Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 317 (2015) 19–25

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Numerically-aided Deductive Safety Proof for a Powertrain Control System

Nikos Aréchiga[a,1], James Kapinski[b], Jyotirmoy V. Deshmukh[b], André Platzer[a] and Bruce Krogh[a]

[a] *Carnegie Mellon University, 5000 Forbes Ave Pittsburgh, PA, USA*

[b] *Toyota Technical Center, 1630 W. 186th, Gardena, CA, USA*

Abstract

The use of deductive techniques, such as theorem provers, has several advantages in safety verification of hybrid systems. There is often a gap, however, between the type of assistance that a theorem prover requires to make progress on a proof task and the assistance that a system designer is able to provide. To address this deficiency we present an extension to the deductive verification framework of differential dynamic logic that allows the theorem prover KeYmaera to *locally reason* about behaviors by leveraging forward invariant sets provided by external methods, such as numerical techniques and designer insights. Our key contribution is a new inference rule, the forward invariant cut rule, introduced into the proof calculus of KeYmaera. We demonstrate the cut rule in action on an example involving an automotive powertrain control systems, in which we make use of a simulation-driven numerical technique to compute a local barrier function.

Keywords: Cyberphysical system, hybrid system, verification, safety property

1 Introduction

Most cyberphysical systems are *hybrid* in nature, i.e., have both continuous state evolution governed by differential equations and discrete mode transitions. Unfortunately, the problem of verifying safety properties for hybrid systems is undecidable [6], and most techniques that are used to verify software are not directly applicable. Many approaches to hybrid system verification focus on creating an overapproximation of the set of system states reachable over a fixed time horizon [9],[3],[4],[2]. While these approaches enjoy a high degree of automation, they are restricted in scope and scalability. An alternative is to employ deductive techniques that attempt to construct a symbolic proof of safety using a semi-interactive theorem prover [10]. Unlike reachable-set computation techniques, theorem provers can handle nonlinear

[1] This work partially supported by the National Science Foundation under Grant NSF EXPEDITION CNS-0926181.

http://dx.doi.org/10.1016/j.entcs.2015.10.003

dynamics directly, without introducing approximation artifacts. Further, theorem provers can handle proof tasks that involve symbolic parameters.

Safety verification of hybrid systems via theorem proving may incorporate human insight in the form of a *safety certificate*, i.e., a symbolic expression representing a set containing all reachable states from a given initial set, while excluding unsafe states [1,10]. However, a designer usually has better insight about local behaviors in different operating regimes rather than overarching knowledge about the entire system. In [8], we demonstrated a numerical technique for discovering local invariants. This technique can be used to search for local invariants in specific regions of interest. In contrast to previous work focused on obtaining a global safety certificate, our approach encourages *local reasoning* and *lazy construction* of such certificates.

To support local reasoning, we introduce a new proof rule called the *forward invariant cut rule* in the calculus of the theorem prover KeYmaera. This rule is similar to an inductive invariant; given a region of operation and a proposed local safety certificate (in the form of a forward invariant), the rule allows us to decompose the overall proof into three proof obligations: (1) a proof of invariance of the proposed certificate, (2) a proof that the local certificate guarantees safety, and (3) a proof of safety of everything *excluding* the behaviors associated with the region pertaining to the local certificate.

We demonstrate this rule in a case study on safety verification for a powertrain control system. This system is a simplified model of a control system responsible for maintaining the air-to-fuel (A/F) ratio in a gasoline engine near an optimal setpoint. We describe the overall proof, but primarily describe the role of the forward invariant cut rule to prove that the A/F ratio remains within 10% of the optimal setpoint in KeYmaera.

2 Hybrid systems and hybrid programs

A hybrid dynamical system consists of a set of continuous-valued state variables $\mathbf{x}$ that take values from a domain $X \subseteq \mathbb{R}^n$ and a discrete-valued state variable q (also known as a *mode*) taken from a finite set Q. The system evolves in continuous or discrete time, and the configuration of a hybrid system at time t can be described by the values of its continuous and discrete state variables. In mode q, the evolution of the continuous-valued state variables is typically described using ordinary differential equations (ODEs) of the form $\dot{\mathbf{x}}(t) = f_q(\mathbf{x}(t))$, where f_q is a function from X to X. Though hybrid systems can have external inputs, here, we consider only *autonomous systems*, i.e., systems in which all transitions depend only on the system states. The state-dependent conditions that allow the system to transition from one discrete state to another (possibly same) discrete state are called *guards*.

While hybrid automata are often a convenient modeling formalism for such systems, here we use the *hybrid programs* notation to facilitate the use of the KeYmaera theorem prover, the workhorse for our deductive approach. To specify hybrid programs and specifications, KeYmaera uses the formalism of *differential dynamic logic* [2] denoted by d$\mathcal{L}$.

[2] The syntax and semantics of d$\mathcal{L}$ are described in detail in [10]; we provide only a minimal overview here.