Temporal Logic Verification Using Simulation

Georgios E. Fainekos[1], Antoine Girard[2], and George J. Pappas[3]

[1] Department of Computer and Information Science, Univ. of Pennsylvania, USA
fainekos@cis.upenn.edu
[2] VERIMAG, 2 avenue de Vignate, 38610 Gières, France
Antoine.Girard@imag.fr
[3] Department of Electrical and Systems Engineering, Univ. of Pennsylvania, USA
pappasg@ee.upenn.edu

Abstract. In this paper, we consider a novel approach to the temporal logic verification problem of continuous dynamical systems. Our methodology has the distinctive feature that enables the verification of the temporal properties of a continuous system by verifying only a finite number of its (simulated) trajectories. The proposed framework comprises two main ideas. First, we take advantage of the fact that in metric spaces we can quantify how close are two different states. Based on that, we define robust, multi-valued semantics for MTL (and LTL) formulas. These capture not only the usual Boolean satisfiability of the formula, but also topological information regarding the distance from unsatisfiability. Second, we use the recently developed notion of bisimulation functions to infer the behavior of a set of trajectories that lie in the neighborhood of the simulated one. If the latter set of trajectories is bounded by the tube of robustness, then we can infer that all the trajectories in the neighborhood of the simulated one satisfy the same temporal specification as the simulated trajectory. The interesting and promising feature of our approach is that the more robust the system is with respect to the temporal logic specification, the less is the number of simulations that are required in order to verify the system.

1 Introduction

Software and hardware design has tremendously benefited from advances in algorithmic verification. Model checking [1] is now a widely used technology in various industrial settings. Thanks to the rapidly growing area of embedded systems with real-time specifications, a similar growth is also being experienced in the area of real-time systems [2]. As the complexity of the physical systems increases and captures continuous or hybrid systems, the verification problems quickly become hard, if not undecidable.

For the verification of hybrid systems, a variety of methods have been proposed [3,4,5,6,7,8] (not an inclusive list). The common characteristic of all these approaches is that they apply to either continuous systems with simple dynamics, or they are computationally expensive and, thus, they can only be used for low dimensional systems (for promising high-dimensional results see [9,10]). Beyond the scope of these techniques, the analysis of complex systems still relies

E. Asarin and P. Bouyer (Eds.): FORMATS 2006, LNCS 4202, pp. 171–186, 2006.

heavily on simulation-based methods for monitoring [11]. Along these lines several authors have proposed simulation techniques that can provide guarantees for uniform coverage [12,13] or even completeness results [14].

This paper develops a simulation-based method for verifying temporal properties of complex continuous systems. In particular, given a continuous dynamical system, a set of initial conditions, a bounded time horizon, and a temporal logic specification expressed in Metric or Linear Temporal Logic [15], we develop a simulation-based algorithm that verifies whether all the system trajectories satisfy the desired temporal property. To achieve this, we build upon two recent notions : a definition of *robust satisfaction* for Metric Temporal Logic (MTL) specifications [16] and the notion of *bisimulation functions* [17]. The definition of robust satisfaction of an MTL specification is meaningful only when state sequences evolve in metric spaces, a very natural assumption for continuous systems. Our proposed robust semantics capture bounds on the magnitude of the state perturbations that can be tolerated without altering the Boolean truth value of the MTL or LTL property. Bisimulation functions, on the other hand, quantify the distance between two approximately bisimilar states and the trajectories initiating from them. Using a bisimulation function we can define a neighborhood of trajectories around a nominal one which have approximately the same behavior as the nominal trajectory. If this neighborhood of the simulated trajectory is contained in the tube of trajectories, which robustly satisfy the specification, then we can safely infer that the neighborhood of trajectories also satisfies the specification.

Based on this observation, we develop an algorithm that, first, samples points in the set of initial conditions of the system using guidance from the bisimulation function. Starting from this set of points, we simulate the system for a bounded horizon. For each of these trajectories we compute an under-approximation of its robustness degree. If the robustness degree bounds the distance computed by the bisimulation function then we are done, otherwise we repeat the procedure. The novelty in our framework is that the number of simulations, which are required for the verification of the system, decreases inversely to the robustness of the system with respect to the temporal property.

Finally, we would like to point out that in the past several authors have also studied the robustness of real time specifications with respect to timed or dense time traces of real time systems [18,19,20], but the robustness is considered with respect to the timing constraints, not state perturbations. The work which is the closest in spirit to this paper appears in [21] where the authors give quantitative semantics to the branching-time logic CTL (called Discounted CTL) in order to achieve robustness with respect to model perturbations.

2 Problem Formulation

Let $\mathbb{R}$ be the set of the real numbers, $\mathbb{Q}$ the set of the rational numbers and $\mathbb{N}$ the set of the natural numbers. We denote the extended real number line by