Science of Computer Programming 162 (2018) 35–54

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

Sound conformance testing for cyber-physical systems: Theory and implementation

Hugo Araujo [a], Gustavo Carvalho [a], Morteza Mohaqeqi [b], Mohammad Reza Mousavi [c,d,*], Augusto Sampaio [a]

[a] Universidade Federal de Pernambuco, Brazil
[b] Uppsala University, Sweden
[c] Halmstad University, Sweden
[d] University of Leicester, UK

ARTICLE INFO

Article history:
Received 18 January 2017
Received in revised form 15 July 2017
Accepted 20 July 2017
Available online 4 August 2017

Keywords:
Cyber-physical systems
Model-based testing
Conformance testing
Soundness
Reachability analysis

ABSTRACT

Conformance testing is a formal and structured approach to verifying system correctness. We propose a conformance testing algorithm for cyber-physical systems, based on the notion of hybrid conformance by Abbas and Fainekos. We show how the dynamics of system specification and the sampling rate play an essential role in making sound verdicts. We specify and prove error bounds that lead to sound test-suites for a given specification and a given sampling rate. We use reachability analysis to find such bounds and implement the proposed approach using the CORA toolbox in Matlab. We apply the implemented approach on a case study from the automotive domain.

1. Introduction

A cornerstone of model-based testing (MBT) [1] is to systematically generate test-cases from a test model, i.e., a specification of system's correct behavior. A rigorous notion of MBT aims at establishing a *conformance relation* by running a number of such generated test-cases [2–6]. Conformance relation is the mathematical formalization of the test technique, which is typically defined as a relation on a common semantic domain of both the test model and the system under test. We refer to such a mathematically-founded notion of MBT, where a rigorous notion of conformance is defined and is properly related to the testing technique, as *conformance testing*.

Fig. 1 provides a schematic view of the notions of conformance relation, conformance testing and the correspondence between them. On the top-left corner, the MBT trajectory starts with a test model. This model is the result of a translation of the requirements, which typically describes the "interesting" scenarios of interaction to test as well as their expected outputs. The top part of Fig. 1 depicts the practical part of MBT, which starts with generating test cases from the test model, applying them to the system under test, and analyzing the outcomes in an iterative manner. The bottom part of Fig. 1 puts these practical activities on a firm theoretical ground. To this end, the test model is given a mathematical meaning, through a mapping called formal semantics. It is also assumed that the system under test *can* be given a mathematical meaning; however, the mathematical object (e.g., the state machine) capturing the behavior of the system under test may

* Corresponding author.
E-mail addresses: hlsa@cin.ufpe.br (H. Araujo), ghpc@cin.ufpe.br (G. Carvalho), morteza.mohaqeqi@it.uu.se (M. Mohaqeqi), m.r.mousavi@hh.se (M.R. Mousavi), acas@cin.ufpe.br (A. Sampaio).

http://dx.doi.org/10.1016/j.scico.2017.07.002

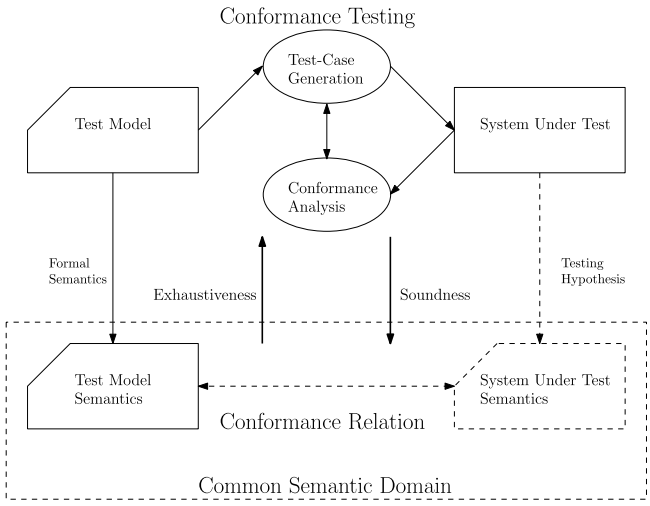

Fig. 1. Schematic view of conformance testing and conformance relation.

be too large to generate and analyze. Hence, the dashed line depicts a purported (not practically available) formal semantics of the system under test, bringing both the test model and the system under test in a common semantic model. The common semantic domain is used to facilitate specifying and reasoning about the conformance relation, but in practice, one does not typically have access to such a rigorous description of behavior, particularly of the system under test (hence, the common semantic domain and the conformance relation are drawn in dashed line denoting that they only exist in theory). Using these two models and the common semantic domain, one devises a conformance relation defining what it means mathematically for a system to conform to a specification. The model-based testing trajectory should ideally precisely characterize the mathematical conformance relation, denoted by the downward and upward arrows in Fig. 1 representing soundness and exhaustiveness, respectively.

Some notions of conformance testing for ordinary reactive systems are both sound and exhaustive [7,8]. However, for cyber-physical systems (CPSs), it is far from trivial to come up with a sound and exhaustive, yet practical, notion of conformance testing. Conformance testing of CPSs [4,9] often involves discrete sampling of continuous signals and hence, for any realistic notion of conformance testing, error margins should be accommodated to allow for slight deviations (e.g., measurement errors) in time and value [10,2,3]. The interaction among the continuous dynamics, the sampling rates and the error margins is an intricate one and if the aforementioned parameters are not in sync, the resulting conformance testing method can be unsound. Exhaustiveness is even more intricate and requires detailed information about the continuous dynamics of the implementation under test (as well as the specification); we focus on soundness and address exhaustiveness briefly and in passing towards the end of this paper.

1.1. Problem definition and contributions

Given a specification and a sampling rate, we seek sufficient conditions for a test-suite under which conformance testing is sound with respect to a given conformance relation. That is, the test-suite only fails on non-conforming implementations.

To make this problem more specific, we take the notion of hybrid conformance by Abbas and Fainekos [10,2,3] as our conformance relation. We then define a straightforward conformance testing algorithm based on this notion and study its soundness. As it turns out, for all reasonable specifications (e.g., specifications with countable minima and maxima in each finite interval) such a conformance testing algorithm may in general result in unsound verdicts. Hence, we specify and prove soundness criteria, based on the error margins (in time and value), the properties of specification's continuous dynamics, and the sampling rate, that guarantee soundness of the test verdicts. These results were first presented in a conference publication [11].

In this paper, we revise our earlier results [11] and significantly extend them. Particularly, finding the right bounds for conformance testing requires a thorough analysis of the system dynamics. To this end, we propose a method based on reachability analysis and implement it using the CORA toolbox [12] in Matlab. To validate our strategy, along with its implementation, we consider a controller to an automotive air–fuel ratio (AFR) control system [13].

1.2. Running example

To illustrate the notions introduced in the paper, we consider the model of a thermostat [6] as our running example. The thermostat has two operation modes to control the temperature. In mode *ON*, a heater is turned on in order to warm up the environment. During the mode *OFF*, the heater is turned off, which leads to a steady decrease in the environment