Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Safe & robust reachability analysis of hybrid systems

Eugenio Moggi [a,*,1], Amin Farjudian [b,2], Adam Duracz [c,3], Walid Taha [d,4]

[a] DIBRIS, Genova Univ., v. Dodecaneso 35, 16146 Genova, Italy
[b] University of Nottingham Ningbo, China
[c] Rice University, Houston, TX, USA
[d] Halmstad University, Halmstad, Sweden

ARTICLE INFO

Article history:
Received 7 August 2017
Received in revised form 6 June 2018
Accepted 9 June 2018
Available online xxxx
Communicated by J.-F. Raskin

Keywords:
Hybrid systems
Reachability
Robustness
Domain theory

ABSTRACT

Hybrid systems—more precisely, their mathematical models—can exhibit behaviors, like *Zeno behaviors*, that are absent in purely discrete or purely continuous systems. First, we observe that, in this context, the usual definition of *reachability*—namely, the reflexive and transitive closure of a transition relation—can be *unsafe*, i.e., it may compute a proper subset of the set of states *reachable in finite time* from a set of initial states. Therefore, we propose *safe reachability*, which always computes a superset of the set of reachable states. Second, in safety analysis of hybrid and continuous systems, it is important to ensure that a reachability analysis is also *robust* w.r.t. small perturbations to the set of initial states and to the system itself, since discrepancies between a system and its mathematical models are unavoidable. We show that, under certain conditions, the *best Scott continuous approximation* of an analysis A is also its *best robust approximation*. Finally, we exemplify the gap between the set of reachable states and the supersets computed by safe reachability and its best robust approximation.

0. Introduction

In a transition system—i.e., a relation $\rightarrow$ on a set of states—reachability is a clearly defined notion, namely, the reflexive and transitive closure $\rightarrow^*$ of $\rightarrow$. Reachability analysis plays an important role in computer-assisted verification and analysis [2], since **safety** (a key system requirement) is usually formalized in terms of **reachability**, namely:

$$\text{state } s \text{ is safe} \iff \text{it is not possible to reach a bad state from } s.$$

For a hybrid system one can define a transition relation $\rightarrow$ on a *continuous and uncountable* state space, but $\rightarrow^*$ captures only the states reachable in finitely many transitions, and they can be a proper subset of those reachable in finite time! Hybrid systems with *Zeno behaviors*—where infinitely many events occur in finite time—are among the systems in which

* Corresponding author.
E-mail addresses: moggi@unige.it (E. Moggi), Amin.Farjudian@gmail.com (A. Farjudian), adam.duracz@rice.edu (A. Duracz), Walid.Taha@hh.se (W. Taha).

[1] Research partially supported by the Swedish Knowledge Foundation.
[2] Work done while the author was a researcher at Halmstad University.
[3] Work done while the author was a PhD student at Halmstad University.
[4] Research partially supported by US NSF award #1736754 "A CPS Approach to Robot Design", the ELLIIT Swedish Strategic Area initiative, and the Swedish Knowledge Foundation project "AstaMoCA: Model-based Communications Architecture for the AstaZero Automotive Safety Facility".

https://doi.org/10.1016/j.tcs.2018.06.020
0304-3975/

the two notions of reachability differ. Zeno behaviors arise naturally when modeling rigid body dynamics with impacts, as illustrated by the system consisting of a bouncing ball (Example 2.8), whose Zeno behavior is due to the modeling of impacts as discrete events.

0.1. Contributions

The first contribution of this paper is the notion of **safe reachability** (Definition 3.6), which gives an over-approximation—i.e., a superset—of the states reachable in finite time, including the case where the hybrid system has Zeno behaviors. Mathematical models are always *simplifications*, through abstractions and approximations, of *real systems*. Simplifications are essential to making analyses manageable. In safety analysis, over-approximations are acceptable, since they can only lead to false negatives, i.e., the analysis may wrongly conclude that (a state s of) the system in unsafe, because the over-approximation includes some unreachable bad states.

The second contribution is to show, under certain assumptions, that the *best Scott continuous approximation* of safe reachability coincides with its *best robust approximation*. In safety analysis robust over-approximations are important, because inaccuracies in the modeling of a cyber-physical system (as well as in its building and testing) are unavoidable, as convincingly argued in [13].

0.2. Background

We build directly on the following papers.

- [15] is an excellent tutorial on hybrid systems, from which we borrow the definition of a hybrid system (Definition 2.1), but we do not use hybrid arcs (and related notions), since they cannot reach nor go beyond *Zeno points*.
- [10,9] introduce topological transition systems (TTS), which we use for defining safe reachability (Definition 3.6). In TTSs on discrete spaces, standard reachability (Definition 3.1) and safe reachability (Definition 3.6) coincide.
- [12] is one among several papers, where Edalat recasts mainstream mathematics in Domain Theory, and shows what is gained by doing so. In the context of this paper, Domain Theory becomes relevant when the Scott and Upper Vietoris topologies on certain *hyperspaces* coincide.

The reachability maps we introduce are arrows in the category of complete lattices and monotonic maps, which is the standard setting for defining and comparing abstract interpretations [8]. Our notion of robustness is related to δ-*safety*, i.e., safety of a system subject to *imprecision* up to δ. [13,19] argue that δ-safety makes the verification task easier, and excludes systems that are safe only under unrealistic assumptions.

0.3. Summary

The rest of the paper is organized as follows:

- Sec. 2 recalls the definition of a hybrid system from [15], defines the corresponding transition relation (Definition 2.3), and gives some examples.
- Sec. 3 introduces two reachability maps Rf and Rs (Definition 3.1 and 3.6, respectively), establishes their properties and how they relate to each other.
- Sec. 4 introduces the notion of robustness (see Definition 4.1) and states two results on the existence of best robust approximations (Corollary 4.4 and 4.5), that follow from more general results on Scott continuous maps.
- Sec. 5 uses the category of complete lattices and monotonic maps (see Definition 5.2) as a framework to discuss approximations and relate reachability maps defined on different complete lattices. In this framework we give a general definition of *best approximation* (Theorem 5.11), and in particular a systematic way to turn a monotonic map f between complete lattices into its best Scott continuous approximation $f^{\boxdot}$ (see Proposition 5.15).
- Sec. 6 recalls and assesses several notions defined in [15] using hybrid arcs, like forward invariant/stable/pre-attractive subset, and gives simpler way to recast or redefine them using the notions introduced in this paper.
- Sec. 7 analyzes (with the aid of pictures) the differences between the under-approximation Rf and several over-approximations (from Rs to $\mathsf{Rs}^{\boxdot}$) of sets of reachable states, for the hybrid systems introduced in Sec. 2.

Appendix A contains proofs that were too long to inline and a section relating robustness and Scott continuity (see Appendix A.1).

1. Mathematical preliminaries

We assume familiarity with the notions of Banach, metric, and topological space, and the definitions of open, closed, and compact subset of a topological space (see, e.g., [7,18]). The relations among spaces are:

Please cite this article in press as: E. Moggi et al., Safe & robust reachability analysis of hybrid systems, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2018.06.020