



UNIVERSITÀ  
DEGLI STUDI  
DI UDINE

## Università degli studi di Udine

ε-Semantics computations on biological systems

*Original*

*Availability:*

This version is available <http://hdl.handle.net/11390/963552> since 2016-11-29T18:03:01Z

*Publisher:*

*Published*

DOI:10.1016/j.ic.2014.01.011

*Terms of use:*

The institutional repository of the University of Udine (<http://air.uniud.it>) is provided by ARIC services. The aim is to enable open access to all the world.

*Publisher copyright*

(Article begins on next page)

# $\epsilon$ -Semantics Computations on Biological Systems<sup>☆</sup>

A. Casagrande<sup>a,\*</sup>, T. Dreossi<sup>b,d</sup>, J. Fabriková<sup>c</sup>, C. Piazza<sup>b,\*</sup>

<sup>a</sup>*Dept. of Mathematics and Geoscience, University of Trieste, via Valerio 12/1 - 34127 TRIESTE, Italy*

<sup>b</sup>*Dept. of Mathematics and Computer Science, University of Udine, via delle Scienze 206 - 33100 UDINE, Italy*

<sup>c</sup>*Faculty of Informatics, Masaryk University, Botanick 68a - 602 00 BRNO, Czech Republic*

<sup>d</sup>*VERIMAG, University Joseph Fourier, 2 avenue de Vignate - 38610 GIERES, France*

---

## Abstract

The assumption of being able to perform infinite precision measurements does not only lead to undecidability, but it also introduces artifacts in the mathematical models that do not correspond to observable behaviours of systems under study. When bounded spatial regions are involved, such issues can be avoided if arbitrarily small sets of points are not definable in the mathematical setting.  $\epsilon$ -semantics were introduced in this spirit. In this paper we investigate the use of  $\epsilon$ -semantics deeper, in the context of reachability analysis of hybrid automata. In particular, we focus on two  $\epsilon$ -semantics and reason about their computability. We then try our approach on biological model analysis to give evidence about the effectiveness of the methodology.

*Keywords:* Hybrid Systems,  $\epsilon$ -Semantics, Reachability problem

---

## 1. Introduction

The growing area of Systems Biology requires the development of techniques and formal models suitable for the description of biological systems.

---

<sup>☆</sup>This work has been partially supported by Istituto Nazionale di Alta Matematica (INdAM).

\*Corresponding authors

*Email addresses:* `acasagrande@units.it` (A. Casagrande),  
`carla.piazza@uniud.it` (C. Piazza)

Often, such class of natural phenomena, can be captured through an abstraction process that involves hybrid systems, i.e., systems consisting of interactions between discrete and continuous components. Hybrid automata are mathematical models particularly suitable to the description of hybrid systems. Therefore, the study and the analysis of biological systems can be reduced to the resolution of reachability problems of hybrid automata. Unfortunately, due to the undecidability of such problem, there are no algorithms able to compute, in a finite amount of time, the reachability set of any hybrid automaton [1].

Several techniques tackling the undecidability of the reachability problem have been proposed in recent years. Many authors working in this field introduce approximation methodologies for the study of hybrid automata. Such approximations can be, for instance, performed by using either numerical calculation [2], symbolic computation [3] or geometrical analysis [4]. The most important factors to be considered are the quality of the approximation with respect to the original reachability set and the relationship between the behaviour of the approximated automaton and that of the modeled system.

*$\epsilon$ -Semantics* is a class of semantics that can avoid the problem of undecidability of the reachability for hybrid automata with bounded invariants. They are not meant to be used as approximations of the standard semantics. On the contrary, they have been introduced to better mimic the behavior of real systems by adopting some natural-inspired constraints. Due to their peculiarity, these semantics are able to capture some indeterminacy which is intrinsic in the real world and, because of that, they appear to be particularly useful in the study of biological systems [5].

However, to make the  $\epsilon$ -semantics framework effective for the analysis of real systems, deeper investigations in two directions are necessary. On the one hand, instances of  $\epsilon$ -semantics capturing interesting behaviours need to be defined. On the other hand, computational techniques and tools have to be introduced on such semantics. This is the main focus of our paper, where we consider sphere semantics and dilated erosion semantics. Sphere semantics amplifies the original behaviour of the system (when this is specified without negations), while dilated erosion removes the behaviour that is not witnessed by a sufficiently large set. Interestingly, we are able to prove that these semantics are computable, introducing a formula translation and exploiting classic decidability results [6]. A natural question at this point would concern the computational complexity of our algorithms. As a matter of fact, in the general case our approach has a double exponential complexity due to

the use of quantifier elimination procedures for semi-algebraic theory. In order to reduce such complexity we introduced simplifications for the type of formulæ we obtain in the reachability analysis. Specifically, we identify some simplification applicable to the translated formulæ to both decrease the number of the quantifier operators and reduce the complexity of the  $\epsilon$ -semantics evaluations.

These optimizations are exploited in the analysis of two biological case studies, a neural oscillator system and a glycemetic control system, demonstrating the fact  $\epsilon$ -semantics represent a valid tool in the field of the system biology. Starting from their canonical representations in form of ODE, we modeled both of them using hybrid automata and we automatically verify properties, such as the convergence to a stable limit cycle and the robustness of reachable states, taking into account, with the help of the  $\epsilon$ -semantics, the non-determinism intrinsically related to the nature of those scenarios.

The paper is organized as follows. Section 2 introduces notation and defines hybrid automata. In Section 3, we present the notion of  $\epsilon$ -semantics and provide a reachability algorithm for hybrid automata based on it that extends the applicability of the classical algorithm to a wider class of hybrid automata. Section 4 describes two examples of  $\epsilon$ -semantics, it shows that these two semantics are definable in the standard theory, and builds the formulæ that define them. As suggested by Section 5, in some specific, but frequent, cases, we can decrease the complexity of these formulæ. In Section 6 we study two real biological cases, a neural oscillator and a glycemetic control system, exploiting all the techniques presented in the previous sections and, finally, Section 7 makes some concluding remarks, comparison with related literature, and suggests future work.

## 2. Hybrid Automata

We first need to introduce some basic notions and conventions. Capital letters  $X$ ,  $X_i$ ,  $Y$ ,  $Y_i$ ,  $W$ , and  $W_i$ , denote variables ranging over the reals, while bold letters  $\mathbf{X}$ ,  $\mathbf{X}_i$ ,  $\mathbf{Y}$ ,  $\mathbf{Y}_i$ ,  $\mathbf{W}$ , and  $\mathbf{W}_i$ , denote tuples of real variables. We assume that every variable occurs either free, or bound by a quantifier in a formula, but never both. This enables us to label variables, rather than occurrences, as free or bound. Sometimes we write  $\varphi[X_1, \dots, X_m]$  to stress the fact that the set of all free variables of  $\varphi$  is  $\{X_1, \dots, X_m\}$ . By extension,  $\varphi[\mathbf{X}_1, \dots, \mathbf{X}_n]$  indicates that the variables of tuples  $\mathbf{X}_1, \dots, \mathbf{X}_n$  are free in  $\varphi$ . We denote the formula obtained from  $\varphi[\mathbf{X}_1, \dots, \mathbf{X}_n]$  by simultaneously re-

placing all the variables  $\mathbf{X}_1, \dots, \mathbf{X}_n$  by  $\mathbf{s}_1, \dots, \mathbf{s}_n$ , where  $\mathbf{s}_i$  is either a constant or a variable, by writing  $\varphi[\mathbf{s}_1, \dots, \mathbf{s}_n]$ .

The notions of first-order formula, models, and theory are defined in the standard way (see [7, 8]). A formula without free variables is called a *sentence*. A *theory*  $\mathcal{T}$  is a set of sentences such that if  $\varphi$  is a logical consequence of  $\mathcal{T}$ , then  $\varphi \in \mathcal{T}$ . A theory  $\mathcal{T}$  admits the *elimination of quantifiers* if, for any formula  $\varphi$ , there exists a quantifier free formula  $\varrho \in \mathcal{T}$  such that  $\varphi$  is equivalent to  $\varrho$  with respect to  $\mathcal{T}$ . A theory  $\mathcal{T}$  is *decidable* if there exists an algorithm for deciding whether a sentence  $\varphi$  belongs to  $\mathcal{T}$  or not.

**Example 1.** Consider the formula  $\varphi \stackrel{\text{def}}{=} \exists X (a * X^2 + b * X + c = 0)$ . It is well known that  $\varphi$  is in the theory of reals with  $+$ ,  $*$ , and  $\geq$  if and only if the unquantified formula  $b^2 - 4ac \geq 0$  holds.

An example of a theory for which our results hold is the first-order theory of  $\langle \mathbb{R}, +, *, =, < \rangle$ , also known as *Tarski's theory* or the theory of *semi-algebraic sets*. Tarski's theory is decidable and admits quantifier elimination.

Given a language  $\mathcal{L}$ , a *semantics* of it is a function  $[\cdot]$  from the set of formulae of  $\mathcal{L}$  to the power set of  $\mathbb{R}^*$  (where  $\mathbb{R}^* = \bigcup_{n \in \mathbb{N}} \mathbb{R}^n$ ) such that  $[\varphi[X_1, \dots, X_n]] \subseteq \mathbb{R}^n$ . The formula  $S[\mathbf{X}]$  *represents* (also *defines*) in  $[\cdot]$  the set  $[S[\mathbf{X}]]$ . If there exists a formula  $S[\mathbf{X}]$  such that  $[S[\mathbf{X}]] = \mathbb{S}$ , then the set  $\mathbb{S}$  is said *definable* in  $[\cdot]$ .

Any theory  $\mathcal{T}$  over a language  $\mathcal{L}$  induces a *standard semantics* defined as  $\{\varphi[X_1, \dots, X_n]\} \stackrel{\text{def}}{=} \{\langle s_1, \dots, s_n \rangle \mid \varphi[p_1, \dots, p_n] \in \mathcal{T}\}$ . Whenever we do not explicitly mention any semantics, we are referring to the standard one.

Let  $\|\cdot\|$  and  $\|\cdot\|$  be two semantics for a first-order language  $\mathcal{L}$  and  $\mathcal{T}$  be a theory over  $\mathcal{L}$ . If  $\|\varphi\| \subseteq \|\varphi\|$  for all  $\varphi \in \mathcal{L}$ ,  $\|\cdot\|$  is said to be an *under-approximation semantics*. Symmetrically, whenever  $\|\varphi\| \subseteq \|\varphi\|$  for all  $\varphi \in \mathcal{L}$ , then  $\|\cdot\|$  is dubbed an *over-approximation semantics*.

We also use several standard notions from topological and metric spaces (see [9]). Given a set  $\mathbb{S} \subseteq \mathbb{R}^n$ ,  $\text{conv}(\mathbb{S})$  denotes the convex hull of  $\mathbb{S}$ . With the symbol  $\delta$  we refer to any metric definable in  $\mathcal{T}$ . Example of such a metric is the *standard euclidean metric* on  $\mathbb{R}^n$  definable in Tarski's theory. With the notation  $B(p, \epsilon)$  we indicate the set of all points at distance smaller than  $\epsilon$  from  $p$ , i.e., the open sphere of radius  $\epsilon$  centered in  $p \in \mathbb{R}^n$ . By extension,  $B(\mathbb{S}, \epsilon)$ , where  $\mathbb{S}$  is a subset of  $\mathbb{R}^n$ , denotes the Minkowski sum of  $B(0, \epsilon)$  and  $\mathbb{S}$ .

### 2.1. Syntax, Semantics, and Reachability

In this section we give a formal definition of hybrid automata for our purposes. There are many different definitions of hybrid automata in the literature. Even if the most common differences between known formalisms reside in the descriptions of continuous and discrete transitions, the semantics attributed to the transitions are almost the same. Here we define hybrid automata through first-order formulæ over the reals.

**Definition 1** (Hybrid Automata - Syntax). *Let  $\mathcal{L}$  be a first-order language. A hybrid automaton  $H$  of dimension  $d(H) \in \mathbb{N}$  over  $\mathcal{L}$  is a tuple  $H = \langle \mathbf{X}, \mathbf{X}', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res \rangle$  where:*

- $\mathbf{X} = \langle X_1, \dots, X_{d(H)} \rangle$  and  $\mathbf{X}' = \langle X'_1, \dots, X'_{d(H)} \rangle$  are two tuples of variables ranging over the reals  $\mathbb{R}$ ;
- $T$  is a variable ranging over  $\mathbb{R}_{\geq 0}$  denoting time;
- $\langle \mathcal{V}, \mathcal{E} \rangle$  is a finite directed graph. Each element of  $\mathcal{V}$  will be dubbed location;
- each location  $v \in \mathcal{V}$  is labeled by the two formulæ  $Dyn(v)[\mathbf{X}, \mathbf{X}', T]$  and  $Inv(v)[\mathbf{X}]$  over  $\mathcal{L}$  such that if  $Inv(v)[p]$  holds then  $Dyn(v)[p, q, 0]$  holds if and only if  $p = q$ ;
- each edge  $e \in \mathcal{E}$  is labeled by the formulæ  $Act(e)[\mathbf{X}]$  and  $Res(e)[\mathbf{X}, \mathbf{X}']$  over  $\mathcal{L}$  which are called activation and reset, respectively.

Intuitively, the formula  $Dyn(v)[\mathbf{X}, \mathbf{X}', T]$  characterizes the dynamics associated to the location  $v$ , while  $Inv(v)[\mathbf{X}]$  denotes the set of the values admitted during the continuous evolution of the automaton inside  $v$ . The formulæ  $Act(e)[\mathbf{X}]$  and  $Res(e)[\mathbf{X}, \mathbf{X}']$  identifies the set of continuous values from which the automaton can jump over the edge  $e$  and a map that should be applied to the continuous values from which the automaton crosses the edge  $e$ . The following section details the formal meaning of these formulæ and describes the semantics of hybrid automata.

Hybrid automaton dynamics are usually described through differential equations (see, e.g., [10, 11]). However, in many cases, solutions or approximated solutions of the differential equations are computed before proceeding with any reasoning on the automata (see, e.g., [11]). Whenever such solutions can be described by polynomial dynamics, we obtain automata which fall under our definition.

Differently from [12], we require that  $Dyn(v) \llbracket p, q, 0 \rrbracket$  implies  $p = q$ . Intuitively, this means that if we are in  $p$  at time 0, we can reach a point different from  $p$  through a continuous dynamic only if we let the time flow. This assumption will allow us to both get continuity of the flow at time 0 and slightly simplify the reachability formulæ with respect to the ones defined in [12].

**Example 2.** Figure 1 depicts a graphical representation of the hybrid automaton  $H_a = \langle \mathbf{X}, \mathbf{X}', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res \rangle$ , where:

- $\mathbf{X} = \langle X_1, X_2 \rangle$
- $\mathcal{V} = \{v_1, v_2\}$  and  $\mathcal{E} = \{e_1, e_2\}$ , where  $e_1 = \langle v_1, v_2 \rangle$  and  $e_2 = \langle v_2, v_1 \rangle$
- $Dyn(v_1)[\mathbf{X}, \mathbf{X}', T] \stackrel{def}{=} X'_1 = X_1 + T \wedge X'_2 = X_2 + T^2$  and  $Dyn(v_2)[\mathbf{X}, \mathbf{X}', T] \stackrel{def}{=} X'_1 = X_1 + T \wedge X'_2 = X_2 + T$
- $Inv(v_1)[\mathbf{X}] \stackrel{def}{=} X_1 \leq 10$  and  $Inv(v_2)[\mathbf{X}] \stackrel{def}{=} X_1 \geq 10$
- $Res(e_1)[\mathbf{X}, \mathbf{X}'] \stackrel{def}{=} Res(e_2)[\mathbf{X}, \mathbf{X}'] \stackrel{def}{=} X'_1 = X_1 \wedge X'_2 = X_2$
- $Act(e_1)[\mathbf{X}] \stackrel{def}{=} Act(e_2)[\mathbf{X}] \stackrel{def}{=} X_1 = 10$

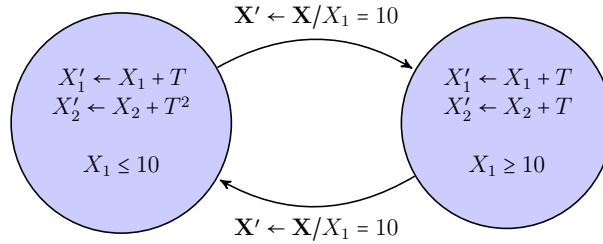


Figure 1: The hybrid automaton  $H_a$ .

Since the automaton  $H_a$  is piecewise defined, we may also represent it as in Figure 2.

## 2.2. Hybrid Automaton Semantics

Intuitively, the formula  $\text{Dyn}(v)[\mathbf{X}, \mathbf{X}', T]$  holds if there exists a continuous flow going from  $\mathbf{X}$  to  $\mathbf{X}'$  in time  $T$ . Our semantics admits an infinite number of continuous flows which can also be self-intersecting.

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

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

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 write  $\ell \rightarrow_C \ell'$  and  $\ell \rightarrow_D \ell'$  to mean that there exists a  $t \in \mathbb{R}_{\geq 0}$  such that  $\ell \xrightarrow{t}_C \ell'$  and that there exists an  $e \in \mathcal{E}$  such that  $\ell \xrightarrow{e}_D \ell'$ , respectively. Moreover, we write  $\ell \rightarrow \ell'$  to denote either  $\ell \rightarrow_C \ell'$  or  $\ell \rightarrow_D \ell'$ .

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

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

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

Given a set of starting points  $\mathbb{I}$  we are interested in problem of finding all the ending points of traces that begin in  $\mathbb{I}$ , i.e., the set of points reachable from  $\mathbb{I}$ .



**Definition 4** (Hybrid Automata - Reachability). 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  $r \in \mathbb{F}$ .

Let  $RSet_H^i(\mathbb{I}) \subseteq \mathbb{R}^{d(H)}$  denote the set of continuous values reachable by  $H$  from a set of initial values  $\mathbb{I} \subseteq \mathbb{R}^{d(H)}$  via traces with exactly  $i$  discrete jumps. Further let  $RSet_H(\mathbb{I}) \stackrel{\text{def}}{=} \bigcup_{i \in \mathbb{N}} RSet_H^i(\mathbb{I})$ .

Notice that we impose that two continuous transitions do not occur consecutively in a trace. In all those hybrid automata whose flows are solutions of autonomous differential equations, the continuous transition relation is transitive, which means that different consecutive continuous transitions can be reduced to a single continuous one. Definition 1 allows also automata whose continuous transition relation is not transitive.

For instance, let us consider the ODE  $\langle \dot{X}_1, \dot{X}_2 \rangle = \langle 1, 2 * T \rangle$ . It corresponds to the formula-based dynamics  $X'_1 = X_1 + T \wedge X'_2 = X_2 + T^2$  and the set of points reachable from  $\langle 0, 0 \rangle$  according to it should be  $R = \{ \langle t, t^2 \rangle | t \in \mathbb{R}_{\geq 0} \}$  (see Figure 2). However, if we allow more than one consecutive continuous transitions, the point  $\langle 2, 1 \rangle$ , which is not meant to in  $R$  by the ODE, will be reachable from  $\langle 0, 0 \rangle$  for example via four continuous evolutions for four time intervals of length 0.5 from  $\langle 0, 0 \rangle$  to  $\langle 0.5, 0.25 \rangle, \langle 1, 0.5 \rangle, \langle 1.5, 0.75 \rangle$ , and finally to  $\langle 2, 1 \rangle$ . In fact, every point from positive quadrant that is under the parabola  $R$  and above the  $X_1$  axis is reachable by a finite number of subsequent continuous transitions, which is not the expected behaviour of the ODE system.

In general, the reachability problem of hybrid automata is undecidable [1]. Intuitively, even if one is able to compute a single transition step, he still has to find a way to perform an unbounded number of subsequent steps.

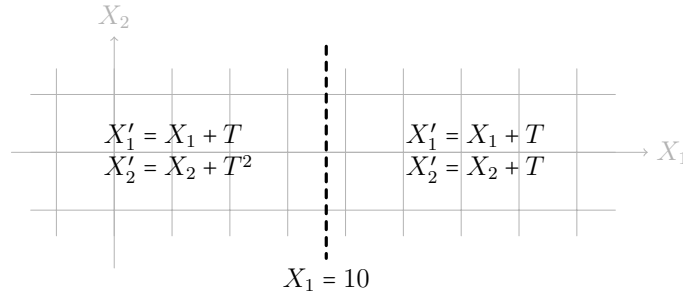


Figure 2: Another graphical representation of the hybrid automaton  $H_a$ .

As for the computation of a single transition, the definition of  $\rightarrow_C$  requires the existence of a continuous function  $f$  which satisfies both formulae  $Inv$  and  $Dyn$ . If we consider only functional automata, i.e., automata whose dynamics have the form  $Dyn(v)[\mathbf{X}, \mathbf{X}', T] \stackrel{def}{=} \mathbf{X}' = f_v(\mathbf{X}, T)$ , such existence can be expressed by any suitable first-order language in which  $f_v$  is expressible. However, there exist non functional automata for which this is not the case. Hybrid automata in Michael's form [12] generalize functional automata still admitting a reduction of the continuous reachability problem over them to a satisfiability problem. On the one hand, they allow to express dynamics involving unknown parameters, which may be useful in many practical applications (e.g., systems biology). On the other hand, they enable us to both over-approximate and under-approximate the reachable set by exploiting the techniques presented in [13] and [5]. For this class of hybrid automata, the set  $RSet_H^i(\mathbb{I})$  is definable with a first-order formula. Still, this does not imply the decidability of reachability, since we would have to check the satisfiability of an infinite set of first-order formulae.

### 3. $\epsilon$ -Semantics

The ability of characterizing dense regions of arbitrarily small size, is the main cause of the undecidability of the reachability problem for hybrid automata. As noticed in [5], such ability may be misleading in some cases. The continuous quantities used in hybrid automata are very often abstractions of large, but discrete, quantities. For instance, in the study of biological systems, the ability of handling values with infinite precision is a model artifact rather than a real property of the original system.

**Theorem 1** ([5]). *Let  $\mathcal{T}$  be a decidable first-order theory over reals and  $H$  be a  $\mathcal{T}$ -hybrid automaton with bounded invariants. If there exists  $\epsilon \in \mathbb{R}_{>0}$  such that, for each  $\mathbb{I} \subseteq \mathbb{R}^{d(H)}$  and for each  $i \in \mathbb{N}$ , the fact  $RSet_H^{i+1}(\mathbb{I}) \neq RSet_H^i(\mathbb{I})$  implies there exists  $a_i \in \mathbb{R}^{d(H)}$  such that  $B(a_i, \epsilon) \subseteq RSet_H^{i+1}(\mathbb{I}) \setminus RSet_H^i(\mathbb{I})$ , then there exists  $j \in \mathbb{N}$  such that  $RSet_H(\mathbb{I}) = RSet_H^j(\mathbb{I})$  and the reachability problem over  $H$  is decidable.*

Since our hybrid automata characterization is based on first-order formulae, it is reasonable to reinterpret the semantics of our automata by giving each formula a “dimension of at least  $\epsilon$ ”;  $\epsilon$ -semantics is a class of semantics which guarantee the decidability of reachability for hybrid automata with bounded invariants when the underline theory  $\mathcal{T}$  is decidable [5].

**Definition 5.** Let  $\mathcal{L}$  be a first-order language,  $\mathcal{T}$  a theory over it, and  $\epsilon \in \mathbb{R}_{>0}$ . For each  $\psi \in \mathcal{L}$  with  $d$  free variables, let  $\llbracket \psi \rrbracket_\epsilon$  be a subset of  $\mathbb{R}^d$  such that:

$$\begin{aligned} (\epsilon) & \text{ either } \llbracket \psi \rrbracket_\epsilon = \emptyset \text{ or there exists } p \in \mathbb{R}^d \text{ such that } B(p, \epsilon) \subseteq \llbracket \psi \rrbracket_\epsilon \\ (\cap) & \llbracket \phi \wedge \varphi \rrbracket_\epsilon \subseteq \llbracket \phi \rrbracket_\epsilon \cap \llbracket \varphi \rrbracket_\epsilon & (\cup) & \llbracket \phi \vee \varphi \rrbracket_\epsilon = \llbracket \phi \rrbracket_\epsilon \cup \llbracket \varphi \rrbracket_\epsilon \\ (\forall) & \llbracket \forall X \psi[X, \mathbf{X}] \rrbracket_\epsilon = \llbracket \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon & (\exists) & \llbracket \exists X \psi[X, \mathbf{X}] \rrbracket_\epsilon = \llbracket \bigvee_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon \\ (\neg) & \llbracket \psi \rrbracket_\epsilon \cap \llbracket \neg \psi \rrbracket_\epsilon = \emptyset \end{aligned}$$

A semantics satisfying the above conditions is called an  $\epsilon$ -semantics for  $\mathcal{T}$ .

Notice that in the above definition we require the theory  $\mathcal{T}$  just to give a meaning to the set  $B(p, \epsilon)$ .

If the standard semantics is not already an  $\epsilon$ -semantics for  $\mathcal{T}$ , then there is no  $\epsilon$ -semantics over-approximating  $\llbracket \cdot \rrbracket$ , i.e., there is no  $\llbracket \cdot \rrbracket_\epsilon$  such that  $\llbracket \psi \rrbracket_\epsilon \supseteq \llbracket \psi \rrbracket$  for all formulæ  $\psi$ . In fact, for every  $\epsilon$ -semantics different from the standard semantics there exists at least one formula  $\phi$  with different standard and  $\epsilon$ -semantics. By the rule  $(\neg)$ ,  $\llbracket \phi \rrbracket_\epsilon \cap \llbracket \neg \phi \rrbracket_\epsilon = \emptyset$ . Hence, if  $\llbracket \phi \rrbracket_\epsilon \supset \llbracket \phi \rrbracket$ , then  $\llbracket \neg \phi \rrbracket_\epsilon \subset \llbracket \neg \phi \rrbracket$ . While if  $\llbracket \phi \rrbracket_\epsilon \subset \llbracket \phi \rrbracket$  and, at the same time,  $\llbracket \phi \rrbracket_\epsilon \neq \llbracket \phi \rrbracket$ , then  $\llbracket \phi \rrbracket \subseteq \llbracket \phi \rrbracket_\epsilon$ . In both cases standard semantics of either  $\neg \phi$ , or  $\phi$  is not over-approximated by its  $\epsilon$ -semantics.

It is well known that, in the standard semantics, the reachability problem over hybrid automata with bounded invariants is not decidable. This is not the case if we use  $\epsilon$ -semantics over a decidable theory in place of the standard one. In particular, [5] introduced an algorithm for evaluating the reachable set of functional automata with transitive dynamics using any computable  $\epsilon$ -semantics. The constraints imposed in [5] on the dynamics were not related to the applicability of the suggested strategy to more general automata, but they were due to the focus of interest of the original article. Indeed, Algorithm 1 supports any hybrid automata in Michael's form, the transitivity condition is not needed.

The main reachability procedure (Algorithm 1) is a variant of breadth first search. Part of its input (apart from the specific  $\epsilon$ -semantics and hybrid automaton) is a collection of first-order formulæ  $I(v)[\mathbf{X}]$  for all locations  $v \in \mathcal{V}$  of the hybrid automaton characterizing sets of initial points in the respective locations. Output of the reachability procedure is again a collection of first-order formulæ  $R(v)[\mathbf{X}]$  representing in each location the set of all points that are reachable from the initial points.

During the computation, the main reachability procedure maintains the set of active locations  $\mathcal{A} \subseteq \mathcal{V}$  and two collections of formulæ  $R(v)[\mathbf{X}]$  and

$N(v)[\mathbf{X}]$ . The  $R$  formulæ represent (location-wise) the set of points that have been reached up to this point of the computation and  $N$  formulæ represents points that are reachable from the already reached points with both a discrete and a successive continuous transitions. The main reachability procedure initializes  $R$  and  $N$  formulæ, poses the current set of active locations to all locations  $\mathcal{V}$ , and, while the set of active locations is nonempty, it updates both  $R$ ,  $N$ , and  $\mathcal{A}$ . In particular, each  $R$  formula is set to the disjunct between itself and the corresponding  $N$  formula meaning that it should now represent what was reachable before the last iteration of the algorithm plus the newly reached points.

There are two auxiliary procedures: *InitRN* and *UpdateActiveAndN*. *InitRN* (Algorithm 2) is called exactly once at the beginning of reachability computation. It initializes all  $N$  formulæ to false and  $R$ s to those formulæ that represent the sets of points that can be reached from initial points by one continuous transition (see line 6 of Algorithm 1).

*UpdateActiveAndN* (Algorithm 3) takes the hybrid automaton, the current  $R$  formulæ, the  $\epsilon$ -semantics and the set  $\mathcal{B} \subseteq \mathcal{V}$  of currently active locations as parameters. It returns the updated set of active locations together with the new  $N$  formulæ. Initially it sets  $\mathcal{A}$  to empty set and  $N$  formulæ to false. Then it considers all the edges  $\langle v, v' \rangle$ , with  $v \in \mathcal{B}$ , and adds those formulæ that evaluate to the set of all points in location  $v'$  reachable by a discrete transition through  $\langle v, v' \rangle$  from  $R$  and a successive continuous transition.

The formula  $N(v')[\mathbf{X}] \wedge \neg R(v')[\mathbf{X}]$  denotes the set of points reached for the first time during the last iteration of the algorithm. Each location  $v'$  for which the  $\epsilon$ -semantics evaluation of the formula is nonempty, i.e., contains at least an open sphere of radius  $\epsilon$ , is added to the set of new active locations  $\mathcal{A}$ .

The **while** loop at line 4 of Algorithm 1 is repeated until the set of active locations is exhausted. Since all the sets  $\{\text{Inv}(v)\}_\epsilon$  are bounded by hypothesis and either  $\{\phi\}_\epsilon = \emptyset$  or  $\{\phi\}_\epsilon \supseteq B(p, \epsilon)$  by the definition of  $\epsilon$ -semantics, we conclude from Theorem 1 that, sooner or later, such a condition will be reached and Algorithm 1 eventually terminates. Its correctness easily follows from the same arguments that were used for the original algorithm in [5].

It is important to notice that at each iteration of the main loop only formula for each edge from an active location is evaluated (see line 9 of Algorithm 3) all the other commands are symbolic manipulations.

---

**Algorithm 1:** Reachability( $H, I(\cdot)[\mathbf{X}], \{\cdot\}_\epsilon$ )

---

**Data:**  $\{\cdot\}_\epsilon$  is a  $\epsilon$ -semantics,  $I(v)[\mathbf{X}]$  is a first-order formula for all  $v \in \mathcal{V}$ , and  $H$  is a hybrid automaton  
 $\langle \mathbf{X}, \mathbf{X}', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res \rangle$  such that  $\{Inv(v)\}_\epsilon$  is bounded for all  $v \in \mathcal{V}$

**Result:**  $R(\cdot)[\mathbf{X}]$  such that  $R(v)[p]$  holds iff there exists a  $v'$  such that  $\langle v, p \rangle$  is reachable in  $H$  from  $\{I(v')[\mathbf{X}]\}$

```

1  $\langle R(\cdot), N(\cdot) \rangle \leftarrow InitRN(H, I(\cdot))$ 
2  $\text{/* initially all the locations are active */}$ 
3  $\mathcal{A} \leftarrow \mathcal{V}$ 
4 while  $\mathcal{A} \neq \emptyset$  do  $\text{/* while there are active locations */}$ 
5   for  $v \in \mathcal{A}$  do  $\text{/* for all active locations */}$ 
6      $R(v)[\mathbf{X}] \leftarrow R(v)[\mathbf{X}] \vee N(v)[\mathbf{X}]$   $\text{/* update reached sets */}$ 
7   end
8    $\text{/* update newly reached sets and active locations */}$ 
9    $\langle \mathcal{A}, N(\cdot) \rangle \leftarrow UpdateActiveAndN(H, R(\cdot)[\mathbf{X}], \mathcal{A}, \{\cdot\}_\epsilon)$ 
10 end
11 return  $R(\cdot)[\mathbf{X}]$ 
```

---



---

**Algorithm 2:** InitRN( $H, I(\cdot)[\mathbf{X}]$ )

---

**Data:**  $H$  is a hybrid automaton  $\langle \mathbf{X}, \mathbf{X}', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res \rangle$   
and  $I(v)[\mathbf{X}]$  is a first-order formula for all  $v \in \mathcal{V}$

**Require:**  $cReach(v)[p, q]$  holds iff  $\langle v, p \rangle \rightarrow_C \langle v, q \rangle$  in  $H$

**Result:** The tuple  $\langle R(\cdot), N(\cdot) \rangle$  such that, for all  $v \in \mathcal{V}$ ,  $N(v) = \perp$  and if there exist a  $r \in \{I(v)\}$  such that  $\langle v, r \rangle \rightarrow_C \langle v, s \rangle$  in  $H$ , then  $s \in \{R(v)\}$

```

1 for  $v \in \mathcal{V}$  do
2    $R(v)[\mathbf{X}] \leftarrow \exists \mathbf{X}' (cReach(v)[\mathbf{X}', \mathbf{X}] \wedge I(v)[\mathbf{X}'])$ 
3    $N(v)[\mathbf{X}] \leftarrow \perp$ 
4 end
5 return  $\langle R(\cdot), N(\cdot) \rangle$ 
```

---

---

**Algorithm 3:** UpdateActiveAndN( $H, R(\cdot)[\mathbf{X}], \mathcal{B}, \{\cdot\}_\epsilon$ )

---

**Data:**  $H$  is a hybrid automaton  $\langle \mathbf{X}, \mathbf{X}', T, \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Res \rangle$ ,  
 $R(v)[\mathbf{X}]$  is a first-order formula for all  $v \in \mathcal{V}$ ,  $\mathcal{B}$  is a subset of  $\mathcal{V}$ ,  
and  $\{\cdot\}_\epsilon$  is a  $\epsilon$ -semantics

**Require:**  $dcReach(e)[p, q]$  holds iff  $e = \langle v, v' \rangle$  and there exists a  $s \in \mathbb{R}^*$   
such that  $\langle v, p \rangle \xrightarrow{e}_D \langle v', s \rangle \rightarrow_C \langle v', q \rangle$  in  $H$

**Result:**  $\langle \mathcal{A}, N(\cdot) \rangle$  such that  $v \in \mathcal{A}$  iff  $\{N(v)[\mathbf{X}] \wedge \neg R(v)[\mathbf{X}]\}_\epsilon \neq \emptyset$   
and, for all  $v \in \mathcal{V}$ ,  $R(v')[p]$  holds and  $N(v)[q]$  holds iff  
 $\langle v', p \rangle \xrightarrow{e}_D \langle v', s \rangle \rightarrow_C \langle v', q \rangle$  for some  $v' \in \mathcal{B}$

```

1 for  $v \in \mathcal{V}$  do
2    $N(v)[\mathbf{X}] \leftarrow \perp$            /* reset newly reached sets */
3 end
4  $\mathcal{A} \leftarrow \emptyset$            /* initially no location is active */
5 for  $\langle v, v' \rangle \in \mathcal{E}$  such that  $v \in \mathcal{B}$  do           /* for all edges leaving a
   location in  $\mathcal{B}$  */
6   /* update newly reached sets and add what is reachable
   through a jump over  $\langle v, v' \rangle$  and a flow on  $v'$  */
7    $N(v')[\mathbf{X}] \leftarrow N(v')[\mathbf{X}] \vee \exists \mathbf{X}' (dcReach(\langle v, v' \rangle)[\mathbf{X}', \mathbf{X}] \wedge R[\mathbf{X}'])$ 
8   /* if a new set has been reached in  $v'$  w.r.t.  $\{\cdot\}_\epsilon$  */
9   if  $\{N(v')[\mathbf{X}] \wedge \neg R(v')[\mathbf{X}]\}_\epsilon \neq \emptyset$  then
10     $\mathcal{A} \leftarrow \mathcal{A} \cup \{v'\}$  /* add  $v'$  to the active locations */
11  end
12 end
13 return  $\langle \mathcal{A}, N(\cdot) \rangle$ 

```

---

#### 4. Two Relevant $\epsilon$ -Semantics

This section presents two computable instances of  $\epsilon$ -semantics: the *sphere semantics* and the *dilated erosion semantics*.

In sphere semantics all atomic formulæ get expanded of an open sphere of radius  $\epsilon$ . In the case of conjunction, only the open spheres that are contained in both conjuncts are considered. This ensures that if the semantics of a conjunction is not empty, it includes at least a sphere of radius  $\epsilon$ . A similar policy is used for negation.

**Definition 6** (Sphere semantics [5]). *Let  $\mathcal{T}$  be a first-order theory over the reals and let  $\epsilon > 0$ . The sphere semantics of  $\psi$  over  $\mathcal{T}$  is the set  $\langle \psi \rangle_\epsilon$  defined by structural induction on  $\psi$  as follows:*

- $\langle t_1 \circ t_2 \rangle_\epsilon \stackrel{\text{def}}{=} B(\langle t_1 \circ t_2 \rangle, \epsilon)$ , for  $\circ \in \{=, <\}$
- $\langle \psi_1 \wedge \psi_2 \rangle_\epsilon \stackrel{\text{def}}{=} \bigcup_{B(p, \epsilon) \subseteq \langle \psi_1 \rangle_\epsilon \cap \langle \psi_2 \rangle_\epsilon} B(p, \epsilon)$
- $\langle \psi_1 \vee \psi_2 \rangle_\epsilon \stackrel{\text{def}}{=} \langle \psi_1 \rangle_\epsilon \cup \langle \psi_2 \rangle_\epsilon$
- $\langle \forall X \psi[X, \mathbf{X}] \rangle_\epsilon \stackrel{\text{def}}{=} \langle \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon$
- $\langle \exists X \psi[X, \mathbf{X}] \rangle_\epsilon \stackrel{\text{def}}{=} \langle \bigvee_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon$
- $\langle \neg \psi \rangle_\epsilon \stackrel{\text{def}}{=} \bigcup_{B(p, \epsilon) \cap \langle \psi \rangle_\epsilon = \emptyset} B(p, \epsilon)$

Sphere semantics has been proved to be an  $\epsilon$ -semantics in [5]. This semantics is neither an over-approximation nor an under-approximation of the standard semantics as shown by the following example.

**Example 3.** *Let us consider the formula  $X < 3$ . Its standard semantics is  $\langle X < 3 \rangle = \{p \in \mathbb{R} \mid p < 3\}$  and its sphere semantics is  $\langle X < 3 \rangle_\epsilon = B(\langle X < 3 \rangle, \epsilon) = \{p \in \mathbb{R} \mid p < 3 + \epsilon\}$ . Hence,  $\langle X < 3 \rangle \subset \langle X < 3 \rangle_\epsilon$ . This implies that sphere semantics is not an under-approximation semantics.*

*On the other hand, if we consider the formula  $\neg(X < 3)$ , we have that its standard semantics is  $\langle \neg(X < 3) \rangle = \{p \in \mathbb{R} \mid p \geq 3\}$ , while its sphere semantics is  $\langle \neg(X < 3) \rangle_\epsilon = \bigcup_{B(p, \epsilon) \cap \langle X < 3 \rangle = \emptyset} B(p, \epsilon) = \langle X - \epsilon > 3 \rangle$ . So,  $\langle \neg(X < 3) \rangle \supset \langle \neg(X < 3) \rangle_\epsilon$  and sphere semantics is not an over-approximation semantics.*

However, since sphere semantics over-approximate atoms, it can be used to verify safety conditions.

Erosion semantics under-approximates the standard one by considering only the centers of spheres of radius  $\epsilon$  that are completely included in the standard semantics. Dilated erosion semantics expands erosion semantics of a sphere of radius  $\epsilon$ .

**Definition 7** (Erosion and DE Semantics). *Let  $\mathcal{T}$  be a first-order theory over the reals and let  $\epsilon > 0$ . The erosion semantics of  $\psi$  over  $\mathcal{T}$  is the set  $\rangle\psi\langle_\epsilon$  defined by structural induction on  $\psi$  as follows:*

- $\rangle t_1 \circ t_2 \langle_\epsilon \stackrel{def}{=} \bigcup_{B(p,\epsilon) \subseteq \{t_1 \circ t_2\}} \{p\}$
- $\rangle \psi_1 \wedge \psi_2 \langle_\epsilon \stackrel{def}{=} \rangle \psi_1 \langle_\epsilon \cap \rangle \psi_2 \langle_\epsilon$       •  $\rangle \psi_1 \vee \psi_2 \langle_\epsilon \stackrel{def}{=} \rangle \psi_1 \langle_\epsilon \cup \rangle \psi_2 \langle_\epsilon$
- $\rangle \forall X \psi[X, \mathbf{X}] \langle_\epsilon \stackrel{def}{=} \bigcap_{r \in \mathbb{R}} \rangle \psi[r, \mathbf{X}] \langle_\epsilon$       •  $\rangle \exists X \psi[X, \mathbf{X}] \langle_\epsilon \stackrel{def}{=} \bigcup_{r \in \mathbb{R}} \rangle \psi[r, \mathbf{X}] \langle_\epsilon$
- $\rangle \neg \psi \langle_\epsilon \stackrel{def}{=} \bigcup_{B(p,\epsilon) \cap \{\psi\} = \emptyset} \{p\}$

The dilated erosion semantics, or simply, DE semantics, of  $\psi$  over  $\mathcal{T}$  is the set

$$\gg \psi \ll_\epsilon \stackrel{def}{=} \bigcup_{p \in \rangle \psi \langle_\epsilon} B(p, \epsilon).$$

Let us notice that, since  $B(p, \epsilon)$  is an open sphere, the DE semantics of  $\psi$  is open regardless of whether  $\rangle \psi \langle_\epsilon$  is open too or not.

**Example 4.** *Let us consider again the formula  $X < 3$ . Its erosion semantics is  $\rangle X < 3 \langle_\epsilon = \bigcup_{B(p,\epsilon) \subseteq \{X < 3\}} \{p\} = \{p \in \mathbb{R} \mid p \leq 3 - \epsilon\}$ . Thus, its DE semantics is  $\gg X < 3 \ll_\epsilon = \bigcup_{p \in \rangle X < 3 \langle_\epsilon} B(p, \epsilon) = \{p \in \mathbb{R} \mid p < 3\}$ .*

*On the other hand, if we consider the formula  $\neg(X < 3)$ , we have that Its erosion semantics is  $\rangle \neg(X < 3) \langle_\epsilon = \bigcup_{B(p,\epsilon) \cap \{X < 3\} = \emptyset} \{p\} = \{p \in \mathbb{R} \mid p \geq 3 + \epsilon\}$  and its DE semantics is  $\gg \neg(X < 3) \ll_\epsilon = \bigcup_{p \in \rangle \neg(X < 3) \langle_\epsilon} B(p, \epsilon) = \{p \in \mathbb{R} \mid p > 3\}$ .*

As  $\rangle \delta(X, 0) < \epsilon \langle_\epsilon$  does not contain a sphere of radius  $\epsilon$ , but it is not empty, the erosion semantics is not an  $\epsilon$ -semantics. However, the DE semantics is an  $\epsilon$ -semantics and it under-approximates the standard semantics.

**Lemma 1.** *For any first-order formula  $\psi$  and  $\epsilon \in \mathbb{R}_{>0}$ ,  $\gg \psi \ll_\epsilon \subseteq \{\psi\}$ . Moreover, the DE semantics  $\gg \cdot \ll_\epsilon$  is an  $\epsilon$ -semantics.*

*Proof.* First, we demonstrate that the DE semantics is an under-approximated semantics, i.e., for any first-order formula  $\psi$  and  $\epsilon \in \mathbb{R}_{>0}$ ,  $\gg \psi \ll_\epsilon \subseteq \{\psi\}$ . The proof is given by structural induction on  $\psi$  itself.

$$\begin{aligned} t_1 \circ t_2, \text{ for } \circ \in \{=, <\}. \text{ By definition of DE semantics, } \gg t_1 \circ t_2 \ll_\epsilon &= B(\rangle t_1 \circ t_2 \langle_\epsilon, \epsilon) \\ &= B\left(\bigcup_{B(p,\epsilon) \subseteq \{t_1 \circ t_2\}} \{p\}, \epsilon\right) = \bigcup_{B(p,\epsilon) \subseteq \{t_1 \circ t_2\}} B(p, \epsilon) \subseteq \{t_1 \circ t_2\}. \end{aligned}$$

$$\begin{aligned} \psi_1 \wedge \psi_2. \gg \psi_1 \wedge \psi_2 \ll_\epsilon &= B(\rangle \psi_1 \wedge \psi_2 \langle_\epsilon, \epsilon) = B(\rangle \psi_1 \langle_\epsilon \cap \rangle \psi_2 \langle_\epsilon, \epsilon) \subseteq B(\rangle \psi_1 \langle_\epsilon, \epsilon) \cap \\ &B(\rangle \psi_2 \langle_\epsilon, \epsilon) = \gg \psi_1 \ll_\epsilon \cap \gg \psi_2 \ll_\epsilon. \text{ By inductive hypothesis, } \gg \psi_1 \ll_\epsilon \subseteq \{\psi_1\} \text{ and } \\ \gg \psi_2 \ll_\epsilon &\subseteq \{\psi_2\}, \text{ hence } \gg \psi_1 \ll_\epsilon \cap \gg \psi_2 \ll_\epsilon \subseteq \{\psi_1\} \cap \{\psi_2\} = \{\psi_1 \wedge \psi_2\}. \end{aligned}$$



$\psi_1 \vee \psi_2$ . By definition,  $\llbracket \psi_1 \vee \psi_2 \rrbracket_\epsilon = B(\langle \psi_1 \vee \psi_2 \rangle_\epsilon, \epsilon) = B(\langle \psi_1 \rangle_\epsilon \cup \langle \psi_2 \rangle_\epsilon, \epsilon) = B(\langle \psi_1 \rangle_\epsilon, \epsilon) \cup B(\langle \psi_2 \rangle_\epsilon, \epsilon) = \llbracket \psi_1 \rrbracket_\epsilon \cup \llbracket \psi_2 \rrbracket_\epsilon$ . Now, by inductive hypothesis we know that  $\llbracket \psi_1 \rrbracket_\epsilon \subseteq \llbracket \psi_1 \rrbracket$  and  $\llbracket \psi_2 \rrbracket_\epsilon \subseteq \llbracket \psi_2 \rrbracket$ , thus  $\llbracket \psi_1 \rrbracket_\epsilon \cup \llbracket \psi_2 \rrbracket_\epsilon \subseteq \llbracket \psi_1 \rrbracket \cup \llbracket \psi_2 \rrbracket = \llbracket \psi_1 \vee \psi_2 \rrbracket$ .

$\forall X \psi[X, \mathbf{X}]$ . By the definition of DE semantics and inductive hypothesis,  $\llbracket \forall X \psi[X, \mathbf{X}] \rrbracket_\epsilon = B(\langle \forall X \psi[X, \mathbf{X}] \rangle_\epsilon, \epsilon) = B(\langle \bigcap_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon) = B(\langle \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon) = \llbracket \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon$ . Applying the inductive step demonstrated in the conjunction case, we can state that  $\llbracket \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon \subseteq \llbracket \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket$  which in terms of the standard semantics corresponds to the formula  $\llbracket \forall X \psi[X, \mathbf{X}] \rrbracket$ .

$\exists X \psi[X, \mathbf{X}]$ . By the definition of DE semantics and inductive hypothesis,  $\llbracket \exists X \psi[X, \mathbf{X}] \rrbracket_\epsilon = B(\langle \exists X \psi[X, \mathbf{X}] \rangle_\epsilon, \epsilon) = B(\langle \bigcup_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon)$ , which is equal to  $B(\langle \bigvee_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon) = \llbracket \bigvee_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon \subseteq \llbracket \bigvee_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket$ , that, by the standard semantics, corresponds to  $\llbracket \exists X \psi[X, \mathbf{X}] \rrbracket$ .

$\neg \psi$ .  $\llbracket \neg \psi \rrbracket_\epsilon = B(\langle \neg \psi \rangle_\epsilon, \epsilon) = B(\langle \bigcup_{B(p, \epsilon) \cap \llbracket \psi \rrbracket = \emptyset} \{p\} \rangle_\epsilon, \epsilon) = \bigcup_{B(p, \epsilon) \cap \llbracket \psi \rrbracket = \emptyset} B(p, \epsilon) \subseteq \llbracket \neg \psi \rrbracket$ .

Let us now demonstrate that the DE semantics is effectively an  $\epsilon$ -semantics, i.e., that it satisfies all the requirements of Definition 5.

Requirement ( $\epsilon$ ) is trivially satisfied since any DE semantics evaluation is performed applying an  $\epsilon$ -expansion. This means that a formula is either empty or large at least as an  $\epsilon$ -sphere. Let  $\psi = \psi_1 \wedge \psi_2$  be a conjunction. By definition,  $\llbracket \psi_1 \wedge \psi_2 \rrbracket_\epsilon = B(\langle \psi_1 \wedge \psi_2 \rangle_\epsilon, \epsilon) = B(\langle \psi_1 \rangle_\epsilon \cap \langle \psi_2 \rangle_\epsilon, \epsilon) \subseteq B(\langle \psi_1 \rangle_\epsilon, \epsilon) \cap B(\langle \psi_2 \rangle_\epsilon, \epsilon) = \llbracket \psi_1 \rrbracket_\epsilon \cap \llbracket \psi_2 \rrbracket_\epsilon$ . Thus, requirement ( $\cap$ ) is satisfied. Similarly, if  $\psi = \psi_1 \vee \psi_2$  is a disjunction, then  $\llbracket \psi_1 \vee \psi_2 \rrbracket_\epsilon = B(\langle \psi_1 \vee \psi_2 \rangle_\epsilon, \epsilon) = B(\langle \psi_1 \rangle_\epsilon \cup \langle \psi_2 \rangle_\epsilon, \epsilon) = B(\langle \psi_1 \rangle_\epsilon, \epsilon) \cup B(\langle \psi_2 \rangle_\epsilon, \epsilon) = \llbracket \psi_1 \rrbracket_\epsilon \cup \llbracket \psi_2 \rrbracket_\epsilon$ , which means that also the requirement ( $\cup$ ) is satisfied. Let  $\psi = \forall X \psi[X, \mathbf{X}]$  be a quantified formula. Thus,  $\llbracket \forall X \psi[X, \mathbf{X}] \rrbracket_\epsilon = B(\langle \forall X \psi[X, \mathbf{X}] \rangle_\epsilon, \epsilon) = B(\langle \bigcap_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon) = B(\langle \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rangle_\epsilon, \epsilon) = \llbracket \bigwedge_{r \in \mathbb{R}} \psi[r, \mathbf{X}] \rrbracket_\epsilon$ . The case of formulae closed by the existential quantifier operator is symmetrical to the universal one, where the unions and disjunctions play the roles of intersections and conjunctions, respectively. Hence, also requirements ( $\forall$ ) and ( $\exists$ ) are satisfied. Finally, since the DE semantics is an under-approximation semantics, we know that  $\llbracket \psi \rrbracket_\epsilon \subseteq \llbracket \psi \rrbracket$  and  $\llbracket \neg \psi \rrbracket_\epsilon \subseteq \llbracket \neg \psi \rrbracket$ . Moreover, by the standard semantics, since it holds that  $\llbracket \psi \rrbracket \cap \llbracket \neg \psi \rrbracket = \emptyset$ , then  $\llbracket \psi \rrbracket_\epsilon \cap \llbracket \neg \psi \rrbracket_\epsilon = \emptyset$  must hold too. Hence, requirement ( $\neg$ ) is always satisfied.  $\square$

The above lemma suggests the use of DE semantics for the evaluation of liveness properties.

At this point, we need to prove that both sphere and DE semantics are computable. To this aim, we introduce mappings from formulæ to formulæ that allow us evaluate sphere and DE semantics exploiting standard semantics. In particular, for any first-order theory  $\mathcal{T}$  such that  $B(p, \epsilon)$  is  $\mathcal{T}$ -definable and any  $\phi \in \mathcal{T}$ , we can build two first-order formulæ,  $\overline{(\phi)}_\epsilon$  and  $(\widetilde{\phi})_\epsilon$ , in  $\mathcal{T}$ , such that  $\llbracket \phi \rrbracket_\epsilon = \llbracket \overline{(\phi)}_\epsilon \rrbracket$  and  $\gg \phi \ll_\epsilon = \llbracket (\widetilde{\phi})_\epsilon \rrbracket$  (see Sections 4.1 and 4.2, respectively). It means that, whenever  $\mathcal{T}$  is decidable, both  $\llbracket \cdot \rrbracket_\epsilon$  and  $\gg \cdot \ll_\epsilon$  are computable.

#### 4.1. From sphere into standard semantics

In our mapping from sphere to standard semantics, we need to distinguish two kind of variables: the  $\epsilon$ -variables (named  $W$ ,  $W_i$ ,  $\mathbf{W}$  and  $\mathbf{W}_i$ ) and standard variables (named  $Y$ ,  $Y_i$ ,  $\mathbf{Y}$  and  $\mathbf{Y}_i$ ) which are introduced to translate the sphere semantics into the standard one. The evaluations of the former will be perturbed by the transformation (being either  $\overline{(\cdot)}_\epsilon$  or  $(\widetilde{\cdot})_\epsilon$ ), while that of the latter will follow the standard semantics.

Let  $\mathcal{T}$  be a first-order theory over the reals,  $\varphi[\mathbf{Y}, \mathbf{W}]$  be any first-order formula, and  $\epsilon \in \mathbb{R}_{>0}$ . We define  $\overline{(\varphi[\mathbf{Y}, \mathbf{W}])}_\epsilon$  by structural induction on  $\varphi[\mathbf{Y}, \mathbf{W}]$  as follow:

- $\overline{((t_1 \circ t_2)[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{\text{def}}{=} \exists \mathbf{Y}_0 ((t_1 \circ t_2)[\mathbf{Y}, \mathbf{Y}_0] \wedge \delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon)$ ,  $\circ \in \{=, <\}$ ;
- $\overline{(\phi[\mathbf{Y}, \mathbf{W}] \wedge \psi[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{\text{def}}{=} \exists \mathbf{Y}_0 (\forall \mathbf{W}_1 (\delta(\mathbf{Y}_0, \mathbf{W}_1) < \epsilon \rightarrow (\overline{(\phi)}_\epsilon \wedge \overline{(\psi)}_\epsilon)[\mathbf{Y}, \mathbf{W}_1]) \wedge \delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon)$ ;
- $\overline{(\phi \vee \psi)}_\epsilon \stackrel{\text{def}}{=} \overline{(\phi)}_\epsilon \vee \overline{(\psi)}_\epsilon$ ;
- $\overline{(\forall W \phi[\mathbf{Y}, W, \mathbf{W}])}_\epsilon \stackrel{\text{def}}{=} \exists \mathbf{Y}_0 (\forall \mathbf{W}_1 (\delta(\mathbf{Y}_0, \mathbf{W}_1) < \epsilon \rightarrow \forall Y (\overline{(\phi[\mathbf{Y}, Y, \mathbf{W}_1])}_\epsilon) \wedge \delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon)$ ;
- $\overline{(\exists W \phi[\mathbf{Y}, W, \mathbf{W}])}_\epsilon \stackrel{\text{def}}{=} \exists Y (\overline{(\phi[\mathbf{Y}, Y, \mathbf{W}])}_\epsilon)$ ;
- $\overline{(\neg \phi[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{\text{def}}{=} \exists \mathbf{Y}_0 (\forall \mathbf{W}_1 (\delta(\mathbf{Y}_0, \mathbf{W}_1) < \epsilon \rightarrow \neg (\overline{(\phi[\mathbf{Y}, \mathbf{W}_1])}_\epsilon) \wedge \delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon)$ .

With regard to the distinction between  $\epsilon$ -variables ( $W$ ,  $W_i$ ,  $\mathbf{W}$  and  $\mathbf{W}_i$ ) and standard variables ( $Y$ ,  $Y_i$ ,  $\mathbf{Y}$  and  $\mathbf{Y}_i$ ), let us notice that the two formulæ  $\overline{(\phi[\mathbf{Y}, W, \mathbf{W}])}_\epsilon$  and  $\overline{(\phi[\mathbf{Y}, Y, \mathbf{W}])}_\epsilon$  may denote different sets. In particular, while  $W$  is perturbed by  $\epsilon$ -semantics,  $Y$  is involved in none of the

Minkowski sums related to above definition. For instance, if  $\phi$  is  $W > 2$ , then  $(\phi[\mathbf{Y}, W, \mathbf{W}])_\epsilon \equiv \exists Y_0 (Y_0 > 2 \wedge \delta(Y_0, W) < \epsilon)$ , while if  $\phi$  is  $W > 2$ , then  $(\phi[\mathbf{Y}, Y, \mathbf{W}])_\epsilon \equiv Y > 2$ .

Now we prove that the sphere semantics of  $\varphi$  and standard semantics of  $(\overline{\varphi})_\epsilon$  are the same and that, provided the decidability of  $\mathcal{T}$ , we can compute sphere semantics of the formula  $\varphi$ .

**Theorem 2** (Semantics Equivalence [14]). *Let  $\mathcal{T}$  be any first-order theory and  $\delta$  be a  $\mathcal{T}$ -definable distance. The sphere semantics  $(\cdot)_\epsilon$  over  $\mathcal{T}$  is  $\mathcal{T}$ -definable in the standard semantics and, in particular,  $(\varphi[\mathbf{X}])_\epsilon = \left\{ \left( \overline{(\varphi)}_\epsilon[\mathbf{X}] \right) \right\}$  for any formula  $\varphi[\mathbf{X}] \in \mathcal{T}$  and all  $\epsilon \in \mathbb{R}_{>0}$ .*

**Corollary 1.** *Let  $\mathcal{T}$  be a first-order theory. If  $\mathcal{T}$  is decidable and the distance  $\delta$  is definable in  $\mathcal{T}$ , then sphere semantics  $(\cdot)_\epsilon$  over  $\mathcal{T}$  is decidable.*

**Example 5.** *Let us consider the formula  $\varphi[X] \stackrel{\text{def}}{=} X > 0 \wedge X < 2$ . We have that  $(X > 0)_\epsilon \equiv \exists X_0 (X_0 > 0 \wedge \delta(X_0, X) < \epsilon) \equiv X_0 + \epsilon > 0$ . By applying the same rule,  $(X < 2)_\epsilon \equiv \exists X_0 (X_0 < 2 \wedge \delta(X_0, X) < \epsilon) \equiv X - 2 - \epsilon < 0$ . Finally, since  $\epsilon$  is a positive real,  $(X > 0 \wedge X < 2)_\epsilon \equiv \exists X_0 (\forall X_1 (\delta(X_0, X_1) < \epsilon \rightarrow X_1 + \epsilon > 0 \wedge X_1 - 2 - \epsilon < 0) \wedge \delta(X_0, X) < \epsilon) \equiv X > -\epsilon \wedge X \leq 2 + \epsilon$ .*

Let us notice that the formula  $(\overline{\psi})_\epsilon$  is syntactically more complex than  $\psi$ . This is mainly due to the possible introduction of new quantifier alternations.

#### 4.2. From DE into standard semantics

As in Section 4.1, to define mappings from both erosion and DE semantics to the standard one, we need to distinguish between  $\epsilon$ -variables (named  $W$ ,  $W_i$ ,  $\mathbf{W}$  and  $\mathbf{W}_i$ ) and standard variables (named  $Y$ ,  $Y_i$ ,  $\mathbf{Y}$  and  $\mathbf{Y}_i$ ).

Let  $\mathcal{T}$  be a first-order theory over the reals,  $\varphi[\mathbf{Y}, \mathbf{W}]$  be any first-order formula, and  $\epsilon \in \mathbb{R}_{>0}$ . There exist two formulæ  $(\widetilde{\varphi})_\epsilon$  and  $(\overline{\varphi})_\epsilon$  such that  $\|\varphi\|_\epsilon = \left\{ (\widetilde{\varphi})_\epsilon \right\}$  and  $\|\varphi\|_\epsilon = \left\{ (\overline{\varphi})_\epsilon \right\}$ . Moreover, we can compute both of them. As a matter of fact, it is easy to prove that

$$(\overline{\varphi[\mathbf{X}]})_\epsilon = \exists \mathbf{X}_0 \left( \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon \wedge (\overline{\varphi[\mathbf{X}_0]})_\epsilon \right).$$

As concern the formula  $(\overline{\psi[\mathbf{Y}, \mathbf{W}]})_\epsilon$ , we define it by structural induction on  $\psi$  as follows:

- $\overbrace{((t_1 \circ t_2)[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{def}{=} \forall \mathbf{Y}_1 (\delta(\mathbf{Y}_1, \mathbf{W}) < \epsilon \rightarrow (t_1 \circ t_2)[\mathbf{Y}, \mathbf{Y}_1]);$
- $\overbrace{((\psi_1 \wedge \psi_2)[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{def}{=} \overbrace{(\psi_1[\mathbf{Y}, \mathbf{W}])}_\epsilon \wedge \overbrace{(\psi_2[\mathbf{Y}, \mathbf{W}])}_\epsilon;$
- $\overbrace{((\psi_1 \vee \psi_2)[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{def}{=} \overbrace{(\psi_1[\mathbf{Y}, \mathbf{W}])}_\epsilon \vee \overbrace{(\psi_2[\mathbf{Y}, \mathbf{W}])}_\epsilon;$
- $\overbrace{(\forall W \psi_1[\mathbf{Y}, W, \mathbf{W}])}_\epsilon \stackrel{def}{=} \forall Y \overbrace{(\psi_1[\mathbf{Y}, Y, \mathbf{W}])}_\epsilon;$
- $\overbrace{(\exists W \psi_1[\mathbf{Y}, W, \mathbf{W}])}_\epsilon \stackrel{def}{=} \exists Y \overbrace{(\psi_1[\mathbf{Y}, Y, \mathbf{W}])}_\epsilon;$
- $\overbrace{(\neg \psi[\mathbf{Y}, \mathbf{W}])}_\epsilon \stackrel{def}{=} \neg \exists \mathbf{Y}_0 (\delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon \wedge \psi[\mathbf{Y}, \mathbf{Y}_0]).$

As done for the sphere semantics, we reduce the computation of  $\rangle \varphi \langle_\epsilon$  to the evaluation of the standard semantics of  $\overbrace{(\varphi)}_\epsilon$ .

**Theorem 3.** *Let  $\mathcal{T}$  be any first-order theory and  $\delta$  be a  $\mathcal{T}$ -definable distance. The erosion semantics  $\rangle \cdot \langle_\epsilon$  of  $\mathcal{T}$  is  $\mathcal{T}$ -definable in the standard semantics and, in particular,  $\rangle \psi[\mathbf{X}] \langle_\epsilon = \left\{ \overbrace{(\psi[\mathbf{X}])}_\epsilon \right\}$  for any formula  $\psi[\mathbf{X}] \in \mathcal{T}$  and all  $\epsilon \in \mathbb{R}_{>0}$ .*

*Proof.* By structural induction on  $\psi$ .

$\psi[\mathbf{Y}, \mathbf{W}]$  is atomic.

By the definition of the erosion semantics,  $\rangle t_1 \circ t_2 \langle_\epsilon = \bigcup_{B(p, \epsilon) \subseteq \{t_1 \circ t_2\}} \{p\}$ , for  $\circ \in \{=, <\}$ . The right-hand term of the last equation is the union of the centers of all the  $\epsilon$ -spheres entirely included into the standard semantics of  $(t_1 \circ t_2)$ . Any point  $\bar{y}$  is included in such a union if and only if all the points belonging to the  $\epsilon$ -sphere centered in  $\bar{y}$  satisfy  $(t_1 \circ t_2)$ . By the standard semantics, the latter sentence holds if and only if the formula  $\forall \mathbf{Y}_1 (\delta(\mathbf{Y}_1, \mathbf{W}) < \epsilon \rightarrow (t_1 \circ t_2)[\mathbf{Y}, \mathbf{Y}_1])$  does the same.

$\psi[\mathbf{Y}, \mathbf{W}]$  has the form  $(\psi_1 \wedge \psi_2)[\mathbf{Y}, \mathbf{W}]$ .

By definition,  $\rangle \psi_1 \wedge \psi_2 \langle_\epsilon \stackrel{def}{=} \rangle \psi_1 \langle_\epsilon \cap \rangle \psi_2 \langle_\epsilon$ , while, by inductive hypothesis both  $\rangle \psi_1 \langle_\epsilon = \left\{ \overbrace{(\psi_1)}_\epsilon \right\}$  and  $\rangle \psi_2 \langle_\epsilon = \left\{ \overbrace{(\psi_2)}_\epsilon \right\}$  hold. From the standard semantics and the definition of  $\overbrace{(\cdot)}_\epsilon$ , we deduce the thesis.

$\psi[\mathbf{Y}, \mathbf{W}]$  has the form  $(\psi_1 \vee \psi_2)[\mathbf{Y}, \mathbf{W}]$ .

Similarly to the previous case, since  $\rangle\psi_1 \vee \psi_2\langle_\epsilon \stackrel{def}{=} \rangle\psi_1\langle_\epsilon \cup \rangle\psi_2\langle_\epsilon$  and by inductive hypothesis both  $\rangle\psi_1\langle_\epsilon = \left\{ \overline{(\psi_1)_\epsilon} \right\}$  and  $\rangle\psi_2\langle_\epsilon = \left\{ \overline{(\psi_2)_\epsilon} \right\}$  hold, we can deduce the thesis directly from the standard semantics and the definition of  $\overline{(\cdot)_\epsilon}$ .

$\psi[\mathbf{Y}, \mathbf{W}]$  has the form  $\forall W \psi_1[\mathbf{Y}, W, \mathbf{W}]$ .

By definition,  $\rangle\forall W \psi_1[\mathbf{Y}, W, \mathbf{W}]\langle_\epsilon \stackrel{def}{=} \bigcap_{r \in \mathbb{R}} \rangle\psi_1[\mathbf{Y}, r, \mathbf{W}]\langle_\epsilon$ . By inductive hypothesis  $\rangle\psi_1[\mathbf{Y}, r, \mathbf{W}]\langle_\epsilon = \left\{ \overline{(\psi_1[\mathbf{Y}, r, \mathbf{W}])_\epsilon} \right\}$  holds, while by the standard semantics  $\bigcap_{r \in \mathbb{R}} \rangle\psi_1[\mathbf{Y}, r, \mathbf{W}]\langle_\epsilon = \left\{ \overline{\forall Y (\psi_1[\mathbf{Y}, Y, \mathbf{W}])_\epsilon} \right\}$  holds too. Hence, from the definition of erosion semantics, we can conclude that the sets  $\left\{ \overline{\forall Y (\psi_1[\mathbf{Y}, Y, \mathbf{W}])_\epsilon} \right\}$  and  $\rangle\forall W \psi_1[\mathbf{Y}, W, \mathbf{W}]\langle_\epsilon$  are identical.

$\psi[\mathbf{Y}, \mathbf{W}]$  has the form  $\exists W \psi_1[\mathbf{Y}, W, \mathbf{W}]$ .

By using the same argument of the previous case, we deduce that  $\rangle\exists W \psi_1[\mathbf{Y}, W, \mathbf{W}]\langle_\epsilon \stackrel{def}{=} \bigcup_{r \in \mathbb{R}} \rangle\psi_1[\mathbf{Y}, r, \mathbf{W}]\langle_\epsilon = \left\{ \overline{\exists Y (\psi_1[\mathbf{Y}, Y, \mathbf{W}])_\epsilon} \right\}$  holds.

$\psi[\mathbf{Y}, \mathbf{W}]$  has the form  $\neg\psi_1[\mathbf{Y}, \mathbf{W}]$ .

By definition,  $\rangle\neg\psi\langle_\epsilon \stackrel{def}{=} \bigcup_{B(p, \epsilon) \cap \{\psi_1\} = \emptyset} \{p\}$ . The right-hand term of the last equation is the union of the centers of all the  $\epsilon$ -spheres which do not intersect the standard semantics of  $\psi_1$ . Any point  $\vec{y}$  belongs to such union if and only if all the points included into the  $\epsilon$ -sphere centered in  $\vec{y}$  do not satisfy  $\psi$ . By the standard semantics, the latter sentence holds if and only if the formula  $\neg\exists \mathbf{Y}_0 (\delta(\mathbf{Y}_0, \mathbf{W}) < \epsilon \wedge \psi[\mathbf{Y}, \mathbf{Y}_0])$  does the same.

□

**Corollary 2.** *Let  $\mathcal{T}$  be a first-order theory. If  $\mathcal{T}$  is decidable and the distance  $\delta$  is definable in  $\mathcal{T}$ , then DE semantics  $\rangle\langle_\epsilon$  over  $\mathcal{T}$  is decidable.*

If in Algorithm 3 we use DE semantics, the emptiness test at line 9 can be performed by using erosion semantics. As a matter of the facts, since

$\llbracket \psi \rrbracket_\epsilon \stackrel{def}{=} \bigcup_{p \in \llbracket \psi \rrbracket_\epsilon} B(p, \epsilon)$ ,  $\llbracket \psi \rrbracket_\epsilon$  is empty if and only if  $\llbracket \psi \rrbracket_\epsilon$  is empty too. This replacement does not affect the result of the computation, but it decreases the complexity of the formulæ whose satisfiability should be tested. In particular, given a formula  $\psi[\mathbf{X}]$ , we have that  $\llbracket \psi \rrbracket_\epsilon = \left\{ \left( \widetilde{\psi} \right)_\epsilon \right\}$  and, by definition,  $\left( \widetilde{\psi} \right)_\epsilon$  has  $|\mathbf{X}|$  existential quantifiers more than  $\widetilde{\psi}$ .

## 5. Formulæ Simplifications

The formulæ translation described in Sections 4.1 and 4.2 allow us to decide sphere and DE semantics. They can be used to evaluate any first-order formula and the complexity of such evaluation depends on that of deciding  $\mathcal{T}$ . However, since we are interested in applying the translations in a quite specific context, i.e., in the evaluation of “reachability formulæ”, we can study syntactic simplifications tailored on those formulæ. Such simplifications may decrease the complexity of decision procedures of the emptiness test on line 9 of Algorithm 1.

The first simplifications that we introduce concern the translations of conjunctions of atomic formulæ from sphere semantics to the standard one. Conjunctions arise naturally in formulæ expressing reachability since, for instance, in the case of a continuous transition, it is necessary to both impose to satisfy the invariant and the dynamics. The simplifications that we describe can be applied only when the atoms represent convex and closed sets.

**Lemma 2.** *Let  $\mathbb{S} \subseteq \mathbb{R}^n$  be a convex and closed set,  $\epsilon \in \mathbb{R}_{>0}$ , and  $p \in \mathbb{R}^n$ . If  $\forall \mathbf{X}_0 (\delta(p, \mathbf{X}_0) < \epsilon \rightarrow \exists \mathbf{X}_1 (\mathbf{X}_1 \in \mathbb{S} \wedge \delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon))$  holds, then  $p \in \mathbb{S}$ .*

*Proof.* The proof is given by contradiction. Let  $p \in (\mathbb{R}^n \setminus \mathbb{S})$  satisfying the assumption of the lemma. By letting  $\mathbf{X}_0 = p$  we get  $\exists \mathbf{X}_1 (\mathbf{X}_1 \in \mathbb{S} \wedge \delta(p, \mathbf{X}_1) < \epsilon)$ , therefore  $B(p, \epsilon) \cap \mathbb{S} \neq \emptyset$ , and  $\delta(p, \mathbb{S}) < \epsilon$ .

Then the distance  $\delta(p, \text{conv}(\mathbb{S}))$  is a nonzero number  $d < \epsilon$ , since  $\mathbb{S} = \text{conv}(\mathbb{S})$  is closed. Let  $q \in \mathbb{S}$  be such a point that  $\delta(q, p) = d$ . We can use the linear separability theorem: because  $p = \text{conv}(p)$  and  $\mathbb{S} = \text{conv}(\mathbb{S})$  are two disjoint convex sets, there exists a separating hyperplane perpendicular to the line through  $q$  and  $p$ .

Let us now consider a point  $v \in B(p, \epsilon)$  on the line going through  $p$  and  $q$  such that  $\delta(v, p) = \epsilon - d/2$  and  $\delta(v, q) = \epsilon + d/2$ . Then  $\delta(v, \mathbb{S}) \geq \delta(v, q) > \epsilon$ , which is a contradiction with the assumption  $\forall \mathbf{X}_0 (\delta(p, \mathbf{X}_0) < \epsilon \rightarrow \exists \mathbf{X}_1 (\mathbf{X}_1 \in \mathbb{S} \wedge \delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon))$ .

$\mathbb{S} \wedge \delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon$ ), if  $d > 0$ . Therefore  $\delta(p, \mathbb{S}) = 0$ , and because  $\mathbb{S}$  is closed,  $p \in \mathbb{S}$ .  $\square$

By exploiting the above lemma, in the case of a convex and closed set represented as conjunction of formulæ, we obtain the following result.

**Theorem 4.** *Let  $\mathcal{T}$  be a first-order theory over the reals,  $\varphi_1[\mathbf{X}], \dots, \varphi_k[\mathbf{X}]$  be  $k$  first-order formulæ  $\mathcal{T}$ -definable, such that sets  $\{\varphi_1\}, \dots, \{\varphi_k\} \subseteq \mathbb{R}^n$  are convex and closed, and let  $\epsilon \in \mathbb{R}_{>0}$ . Then the formula*

$$\psi[\mathbf{X}] \stackrel{def}{=} \exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \bigwedge_{i=1}^k \exists \mathbf{X}_{i+1} (\varphi_i[\mathbf{X}_{i+1}] \wedge \delta(\mathbf{X}_{i+1}, \mathbf{X}_1) < \epsilon)) \wedge \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon)$$

*is equivalent to the formula*

$$\theta[\mathbf{X}] \stackrel{def}{=} \exists \mathbf{X}_0 ((\bigwedge_{i=1}^k \varphi_i[\mathbf{X}_0]) \wedge \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon).$$

*Proof.*  $(\Rightarrow)$  Let  $\psi[q]$  hold for a point  $q \in \mathbb{R}^n$ . That is equivalent to the formula  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\mathbf{X}_1 \in B(\mathbf{X}_0, \epsilon) \rightarrow \bigwedge_{i=1}^k \exists \mathbf{X}_{i+1} (\mathbf{X}_{i+1} \in \{\varphi_i\} \cap B(\mathbf{X}_1, \epsilon))) \wedge \mathbf{X}_0 \in B(q, \epsilon))$ .

Now we can use Lemma 2, letting  $p = \mathbf{X}_0, \mathbb{S} = \{\varphi_i\}$  and get for any choice of  $i \in \{1, \dots, k\}$  that  $\mathbf{X}_0 \in \{\varphi_i\}$ . Then,  $\theta[q] = \exists \mathbf{X}_0 (\mathbf{X}_0 \in (\bigcap_{i=1}^k \{\varphi_i\}) \wedge \delta(q, \mathbf{X}_0) < \epsilon)$  is true for the given point  $q \in \mathbb{R}^n$ .

$(\Leftarrow)$  Let  $\theta[q]$  hold for a point  $q \in \mathbb{R}^n$ . That means the same as the formula  $\exists \mathbf{X}_0 (\mathbf{X}_0 \in (\bigcap_{i=1}^k \{\varphi_i\}) \cap B(q, \epsilon))$ , which implies  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \mathbf{X}_0 \in \bigcap_{i=1}^k \{\varphi_i\} \wedge \delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon))$ , that in turn implies  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \bigwedge_{i=1}^k \exists \mathbf{X}_{i+1} (\mathbf{X}_{i+1} \in \{\varphi_i\} \wedge \delta(\mathbf{X}_{i+1}, \mathbf{X}_1) < \epsilon)))$ , because from above there exists at least  $\mathbf{X}_2 = \mathbf{X}_0, \mathbf{X}_3 = \mathbf{X}_0, \dots, \mathbf{X}_{k+1} = \mathbf{X}_0$  for every  $\mathbf{X}_1 \in B(\mathbf{X}_0, \epsilon)$ . Which means  $\psi[q]$  holds.  $\square$

Similarly, when the convex and closed set is represented as a disjunction of formulæ, we get the following theorem.

**Theorem 5.** *Let  $\mathcal{T}$  be a first-order theory over the reals,  $\varphi_1[\mathbf{X}], \dots, \varphi_k[\mathbf{X}]$  be  $k$  first-order formulæ  $\mathcal{T}$ -definable, such that the union of sets  $\{\varphi_1\}, \dots, \{\varphi_k\} \subseteq \mathbb{R}^n$  is a convex and closed subset of  $\mathbb{R}^n$ , and let  $\epsilon \in \mathbb{R}_{>0}$ .*

*Then the formula*

$$\psi[\mathbf{X}] \stackrel{def}{=} \exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \bigvee_{i=1}^k \exists \mathbf{X}_{i+1} (\varphi_i[\mathbf{X}_{i+1}] \wedge \delta(\mathbf{X}_{i+1}, \mathbf{X}_1) < \epsilon)) \wedge \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon)$$

is equivalent to the formula

$$\theta[\mathbf{X}] \stackrel{def}{=} \exists \mathbf{X}_0 ((\bigvee_{i=1}^k \varphi_i[\mathbf{X}_0]) \wedge \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon).$$

*Proof.* ( $\Rightarrow$ ) Let  $\psi[q]$  hold for a point  $q \in \mathbb{R}^n$ . That is equivalent to the formula  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\mathbf{X}_1 \in B(\mathbf{X}_0, \epsilon) \rightarrow \bigvee_{i=1}^k \exists \mathbf{X}_{i+1} (\mathbf{X}_{i+1} \in \{\varphi_i\} \cap B(\mathbf{X}_1, \epsilon))) \wedge \mathbf{X}_0 \in B(q, \epsilon))$ , which is equivalent to  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\mathbf{X}_1 \in B(\mathbf{X}_0, \epsilon) \rightarrow \exists \mathbf{X}_2 (\mathbf{X}_2 \in (\bigcup_{i=1}^k \{\varphi_i\}) \cap B(\mathbf{X}_1, \epsilon))) \wedge \mathbf{X}_0 \in B(q, \epsilon))$ .

Now we can use Lemma 2, letting  $p = \mathbf{X}_0$ ,  $\mathbb{S} = \bigcup_{i=1}^k \{\varphi_i\}$ , and get  $\mathbf{X}_0 \in \bigcup_{i=1}^k \{\varphi_i[\mathbf{X}]\} = \{\bigvee_{i=1}^k \varphi_i[\mathbf{X}]\}$ . Then  $\theta[q] = \exists \mathbf{X}_0 ((\bigvee_{i=1}^k \varphi_i[\mathbf{X}_0]) \wedge \delta(q, \mathbf{X}_0) < \epsilon)$  is true for the given point  $q \in \mathbb{R}^n$ .

( $\Leftarrow$ ) Let  $\theta[q]$  hold for a point  $q \in \mathbb{R}^n$ . That means the same as the formula  $\exists \mathbf{X}_0 (\mathbf{X}_0 \in (\bigcup_{i=1}^k \{\varphi_i\}) \cap B(q, \epsilon))$ , which implies  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \mathbf{X}_0 \in \bigcup_{i=1}^k \{\varphi_i\}) \wedge \delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon)$ , that in turn implies  $\exists \mathbf{X}_0 (\forall \mathbf{X}_1 (\delta(\mathbf{X}_0, \mathbf{X}_1) < \epsilon \rightarrow \bigvee_{i=1}^k \exists \mathbf{X}_{i+1} (\mathbf{X}_{i+1} \in \{\varphi_i\} \wedge \delta(\mathbf{X}_{i+1}, \mathbf{X}_1) < \epsilon)))$ , because from above, there exists  $i \in \{1, 2, \dots, k\}$  satisfying  $\mathbf{X}_0 \in \{\varphi_i\}$ , which means  $\psi[q]$  holds.  $\square$

By applying above results to sphere semantics translation, we obtain the following simplification.

**Corollary 3.** *Let  $\mathcal{T}$  be a first-order theory over the reals,  $\varphi_1[\mathbf{X}]$  and  $\varphi_2[\mathbf{X}]$  be first-order formulæ  $\mathcal{T}$ -definable, such that both the sets  $\{\varphi_1\}$  and  $\{\varphi_2\}$  are subsets of  $\mathbb{R}^n$  are convex and closed, and let  $\epsilon \in \mathbb{R}_{>0}$ . Then*

$$(\varphi_1[\mathbf{X}] \wedge \varphi_2[\mathbf{X}])_\epsilon = \{\exists \mathbf{X}_0 (\varphi_1[\mathbf{X}_0] \wedge \varphi_2[\mathbf{X}_0] \wedge \delta(\mathbf{X}, \mathbf{X}_0) < \epsilon)\}.$$

In the case of closed formulæ, both sphere and DE semantics are equivalent to the standard one. This is mainly due to the fact that in both semantics the rules for atoms only expand (shrink, respectively) variables. Moreover, the rules for quantifiers replace variables with constants.

**Theorem 6.** *If  $\varphi$  is a formula without free variables, then  $\gg \varphi \ll_\epsilon = \gg \varphi \ll_\epsilon = \{\varphi\}$ .*

*Proof.* As first thing, let notice that the standard evaluation of a formula  $\psi$  without free variables is a truth value which can be true ( $\top$ ) or false ( $\perp$ ). Hence, the standard semantics of a formula without free variables is either  $\{\psi\} = \mathbb{R}^*$  or  $\{\psi\} = \emptyset$ . Moreover, the  $\epsilon$ -expansions of such kind of sets, correspond to the sets themselves, i.e.,  $B(\mathbb{R}^*, \epsilon) = \mathbb{R}^*$  and  $B(\emptyset, \epsilon) = \emptyset$ . Let first demonstrate by structural induction on a formula  $\psi$  without free variables that  $\gg \psi \ll_\epsilon = \{\psi\}$ .



$t_1 \circ t_2$ , for  $\circ \in \{=, <\}$ .  $\rangle t_1 \circ t_2 \langle_\epsilon$  is defined as the union of all the centers of the  $\epsilon$ -spheres entirely included into  $\llbracket t_1 \circ t_2 \rrbracket$ . Since  $(t_1 \circ t_2)$  is without free variables, either  $\llbracket t_1 \circ t_2 \rrbracket = \mathbb{R}^*$  or  $\llbracket t_1 \circ t_2 \rrbracket = \emptyset$ . Let notice that both  $\bigcup_{B(p,\epsilon) \subseteq \mathbb{R}^*} \{p\} = \mathbb{R}^*$  and  $\bigcup_{B(p,\epsilon) \subseteq \emptyset} \{p\} = \emptyset$  hold. But this means that if  $(t_1 \circ t_2)$  is true, then  $\llbracket t_1 \circ t_2 \rrbracket = \mathbb{R}^* \Rightarrow \rangle t_1 \circ t_2 \langle_\epsilon$ , while if  $(t_1 \circ t_2)$  is false, then  $\llbracket t_1 \circ t_2 \rrbracket = \emptyset \Rightarrow \rangle t_1 \circ t_2 \langle_\epsilon$ . Then we can state that  $\llbracket t_1 \circ t_2 \rrbracket = \rangle t_1 \circ t_2 \langle_\epsilon$ .

$\psi_1 \wedge \psi_2$ . By the definition of erosion semantics  $\rangle \psi_1 \wedge \psi_2 \langle_\epsilon \stackrel{def}{=} \rangle \psi_1 \langle_\epsilon \cap \rangle \psi_2 \langle_\epsilon$ . Moreover, by inductive hypothesis we know that  $\rangle \psi_1 \langle_\epsilon = \llbracket \psi_1 \rrbracket$  and  $\rangle \psi_2 \langle_\epsilon = \llbracket \psi_2 \rrbracket$ . Hence,  $\llbracket \psi_1 \wedge \psi_2 \rrbracket = \llbracket \psi_1 \rrbracket \cap \llbracket \psi_2 \rrbracket = \rangle \psi_1 \langle_\epsilon \cap \rangle \psi_2 \langle_\epsilon = \rangle \psi_1 \wedge \psi_2 \langle_\epsilon$  holds.

$\psi_1 \vee \psi_2$ . Similarly to the previous case, exploiting the erosion semantics' definition and the inductive hypothesis, we have that the equalities  $\llbracket \psi_1 \vee \psi_2 \rrbracket = \llbracket \psi_1 \rrbracket \cup \llbracket \psi_2 \rrbracket = \rangle \psi_1 \langle_\epsilon \cup \rangle \psi_2 \langle_\epsilon = \rangle \psi_1 \vee \psi_2 \langle_\epsilon$  hold.

$\forall W \psi[W]$ . In this case,  $\rangle \forall W \psi[W] \langle_\epsilon \stackrel{def}{=} \bigcap_{r \in \mathbb{R}} \rangle \psi[r] \langle_\epsilon$ . By inductive hypothesis it holds that  $\rangle \psi[r] \langle_\epsilon = \llbracket \psi[r] \rrbracket$ . Thus, by the standard semantics it follows that  $\rangle \forall W \psi[W] \langle_\epsilon = \bigcap_{r \in \mathbb{R}} \rangle \psi[r] \langle_\epsilon = \bigcap_{r \in \mathbb{R}} \llbracket \psi[r] \rrbracket = \llbracket \forall W \psi[W] \rrbracket$ .

$\exists W \psi[W]$ . Similarly to the previous case, exploiting the erosion semantics' definition and the inductive hypothesis, we have that the equalities  $\rangle \exists W \psi[W] \langle_\epsilon = \bigcup_{r \in \mathbb{R}} \rangle \psi[r] \langle_\epsilon = \bigcup_{r \in \mathbb{R}} \llbracket \psi[r] \rrbracket = \llbracket \exists W \psi[W] \rrbracket$  hold.

$\neg \psi$ . By the definition of erosion semantics  $\rangle \neg \psi \langle_\epsilon = \bigcup_{B(p,\epsilon) \cap \llbracket \psi \rrbracket = \emptyset} \{p\}$ . Note that if  $\psi$  is true, then  $\rangle \neg \psi \langle_\epsilon = \bigcup_{B(p,\epsilon) \cap \mathbb{R}^* = \emptyset} \{p\} = \emptyset = \llbracket \neg \psi \rrbracket$ , while if  $\psi$  is false, then  $\rangle \neg \psi \langle_\epsilon = \bigcup_{B(p,\epsilon) \cap \emptyset = \emptyset} \{p\} = \mathbb{R}^* = \llbracket \neg \psi \rrbracket$ , which means that  $\rangle \neg \psi \langle_\epsilon = \llbracket \neg \psi \rrbracket$ .

Finally, the DE semantics  $\llbracket \cdot \rrbracket_\epsilon$  of a formula  $\psi$  is defined as  $B(\rangle \psi \langle_\epsilon, \epsilon)$ . If  $\psi$  is without free variables, we know that  $B(\rangle \psi \langle_\epsilon, \epsilon) = B(\llbracket \psi \rrbracket, \epsilon)$ . Moreover, since in this case  $\llbracket \psi \rrbracket$  is either  $\mathbb{R}^*$  or  $\emptyset$ , it holds that  $B(\llbracket \psi \rrbracket, \epsilon) = \llbracket \psi \rrbracket$ , which in turn means that  $\llbracket \psi \rrbracket_\epsilon = B(\llbracket \psi \rrbracket, \epsilon) = \llbracket \psi \rrbracket$ . In conclusion we can state that if a formula  $\psi$  is without free variables, then  $\llbracket \psi \rrbracket_\epsilon = \rangle \psi \langle_\epsilon = \llbracket \psi \rrbracket$ .  $\square$

## 6. Analysis of Two Biological Hybrid Models

In order to investigate the effectiveness of the proposed methods, we performed  $\epsilon$ -semantics based analysis on two biological models that represent a neural oscillator system and a glycemic control in diabetic patients, respectively. In this section, we present the investigated models and detail the results of these analysis.

### 6.1. Neural Oscillator

Oscillatory electrical stimuli have been considered central for the activities of several brain regions since the '80s. It was shown that they play an important role in the olfactory information processing [15] and they were observed in the hippocampus [16], in the thalamus [17], and in the cortex [18]. Many studies suggested that, in the mammalian visual system, neuron signals may be grouped together through in-phase oscillations [19]. Hence, the development and analysis of models representing oscillatory phenomena assume a great importance in understanding the neurophysiological activities.

A simple continuous model of a single oscillator has been proposed in [20]. The model describes the evolutions of one excitatory neuron ( $N_e$ ) and one inhibitory neuron ( $N_i$ ) by mean of the ordinary differential system.

$$f(\tau, \lambda) : \begin{cases} \dot{X}_e = -\frac{X_e}{\tau} + \tanh(\lambda * X_e) - \tanh(\lambda * X_i) \\ \dot{X}_i = -\frac{X_i}{\tau} + \tanh(\lambda * X_i) + \tanh(\lambda * X_e) \end{cases}, \quad (1)$$

where  $X_e$  and  $X_i$  are the output of  $N_e$  and  $N_i$ , respectively,  $\tau$  is a characteristic time constant, and  $\lambda > 0$  is the amplification gain.

Hopf bifurcation characterizes a qualitative change in the evolution of  $f(\tau, \lambda)$ : if  $\tau * \lambda \leq 1$ , then the point  $(0,0)$  is the unique global attractor of the system. If, otherwise,  $\tau * \lambda > 1$ , all the evolutions converge to a limit cycle attractor whose period is about  $\frac{2\pi}{\lambda}$  and the origin is an unstable equilibrium [21]. Fig. 3 depicts two simulations of the system  $f(3,1)$ : one from a point internal to the limit cycle and one from an external point.

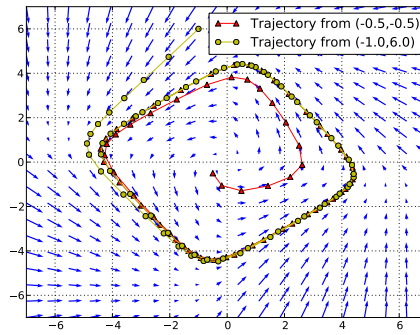


Figure 3: Two evolutions of the system  $f(3,1)$ . They both converge to a limit cycle.

Even if  $f(\tau, \lambda)$  is rather simple, the ability of analyzing a complex system obtained by composing multiple copies of this model is limited due to the non-linearity of  $f(\tau, \lambda)$  itself. For this reason, we are interested in the development of a piecewise affine hybrid model whose behaviour fairly approximates System (1) and that can be automatically analyzed and composed.

Moreover, while the limit cycle revealed by the differential-based model is also exhibited by the real system, the unstable equilibrium is not observable in nature as minimal disturbances always move the system itself away from the origin. Hence, the differential-based model fails to represent the exact system evolution with respect to point  $\langle 0, 0 \rangle$  and, because of this, we decided to investigate it by using  $\epsilon$ -based analysis.

We approximated the nonlinear part of the System (1) (i.e.,  $\tanh(\lambda * X)$ ) by the piecewise function  $h_{\lambda, \alpha}(z)$  defined as follow:

$$h_{\lambda, \alpha}(z) \stackrel{\text{def}}{=} \begin{cases} -1 & \text{if } z < -\frac{\alpha}{\lambda} \\ \frac{\lambda}{\alpha} * z & \text{if } -\frac{\alpha}{\lambda} \leq z < \frac{\alpha}{\lambda} \\ 1 & \text{if } z \geq \frac{\alpha}{\lambda} \end{cases} , \quad (2)$$

where  $\alpha$  is the approximation coefficient which determines the slope of the central segment (see Figure 4). This leads to the hybrid automaton  $H_{\tilde{f}}$  depicted in Figure 5.

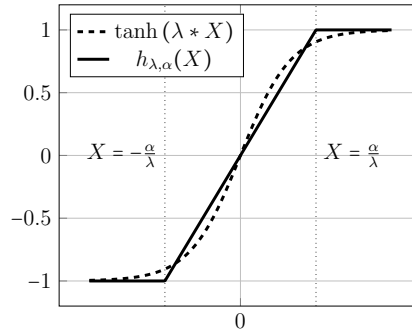


Figure 4:  $h_{\lambda, \alpha}(X)$  approximating  $\tanh(\lambda * X)$ .

We intend to study  $H_{\tilde{f}}$  behaviour through sphere semantics, exploiting cylindrical algebraic decomposition tools to automatically compute it. In particular, we want to prove that each point in the space reaches a bounded region which includes the limit cycle. Notice that in this example our automata have unbounded invariants, hence the termination of sphere semantics reachability algorithm is not guaranteed.

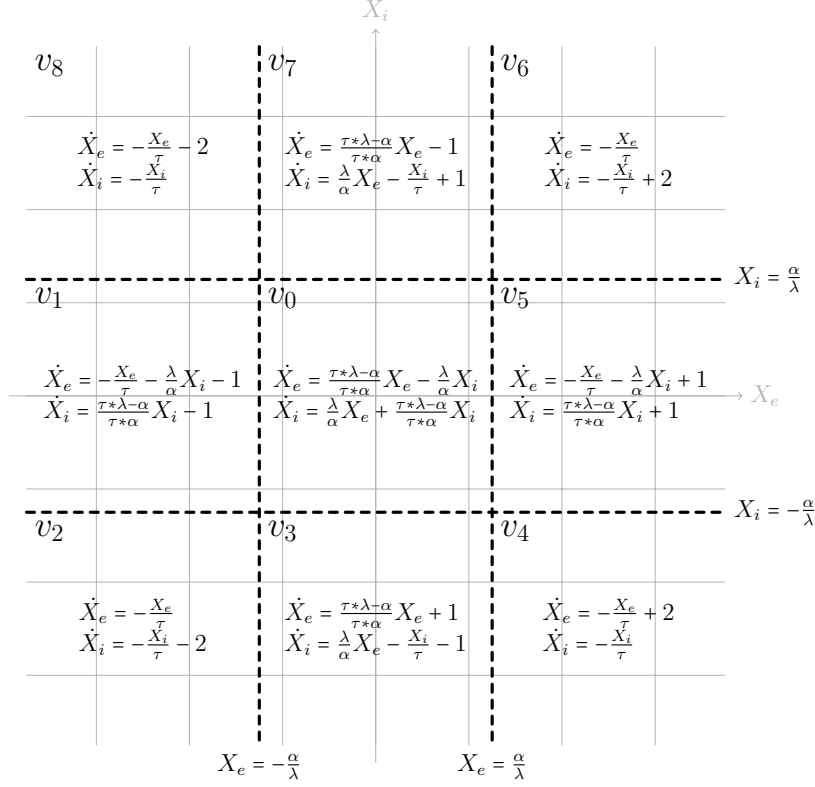


Figure 5: A graphical representation of the hybrid automaton  $H_{\tilde{f}}$  associated to the function  $\tilde{f}_{\alpha}(\tau, \lambda)$ .

First of all, we replace the differential equations with the corresponding first-degree Taylor polynomials. In order to keep the presentation simple, in this section we fix the parameters as follows  $\tau = 3$ ,  $\lambda = 1$ ,  $\alpha = 2$ . Hence, the activations correspond to the axis  $X_i = \pm 2$  and  $X_e = \pm 2$ .

We start computing the intersections of the limit cycle with the activation regions. For instance, there is one single point in the intersection between the limit cycle and the segment defined by  $X_i = 2$  and  $X_e > 0$ ; we denote it by  $Q_0 \stackrel{def}{=} \langle x_{Q_0}, 2 \rangle$ . Similarly,  $Q_1 \stackrel{def}{=} \langle 2, y_{Q_1} \rangle$  will be the intersection between the limit cycle and the region  $X_e = 2$  and  $X_i > 0$ . Let us now consider a point  $P_0$  located on  $X_i = 2$  such that its distance  $d_0$  from  $Q_0$  is at least  $2\epsilon$ , i.e.,  $P_0 \stackrel{def}{=} \langle x_{P_0}, 2 \rangle$  and  $\delta(Q_0, P_0) \stackrel{def}{=} d_0 > 2\epsilon$ . Moreover, let  $P_1$  a point laying on  $X_e = 2$  that, according to the sphere semantics, is reachable through a

continuous evaluation from  $P_0$ .

If we could prove that the distance  $d_1$  between such  $P_1$  and  $Q_1$ , i.e.,  $d_1 \stackrel{def}{=} \delta(Q_1, P_1)$ , is always smaller than  $d_0$ , then we would be able to conclude that all the points which start from a distance of at least  $2\epsilon$  from the limit cycle converge to a flow tube having diameter  $2\epsilon$  that includes the limit cycle. Of course, to this end, we need to prove this property on all locations.

We can formalize this property through a first-order formula. In order to generalize it and enable us to write analogous formulæ for different locations, we denote with  $r$  and  $s$  the straight lines  $X_i = 2$  and  $X_e = 2$ , respectively, and with the notation  $Q_0 \in (r \cap C \cap (X_e > 0))$  the membership of  $Q_0$  to the intersection of straight line  $r$  with limit cycle  $C$  and positive  $X_e$  semi-plane. Moreover, by writing  $P_0 \rightarrow_C P_1$  we denote the first-order formula representing the continuous transition from  $P_0$  to  $P_1$  and, hence,  $\overline{(P_0 \rightarrow_C P_1)}_\epsilon$  characterizes the sphere semantics of such continuous transition. Thus, our desired property can be expressed as: The property stating the convergence to the limit flow tube in location  $v_6$  can be expressed as:

$$\begin{aligned} \forall Q_0 Q_1 \forall P_0 P_1 & \left( (Q_0 \in (r \cap C \cap (X_e > 0))) \wedge Q_1 \in (s \cap C \cap (X_i > 0))) \wedge \right. \\ & P_0 \in (r \cap (X_e > 0)) \wedge P_1 \in (s \cap (X_e > 0)) \wedge \\ & \left. \delta(Q_0, P_0) > 2\epsilon \wedge \overline{(P_0 \rightarrow_C P_1)}_\epsilon \rightarrow \delta(Q_1, P_1) < \delta(Q_0, P_0) \right). \end{aligned} \quad (3)$$

For all the locations, but  $v_0$ , we can automatically compute a formula analogous to the above one and express the same property. This can be easily done by changing the roles of activation border lines  $r$  and  $s$ .

We used a Python package, named `pyHybridAnalysis` [22] (available at <http://www.dmi.units.it/~casagran/pyHybridAnalysis/>), to encode both the  $\epsilon$ -semantics framework and the simplifications presented in Section 5. Moreover, this package provides easy-to-use interfaces to REDLOG [23] and allows us to test the satisfiability of a formula. We used it to both evaluate  $\overline{(P_0 \rightarrow_C P_1)}_\epsilon$  and prove our conjectures. In particular, Formula 3 with  $\delta$  induced by maximum norm, has been evaluated to `true` in about 25 seconds on a MacBook Pro Late 2011 having 8GB RAM. This result has been achieved mainly thank to the linear dynamics approximation and the simplifications presented in Section 5. As a matter of facts, without applying formula simplification, we were not able to get any result after 1 hour.

One could argue that the linear dynamics, which has been used in the analysis, roughly approximates the original system. However, we can easily improve the precision of our model by augmenting the number of its locations

(e.g., see Figure 6). This only increase the number of formulæ we have to check and not their complexity.

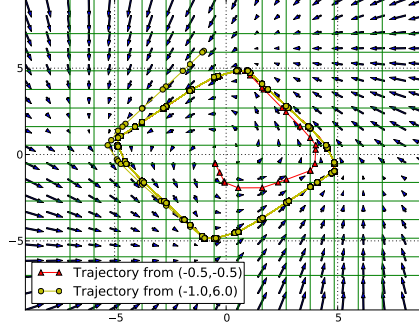


Figure 6: In order to better approximate the original system still using linear dynamics we can increase the number of automaton's locations.

As far as  $\langle 0, 0 \rangle$  is concerned, it is immediate to prove that, according to sphere semantics, it reaches points different from itself and, hence, the limit flow tube, while this not the case for the standard semantics. This is a very simple example on which standard reachability fails to capture the behaviour of the real system.

Other interesting properties that can be automatically verified express the fact that by applying the sphere semantics there are points that cross the limit cycle. Since natural phenomena are subject to noises, this appear to be more coherent to the modeled system than what happen by applying standard semantics.

## 6.2. Glycemic control in Diabetic Patients

The glycemic control in diabetic patients consists in monitoring and correcting the blood glucose level of a patient affected by diabetes. Since it is well known that a good glycemic control plays an important role in the diabetes care, it is important to develop and study models that may be useful in the design of insulin infusion devices.

The investigated hybrid automaton is based on the continuous model pre-

sented in [24]. The overall system is depicted by the following system.

$$\begin{aligned}\dot{G} &= -p_1 G - X(G + G_B) + g(t) \\ \dot{X} &= -p_2 X + p_3 I \\ \dot{I} &= -n(I + I_B) + \frac{1}{V_I} i(t)\end{aligned}$$

where the functions  $g(t)$  and  $i(t)$  directly depend on  $G$  and  $t$ , respectively, and are piecewise defined as:

$$i(t) = \begin{cases} \frac{25}{3} & G(t) \leq 4 \\ \frac{25}{3}(G(t) - 3) & G(t) \in [4, 8] \\ \frac{125}{3} & G(t) \geq 8 \end{cases} \quad g(t) = \begin{cases} \frac{t}{60} & t \leq 30 \\ \frac{120-t}{180} & t \in [30, 120] \\ 0 & t \geq 120 \end{cases}.$$

The variable  $G$  characterizes the plasma glucose concentration,  $X$  the insulin concentration in the remote compartment, while  $I$  is the free plasma insulin concentration. The constants  $G_B$  and  $I_B$  represent the basal reference values of plasma glucose and insulin, respectively, while  $i(t)$  and  $g(t)$  describe the infusion evolution of glucose and insulin into the bloodstream of the patient.

First of all, we divided the space into nine different sectors, according to the combination between the different evolutions of the functions  $g(t)$  and  $i(t)$ . Since the phases of  $g(t)$  directly depend on time, we added a further variable to our model: the time variable  $T$  that measures the time since the beginning of the simulation. We approximate the differential equations with the corresponding first-degree Taylor polynomials. The resultant hybrid automaton is depicted in Figure 7, where all the activations are satisfied when the variables  $G$  and  $T$  assume the values that lie on the dashed straight lines, while the resets are simply identity functions.

We may want to test whether the glucose concentration does not grow too fast. Such a behaviour can be verified by testing that the half-space above a given line is not reachable: the higher the slope of the line, the greater the growth of the glucose concentration. We chose the half-space  $6 * (t + 105) \leq 135G$  and we checked that this region is not reachable from  $G \in [-2, 2] \wedge X = 0 \wedge I \in [-0.1, 0.1]$ . Such verification was performed exploiting both the  $\epsilon$ -semantics presented in Section 4. Sphere semantics was used as parameter of Algorithm 1 in order to obtain a halting criterion that, also in this case, takes into account natural noise. Then, we evaluated the formula returned by the algorithm in DE semantics, with the purpose of considering

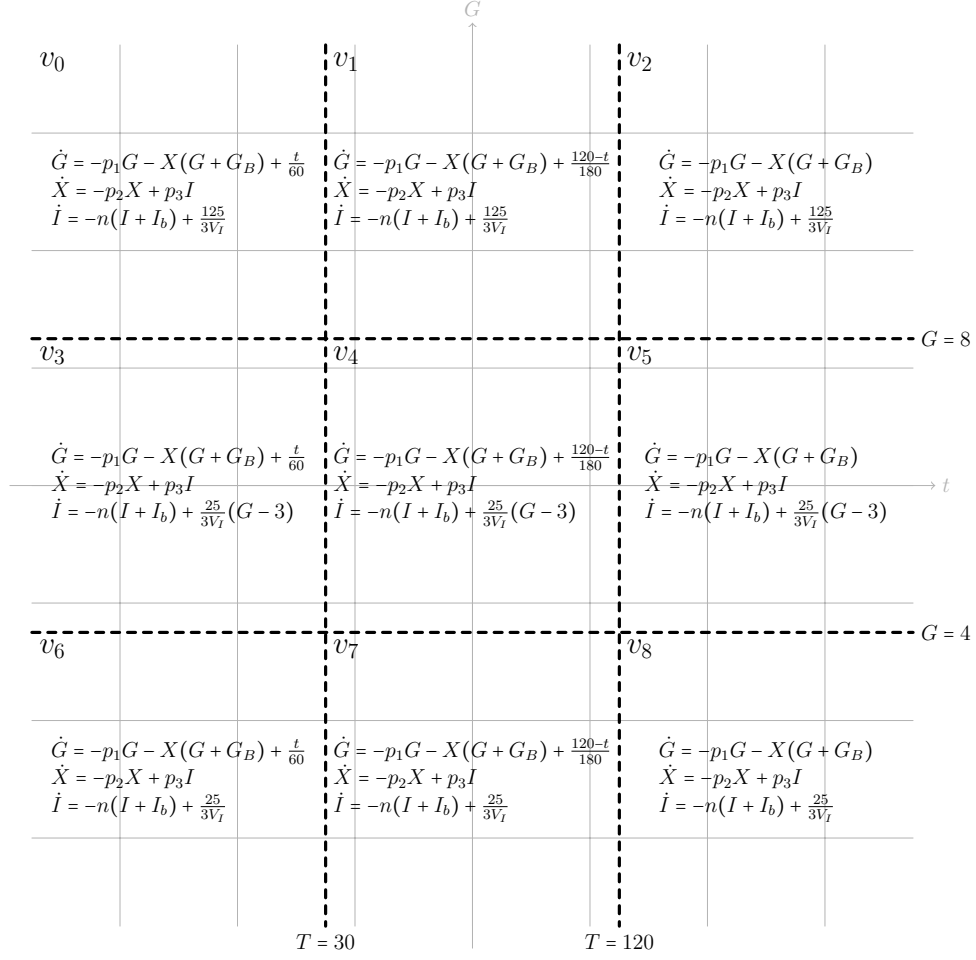


Figure 7: A graphical representation of the glycemic control hybrid automaton.



only states that are *robustly* reachable. This means that we allow the system to be above the half-space, but only for an  $\epsilon$ .

Notice that, by passing DE semantics to Algorithm 1, the result of the computation would have been the empty set. This is due to the fact that activation formulæ characterize lines which cannot include spheres.

## 7. Conclusions

This work describes a new reachability algorithm based on  $\epsilon$ -semantics which enables us to analyze any hybrid automaton in Michael’s form. It introduces two  $\epsilon$ -semantics whose evaluations can be reduced to the decidability of first-order formulæ, and, finally, it shows how to simplify such formulæ. Two biological applications are considered to show the effectiveness of the approach: a neural oscillator whose components derive from the approximation of the continuous model presented in [20], and a glyceimic control in diabetic patients based on the continuous model provided in [24].

In the neural oscillator, our analysis reveals that any point which begins its evolution from a distance of at least  $2\epsilon$  from the limit cycle, converges to a flow tube which has a diameter of  $2\epsilon$  and that includes the limit cycle. The use of linear dynamics together with formula simplifications and local reformulation of the analyzed property allowed us to efficiently investigate the system.

In the study of the glyceimic control we verified the low grow of glucose concentration combining two different  $\epsilon$ -semantics. In particular, sphere semantics was exploited in the reachability computation to introduce noise, while DE semantics ensured that we considered only robust behaviours.

Among all the works concerning approximation techniques over hybrid automata, the closest to our approach are [13, 25, 26]. Fränzle in [13] presents a model of noise over hybrid automata. The introduction of noise ensures in many cases the (semi-)decidability of the reachability problem. Another result of (semi-)decidability always based on the concept of perturbation and concerning the safety verification of hybrid systems is given by Ratschan in [25]. Furthermore,  $\epsilon$ -(bi)simulation [26] relations, which are essentially relaxations on the infinite precision required by simulation and bisimulation, represent tools able to remove complexity and undecidability issues related to the analysis of the investigated model. Some more comparisons can be found in [27].

In the examples that we considered, some natural behaviours, which are not captured by standard semantics, emerged by using  $\epsilon$ -semantics. On the other hand, we still lack a general method to prove that  $\epsilon$ -semantics do not neglect essential behaviours. To this aim, as future work, we are interested in deeper analyzing the relationship between standard and  $\epsilon$ -semantics when  $\epsilon$  tends to 0.

As far as the examples are concerned, we plan to analyze the behaviour of a group of neural oscillators by combining several hybrid automata. Moreover, it is in our interest to extend the study of the glycemic control to the computation of the whole reachability set, eventually defining new  $\epsilon$ -semantics and formulæ simplifications to make the computation of the reachability set more efficient.

## References

- [1] T. A. Henzinger, P. W. Kopke, A. Puri, P. Varaiya, What's decidable about hybrid automata?, in: Proc. of ACM Symposium on Theory of Computing (STOCS'95), 1995, pp. 373–382.
- [2] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, O. Maler, SpaceEx: Scalable Verification of Hybrid Systems, in: Proc. 23rd International Conference on Computer Aided Verification (CAV), Lecture Notes in Computer Science, Springer, 2011, pp. 379–395.
- [3] A. Platzer, Logical Analysis of Hybrid Systems - Proving Theorems for Complex Dynamics, Springer, 2010.
- [4] S. Sankaranarayanan, T. Dang, F. Ivančić, Symbolic model checking of hybrid systems using template polyhedra, in: Proc. of 14th Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 08), Vol. 4963 of Lecture Notes in Computer Science, springer, 2008, pp. 188–202.
- [5] A. Casagrade, C. Piazza, A. Policriti, Discrete semantics for hybrid automata. avoiding misleading assumptions in systems biology., Discrete Event Dynamic Systems 19 (4) (2009) 471–493.
- [6] G. E. Collins, Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition, in: Proc. of the

2nd GI Conference on Automata Theory and Formal Languages, Vol. 33 of Lecture Notes in Computer Science, Springer, 1975, pp. 134–183.

- [7] H. B. Enderton, A Mathematical Introduction to Logic, ii Edition, Harcourt/Academic Press, 2001.
- [8] E. Mendelson, Introduction to Mathematical Logic, iv Edition, CRC Press, 1997.
- [9] B. Mendelson, Introduction to Topology: Third Edition, Dover Books on Mathematics, 1990.
- [10] G. Lafferriere, G. J. Pappas, S. Yovine, Symbolic Reachability Computation for Families of Linear Vector Fields, J. Symb. Comp. 32 (3) (2001) 231–253.
- [11] G. Lafferriere, G. J. Pappas, S. Sastry, O-minimal hybrid systems, Mathematics of Control, Signals, and Systems 13 (2000) 1–21.
- [12] A. Casagrande, C. Piazza, A. Policriti, B. Mishra, Inclusion dynamics hybrid automata, Inform. and Comput. 206 (12) (2008) 1394–1424.
- [13] M. Fränzle, Analysis of hybrid systems: An ounce of realism can save an infinity of states, in: J. Flum, M. Rodríguez-Artalejo (Eds.), Computer, Science, and Logic (CSL 99), Vol. 1683 of Lecture Notes in Computer Science, Springer, 1999, pp. 126–140.
- [14] A. Casagrande, T. Dreossi, C. Piazza, Hybrid automata and  $\epsilon$ -analysis on a neural oscillator, in: Proc. of the 1st International Workshop on Hybrid Systems and Biology (HSB 2012), Vol. 92 of EPTCS, 2012, pp. 58–72.
- [15] W. J. Freeman, C. A. Skarda, Spatial EEG patterns, non-linear dynamics and perception: the neo-Sherringtonian view., Brain Res 357 (3) (1985) 147–175.
- [16] R. D. Traub, R. Miles, Neuronal Networks of the Hippocampus, Cambridge University Press, New York, NY, USA, 1991.
- [17] M. Steriade, R. R. Llinás, The functional states of the thalamus and the associated neuronal interplay., Physiological reviews 68 (3) (1988) 649–742.

- [18] L. R. Silva, Y. Amitai, B. W. Connors, Intrinsic oscillations of neocortex generated by layer 5 pyramidal neurons., *Science* 251 (4992) (1991) 432–5.
- [19] C. M. Gray, P. Konig, A. K. Engel, W. Singer, Oscillatory responses in cat visual cortex exhibit inter-columnar synchronization which reflects global stimulus properties, *Nature* 338 (6213) (1989) 334–337.
- [20] A. Tonnelier, S. Meignen, H. Bosch, J. Demongeot, Synchronization and desynchronization of neural oscillators, *Neural Networks* 12 (9) (1999) 1213 – 1228.
- [21] A. F. Atiya, P. Baldi, Oscillations and synchronizations in neural networks: an exploration of the labeling hypothesis, *Int. J. Neural Syst.* 1 (2) (1989) 103–124.
- [22] A. Casagrande, T. Dreossi, **pyHybridAnalysis**: a Package for  $\epsilon$ -Semantics Analysis of Hybrid Systems, in: *Proc. of the 16th Euromicro Conference on Digital System Design (DSD 2013)*, IEEE Computer Society Press, 2013, pp. 815–818.
- [23] A. Dolzmann, T. Sturm, REDLOG: computer algebra meets computer logic, *SIGSAM Bull.* 31 (2) (1997) 2–9.
- [24] S. M. Furler, E. W. Kraegen, R. H. Smallwood, D. J. Chisholm, et al., Blood glucose control by intermittent loop closure in the basal mode: computer simulation studies with a diabetic model, *Diabetes care* 8 (6) (1985) 553–561.
- [25] S. Ratschan, Safety verification of non-linear hybrid systems is quasi-semidecidable, in: *Proc. 7th Annual Conference of Theory and Applications of Models of Computation (TAMC 2010)*, Vol. 6108 of *Lecture Notes in Computer Science*, springer, 2010, pp. 397–408.
- [26] A. Girard, G. J. Pappas, Approximation metrics for discrete and continuous systems, *IEEE Trans. Automat. Control* 52 (5) (2007) 782–798.
- [27] A. Casagrande, C. Piazza, Model checking on hybrid automata, in: *Proc. of the 15th Euromicro Conference on Digital System Design (DSD 2012)*, IEEE Computer Society Press, 2012, pp. 493–500.