Available online at www.sciencedirect.com
ScienceDirect
Information and Computation 205 (2007) 1575–1607
Information and Computation
www.elsevier.com/locate/ic

Taylor approximation for hybrid systems ☆

Ruggero Lanotte *, Simone Tini

Dipartimento di Scienze della Cultura, Politiche e dell'Informazione, Università dell'Insubria, Via Valleggio 11, I-22100 Como, Italy

Received 29 August 2005; revised 7 February 2007
Available online 10 August 2007

Abstract

We propose a new approximation technique for Hybrid Automata. Given any Hybrid Automaton H, we call $Approx(H,k)$ the Polynomial Hybrid Automaton obtained by approximating each formula ϕ in H with the formulae ϕ_k obtained by replacing the functions in ϕ with their Taylor polynomial of degree k. We prove that $Approx(H,k)$ is an over-approximation of H. We study the conditions ensuring that, given any $\epsilon > 0$, some k_0 exists such that, for all $k > k_0$, the "distance" between any vector satisfying ϕ_k and at least one vector satisfying ϕ is less than ϵ. We study also conditions ensuring that, given any $\epsilon > 0$, some k_0 exists such that, for all $k > k_0$, the "distance" between any configuration reached by $Approx(H,k)$ in n steps and at least one configuration reached by H in n steps is less than ϵ.

1. Introduction

Hybrid Automata [1,4] are a widely studied model for *hybrid systems* [25], i.e., dynamical systems combining discrete and continuous state changes. Hybrid Automata extend classic finite state machines with continuously evolving *variables*, and exhibit two kinds of state changes: discrete jump transitions, occurring instantaneously, and continuous flow transitions, occurring while time elapses. These two kinds of transitions are guarded by *jump conditions* and *activity functions*, respectively, which are formulae expressing constraints on the source and target value of the variables.

1.1. Reachability

Most of hybrid system applications are safety critical and require guarantees of safe operation. To analyze *safety properties* (i.e., properties requiring that a given set of *bad configurations* cannot be reached), the decidability of *reachability* problem (i.e., whether or not a given configuration can be reached) is determinant. Unfortunately, for most classes of hybrid systems, reachability is undecidable [14]. However, for some of these

☆ A preliminary version of this paper was presented at HSCC '05 [20]. The authors wish to thank Annalisa Panati for fruitful discussions.
* Corresponding author.
E-mail addresses: ruggero.lanotte@uninsubria.it (R. Lanotte), simone.tini@uninsubria.it (S. Tini).

0890-5401/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2007.05.004

classes, computing the successors (or predecessors) of configurations sets is reasonably efficient, and, therefore, reachability *in a limited number of steps* is decidable.

There are also classes of hybrid systems for which the successors of configuration sets are not computable. A new methodology has been proposed in [13] to fill this gap. First of all, according to [13], an Hybrid Automaton H' is an *approximation* of another Hybrid Automaton H iff H' is obtained from H by weakening activity functions and jump conditions. In such a way, the set of all the possible computations of H' is a superset of the set of all the possible computations of H, and, hence, if we prove that a *bad* configuration cannot be reached by H' in n steps, then we can infer that it cannot be reached by H in n steps. In order to be sure that such a proof is possible, in [13] it is required that the approximation H' is in the class of the *Linear Hybrid Automata*, for which the successors of configuration sets are computable.

The notion of approximation is then strengthened in [13] with the notion of ϵ-*approximation*: Given any $\epsilon > 0$, H' is an ϵ-*approximation* of H iff, given any vector v' satisfying an activity function (resp. jump condition) in H', there is a vector v satisfying the corresponding activity function (resp. jump condition) in H such that the *distance* between v' and v is below ϵ. This notion of ϵ-approximation is motivated by the need to limit the *error* introduced by the approximation. Finally, any *approximation operator* γ mapping Hybrid Automata into their approximations is *asymptotically complete* iff, for any $\epsilon > 0$ and for any hybrid automaton H, an ϵ-approximation of H can be given by γ. In [13] an asymptotically complete approximation operator, called *rationally rectangular phase-portrait approximation operator*, is given which approximates any jump condition or activity function by a predicate satisfied by all points lying in a space consisting of a products of intervals with rational endpoints.

1.2. Our contribution

In the present paper, we propose a new approximation technique. Our idea is to weaken jump conditions and activity functions by replacing functions over variables with their polynomial of Taylor. More precisely, given any Hybrid Automaton H and natural k, $\mathbf{A}(H,k)$ is the set of the Hybrid Automata that are obtained by replacing in jump conditions and activity functions of H each function $f(\overrightarrow{x})$ over the variables $\overrightarrow{x}$ with the *polynomial of Taylor for f of degree k with respect to vector* $\overrightarrow{v}$, denoted $P^k(f,\overrightarrow{x},\overrightarrow{v})$, where $\overrightarrow{v}$ is a vector in the domain of f. Of course, to define $\mathbf{A}(H,k)$ we require that all functions $f(\overrightarrow{x})$ are derivable k times. Notice that $\mathbf{A}(H,k)$ is in the class of *Polynomial Hybrid Automata*, for which computing the successors of configuration sets is decidable [29].

We shall prove that each Polynomial Hybrid Automaton H_k in $\mathbf{A}(H,k)$ is an approximation for H according to [13], i.e., that all jump conditions and activity functions of H_k are less demanding than those of H. We shall study the conditions ensuring that our approximation is asymptotically complete, in the sense that, for each $\epsilon > 0$ there exists some k_0 such that, for all $k > k_0$, $\mathbf{A}(H,k)$ contains only ϵ-approximations for H. We note that looking for more accurate approximations for H is in some sense mechanizable, since it simply requires taking increasing values for k.

Now, looking for ϵ-approximations for small values of ϵ is a strategy suggested in [13] to limit the error of the approximation. We observe that this analysis of the error is *syntactic*, in the sense that it does not consider the behavior of H and its approximation. In general, one expects explosion of the error. In fact, by approximating one activity function or one jump condition, an error is generated which implies the reachability of some configurations that were originally unreachable. If in these configurations the behaviors are once more affected by new errors caused by the approximation of other activity functions and jump conditions, error could explode dramatically. In this paper we take a step toward a *semantic* analysis of the error. We study conditions ensuring that, when k tends to the infinity, the behavior of any $H_k \in \mathbf{A}(H,k)$ gets close to the behavior of H. More precisely, these conditions ensure that, for each $\epsilon > 0$, there is some k_0 such that, for all $k > k_0$, if any $H_k \in \mathbf{A}(H,k)$ reaches a configuration c in n steps, then H reaches a configuration c' in n steps such that the *distance* between c and c' is below ϵ.

1.3. Related works

Approximation is a strategy widely used for the analysis of hybrid systems. However, the literature presents different notions of approximation, that we briefly comment on in this section. Several papers (see, e.g., [3,1,5,