Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 317 (2015) 71–83

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Theorem-Proving Analysis of Digital Control Logic Interacting with Continuous Dynamics

Geoffrey C. Hulette[1], Robert C. Armstrong, Jackson R. Mayo, Joseph R. Ruthruff

Sandia National Laboratories, P.O. Box 969, Livermore, California 94551-0969, USA

Abstract

This work outlines an equation-based formulation of a digital control program and transducer interacting with a continuous physical process, and an approach using the Coq theorem prover for verifying the performance of the combined hybrid system. Considering thermal dynamics with linear dissipation for simplicity, we focus on a generalizable, physically consistent description of the interaction of the real-valued temperature and the digital program acting as a thermostat. Of interest in this work is the discovery and formal proof of bounds on the temperature, the degree of variation, and other performance characteristics. Our approach explicitly addresses the need to mathematically represent the decision problem inherent in an analog-to-digital converter, which for rare values can take an arbitrarily long time to produce a digital answer (the so-called Buridan's Principle); this constraint ineluctably manifests itself in the verification of thermostat performance. Furthermore, the temporal causality constraints in the thermal physics must be made explicit to obtain a consistent model for analysis. We discuss the significance of these findings toward the verification of digital control for more complex physical variables and fields.

Keywords: formal methods, theorem proving, hybrid systems, cyber-physical systems

1 Introduction

Formal verification of hybrid or cyber-physical systems [2] can be viewed as a broader extension of numerical software verification – one in which real-valued variables and functions are modeled not merely for purposes of understanding their representation in a digital computation, but as actual physical phenomena with which a digital computation interacts. This viewpoint indicates a need both (1) to extend formal verification techniques for reasoning about digital computation to include continuous dynamics, and (2) to ensure the consistency of such hybrid models with physics, including the physics of digital computation itself. That is, since all extant systems are believed to be ultimately physically continuous, it is important to understand

[1] Email: ghulett@sandia.gov

http://dx.doi.org/10.1016/j.entcs.2015.10.008

under what circumstances parts of a system can be modeled as digital, and how to reason formally about the entire system.

Much research and development work has targeted enabling formal verification of hybrid systems, typically in the form of model checking for so-called hybrid automata [3,9]. We argue that this existing work is in different ways too broad and too narrow: Modeling approaches that freely combine discrete and continuous dynamics can readily introduce ill-posed and unphysical behavior due to the delicate interaction between the two types of dynamics [7]. And reasoning about hybrid systems via model checking is limited to properties that can be verified conservatively by enumeration of discrete regions within the continuous state space; even approaches using theorem proving have implemented model-checking strategies [14] or have relied on restrictive logics to formally model hybrid systems [12]. Work exists on formally analyzing continuous differential equations via theorem proving, but without modeling a coupling to digital logic [13]. We propose an approach that can leverage the full power of higher-order logic in the Coq theorem prover [5] to reason about physically consistent hybrid digital-physical models. Unlike model-checking approaches, our goal is not to completely automate the verification, but rather to provide maximum power and scalability for reasoning rigorously about properties of interest, leveraging understanding of system design for both the digital and physical elements.

In the remainder of this paper we present the physical modeling considerations that motivate this work (Sec. 2); a simple hybrid thermostat model used to illustrate our approach (Sec. 3); an analysis of that model using informal mathematics to convey the key ideas (Sec. 4); a corresponding formal analysis in the Coq theorem prover (Sec. 5); and a conclusion (Sec. 6).

Excerpts of the formal analysis are shown in this paper, and the full Coq implementation is available online [1].

2 Physics of Hybrid Modeling

The novelty of this work lies in a formal proof for an almost trivial cyber-physical system but with faithful modeling of continuous physical variables as real numbers coupled consistently to the digital control program. A noted limitation [13] of typical approaches to cyber-physical problems is that continuous physics is first "digitized" and the resulting, completely digital model is then analyzed [3]. We observe that this common strategy can obscure important physical constraints. One such constraint is causality, the requirement that a physical effect cannot precede its cause in time. Another is the Arbiter's Problem [4], also known as Buridan's Principle [10], a fundamental property of physics stating that a discrete decision based on a continuous variable (i.e., an analog-to-digital conversion) cannot be guaranteed to complete in bounded time; this property must be accounted for in any analysis seeking formal guarantees about discrete decisions on real numbers. Interestingly, both of these physical constraints are also closely related to considerations of computability, as is natural if the viewpoint is taken that the physical universe itself may arise from an