | [:] composition axiom | 151 |
| L 5.7 | [*] iteration axiom | 153 |
| L 5.8 | ⟨·⟩ duality axiom | 155 |
| T 5.1 | Soundness | 157 |
| L 5.9 | K modal modus ponens axiom | 159 |
| L 5.10 | [∧] boxes distribute over conjunctions | 159 |
| L 5.11 | V vacuous axiom | 160 |
| L 5.12 | G Gödel generalization rule | 160 |
| L 5.13 | M[·] monotonicity rule | 161 |
| L 6.1 | ∧R conjunction rule | 183 |
| T 6.1 | Soundness | 184 |
| L 6.2 | Contextual equivalence | 186 |
| L 6.3 | ℝ Real arithmetic | 193 |
| T 6.2 | Tarski's quantifier elimination | 195 |
| L 6.4 | i∀ reintroducing universal quantifiers | 196 |
| L 6.5 | [:=]= equational assignment rule | 202 |
| T 6.1 | Soundness | 204 |
| L 5.7 | [*] iteration axiom | 216 |
| L 7.2 | I induction axiom | 217 |
| L 5.12 | G Gödel generalization rule | 217 |
| L 7.4 | ind induction rule | 218 |

| | | |
|---------|---|-----|
| L 5.13 | M[.] monotonicity rule | 220 |
| L 7.6 | loop invariant rule | 221 |
| P 7.1 | Quantum is safe | 229 |
| L 5.10 | $\Box\wedge$ boxes distribute over conjunctions | 231 |
| L 5.11 | V vacuous axiom | 231 |
| L 7.9 | MR monotonicity right rule | 237 |
| L 7.10 | $\overleftarrow{[*]}$ backwards iteration axiom | 239 |
| L 7.11 | $[**]$ double iteration axiom | 240 |
| P 8.1 | Event-triggered ping pong is safe | 263 |
| P 9.1 | Time-triggered ping pong is safe | 280 |
| L 10.1 | Derivation lemma | 302 |
| L 10.2 | Differential lemma | 303 |
| L 10.3 | Differential invariant term axiom | 304 |
| L 10.4 | Differential assignment | 306 |
| L 10.5 | DE differential effect axiom | 306 |
| L 10.6 | Differential invariant term rule | 308 |
| T 10.1 | Lie's characterization of invariant terms | 318 |
| L 10.1 | Derivation lemma | 326 |
| L 10.2 | Differential lemma | 327 |
| L 10.4 | Differential assignment | 327 |
| L 10.5 | DE differential effect axiom | 327 |
| L 11.5 | DW differential weakening axiom | 327 |
| L 11.6 | dW differential weakening proof rule | 328 |
| L 11.7 | dI differential invariant proof rule | 331 |
| L 5.10 | $\Box\wedge$ boxes distribute over conjunctions | 337 |
| L 11.9 | DI differential invariant axiom | 340 |
| L 11.7 | dI differential invariant proof rule | 340 |
| L 11.11 | dC differential cut proof rule | 347 |
| P 11.1 | Increasingly damped oscillation | 348 |
| L 11.12 | DC differential cut axiom | 349 |
| P 11.2 | Aerodynamic Quantum is safe | 357 |
| L 12.1 | iG discrete ghost rule | 367 |
| L 6.5 | $[:=]=$ equational assignment rule | 368 |
| L 12.3 | DG differential ghost axiom | 379 |
| L 12.4 | dG differential ghost rule | 380 |
| L 12.5 | dA differential auxiliaries rule | 380 |
| P 12.1 | Aerodynamic velocity limits | 386 |
| L 13.1 | Differential invariants and propositional logic | 402 |
| L 13.2 | Differential invariants and arithmetic | 403 |
| P 13.1 | Equational deductive power | 406 |
| P 13.2 | Equational incompleteness | 407 |
| P 13.3 | Strict barrier incompleteness | 410 |
| P 13.4 | Equational definability | 412 |
| T 13.1 | Atomic incompleteness | 413 |
| L 15.1 | Monotonicity | 456 |

| | | |
|---------|--|-----|
| L 15.2 | Intersection closure | 471 |
| L 15.3 | Transfinite inflation leads to a least fixpoint | 473 |
| L 15.1 | Monotonicity | 483 |
| T 16.1 | Consistency & determinacy | 485 |
| L 16.2 | [·] determinacy axiom | 486 |
| L 16.3 | M monotonicity rule | 487 |
| L 16.4 | $\langle := \rangle$ assignment axiom | 488 |
| L 16.5 | $\langle \prime \rangle$ solution axiom | 488 |
| L 16.6 | $\langle \prime \rangle$ solution with domains axiom | 489 |
| L 16.7 | $\langle ? \rangle$ test axiom | 490 |
| L 16.8 | $\langle \cup \rangle$ axiom of choice | 491 |
| L 16.9 | $\langle ; \rangle$ composition axiom | 492 |
| L 16.10 | $\langle ^d \rangle$ duality axiom | 493 |
| L 16.11 | $\langle * \rangle$ iteration axiom | 495 |
| L 16.12 | FP fixpoint rule | 496 |
| P 16.1 | Push-around carts are safe | 498 |
| P 16.2 | Robot dance is safe | 499 |
| T 16.2 | Soundness of dGL | 502 |
| T 16.3 | Relative completeness of dGL | 504 |
| L 16.13 | Evolution domain reduction | 505 |
| T 16.1 | Consistency & determinacy | 513 |
| L 18.1 | V vacuous axiom | 538 |
| L 18.2 | $[:=]$ assignment axiom | 538 |
| T 18.1 | Uniform substitution | 539 |
| L 18.3 | Uniform substitution for formulas | 548 |
| T 18.1 | Uniform substitution | 548 |
| P 19.1 | Correct bouncing ball model monitor | 571 |
| T 6.2 | Tarski's quantifier elimination | 584 |
| T 20.2 | Virtual substitution of linear equations | 590 |
| L 20.1 | Uniform substitution of linear equations | 590 |
| T 20.3 | Virtual substitution of quadratic equations | 592 |
| L 20.2 | Virtual substitution lemma for square roots | 596 |
| T 20.3 | Virtual substitution of quadratic equations | 609 |
| L 21.1 | Virtual substitution lemma for infinities | 612 |
| L 21.2 | Virtual substitution lemma for infinitesimals | 618 |
| T 21.2 | Virtual substitution of quadratic constraints | 619 |
| T 21.3 | Tarski-Seidenberg | 625 |