Approximated Symbolic Computations over Hybrid Automata[*]

Alberto Casagrande
Dept. of Mathematics and Geosciences
University of Trieste, Italy
acasagrande@units.it

Tommaso Dreossi   Carla Piazza
Dept. of Mathematics and Computer Science
University of Udine, Italy
tommaso.dreossi@uniud.it   carla.piazza@uniud.it

Hybrid automata are a natural framework for modeling and analyzing systems which exhibit a mixed discrete continuous behaviour. However, the standard operational semantics defined over such models implicitly assume perfect knowledge of the real systems and infinite precision measurements. Such assumptions are not only unrealistic, but often lead to the construction of misleading models. For these reasons we believe that it is necessary to introduce more flexible semantics able to manage with noise, partial information, and finite precision instruments. In particular, in this paper we integrate in a single framework based on approximated semantics different over and under-approximation techniques for hybrid automata. Our framework allows to both compare, mix, and generalize such techniques obtaining different approximated reachability algorithms.

1 Introduction

Hybrid automata were proposed to model hybrid systems, i.e., systems consisting of interaction between discrete and continuous components [1]. Automatic deduction of properties for such systems is strictly related to the concept of state reachability. In particular, given a set of initial states, we ask whether there are executions of the system that lead to specific final states. In general, it has been proved that such problem is undecidable, i.e., algorithms which provide the correct answer for any instance of such problem cannot exist [11]. However, imposing syntactic restrictions, several subclasses of hybrid automata over which the reachability problem is decidable have been identified [13, 6].

Different approaches, such as the introduction of *noise in hybrid automata* [9] and the use of approximated semantics (ε*-semantics* [5]), have been proposed with the aim of both tackling the undecidability of the reachability problem and introducing hybrid automata semantics able of capturing some indeterminacy which is intrinsic in real world hybrid systems (e.g., experimental approximations, environmental disturbances, etc.). In [12], the authors observed that undecidability cannot be removed by simply replacing trajectories with open flow tubes. More drastic changes at a semantics level are required. Many works proposed so far go in this direction (see [9, 10, 22, 5]). Comparisons between these approaches on multistable and Zeno examples can be found in [4].

We proceed investigating in the direction of ε, and more in general *approximated*, semantics with the aim of introducing a general framework for the use, comparison, and composition of different approximation methods. Similarly to [9], our framework relies on polynomial dynamics. As shown by different authors (see e.g. [17, 18]), this is not a strong restriction since arbitrary flow functions can be approximated with polynomial flows. Moreover, the standard numeric algorithms used to generate the solutions of a system of differential equations and to integrate them are based on polynomials. Such considerations are exploited also in [19] where Fränzle's results are applied "*[...] after explicitly solving*

[*] This work has been partially supported by Istituto Nazionale di Alta Matematica (INdAM).

Bortolussi, Bujorianu, Pola (Eds.): HAS 2013
EPTCS 124, 2013, pp. 43–57, doi:10.4204/EPTCS.124.6

flow constraints [...]". While in [18] the focus is on approximating hybrid systems with polynomial, here we start from polynomial systems and approximate their semantics with the aim of removing infinite precision and avoid unrealistic behaviors. Differently from [9] and [19], we do not refer to robust systems. Indeed, multistable systems cannot be naturally modeled through robust automata [4].

In more details, in this work, we propose a framework that, on the one hand, exploits Fränzle's approach, reformulated in terms of over-approximating semantics, and on the other, is based on ε-semantics for under-approximating the reachable set. Neither approach relies on fixed-grid discretizations, but on local perturbations on reachable points. In particular, in a quantum-physics fashion, ε-semantics pertubates the observed states, but not the continuous evolution, which proceeds with infinite precision as long as it is not observed.

We implemented our framework exploiting translations of approximated semantics into first-order formulæ over the reals. Such translations allow us to exploit available tools for quantifier eliminations, such as `Redlog` and `QEPCAD`, to implement our reachability algorithms. We tested our implementation on a railroad crossing scenario.

The paper is organized as follows. In Section 2 we present the notation and our definition of hybrid automaton. Section 3 introduces the notion of approximating semantics and briefly reviews *ε-semantics*, while Section 4 instantiates *disturbed automata* in our formalism. In Section 5, the standard semantics of disturbed automata and the related reachability algorithm are expressed in terms of an over-approximated semantics, while a ε-semantics, under-approximating the standard one, is introduced. In Section 6, we briefly describe our implementation of the presented framework and test it on the railroad case-study. Finally, Section 7 ends the paper with some general comments on the difference between the compared approaches and suggests further developments.

2 Hybrid Automata

2.1 Preliminaries

We now introduce some notations and conventions. Capital letters X, X', X_m, and X'_m, where $m \in \mathbb{N}$, denote variables ranging over $\mathbb{R}$, while Z denotes the vector of variables $\langle X_1, \ldots, X_d \rangle$ and Z' denotes the vector $\langle X'_1, \ldots, X'_d \rangle$. The variable T models time and ranges over $\mathbb{R}_{\geq 0}$. We use $p, q, r, s, \ldots$ to denote d-dimensional vectors of real numbers.

As far as the standard notions of first-order languages, models, and theories are concerned the reader may refer, for example, to [16]. In this paper we refer to the first-order theory of $(\mathbb{R}, 0, 1, +, *, =, <)$, also known as the theory of *semi-algebraic sets* or Tarski's theory [21]. Such theory is decidable, i.e., algorithms to check satisfiability of formulæ have been defined (see, e.g., [3]).

We write $\varphi[X_1, \ldots, X_m]$ to stress the fact that the set of free variables of the first-order formula φ is included in the set of variables $\{X_1, \ldots, X_m\}$. If $\{Z_1, \ldots, Z_n\}$ is a set of variable vectors, $\varphi[Z_1, \ldots, Z_n]$ indicates that the free variables of φ are included in the set of components of $Z_1, \ldots, Z_n$. Given a formula $\varphi[Z_1, \ldots, Z_i, \ldots, Z_n]$ and a vector p of the same dimension as the variable vector Z_i, the formula obtained by component-wise substitution of Z_i with p is denoted by $\varphi[Z_1, \ldots, Z_{i-1}, p, Z_{i+1}, \ldots, Z_n]$. We use $\bot$ and $\top$ as shortcuts to denote the two formulæ $0 = 1$ and $1 = 1$, respectively.

The set of formalæ having n free-variables is denoted by $\mathcal{F}_n$, while $\{\!|\varphi|\!\}$, where φ is any generic formula in $\mathcal{F}_n$, is the *standard semantics* of $\varphi \in \mathcal{F}_n$ i.e. the set of points of $\mathbb{R}^n$ satisfying φ. More formally, $\{\!|\cdot|\!\} : \bigcup_{n \in \mathbb{N}} \mathcal{F}_n \to \bigcup_{n \in \mathbb{N}} \wp(\mathbb{R}^n)$ with $\{\!|\varphi[X_1, \ldots, X_n]|\!\} \overset{def}{=} \{\langle p_1, \ldots, p_n \rangle \in \mathbb{R}^n \mid \varphi[p_1, \ldots, p_n] \text{ holds}\}$.

On the other hand, given a set $\mathbb{S} \subseteq \mathbb{R}^n$ we say that a formula $S[Z]$ *represents* (also *defines*) $\mathbb{S}$ if

$\{\!|S[Z]|\!\} = \mathbb{S}$. Not all the subsets of $\mathbb{R}^n$ can be represented through a formula.

We also use some standard notions from topological and metric spaces (see [15]). Although we implicitly refer to the *standard euclidean metric* δ over $\mathbb{R}^n$, our results can be generalized to any metric definable in Tarski's theory. We write $B(p,\varepsilon)$ to indicate the open sphere of radius ε centered in $p \in \mathbb{R}^n$. By extension, $B(\mathbb{S},\varepsilon)$, where $\mathbb{S}$ is a subset of $\mathbb{R}^n$, denotes the Minkowski sum of $B(0,\varepsilon)$ and $\mathbb{S}$.

A set $\mathbb{S}$ is said to be α*-paraconvex*, where $\alpha \in [0,1]$, if for each $B(p,\varepsilon)$ (with p and ε generic) and for each $q \in conv(\mathbb{S} \cap B(p,\varepsilon))$ it holds that $\delta(q,\mathbb{S}) \leq \alpha * \varepsilon$, where $conv(\mathbb{S} \cap B(p,\varepsilon))$ is the convex hull of $\mathbb{S} \cap B(\{p\},\varepsilon)$ and $\delta(q,\mathbb{S}) = inf\{\delta(q,p) \mid p \in \mathbb{S}\}$. Let $\mathcal{I} \subseteq \mathbb{R}$ be an interval and $f : \mathcal{I} \to \mathbb{R}^n$. We say that f is *continuous* if for each $t \in \mathcal{I}$ and for each neighborhood $U_{f(t)}$ of $f(t)$ there exists a neighborhood U_t of t in $\mathcal{I}$ such that for each $t' \in U_t$ it holds $f(t') \in U_{f(t)}$. Moreover, a set-valued map $F : \mathcal{I} \to \wp(\mathbb{R}^n)$ is *lower semi-continuous* if for each $t \in \mathcal{I}$, for each $y \in F(t)$, and for each neighborhood U_y of y, there exists a neighborhood U_t of t in $\mathcal{I}$ such that for each $t' \in U_t$ it holds $F(t') \cap U_y \neq \emptyset$. The notion of lower semi-continuity and α-paraconvexity are at the basis of Michael's selection theorems (see, e.g., [2]) which guarantee the existence of a continuous flow inside a set-valued map. In particular, given a set-valued map $F : \mathcal{I} \to \wp(\mathbb{R}^n)$ the *selection problem* over F requires to find (if there exists one) a continuous function $f : \mathcal{I} \to \mathbb{R}^n$ such that for each $t \in \mathcal{I}$ it holds that $f(t) \in F(t)$.

2.2 Syntax

In this section we give the formal definition of hybrid automata. Many different definitions can be found in the literature. Most common differences between those formalisms reside in the descriptions of continuous and discrete transitions, while the semantics attributed to the transitions are almost the same. Here we follow the approach used in [6] and [5] where automata are defined through first-order formulæ over the reals and, in particular, semi-algebraic formulæ.

Definition 1 (Hybrid Automata - Syntax)**.** *A hybrid automaton* $H = (Z, Z', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res)$ *of dimension* $d(H)$ *consists of the following components:*

- $Z = \langle X_1, \ldots, X_{d(H)} \rangle$ *and* $Z' = \langle X'_1, \ldots, X'_{d(H)} \rangle$ *are two vectors of variables ranging over the reals* $\mathbb{R}$*;*
- T *is a variable ranging over* $\mathbb{R}_{\geq 0}$*;*
- $\langle \mathcal{V}, \mathcal{E} \rangle$ *is a finite directed graph. Each element of* $\mathcal{V}$ *will be dubbed* location*;*
- *each vertex* $v \in \mathcal{V}$ *is labeled by the two formulæ* $Inv(v)[Z]$ *and* $Dyn(v)[Z,Z',T]$*; it should holds that, when* $Inv(v)[p]$ *is true,* $Dyn(v)[p,q,0]$ *is true if and only if* $p = q$*;*
- *each edge* $e \in \mathcal{E}$ *is labeled by the two formulæ* $Act(e)[Z]$ *and* $Res(e)[Z,Z']$.

Intuitively, $Dyn(v)$ represents the dynamics associated to the location v, $Inv(v)$ denotes the set of continuous values admitted during the evolution in v, $Act(e)$ identifies the set of continuous values from which the automaton can jump over the edge e, and $Res(e)$ characterizes a map that should be applied to the continuous values from which the automaton crosses the edge e. Section 2.3 details the formal meaning of these formulæ and describes the semantics of hybrid automata.

While hybrid automaton dynamics are classically described by using differential equations (see, e.g., [14, 13]), we adopt an approach based on first-order formulæ. However, in many cases, solutions, or approximated solutions, of the differential equations are computed before the automaton analysis (see, e.g., [13]). Whenever such (approximated) solutions are polynomials, the same dynamics expressed by differential equations can be defined in Tarski's theory.

Comparing our definition with the one in [6], we can notice that we add the condition $Dyn(v)[p,q,0]$ *implies* $p = q$. Intuitively, this means that if we are in p at time 0, we can reach a point different from

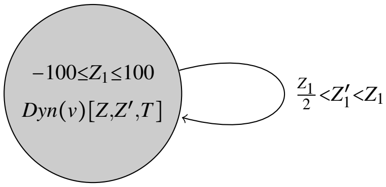

Figure 1: The hybrid automaton described in Example 1.

p through a continuous dynamics only if we let time flow. This assumption allows us to both get flow continuity at time 0 and slightly simplify the reachability formulæ with respect to the ones defined in [6].

Example 1. *Figure 1 depicts a graphical representation of the hybrid automaton $H = (Z, Z', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res)$, where $Z = \langle Z_1 \rangle$ and $Z' = \langle Z_1' \rangle$ and both Z_1 and Z_1' are variables over $\mathbb{R}$; $\mathcal{V} = \{v\}$ and $\mathcal{E} = \{(v,v)\}$; $Inv(v)[Z] \overset{def}{=} -100 \leq Z_1 \leq 100$; $Dyn(v)[Z,Z',T] \overset{def}{=} (T = 0 \wedge Z_1' = Z_1) \vee (T > 0 \wedge Z_1 < 2 * Z_1' \leq 2 * Z_1)$; $Res((v,v))[Z,Z'] \overset{def}{=} Z_1 < 2 * Z_1' < 2 * Z_1$; $Act((v,v))[Z] \overset{def}{=} \top$.*

2.3 Standard Semantics

The formula $Dyn(v)[Z,Z',T]$ holds if there exists a continuous flow going from Z to Z' in T time-instants. We admit an infinite number of flows, which can also be self-intersecting. Our semantics imposes the continuity of such flows.

Definition 2 (Hybrid Automata - Semantics)**.** *A* state *ℓ of H is a pair $\langle v, r \rangle$, where $v \in \mathcal{V}$ is a location and $s = \langle s_1, \ldots, s_{d(H)} \rangle \in \mathbb{R}^{d(H)}$ is an assignment of values for the variables of Z. A state $\langle v, s \rangle$ is* admissible *if $Inv(v)[s]$ is true. We have two kind of transitions:*

- *the* continuous transition relation $\to_C$*:*
  $\langle v, s \rangle \to_C \langle v, r \rangle \iff$ *there exists $f : \mathbb{R}_{\geq 0} \to \mathbb{R}^{d(H)}$ continuous function such that $s = f(0)$, there exists $t \geq 0$ such that $r = f(t)$, and for each $t' \in [0,t]$ $Inv(v)[f(t')]$ and $Dyn(v)[s, f(t'), t']$ hold;*
- *the* discrete transition relation $\to_D$*:*
  $\langle v, s \rangle \to_D \langle u, r \rangle \iff (v,u) \in \mathcal{E}$ *and both the formulæ $Act((v,u))[s]$ and $Res((v,u))[s,r]$ holds.*

Combining continuous and discrete transitions, we introduce the notions of *trace* and *reachability*. A trace is a sequence of continuous and discrete transitions. A point r is reachable from a point s if there is a trace starting from s and ending in r. We use $\ell \to \ell'$ to denote that either $\ell \to_C \ell'$ or $\ell \to_D \ell'$.

Definition 3 (Hybrid Automata - Reachability)**.** *A* trace *of length n of H is a sequence of admissible states $\ell_0, \ell_1, \ldots, \ell_n$, with $n \in \mathbb{N}_{>0}$, such that:*

- *for each $j \in [1,n]$ it holds $\ell_{j-1} \to \ell_j$;*
- *for each $j \in [1, n-1]$ if $\ell_{j-1} \not\to_D \ell_j$, then $\ell_j \to_D \ell_{j+1}$.*

In H, $s \in \mathbb{R}^{d(H)}$ reaches *$r \in \mathbb{R}^{d(H)}$ if there exists a trace $\ell_0, \ldots, \ell_n$ of H such that $\ell_0 = \langle v, s \rangle$ and $\ell_n = \langle u, r \rangle$, for some $v, u \in \mathcal{V}$. A set $\mathbb{I} \subseteq \mathbb{R}^{d(H)}$* reaches *$\mathbb{F} \subseteq \mathbb{R}^{d(H)}$ if there exists $s \in \mathbb{I}$ which reaches $r \in \mathbb{F}$.*

We impose the condition that, in a trace, continuous transitions do not occur consecutively. In hybrid automata whose flows are solutions of autonomous differential equations, the continuous transition relation is transitive, hence if a trace contains a sequences of consecutive continuous transitions, it can be reduced to a trace without consecutive continuous transitions. However, Definition 1 allows also automata whose continuous transition relation is not transitive. This can occur when the dynamics are solutions of non-autonomous differential equations. For instance, if the formula based dynamics are $\langle X_0+T, Y_0+T^2\rangle$, the set of points reachable from $\langle 0,0\rangle$ is, of course, $R=\{\langle t,t^2\rangle | t\in\mathbb{R}_{\geq 0}\}$. However, since, for every $r\in\mathbb{R}$, there exists a tuple $\langle t, r*t\rangle$ in R, by admitting multiple successive continuous transitions we would have obtained $\mathbb{R}^2$ as the reachability set which is visibly wrong.

Let us consider the case of hybrid automata whose dynamics are of the form $Dyn(v)[Z,Z',T] \overset{def}{=} Z' = f_v(Z,T)$, with f_v continuous (e.g., the case of solutions of vector fields). Let us call such automata *functional automata*. For functional automata it is easy to write a formula $R^i_H[Z,Z']$ which models the reachability with i discrete transitions (see, e.g., [6]). Since, such formulæ are first-order formulæ whose satisfiability is decidable, we can summarize this result saying that for this class of automata reachability within a fixed number of discrete transitions is decidable. However, the possibility of characterizing reachability within a fixed number of discrete transitions through formulæ does not imply the decidability of the reachability problem. As a matter of fact, even if the satisfiability of $R^i_H[Z,Z']$ is decidable, in order to solve the reachability problem we would need to test the satisfiability of an infinite number of formulæ, i.e., one for each $i\in\mathbb{N}$.

If we do not impose any further condition on the dynamics, it is not possible to write a first-order formula representing a continuous transition. As a matter of fact, our definition of $\rightarrow_C$ requires the existence of a continuous function f which satisfies the constraints Inv and Dyn, i.e., it requires to decide whether a selection problem has a solution (see Section 2.1). However, selection problems are neither expressible in our first-order language nor decidable in the general case. This is the main difference between our approach and the one presented in [9], where the continuity of the continuous transitions (called *act*) is not imposed.

In the next section we introduce a class of hybrid automata which generalizes functional automata still allowing to translate continuous transitions into formulæ.

2.4 Michael's Form Automata

In order to ensure the existence of a continuous function satisfying both invariant and dynamic constraints we need to check that such constraints meet the hypothesis of a selection theorem [2]. In particular, as in [6], we consider a class of automata based on Michael's selection result. The following definitions express Michael's hypothesis in the context of hybrid automata.

First we characterize the set valued map from which the continuous selection will take place.

Definition 4 (I^v_p,F^v_p)**.** *Let H be a hybrid automaton. Let v be a location of H and $p\in\mathbb{R}^{d(H)}$ such that $Inv(v)[p]$ holds. I^v_p is the interval of time instants satisfying the following: $\forall T\in I^v_p\ \exists Z'(Dyn(v)[p,Z',T]\wedge Inv(v)[Z'])$. The time instant 0 belongs to I^v_p, and I^v_p is maximal with respect to the first two requirements.*

The function $F^v_p : I^v_p \rightarrow \wp(\mathbb{R}^{d(H)})$ is defined as $F^v_p(T)=\{q \mid Dyn(v)[p,q,T]\wedge Inv(v)[q]\}$.

Since Michael's theorem [2] requires lower semi-continuity, closedness, and α-paraconvexity (see Section 2.1), we obtain the following class of hybrid automata.

Definition 5 (MF Automata [6])**.** *We say that a hybrid automaton H is in* Michael's Form*, or simply a* MF *automaton, if for each state $v\in\mathcal{V}$ and for each point $p\in\mathbb{R}^{d(H)}$ such that $Inv(v)[p]$ holds, the function F^v_p is lower semi-continuous, and for each $t\in I^v_p$ the set $F^v_p(t)$ is closed and α-paraconvex.*

As proved in [6] if a hybrid automaton is in Michael's form continuous transitions can be characterized through a formula. As a consequence, reachability within a fixed number of discrete transitions can be mapped into a satisfiability problem over semi-algebraic formulæ, as follows.

Let H be a MF automaton, and $v \in \mathcal{V}$ one of its locations. Consider the formula:

$$Tp(v)[Z,T] \overset{def}{=} \forall T'(0 \leq T' \wedge T' \leq T \rightarrow \exists Z'(Dyn(v)[Z,Z',T'] \wedge Inv(v)[Z'])).$$

If p satisfies $Inv(v)$, then it follows that $t \in I_p^v$ if and only if $Tp(v)[p,t]$ is true.

Definition 6 (MF Automata - Reachability Formula [6]). *Let H be a MF automaton. The formula $Reach_H^i(v,v')[Z,Z']$ is inductively defined as follows:*

$$Reach_H^0(v,v')[Z,Z'] \overset{def}{=} \begin{cases} \bot & \textit{if } v \neq v', \\ \exists T(T \geq 0 \wedge Dyn(v)[Z,Z',T] \wedge Tp(v)[Z,T]) \wedge \\ \qquad Inv(v)[Z] \wedge Inv(v)[Z'] & \textit{otherwise.} \end{cases}$$

$$Reach_H^{i+1}(v,v')[Z,Z'] \overset{def}{=} \bigvee_{\tilde{v} \in \mathcal{V}} (\exists Z_1 \exists Z_2 (Reach_H^i(v,\tilde{v})[Z,Z_1] \wedge Act((\tilde{v},v'))[Z_1] \wedge$$
$$Res((\tilde{v},v'))[Z_1,Z_2] \wedge Reach_H^0(v',v')[Z_2,Z'])).$$

Moreover, we define the formulæ:

$$Reach_H^i[Z,Z'] \overset{def}{=} \bigvee_{v,v' \in \mathcal{V}} Reach_H^i(v,v')[Z,Z'] \qquad \textit{and} \qquad Reach_H^{\leq i}[Z,Z'] \overset{def}{=} \bigvee_{j=0}^{i} Reach_H^j[Z,Z'].$$

As immediate consequence of [6], the above defined formulæ correctly characterize the notion of reachability within a fixed number of discrete transitions.

Lemma 1. *Let H be a MF automaton. Let $\mathbb{I}, \mathbb{F} \subseteq \mathbb{R}^{d(H)}$ be represented by the formulæ $I[Z], F[Z]$, respectively. The set $\mathbb{I}$ reaches the set $\mathbb{F}$ if and only if there exists $i \in \mathbb{N}$ such that the formula $Reach_H^i[Z,Z'] \wedge I[Z] \wedge F[Z']$ is satisfiable.*

In [6] it has also been shown that given a hybrid automaton H it is possible to decide whether it is a MF automaton or not, again through satisfiability problems over semi-algebraic formulæ.

Example 2. *Let us consider the Example 1. It is immediate to see that H is a MF automaton.*

In this case $Tp(v)[Z,T]$ is the formula $-100 \leq Z_1 \leq 100$, and hence $Reach_H^0[Z,Z']$ becomes $-100 \leq Z_1 \leq 100 \wedge -100 \leq Z_1' \leq 100 \wedge \frac{Z_1}{2} < Z_1' \leq Z_1$.

For this automaton, the computation of the reachability set does not converge. More precisely, at each iteration, while the reach set upper bound remains constant, the lower bound decreases by a quarter with respect to the lower bound of the previous reach set. Thus, only after an infinite number of iterations the lower bound would converge to zero.

3 Approximated Semantics

The standard semantics $\{\!|\varphi|\!\}$ of a formula φ with n free-variables over the reals is a subset of $\mathbb{R}^n$. Hence, once we have fixed a standard semantics function $\{\!|\cdot|\!\}$ which maps formulæ with n free-variables into subsets of $\mathbb{R}^n$, every other function of this type can be seen as an approximated semantics.

Definition 7 (Approximated Semantics). *An* approximated semantics *is a function $||\cdot|| : \bigcup_{n \in \mathbb{N}} \mathcal{F}_n \rightarrow \bigcup_{n \in \mathbb{N}} \wp(\mathbb{R}^n)$ such that for each $\varphi \in \mathcal{F}_n$, it holds that $||\varphi|| \subseteq \mathbb{R}^n$.*

If $\lfloor\!|\cdot|\!\rfloor$ is an approximated semantics such that for each formula φ it holds $\lfloor\!|\varphi|\!\rfloor \subseteq \{\!|\varphi|\!\}$, we can say that $\lfloor\!|\cdot|\!\rfloor$ is an *under-approximation* of the standard semantics, or simply an *under-approximation semantics*. Similarly, if $\lceil\!|\cdot|\!\rceil$ is such that $\{\!|\varphi|\!\} \subseteq \lceil\!|\varphi|\!\rceil$ is always true, then $\lceil\!|\cdot|\!\rceil$ is an *over-approximation semantics*. There are approximated semantics which are neither under nor over-approximations.

In [5] the authors observe that dense unbounded domains, which are the cause of undecidability of the reachability problem, are often abstractions of real world domains. In particular, they notice that, especially in the context of biological simulation, it is useful to avoid the ability to distinguish between values whose distance is less than a fixed ε. They introduce a new class of semantics for first-order formulæ, called ε-semantics, which guarantee the decidability of reachability in the case of automata with bounded invariants.

Definition 8 (ε-Semantics [5])**.** *Let $\varepsilon \in \mathbb{R}_{>0}$. For each formula $\psi \in \mathcal{F}_n$ let $\{\!|\psi|\!\}_\varepsilon \subseteq \mathbb{R}^n$, be such that:*

(ε) $\{\!|\psi|\!\}_\varepsilon = \varnothing$ *or exists $p \in \mathbb{R}^n$ s.t. $B(p,\varepsilon) \subseteq \{\!|\psi|\!\}_\varepsilon$*

($\cap$) $\{\!|\psi_1 \wedge \psi_2|\!\}_\varepsilon \subseteq \{\!|\psi_1|\!\}_\varepsilon \cap \{\!|\psi_2|\!\}_\varepsilon$

($\cup$) $\{\!|\psi_1 \vee \psi_2|\!\}_\varepsilon = \{\!|\psi_1|\!\}_\varepsilon \cup \{\!|\psi_2|\!\}_\varepsilon$

($\forall$) $\{\!|\forall X \psi[X,Z]|\!\}_\varepsilon = \{\!| \bigwedge_{r\in\mathbb{R}} \psi[r,Z]|\!\}_\varepsilon$

($\exists$) $\{\!|\exists X \psi[X,Z]|\!\}_\varepsilon = \bigcup_{r\in\mathbb{R}} \{\!|\psi[r,Z]|\!\}_\varepsilon$

($\neg$) $\{\!|\psi|\!\}_\varepsilon \cap \{\!|\neg\psi|\!\}_\varepsilon = \varnothing$

Any semantics $\{\!|\cdot|\!\}_\varepsilon$ satisfying the above conditions is said to be an ε-semantics.

In the above definition, as done in [5], with a slight abuse of notation we use $\bigwedge_{r\in\mathbb{R}} \psi$ to treat an infinite conjunction of formulæ as a formula. The Algorithm 1, given in [5], computes the sets of reachable states of a given automaton and describes sets of points through formulæ.

Algorithm 1 Reachability($H, I[Z], \{\!|\cdot|\!\}_\varepsilon$)

```
$R[Z] \leftarrow I[Z]$
$N[Z] \leftarrow \bot$
repeat
    $R[Z] \leftarrow R[Z] \vee N[Z]$
    $N[Z] \leftarrow \exists Z'(Reach_H^{\leq 1}[Z',Z] \wedge R[Z'])$
until $\{\!|N[Z] \wedge \neg R[Z]|\!\}_\varepsilon \neq \varnothing$ is true
return $\{\!|R[Z]|\!\}_\varepsilon$
```

The reachability is computed incrementing at each step the number of discrete transitions: new reachable sets of points are computed until they become too small to be identified in the ε-semantics. In the case of hybrid automata with bounded invariants such reachability algorithm always terminates. If we replace the ε-semantics with the standard one, each step of the above algorithm under-approximates the set of reachable points. However, it still may not end even in the case of bounded invariants.

The *sphere semantics* $(\!|\cdot|\!)_\varepsilon$ (see e.g., [5]) is an ε-semantics which is neither an over nor an under-approximation semantics. The set $(\!|\psi|\!)_\varepsilon$, where $\varepsilon \in \mathbb{R}_{>0}$, is defined as follows:

(ε) $(\!|t_1 \circ t_2|\!)_\varepsilon \overset{def}{=} B(\{\!|t_1 \circ t_2|\!\}, \varepsilon)$, for $\circ \in \{=, <\}$

($\cap$) $(\!|\psi_1 \wedge \psi_2|\!)_\varepsilon \overset{def}{=} \bigcup_{B(p,\varepsilon)\subseteq(\!|\psi_1|\!)_\varepsilon \cap (\!|\psi_2|\!)_\varepsilon} B(p,\varepsilon)$

($\cup$) $(\!|\psi_1 \vee \psi_2|\!)_\varepsilon \overset{def}{=} (\!|\psi_1|\!)_\varepsilon \cup (\!|\psi_2|\!)_\varepsilon$

($\forall$) $(\!|\forall X \psi[X,Z]|\!)_\varepsilon \overset{def}{=} \bigcup_{B(p,\varepsilon)\subseteq \bigcap_{r\in\mathbb{R}} (\!|\psi[r,Z]|\!)_\varepsilon} B(p,\varepsilon)$

($\exists$) $(\!|\exists X \psi[X,Z]|\!)_\varepsilon \overset{def}{=} \bigcup_{r\in\mathbb{R}} (\!|\psi[r,Z]|\!)_\varepsilon$

($\neg$) $(\!|\neg\psi|\!)_\varepsilon \overset{def}{=} \bigcup_{B(p,\varepsilon)\cap(\!|\psi|\!)_\varepsilon = \varnothing} B(p,\varepsilon)$

Example 3. *Let H be as in Example 1. The sphere semantics with $\varepsilon = 0.5$ gives us* $(\![Reach^0_H[10,Z']]\!)_\varepsilon = (4.5,10.5)$*,* $(\![Reach^1_H[10,Z']]\!)_\varepsilon = (0.75,10.5)$*,* $(\![Reach^2_H\ [10,Z']]\!)_\varepsilon = (-0.19,10.5)$*, and* $(\![Reach^3_H[10,Z']]\!)_\varepsilon = (-0.42,10.5)$*. Thus, the reachability algorithm described in [5] over H, instantiated with the sphere semantics with $\varepsilon = 0.5$, halts and returns as result the set* $(-0.19,10.5)$*, since the difference between* $(\![Reach^2_H[10,Z']]\!)_\varepsilon$ *and* $(\![Reach^3_H[10,Z']]\!)_\varepsilon$ *is smaller than an open sphere of radius $\varepsilon = 0.5$.*

This example also points out that whenever a variable is quantified in a formula, the ε-semantics evaluates it with all the possible constants, and hence there are no approximation effects on it. As a matter of fact $(\![Reach^1_H[10,Z']]\!)_\varepsilon$ *does not include the interval* $[10.5,11,5)$ *which would be included if the quantified variables in the formula* $Reach^1_H[10,Z']$ *were over-approximated.*

It is immediate to prove that, due to rule $(\neg)$, ε-semantics are never over-approximation semantics. As a consequence of this fact and of the structure of the reachability algorithm, the approach proposed in [5] is not taylored for over-approximating reachability. In Section 5.2 we show how to exploit ε-semantics for under-approximation.

4 Disturbed Automata

In this section we present the approach proposed by Fränzle in [9] for the over-approximation of reachability. In particular, we briefly recall the framework described in [9] and then we establish some general relationships with the framework we introduced in Section 2.

Fränzle noticed that real hybrid systems are always subject to noise, suspecting that their continuous components can provide only finite memory. If so, the state space of such automata would be the product of the size of the discrete state space and the effective size of the continuous state space modulo noise. This means that the reach set computation of hybrid automata modeling real systems, should converge finitely, yielding decidability of state reachability.

The definition of hybrid automata given in [9] slightly differs from Definition 1. Specifically, activations and resets are characterized by a single formula called *transition predicate* $trans_{v\to v'}$. Similarly, invariants and dynamic laws are merged in the *activity predicate* act_v, which does not impose any constraint on the continuity of the dynamic laws.

Definition 9 (Fränzle Hybrid Automata - Syntax [9])**.** *A* Fränzle hybrid automaton $H = (\mathcal{V}, Z', (act_v)_{v\in\mathcal{V}}, (trans_{v\to v'})_{v,v'\in\mathcal{V}}, (initial_v)_{v\in\mathcal{V}}, (safe_v)_{v\in\mathcal{V}})$ *of dimension $d \in \mathbb{N}$ consists of the following components:*

- *$\mathcal{V}$ is a finite set, representing the discrete locations;*
- *Z is a vector of variable names of dimension d, representing the continuous variables of H;*
- *each $v \in \mathcal{V}$ is labeled with a formula $act_v[Z,Z']$ representing the continuous activities and corresponding state constraints;*
- *each pair of locations $v, v' \in \mathcal{V}$ is labeled with a formula $trans_{v\to v'}[Z,Z']$ representing the discrete transitions and their guarding conditions;*
- *each $v \in \mathcal{V}$ is labeled with the formulæ $initial_v[Z]$ and $safe_v[Z]$ representing the initial and the safe states of the hybrid automaton.*

As far as the semantics is concerned, the reachability formula $\Phi(H)^i_{v\to v'}$ is defined as follows [9]:

$$\Phi(H)^0_{v\to v'}[Z,Z'] \overset{def}{=} \begin{cases} act_v[Z,Z'] & \text{if } v = v', \\ \bot & \text{otherwise.} \end{cases}$$

$$\Phi(H)^{i+1}_{v\to v'}[Z,Z'] \overset{def}{=} \bigvee_{\tilde{v}\in\mathcal{V}} \exists Z_1 \exists Z_2 (\Phi(H)^{i}_{v\to\tilde{v}}[Z,Z_1] \wedge trans_{\tilde{v}\to v'}[Z_1,Z_2] \wedge act_{v'}[Z_2,Z']).$$

An automaton is said to be *safe* if the initial states can only reach *safe* states.

We formalize how a MF automaton can be mapped into an automaton w.r.t. Definition 9.

Definition 10 (Corresponding Fränzle Automaton)**.** *Given a MF automaton $H = (Z,Z',T,\mathcal{V},\mathcal{E},Inv,Dyn,Act,Res)$ and two formulæ $I[Z]$ and $F[Z]$, the* corresponding Fränzle automaton *is the automaton $Fr(H,I,F) \overset{def}{=} (\mathcal{V}, Z', (act_v\,)_{v\in\mathcal{V}}, (trans_{v\to v'})_{v,v'\in\mathcal{V}}, (initial_v)_{v\in\mathcal{V}}, (safe_v)_{v\in\mathcal{V}})$ where:*

- *for each $v \in \mathcal{V}$, $act_v \overset{def}{=} Reach^0_H(v,v)$, $initial_v \overset{def}{=} Inv(v)[Z] \wedge I[Z]$, and $safe_v \overset{def}{=} Inv(v)[Z] \wedge \neg F[Z]$;*
- *for each $e = (v,v') \in \mathcal{E}$, $trans_{v\to v'} \overset{def}{=} Act(e) \wedge Res(e)$, while for each $(v,v') \notin \mathcal{E}$, $trans_{v\to v'} \overset{def}{=} \perp$.*

Such translation establishes the following relationship between the formulæ $\Phi(Fr(H,I,F))^i_{v\to v'}$ of [9] and our reachability formulæ.

Lemma 2. *Let H be a MF automaton, $I[Z]$ and $F[Z]$ be two formulæ. Let $Fr(H,I,F)$ be the corresponding Fränzle automaton. For each $i \in \mathbb{N}$ it holds that $\{\!|\Phi(Fr(H,I,F))^i_{v\to v'}[Z,Z']|\!\} = \{\!|Reach^i_H(v,v')[Z,Z']|\!\}$.*

Hence, our notion of reachability corresponds to a non safety condition.

Theorem 1. *Let H be a MF automaton, $I[Z]$ and $F[Z]$ be two formulæ representing $\mathbb{I}$ and $\mathbb{F}$, respectively. Let $Fr(H,I,F)$ be the corresponding Fränzle automaton. $\mathbb{I}$ reaches $\mathbb{F}$ in H if and only if $Fr(H,I,F)$ is not safe.*

Given a hybrid automaton H, Fränzle defines $\widetilde{H}$, called the *disturbed variant of noise level* ε, as the automaton obtained from H perturbing all the activity predicates, i.e., expanding the activity predicates by an open sphere of radius ε. Thus, since every activity predicate of an automaton $Fr(H,I,F)$ corresponds to the reachability formula $Reach^0_H$, we can define a disturbed variant of H as follows.

Definition 11 (Disturbed Automata)**.** *Let us consider a MF automaton H. The MF automaton $\widetilde{H} = (Z,Z',T,\mathcal{V},\mathcal{E}, \widetilde{Inv},\widetilde{Dyn},Act,Res)$ is a* disturbed variant *of H if and only if for each $v \in \mathcal{V}$ it holds that $\{\!|Reach^0_H(v,v)[Z,Z']|\!\} \subseteq \{\!|Reach^0_{\widetilde{H}}\,(v,v)[Z,Z']|\!\}$.*

Moreover, let $\varepsilon \in \mathbb{R}_{>0}$. We say that a disturbance $\widetilde{H}$ of H is a disturbance of noise level ε or more *if and only if for each $v \in \mathcal{V}$ it holds that $\{\!|\exists Z''(Reach^0_H(v,v)[Z,Z''] \wedge \delta(Z'',Z') < \varepsilon)|\!\} \subseteq \{\!|Reach^0_{\widetilde{H}}(v,v)[Z,Z']|\!\}$.*

In the above definition we refer to the standard euclidian distance δ. Our definition of disturbed variants is an instance of Fränzle definition in the following sense.

Lemma 3. *Let H be a MF automaton. $I[Z]$ and $F[Z]$ be two formulæ. Let $Fr(H,I,F)$ be the corresponding Fränzle automaton. If $\widetilde{H}$ is a disturbed variant of H, $Fr(\widetilde{H},I,F)$ is a disturbed variant of $Fr(H,I,F)$ w.r.t. Fränzle's definition. If $\widetilde{H}$ is a disturbance of noise level ε or more, so is $Fr(\widetilde{H},I,F)$.*

As a consequence, exploiting Lemma 2 of [9], we get the following theorem which states how $\widetilde{H}$ can be used to over-approximate reachability over H.

Theorem 2. *Let H be a MF automaton, $\widetilde{H}$ be a disturbed variant of H of noise level $\gamma > 0$, and $I[Z]$ be a formula. If $\{\!|\widetilde{Inv}(v)[Z]|\!\}$ is bounded for each $v \in \mathcal{V}$, then there exists $i \in \mathbb{N}$ such that:*

$$\bigcup_{n\in\mathbb{N}} \{\!|Reach^n_H[Z,Z'] \wedge I[Z]|\!\} \subseteq \bigcup_{n=0}^{i} \{\!|Reach^n_{\widetilde{H}}[Z,Z'] \wedge I[Z]|\!\}.$$

Moreover, i can be effectively computed.

5 Mixing the Approaches

In this section we first re-describe Fränzle's reachability algorithm in terms of approximated semantics, obtaining an over-approximation reachability algorithm which does not explicitly refer to $\widetilde{H}$. Then we focus on under-approximations of reachability based on ε-semantics.

5.1 Over-Approximation

We define a new approximated semantics, named *tilde semantics*, which captures the introduction of noise in hybrid automata.

Definition 12 (Tilde Semantics)**.** *Let ψ be a formula and let $\varepsilon \in \mathbb{R}_{>0}$. The* tilde semantics *of ψ is $\langle\!|\psi|\!\rangle_\varepsilon \overset{def}{=} B(\{\!|\psi|\!\},\varepsilon)$.*

Such semantics applied to H under-approximates each ε-disturbance of H in the following sense.

Theorem 3. *Let H be a MF automaton and $\widetilde{H}$ be a disturbance of noise level ε or more. For each $v,v' \in \mathcal{V}$, for each $p \in \mathbb{R}^{d(H)}$ it holds that $\langle\!|Reach^i_H(v,v')[p,Z']|\!\rangle_\varepsilon \subseteq \{\!|Reach^i_{\widetilde{H}}(v,v')[p,Z']|\!\}$.*

Hence, exploiting Theorem 3 we get the following result.

Corollary 1. *Let H be a MF automaton, $\widetilde{H}$ be a disturbance of noise level ε or more with respect to δ, and $I[Z]$ be a formula. If for each $v \in \mathcal{V}$ it holds that $\{\!|\widetilde{Inv}(v)[Z]|\!\}$ is bounded, then there exists $i \in \mathbb{N}$ such that $\bigcup_{n\in\mathbb{N}}\{\!|Reach^n_H[Z,Z'] \wedge I[Z]|\!\} \subseteq \bigcup_{n\in\mathbb{N}}\langle\!|Reach^n_H[Z,Z'] \wedge I[Z]|\!\rangle_\varepsilon \subseteq \bigcup_{n=0}^{i}\{\!|Reach^n_{\widetilde{H}}[Z,Z'] \wedge I[Z]|\!\}$. Moreover, i can be effectively computed.*

The following definition characterizes an ε-disturbance whose semantics is minimal, i.e., it is included in all ε-disturbance semantics.

Definition 13 (Tilde Transformation)**.** *Let $\mathcal{T}$ be a first-order theory over the reals, $\psi[Z]$ be any first-order formula $\mathcal{T}$-definable, and $\varepsilon \in \mathbb{R}_{>0}$. The* tilde transformation *of $\psi[Z]$ is defined as follows:*

$$\widetilde{(\psi[Z])}_\varepsilon \overset{def}{=} \exists Z_0(\psi[Z_0] \wedge \delta(Z_0,Z) < \varepsilon).$$

Theorem 4. *Let $\mathcal{T}$ be any first-order theory and $\psi[X] \in \mathcal{T}$. The tilde semantics of $\psi[X]$ is $\mathcal{T}$-definable and, in particular, $\langle\!|\psi[X]|\!\rangle_\varepsilon = \{\!|\widetilde{(\psi[X])}_\varepsilon|\!\}$ for all $\varepsilon \in \mathbb{R}_{>0}$.*

Definition 14 (Minimum Disturbed Variant)**.** *Let H be a MF automaton, $I[Z]$ and $F[Z]$ be formulæ, and $\varepsilon \in \mathbb{R}_{>0}$. The* minimum ε disturbed variant of *H, $Fr\widetilde{(H,I,F)} = (\mathcal{V},Z', (\widetilde{act}_v)_{v\in\mathcal{V}},(\widetilde{trans}_{v\to v'})_{v,v'\in\mathcal{V}}, (\widetilde{initial}_v)_{v\in\mathcal{V}},(\widetilde{safe}_v)_{v\in\mathcal{V}})$, is the disturbed variant of $Fr(H,I,F)$ of noise level ε obtained considering for each $v \in \mathcal{V}$, $\widetilde{act}_v \overset{def}{=} \exists Z''(Reach^0_H(v,v)[Z,Z''] \wedge \delta(Z'',Z') < \varepsilon)$, while the other components are defined as for $Fr(H,I,F)$.*

Tilde semantics precisely captures the continuous semantics of $Fr\widetilde{(H,I,F)}$.

Lemma 4. *Let H be a MF automaton, $I[Z]$ and $F[Z]$ be formulæ, and $\varepsilon \in \mathbb{R}_{>0}$. $Fr\widetilde{(H,I,F)}$ is an ε disturbed variant of $Fr(H,I,F)$. Moreover, for each $v \in \mathcal{V}$ and $p \in \mathbb{R}^{d(H)}$ it holds $\langle\!|Reach^0_H(v,v)[p,Z']|\!\rangle_\varepsilon = \{\!|\Phi(Fr\widetilde{(H,I,F)})^0_{v\to v}[p,Z']|\!\}$.*

The above result cannot be generalized to $Reach^n_H$ and $\Phi(Fr\widetilde{(H,I,F)})^n$. In particular, the tilde semantics of the first-one in the general case is strictly included in the standard semantics of the second one. This is due to the fact that the first formula is built closing intermediate steps through quantifiers, which means that the intermediate steps are not approximated. On the other hand, in the second formula each step is over-approximated.

Lemma 4 enables us to rephrase the algorithm described by Fränzle as Algorithm 2.

Algorithm 2 Tilde$(H, I[Z], \varepsilon)$

```
$R \leftarrow \bigcup_{p\in\{\!|I[Z]|\!\}} (\!|Reach^0_H[p,Z']|\!)_\varepsilon$
repeat
    $V \leftarrow R$
    $R \leftarrow \bigcup_{p\in R} \{\!| \bigvee_{(v,v')\in\mathcal{E}} (Act((v,v'))[p] \wedge Res((v,v'))[p,Z']|\!\}$
    $R \leftarrow \bigcup_{p\in R} (\!|Reach^0_H[p,Z']|\!)_\varepsilon$
    $R \leftarrow R \cup V$
until $\bigcup_{p\in V} \{\!|Reach^{\leq 1}_H[p,Z']|\!\} \nsubseteq V$ is true
return $V$
```

Theorem 5. *Let H be a MF automaton with bounded invariants, $I[Z]$ be a formula, and $\varepsilon \in \mathbb{R}_{>0}$.* Tilde$(H, I[Z], \varepsilon)$ *always terminates returning a set R such that $\bigcup_{n\in\mathbb{N}} \{\!|Reach^n_H[Z,Z'] \wedge I[Z]|\!\} \subseteq R$, i.e., it over-approximate reachability.*

Example 4. *Let us consider the hybrid automaton H described by Example 1. The sets R and V calculated by the first three iterations of Algorithm 2, with $\{\!|I[Z]|\!\} = \{10\}$ and $\varepsilon = 0.5$, are $R^1 = (4.5, 10.5)$ and $V^1 = (1.13, 10.5)$, $R^2 = (0.75, 10.5)$ and $V^2 = (0.19, 10.5)$, $R^3 = (-0.19, 10.5)$ and $V^3 = (-0.05, 10.5)$. Since $V^3 \subset R^3$, the algorithm halts and returns as result the set $(-0.19, 10.5)$, which is an over-approximation of the standard reach set of H, i.e., $(0, 10]$.*

5.2 Under-Approximation

Fränzle's approach can be used to under-approximate reachability over H by defining an automaton H' such that $\widetilde{H'} = H$. However, this would give us an under-approximation algorithm in which at each step an under-approximation of $Reach^1$ is applied. In this section we show that the approach proposed in [5] can always be used to under-approximate reachability, no matter which ε-semantics is considered. Moreover, when the considered ε-semantics is an under-approximation semantics, we get an algorithm in which the same under-approximations are applied to both termination conditions and output.

We start introducing a new semantics, called *bottom semantics*.

Definition 15. *Let ψ be a formula and $\varepsilon \in \mathbb{R}_{>0}$. The set $]\!]\psi[\![_\varepsilon$ is the* bottom semantics *of ψ and it is defined by structural induction on ψ itself as follows:*

- $]\!]t_1 \circ t_2[\![_\varepsilon = \bigcup_{B(p,\varepsilon)\subseteq\{\!|t_1\circ t_2|\!\}} B(p,\varepsilon)$, *for* $\circ \in \{=, <\}$;
- $]\!]\psi_1 \wedge \psi_2[\![_\varepsilon = \bigcup_{B(p,\varepsilon)\subseteq]\!]\psi_1[\![_\varepsilon \cap]\!]\psi_2[\![_\varepsilon} B(p,\varepsilon)$;
- $]\!]\psi_1 \vee \psi_2[\![_\varepsilon =]\!]\psi_1[\![_\varepsilon \cup]\!]\psi_2[\![_\varepsilon$;
- $]\!]\forall X \psi[X,Z][\![_\varepsilon = \bigcup_{B(p,\varepsilon)\subseteq\bigcap_{r\in\mathbb{R}}]\!]\psi[r,Z][\![_\varepsilon} B(p,\varepsilon)$;
- $]\!]\exists X \psi[X,Z][\![_\varepsilon = \bigcup_{r\in\mathbb{R}}]\!]\psi[r,Z][\![_\varepsilon$;
- $]\!]\neg\psi[\![_\varepsilon = \bigcup_{B(p,\varepsilon)\cap\{\!|\psi|\!\}=\varnothing} B(p,\varepsilon)$.

The bottom semantics is an ε-semantics. Moreover, any variable assignment, that satisfies a formula ψ in the bottom semantics, satisfies ψ in the standard Tarski's semantics too.

Lemma 5. *The bottom semantics is an ε-semantics. Moreover, $]\!]\psi[\![_\varepsilon \subseteq \{\!|\psi|\!\}$ for each formula ψ.*

The bottom semantics is definable in the Tarski's theory, i.e., if ψ is a formula of the first-order language of the reals equipped of sum, product and comparison relations, then there exists a formula $\widehat{\psi}_\varepsilon$ such that $]\!]\psi[\![_\varepsilon = \{\!|\widehat{\psi}_\varepsilon|\!\}$. Moreover, $\widehat{\psi}_\varepsilon$ is computable.

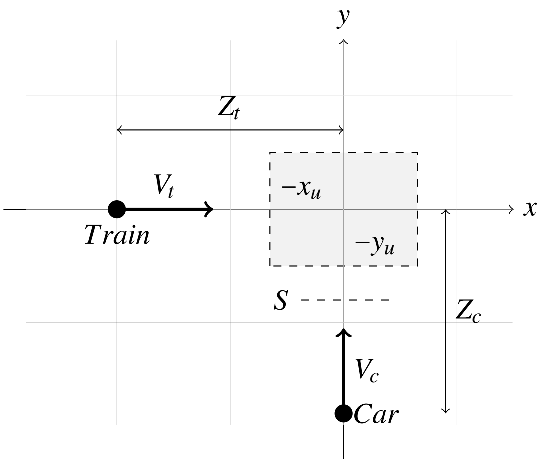

Figure 2: A case of study: a railroad crossing.

6 Implementation and Tests

We implemented our framework and algorithms exploiting the translations of approximated semantics into the standard one, and then relying on quantifier elimination packages. In particular, we developed a tool to work with Tarski's formulæ and to compute, given a formula ψ, the formulæ $\widetilde{\psi}_\varepsilon$ and $\widehat{\psi}_\varepsilon$. The evaluation of the termination conditions of both the algorithms are obtained by first translating the ε-semantics of the involved formulæ in the corresponding Tarski's formulæ, and then using `Redlog-QEPCAD` to eliminate the quantifiers as described in [20].

We tested our implementation on a railroad crossing scenario without barriers (see Figure 2): a train and a car are simultaneously approaching to the railroad crossing at coordinates $(0,0)$; the train is moving along the x axis with speed V_t while the car has speed V_c and runs the y axis. The variables Z_t and Z_c denote the distances between the railroad crossing and the train and between the railroad crossing and the car, respectively. The car sensors can identify the approaching train only above the line S. At that point it can decide to either accelerate or slow down. The car acceleration A_c should be once and for all and cannot be changed anymore. Our goal is to select an A_c such that the two vehicles pass safely through the railroad crossing.

In this case-study, we suppose we do not know with absolute precision the speeds of the two vehicles. This means that, in a specific instant, the velocities belong to an interval, rather than being a single value. For this reason, we will use inequalities to describe the dynamic laws.

We model the scenario depicted in Figure 2 by a hybrid automaton $H = (Z, Z', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res)$ where:

- $Z = \langle Z_t, Z_c, V_t, V_c, A_c \rangle$ and $Z' = \langle Z'_t, Z'_c, V'_t, V'_c, A'_c \rangle$ are variables over $\mathbb{R}^5$;
- $\mathcal{V} = \{q_0, q_c, q_s, q_u\}$ and $\mathcal{E} = \{e_0 = (q_0, q_c), e_1 = (q_c, q_u), e_2 = (q_c, q_s)\}$;
- $Inv(q_0) \overset{def}{=} Z_c \leq S \wedge V_c \in [c_m, c_M] \wedge V_t \in [t_m, t_M]$;
  $Inv(q_c) \overset{def}{=} ((Z_c \in [S, y_u] \wedge Z_t \leq -x_u) \vee (Z_c \in [S, -y_u] \wedge Z_t \in [-x_u, x_u])) \wedge V_c \in [c_m, c_M] \wedge V_t \in [t_m, t_M]$;
  $Inv(q_u) \overset{def}{=} Z_c \in [-y_u, y_u] \wedge Z_t \in [-x_u, x_u] \wedge V_c \in [c_m,\ c_M] \wedge V_t \in [t_m, t_M]$;
  $Inv(q_s) \overset{def}{=} (Z_c \geq y_u \vee Z_t \geq x_u) \wedge V_c \in [c_m, c_M] \wedge V_t \in [t_m, t_M]$;

- $Dyn(q_c) \overset{def}{=} V_c' - A_c * T - V_c \in [-d,d] \wedge 2 * Z_c' - A_c * T^2 - 2 * V_c * T - 2 * Z_c \in [-d,d] \wedge Z_t' - V_t * T - Z_t \in [-d,d]$;
  $Dyn(q_u) \overset{def}{=} Dyn(q_s) \overset{def}{=} Dyn(q_0)[Z,Z',T] \overset{def}{=} Z_t' - Z_t \in [t_m,t_M] * T \wedge Z_c' - Z_c \in [c_m,c_M] * T$;
- $Act(e_0) \overset{def}{=} Z_c = S$; $Act(e_1) \overset{def}{=} (Z_c \geq -y_u - d \wedge Z_t \in [-x_u,x_u]) \vee (Z_t \geq -x_u - d \wedge Z_c \in [-y_u,y_u])$;
  $Act(e_2) \overset{def}{=} (Z_c = y_u \wedge Z_t < -x_u) \vee (Z_t = x_u \wedge Z_c < -y_u)$.
- $Res(e_2) \overset{def}{=} Res(e_1) \overset{def}{=} A_c' \in [E_m,E_M] \wedge V_c' \in [c_m,c_M] \wedge V_t' \in [t_m,t_M]$; $Res(e_0) \overset{def}{=} A_c' \in [E_m,E_M]$.

where $c_m = 1$ and $C_m = 3$ are the minimal and the maximal admitted speed for the car, $t_m = 1$ and $T_m = 3$ are the minimal and the maximal admitted speed for the train, and $E_m = 0$ and $E_M = 10$ are the minimal and the maximal admitted car acceleration, respectively.

Location q_0 corresponds to the phase in which the train and the car are far apart from the crossing. When the car reaches the S line, the automaton goes to location q_c and the car non-deterministically chooses its acceleration. Whenever the car and the train cross the intersection at the same time, a collision occurs and the automaton goes to the location q_u. The q_s represents the safe situation in which at least one of the two vehicles has passed through the crossing, while the other has not yet reached it.

We would like to decide, once the car has reached the position S, which accelerations avoid the collision as a function of train speed, train position, and car speed.

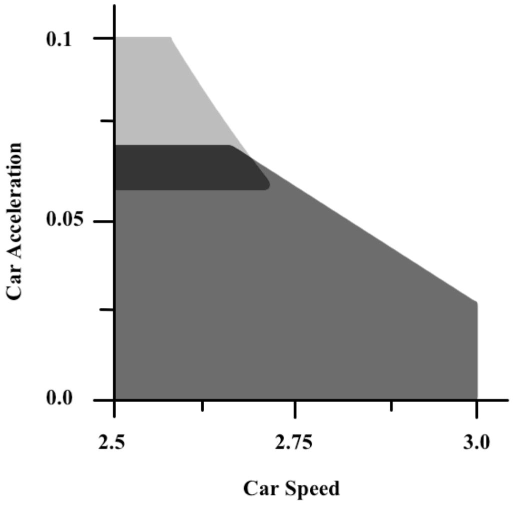

Figure 3: A graphical representation of the analysis performed on the test case with $y_u = 2$, $x_u = 4$, and $d = 0.2$. This figure depicts the space plane defined by the values $V_t = 2$ and $Z_t = -20$ in the region $V_c \in [2.5, 3.0]$ and $A_c \in [0, 0.1]$. The light, medium, and dark gray represent the sets $\rrbracket \psi_{\text{sf}} \llbracket_{\varepsilon} \setminus \llparenthesis \psi_{\text{un}} \rrparenthesis_{\varepsilon}$, $\rrbracket \psi_{\text{sf}} \llbracket_{\varepsilon} \cap \llparenthesis \psi_{\text{un}} \rrparenthesis_{\varepsilon}$, and $\llparenthesis \psi_{\text{un}} \rrparenthesis_{\varepsilon} \setminus \rrbracket \psi_{\text{sf}} \llbracket_{\varepsilon}$, respectively. If, given a car speed, we select an opportune acceleration such that the corresponding point is light gray colored, then we will certainly avoid the collision.

We modeled the automaton that represents the railroad crossing and we computed the two formulæ ψ_{un} and ψ_{sf}: the former represents all the situations in which the car has both reached the line S and selected an acceleration A_c that, sooner or later, leads to a collision; the latter characterizes all the states that avoid the collision itself. The formula ψ_{un} depicts a jump over the edge (q_0, q_c) and a successive continuous evolution ending up into the activation region of (q_c,q_u), while ψ_{sf} concludes the evolution into the activation of (q_c,q_s). We symbolically evaluated the tilde semantics of ψ_{un} and the bottom semantics of ψ_{sf} obtaining unquantified formulæ, ψ'_{un} and ψ'_{sf}, respectively, in 4 free variables which represent the train speed, the train position, the car speed, and the car acceleration at the beginning of the computation in the two opposite situation. In order to avoid the collision, whenever the car reaches line S and selects an acceleration A_c, it has to check that the current state satisfies ψ'_{sf} and does not satisfy ψ'_{un}. Figure 3 depicts the evaluation of such formulæ in a portion of the state space.

7 Conclusions

In this paper we considered Michael's form hybrid automata, a class of automata particularly suitable for approximations. On the basis of the observation that infinite precision of the models does not reflect real systems behaviors, we introduced and discussed different approximation techniques over this class of automata. On the one hand, our comparison points out that disturbed automata cannot be formulated in terms of an ε-semantics. As a matter of fact, ε-semantics never over-approximate standard semantics. On the other hand, we demonstrate that Fränzle's approach can be modeled through a new semantics (tilde semantics) which provides an over-approximation of the original reach space of the hybrid automaton. However, it is important to notice that Fränzle's reachability algorithm cannot be mapped into a completely symbolic algorithm (similar to the one presented in [5]) since at each iteration it over-approximates the reached set, while a symbolic algorithm would construct a new formula (nesting quantifiers) at each step and evaluate its approximated semantics only at the end of the computation. Hence, since quantified variables are never approximated, such a symbolic algorithm would over-approximate only the last step.

Drawing inspiration from both disturbed hybrid automata and symbolic algorithms, we formalized a new ε-semantics (bottom semantics) which plays a symmetrical role with respect to the introduction of noise. If the disturbance of the continuous components expands trajectories, the application of bottom semantics reduces it, under-approximating the reachability set. So, we can say the bottom semantics describes a process of noise filtering in hybrid automata. In particular, since we exploit on bottom semantics the symbolic algorithmic approach described in [5], we use the same level of approximation for both halting conditions and output. Of course, reachability could be under-approximated using standard semantics and simply halting computation after a finite number of discrete steps. The meaning of our under-approximation is that we interpret bottom semantics as the "correct" semantics for noise filtering.

As future work we plan to extend our comparisons to other general frameworks for approximation techniques, such as the ones based on topology (see, e.g., [7, 8]). In those frameworks instead of using distances among points, as we did, the authors defined distances among trajectories. Some basic differences between our approach and the one used in [7] can be noticed considering the bouncing ball example presented both in [5] and in [7]. While in [5] the infinite sequence of bounces cannot be observed since at a certain point these are smaller than the ε-precision, in [7] a compactification of the space is introduced to ensure convergence.

References

[1] R. Alur, C. Courcoubetis, T. A. Henzinger & P. H. Ho (1993): *Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems*. In: *Hybrid Systems*, *LNCS* 736, Springer, pp. 209–229, doi:10.1007/3-540-57318-6_30.

[2] J. P. Aubin & A. Cellina (1984): *Differential Inclusions*. A Series of Comprehensive Studies in Mathematics 264, Springer, doi:10.1007/978-3-642-69512-4.

[3] S. Basu (1997): *An Improved Algorithm for Quantifier Elimination Over Real Closed Fields*. In: IEEE Symposium on Foundations of Computer Science (FOCS'97), IEEE Computer Society Press, pp. 56–65, doi:10.1109/SFCS.1997.646093.

[4] A. Casagrande, T. Dreossi & C. Piazza (2012): *Hybrid Automata and ε-Analysis on a Neural Oscillator*. In: Proc. of the 1st International Workshop on Hybrid Systems and Biology, EPTCS 92, pp. 58–72, doi:10.4204/EPTCS.92.5.

[5] A. Casagrande, C. Piazza & A. Policriti (2009): *Discrete Semantics for Hybrid Automata*. Discrete Event Dynamic Systems 19(4), pp. 471–493, doi:10.1007/s10626-009-0082-7.

[6] A. Casagrande, C. Piazza, A. Policriti & B. Mishra (2008): *Inclusion dynamics hybrid automata*. Information and Computation 206(12), pp. 1394–1424, doi:10.1016/j.ic.2008.09.001.

[7] Pieter Collins (2005): *Hybrid Trajectory Spaces*. Technical Report, Centrum voor Wiskunde en Informatica (CWI).

[8] J. Davoren & I. Epstein (2008): *Topologies, Convergence, and Uniformities in General Hybrid Path Spaces,*. Preprint.

[9] M. Fränzle (1999): *Analysis of Hybrid Systems: An ounce of realism can save an infinity of states*. In: Computer Science Logic (CSL'99), LNCS 1683, Springer, pp. 126–140, doi:10.1007/3-540-48168-0_10.

[10] A. Girard, A. A. Julius & G. J. Pappas (2008): *Approximate Simulation Relations for Hybrid Systems*. Discrete Event Dynamic Systems 18(2), pp. 163–179, doi:10.1007/s10626-007-0029-9.

[11] T. A. Henzinger, P. W. Kopke, A. Puri & P. Varaiya (1995): *What's decidable about hybrid automata?* In: Proc. of ACM Symposium on Theory of Computing (STOCS'95), ACM, pp. 373–382, doi:10.1145/225058.225162.

[12] T. A. Henzinger & J.-F. Raskin (2000): *Robust Undecidability of Timed and Hybrid Systems*. In: Proc. of the 3rd International Workshop Hybrid Systems: Computation and Control (HSCC'00), LNCS 1790, Springer, pp. 145–159, doi:10.1007/3-540-46430-1_15.

[13] G. Lafferriere, G. J. Pappas & S. Sastry (2000): *O-minimal Hybrid Systems*. Mathematics of Control, Signals, and Systems 13, pp. 1–21, doi:10.1007/PL00009858.

[14] G. Lafferriere, G. J. Pappas & S. Yovine (2001): *Symbolic Reachability Computation for Families of Linear Vector Fields*. J. Symb. Comput. 32(3), pp. 231–253, doi:10.1006/jsco.2001.0472.

[15] B. Mendelson (1990): *Introduction to Topology*, III edition. Dover Books on Mathematics.

[16] E. Mendelson (1997): *Introduction to Mathematical Logic*, IV edition. CRC Press.

[17] C. Piazza, M. Antoniotti, V. Mysore, A. Policriti, F. Winkler & B. Mishra (2005): *Algorithmic Algebraic Model Checking I: The Case of Biochemical Systems and their Reachability Analysis*. CIMS-TR 2005-859, Courant Institute Of Mathematical Sciences.

[18] P. Prabhakar, V. Vladimerou, M. Viswanathan & G. E. Dullerud (2009): *Verifying Tolerant Systems Using Polynomial Approximations*. In: Proc. of the 30th IEEE Real-Time Systems Symposium (RTSS'09), IEEE Computer Society Press, pp. 181–190, doi:10.1109/RTSS.2009.28.

[19] S. Ratschan (2010): *Safety Verification of Non-linear Hybrid Systems Is Quasi-Semidecidable*. In: Proc. of the 7th Conference on Theory and Applications of Models of Computation (TAMC'10), LNCS 6108, Springer, pp. 397–408, doi:10.1007/978-3-642-13562-0_36.

[20] T. Sturm & A. Tiwari (2011): *Verification and synthesis using real quantifier elimination*. In: Proc. of the 36th international symposium on Symbolic and algebraic computation (ISSAC'11), ACM, pp. 329–336, doi:10.1145/1993886.1993935.

[21] A. Tarski (1951): *A Decision Method for Elementary Algebra and Geometry*. Univ. California Press.

[22] A. Tiwari & G. Khanna (2002): *Series of Abstractions for Hybrid Automata*. In: Proc. of Hybrid Systems: Computation and Control (HSCC'02), LNCS 2289, Springer, pp. 465–478, doi:10.1007/3-540-45873-5_36.