Part I
Logics and Proof Calculi for Hybrid Systems

Overview In this part, which is the core part of this book, we introduce novel logics and proof calculi that form the new conceptual, formal, and technical basis for the logical analysis of hybrid systems. In Chap. 2, we introduce the differential dynamic logic $\mathsf{d}\mathcal{L}$ as a variant of dynamic logic that is suitable for specifying and verifying properties of hybrid systems. It generalises classical dynamic logic to dynamic logic over the reals in the presence of hybrid dynamics with interacting discrete state transitions and continuous state evolutions along differential equations. As a verification technique, we present a new compositional proof calculus for $\mathsf{d}\mathcal{L}$ that is suitable for automation and integrates handling of real quantifiers by generalising Skolemisation and free variables to the reals. In Chap. 2, we also prove completeness relative to differential equations as the most fundamental theoretical result in this book.

In Chap. 3, we introduce the differential-algebraic logic DAL that extends the class of hybrid system models by allowing more general differential-algebraic equations, differential inequalities, and quantified nondeterminism. Further, we present a uniform theory of differential induction, differential invariants, differential variants, and differential strengthening as central symbolic verification techniques for handling challenging continuous dynamics in hybrid systems without having to solve their differential equations.

In Chap. 4, we address the handling of temporal properties and introduce the differential temporal dynamic logic dTL along with a calculus that reduces temporal properties to $\mathsf{d}\mathcal{L}$ properties. The extensions of $\mathsf{d}\mathcal{L}$ that we present in Chap. 3 and Chap. 4 are complementary and compatible. Their direct modular combination immediately defines the differential-algebraic temporal dynamic logic DATL.

The logics and proof techniques developed in this part will form the basis for the automation techniques developed in Part II. They also form the foundation for the formal verification tool KeYmaera. We will also use the differential dynamic logics to formalise safety-critical properties of the train and aircraft control studies in Part III and prove them with the proof techniques we develop in Part I.