Inclusion Dynamics Hybrid Automata ⋆

Alberto Casagrande [a,b,c] Carla Piazza [a,*] Alberto Policriti [a,c]
Bud Mishra [d,e]

[a] *DIMI, Università di Udine, Via delle Scienze, 206, 33100 Udine, Italy*
[b] *DISA, Università di Udine, Via delle Scienze, 208, 33100 Udine, Italy*
[c] *Istituto di Genomica Applicata, Via J.Linussio, 51, 33100 Udine, Italy*
[d] *Courant Institute of Mathematical Science, NYU, New York, U.S.A.*
[e] *NYU School of Medicine, 550 First Avenue, New York, 10016 U.S.A.*

Abstract

Hybrid systems are dynamical systems with the ability to describe mixed discrete-continuous evolution of a wide range of systems. Consequently, at first glance, hybrid systems appear powerful but recalcitrant, neither yielding to analysis and reasoning through a purely continuous-time modeling as with systems of differential equations, nor open to inferential processes commonly used for discrete state-transition systems such as finite state automata. A convenient and popular model, called hybrid automata, was introduced to model them and has spurred much interest on its tractability as a tool for inference and model checking in a general setting. Intuitively, a hybrid automaton is simply a "finite-state" automaton with each state augmented by continuous variables, which evolve according to a set of well-defined continuous laws, each specified separately for each state. This article investigates both the notion of hybrid automaton and the model checking problem over such structure. In particular, it relates first-order theories and analysis results on multivalued maps and reduces the bounded reachability problem for hybrid automata whose continuous laws are expressed by inclusions ($x' \in f(x,t)$) to a decidability problem for first-order formulæ over the reals. Furthermore, the paper introduces a class of hybrid automata for which the reachability problem can be decided and shows that the problem of deciding whether a hybrid automaton belongs to this class can be again decided using first-order formulæ over the reals. Despite the fact that the bisimulation quotient for this class of hybrid automata can be infinite, we show that our techniques permit effective model checking for a nontrivial fragment of CTL.

Key words: Hybrid Automata; First-order Logics over the Reals; Model Checking

1 Introduction

Over the last century, we have come to accept a discrete description of nature in a quantum mechanical framework, where system configurations are in terms of superpositions of discrete states. Nonetheless, in the meso- or macroscopic world, we still revert to the classical laws of nature, described in terms of continuous dynamics of continuous variables. For instance, Newton's equation of gravitation, Maxwell's laws of electromagnetic theory, or kinetic theories based on statistical mechanics, etc. all describe the macroscopic nature quite faithfully, albeit approximately, through differential equations describing continuous evolution over real domains. In contrast, many natural and engineered systems possessing memory (e.g., digital circuits, or gene regulatory networks), are best described in terms of discrete state-transition systems, where the system moves from one configuration to a non-neighboring configuration in an infinitesimally small amount time, while resting in a small neighborhood of a quasi-stable configuration between any two consecutive transitions. In principle, such discrete-state models can be described by a suitably formulated continuous system, but then such a system would suffer from unacceptable intractability. In reality, however, nature often refuses to follow this dichotomy neatly; unfortunately for the mathematical modelers, there do exist many interesting systems that can be best described in a mixed discrete-continuous formalism, which can neither be characterized properly using a completely discrete model nor a purely continuous model. Such systems consist of a discrete program within a continuously changing environment and are dubbed hybrid systems because of this underlying hybrid nature of the dynamics.

In order to model hybrid systems, Alur et al. introduced in [1] the notion of *hybrid automata*. Intuitively a hybrid automaton is a "finite-state" automaton [2] with continuous variables which evolve according to a set of continuous laws, called *dynamics*, characterizing each discrete *location*. The continuous evolution of the hybrid automaton is ruled in each location by exactly one dynamic and the dynamic may change from location to location. Moreover, each location is characterized by a set of continuous values, called *invariant*, which defines the allowed continuous part of the state. Each of the hybrid automaton's states must maintain its continuous part inside (satisfying) the invariant. Finally, each of the edges, e, of the hybrid automaton is labeled by a pair consisting of a set of continuous states and a map R_e, referred to as *activation* and *reset*, respectively. The automaton can cross an edge only if

⋆ This work is partially done in the framework of the HYCON Network of Excellence, and supported by NSF's ITR programs, DARPA's BioCOMP/Biospice program, NYU CCPR/DHS program, PRIN'05 program 2005015491, PRIN "BISCA" 2006011235, and regional project BIOCHECK.

* Corresponding author.
Email address: carla.piazza@dimi.uniud.it (Carla Piazza).

the continuous part p of its state enters into the edge's activation region and after crossing an edge the continuous part of the automaton state is set to the value $R_e(p)$. We present a formal definition of hybrid automaton in Section 3. A simple example of hybrid automaton representing a thermostat is depicted in Figure 1. In particular, the modeled thermostat controls a heater and it switches the heater either on, if the temperature is lower than 15° Celsius, or off, if the temperature is higher than or equal to 20° Celsius.

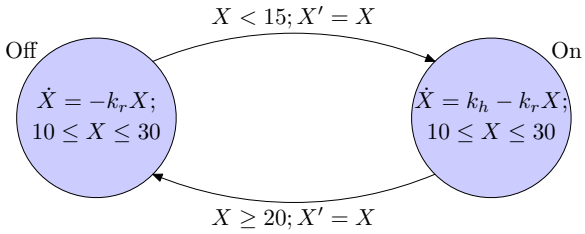


Figure 1. A simple thermostat.

Traditionally, hybrid automaton dynamics are specified by either differential equations or inclusions [1,3]: given a differential formula, its solutions are the hybrid automaton's corresponding dynamics. For instance, if the dynamic in a location is represented by the differential equation $\dot{x} = \mathcal{F}(x,t)$ and $f(x,t)$ is solution of such differential equation, then $x' = f(x,t)$ is the dynamic, i.e., x' can be reached from x after a t-timed continuous evolution. An alternative approach consists in defining the dynamics through a set of formulæ. These formulæ do not involve derivatives and explicitly constraint the hybrid automaton's evolution. This approach is studied in [4,5,6] where dynamics are expressed by formulæ of the form $x' = f(x,t)$. Specifying the dynamics by differential equation or inclusions has some advantages against a more explicit representation through formulæ. First of all, dynamics usually represent evolution ruled by natural laws and usually physical laws are described by differential equations. Hence, specifying dynamics by differential equations does not require any preprocessing in the hybrid automata definition. Moreover, not all differential equations have a computable solution, thus there exist dynamics which can be exactly specified by a differential equation, but not by a formula. Finally, since the solutions of any Cauchy problem are continuous, specifying dynamics by differential equations guarantees the continuity of the dynamics themselves. However, this way of defining dynamics has some drawbacks too. In particular, by specifying dynamics by formulæ, we run the risk of defining dynamics which may not be differentiable, while in contrast, if we are defining dynamics by differential equations, this problem is automatically ruled out. Moreover, as already noted, since not all differential equations have a computable solution, when dynamics are specified by differential equations, it may result in models whose dynamics cannot be evaluated exactly. These two approaches, namely, specifying dynamics via formulæ versus doing so via differential equations, have different implications from a computational

viewpoint: in the first case, using formulæ enables one to exploit quantifier elimination and decidability results over first-order logic to directly evaluate reachability (of one state from a given initial state); however, in the later case, i.e., when using differential equations to define dynamics, one first needs some preprocessing to compute the dynamics themselves whenever it is possible.

Using hybrid automata, we can study hybrid systems and verify properties over them. In particular, several techniques have been proposed to verify properties expressed in some kind of temporal logic, such as CTL* or TCTL, over hybrid automata, e.g., see [7,1,8,9,10]. These techniques are mainly based on finite state model checking approaches and exploit equivalence reductions (i.e., simulation or bisimulation) [11,12,13] to reduce the number of system's states. In particular, if a hybrid automaton has either a finite simulation quotient or a finite bisimulation quotient, then the property can be verified on the reduced model through standard model checking algorithms. Since simulation preserves LTL and bisimulation preserves CTL*, if the property holds on the reduced model, then it also holds on the original hybrid automaton. During the last few years, many such techniques had been successfully used to verify specifications of communication protocols and controllers [14,15,16,17]. More recently there have also been several successful applications and consequently a growing interest in their use in analyzing biological systems [18,19,20,21].

An interesting verification problem is the one involving safety condition which requires checking whether a certain property φ, describing all safe situations, never fails during the hybrid automaton's evolution. Such problem can be naturally reduced to a *reachability* problem over hybrid automata. As a matter of fact, to prove that a certain property φ is true during the entire evolution of a hybrid automaton H, we only need to prove that all the states in which φ is false are not reachable by H. Unfortunately, it has been proven in [22] that the *halting problem* for Turing machines can be reduced to a reachability problem for a particular class of hybrid automata. Hence, the reachability problem is not decidable in general. However, there have been proposed many non-trivial (or non-degenerate) classes of hybrid automata for which either reachability problem or (more generally) temporal logic verification is decidable. In [9] Alur et al. introduced *multirate automata* as an extensions of *timed automata* [23]. Such hybrid automata are characterized by resets which are either identity or constant function zero. Moreover, their continuous variables evolve like clocks with rational rates (i.e., x becomes $c \cdot t + x$, where $c \in \mathbb{Q}$, in time t). In the same work it has been proven that the reachability problem over multirate automata is not decidable in general. However, by imposing a restriction on dynamics called *simplicity condition*, decidability for reachability problem and finite bisimulation are shown to be achievable. Puri and Varaiya in [3] introduced *rectangular hybrid automata* whose dynamics can be characterized by a differential inclusion of the type $\dot{x} \in [l, u]$, where l and u are rational numbers. Even if Kopke had proved in [24] that reachability is in general undecidable

for such classes of hybrid automata and that three dimensional rectangular automata have infinite simulation quotient, they showed that, under a condition called *initialized condition*, reachability can be decided. Finally, Lafferriere, Pappas and Sastry introduced *o-minimal hybrid automata* in [25]. Such classes of hybrid automata guarantee finite bisimulation quotient, provided that a constant reset condition is imposed on all of automaton's edges.

This article aims at studying hybrid automata whose dynamics are *inclusion dynamics* defined by formulæ. We model hybrid automata having dynamics of the type $x' \in f(x,t)$ and we reduce model checking problems over them to decidability problems over first-order formulæ. Since in this theory $f(x,t)$ need not be differentiable, such kind of dynamics generalizes dynamics defined by differential inclusions. We show that imposing continuity on $f(x,t)$ with respect to t does not suffice to guarantee the existence of a proper continuous evolution satisfying the dynamics. As a consequence, we propose a set of stronger conditions, which relies not only on the existence of such evolution, but also on the decidability of satisfiability problem for certain first-order formulæ, as described below. Since such results can be achieved using a Michael's selection theorem [26], if a hybrid automaton satisfies such conditions, it is said to be in *Michael's form*. Exploiting Michael's form, we present a class of hybrid automata for which reachability problems can be reduced to a decidability problem for first-order formulæ. We show that even if its bisimulation quotient is infinite and the finiteness of its simulation quotient is still an open problem, model checking over a CTL sub-logic (not preserved under simulation) can be reduced to a decidability problem for first-order formulæ too. We demonstrate that our decidability results cannot be achieved exploiting standard equivalence reduction techniques such as simulation and bisimulation. Finally, using similar techniques, we prove that the membership problem of deciding whether a hybrid automaton belongs to this decidable class of automata, is also decidable, because it can be reduced to the earlier class of decidability problems for model checking of hybrid automata. The class of automata we study in this article is a generalization of o-minimal hybrid automata, since from each point we can have an infinite number of continuous trajectories. This approach allows one to model situations in which the dynamics are not exactly known, e.g., some parameters are missing, as in the case with many models of biochemical pathways. Here, we focus only on the computability of the reductions from temporal formula to the associated first-order formula, without placing any particular emphasis on their computational complexity. That is to say, we make no effort at presenting the most efficient reductions, but merely prove that such reductions can be computed in an effective manner.

More specifically, the article is organized as follows:

Section 2 reviews the notion of first-order theory, describes some important theories over real numbers, and presents some decidability results over them.

Section 3 introduces the formal definition of hybrid automata.

Section 4 shows that not all hybrid automata whose dynamics are continuous have a continuous evolution. Moreover, it proposes a set of conditions, called *Michael's form*, which lets us reduce the problem of verifying the existence of such evolution to a decidability problem over first-order formulæ and next it shows how such conditions can be tested. Finally, it gives an effective reduction from reachability problems over hybrid automata in Michael's form to decidability problems for first-order formulæ under the assumption of a finite number of discrete transitions over locations.

Section 5 introduces a class of hybrid automata, called *FOCoRe*, which are in Michael's form and whose resets are restricted to constant maps. It shows that every FOCoRe's evolution can be reduced to a canonical form comprising FOCoRe's evolution whose number of discrete transitions is bounded by the number of automaton's discrete edges and, hence, that the reachability problem can be decided. Moreover, it proves that FOCoRe automata have infinite bisimulation quotient in general, and yet model checking over a particular CTL sub-logic, called $\Phi_{\mathcal{P}}$, is still decidable.

Section 6 sketches a complex biological that can be modeled by using the proposed methods.

Section 7 ends the article with some comments, some practical applications, and some open problems and future works that remain to be addressed.

Part of the material presented in this paper appeared in [27,28].

2 Theories and Decidability

In this section, we review the notion of first-order theory, we describe some interesting theories and we introduce some decidability results over them. For a more detailed treatment of these notions, the reader may refer to [29,30].

2.1 Languages, Theories, and Models

A *first-order language* $\mathcal{L}$ is a tuple $\mathcal{L} = \langle \mathit{Var}, \mathit{Const}, \mathit{Funct}, \mathit{Rel}, \mathrm{Ar} \rangle$, where *Var* is a set of variables, *Const* is a set of constant values, *Funct* is a set of functional operators, *Rel* is a set of relational symbols, and the "arity" function $\mathrm{Ar} : \mathit{Funct} \cup \mathit{Rel} \to (\mathbb{N} \setminus \{0\})$ associates to each element of *Funct* and *Rel* the number of arguments it takes.

A *term* of $\mathcal{L}$ can be defined as:

$$\mathit{term} ::= X \mid c \mid \mathbf{f}(\mathit{term}_1, \ldots, \mathit{term}_{\mathrm{Ar}(\mathbf{f})})$$

where X is a variable in *Var*, c is a constant in *Const*, and $\mathbf{f}$ is a function in *Funct*.

An *atomic formula* φ_{a} of $\mathcal{L}$ has the form $\top$ or $\bot$ (standing for *true* and *false*, respectively) or $\mathbf{R}(term_1, \ldots, term_{\mathrm{Ar}(\mathbf{R})})$, where $\mathbf{R}$ is a relational operator in *Rel* and $term_i$ is a term of $\mathcal{L}$ for all $i \in [1, \mathrm{Ar}(\mathbf{R})]$. Moreover, a *formula* φ of $\mathcal{L}$ is defined as follows:

$$\varphi ::= \varphi_{\mathrm{a}} \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi_1 \mid \forall X\, \varphi_1$$

where φ_{a} is an atomic formula of $\mathcal{L}$, X is a variable in *Var*, and φ_i is a formula of $\mathcal{L}$ for all $i \in \{1, 2\}$. We define $\varphi_1 \wedge \varphi_2$ as a short hand for $\neg(\neg\varphi_1 \vee \neg\varphi_2)$, $\varphi_1 \multimap \varphi_2$ as a short hand for $(\neg\varphi_1) \vee \varphi_2$, and $\exists X\, \varphi_1$ as a short hand for $\neg\forall X\, \neg\varphi_1$. The two symbols $\exists$ and $\forall$ are called *quantifiers*.

An occurrence of a variable $X \in Var$ is *bound* or *quantified* in a formula φ, if it occurs in a φ's sub-formula of the kind either $\forall X\, \bar{\varphi}$ or $\exists X\, \bar{\varphi}$. An occurrence of a variable is *free* if it is not bound. Modulo renaming we can safely assume that the variables which occur bound in a formula do not occur free, and vice versa. A *sentence* is a formula such that all the variable occurrences are bound. The set of free variables occurring in the first-order formula φ is denoted by $Free(\varphi)$. We will use the notation $\varphi[X_1, \ldots, X_m]$ ($\varphi[X]$, where $X = (X_1, \ldots, X_m)$) to stress the fact that $Free(\varphi)$ includes the set of variables $\{X_1, \ldots, X_m\}$ (the set of components of the vector X, respectively).

A *model* of a language $\mathcal{L}$ is tuple $\mathcal{M} = \langle M, \mathtt{Const}, \mathtt{Funct}, \mathtt{Rel}\rangle$ where:

- M is a nonempty set called *support*;
- $\mathtt{Const} : Const \to C \subseteq M$ is an interpretation for (the elements of) *Const*;
- $\mathtt{Funct} : Funct \to \bigcup_{k=1}^{\infty} \left(\prod_{i=1}^{k} M \to M\right)$, with $\mathtt{Funct}\,(\mathbf{f}) : \prod_{i=1}^{\mathrm{Ar}(\mathbf{f})} M \to M$, is an interpretation for (the elements of) *Funct*;
- $\mathtt{Rel} : Rel \to \bigcup_{k=1}^{\infty} \left(\prod_{i=1}^{k} M \to \{\top, \bot\}\right)$, with $\mathtt{Rel}\,(\mathbf{R}) : \prod_{i=1}^{\mathrm{Ar}(\mathbf{R})} M \to \{\top, \bot\}$, is an interpretation for (the elements of) *Rel*;

Let $\mathcal{M}$ be a model of $\mathcal{L}$ with support M, $\varphi[X_1, \ldots, X_i, \ldots, X_m]$ be a formula of $\mathcal{L}$, and $p \in M$. The expression obtained by replacing X_i by p is denoted by $\varphi[X_1, \ldots, X_{i-1}, p, X_{i+1}, \ldots, X_n]$ and, strictly speaking, is to be intended as obtained after adding a new constant c_p to the language. With a slight abuse of notation we will use formulæ to also denote these expressions.

The semantics of $\mathcal{L}$-formulæ with respect to a model $\mathcal{M}$ is defined in the standard way (see [29,30]). In particular, we say that a formula $\varphi_a[p_1, \ldots, p_m]$, where φ_a is atomic, holds in $\mathcal{M}$ if applying the interpretations of the constant, functional, and relational operators we obtain the truth value $\top$. The formula $\varphi_1[p_1, \ldots, p_m] \vee \varphi_2[p_1, \ldots, p_m]$ holds in $\mathcal{M}$ if either the first or the second disjunct holds in $\mathcal{M}$. The formula $\neg\varphi_1[p_1, \ldots, p_m]$ holds in $\mathcal{M}$ if $\varphi_1[p_1, \ldots, p_m]$

does not. The formula $\forall X\, \varphi_1[X, p_1, \ldots, p_m]$ holds in $\mathcal{M}$ if for each $p \in M$ the formula $\varphi_1[p, p_1, \ldots, p_m]$ holds. We say that a formula $\varphi[X_1, \ldots, X_m]$ in $\mathcal{L}$ is *satisfiable* in $\mathcal{M}$ if there exist $p_1, \ldots, p_m \in M$ such that $\varphi[p_1, \ldots, p_m]$ holds in $\mathcal{M}$. Moreover, we say that $\varphi[X_1, \ldots, X_m]$ is *valid* if $\varphi[p_1, \ldots, p_m]$ holds in $\mathcal{M}$ for all $p_1, \ldots, p_m \in M$. When the model $\mathcal{M}$ is clear from the context we will simply say that a formula holds (is satisfiable or is valid, respectively).

When we speak of models over M, where M is a nonempty set, we are referring to those models whose support is M. Besides, when $\mathtt{Const} : \mathit{Const} \to C$ is clear from the context, we use $\langle M, C, \mathtt{Funct}, \mathtt{Rel}\rangle$ to mean $\langle M, \mathtt{Const}, \mathtt{Funct}, \mathtt{Rel}\rangle$.

Example 1 *Consider the language* $\mathcal{L}_R \stackrel{\text{def}}{=} \langle \mathit{Var}, \mathbb{Z}, \{+, *\}, \{\geq\}, \mathit{Ar}\rangle$. *A model for the language* $\mathcal{L}_R$ *is the tuple* $\langle \mathbb{R}, \mathbb{Z}, \mathtt{Funct}, \mathtt{Rel}\rangle$ *where* Funct *and* Rel *are the usual interpretations for* $\{+, *\}$ *and* $\{\geq\}$*, respectively and we have a constant for each element in* $\mathbb{Z}$.

Notice that such a model can be "simplified" to $\mathcal{M}_0 \stackrel{\text{def}}{=} \langle \mathbb{R}, \{0, 1\}, \mathtt{Funct}, \mathtt{Rel}\rangle$, *in the sense that for each formula* φ_R *in the language* $\mathcal{L}_R$ *there exists a formula* φ_0 *in the language* $\mathcal{L}_0 \stackrel{\text{def}}{=} \langle \mathit{Var}, \{0, 1\}, \{+, *\}, \{\geq\}, \mathit{Ar}\rangle$ *such that* φ_R *is satisfiable in* $\mathcal{M}_R \stackrel{\text{def}}{=} \langle \mathbb{R}, \mathbb{Z}, \mathtt{Funct}, \mathtt{Rel}\rangle$ *if and only if* φ_0 *is satisfiable in* $\mathcal{M}_0 \stackrel{\text{def}}{=} \langle \mathbb{R}, \{0, 1\}, \mathtt{Funct}, \mathtt{Rel}\rangle$.

Given a set Γ of sentences and a sentence φ, we say that φ is a *logical consequence* of Γ (denoted, $\Gamma \models \varphi$) if for each model $\mathcal{M}$ it holds that if each formula of Γ is valid in $\mathcal{M}$ ($\mathcal{M} \models \Gamma$), then φ is valid in $\mathcal{M}$. As a consequence of completeness of first-order logic, we may equivalently say that φ is provable from Γ (see [29,30]). A *theory* $\mathcal{T}$ is a set of sentences such that if $\mathcal{T} \models \varphi$, then $\varphi \in \mathcal{T}$. Given a language $\mathcal{L}$ and a model $\mathcal{M}$ the *complete theory* $\mathcal{T}(\mathcal{M})$ of $\mathcal{M}$, is the set of all the sentences of $\mathcal{L}$ which are valid in $\mathcal{M}$. Given a model $\langle M, C, \mathtt{Funct}, \mathtt{Rel}\rangle$, we also indicate its complete theory by either $\langle M, C, \mathtt{Funct}, \mathtt{Rel}\rangle$ or $\langle M, C, f_0, \ldots, f_n, r_0, \ldots r_m\rangle$, where $\mathtt{Funct} = \{f_0, \ldots, f_n\}$ and $\mathtt{Rel} = \{r_0, \ldots, r_m\}$. Notice that for each model $\mathcal{M}$ it holds that for each sentence φ, either $\varphi \in \mathcal{T}(\mathcal{M})$ or $\neg\varphi \in \mathcal{T}(\mathcal{M})$. Two formulæ $\varphi_1[X]$ and $\varphi_2[Y]$, where X and Y are two vectors of variables, are equivalent with respect to a theory $\mathcal{T}$ if it holds that $\mathcal{T} \models \forall X, Y(\varphi_1[X] \leftrightarrow \varphi_2[Y])$. We say that a theory $\mathcal{T}$ admits the so-called *elimination of quantifiers*, if, for any formula φ, there exists a quantifier free formula ϱ such that φ is equivalent to ϱ with respect to $\mathcal{T}$. If there exists an algorithm for deciding whether a sentence φ belongs to $\mathcal{T}$ or not, we say that $\mathcal{T}$ is *decidable*. Notice that given a model $\mathcal{M}$, its complete theory $\mathcal{T}(\mathcal{M})$ is decidable if and only if both the satisfiability and the validity of formulæ in $\mathcal{M}$ are decidable.

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

In the rest of this paper we will only refer to theories of the form $\mathcal{T}(\mathcal{M})$ for some model $\mathcal{M}$.

2.2 O-Minimal Theories

An interesting class of theories is the class of *o-minimal theories* [31,32]. Given a language $\mathcal{L}$ and a model $\mathcal{M}$ of $\mathcal{L}$ with support M we say that a set $S \subseteq M^k$ is *definable* if and only if there exists a formula $\varphi[X_1, \ldots, X_k]$ such that $\varphi[p_1, \ldots, p_k]$ holds in $\mathcal{M}$ if and only if $(p_1, \ldots, p_k) \in S$.

Definition 3 (O-Minimal Theory) *Let $\mathcal{L}$ be a first-order language whose set of relational symbols includes a binary symbol $\leq$ and let $\mathcal{M}$ be a model of $\mathcal{L}$ in which $\leq$ is interpreted as a linear order. The theory $\mathcal{T}(\mathcal{M})$ is* order minimal*, or simply* o-minimal*, if every set definable in $\mathcal{T}(\mathcal{M})$ is a finite union of points and intervals (with respect to $\leq$).*

The class of o-minimal theories includes many interesting theories over $\mathbb{R}$. Below we recall a few of them.

The theory $\mathbb{R} = \langle \mathbb{R}, 0, 1, +, *, \geq \rangle$ is called *semi-algebraic theory*. In [33], Tarski showed that such theory admits elimination of quantifiers and that it is decidable. Unfortunately, Tarski's algorithm has a computational complexity, which could not even be expressed as a bounded tower of exponents of the input size. In [34] Collins presented an algorithm, called *Cylindrical Algebraic Decomposition* (CAD), to decide the satisfiability of a formula φ of $\mathcal{L}_R$. Later Hoon Hong, using many useful and practical heuristics, created the first practical quantifier elimination software `Qepcad`. Alternative CAD-based methods that are doubly exponential in the number of quantifier alternations rather than the number of variables, have been proposed by Grigorév [35,36] and Renegar [37,38,39]. New quantifier elimination approaches have been proposed by Basu, Pollack, and Roy in [40,41,42]. The total time complexity (bit-complexity) [43,44] of the semi-algebraic decision procedures, mentioned above, are summarized in Table 1, under the hypothesis that the coefficients of the polynomials can be stored with at most B bits and that the input formulæ have the form:

$$(Q_1 X^{[1]})(Q_2 X^{[2]}) \ldots (Q_l X^{[l]})(\varphi[X^{[1]}, \ldots, X^{[l]}])$$

where $Q_i \in \{\forall, \exists\}$ and $Q_j \neq Q_{j+1}$, $X^{[i]}$ is a partition of all the variables in φ, with $|X^{[i]}| = n_i$, and φ is a quantifier-free formula with atomic formulæ consisting of m polynomials of equalities and inequalities of total degree d having the form

$$g_k(X^{[1]}, \ldots, X^{[l]}) \geq 0, \qquad k = 1, \ldots, m.$$

Type	Time Complexity	Source
General	$B^3(md)^{2^{O(\sum n_i)}}$	[34]
Existential	$B^{O(1)}(md)^{O(n^2)}$	[36]
General	$B^{O(1)}(md)^{\left(O(\sum n_i)\right)^{4*l-2}}$	[35]
Existential	$B^{1+o(1)}(m)^{(1+\sum n_i)}(d)^{O\left(\left(\sum n_i\right)^2\right)}$	[45,46]
General	$(B\log B\log\log B)(md)^{(2^{O(l)})\prod n_i}$	[37,38,39]
Existential	$(B\log B\log\log B)m(m/s)^s d^{O(\sum n_i)}$	[41,42]
General	$(B\log B\log\log B)(m)^{\prod(n_i+1)}d^{\prod O(n_i)}$	[41,42]

Table 1
Decision procedure complexity for $\langle\mathbb{R},0,1,+,*,\geq\rangle$.

Let *an* be the set of all the real-analytic functions from $[-1,1]^n$ to $\mathbb{R}$. Consider the theory $\mathbb{R}_{\text{an}}=\langle\mathbb{R},0,1,+,*,(f)_{f\in an},\geq\rangle$ obtained from $\langle\mathbb{R},0,1,+,*,\geq\rangle$ by adding all the functions in *an*. This theory can describe the behavior of some periodic trajectories such as sine and cosine functions in a bound interval. Van den Dries noticed in [47] that $\mathbb{R}_{\text{an}}$ is model complete. Hence, by Khovanskĭ's finiteness theorem (see [48]), $\mathbb{R}_{an}$ is also o-minimal. Moreover, Denef and Van den Dries gave in [49] a proof of model completeness and o-minimality of $\mathbb{R}_{\text{an}}$ using Weirstrass preparation theorem. Finally, in [50] it was shown that this theory admits the elimination of quantifiers after adding the function $1/x$ (with $1/0=0$).

Another interesting theory is $\mathbb{R}_{\text{exp}}=\langle\mathbb{R},0,1,+,*,e^x,\geq\rangle$ which is obtained by $(\mathbb{R},0,1,\ +,*,\geq)$ adding the exponential function e^x. Wilkie showed in [51] that this theory is model complete and, as a direct consequence of Khovanskĭ's results [48], it is also o-minimal. Moreover, in [32] van den Dries proved that an extension of $\langle\mathbb{R},0,1,+,*,\geq\rangle$ by a family of total real analytic functions admits the elimination of quantifiers if and only if such functions are semi-algebraic. Furthermore, Macintyre and Wilkie presented in [52] an algorithm to decide $\mathbb{R}_{\text{exp}}$ provided that Schanuel's conjecture (see [53,54]) holds.

In [55], Wilkie's method and Khovanskĭ's results are used to prove that the semi-algebraic theory extended by exponential operator and analytic functions, $\mathbb{R}_{\text{an,exp}}=\langle\mathbb{R},0,1,+,*,(f)_{f\in an},e^x,\geq\rangle$, is model complete and o-minimal. In [50], a different proof of these properties is given and it is proved also that the theory $\mathbb{R}_{\text{an,exp,log}}=\langle\mathbb{R},0,1,+,*,(f)_{f\in an},e^x,\log x,\geq\rangle$ admits the elimination of quantifiers. Recently, Lion and Rolin gave a geometric proof of $\mathbb{R}_{\text{an,exp}}$'s o-minimality and model completeness in [56]. Finally, in [57], Wilkie gave sufficient and necessary conditions for an extension of semi-algebraic theory by total C^∞ functions to be o-minimal. In particular, semi-algebraic theory extended by total C^∞ Pfaffian functions is o-minimal.

3 Hybrid Automata

The notion of *hybrid automata* was first introduced in [58,1] as a model and specification language for hybrid systems, i.e., systems consisting of a discrete program within a continuously changing environment. In the following subsections we introduce both syntax and semantics of such formalism.

3.1 Syntax

First, we introduce some notations and conventions. If $p = (p_1, \ldots, p_k)$ and $s = (s_1, \ldots, s_k)$ are vectors in $\mathbb{R}^k$, $r \in \mathbb{R}_{\geq 0}$, $\mp \in \{-, +\}$, and $\asymp \in \{\leq, <, =, >, \geq\}$, then we will use $p \mp s$ to denote the vector $(p_1 \mp s_1, \ldots, p_k \mp s_k)$ and $\|s\| \asymp r$ to indicate the relation $(s_1^2 + \ldots + s_k^2) \asymp r^2$. Indexed capital letter variables Z_m, Z'_m, and Z''_m, where $m \in \mathbb{N}$, denote variables ranging over $\mathbb{R}$, while Z, Z', and Z'' denote vectors of variables $(Z_1, \ldots, Z_k)$, $(Z'_1, \ldots, Z'_k)$, and $\left(Z''_1, \ldots, Z''_k\right)$, respectively. The temporal variables T, T', T_1, ...model time and range over $\mathbb{R}_{\geq 0}$. In the following, given a formula $\psi[Z]$ and a model $\mathcal{M}$, we will denote the set of tuple of values satisfying ψ in $\mathcal{M}$ as $Sat(\mathcal{M}, \psi)$, i.e., $Sat(\mathcal{M}, \psi) \stackrel{\text{def}}{=} \{p \mid \mathcal{M} \models \psi[p]\}$. When $\mathcal{M}$ is clear from the context we will simply write $Sat(\psi)$.

We are now ready to formally introduce hybrid automata. For each state of a discrete automaton we have an *invariant* condition and a dynamic law. This dynamic law may depend on the initial conditions, i.e., on the values of the continuous variables at the beginning of the evolution in the state. The jumps from one discrete state to another are regulated by the so-called *activation* and *reset* conditions.

Definition 4 (Hybrid Automaton) *Let $\mathcal{L}$ be a first-order language over the reals, $\mathcal{M}$ be a model of $\mathcal{L}$, and Inv, Dyn, Act and Reset be formulæ of $\mathcal{L}$. A* hybrid automaton *(of dimension k) $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Reset\rangle$ over $\mathcal{M}$, consists of the following components:*

(1) $Z = (Z_1, \ldots, Z_k)$ and $Z' = (Z'_1, \ldots, Z'_k)$ are two vectors of variables ranging over the reals;
(2) $\langle \mathcal{V}, \mathcal{E}\rangle$ is a finite directed graph; the vertexes of $\mathcal{V}$ are called locations*, or* control modes*, the directed edges in $\mathcal{E}$ are also called* control switches*;*
(3) Each $v \in \mathcal{V}$ is labeled by the two formulæ $Inv(v)[Z]$ and $Dyn(v)[Z, Z', T]$ such that if $Inv(v)[p]$ holds in $\mathcal{M}$, then $Dyn(v)[p, p, 0]$ holds as well;
(4) Each $e \in \mathcal{E}$ is labeled by the formulæ $Act(e)[Z]$ and $Reset(e)[Z, Z']$.

The formulæ $Inv(v)[Z]$ and $Dyn(v)[Z, Z', T]$ are said to be *invariant* of v

and *dynamics* of v, respectively, while $Act(e)[Z]$ and $Reset(e)[Z, Z']$ are called *activation* of e and *reset* of e, respectively. Moreover, if a reset does not depend on Z, then it is said to be a *constant reset*. The formula $Dyn(v)$ is said to be *time-invariant*, if for all $t \in R_{\geq 0}$ the following is true: $Dyn(v)[Z, Z', T]$ holds if and only if does $Dyn(v)[Z, Z', T + t]$.

From above formulæ, we can define the formula

$$\overline{Reset}(e)[Z] \stackrel{\text{def}}{=} \exists Z'\, Inv(v)[Z'] \wedge Act(e)[Z'] \wedge Reset(e)[Z', Z] \wedge Inv(u)[Z],$$

where $e = \langle v, u \rangle$.

In the rest of this paper, we write $\mathcal{I}(v)$, $\mathcal{A}(e)$, and $\mathcal{R}(e)$ to mean $Sat(Inv(v))$, $Sat(Act(e))$, and $Sat(\overline{Reset}(e))$, respectively.

A *class* of hybrid automata is a set of hybrid automata satisfying a specific set of properties. Such properties are said to be (defining) *properties of the class*. If there exists a first-order language $\mathcal{L}$ and a model $\mathcal{M}$ for it such that each property of a class $\mathcal{H}$ is characterizable by a formula of $\mathcal{L}$ which is in $\mathcal{T}(\mathcal{M})$ if and only if the property holds, then we say that $\mathcal{H}$ is *first-order definable by $\mathcal{L}$ and $\mathcal{M}$* or, simply, *first-order definable*. Analogously, a decision problem P is said to be first-order definable by $\mathcal{L}$ and $\mathcal{M}$ or first-order definable, if there exists an algorithm mapping each instance p of P into a formula ϕ_p of $\mathcal{L}$ such that $\phi_p \in \mathcal{T}(\mathcal{M})$ if and only if the answer to p is *true*.

In the preceding definition of hybrid automaton, we use the formulæ in *DynSet* to describe the continuous evolution without using temporal derivatives, thus avoiding the classical approach based on differential equations. Our approach is similar to the one followed in [6]. In [25], even though automata are defined with differential equations, it is necessary to compute their solutions in order to apply the bisimulation algorithm and express these solutions by $Dyn(v)[Z, Z', T]$, whose intuitive meaning is that from Z after T instants the continuous flow can reach Z'. Thus, our hybrid automata generalize several recently discovered notions in the hybrid systems theory. Note, as an example, that o-minimal hybrid automata [25,6] are a special case of our hybrid automata, since we do not impose restrictions on the formulæ and on the resets. Moreover, we admit an *infinite number of flows*, which can also be *self-intersecting*. Similarly, rectangular hybrid automata [3,59,24] can be easily mapped into a subclass of our definition.

Sometimes we may wish to simply express hybrid automaton dynamics using differential expressions (either equations or inclusions). Let $\mathcal{R}$ be a function assigning to each vertex $v \in \mathcal{V}$ a system of differential inclusions (that can become a system of differential equations, as a particular case). We use the notation $H = \langle Z,\ Z',\ \mathcal{V},\ \mathcal{E},\ Inv,\ \mathcal{R},\ Act,\ Reset \rangle$ if place of of $H = \langle Z,\ Z',\ \mathcal{V},\ \mathcal{E},\ Inv,\ Dyn,\ Act,\ Reset \rangle$ to denote the fact that, for each vertex $v \in \mathcal{V}$,

the formula $Dyn(v)[Z, Z', T]$ corresponds to the solution of the differential inclusions $\mathcal{R}(v)$ when the starting point is Z.

3.2 Semantics and Reachability

To formalize the semantics of hybrid automata, we first need to introduce the concept of hybrid automaton's state.

Definition 5 (States) *Let H be a hybrid automaton over $\mathcal{M}$ of dimension k. A* state *q of H is a pair $\langle v, r\rangle$, where $v \in \mathcal{V}$ is a location and $r = (r_1, \ldots, r_k) \in \mathbb{R}^k$ is an assignment of values for the variables of Z. A state $\langle v, r\rangle$ is said to be* admissible *if $Inv(v)[r]$ holds in $\mathcal{M}$.*

Intuitively, an execution of a hybrid automaton corresponds to a sequence of transitions from one state of the automaton to another. Hybrid automata have two kinds of transition (and reachability) relations: *continuous transition (reachability) relations*, capturing the continuous evolution of a state according to both formulæ $Dyn(v)$ and $Inv(v)$, and *discrete transition (reachability) relation*, capturing changes of location driven by the formula $Reset(e)$ and the formula $Act(e)$.

More formally, we can define hybrid automaton semantics as follow.

Definition 6 (Hybrid Automaton - Semantics) *Let H be a hybrid automaton over $\mathcal{M}$ of dimension k. The* continuous reachability transition relations $\xrightarrow{t}_C$ *between admissible states is defined as follows:*

$$\langle v, r\rangle \xrightarrow{t}_C \langle v, s\rangle \iff \begin{array}{l}\text{there exists } f : \mathbb{R}_{\geq 0} \to \mathbb{R}^k \text{ continuous function such that } r = f(0),\ s = f(t), \text{ and for each } t' \in [0, t] \text{ the formulæ } Inv(v)[f(t')] \\ \text{and } Dyn(v)[r, f(t'), t'] \text{ hold in } \mathcal{M}.\ f \text{ is called} \\ \text{flow function.}\end{array}$$

The discrete reachability transition relation $\xrightarrow{e}_D$*, where $e \in \mathcal{E}$, between admissible states is defined as follows:*

$$\langle v, r\rangle \xrightarrow{\langle v,u\rangle}_D \langle u, s\rangle \iff \begin{array}{l}\langle v, u\rangle \in \mathcal{E} \text{ and the formulæ } Inv(v)[r], \\ Act(\langle v, u\rangle)[r], \quad Reset(\langle v, u\rangle)[r, s], \quad \text{and} \\ Inv(u)[s] \text{ hold in } \mathcal{M}.\end{array}$$

We use the notation $\ell \xrightarrow{\lambda} \ell'$ to indicate that either $\ell \xrightarrow{\lambda}_C \ell'$, if $\lambda \in \mathbb{R}_{\geq 0}$, or $\ell \xrightarrow{\lambda}_D \ell'$, when $\lambda \in \mathcal{E}$. Furthermore, we write $\ell \rightarrow_C \ell'$ to denote that there exists a t such that $\ell \xrightarrow{t}_C \ell'$.

Remark 7 *There exist results in the literature, for example [60,61], that imply a semantics with respect to which the hybrid automaton is allowed to "touch" states momentarily without satisfying the state's invariant; in such cases, a discrete transition must immediately bring the automaton from such "bad" states to other "good" states where the automaton will satisfy the new invariant. In our view, invariants should be always satisfied as they are conditions* sine qua non *hybrid evolutions cannot be considered valid. For instance, if we aim to model the temperature of a cooler bringing helium to liquid state, we may use as invariant the formula* $Inv(v)[Z] = Z > 0$. *This invariant models the fact that it is not possible to cool an object to* 0 *Kelvin (see [62,63]). If we use the semantics used in [60,61], we are implicitly disregarding certain natural limits or physical laws, in this case, by admitting a thermodynamic absurdity that the cooler could bring helium to 0 degree Kelvin, even though momentarily. On the contrary, if we use the above semantics such behavior is not allowed. The semantics suggested in [60,61] allows more hybrid evolutions than our semantics only when the regions satisfying invariants are open. In such cases, our semantics captures the same hybrid evolutions by considering the automaton whose invariants are the closures of the original invariants.*

Example 8 *Let* H *be a hybrid automaton with* $\mathcal{V} = \{v\}$, $\mathcal{E} = \{\langle v, v\rangle\}$, *and in which* $Dyn(v)[Z, Z', T]$ *is* $Z' = e^T * Z$, $Inv(v)[Z]$ *is* $1 \leq Z < e^2$, $Reset(e)[Z, Z']$ *is* $Z' = 1$, *and* $Act(e)[Z]$ *is* $4 \leq Z \leq e^2$. *Moreover, let* tr *be the transition sequence* $\langle v, 1\rangle \xrightarrow{2}_C \langle v, e^2\rangle \xrightarrow{\langle v,v\rangle}_D \langle v, 1\rangle$. *By the semantics proposed in [60,61],* tr *is valid, while it is not valid by our semantics. However, if we consider the hybrid automaton* H' *having the same locations, edges, dynamics, activations, and resets of* H *and whose invariants are defined by the formula* $Inv(v)[Z]$ *equal to* $1 \leq Z \leq e^2$, *then, by our semantics,* tr *is a valid sequence for* H'.

Without loss of generality, we consider only hybrid automata whose formulæ are satisfiable. This assumption is not restrictive since if this is not the case we can transform the automaton and eliminate the unsatisfiable formulæ. For instance, if there exists an edge e such that $Reset(e)[Z, Z']$ is unsatisfiable we can simply delete the edge from the automaton.

Henceforth, we will omit to mention the model over which the automaton is constructed and the automaton dimension, unless it is unclear in the context.

Definition 9 (Trace) *Let* H *be a hybrid automaton and let* $J \subseteq \mathbb{N}$ *be an initial segment of* $\mathbb{N}$ *(*$|J| > 1$*).*

A trace *of* H *is a sequence* $(\ell_j)_{j\in J}$ *of admissible states such that:*

(1) for all $j \in J \setminus \{0\}$ *there exists a* λ *in* $\mathcal{E} \cup \mathbb{R}_{\geq 0}$ $\ell_{j-1} \xrightarrow{\lambda} \ell_j$;
(2) for all $j \in J \setminus \{0, 1\}$ *there exists an* e *in* $\mathcal{E}$ *and a* λ *in* $\mathcal{E} \cup \mathbb{R}_{\geq 0}$ *such that either* $\ell_{j-2} \xrightarrow{\lambda} \ell_{j-1} \xrightarrow{e}_D \ell_j$, *or* $\ell_{j-2} \xrightarrow{e}_D \ell_{j-1} \xrightarrow{\lambda} \ell_j$.

Remark 10 *Condition 2 in the above definition has been introduced to define a notion of hybrid trace analogous to the notion of trajectory defined in dynamical systems. In particular, if we relax Condition 2, we must assume transitive dynamics. For the sake of concreteness, consider the model of an automatic archer in a 2-dimensional world. The archer's goal is to hit a target τ with an arrow. Trajectories of the arrow is defined by two parameters, namely, gravity g and an initial linear velocity of magnitude v, which is assumed, for simplicity, to remain same over a succession of attempts by the archer. After each successive throw, the archer adjusts the angle of next throw according to the final position of the arrow: if the arrow lands ahead of target, then the throwing angle will be decreased proportionally, if, on the other hand, the arrow lands behind target, then the throwing angle will be increased proportionally.*

The hybrid automata describing such system consists of one vertex, v, and one edge, e: the arrow trajectories are modeled by the continuous dynamics in v, while the adjustments of throwing angle are represented by resets on e. The automata has three continuous variables, X_p, Y_p, and θ, representing the arrow position with respect to y-axis, the arrow position with respect to x-axis, and the throwing angle, respectively. Assuming the archer in position $\langle X_p, Y_p\rangle$, $Dyn(v)[Z, Z', T] \stackrel{\text{def}}{=} Y_p' = -\frac{1}{2}gT^2 + \sin\theta vT + Y_p \wedge X_p' = \sin\theta vT + X_p \wedge \theta' = \theta$ and $Inv(v)[Z] \stackrel{\text{def}}{=} Y_p \geq 0 \wedge \theta \in [0, \frac{\pi}{2})$, where $Z' = \langle X_p', Y_p', \theta'\rangle$ and $Z = \langle X_p, Y_p, \theta\rangle$, can describe dynamics and invariant on v, respectively. The activation region can be characterized as $Act(e)[Z] \stackrel{\text{def}}{=} X_p > 0 \wedge Y_p = 0$ and the reset can be $Reset(e)[Z, Z'] \stackrel{\text{def}}{=} X_p' = 0 \wedge Y_p' = 0 \wedge \theta' = \Phi_\tau(\theta, X_p)$, where Φ_τ is a function which updates θ according to the distance by which arrow misses its target.

It is easy to prove that the continuous dynamics of such automaton is not transitive i.e., even if the archer can throw an arrow from $\langle X_p, Y_p\rangle$ to $\langle X_p', Y_p'\rangle$ and from $\langle X_p', Y_p'\rangle$ to $\langle X_p'', Y_p''\rangle$ by using the same throwing angle, it is not true that the archer can throw an arrow from $\langle X_p, Y_p\rangle$ to $\langle X_p'', Y_p''\rangle$. It is also obvious that the continuous evolution cannot be split into two or more "sub-evolutions" i.e., even if the archer can throw an arrow from $\langle X_p, Y_p\rangle$ to $\langle X_p', Y_p'\rangle$ by using a throwing angle θ in time T, it does not hold that there exists a time $T' \in (0, T)$ such that the archer can throw an arrow from $\langle X_p, Y_p\rangle$ to $\langle X_p'', Y_p''\rangle$ with throwing angle θ in time T' and from $\langle X_p'', Y_p''\rangle$ to $\langle X_p', Y_p'\rangle$ with the same throwing angle in time $T - T'$. In particular, the model has an intrinsic interleaving behavior which does not admit two consecutive transitions of the same kind.

For such reasons such as this, to handle systems lacking autonomous dynamics, we imposed Condition 2. Notice that the continuous dynamics of the proposed automaton can be turned into a transitive one by adding a variable which represents the evolution of the y-velocity during the arrow trajectory. By doing so, we would increase the complexity of the formulæ involved in the decision procedure, even if we would not necessarily improve the accuracy of the model.

Clearly, a more classical notion of traces can be used in place of Definition 9, if the transitivity of dynamics is explicitly required.

Definition 11 (Transitive Trace) *Let H be a hybrid automaton whose dynamics are time-invariant and let $J \subseteq \mathbb{N}$ be an initial segment of $\mathbb{N}$ ($|J| > 1$).*

A transitive trace *of H is a sequence $(\ell_j)_{j \in J}$ of admissible states such that $\ell_{j-1} \xrightarrow{\lambda} \ell_j$, with $\lambda \in \mathcal{E} \cup \mathbb{R}_{\geq 0}$, for all $j \in J \setminus \{0\}$.*

Notice that a transitive trace can always be "compacted" in a new trace satisfying Definition 9. Details are omitted.

There exist traces which do not spend much time in continuous evolution and, in fact, time does not even advance on them. Hybrid automata admitting such traces are called *Zeno* hybrid automata.

We can now introduce formally the notion of *reachability*.

Definition 12 (Reachability) *Let H be a hybrid automaton of dimension k. A point $r \in \mathbb{R}^k$* reaches *a point $s \in \mathbb{R}^k$ (in time t) if there exists a trace $tr = \langle v, r \rangle, \ldots, \langle u, s \rangle$, for some $v, u \in \mathcal{V}$ (and t is the sum of the elapsed times in continuous transitions).*

We use $ReachSet(r)$ to denote the set of points reachable from r. Moreover, given a region $R \subseteq \mathbb{R}^k$ we use $ReachSet(R)$ to denote the set $\cup_{r \in R} ReachSet(r)$.

One may attempt to compute reachability relation by simply iterating over the computation of points reachable through continuous and discrete transitions. Unfortunately, this procedure is not effective in general. In fact, transitions might be characterizable only by undecidable formulæ and, even if single transitions are computable, the global procedure is not guaranteed to terminate.

Given a trace of H we can identify a path of $\langle \mathcal{V}, \mathcal{E} \rangle$ as follows.

Definition 13 (Corresponding Path) *Let H be a hybrid automaton. The* corresponding path *of a trace $tr = (\langle v_i, r \rangle)_{i \in I}$ of H, is the path (sequence of nodes) $ph = (v_i)_{i \in I}$ on the graph $\langle \mathcal{V}, \mathcal{E} \rangle$. In this case, we also say that ph* corresponds *to tr.*

Example 14 *If $tr = \langle v, r_0 \rangle, \langle v, r_1 \rangle, \langle u, r_2 \rangle, \langle v, r_3 \rangle$, then the corresponding path of tr is $ph = \langle v, u, v \rangle$.*

To verify specifications on hybrid automata, one may want to consider their transition systems and apply classical model checking techniques (see e.g., [64]). Unfortunately, hybrid automata have infinite state systems and the standard model checking techniques, which work on finite state models, cannot be directly applied in this context. To solve this problem, many authors suggested the use of equivalence reductions based on relations such as simulation and bisimulation. Since bisimulation preserves branching-time temporal logics such as CTL and CTL*, whenever the bisimulation quotient of a system is finite, we could verify CTL and CTL* properties of the system applying finite model checking techniques on its bisimulation quotient. In a similar vein, if the simulation quotient is finite we may also attempt to verify LTL properties of the system by applying finite model checking techniques on its simulation quotient. Bisimulation has the advantage of preserving more expressive logics, but in many cases it produces infinite quotients. On the other hand, simulation preserves less expressive logics, but it can also reduce a significantly larger class of automata to finite state models.

Since on a single hybrid automaton we can consider both timed and untimed semantics, we can compute (bi)simulation on both of them. For these reasons, we distinguish between the so called *timed-abstract simulations/bisimulations*, computed on the untimed semantics, and the *timed simulation/bisimulation*, evaluated on timed semantics. When we talk about simulation and bisimulation, we refer to timed-abstract simulation and bisimulation, respectively.

An interesting instance of the model checking problem is the verification of *safety properties*: given a hybrid automaton H and a property ϕ, we may wish to test whether ϕ holds along all of H's trajectories. Since this is the case if and only if there is no reachable state in which ϕ does not hold, the verification of safety properties naturally reduces to the reachability problem. Even if it has been proven in [22] that reachability is generally undecidable, many interesting classes of hybrid automata over which reachability is decidable have been characterized in the literature [24,59,25,6]. A common approach for deciding reachability of hybrid automata employs the technique of discretizing the automata either using equivalence relations which strongly preserve reachability (e.g., bisimulation [25]) or using abstractions (e.g., predicate abstraction [65,66]). In this paper, instead, we study reachability on hybrid automata by translating the reachability problem into first-order formulæ over the reals. In particular, we make use of the following results (whose proof is obvious):

Theorem 15 *If a class $\mathcal{H}$ of hybrid automata is first-order definable by a language $\mathcal{L}$ and a model $\mathcal{M}$, with $\mathcal{T}(\mathcal{M})$ decidable, then the membership problem for a given hybrid automata H in $\mathcal{H}$ is decidable.*

Theorem 16 *If the reachability problem for a given hybrid automaton H is first-order definable by a language $\mathcal{L}$ and a model $\mathcal{M}$, with $\mathcal{T}(\mathcal{M})$ decidable, then the reachability problem for H is decidable.*

The formulæ we get from the translation include formulæ occurring in the automata and we are interested in the evaluation of these formulæ in the model $\mathcal{M}$ over which the automaton is defined. Hence, to obtain decidability results we will ultimately exploit properties of the theory $\mathcal{T}(\mathcal{M})$.

4 Dynamics and Flow Selections

As remarked in Section 3, we allow the use of first-order formulæ, in place of differential equations and inclusions, to define hybrid automaton's flows. In particular, the dynamics are described through formulæ. Since, in general, given a dynamic, we cannot guarantee the existence of a corresponding flow function, in this section we introduce and study a set of properties which ensure such existence. The conditions we will impose on dynamics, will allow us to use Michael's selection theorem (see [26,67]) to translate a reachability problem into a first-order satisfiability problem over the reals.

The novelty of our approach mainly lies in the use of continuous selection results [67] which allow us to consider hybrid automata whose dynamics correspond to non-autonomous differential inclusions. As a direct consequence of such results, we can derive first-order formulæ to encode reachability problems.

All the formulæ presented in this and in the following sections are built upon *Inv*, *Dyn*, *Act*, and *Reset* by using standard connectives and first-order quantifiers. It follows that, if we are considering an automaton over a model $\mathcal{M}$, all the presented formulæ are evaluated with respect to the theory $\mathcal{T}(\mathcal{M})$. Hence, whenever $\mathcal{T}(\mathcal{M})$ is decidable, the decidability of the problems which are reduced to such formulæ follows.

4.1 Dynamics and Selection Problem

Assuming the continuity of F, the existence of a continuous solution for the Cauchy problem

$$\begin{cases} \dot{x}(t) = F(t, x(t)) \\ x(0) = c \end{cases} \tag{1}$$

is ensured by Cauchy-Kovalevskaya's theorem (see [68]). Hence, specifying hybrid automaton dynamics through differential equations has the side-effect of

guaranteeing the existence of a continuous differentiable flow function satisfying the dynamics. This remark can be exploited when dynamics is specified by differential equations, which lead to first-order formula trajectories [25,69].

As remarked we allow the use of formulæ, in place of differential equations and inclusions, to define hybrid automaton's flows. This choice lets us model hybrid automata whose dynamics are not differentiable, but it does not guarantee the existence of a continuous flow function satisfying the dynamics. In particular, given two formulæ $Dyn(v)[Z, Z', T]$ and $Inv(v)[Z]$ specifying the dynamics in a location v and its invariant, respectively, we are not guaranteed that $\langle v, p\rangle \xrightarrow{t}_C \langle v, q_t\rangle$. This is the case even if for all $t \in \mathbb{R}_{\geq 0}$, there exists a $q_t \in \mathbb{R}^k$ such that $Dyn(v)[p, q_t, t] \wedge Inv(v)[q_t]$ holds (see Example 20). Hence, we need to find a set of sufficient conditions for the existence of a continuous function satisfying the dynamics. To this end we formulate the flow specification as a *selection problem*.

In general, given a family of sets $\{S_x : x \in X\}$, a *selection*, or *choice function*, is a function $f : X \to \bigcup_{x\in X} S_x$ such that, for each $x \in X$, $f(x) \in S_x$. If X is finite, then the existence of a selection is obvious. Otherwise, it is necessary to assume (some form of) the *axiom of choice*[67,70]. The reader should notice that the axiom of choice does not guarantee continuity. In particular, there exist families of sets which have no continuous selection.

To find a set of sufficient conditions for the continuity of the selection, we need to introduce both the notions of *lower semi-continuity* (see [67]) and *α-paraconvexity* (see [71]).

Definition 17 (Lower Semi-Continuous Map) *Let $F : X \to 2^Y$ be a map from X to 2^Y. We define F to be* lower semi-continuous *(l.s.c.) if for each $x \in X$, for each $y \in F(x)$, and for each neighborhood U_y of y, there exists a neighborhood U_x of x such that for each $x' \in U_x$ it holds $F(x') \cap U_y \neq \emptyset$.*

We recall that a *Banach space* is a normed vector space in which every Cauchy sequence has a limit, i.e., the space is *complete* (see, e.g., [67]).

Definition 18 (α-Paraconvex Set) *Let L be a normed linear space with metric γ and let α be a real number in $[0, 1]$. A set $P \subseteq L$ is* α-paraconvex *if $\gamma(q, P) \leq \alpha * r$ for all open sphere, S_r, with radius r, and for all q in the convex hull of $S_r(p) \cap P$.*

A set is called *paraconvex* if it is α-paraconvex for some $\alpha < 1$. Notice that if a set is convex, then it is also paraconvex, whereas there exist sets which are paraconvex and non-convex.

Exploiting lower semi-continuity and properties of Banach spaces, Michael proved the following result (see [71]).

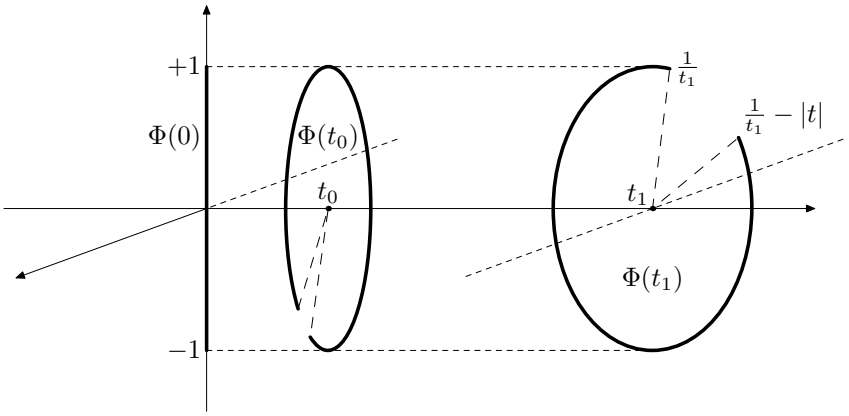


Figure 2. The map Φ of Example 20.

Theorem 19 (Michael's Selection Theorem) *Let X and Y be a metric space and a Banach space, respectively. Let F be a lower semi-continuous function from X into the closed α-paraconvex subsets of Y, with $\alpha \in [0, 1[$. Then there exists a continuous selection function $f : X \to Y$ for F, that is f is continuous and $\forall x \in X$ we have $f(x) \in F(x)$.*

The preceding result provides us the sufficient condition we were looking for. Notice that the result is proven under the hypothesis that $F(x)$ is α-paraconvex and closed for all $x \in X$. Both the closure and the α-paraconvexity of $F(x)$ are necessary. As a matter of fact, there exists a continuous map from the open interval $(-1, +1)$ into closed and not α-paraconvex subsets of $\mathbb{R}^2$ which has no continuous selection, as illustrated by Example 20 below.

The first selection theorem identified by Michael in [26] has a simpler formulation, but with conditions stricter in comparison to the one above. In particular, it requires convexity, instead of α-paraconvexity, for all $y \in Y$. Despite this drawback, we adopt the above version to allow applications to a wider set of systems; e.g., systems like the one presented in Section 6.

Example 20 (From [67]) *Consider the map $\Phi : (-2\pi, +2\pi) \to 2^{\mathbb{R}^2}$ defined as follow:*

$$\Phi(t) \stackrel{\text{def}}{=} \begin{cases} \left\{(t\cos\theta, \sin\theta) \;\middle|\; \frac{1}{t} \leq \theta \leq \frac{1}{t} + 2\pi - |t|\right\} & \text{if } t \neq 0 \\ \{(x, y) \mid -1 \leq y \leq 1 \wedge x = 0\} & \text{otherwise} \end{cases}$$

By definition, if $t = 0$, $\Phi(t)$ is the set of points in the segment between $(0, 1)$ and $(0, -1)$. Otherwise, if $t \neq 0$, $\Phi(t)$ is a subset of an ellipsoid in $\mathbb{R}^2$ obtained after removing the section from angle $\frac{1}{t} - |t|$ to angle $\frac{1}{t}$. Hence, as t gets smaller, the arc length of the removed section decreases, while the removed section itself spins around the origin at increasing angular speed. Moreover, the x-width of $\Phi(t)$ shrinks to zero as $t \to 0$, collapsing $\Phi(t)$ to $\Phi(0)$.

The function Φ can be easily proved to be lower semi-continuous over the entire open interval $(-2\pi, +2\pi)$, and yet there is no continuous selection defined on this interval. As a matter of fact, if we assume for the sake of contradiction that there exists a selection $f(t)$ continuous in $(-2\pi, 2\pi)$, then there should exist $\lim_{t\to 0} f(t)$. But by definition of Φ, the second component of f is forced to bounce between 2π and -2π as fast as t gets close to zero. Hence, $\lim_{t\to 0} f(t)$ does not exist and $f(t)$ cannot be continuous.

Notice that, since there exists no $\alpha < 1$ such that $\Phi(t)$ is α-paraconvex for all t, Φ does not satisfy the hypothesis of Theorem 19.

4.2 Michael's Form

In this section, we exploit Theorem 19 and we present a set of conditions which guarantee the existence of a valid continuous transition.

First of all, we need to characterize those time instants at which the automata, starting from a point p in a location v, can reach a point q while remaining inside the invariant set of v. We recall that an interval over $\mathbb{R}_{\geq 0}$ is a set of the form $\{r \in \mathbb{R}_{\geq 0} \mid a \prec_1 r \prec_2 b\}$, where $\prec_1$, $\prec_2$ are in $\{<, \leq\}$, $a \in \mathbb{R}_{\geq 0}$, $b \in \mathbb{R}_{\geq 0} \cup \{+\infty\}$, and $a \leq b$.

The following simple lemma holds since $Inv(v)[p]$ implies $Dyn(v)[p, p, 0]$.

Lemma 21 *Let H be a hybrid automaton. Let $p \in \mathbb{R}^k$ be such that $Inv(v)[p]$ holds. The formula $\exists Z'(Dyn(v)[p, Z', 0] \wedge Inv(v)[Z'])$ holds.*

The above lemma allows us to focus on the initial segment of time instants, for which there are dynamics that start from p and remain inside the invariant of v—these dynamics are the main *foci* of our interest.

Definition 22 ($I^H_{v,p}$ and $F^H_{v,p}$) *Let H be a hybrid automaton. Let v be a location of H and p be such that $Inv(v)[p]$ holds. $I^H_{v,p}$ is the interval of time instants satisfying the following conditions:*

- *the formula $\forall T \in I^H_{v,p}\ \exists Z'(Dyn(v)[p, Z', T] \wedge Inv(v)[Z'])$ holds;*
- *$0 \in I^H_{v,p}$;*
- *$I^H_{v,p}$ is maximal with respect to the above requirements.*

Define the function $F^H_{v,p} \colon I^H_{v,p} \to 2^{\mathbb{R}^k}$ as:

$$F^H_{v,p}(t) \stackrel{\text{def}}{=} \{q \mid Dyn(v)[p, q, t] \text{ and } Inv(v)[q]\}.$$

We now possess all the ingredients to introduce *Michael's Form*.

Definition 23 (Michael's Form) *Let H be a hybrid automaton. We say that H is in* Michael's form *if for each $v \in \mathcal{V}$ and for all p such that $Inv(v)[p]$ holds, there exists an $\alpha \in [0, 1[$ such that the function $F^H_{v,p}$ is lower semi-continuous, and, for each $t \in I^H_{v,p}$, the set $F^H_{v,p}(t)$ is closed and α-paraconvex.*

Definition 23 imposes a certain kind of continuity on the set of trajectories and it requires that for each p and for each time instant t, the set of points reachable from p at time t is a closed α-paraconvex set. This condition will allow us to exploit Michael's selection theorem to find valid continuous flows.

Example 24 *Let $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Reset\rangle$ where:*

- *$Z = (Z_1, Z_2)$ and $Z' = (Z'_1, Z'_2)$;*
- *$\mathcal{V} = \{v\}$ and $\mathcal{E} = \{e\}$, where e goes form v to v;*
- *$Inv(v)[Z]$ is $(0 \leq Z_1 \leq 1 \wedge 0 \leq Z_2 \leq 1)$;*
- *$Dyn(v)[Z, Z', T]$ is $(Z'_1 = T + Z_1 \wedge Z'_2 \geq T^2 + Z_2)$;*
- *$Act(e)[Z]$ is $(Z_1 = 1 \vee Z_2 = (1 - Z_1)^4)$;*
- *$Reset(e)[Z, Z']$ is $(Z'_1 = (Z_1)^3 + 1 \wedge Z'_2 = 1)$.*

The formulæ in H are first-order formulæ over the reals. If $p = (p_1, p_2)$, with $0 \leq p_1, p_2 \leq 1$, then the function $F^H_{v,p}$ is defined as $F^H_{v,p}(t) = \{(q_1, q_2) \mid q_1 = t + p_1, q_2 \geq t^2 + p_2,$ and $q_1, q_2 \in [0, 1]\}$. It is easy to see that $p \in F^H_{v,p}(0)$ and for each t the set $F^H_{v,p}(t)$ is closed and convex, since it is a segment. Moreover, this function is lower semi-continuous over the interval $I^H_{v,p}$. Hence, H is in Michael's form.

Notice that all dynamics expressed by not parametric ODE are in Michael's Form. To see this, simply notice that from each point p and any time t, there exists just one p' reachable from p in time t. Hence, the set of all points reachable from p in time t is (trivially) closed and convex. Moreover, since the trajectory is defined by differential equations, the dynamics is continuous and, thus, by definition, it is in Michael's Form.

We now show how to automatically identify a hybrid automaton in Michael's form. We present a first-order formula which holds if and only if the hybrid automaton under consideration is in Michael's form. In order to write this formula we need to use some standard constants, operators and relations over the reals, i.e., 0, $+$, $-$, $*$, and $\leq$. We assume that the model $\mathcal{M}$ over which our automaton is defined interprets these symbols in the standard way.

First of all, we need to characterize both $I^H_{v,p}$ and $F^H_{v,p}$ by some formulæ. Consider the following formulæ.

$$\phi(H, v)[Z, Z', T] \stackrel{\text{def}}{=} Dyn(v)[Z, Z', T] \wedge Inv(v)[Z']$$

$$\psi(H, v)[Z, T] \stackrel{\text{def}}{=} \forall T' \ (0 \leq T' \leq T \rightarrow (\exists Z' \, \phi(H, v)[Z, Z', T']))$$

By definition of $F^H_{v,p}$, it is easy to prove that $q \in F^H_{v,p}(t)$ if and only if the formula $\phi(H,v)[p,q,t]$ holds. Moreover, by definition of $I^H_{v,p}$, we can deduce that $t \in I^H_{v,p}$ if and only if the formula $\psi(H,v)[p,t]$ holds.

Lemma 25 *Let H be a hybrid automaton in Michael's form. Consider the first-order formula*

$$\psi(H,v)[Z,T] \stackrel{\text{def}}{=} \forall 0 \leq T' \leq T \, \exists Z'(Dyn(v)[Z,Z',T'] \wedge Inv(v)[Z'])$$

Assume r to be such that $Inv(v)[r]$ holds. It follows that:

$$t \in I^H_{v,r} \iff \psi(H,v)[r,t] \text{ holds}$$

PROOF. ($\Rightarrow$) If $t \in I^H_{v,r}$, then from definition of $I^H_{v,r}$, it follows that for each $t' \in [0,t]$ the formula $\exists Z'(Dyn(v)[r,Z',t'] \wedge Inv(v)[Z'])$ holds. Hence, $\psi(H,v)[r,t]$ is true.

($\Leftarrow$) If $\psi(H,v)[r,t]$ is true, then the formula $\exists Z'(Dyn(v)[r,Z',t'] \wedge Inv(v)[Z'])$ holds for each $t' \in [0,t]$, i.e., $t \in I^H_{v,r}$. $\square$

The first-order formula expressing the lower semi-continuity property for $F^H_{v,Z}$ is the following one.

$$\begin{aligned}\text{lsc}(H,v)[Z] \stackrel{\text{def}}{=} \forall T \geq 0 \, \forall Z' \; ((\psi(H,v)[Z,T] \wedge \phi(H,v)[Z,Z',T]) \rightarrowtriangle \\ (\forall E > 0 \exists D > 0 \forall T' \, ((\|T - T'\| < D \wedge \psi(H,v)[Z,T']) \rightarrowtriangle \\ (\exists Z'' \, (\phi(H,v)[Z,Z'',T'] \wedge \|Z'' - Z'\| < E)))))\end{aligned}$$

It is easy to see that $F^H_{v,p}$ is lower semi-continuous if and only if $\text{lsc}(H,v)[p]$ holds. The following formula states that $F^H_{v,Z}(T)$ is a closed set.

$$\begin{aligned}\text{Closed}(H,v)[Z,T] \stackrel{\text{def}}{=} \forall Z' \; ((\forall E > 0 \; \exists Z'' \; (\phi(H,v)[Z,Z'',T] \wedge \\ \|Z' - Z''\| < E)) \rightarrowtriangle \phi(H,v)[Z,Z',T])\end{aligned}$$

With respect to the other properties defining Michael's form, α-paraconvexity has the most complex first-order characterization. For this reason, to write a first-order formula, which defines it, we first need to characterize the properties Between$[p,p',p'']$, O-Sphere$(p,r)[p']$, and C-Sphere$(p,r)[p']$, which hold if and only if p' lies in the segment between p and p'', p' lies in the open sphere of radius r centered in p, and p' lies in the closed sphere of radius r centered in p, respectively.

$$\text{Between}[Z, Z', Z''] \stackrel{\text{def}}{=} \bigwedge_{j=1}^{n} \Bigg(X'_j < X_j \wedge X_j < X''_j \wedge \bigvee_{i \neq j}^{n} (X_i - X'_i) * (X''_j - X'_j) = (X''_i - X'_i) * (X_j - X'_j) \Bigg)$$

$$\text{O-Sphere}(Z', X)[Z] \stackrel{\text{def}}{=} X > \|Z - Z'\|$$

$$\text{C-Sphere}(Z', X)[Z] \stackrel{\text{def}}{=} X \geq \|Z - Z'\|$$

By using above formulæ we can specify the formula $\text{Convexify}(\phi)[p]$ which holds if and only if p lies in the convexification of the set defined by ϕ.

$$\text{Convexify}(\phi)[Z] \stackrel{\text{def}}{=} \phi[Z] \vee \exists Z', Z'' \, (\phi[Z'] \wedge \phi[Z''] \wedge \text{Between}[Z, Z', Z''])$$

The above formulæ are quite simple and their correctness can be easily verified. By using them, we can write the formula $\text{ParaConv}(\phi, X_\alpha)$ which holds if and only if the set defined by ϕ is X_α-paraconvex.

$$\begin{aligned} \text{ParaConv}(\phi, X_\alpha) \stackrel{\text{def}}{=} \forall X > 0 \forall Z, Z' (&\text{Convexify}\,(\phi \wedge \text{O-Sphere}(Z', X))\,[Z] \twoheadrightarrow \\ &\exists Z''(\phi[Z''] \wedge \text{C-Sphere}(Z'', X_\alpha * X)[Z])) \end{aligned}$$

Finally, in order to guarantee Michael's form, we need a formula which holds if and only if for all points p in the invariant there exists an α in $[0, 1)$ such that for all times t in $I^H_{v,p}$, $F^H_{v,p}$ is lower semi-continuous and $F^H_{v,p}(t)$ is closed and α-paraconvex. Such a formula may be defined by $\text{MForm}(H, v)$ as:

$$\begin{aligned} \text{MForm}(H, v) \stackrel{\text{def}}{=} \forall Z \, \Big(Inv(v)[Z] \twoheadrightarrow \Big(&\exists X_\alpha 0 \leq X_\alpha < 1 \wedge \\ &\forall T \, \Big(\psi(H, v)[Z, T] \twoheadrightarrow \Big(\text{ParaConv}(\overline{\phi}\,(H, v, Z, T)\,, X_\alpha) \wedge \\ &\text{Closed}(H, v)[Z, T] \Big) \Big) \Big) \wedge \text{lsc}(H, v)[Z] \Big) \end{aligned}$$

where $\overline{\phi}\,(H, v, Z, T)\,[Z'] \stackrel{\text{def}}{=} \phi(H, v)[Z, Z', T]$.

Since the locations of a hybrid automaton are finite, we can write the formula:

$$\bigwedge_{v \in \mathcal{V}} \text{MForm}(H, v)$$

which holds if and only if the corresponding automaton is in Michael's form.

Notice that, if H is defined over a model $\mathcal{M}$ such that $\mathcal{T}(\mathcal{M})$ is decidable, then we can decide whether H is in Michael's form or not.

Given a hybrid automaton H in Michael's form and a starting region $R \subseteq \mathbb{R}^k$ characterized by a first-order formula ρ over the reals, we may wish to compute the region $\mathit{ReachSet}(R) \subseteq \mathbb{R}^k$ of points that can be reached starting from a point in R and following a trace of H.

Our approach will exploit Michael's selection theorem. In particular, Michael's selection theorem will guarantee the correctness of a translation into appropriate first-order formulæ of our reachability and model checking problems.

As already noticed in the previous section, we assume that some standard operators and relations over the reals are included in the first-order language over which our automata are defined (e.g., 0, +, $\leq$) and that these are interpreted in the standard way.

As a direct consequence of Lemma 25, we can prove the following result.

Theorem 26 *Let H be a hybrid automaton in Michael's form. Consider the first-order formula*

$$\begin{aligned} C\text{-}\mathit{Reach}(H,v)[Z,Z',T] \stackrel{\text{def}}{=} \; & (\,(T>0 \wedge \mathit{Dyn}(v)[Z,Z',T] \wedge \psi(H,v)[Z,T]) \vee \\ & (T=0 \wedge Z=Z')\,) \wedge \mathit{Inv}(v)[Z] \wedge \mathit{Inv}(v)[Z'] \end{aligned}$$

Then following holds:

$$\langle v,r\rangle \xrightarrow{t}_C \langle v,s\rangle \iff C\text{-}\mathit{Reach}(H,v)[r,s,t] \text{ holds}$$

PROOF. ($\Rightarrow$) By Definition 6 we have that $\langle v,r\rangle \xrightarrow{t}_C \langle v,s\rangle$ if and only if there exists $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}^k$ continuous function such that $r = f(0)$, $s = f(t)$, and the formulæ $\mathit{Inv}(v)[f(t')]$ and $\mathit{Dyn}(v)[r, f(t'), t']$ hold for each $t' \in [0,t]$.

From the fact that for each $t' \in [0,t]$ $\mathit{Dyn}(v)[r, f(t'), t'] \wedge \mathit{Inv}(v)[f(t')]$ holds, it follows that $\psi(H,v)[r,t]$ holds. Hence we deduce that all the formulæ $\mathit{Inv}(v)[r]$, $\mathit{Inv}(v)[s]$, $\mathit{Dyn}(v)[r,s,t]$, and $\psi(H,v)[r,t]$ hold, as stated.

($\Leftarrow$) Let us assume that $t = 0$, $r = s$, $\mathit{Inv}(v)[r]$, and $\mathit{Inv}(v)[s]$ all hold. Then every continuous function f such that $f(0) = s$ is a valid flow and, thus, $\langle v,r\rangle \xrightarrow{t}_C \langle v,s\rangle$ holds by definition. Let us assume that $t > 0$, $\mathit{Dyn}(v)[r,s,t]$, $\psi(H,v)[r,t]$, $\mathit{Inv}(v)[r]$, and $\mathit{Inv}(v)[s]$ hold. By Lemma 25 we have that $t \in I^H_{v,r}$. Moreover, s belongs to $F^H_{v,r}(t)$, which is lower semi-continuous with closed and

α-paraconvex images. Consider the function $\tilde{F}\colon [0,t] \to 2^{\mathbb{R}^k}$ defined as:

$$\tilde{F}(T) = \begin{cases} \{r\} & \text{if } T = 0 \\ F^H_{v,r}(T) & \text{if } 0 < T < t \\ \{s\} & \text{if } T = t \end{cases}$$

It is immediately seen that for each $t' \in [0,t]$ $\tilde{F}(t')$ is closed and α-paraconvex. We prove that $\tilde{F}$ is lower semi-continuous on $[0,t]$. Let $t' \in [0,t]$. We need to consider three distinct cases: (a) $t' = 0$; (b) $0 < t' < t$; (c) $t' = t$.

(a) If $t' = 0$ and $y \in \tilde{F}(0)$, then $y = r$. Let U_r be a neighborhood of r. Since, $F^H_{v,r}$ is lower semi-continuous there exists a neighborhood U_0 of 0 in $I^H_{v,r}$ such that for each t'' in U_0 it holds that $F^H_{v,r}(t'') \cap U_r \neq \emptyset$. Since, $[0,t] \subseteq I^H_{v,r}$ we get that $U_0' = U_0 \cap [0,t)$ is a neighborhood of 0 in $[0,t]$. If $t'' \in U_0'$, there are two possible subcases: either $t'' = 0$ or $0 < t'' < t$. If $t'' = 0$, then $\tilde{F}(0) \cap U_r = \{r\} \neq \emptyset$. If, on the other hand, $0 < t'' < t$, then $\tilde{F}(t'') \cap U_r = F^H_{v,r}(t'') \cap U_r \neq \emptyset$.

(b) If $0 < t' < t$ and $y \in \tilde{F}(t')$, then $y \in F^H_{v,r}(t')$. Let U_y be a neighborhood of y. Since $F^H_{v,r}$ is lower semi-continuous, there exists a neighborhood $U_{t'}$ of t' in $I^H_{v,r}$ such that for each t'' in $U_{t'}$ it holds that $F^H_{v,r}(t'') \cap U_y \neq \emptyset$. Since $t' \in (0,t) \subseteq I^H_{v,r}$, we conclude that $U_{t'}' = U_{t'} \cap (0,t)$ is a neighborhood of t' in $[0,t]$. If $t'' \in U_{t'}'$, then $\tilde{F}(t'') \cap U_r = F^H_{v,r}(t'') \cap U_r \neq \emptyset$.

(c) If $t' = t$ and $y \in \tilde{F}(t)$, then $y = s$. Let U_s be a neighborhood of s. Since $F^H_{v,r}$ is lower semi-continuous, there exists a neighborhood U_t of t in $I^H_{v,r}$ such that for each t'' in U_t, it holds that $F^H_{v,r}(t'') \cap U_s \neq \emptyset$. Since $[0,t] \subseteq I^H_{v,r}$, we get that $U_t' = U_t \cap (0,t]$ is a neighborhood of t in $[0,t]$. If $t'' \in U_t'$, then there are two possible sub-cases: namely, either $t'' = t$ or $0 < t'' < t$. If $t'' = t$, then $\tilde{F}(0) \cap U_s = \{s\} \neq \emptyset$. If $0 < t'' < t$, then $\tilde{F}(t'') \cap U_s = F^H_{v,r}(t'') \cap U_s \neq \emptyset$.

Since $\tilde{F}\colon [0,t] \to 2^{\mathbb{R}^k}$ is lower semi-continuous, $[0,t]$ is a metric space, $\mathbb{R}^k$ is a Banach space, and $\tilde{F}(t')$ is closed and α-paraconvex, for each t' in $[0,t]$, by Theorem 19, we may deduce the following: there exists $f\colon [0,t] \to \mathbb{R}^k$ continuous selection for $\tilde{F}$. Hence, by definition of continuous selection (see [67]), f is a continuous function such that for each $t' \in [0,t]$ it holds $f(t') \in \tilde{F}(t')$. From this last statement, we further deduce that: $f(0) = r$; $f(t) = s$; for each $0 < t' < t$ it holds that $f(t') \in F^H_{v,r}(t')$, i.e., $Dyn(v)[r, f(t'), t']$ and $Inv(v)[f(t')]$. Consider the function $\tilde{f}\colon \mathbb{R}_{\geq 0} \to \mathbb{R}^k$ defined as:

$$\tilde{f}(T) = \begin{cases} f(T) & \text{if } T \in [0,t] \\ s & \text{if } T > t \end{cases}$$

We conclude that $\langle v, r\rangle \xrightarrow{t}_C \langle v, s\rangle$, as desired. $\square$

One may observe that for any edge $\langle v, u\rangle \in \mathcal{E}$ the discrete reachability is characterized by the first-order formula

$$\begin{aligned} \textit{D-Reach}(H, \langle v, u\rangle)[Z, Z'] \stackrel{\text{def}}{=}\ & \textit{Inv}(v)[Z] \wedge \textit{Act}(\langle v, u\rangle)[Z] \wedge \\ & \textit{Reset}(\langle v, u\rangle)[Z, Z'] \wedge \textit{Inv}(v)[Z'] \end{aligned}$$

Given a point $r \in \mathbb{R}^k$, we see that the formula $\textit{C-Reach}(H, v)[r, Z', t]$, as defined in Theorem 26 and with free variables in Z', characterizes the set of points reachable from r at v using only continuous dynamics. Similarly, the first-order formula $\textit{D-Reach}(H, e)[r, Z']$ defines the set of points reachable from r using the discrete transition e.

Suppose that a point r reaches a point s in time t through a trace tr, whose corresponding path is $ph = \langle v, u\rangle$. Since $\textit{Dyn}(v)[r, r, 0]$ and $\textit{Dyn}(u)[s, s, 0]$ hold by Definition 4, $\langle v, r\rangle \xrightarrow{0}_C \langle v, r\rangle$ and $\langle u, s\rangle \xrightarrow{0}_C \langle u, s\rangle$. Hence, tr is equivalent to tr' of the form $\langle v, r\rangle \xrightarrow{t'}_C \langle v, r_1\rangle \xrightarrow{\langle v,u\rangle}_D \langle u, s_1\rangle \xrightarrow{t''}_C \langle u, s\rangle$ where $t = t' + t''$. Thus, the reachability can always be expressed through a trace whose corresponding path is $ph = \langle v, u\rangle$ and results in the following first-order formula:

$$\begin{aligned} \overline{\textit{Reach}}(H, ph)[Z^0, Z^1, Z^2, Z^3, T] \stackrel{\text{def}}{=}\ & \exists T_1 \geq 0, T_2 \geq 0\, (T = T_1 + T_2 \wedge \\ & \textit{C-Reach}(H, v)[Z^0, Z^1, T_1] \wedge \\ & \textit{D-Reach}(H, \langle v, u\rangle)[Z^1, Z^2] \wedge \\ & \textit{C-Reach}(H, u)[Z^2, Z^3, T_2]\big) \end{aligned}$$

If we have a path $ph = (v_i)_{i\in[0,h]}$ in the graph $\langle \mathcal{V}, \mathcal{E}\rangle$, then following two cases are possible: either it corresponds to a trace of H or it does not. In both cases, we can express the desired reachability relation with a first-order formula, which characterizes all the pairs of $\mathbb{R}^k$ that can be connected in H through a trace corresponding to path $ph = (v_i)_{i\in[0,h]}$, with $e_i = \langle v_i, v_{i+1}\rangle$

$$\begin{aligned} \overline{\textit{Reach}}(H, ph)[Z^0, \ldots, Z^{2h+1}, T] \stackrel{\text{def}}{=}\ & \exists T_0 \geq 0, \ldots, T_h \geq 0\ \Bigg(T = \sum_{i=0}^{h} T_i \wedge \\ & \textit{C-Reach}(H, v_0)[Z^0, Z^1, T_0] \wedge \\ & \bigwedge_{i\in[0,h-1]} \big(\textit{D-Reach}(H, e_i)[Z^{2i+1}, Z^{2i+2}] \wedge \\ & \textit{C-Reach}(H, v_{i+1})[Z^{2i+2}, Z^{2i+3}, T_{i+1}]\big)\Bigg) \end{aligned}$$

The above formula considers only traces in which continuous and discrete transitions are alternating. This constraint is not restrictive since, by reachability and trace definitions, any trace can be mapped into a trace which satisfies the continuous/discrete alternation and has the same starting and finishing states. The following lemma proves that the formula $\overline{\textit{Reach}}(H, ph)[Z^0, \ldots, Z^{2h+1}, T]$ is correct and complete.

Lemma 27 *Let $H = \langle Z,\ Z',\ \mathcal{V},\ \mathcal{E},\ Inv,\ Dyn,\ Act,\ Reset\rangle$ be a hybrid automaton in Michael's form and $ph = (v_i)_{i\in[0,h]}$ be a path in $\langle \mathcal{V}, \mathcal{E}\rangle$. It holds that r reaches s in time t through a trace tr whose corresponding path is ph if and only if $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$ is satisfiable.*

PROOF. ($\Rightarrow$) Let $tr = (\ell_i)_{i\in[0,n]}$ with $\ell_0 = \langle v_0, r\rangle$ and $\ell_n = \langle v_n, s\rangle$. Since, by Definition 4, $Dyn(v)[r, r, 0]$ and $Dyn(u)[s, s, 0]$ hold, if there are two consecutive discrete transitions $\ell_i \xrightarrow{e}_D \ell_{i+1} \xrightarrow{e'}_D \ell_{i+2}$ in tr, we can replace them by $\ell_i \xrightarrow{e}_D \ell_{i+1} \xrightarrow{0}_C \ell_{i+1} \xrightarrow{e'}_D \ell_{i+2}$. Hence, we may assume that in tr discrete and continuous transitions are alternated. We may further assume tr starts and ends with a continuous transition, since, otherwise, we may simply add either $\ell_0 \xrightarrow{0}_C \ell_0$ or $\ell_n \xrightarrow{0}_C \ell_n$ or both. Thus, we have that $n = 2h$. Let $\ell_i = \langle v_i, r_i\rangle$ and consider the valuation, which replaces Z^i by r_i in the formula $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$. By induction on h, we can prove that this valuation satisfies $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$.

($\Leftarrow$) Since $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$ is satisfiable, there exists an assignment to the Z^i's which satisfies it by replacing Z^i with z_i. Consider the trace $tr = (\ell_i)_{i\in[0,2h]}$ such that $\ell_0 = \langle v, r\rangle$, $\ell_{2h} = \langle v_h, s\rangle$, and for each $i \in [1, h-1]$, we have $\ell_{2i-1} = \langle v_{i-1}, z_{2i-1}\rangle$ and $\ell_{2i} = \langle v_i, z_{2i}\rangle$. By induction on the length of ph, we can prove that tr is a trace of H, which connects r to s in time t. □

Let ph be a path of length h. Consider the formula

$$Reach(H, ph)[Z, Z', T] \stackrel{\text{def}}{=} \exists Z^1, \ldots, Z^{2h}\ \overline{Reach}(H, ph)[Z, Z^1, \ldots, Z^{2h}, Z', T]$$

Since $Reach(H, ph)[r, s, t]$ holds if and only if $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$ is satisfiable, by Lemma 27, r reaches s in time t if and only if there exists a path ph of $\langle \mathcal{V}, \mathcal{E}\rangle$ such that the formula $Reach(H, ph)[r, s, t]$ holds. So, we could characterize reachability for a hybrid automaton in Michael's form, considering the disjunction of all the formulæ for all the paths of $\langle \mathcal{V}, \mathcal{E}\rangle$. Unfortunately, if $\langle \mathcal{V}, \mathcal{E}\rangle$ has a cycle, then it has an infinite number of paths and this straightforward approach fails. In Section 5 we introduce a class of hybrid automata whose traces corresponds to paths of finite length.

5 First-Order Constant Reset Hybrid Automata

In this section we introduce and study a class of hybrid automata, *First-Order Constant Reset* hybrid automata (FOCoRe). Such automata are in Michael's form and their resets are constant as in the class of o-minimal hybrid automata. Even though FOCoRe automata do not admit finite bisimulation quotient, we

can translate reachability problems into satisfiability of a particular first-order formula over the reals. It follows that if the specifying theory is decidable, then the reachability problem is decidable.

5.1 FOCoRe Definition

A FOCoRe automaton is simply a hybrid automaton in Michael's form whose resets are constant. More formally we can define it as follows.

Definition 28 (First-Order Constant Reset Automata) *We say that a hybrid automaton H is a* first-order constant reset *hybrid automaton, or simply a* FOCoRe*, if:*

(1) H is in Michael's form;
(2) All the resets, $Reset(e)[Z, Z']$, of H are constant i.e., if $Reset(e)[p, s]$ holds, then $Reset(e)[r, s]$ holds too for all p, s, and r in $\mathbb{R}^k$.

Condition 1 will allow us to exploit Theorem 26 to check the existence of a valid continuous flows. Condition 2 is exactly the condition imposed on o-minimal hybrid automata.

Example 29 *Let $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Reset\rangle$ where:*

- *$Z = (Z_1, Z_2)$ and $Z' = (Z'_1, Z'_2)$;*
- *$\mathcal{V} = \{v\}$ and $\mathcal{E} = \{e\}$, where e goes form v to v;*
- *$Inv(v)[Z]$ is $(0 \leq Z_1 \leq 1 \wedge 0 \leq Z_2 \leq 1)$;*
- *$Dyn(v)[Z, Z', T]$ is $(Z'_1 = T + Z_1 \wedge Z'_2 \geq T^2 + Z_2)$;*
- *$Act(e)[Z]$ is $(Z_1 = 1 \vee Z_2 = 1)$;*
- *$Reset(e)[Z, Z']$ is $(Z'_1 = 1 \wedge Z'_2 = 1)$.*

The formulæ in H are first-order formulæ over the reals. If $p = (p_1, p_2)$, with $0 \leq p_1, p_2 \leq 1$, then the function $F^H_{v,p}$ is defined as $F^H_{v,p}(t) = \{(q_1, q_2) \mid q_1 = t + p_1, q_2 \geq t^2 + p_2,$ and $0 \leq q_1, q_2 \leq 1\}$. It is easy to see that $p \in F^H_{v,p}(0)$ and for each t the set $F^H_{v,p}(t)$ is closed and convex, since it is a segment. Moreover, this function is lower semi-continuous over the interval $I^H_{v,p}$. It follows that H is in Michael's form. Finally, $Reset(e)[Z, Z']$ does not depend on Z. Hence, H is a FOCoRe automaton.

O-minimal hybrid automata [25,6] are easily seen as special cases of FOCoRe automata. As a matter of fact, o-minimal hybrid automata allow only one continuous flow from each point, hence an o-minimal hybrid automaton is a FOCoRe for which the set $F^H_{v,p}(t)$ reduces to a singleton, which is obviously closed and convex, for each time instant t. The continuity of the flow immediately implies the lower semi-continuity of $F^H_{v,p}(t)$ over $I^H_{v,p}$. On the other

hand, the class FOCoRe is not included in the class of o-minimal hybrid automata, since from each point we allow a set of flows. Moreover, FOCoRe's flows are not necessarily solutions of autonomous differential inclusions and their dynamics are not o-minimal in general.

Notice that the identification of a FOCoRe automaton can be carried out automatically. In particular, in the remaining part of the section we present a first-order formula which holds if and only if a particular automaton under consideration is a FOCoRe.

As detailed in Section 4.2, a hybrid automaton H is in Michael's form if and only if the following formula holds:

$$\bigwedge_{v \in \mathcal{V}} \mathrm{MForm}(H, v)$$

Let us consider Condition 2 of FOCoRe definition. We just need to characterize the fact that, for all points $p, p', q \in \mathbb{R}^k$, if $\mathit{Reset}(e)[p, q]$ holds, then $\mathit{Reset}(e)[p', q]$ does too. It is easy to prove that following formula expresses this fact.

$$\mathrm{ConstReset}(H, e) \stackrel{\text{def}}{=} \forall Z_1, Z', Z_2, Z'' \left((\mathit{Reset}(e)[Z_1, Z'] \wedge \mathit{Reset}(e)[Z_2, Z'']) \rightarrowtriangle \mathit{Reset}(e)[Z_1, Z''] \right)$$

Since both edges and locations are bounded, we can write the formula:

$$\bigwedge_{v \in \mathcal{V}} \mathrm{MForm}(H, e) \ \wedge \ \bigwedge_{e \in \mathcal{E}} \mathrm{ConstReset}(H, e)$$

which holds if and only if the corresponding hybrid automaton is a FOCoRe.

5.2 Reachability

Given a FOCoRe automaton H and a starting region $R \subseteq \mathbb{R}^k$ characterized by a first-order formula ρ over the reals, we may wish to compute the region $\mathit{ReachSet}(R) \subseteq \mathbb{R}^k$ of points that can be reached starting from a point in R and following a trace of H.

More generally, given a formula Q of a temporal logic, we may also be interested in determining the points of R which satisfy Q. In the case of o-minimal hybrid automata, reachability as well as other temporal logic properties are checked through bisimulation. This technique can be applied whenever we consider a class $\mathcal{C}$ of hybrid automata, which has the finite bisimulation property, i.e., each automaton in $\mathcal{C}$ has a finite bisimulation quotient. Unfortunately, the class of FOCoRe does not possess the finite bisimulation property, as we will show in Section 5.3.

Our approach will instead exploit the properties of Michael's form and constant resets. In this section, we demonstrate how the reachability problem over FOCoRe $\mathcal{T}$-automata can be reduced to the satisfiability of a first-order formula over the theory $\mathcal{T}$. From this note entails the decidability of the reachability problem over the FOCoRe which are expressed in a decidable theory.

In Section 4.3, we derived the formula $\overline{Reach}$ such that if H is a hybrid automaton in Michael's form, $ph = \langle v_0, \ldots, v_h \rangle$ is a path in $\langle \mathcal{V}, \mathcal{E} \rangle$ and $r, s \in \mathbb{R}^k$, then r reaches s in time t through a trace tr whose corresponding path is ph if and only if the first-order formula $\overline{Reach}(H, ph)[r, Z^1, \ldots, Z^{2h}, s, t]$ is satisfiable. As remarked at the end of the same section, if $\langle \mathcal{V}, \mathcal{E} \rangle$ has a cycle, then it has an infinite number of paths and, thus the formula $\overline{Reach}$ cannot be used directly to specify an effective method to reduce a reachability problem over H to a satisfiability problem in a first-order theory. In the specific case of FOCoRe, we can exploit the constant resets feature and ignore all the paths of $\langle \mathcal{V}, \mathcal{E} \rangle$ whose length exceeds $|\mathcal{E}|$. Below, we denote the set of those paths in $\langle \mathcal{V}, \mathcal{E} \rangle$ of length at most $|\mathcal{E}|$ as $\overline{P}_{\mathcal{E}}$ and we write $\overline{P}_{\mathcal{E}}(v)$ to denote the set of path in $\overline{P}_{\mathcal{E}}$ starting from v.

Theorem 30 *Let H be a FOCoRe automaton of dimension k. Point $s \in \mathbb{R}^k$ is reachable from $r \in \mathbb{R}^k$ by H if and only if there exists a path $ph \in \overline{P}_{\mathcal{E}}$ of length at most $|\mathcal{E}|$ such that the formula $\exists T \geq 0\, Reach(H, ph)[r, s, T]$ holds.*

PROOF. The complete proof of the preceding theorem is reported in Appendix on page 48.

Given a FOCoRe automaton H, if $\overline{P}_{\mathcal{E}}$ is the set of paths of $\langle \mathcal{V}, \mathcal{E} \rangle$ of length at most $|\mathcal{E}|$, we can define the first-order formula $\mathcal{P}_H[Z, Z']$ as follows:

$$\mathcal{P}_H[Z, Z'] \stackrel{\text{def}}{=} \bigvee_{ph \in \overline{P}_{\mathcal{E}}} \exists T \geq 0\, Reach(H, ph)[Z, Z', T]$$

From Theorem 30, it follows that, given a FOCoRe H, $s \in ReachSet(r)$ if and only if the formula $\mathcal{P}_H[r, s]$ holds. We can now characterize the set of points reachable from a first-order definable set $R \subseteq \mathbb{R}^k$.

Corollary 31 *Let H be a FOCoRe automaton and $\rho[Z]$ be a first-order formula. The set $ReachSet(Sat(\rho))$ is characterized by the first-order formula*

$$\mathcal{S}_H(\rho)[Z'] \stackrel{\text{def}}{=} \exists Z\, (\rho[Z] \wedge \mathcal{P}_H[Z, Z'])$$

Thus we have reduced our reachability problem to that of deciding the satisfiability of an existential first-order formula and we get the following corollary.

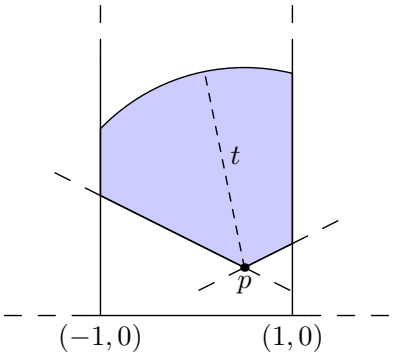


Figure 3. The H_{inf}'s dynamic.

Corollary 32 *Let H be a FOCoRe over a model $\mathcal{M}$. If $\mathcal{T}(\mathcal{M})$ is decidable, then the reachability problem for H is decidable.*

5.3 FOCoRe and Bisimulation

In this section we prove that there exists a FOCoRe which does not admit a finite bisimulation quotient. In particular, we prove that the hybrid automaton $H_{\text{inf}} = \langle Z,\ Z',\ \mathcal{V},\ \mathcal{E},\ Inv,\ Dyn,\ Act,\ Reset \rangle$ where:

- $Z = (Z_1, Z_2)$ and $Z' = (Z_1', Z_2')$, where Z_1, Z_2, Z_1' and Z_2' are real variables,
- $\mathcal{V} = \{v\}$ and $\mathcal{E} = \{e\}$, where e goes form v to v,
- $Inv(v)[Z]$ is $(-1 \leq Z_1 \leq 1 \wedge Z_2 > 0)$,
- $Dyn(v)[Z, Z', T]$ is $up\,[Z, Z'] \wedge up'\,[Z, Z'] \wedge \|Z' - Z\| \leq T$, where $up\,[Z, Z']$ is $Z_2' \geq Z_2 Z_1' + Z_2(1 - Z_1)$ and $up'\,[Z, Z']$ is $Z_2' \geq -Z_2 Z_1' + Z_2(1 + Z_1)$,
- $Act(e)[Z]$ is $(Z_1 = 1 \wedge 0 < Z_2 \leq 1)$,
- $Reset(e)[Z, Z']$ is $(Z_1' = -1 \wedge 0 < Z_2' \leq 1)$,

is a FOCoRe and does not admit a finite bisimulation quotient.

Lemma 33 *H_{inf} is a FOCoRe automaton.*

PROOF. The complete proof is to be found in Appendix on page 51.

To prove that the automaton H_{inf} does not admit finite bisimulation quotient, we have to exploit the constant reset condition in the FOCoRe's definition. In particular, by $\text{Pre}_\sigma\,(P)$'s definition, and by constant reset condition, it follows that:

$$\text{Pre}_e\,(P) = \begin{cases} \emptyset & \text{if } P \cap \mathcal{R}(e) = \emptyset \\ \mathcal{A}(e) & \text{if } P \cap \mathcal{R}(e) \neq \emptyset \end{cases}$$

Thus, as reported in [25], H_{inf} admits a finite bisimulation quotient if and only if Algorithm 1 terminates, when the initial partition is the partition $\mathcal{S}_v$ induced by the set $\mathcal{A}_v = \{\mathcal{I}(v)\} \cup \bigcup_{\langle v',v\rangle\in\mathcal{E}} \{\mathcal{R}(\langle v',v\rangle)\} \cup \bigcup_{\langle v,v'\rangle\in\mathcal{E}} \{\mathcal{A}(\langle v,v'\rangle)\}$.

Algorithm 1 Bisimulation algorithm for hybrid systems with constant resets

```
for v ∈ V do
  S_v ← compute_initial_partition_from(A_v)
  while ∃P, P' ∈ S_v such that ∅ ≠ P ∩ Pre_v(P') ≠ P do
    P_1 ← P ∩ Pre_v(P')
    P_2 ← P \ Pre_v(P')
    S_v ← (S_v \ {P}) ∪ {P_1, P_2}
  end while
end for
X/∼ ← ⋃_v ⟨v, S_v⟩
```

However, the following results allow us to conclude that Algorithm 1 does not terminate on H_{inf} and consequently, H_{inf} does not admit finite bisimulation quotient. Below, we prove that, considering the H_{inf} automaton, there exists two sets satisfying the `while` condition at the end of each cycle of Algorithm 1. In particular, we prove that each of algorithm's iteration adds to $\mathcal{S}_v$ a non-empty set P_1 smaller than P such that P_1 and P' satisfy the *while* condition.

Theorem 34 *The automaton H_{inf} does not admit finite bisimulation quotient.*

PROOF. The complete proof of the preceding theorem is presented in Appendix on page 56.

Next corollary follows from Lemma 33 and Theorem 34.

Corollary 35 *There exist FOCoRe automata that do not admit finite bisimulation quotient.*

PROOF. By Lemma 33, H_{inf} is a FOCoRe automaton and, by Theorem 34, H_{inf} does not admit finite bisimulation quotient. □

To complete our analysis we briefly comment on the connection between FOCoRe and rectangular automata (see [24]).

It is easy to see that there exist FOCoRe which are not rectangular automata and there exist rectangular automata which are not FOCoRe. In particular, the automaton H_{inf} introduced above is a FOCoRe which is not rectangular, since its dynamics cannot be expressed as a differential inclusion of the kind

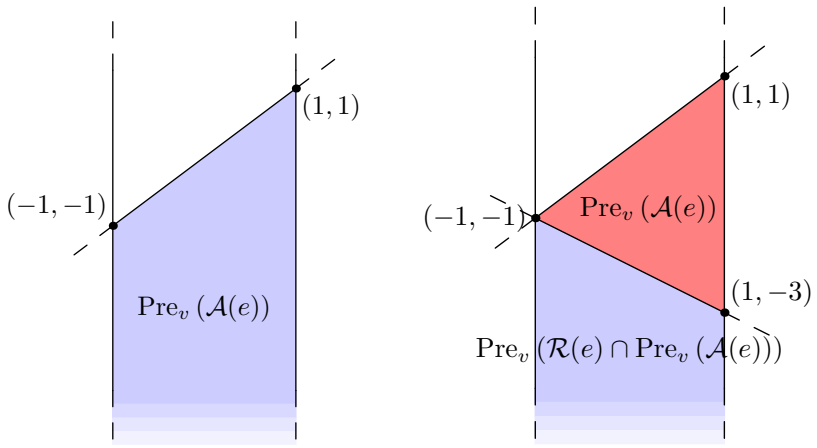
$\dot{Z} \in [c_l, c_u]$ with $c_l, c_u \in \mathbb{Q} \cup \infty$. Moreover, the automaton used to prove that rectangular automata do not always possess finite bisimulation quotient (see Theorem 6.1.1, page 113, [24]) is not a FOCoRe, since it is defined by non constant resets.

Notice also that the class "*FOCoRe* $\cap$ rectangular" is not empty and that there exist automata in "*FOCoRe* $\cap$ rectangular" which do not admit a finite bisimulation quotient (see Example 36). However, to prove such a result it is necessary to exploit unbounded region conditions, while in proving the infinity of the bisimulation quotient for both rectangular automata and FOCoRe, bounded partitions are sufficient.

Example 36 *Let H be the automaton $\langle Z,\ Z',\ \mathcal{V},\ \mathcal{E},\ Inv,\ Dyn,\ Act,\ Reset\rangle$ where:*

- $Z = (Z_1, Z_2)$ *and* $Z' = (Z_1', Z_2')$, *where* Z_1, Z_2, Z_1' *and* Z_2' *are real variables,*
- $\mathcal{V} = \{v\}$ *and* $\mathcal{E} = \{e\}$, *where* e *goes form* v *to* v,
- $Inv(v)[Z]$ *is* $-1 \leq Z_1 \leq 1$,
- $Dyn(v)[Z, Z', T]$ *is* $Z_1' = T + Z_1 \ \wedge\ Z_2' \geq -T + Z_2 \ \wedge\ Z_2' \leq T + Z_2$,
- $Act(e)[Z]$ *is* $(Z_1 = 1 \wedge Z_2 \leq 1)$,
- $Reset(e)[Z, Z']$ *is* $(Z_1' = -1 \wedge Z_2' \leq 1)$.

Notice that H differs from H_{inf} because of their dynamics. However, since dynamics of H can be expressed as $\dot{Z}_1 = 1$ and $\dot{Z}_2 = [-1, 1]$, H is a rectangular automaton. Moreover, it is easy to prove that H is also a FOCoRe.



(a) $\mathrm{Pre}_v(\mathcal{A}(e))$ (b) $\mathrm{Pre}_v(\mathcal{R}(e) \cap \mathrm{Pre}_v(\mathcal{A}(e)))$

Figure 4. Preimages of the automaton H.

The automaton H does not admit a finite bisimulation quotient. To prove such statement, let us consider Algorithm 1. The two sets $Pre_v(\mathcal{A}(e))$ and $Pre_v(\mathcal{R}(e) \cap Pre_v(\mathcal{A}(e)))$ are depicted in Figures 4(a) and 4(b), respectively. Since, they split $\mathcal{R}(e)$ and $\mathcal{A}(e)$, the condition of ***while*** *holds and the algo-*

rithm does not stop. In the same way, at every step of the algorithm, a set of the approximate bisimulation partition will be split into two sets. Since invariant has no lower bound, we will have the same situation at every step and the algorithm will never stop. Hence, H does not admit a finite bisimulation quotient.

5.4 Model Checking

Despite the absence of a finite bisimulation result for FOCoRe, we can still show, by building upon the decidability of the reachability problem, that a substantial and interesting fragment of CTL can be decided over FOCoRe automata. Since this fragment is not included in LTL, it is not possible to use simulation equivalence to reduce the model.

Given a FOCoRe automaton of dimension k, let $\mathcal{P} = \{P_1[Z], \ldots, P_m[Z]\}$ be a set of atomic propositions whose elements are first-order formulæ over the reals with k free-variables and let $\Phi_{\mathcal{P}}$ be the set of formulæ defined by:

$$Q ::= P[Z] \mid \neg P[Z] \mid Q_1 \vee Q_2 \mid \mathtt{E}\Diamond Q_1 \mid \mathtt{A}\Box Q_1$$

Notice that the formula $\mathtt{E}\Diamond\mathtt{A}\Box P[Z]$, which belongs to $\Phi_{\mathcal{P}}$, distinguishes models which are simulation equivalent. (see [27]).

We define the semantics of the formulæ of $\Phi_{\mathcal{P}}$ by structural induction. Our semantics corresponds to the standard CTL semantics on the transition system defined by the untimed semantics of hybrid automata.

Definition 37 ($\Phi_{\mathcal{P}}$ - Semantics) *Let H be a hybrid automaton. Given a state $\ell = \langle v, r\rangle$ of H, we say that ℓ* satisfies *the $\Phi_{\mathcal{P}}$ formula Q, denoted by $\ell \Vdash Q$, if and only if:*

- *$\ell \Vdash P[Z]$ iff $P[r]$ holds;*
- *$\ell \Vdash Q_1 \vee Q_2$ iff $\ell \Vdash Q_1$ or $\ell \Vdash Q_2$;*
- *$\ell \Vdash \neg Q_1$ iff $\ell \not\Vdash Q_1$;*
- *$\ell \Vdash \mathtt{E}\Diamond Q_1$ iff there exists state ℓ' reachable from ℓ such that $\ell' \Vdash Q_1$;*
- *$\ell \Vdash \mathtt{A}\Box Q_1$ iff for each state ℓ' reachable from ℓ it holds $\ell' \Vdash Q_1$.*

Given a FOCoRe automaton H, an admissible state ℓ and a formula $Q \in \Phi_{\mathcal{P}}$, we can decide $\ell \Vdash Q$ by reducing the problem to the validity problem for a first-order formula as follows.

Definition 38 *Let H be a FOCoRe, Q be a formula of $\Phi_{\mathcal{P}}$, and v be a state of H. We define the first-order formula $\varrho\,(H, Q, v)\,[Z]$ as follows:*

- $\varrho\,(H, P[Z], v)\,[Z]$ *is* $Inv(v)[Z] \wedge P[Z]$;
- $\varrho\,(H, \neg\, P[Z], v)\,[Z]$ *is* $Inv(v)[Z] \wedge \neg P[Z]$;
- $\varrho\,(H, Q_1 \vee Q_2, v)\,[Z]$ *is* $\varrho\,(H, Q_1, v)\,[Z] \vee \varrho\,(H, Q_2, v)\,[Z]$;
- $\varrho\,(H, \mathtt{E}\Diamond\, Q_1, v)\,[Z]$ *is*

$$\bigvee_{ph \in \overline{P}_{\mathcal{E}}(v)} (\exists Z'(\exists T \geq 0\, Reach(H, ph)[Z, Z', T] \;\wedge\; \varrho\,(H, Q_1, u_{ph})\,[Z']));$$

- $\varrho\,(H, \mathtt{A}\Box\, Q_1, v)\,[Z]$ *is*

$$\bigwedge_{ph \in \overline{P}_{\mathcal{E}}(v)} (\forall Z'(\exists T \geq 0\, Reach(H, ph)[Z, Z', T] \twoheadrightarrow \varrho\,(H, Q_1, u_{ph})\,[Z']));$$

where we use $u_{ph} \in \mathcal{V}$ *to denote the last node of* $ph \in \overline{P}_{\mathcal{E}}(v)$.

The following theorem associates the validity of the formula $\varrho\,(H, Q, v)$ with the $\Phi_{\mathcal{P}}$-formula Q.

Theorem 39 *Let H be a FOCoRe automaton and Q be a formula of $\Phi_{\mathcal{P}}$. The formula $\varrho\,(H, Q, v)\,[r]$ holds if and only if $\langle v, r\rangle \Vdash Q$.*

PROOF. The complete proof of the preceding theorem is reported in Appendix on page 57.

We can give some partial results over $\Phi_{\mathcal{P}}$ extended with the operator $\mathtt{EU}$. Consider the following grammar obtained from $\Phi_{\mathcal{P}}$ by adding such an operator.

$$Q ::= P[Z] \mid \neg\, P[Z] \mid Q_1 \vee Q_2 \mid \mathtt{E}\Diamond\, Q_1 \mid \mathtt{A}\Box\, Q_1 \mid \mathtt{E}\,(Q_1 \mathtt{U}\, Q_2)$$

In the rest of this section we will call this language $\Phi_{\mathtt{U},\mathcal{P}}$.

To define the semantics of the until operator we need to introduce the notion of admissible function. If we have $\langle v, r\rangle \rightarrow_C \langle v, s\rangle$, then an admissible function is a continuous function which leads from r to s satisfying the dynamics and invariant conditions.

Definition 40 ((r, s, v) admissible function) *Let H be a hybrid automaton and let $\langle v, r\rangle$ and $\langle v, s\rangle$ be two states of H such $\langle v, r\rangle \rightarrow_C \langle v, s\rangle$. An (r, s, v)* admissible function *is a continuous function $f : [0, t] \rightarrow \mathbb{R}^k$ such that $r = f(0)$, $s = f(t)$, and, for each $t' \in [0, t]$, both $Inv(v)[f(t')]$ and $Dyn(v)[r, f(t'), t']$ hold.*

Notice that, if $\langle v, r\rangle \rightarrow_C \langle v, s\rangle$, there always exists at least one (r, s, v) admissible function.

We only define the until operator, since the remaining is defined as in $\Phi_{\mathcal{P}}$.

Definition 41 ($\Phi_{\mathtt{U},\mathcal{P}}$ - Semantics) *Let H be a hybrid automaton. Given a state $\ell_0 = \langle v_0, r_0\rangle$ of H, we say that ℓ_0* satisfies *the $\Phi_{\mathtt{U},\mathcal{P}}$ formula $Q_1 \mathtt{U}\, Q_2$, denoted by $\ell_0 \Vdash \mathtt{E}\,(Q_1 \mathtt{U}\, Q_2)$, if and only if there exists a trace of the form $\langle v_0, r_0\rangle, \ldots, \langle v_n, r_n\rangle$ such that:*

- *for each $i \in [0, n-1]$ it holds $\langle v_i, r_i\rangle \Vdash Q_1$;*
- *$\langle v_n, r_n\rangle \Vdash Q_2$;*
- *for each $i \in [0, n-1]$ if $\langle v_i, r_i\rangle \rightarrow_C \langle v_{i+1}, r_{i+1}\rangle$, then there is an (r_i, r_{i+1}, v_i) admissible function $f : [0, t] \rightarrow \mathbb{R}^k$ such that for each $t' \in (0, t)$ it holds that $\langle v_i, f(t')\rangle \Vdash Q_1$.*

We can prove the following result.

Theorem 42 *Let $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Reset\rangle$ be a FOCoRe and $v \in \mathcal{V}$ be a location of H. Moreover, let Q_1 and Q_2 be two formulæ of $\Phi_{\mathtt{U},\mathcal{P}}$ and H' be the hybrid automaton $H' = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv', Dyn, Act, Reset\rangle$, where the invariants Inv' are defined as*

$$Inv'(v)[Z] \stackrel{\text{def}}{=} Inv(v)[Z] \wedge (\varrho\,(H, Q_1, v)\,[Z] \vee \varrho\,(H, Q_2, v)\,[Z])$$

for all $v \in \mathcal{V}$ Consider the formula $\overline{\varrho}\,(H, H', \mathtt{E}(Q_1 \mathtt{U}\, Q_2), v)\,[Z]$ defined by

$$\overline{\varrho}\,(H, H', \mathtt{E}(Q_1 \mathtt{U}\, Q_2), v)\,[Z] \stackrel{\text{def}}{=} \left(\exists T \geq 0\, \exists Z' \bigvee_{ph \in \overline{P}_{\mathcal{E}}(v)} Reach(H', ph)[Z, Z', T] \wedge \varrho\,(H, Q_2, u_{ph})\,[Z'] \right)$$

If the automaton H' is a FOCoRe and the formula $\overline{\varrho}\,(H, H', \mathtt{E}(Q_1 \mathtt{U}\, Q_2), v)\,[r]$ holds, then $\langle v, r\rangle \Vdash \mathtt{E}(Q_1 \mathtt{U}\, Q_2)$.

PROOF. The complete proof of the preceding theorem is presented in Appendix on page 57.

If we consider only transitive dynamics (i.e., dynamics which satisfy the formula $Dyn(v)[Z, Z', T] \wedge Dyn(v)[Z', Z'', T'] \rightarrow Dyn(v)[Z, Z'', T + T']$), then we can prove the following result.

Theorem 43 *Let $H = \langle Z, Z', \mathcal{V}, \mathcal{E}, Inv, Dyn, Act, Reset\rangle$ and $v \in \mathcal{V}$ be a H's location. Moreover, let Q_1 and Q_2 be two $\Phi_{\mathtt{U},\mathcal{P}}$ formulæ and H' be the hybrid automaton $\langle Z, Z', \mathcal{V}, \mathcal{E}, Inv', Dyn, Act, Reset\rangle$ where $Inv'(v)[Z] \stackrel{\text{def}}{=} Inv(v)[Z] \wedge \varrho\,(H, Q_1, v)\,[Z]$ for all $v \in \mathcal{V}$. Consider the formula $\widetilde{\varrho}\,(H, H', \mathtt{E}\, Q_1 \mathtt{U}\, Q_2, v)\,[Z]$*

defined by

$$\exists Z'\ \exists T \geq 0\ \Bigg(\Bigg(\forall 0 \leq T' < T\ \exists Z'' \bigvee_{ph \in \overline{P}_{\mathcal{E}}(v)} \bigvee_{ph' \in \overline{P}_{\mathcal{E}}(u_{ph})} (Reach(H', ph)[Z, Z'', T'] \wedge Reach(H, ph')[Z'', Z', T - T'] \wedge \varrho\,(H, Q_2, u_{ph'})\,[Z'])\Bigg) \vee \Bigg(\exists T' > 0\ \forall 0 < T'' \leq T'\ \exists Z'' \bigvee_{ph \in \overline{P}_{\mathcal{E}}(v)} \bigvee_{ph' \in \overline{P}_{\mathcal{E}}(u_{ph})} (Reach(H', ph)[Z, Z', T] \wedge Reach(H, ph')[Z', Z'', T''] \wedge \varrho\,(H, Q_2, u_{ph'})\,[Z''])\Bigg)\Bigg)$$

where we use $u_p \in \mathcal{V}$ to denote the last node of a path p. If H and H' are FOCoRe, the continuous dynamics is transitive, and $\widetilde{\varrho}\,(H, H', \mathtt{E}\,Q_1\mathtt{U}\,Q_2, v)\,[q]$ holds, then $\langle v, q\rangle \Vdash \mathtt{E}\,Q_1\mathtt{U}\,Q_2$.

PROOF. The complete proof of the preceding theorem is presented in Appendix on page 61.

Despite the obvious limitations of the above results, in that they do not guarantee the decidability of $\Phi_{\mathtt{U},\mathcal{P}}$, they still give us sufficient conditions to prove the existence of a trajectory $(\rho_i)_{i\in I}$ leaving a state $\langle v, r\rangle$ such that the properties Q_1 holds on $(\rho_i)_{i\in I}$ until the Q_2 does. Verifying existence of such properties is crucial in safety verification, when we require that a property fails to hold as long as some security states have not been reached. For these reasons, we argue that, even though Theorem 42 and Theorem 43 do not quite succeed in producing a complete algorithm for deciding $\langle v, q\rangle \Vdash \mathtt{E}\,Q_1\mathtt{U}\,Q_2$, they will still prove important in practice, especially in safety verification of FOCoRe.

6 A Biological Application

RNA silencing is a mechanism widely used by eukaryotes to suppress the effects of unwanted gene transcriptions and is believed to have evolved to

provide defense against either viruses or transposons. Thus, like a miniature immune systems, it protects cells from alien genetic materials in three ways: (a) identifying non-self-elements, (b) producing a specific responses, and (c) raising such responses until the threat is cleared.

Bergstrom et al. provide, in [72], a formal model of RNA silencing and identify 4 main actors in the silencing mechanism: mRNA, dsRNA, RNA-induced silencing complex (RISC), and RISC-mRNA complex. In the same papers, the authors also propose the following system of differential equations, obtained from mass-action kinetics laws, to model the evolution of the silencing mechanisms.

$$\begin{aligned}
\dot{D}(t) &= -a * D(t) + g * C(t) \\
\dot{R}(t) &= a * n * D(t) - d_R * R(t) - b * R(t) * M(t) \\
\dot{C}(t) &= b * R(t) * M(t) - (g + d_C * (t)) * C(t) \\
\dot{M}(t) &= h - d_M * M(t) - b * R(t) * M(t)
\end{aligned}$$

where D, R, C, and M represent dsRNA, RISC, RISC-mRNA, and mRNA quantities, respectively, and a, g, d_R, b, d_C, h, and d_M are environmental coefficients which vary because of an assortment of reasons that are left unaccounted for in the model. In particular, it would be more reasonable to assume that the rate of regeneration of dsRNA is not a fixed constant, but varies in a continuous manner with its value ranging in an interval $[g_{\min}, g_{\max}]$ as the system evolves. These ranges may further differ from one transcriptome to another depending on the base composition. Consequently, all possible behavior of the system, modeled as above, cannot be properly inferred from a single simulation.

In order to capture the complete set of behaviors of this biological system, we may approximate its solution by a process, essentially "integrating semi-algebraic hybrid automaton", which roughly mimics the steps of a numerical integration algorithm by using dynamics to simulate step function together with interleaving steps and resets. The resulting automaton is thus equipped with just one location and one transition: its dynamics are finite approximations obtained from a suitably truncated Taylor series and its reset is identity. Notice that since the dynamics are polynomial, they are Hausdorff continuous.

Thus, if we constrain g to vary only within a close interval G, then the set of points, $F[X, G](t)$, reachable from any point X with a generic t-timed continuous evolution is closed. Moreover, for all α and all t, there exists a finite partition, $\mathcal{P}(G)$, of G such that $F[X, \overline{G}](\bar{t})$ is α-paraconvex and

$$F[X, G](\bar{t}) = \bigcup_{\bar{G} \in \mathcal{P}(G)} F[X, \overline{G}](\bar{t}) \tag{2}$$

for all $\overline{G} \in \mathcal{P}(G)$ and all $\bar{t} \in [0, t]$. It follows that $F[X, G]$ is piece-wise in

Michael's form and, by Lemma 25, we can always deduce the existence of a continuous flow from X to Y for any $Y \in F[X, G](t)$. We omit an exhaustive discussion of various topics related to this example and postpone a formal proof of these intuitive observations to future work.

Notice that using α-paraconvexity in place of the —less demanding— convexity in Definition 23, gave us the possibility of partitioning G as above and, ultimately, of proving that the considered system could be represented by a hybrid automaton in Michael's form.

Since the dynamics of the automaton arising in this example models the solution of an ODE, the fact that the reachability can be solved in this approximate sense is not wholly unexpected. However, the systems of the kind, we encountered in the context of modeling RNA silencing, encompass many of the subtle issues that arise quite frequently in systems biology. Note that like RNA silencing, many biological processes evolve to acquire robustness and universality: in other words, these processes work almost equally well for practically all of the genes independent of how these genes and their orthologs in other organisms vary from species to species, and they continue to carry out their functional roles irrespective of how their micro-environments fluctuate. Traditionally, the difficulties, posed to the systems biology models by these structures, are circumvented by grossly simplifying it to a toy model (e.g., certain environmental properties are assumed to hold constant, etc.). However, by building on the hybrid automata model, developed here, it is seen that one can reason about rather realistic models without too coarse a simplification or too idealistic an approximation.

7 Conclusions

In this article, we considered the model checking problem over hybrid automata. We exploited some well known results taken from both logic and analysis and we gave an example of how a tighter interaction between these two mathematical fields can still bring some interesting results in the field of hybrid system verification. As a consequence, we are now convinced that further improvements in this field will only come through a cross-disciplinary consilience of many fields such as logic, analysis, algebra, symbolic computation, algorithms, and computer science. Development of more efficient algorithms to decide polynomial formulæ and proving the decidability of theories such as $\langle \mathbb{R}, 0, 1, +, *, e^x, \geq \rangle$ or $\langle \mathbb{R}, 0, 1, +, *, (f)_{f \in an}, \geq \rangle$ will become the fundamental aims of this emerging field in the future. We will benefit in these efforts if we could identify general analysis results which allow us to reduce continuous reachability to either small formulæ decidability or low complexity methods. Finally, we expect new developments in computer science (e.g.,

symbolic computation, computations modeled by dynamical systems, symbolic model checking, etc.) will harvest such important breakthrough results and discriminatively effective algorithms, which will obviate the mostly futile semi-decidable heuristics that are now in use.

In particular, in this work we considered hybrid automata whose dynamics are inclusion dynamics defined by first-order formulæ. We showed that even if the automaton's dynamics are continuous, we cannot guarantee the existence of a continuous transition satisfying the dynamics themselves. For this reason, we defined a set of conditions which relates the existence of such continuous transition and the truth value of a first-order formula. Since such results are obtained using the selection theorem of Michael [26], we say that a hybrid automaton satisfying such conditions is in Michael's form. If H is a hybrid automaton in Michael's form, then we were able to write the first-order formula $Reach(H, ph)[Z, Z', T]$ which holds if and only if H can reach Z' from Z in time T through a trace whose corresponding path is ph. Exploiting this result, we presented the class of *First Order Constant Reset* automata, *FOCoRe*. A FOCoRe is a first-order hybrid automaton in Michael's form whose resets are constant maps. Aided by the constant reset condition, we were able to prove that we can reduce the general reachability problem over any FOCoRe H to a simpler reachability problem over the traces of length at most equal to the number of H's discrete edges. It follows that the reachability problem for FOCoRe is decidable. We introduced a CTL sub-logic called $\Phi_{\mathcal{P}}$ and we proved that model checking problems expressed within $\Phi_{\mathcal{P}}$ are decidable over FOCoRe. Notice that, since $\Phi_{\mathcal{P}}$ is not preserved by simulation and since there exist FOCoRe having infinite bisimulation quotient, our decidability results cannot be achieved exploiting standard equivalence reduction techniques.

As far as applications of our class of hybrid automata are concerned we briefly discuss some cases coming from Systems Biology. KMA (kinetic mass action) based systems of ODE models have begun to be considered limited in their applicability, and it is now felt that their generalizations require many changes to the representation of the underlying mathematical models. These generalizations must recognize that a biological cell is not a well-mixed system and often involve interactions among small number of molecules (low copy number). They must also account for the enormous amount of uncertainty that exist about their parameters. Such stochasticities, uncertainties, and unmodeled dependencies on local micro-environment, etc. can be expressed in a system allowing for the non-determinism in the flow and easily represented via inclusion formalisms.

Hybrid automata have been already used to model different biological systems (see, e.g., [18,19]). In particular, they facilitate modeling of systems whose laws drastically change during different developmental stages or epochs of a limit cycle (e.g., cell cycle, circadian or ultradian rhythms, etc.). In this context

each phase is modeled through a different state while each phase change corresponds to a discrete edge. The jumps from one phase to another usually occur when the reactants (e.g., morphogens, transcriptional factors, or microRNAs) reach limit values. One could imagine that the resets in these cases should be the identity function. However, it is reasonable to introduce some non-determinism on the jumps, since: (1) the exact jump conditions are not always exactly/ completely known; (2) they can be subject to variations due to external conditions. Hence, constant resets from the activation region to itself are quite natural in this context. The continuous dynamics of each state can be inferred using standard techniques (e.g., Michaelis-Menten, S-systems). Unfortunately, many parameters are necessary to determine a single-function continuous evolution. When some parameters are unknown we can only infer a set of possible continuous evolutions for each state. Applying analysis techniques, such as Taylor approximation method, we can now approximate these continuous evolutions with polynomials, in order to get a FOCoRe model of the system.

Furthermore, biological systems are not time-invariant, nor do they operate in a uniform time-scale. For instance, a cell's behavior is clearly dependent on its time-dependent micro-environment (e.g., where the organism is in its developmental processes, etc.). Thus a model that keeps the systems just general enough can be easily argued to be very prudent, especially in the context of biology. The faster reactions, mediated by a signaling event (e.g., a ligand binding to a receptor) or internal state change (e.g., a flagella switching from a CW rotation to CCW), are easily represented by explicitly including the natural hybrid-ness of the system, although, in this context, they require a need to go beyond the constant reset constraints.

An interesting general technique which uses hybrid automata to model cellular processes has been presented in [73], where the authors proposed a translation of (M, R)-systems [74,75] into hybrid automata. (M, R)-systems model metabolic processes always distinguishing four phases: normal phase, repair phase, replication phase, and mutation phase. In each phase environmental input are involved and the jumps from one phase to another are highly non-deterministic. In the translation proposed in [73] from (M, R)-systems to hybrid automata the dependence from environmental inputs is modeled adding parameters to the continuous dynamics, while the non-deterministic jumps are modeled using constant resets. When the variations of the environmental inputs are not completely known the automata proposed in [73] can be approximated by FOCoRe automata.

In the future, we plan to further study the expressiveness of first-order theories in hybrid automaton context. Since the Michael's form can guarantee the existence of a continuous transition for any kind of first-order dynamic, we would like to investigate the possibility of relaxing it by restricting the specification

theories to o-minimal theories. As a matter of fact, even if Example 20 proves the existence of a continuous map for which there is no continuous selection, such an example does not satisfy o-minimality. Moreover, we are interested in the possibility of exploiting first-order theories over reals with restricted variables over naturals to study synchronization problems over hybrid automata. Finally, we will focus, in the near future, on applying the techniques presented here to study stability of hybrid systems.

References

[1] R. Alur, C. Courcoubetis, T. A. Henzinger, P.-H. Ho, Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems, in: R. L. Grossman, A. Nerode, A. P. Ravn, H. Rischel (Eds.), Hybrid Systems, Vol. 736 of LNCS, Springer-Verlag, 1993, pp. 209–229.

[2] J. E. Hopcroft, J. D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, 1979.

[3] A. Puri, P. Varaiya, Decidability of hybrid systems with rectangular differential inclusions, in: D. L. Dill (Ed.), Proceedings of International Conference on Computer Aided Verification (CAV'94), Vol. 818 of LNCS, Springer-Verlag, 1994, pp. 95–104.

[4] M. Fränzle, Analysis of Hybrid Systems: An ounce of realism can save an infinity of states, in: J. Flum, M. Rodríguez-Artalejo (Eds.), Proceedings of Computer Science Logic (CSL'99), Vol. 1683 of LNCS, Springer-Verlag, 1999, pp. 126–140.

[5] H. Anai, V. Weispfenning, Reach set computations using real quantifier elimination, in: M. D. D. Benedetto, A. Sangiovanni-Vincentelli (Eds.), Proceedings of Hybrid Systems: Computation and Control (HSCC'01), Vol. 2034 of LNCS, Springer-Verlag, 2001, pp. 232–246.

[6] T. Brihaye, C. Michaux, C. Rivière, C. Troestler, On O-Minimal Hybrid Systems, in: R. Alur, G. J. Pappas (Eds.), Proceedings of Hybrid Systems: Computation and Control (HSCC'04), Vol. 2993 of LNCS, Springer-Verlag, 2004, pp. 219–233.

[7] X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, An approach to the description and analysis of hybrid systems, in: R. L. Grossman, A. Nerode, A. P. Ravn, H. Rischel (Eds.), Hybrid Systems, Vol. 736 of LNCS, Springer-Verlag, 1993, pp. 149–178.

[8] R. Alur, C. Courcoubetis, D. Dill, Model-checking in dense real-time, Information and Computation 104 (1) (1993) 2–34.

[9] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine, The algorithmic analysis of hybrid systems, Theoretical Computer Science 138 (1) (1995) 3–34.

[10] P. Tabuada, G. J. Pappas, Model checking ltl over controllable linear systems is decidable., in: O. Maler, A. Pnueli (Eds.), HSCC, Vol. 2623 of LNCS, Springer-Verlag, 2003, pp. 498–513.

[11] R. Milner, An algebraic definition of simulation between programs, Tech. rep., Stanford University (1971).

[12] J. van Benthem, Modal Correspondence Theory, Ph.D. thesis, Department of Mathematics, University of Amsterdam, advisers - M. H. L and S. K. Thomassen (1978).

[13] R. Alur, C. Courcoubetis, N. Halbwachs, D. Dill, H. Wong-Toi, Minimization of timed transition systems (extended abstract), in: Proceedings of the Third International Conference on Concurrency Theory (CONCUR'92), Vol. 630, Springer-Verlag, 1992, pp. 340–354, lNCS.

[14] K. G. Larsen, M. Mikucionis, B. Nielsen, A. Skou, Testing real-time embedded software using uppaal-tron: an industrial case study, in: Proceedings of the Fifth ACM international conference on Embedded software (EMSOFT'05), ACM Press, 2005, pp. 299–306.

[15] J.-R. Abrial, E. Börger, H. Langmaack, The steam boiler case study: Competition of formal program specification and development methods, in: J.-R. Abrial, E. Börger, H. Langmaack (Eds.), Formal Methods for Industrial Applications, Vol. 1165 of LNCS, Springer-Verlag, 1996, pp. 1–12.

[16] M. Archer, C. Heitmeyer, Verifying hybrid systems modeled as timed automata: A case study, in: O. Maler (Ed.), Proceedings of the Conference on Hybrid and Real-Time Systems (HART'97), Vol. 1201 of LNCS, Springer-Verlag, 1997, pp. 171–185.

[17] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, G. M. Miconi, U. Pozzi, T. Villa, H. Wong-Toi, A. L. Sangiovanni-Vincentelli, Maximal safe set computation for idle speed control of an automotive engine, in: N. A. Lynch, B. H. Krogh (Eds.), HSCC, Vol. 1790 of LNCS, Springer-Verlag, 2000, pp. 32–44.

[18] R. Alur, C. Belta, F. Ivancic, V. Kumar, M. Mintz, G. J. Pappas, H. Rubin, J. Schug, Hybrid Modeling and Simulation of Biomolecular Networks, in: Proceedings of Hybrid Systems: Computation and Control (HSCC'01), Vol. 2034 of LNCS, Springer-Verlag, 2001, pp. 19–32.

[19] R. Ghosh, A. Tiwari, C. Tomlin, Automated Symbolic Reachability Analysis; with Application to Delta-Notch Signaling Automata, in: O. Maler, A. Pnueli (Eds.), Proceedings of Hybrid Systems: Computation and Control (HSCC'03), Vol. 2623 of LNCS, Springer-Verlag, 2003, pp. 233–248.

[20] M. Antoniotti, C. Piazza, A. Policriti, M. Simeoni, B. Mishra, Taming the Complexity of Biochemical Models through Bisimulation and Collapsing: Theory and Practice, Theoretical Computer Science 325 (1) (2004) 45–67.

[21] C. Piazza, M. Antoniotti, V. Mysore, A. Policriti, F. Winkler, B. Mishra, Algorithmic Algebraic Model Checking I: Challenges from Systems Biology, in:

K. Etessami, S. K. Rajamani (Eds.), Proceedings Computer Aided Verification (CAV'05), No. 3576 in LNCS, Springer-Verlag, 2005, pp. 5–19.

[22] T. A. Henzinger, P. W. Kopke, A. Puri, P. Varaiya, What's decidable about hybrid automata?, in: Proceedings of the Twenty-Seventh Annual ACM Symposium on the Theory of Computing (STOC '95), ACM Press, 1995, pp. 373–382.

[23] R. Alur, D. L. Dill, A theory of timed automata, Theoretical Computer Science 126 (2) (1994) 183–235.

[24] P. W. Kopke, The theory of rectangular hybrid automata, Ph.D. thesis, Faculty of the Graduate School, Cornell University, advisor - T. A. Henzinger (1996).

[25] G. Lafferriere, G. J. Pappas, S. Sastry, O-Minimal Hybrid Systems, Mathematics of Control, Signals, and Systems 13 (2000) 1–21.

[26] E. Michael, Continuous selections I, Annals of Mathematica 63 (1956) 361–382.

[27] A. Casagrande, C. Piazza, B. Mishra, Semi-Algebraic Constant Reset Hybrid Automata - SACoRe, in: Proceedings of the 44rd Conference on Decision and Control and European Control Conference (CDC-ECC'05), IEEE Computer Society Press, 2005, pp. 678–683.

[28] A. Casagrande, Hybrid Systems: A First-Order Approach to Verification and Approximation Techniques, Ph.D. thesis, Department of Mathematics and Computer Science, University of Udine, Udine, Italy, advisers - Prof. Alberto Policriti and Prof. Tiziano Villa (March 2006).

[29] H. B. Enderton, A Mathematical Introduction to Logic, ii Edition, Harcourt/Academic Press, 2001.

[30] E. Mendelson, Introduction to Mathematical Logic, iv Edition, CRC Press, 1997.

[31] L. van den Dries, C. Miller, Geometric categories and o-minimal structures, Duke Math. Journal 84 (1996) 497–540.

[32] L. van den Dries, Tame topology and O-minimal structures, Vol. 248 of London Mathematical Society Lecture Note Series, Cambridge University Press, 1998.

[33] A. Tarski, A Decision Method for Elementary Algebra and Geometry, Univ. California Press, 1951.

[34] G. E. Collins, Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition, in: Proceedings of the Second GI Conference on Automata Theory and Formal Languages, Vol. 33 of LNCS, Springer-Verlag, 1975, pp. 134–183.

[35] D. Grigorév, Complexity of deciding tarski algebra, Journal of Symbolic Computation 5 (1-2) (1988) 65–108.

[36] D. Grigorév, N. Vorobjov, Counting connected components of a semialgebraic set in subexponential time, Computational Complexity 2 (2) (1992) 133–186.

[37] J. Renegar, On the computational complexity and geometry of the first-order theory of the reals. Part I: Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals, Journal of Symbolic Computation 13 (3) (1992) 255–299.

[38] J. Renegar, On the computational complexity and geometry of the first-order theory of the reals. Part II: The general decision problem. Preliminaries for quantifier elimination, Journal of Symbolic Computation 13 (3) (1992) 301–327.

[39] J. Renegar, On the computational complexity and geometry of the first-order theory of the reals. Part III: Quantifier elimination, Journal of Symbolic Computation 13 (3) (1992) 329–352.

[40] S. Basu, Algorithms in semi-algebraic geometry, Ph.D. thesis, Department of Computer Science, New York University, adviser - Richard Pollack (1996).

[41] S. Basu, An improved algorithm for quantifier elimination over real closed fields, in: Proceedings of the Thirty-Eighth Annual Symposium on Foundations of Computer Science (FOCS '97), IEEE Computer Society Press, 1997, pp. 56–65.

[42] S. Basu, R. Pollack, M.-F. Roy, On the combinatorial and algebraic complexity of quantifier elimination, Journal of the Association for Computing Machinery 43 (6) (1996) 1002–1045.

[43] B. Mishra, Algorithmic Algebra, Springer-Verlag New York, Inc., 1993.

[44] B. Mishra, Computational real algebraic geometry, in: J. E. Goodman, J. O'Rourke (Eds.), Handbook of Discrete and Computational Geometry: (Second Edition), CRC Press, Boca Raton, FL, 2004, pp. 740–764.

[45] J. Canny, Some algebraic and geometric computations in PSPACE, in: Proceedings of the Twentieth annual ACM symposium on Theory of computing (STOC '88), ACM Press, 1988, pp. 460–469.

[46] J. Canny, Improved algorithms for sign determination and existential quantifier elimination, The Computer Journal 36 (5) (1993) 409–418.
URL `citeseer.ist.psu.edu/canny93improved.html`

[47] L. van den Dries, A generalization of the Tarski-Seidenberg theorem and some nondefinability results, Bulletin of American Mathematical Society (New Series) 15 (2) (1986) 189–193.

[48] A. G. Khovanskiĭ, On a class of systems of transcendental equations, Soviet Math. Dokl. 22 (1980) 762–765.

[49] J. Denef, L. van den Dries, p-adic and real subanalytic sets, Annals of Mathematica 128 (1) (1988) 79–138.

[50] L. van den Dries, A. Macintyre, D. Marker, The elementary theory of restricted analytic functions with exponentiation, Annals of Mathematica 140 (1) (1994) 183–205.

[51] A. J. Wilkie, Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function, Journal of the American Mathematical Society 9 (4) (1996) 1051–1094.

[52] A. Macintyre, A. J. Wilkie, On the decidability of the real exponential field, in: P. G. Odifreddi (Ed.), Kreiseliana, about and around Georg Kreisel, A. K. Peters, 1996, pp. 441–467.

[53] G. V. Chudnovsky, Contributions to the Theory of Transcendental Numbers, No. 19 in Mathematical Surveys and Monographs, American Mathematical Society, 1984.

[54] A. Macintyre, Schanuel's conjecture and free exponential rings., Annals of Pure and Applied Logic 51 (3) (1991) 241–246.

[55] L. van den Dries, C. Miller, On the real exponential field with restricted analytic functions, Israel Journal of Mathematics 85 (1-3) (1994) 19–56.

[56] J.-M. Lion, J.-P. Rolin, Théorème de préparation pour les fonctions logarithmico-exponentielles, Annales de l'institut Fourier 47 (3) (1997) 859–884.

[57] A. J. Wilkie, A theorem of the complement and some new O-minimal structures, Selecta Mathematica, New Series 5 (4) (1999) 397–421.

[58] O. Maler, Z. Manna, A. Pnueli, From timed to hybrid systems, in: J. W. de Bakker, C. Huizing, W. P. de Roever, G. Rozenberg (Eds.), Real-Time: Theory in Practice, Vol. 600, Springer-Verlag, 1991, pp. 447–484.
URL `citeseer.nj.nec.com/maler92from.html`

[59] T. A. Henzinger, P. W. Kopke, State Equivalences for Rectangular Hybrid Automata, in: U. Montanari, V. Sassone (Eds.), Proceedings of International Conference on Concurrency Theory (Concur'96), Vol. 1119 of LNCS, Springer-Verlag, 1996, pp. 530–545.

[60] T. A. Henzinger, The Theory of Hybrid Automata, in: Proceedings of the Eleventh Symposium on Logic in Computer Science (LICS'96), IEEE Computer Society Press, 1996, pp. 278–292.

[61] J. Lygeros, K. H. Johansson, S. N. Simić, J. Zhang, S. Sastry, Continuity and invariance in hybrid automata, in: Proceedings of the Fortieth IEEE Conference on Decision and Control (CDC '01), IEEE Computer Society Press, 2001, pp. 340–345.

[62] H. B. Callen, Thermodynamics, John Wiley & Sons, Inc., 1960.

[63] E. Fermi, Thermodynamics, Dover Publications, 1937.

[64] E. M. Clarke, O. Grumberg, D. A. Peled, Model checking, MIT Press, 1999.

[65] R. Alur, T. Dang, F. Ivancic, Reachability analysis of hybrid systems via predicate abstraction., in: C. Tomlin, M. R. Greenstreet (Eds.), Hybrid Systems: Computation and Control, 5th International Workshop, HSCC 2002, March 25-27, 2002, Proceedings, Vol. 2289 of LNCS, Springer-Verlag, 2002, pp. 35–48.

[66] A. Tiwari, G. Khanna, Series of Abstraction for Hybrid Automata, in: C. Tomlin, M. R. Greenstreet (Eds.), Hybrid Systems: Computation and Control, 5th International Workshop, HSCC 2002, March 25-27, 2002, Proceedings, Vol. 2289 of LNCS, Springer-Verlag, 2002, pp. 465–478.

[67] J. P. Aubin, A. Cellina, Differential Inclusions, Vol. 264 of A Series of Comprehensive Studies in Mathematics, Springer-Verlag, 1984.

[68] M. Safonov, The abstract Cauchy-Kovalevskaya theorem in a weighted Banach space, Communications on Pure and Applied Mathmatics 48 (1995) 629–643.

[69] G. Lafferriere, G. J. Pappas, S. Yovine, Symbolic Reachability Computation for Families of Linear Vector Fields, Journal of Symbolic Computation 32 (3) (2001) 231–253.

[70] T. Jech, The Axiom of Choice, North Holland, 1973.

[71] E. Michael, Paraconvex sets, Mathematica Scandinavica 7 (2) (1959) 372–375.

[72] R. A. Carl T. Bergstrom, Erin McKittrick, Mathematical models of rna silencing: Unidirectional amplification limits accidental self-directed reactions, PNAS 100 (10) (2003) 11511–11516.

[73] K. H. Cho, K. H. Johansson, O. Wolkenhauer, A hybrid systems framework for cellular processes, BioSystems 80 (2005) 273–282.

[74] R. Rosen, Some realizations of (m,r)-systems and their interpretation, Bull. Math. Biophys. 33 (1971) 303–319.

[75] J. L. Casti, The theory of metabolism-repair systems, Appl. Math. Comput. 28 (1988) 113–154.

Appendix

Proof of Theorem 30

PROOF. ($\Leftarrow$) If there exists a path such that $\exists T \geq 0\, \mathit{Reach}(H, ph)[r, s, T]$ holds, then, by definition of *Reach*, $\exists T \geq 0\, \overline{\mathit{Reach}}(H, ph)[r, Z^1, \ldots, Z^{2|ph|}, s, T]$ is satisfiable and, by Lemma 27, r reaches s in H.

($\Rightarrow$) Conversely, if $s \in \mathit{ReachSet}(r)$, by Lemma 27, there exists a path ph such that the formula $\exists T \geq 0\, \overline{\mathit{Reach}}(H, ph)[r, Z^1, \ldots, Z^{2|ph|}, s, T]$ is satisfiable; let ph be one such path of minimal length. Thus, by definition of *Reach*, the formula $\exists T \geq 0\, \mathit{Reach}(H, ph)[r, s, T]$ holds. Moreover, if the length of ph is less than or equal to $|\mathcal{E}|$, then $ph \in \overline{P}_{\mathcal{E}}$ and we are done. If, on the other hand, ph is longer than $|\mathcal{E}|$, then ph is of the form $\langle v_0, v_1, \ldots, v_h \rangle$ with $h > |\mathcal{E}|$. Hence, by the pigeonhole principle applied to edges, there must exist at least

one repeated subsequence v_i, v_{i+1} in ph. Let ph' be the path obtained from ph by removing all such repetitions, i.e.: if in ph there is a subsequence of the form $v_i, v_{i+1}, \ldots, v_j, v_{j+1}, v_{j+2}$, with $v_i = v_j$ and $v_{i+1} = v_{j+1}$, then we replace it with v_i, v_{i+1}, v_{j+2}. Since we can show that ph' satisfies all the requirements and since it is strictly shorter than ph, we derive a contradiction. In the following, we prove that $\exists T \geq 0\, \overline{Reach}(H, ph')[r, \ldots, s, T]$ is satisfiable. It is sufficient to prove the thesis in the case ph' has been obtained from ph with only one removal. Let ph be of the form $v_0, \ldots, v_i, v_{i+1}, \ldots, v_j, v_{j+1}, v_{j+2}, \ldots, v_h$ with $v_i = v_j$ and $v_{i+1} = v_{j+1}$ and ph' be $v_0, \ldots, v_i, v_{i+1}, v_{j+2}, v_h$. The formula $\overline{Reach}(H, ph)[r, \ldots, s, T]$ is of the form:

$$
\begin{aligned}
\exists T_0 \geq 0, \ldots, T_h \geq 0 \Bigg(T = \sum_{l=0}^{h} T_l \ \wedge \ & C\text{-}Reach(H, v_0)[r, Z^1, T_0] \wedge \\
& \ldots \\
& C\text{-}Reach(H, v_i)[Z^{2i}, Z^{2i+1}, T_i] \wedge \\
& D\text{-}Reach(H, \langle v_i, v_{i+1} \rangle)[Z^{2i+1}, Z^{2(i+1)}] \wedge \\
& \ldots \\
& C\text{-}Reach(H, v_j)[Z^{2j}, Z^{2j+1}, T_j] \wedge \\
& D\text{-}Reach(H, \langle v_j, v_{j+1} \rangle)[Z^{2j+1}, Z^{2(j+1)}] \wedge \\
& C\text{-}Reach(H, v_{j+1})[Z^{2(j+1)}, Z^{2(j+1)+1}, T_{j+1}] \wedge \\
& D\text{-}Reach(H, \langle v_{j+1}, v_{j+2} \rangle)[Z^{2(j+1)+1}, Z^{2(j+2)}] \wedge \\
& \ldots \\
& C\text{-}Reach(H, v_h)[Z^{2h}, s, T_h] \Bigg)
\end{aligned}
$$

while the formula $\overline{Reach}(H, ph')[r, \ldots, s, T]$ is of the form:

$$
\begin{aligned}
& \exists T_0 \geq 0, \ldots, T_{i+1} \geq 0 \\
& \quad \exists T_{j+2} \geq 0, \ldots, T_h \geq 0 \Bigg(T = \left(\sum_{l=0}^{i+1} T_l + \sum_{l=j+2}^{h} T_l \right) \ \wedge \\
& \qquad C\text{-}Reach(H, v_0)[r, Z^1, T_0] \wedge \\
& \qquad \ldots \\
& \qquad C\text{-}Reach(H, v_i)[Z^{2i}, Z^{2i+1}, T_i] \wedge \\
& \qquad D\text{-}Reach(H, \langle v_i, v_{i+1} \rangle)[Z^{2i+1}, Z^{2(i+1)}] \wedge \\
& \qquad C\text{-}Reach(H, v_{i+1})[Z^{2(i+1)}, Z^{2(i+1)+1}, T_{i+1}] \wedge \\
& \qquad D\text{-}Reach(H, \langle v_{i+1}, v_{j+2} \rangle)[Z^{2(i+1)+1}, Z^{2(j+2)}] \wedge \\
& \qquad \ldots \\
& \qquad C\text{-}Reach(H, v_h)[Z^{2h}, s, T_h] \Bigg)
\end{aligned}
$$

where we keep the indexing of ph from $j+2$ to $2h$.

Let us assume that $\exists T \geq 0\, \overline{Reach}(H, ph)[r, \ldots, s, T]$ can be satisfied by replacing Z^a with z^a for each $a \leq 2h$. To satisfy $\exists T \geq 0\, \overline{Reach}(H, ph')[r, \ldots, s, T]$ we replace Z^a by z^a for each $a \neq 2(i+1), 2(i+1)+1$. Moreover, we replace $Z^{2(i+1)}$ by $z^{2(j+1)}$ and $Z^{2(i+1)+1}$ by $z^{2(j+1)+1}$. In the following part of the proof, we prove that such a replacement satisfies $\exists T \geq 0\, \overline{Reach}(H, ph')[r, \ldots, s, T]$. Since the first replacement satisfies $\exists T \geq 0\, \overline{Reach}(H, ph)[r, \ldots, s, T]$, we have that both the formulæ

$$Inv(v_i)[z^{2i+1}] \wedge Act(\langle v_i, v_{i+1}\rangle)[z^{2i+1}] \wedge \\ Reset(\langle v_i, v_{i+1}\rangle)[z^{2(i+1)}] \wedge Inv(v_{i+1})[z^{2(i+1)}]$$

and

$$Inv(v_i)[z^{2j+1}] \wedge Act(\langle v_i, v_{i+1}\rangle)[z^{2j+1}] \wedge \\ Reset(\langle v_i, v_{i+1}\rangle)[z^{2(j+1)}] \wedge Inv(v_{i+1})[z^{2(j+1)}]$$

hold. It follows that

$$Inv(v_i)[z^{2i+1}] \wedge Act(\langle v_i, v_{i+1}\rangle)[z^{2i+1}] \wedge \\ Reset(\langle v_i, v_{i+1}\rangle)[z^{2(j+1)}] \wedge Inv(v_{i+1})[z^{2(j+1)}]$$

also holds, thus $D\text{-}Reach(H, \langle v_i, v_{i+1}\rangle)[z^{2i+1}, z^{2(j+1)}]$ holds. The rest of the proof follows from the fact that the replacement satisfies the formula

$$\exists T \geq 0\, \overline{Reach}(H, ph)[r, \ldots, s, T]$$

Hence $\exists T \geq 0\, \overline{Reach}(H, ph')[r, \ldots, s, T]$ is satisfiable, and the formula $\exists T \geq 0\, Reach(H, ph')[r, s, T]$ holds, by definition of $Reach$. □

Proof of Lemma 33

PROOF. To prove that H_{inf} is a FOCoRe automaton, we need to show that it is in Michael's form and that its resets are constant. To prove the condition required by the definition of Michael's form, we have to prove that for each $v \in \mathcal{V}$ and $p = (p_1, p_2) \in \mathbb{R}^2$ such that $Inv(v)[p]$ holds, the function $F^H_{v,p}$ is lower semi-continuous and, for all $t \in I^H_{v,p}$, $F^H_{v,p}(t)$ is a closed and convex set. As we have defined H_{inf}, for all $t \in \mathbb{R}_{\geq 0}$, $Dyn(v)[p, Z', t]$ is $Z'_2 \geq p_2 Z'_1 + p_2(1 - p_1) \wedge Z'_2 \geq -p_2 Z'_1 + p_2(1 + p_1) \wedge \|Z' - p\| \leq t$, where $Z' = (Z'_1, Z'_2)$. Thus for all $t \in \mathbb{R}_{\geq 0}$ and all $p \in \mathbb{R}^2$, $Dyn(v)[p, p, t]$ holds and, if $Inv(v)[p]$ holds, for all $t \in \mathbb{R}_{\geq 0}$, $Dyn(v)[p, p, t] \wedge Inv(v)[p]$ holds too. Hence, for all $t \in \mathbb{R}_{\geq 0}$, the formula $\exists Z'\ (Dyn(v)[p, Z', t] \wedge Inv(v)[Z'])$ holds. It follows that $I^H_{v,p} = [0, +\infty)$. We now prove that $F^H_{v,p}$ is convex. For all $t \in I^H_{v,p}$,

$F^H_{v,p}$ is such that $F^H_{v,p}(t) = \{q \mid Dyn(v)[p,q,t] \wedge Inv(v)[q]\}$, where $q = (q_1, q_2)$. Hence, by Dyn's definition, $F^H_{v,p}(t) = Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v)) \cap Sat(\|p - Z\| \leq t)$. Since the intersection of convex sets is convex, to deduce the convexity of $F^H_{v,p}(t)$, we will prove the convexity of $Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$, and $Sat(\|p - Z\| \leq t)$. A set S is convex if and only if for all $q, \bar{q} \in S$, all points of the segment between q and $\bar{q}$ are contained in S. The convexity of $Sat(\|p - Z\| \leq t)$ is obvious, hence we have to prove the convexity of $Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$. In particular, we need to prove that for all $p = (p_1, p_2)$, $q = (q_1, q_2)$, $r = (r_1, r_2) \in \mathbb{R}^2$, and for all $\alpha \in [0,1]$, if $q,\ r \in Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$ then $(s_1, s_2) \in Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$, where $s_1 = (1-\alpha)q_1 + \alpha r_1$ and $s_2 = (1-\alpha)q_2 + \alpha r_2$. If $q \in Sat(up\,[p,Z] \wedge up'\,[p,Z])$ then $q_2 \geq p_2 q_1 + p_2(1-p_1) \wedge q_2 \geq -p_2 q_1 + p_2(1+p_1)$ and if $r \in Sat(up\,[p,Z] \wedge up'\,[p,Z])$ then $r_2 \geq p_2 r_1 + p_2(1-p_1) \wedge r_2 \geq -p_2 r_1 + p_2(1+p_1)$. Thus:

$$\begin{aligned} s_2 &= (1-\alpha)q_2 + \alpha r_2 \\ &\geq (1-\alpha)\left(p_2 q_1 + p_2(1-p_1)\right) + \alpha\left(p_2 r_1 + p_2(1-p_1)\right) \\ &\geq p_2\left((1-\alpha)q_1 + \alpha r_1\right) + p_2(1-p_1)\left((1-\alpha) + \alpha\right). \end{aligned}$$

But, $s_1 = (1-\alpha)q_1 + \alpha r_1$ hence:

$$\begin{aligned} s_2 &\geq p_2\left((1-\alpha)q_1 + \alpha r_1\right) + p_2(1-p_1)\left((1-\alpha) + \alpha\right) \\ &\geq p_2\left((1-\alpha)q_1 + \alpha r_1\right) + p_2(1-p_1) \\ &\geq p_2 s_1 + p_2(1-p_1). \end{aligned}$$

Symmetrically:

$$\begin{aligned} s_2 &= (1-\alpha)q_2 + \alpha r_2 \\ &\geq (1-\alpha)\left(p_2(1+p_1) - p_2 q_1\right) + \alpha\left(p_2(1+p_1) - p_2 q_1\right) \\ &\geq -p_2\left((1-\alpha)q_1 + \alpha r_1\right) + p_2(1+p_1)\left((1-\alpha) + \alpha\right) \\ &\geq -p_2 s_1 + p_2(1+p_1), \end{aligned}$$

thus, for all s lying on the segment between q and r, the formula $up\,[p,s] \wedge up'\,[p,s]$ holds. Moreover, if $Inv(v)[q]$ and $Inv(v)[r]$ then $-1 \leq q_1 \leq 1 \wedge q_2 > 0$ and $-1 \leq r_1 \leq 1 \wedge r_2 > 0$, thus $s_2 = (1-\alpha)q_2 + \alpha r_2 \geq (1-\alpha)0 + \alpha 0 \geq 0$. Furthermore, $s_1 = (1-\alpha)q_1 + \alpha r_1 \geq -(1-\alpha) - \alpha \geq -1$ and $s_1 = (1-\alpha)q_1 + \alpha r_1 \leq (1-\alpha) + \alpha \leq 1$ and hence, for all s belonging to the segment between q and r, the formula $Inv(v)[s]$ holds. Thus for all $q, r \in Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$ and for all s belonging to the segment between q and r, $s \in Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v))$. Hence we have demonstrated the convexity of $F^H_{v,p}(t)$.

We now prove that $F^H_{v,p}$ is lower semi-continuous. By Definition 17, $F^H_{v,p}$ is lower semi-continuous if and only if for all $q \in F^H_{v,p}(t)$ and for all neighborhoods $U_{q,\epsilon} = \{q' \mid \|q' - q\| < \epsilon\}$ of q there exists a neighborhood $U_{t,\delta} = \{t' \mid |t' - t| < \delta\}$

of t such that $\forall t' \in U_{t,\delta}$ the set $(F^H_{v,p}(t') \cap U_{q,\epsilon})$ is not empty. Now we prove that, for all $q \in F^H_{v,p}(t)$ and for all $\epsilon > 0$, $\delta = \frac{\epsilon}{2}$ is such that $\forall t' \in U_{t,\delta}$ $r \in (F^H_{v,p}(t') \cap U_{q,\epsilon})$, where r is the point in the segment between p and q such that $\|r-q\| = \frac{2\epsilon}{3}$. Since $F^H_{v,p}(t)$ is convex and both q and p are in $F^H_{v,p}(t)$, then $r \in F^H_{v,p}(t)$. Notice that, since $F^H_{v,p}(t) = Sat(up\,[p,Z] \wedge up'\,[p,Z] \wedge Inv(v)) \cap Sat(\|p-Z\| \leq t)$, it holds that if $t' \geq t$, then $F^H_{v,p}(t') \supseteq F^H_{v,p}(t)$. Thus if $t' \geq t$, then $r \in F^H_{v,p}(t')$. So assume that $t' < t$. By definition of r, it follows directly that $\|r-q\| + \|p-r\| = \|p-q\|$. Moreover, since by hypothesis $q \in F^H_{v,p}(t)$, $\|p-q\| \leq t$. Hence $\frac{2\epsilon}{3} + \|p-r\| \leq t$ holds, but this formula holds if and only if $\|p-r\| \leq t - \frac{2\epsilon}{3}$. Furthermore, by hypothesis $\|t'-t\| < \frac{\epsilon}{2}$ and $t' < t$, thus $t < t' + \frac{\epsilon}{2}$. It follows that $\|p-r\| \leq t - \frac{2\epsilon}{3} < t' - \frac{\epsilon}{6}$. But $\epsilon > 0$ then $\|p-r\| \leq t'$. Moreover, since $r \in F^H_{v,p}(t)$, the formula $up\,[p,r] \wedge up'\,[p,r] \wedge Inv(v)[r]$ holds. Hence $r \in Sat(up\,[p,Z] \wedge up'\,[p,Z] \wedge Inv(v)) \cap Sat(\|p-Z\| \leq t') = F^H_{v,p}(t')$ and the function $F^H_{v,p}$ is lower semi-continuous. We now need to prove that, for all p and for all $t \in I^H_{v,p}$, the set $F^H_{v,p}(t)$ is closed. By definition, $F^H_{v,p}(t) = Sat(up\,[p,Z] \wedge up'\,[p,Z]) \cap Sat(Inv(v)) \cap Sat(\|p-Z\| \leq t)$. By definition of our automaton, if $p = (p_1,p_2)$ and $q = (q_1,q_2)$, then $up\,[p,q] \wedge up'\,[p,q]$ is $q_2 \geq p_2 q_1 + p_2(1-p_1) \wedge q_2 \geq -p_2 q_1 + p_2(1+p_1) \wedge \|p-q\| \leq t$. Moreover, the formula $q_2 \geq -p_2 q_1 + p_2(1+p_1)$ holds if and only if $p_2 q_1 \geq -q_2 + p_2(1+p_1)$ holds. Thus, from $Dyn(v)[p,q,t]$, it follows that:

$$\begin{aligned} q_2 &\geq p_2 q_1 + p_2(1-p_1) \\ &\geq -q_2 + p_2(1+p_1) + p_2(1-p_1) \\ &\geq -q_2 + 2p_2, \end{aligned}$$

and then $q_2 \geq p_2$. Since $Inv(v)[q]$ is $-1 \leq q_1 \leq 1 \wedge q_2 > 0$ and $q_2 > p_2 \wedge Inv(v)[p]$ implies $q_2 > 0$, for all $p \in \mathbb{R}^2$ such that $Inv(v)[p]$ and for all $t \in I^H_{v,p}$, $F^H_{v,p}(t) = \{q \,|\, q_2 \geq p_2 q_1 + p_2(1-p_1) \wedge q_2 \geq -p_2 q_1 + p_2(1+p_1) \wedge -1 \leq q_1 \leq 1 \wedge \|p-q\| \leq t\}$, where $q = (q_1,q_2)$. Hence, since $F^H_{v,p}(t)$ is an intersection of closed sets, $F^H_{v,p}(t)$ is a closed set. It follows that $H_{\inf}$ is a FOCoRe automaton. □

Lemma 44 *For the automaton H_{inf}, if the formula $Inv(v)[p]$ holds then, for each $t \in \mathbb{R}_{\geq 0}$, $\psi(H,v)[p,t]$ holds.*

PROOF. By definition, $\psi(H,v)[p,t]$ is $\forall 0 \leq T' \leq t\ \exists Z' Dyn(v)[p,Z',T'] \wedge Inv(v)[Z']$. Moreover, by $H_{\inf}$'s definition, $Dyn(v)[p,Z',T]$ is $Z'_2 \geq p_2 Z'_1 + p_2(1-p_1) \wedge Z'_2 \geq -p_2 Z'_1 + p_2(1+p_1) \wedge \|p-Z'\| \leq T$ and $Inv(v)[p]$ is $-1 \leq p_1 \leq 1 \wedge p_2 > 0$, where $p = (p_1,p_2)$ and $Z' = (Z'_1, Z'_2)$. It follows that, for all $t \in \mathbb{R}_{\geq 0}$, $Dyn(v)[p,p,t]$ holds. Thus if $Inv(v)[p]$ holds then, for all $t \in \mathbb{R}_{\geq 0}$, $\exists Z' Dyn(v)[p,Z',t] \wedge Inv(v)[Z']$ holds. Hence, by definition of the formula $\psi(H,v)[p,t]$, if $Inv(v)[p]$ holds then, for all $t \in \mathbb{R}_{\geq 0}$, $\psi(H,v)[p,t]$ holds too. □

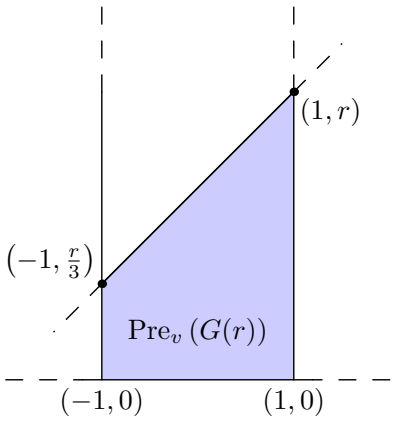


Figure .1. The gray colored points are in $\mathrm{Pre}_v\,(G(r))$.

Lemma 45 *Let* $G(r) = \{(p_1, p_2) \mid p_1 = 1 \wedge 0 < p_2 \leq r\} \subseteq \mathbb{R}^2$. *For the automaton* H_{inf}, $Pre_v\,(G(r)) = \{p \mid 3p_2 \leq r(p_1 + 2) \wedge Inv(v)[p]\}$, *where* $p = (p_1, p_2)$ *and* $v \in \mathcal{V}$.

PROOF. By definitions, $G(r) = \{(p_1, p_2) \mid p_1 = 1 \wedge 0 < p_2 \leq r\}$ and $Inv(v)[(p_1, p_2)]$ is $p_2 > 0 \wedge -1 \leq p_1 \leq 1$. Hence, each point p in $G(r)$ is such that $Inv(v)[p]$ and then, by Lemma 44 for each $t \in \mathbb{R}_{\geq 0}$ it holds that $\psi(H, v)[p, t]$. Thus, from Theorem 26, it follows that $\mathrm{Pre}_v\,(G(r)) = \{p \in \mathbb{R}^2 \mid \exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[p, q, T] \wedge Inv(v)[p]\}$. We can now prove that for all $(p_1, p_2) \in \mathcal{I}(v)$ the formula $\exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[(p_1, p_2), q, T]$ holds if and only if $p_2 \leq \frac{r}{3}(p_1 + 2)$ holds. We proceed as follows: first we show that, for all $(p_1, p_2) \in \mathcal{I}(v)$, if $p_2 \leq \frac{r}{3}(p_1 + 2)$ does not hold then neither does $\exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[(p_1, p_2), q, T]$ (claim 1); next we show that, for all $(p_1, p_2) \in \mathcal{I}(v)$, $\neg\,(\exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[(p_1, p_2), q, T])$ implies the formula $p_2 > \frac{r}{3}(p_1 + 2)$ (claim 2).

(1) By definition, $Dyn(v)[p, q, T]$ is $q_2 \geq p_2 q_1 + p_2(1 - p_1) \wedge q_2 \geq -p_2 q_1 + p_2(1 + p_1) \wedge \|p - q\| \leq T$. Thus, if, for the sake of contradiction, we assume that both conditions, $p_2 > \frac{r}{3}(p_1 + 2)$ and $\exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[(p_1, p_2), q, T]$, hold then:

$$q_2 \geq p_2 q_1 + p_2(1 - p_1) > \frac{r}{3}(p_1 + 2)\,(q_1 + (1 - p_1))$$

Since $(q_1, q_2) \in G(r)$ and $(p_1, p_2) \in \mathcal{I}(v)$, it follows that $q_1 = 1$ and $p_1 \leq 1$ hence:

$$\begin{aligned} q_2 &> \frac{r}{3}(p_1 + 2)\,(q_1 + (1 - p_1)) > \frac{r}{3}(p_1 + 2)(2 - p_1) \\ &> \frac{r}{3}(4 - p_1^2) > \frac{r}{3}(4 - 1) > r \end{aligned}$$

But, by definition, $G(r) = \{(q_1, q_2) \mid q_1 = 1 \wedge 0 < q_2 \leq r\}$. Hence, the equation above contradicts our initial hypothesis. Thus, for all $(p_1, p_2) \in$

$\mathcal{I}(v)$, if $p_2 > \frac{r}{3}(p_1+2)$ holds then $\exists q \in G(r)\ \exists T \geq 0\ Dyn(v)[(p_1,p_2),q,T]$ does not.

(2) By definition, $Dyn(v)[p,q,T]$ is $q_2 \geq p_2q_1 + p_2(1-p_1) \wedge q_2 \geq -p_2q_1 + p_2(1+p_1) \wedge \|p-q\| \leq T$, and if, for the sake of contradiction, we assume that both formulæ $\forall q \in G(r)\ \forall T \geq 0\ \neg Dyn(v)[p,q,T]$ and $p_2 \leq \frac{r}{3}(p_1+2)$ hold then either $q_2 < p_2q_1 + p_2(1-p_1)$, $q_2 < -p_2q_1 + p_2(1+p_1)$ or $\forall q \in G(r) \forall T \geq 0\, \|p-q\| > T$. If the formula $q_2 < p_2q_1 + p_2(1-p_1)$ holds then:

$$q_2 < p_2q_1 + p_2(1-p_1) < \frac{r}{3}(p_1+2)\,(q_1+(1-p_1))$$

Since $(q_1,q_2) \in G(r)$ and $(p_1,p_2) \in \mathcal{I}(v)$, it follows that $q_1 = 1$ and $p_1 \geq -1$ hence:

$$\begin{aligned} q_2 &< \frac{r}{3}(p_1+2)\,(q_1+(1-p_1)) < \frac{r}{3}(p_1+2)(2-p_1) \\ &< \frac{r}{3}(4-p_1^2) < \frac{r}{3}(4-1) < r \end{aligned}$$

But, by definition, $G(r) = \{(q_1,q_2) \mid q_1 = 1 \wedge 0 < q_2 \leq r\}$ and, in particular, $(1,r) \in G(r)$. Hence, the formula $q_2 < p_2q_1 + p_2(1-p_1)$ contradicts our hypothesis.

Let us assume that the formula $q_2 < -p_2q_1 + p_2(1+p_1)$ holds. Since $(q_1,q_2) \in G(r)$ and $(p_1,p_2) \in \mathcal{I}(v)$, by hypothesis, $q_1 = 1$ and $p_1 \leq 1$. It follows that

$$q_2 < -p_2q_1 + p_2(1+p_1) < -p_2 + p_2(1+1) = p_2$$

Moreover, the formula $p_2 \leq \frac{r}{3}(p_1+2)$ holds by hypothesis, thus

$$q_2 < p_2 \leq \frac{r}{3}(p_1+2) \leq \frac{r}{3} = r$$

But by definition, $G(r) = \{(q_1,q_2) \mid q_1 = 1 \wedge 0 < q_2 \leq r\}$ and, in particular, $(1,r) \in G(r)$. Hence, the formula $q_2 < -p_2q_1 + p_2(1+p_1)$ contradicts our hypothesis.

Let us first assume that $\forall q \in G(r) \forall T \geq 0\, \|p-q\| > T$ holds. Let us over-estimate the maximum of $\|p-q\|$ when $p \in \mathcal{I}(v)$, $q \in G(r)$, and $p_2 \leq \frac{r}{3}(p_1+2)$.

$$\begin{aligned} \max \|p-q\| &\leq \max \sqrt[2]{(p_1-q_1)^2 + (p_2-q_2)^2} \\ &\leq \sqrt[2]{\max(p_1-q_1)^2 + \max(p_2-q_2)^2} \\ &\leq \sqrt[2]{\max(\max p_1 - \min q_1, \min p_1 - \max q_1)^2 + \max(p_2-q_2)^2} \end{aligned}$$

Since $(q_1,q_2) \in G(r)$, $(p_1,p_2) \in \mathcal{I}(v)$, and $p_2 \leq \frac{r}{3}(p_1+2)$ by hypothesis,

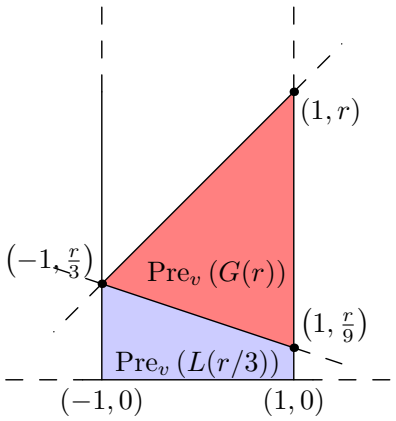


Figure .2. The lighter gray colored points are in $\mathrm{Pre}_v\,(L(r/3))$.

it follows that $q_1 = 1$, $q_2 \in (0, r]$, $p_1 \in [-1, 1]$, and $p_2 > 0$. Moreover:

$$p_2 \leq \frac{r}{3}\,(p_1 + 2) \leq \frac{r}{3}\,(1 + 2) = r$$

Thus:

$$\begin{aligned}
\max \|p - q\| &\leq \sqrt[2]{\max\left(\max p_1 - \min q_1, \min p_1 - \max q_1\right)^2 + \max\left(p_2 - q_2\right)^2} \\
&\leq \sqrt[2]{\max\left(1 - 1, -1 - 1\right)^2 + \max\left(p_2 - q_2\right)^2} \\
&\leq \sqrt[2]{4 + \max\left(\max p_2 - \min q_2, \min p_2 - \max q_2\right)^2} \\
&\leq \sqrt[2]{4 + \max\left(r - 0, 0 - r\right)^2} \\
&\leq \sqrt[2]{4 + r^2}
\end{aligned}$$

It follows that $\sqrt[2]{4 + r^2}$ is greater or equal to $\|p - q\|$ for all $q \in G(r)$ and all $p \in \mathcal{I}(v)$ satisfying $p_2 \leq \frac{r}{3}(p_1 + 2)$. Hence, the formula $\forall q \in G(r) \forall T \geq 0\, \|p - q\| > T$ contradicts our hypothesis.
Thus, if $\neg\left(\exists q \in G(r)\ \exists T \geq 0\ \mathit{Dyn}(v)[(p_1, p_2), q, T]\right)$ holds then so does $p_2 > \frac{r}{3}(p_1 + 2)$ for all $(p_1, p_2) \in \mathcal{I}(v)$.

It follows that $\mathrm{Pre}_v\,(G(r)) = \left\{(p_1, p_2)\ \ |p_2 \leq \frac{r}{3}(p_1 + 2) \wedge \mathit{Inv}(v)[p]\right\}$. □

Lemma 46 *$L(r) = \{(p_1, p_2) \mid p_1 = -1 \wedge 0 < p_2 \leq r\} \subseteq \mathbb{R}^2$. The automaton H_{inf} satisfies $\mathit{Pre}_v\,(L(r)) = \{p\ |3p_2 \leq r(2 - p_1) \wedge \mathit{Inv}(v)[p]\}$, where $p = (p_1, p_2)$ and $v \in \mathcal{V}$.*

PROOF. The proof is analogous to the proof of Lemma 45. □

Proof of Theorem 34

PROOF. Our proof that H_{inf} does not admit finite bisimulation quotient relies on showing that Algorithm 1 does not terminate on H_{inf}. At the beginning of the computation, Algorithm 1 uses $\mathcal{S}_v = \{\mathcal{R}(e), \mathcal{A}(e), \mathcal{I}(v) \setminus (\mathcal{R}(e) \cup \mathcal{A}(e))\}$ as initial partition. Since $L(1) = \mathcal{R}(e)$ and $G(1) = \mathcal{A}(e)$, we have that $\mathcal{S}_v = \{L(1), G(1), \mathcal{I}(v) \setminus (L(1) \cup G(1))\}$. If $p = (p_1, p_2)$ then, by Lemma 46 and G's definition:

$$\begin{aligned}\text{Pre}_v\left(L(r)\right) \cap G(r') &= \{Z \mid p_2 \leq \frac{r}{3}(2 - p_1) \wedge \mathit{Inv}(v)[Z] \wedge p_1 = 1 \wedge 0 < p_2 \leq r'\} \\ &= \{Z \mid p_2 \leq \frac{r}{3} \wedge \mathit{Inv}(v)[Z] \wedge p_1 = 1 \wedge 0 < p_2 \leq r'\} \\ &= G\left(\frac{r}{3}\right)\end{aligned}$$

Similarly, by Lemma 45 and L's definition: $\text{Pre}_v\left(G(r')\right) \cap L(r) = L\left(\frac{r'}{3}\right)$. Thus, if $r < 3r'$ and $r, r' \in \mathbb{R}_{\geq 0}$ then $\emptyset \neq \text{Pre}_v\left(L(r)\right) \cap G(r') \neq G(r')$ and then the algorithm removes $G(r')$ from $\mathcal{S}_v$ and it inserts the sets $G\left(\frac{r}{3}\right)$ and $G(r') \setminus G\left(\frac{r}{3}\right)$ in $\mathcal{S}_v$. Otherwise, $r \geq 3r'$ holds and if $r, r' \in \mathbb{R}_{\geq 0}$ then $3r > r \geq 3r' > r'$. It follows that $\emptyset \neq \text{Pre}_v\left(G(r')\right) \cap L(r) \neq L(r)$ and then the algorithm removes $L(r)$ from $\mathcal{S}_v$ and it inserts the sets $L\left(\frac{r'}{3}\right)$ and $L(r) \setminus L\left(\frac{r'}{3}\right)$ in $\mathcal{S}_v$. Hence, since the initial partition contains both $L(1)$ and $G(1)$, during the subsequent computation steps, there will exist $r, r' \in (0, 1]$ such that $L(r), G(r') \in \mathcal{S}_v$. Moreover, at each computation steps $\exists P, P' \in \mathcal{S}_v \mid \emptyset \neq \text{Pre}_v\left(P\right) \cap P' \neq P'$ in particular, if $r < 3r'$ then $P = L(r)$ and $P' = G(r')$, since, Otherwise, $P = G(r')$ and $P' = L(r)$. It follows then that Algorithm 1 does not terminate, leading to the conclusion that H_{inf} does not admit finite bisimulation. □

Proof of Theorem 39

PROOF. We proceed by structural induction on Q. The only interesting cases are the formulæ $\mathtt{E}\Diamond Q_1$ and $\mathtt{A}\Box Q_1$. We prove the statement in the case $\mathtt{E}\Diamond Q_1$, since the other case has a similar proof.

($\Rightarrow$) By Definition 37, $\langle v, r\rangle \Vdash \mathtt{E}\Diamond Q_1$ holds if and only if, for some state $\langle v', s\rangle$ reachable from $\langle v, r\rangle$, it holds that $\langle v', s\rangle \Vdash Q_1$. But, by Lemma 30, we can deduce that $\langle v', s\rangle$ is reachable from $\langle v, r\rangle$ if and only if there exists a $ph \in \overline{P}_{\mathcal{E}}(v)$ such that $\exists T \geq 0\, \mathit{Reach}(H, ph)[r, s, T]$ holds and $v' = u_{ph}$. Moreover, by inductive hypothesis, $\langle v', Z\rangle \Vdash Q_1$ holds if and only if $\varrho\left(H, Q_1, v'\right)[Z]$ holds. Thus $\langle v, r\rangle \Vdash \mathtt{E}\Diamond Q_1$ holds if and only if there exists a $ph \in \overline{P}_{\mathcal{E}}(v)$ such that $\exists Z'(\exists T \geq 0\, \mathit{Reach}(H, ph)[r, Z', T] \wedge \varrho\left(H, Q_1, u_{ph}\right)[Z'])$ holds, and then, if and only if $\varrho\left(H, \mathtt{E}\Diamond Q_1, v\right)[r]$.

($\Leftarrow$) If $\varrho\,(H, \mathtt{E}\Diamond Q_1, v)\,[r]$ holds, then one of its disjoint clauses must hold. Let ph be the path whose disjoint holds. By Lemma 30, we can deduce that if the formula $\exists T \geq 0\, \mathit{Reach}(H, ph)[r, s, T]$ holds, and $ph \in \overline{P}_{\mathcal{E}}(v)$, then $\langle u_{ph}, s\rangle$ is reachable from $\langle v, r\rangle$. Moreover, by inductive hypothesis, $\langle u_{ph}, Z\rangle \Vdash Q_1$ holds if and only if $\varrho\,(H, Q_1, u_{ph})\,[Z]$ holds. Hence, by $\Phi_{\mathcal{P}}$'s semantics, if $\varrho\,(H, \mathtt{E}\Diamond Q_1, v)\,[r]$ holds, then $\langle u_{ph}, s\rangle$ is reachable from $\langle v, r\rangle$ and $\langle u_{ph}, s\rangle \Vdash Q_1$. It follows that $\langle v, r\rangle \Vdash \mathtt{E}\Diamond Q_1$ holds. $\square$

Proof of Theorem 42

PROOF. By Lemma 27 and by *Reach*'s definition, if H' is a FOCoRe, then the formula $\mathit{Reach}(H', ph)[p, q, t]$ holds if and only if H' reaches q from p in time t through a trace whose corresponding path is ph. Moreover, by hypothesis, $\mathit{Inv}'(v)[Z] \stackrel{\text{def}}{=} \mathit{Inv}(v)[Z] \wedge (\varrho\,(H, Q_1, v)\,[Z] \vee \varrho\,(H, Q_2, v)\,[Z])$ for all $v \in \mathcal{V}$. Hence if the formula $\mathit{Reach}(H', ph)[p, q, t]$ holds, then during the evolution from p to q satisfy either $\varrho\,(H, Q_1, v)\,[Z]$ or $\varrho\,(H, Q_2, v)\,[Z]$. Furthermore, since H and H' have the same dynamics, activations, and resets, if the formula $\mathit{Reach}(H', ph)[p, q, t]$ holds, then $\mathit{Reach}(H, ph)[p, q, t]$ holds too. Now consider the formula $\overline{\varrho}\,(H, H', \mathtt{E}(Q_1 \mathtt{U}\, Q_2), v)\,[Z]$. If $\overline{\varrho}\,(H, H', \mathtt{E}(Q_1 \mathtt{U}\, Q_2), v)\,[r]$ holds, then

$$\exists T \geq 0\, \exists Z' \bigvee_{ph \in \overline{P}_{\mathcal{E}}(v)} \mathit{Reach}(H', ph)[r, Z', T] \wedge \varrho\,(H, Q_2, u_{ph})\,[Z']$$

holds too. By above considerations, it follows that there exists an evolution of H from r to p satisfying $\varrho\,(H, Q_2, u_{ph})\,[p]$ such that during all the evolution either $\varrho\,(H, Q_1, u_{ph})\,[Z]$ or $\varrho\,(H, Q_2, u_{ph})\,[Z]$ holds. Thus $\langle v, r\rangle \Vdash \mathtt{E}(Q_1 \mathtt{U}\, Q_2)$ by Theorem 39 and by $\Phi_{\mathtt{U},\mathcal{P}}$ semantics. $\square$

Lemma 47 *Let H be a hybrid automaton. If Dyn is a transitive dynamics, then C-$\mathit{Reach}(H, v)[r, s, t]$ holds if and only if the following formula holds*

$$\exists Z''\, \exists 0 \leq T' \leq t\, (C\text{-}\mathit{Reach}(H, v)[r, Z'', T'] \wedge C\text{-}\mathit{Reach}(H, v)[Z'', s, t - T'])$$

PROOF. ($\Rightarrow$) By *Dyn*'s definition, the formula C-$\mathit{Reach}(H, v)[r, r, 0]$ holds for all r. Hence if the formula C-$\mathit{Reach}(H, v)[r, s, t]$ holds, then

$$C\text{-}\mathit{Reach}(H, v)[r, s, t] \wedge C\text{-}\mathit{Reach}(H, v)[s, s, 0]$$

holds too. It follows that there exist a w and a $t' \geq 0$ such that the following holds

$$C\text{-}\mathit{Reach}(H, v)[r, w, t'] \wedge C\text{-}\mathit{Reach}(H, v)[w, s, t - t']$$

In particular, this holds with $w = s$ and $t' = t$.

($\Leftarrow$) Consider the formula

$$\phi[Z, Z', T] \stackrel{\text{def}}{=} \exists Z'' \, \exists 0 \leq T' \leq T \, (C\text{-}Reach(H, v)[Z, Z'', T'] \wedge \\ C\text{-}Reach(H, v)[Z'', Z', T - T'])$$

If there exist p, q and $t, t' \geq 0$ such that both $t = t'$ and $\phi[p, q, t]$ hold, then $C\text{-}Reach(H, v)[p, q, t] \wedge C\text{-}Reach(H, v)[q, q, 0]$, and thus $\phi[p, q, t]$ implies that it holds $C\text{-}Reach(H, v)[p, q, t]$. Moreover, if there exist p, q and $t, t' \geq 0$ such that both $t' = 0$ and $\phi[p, q, t]$ hold, then $C\text{-}Reach(H, v)[p, p, 0] \wedge C\text{-}Reach(H, v)[p, q, t]$, indeed $\phi[p, q, t]$ implies $C\text{-}Reach(H, v)[p, q, t]$. Hence, in the following part of the proof, we consider the case in which both $T' \neq T$ and $T' \neq 0$ hold. By $C\text{-}Reach$'s definition, $C\text{-}Reach(H, v)[r, s, t]$ holds if and only if it holds that

$$(\,(t > 0 \wedge Dyn(v)[r, s, t] \wedge \psi(H, v)[r, t]) \vee \\ (t = 0 \wedge r = s)\,) \wedge Inv(v)[r] \wedge Inv(v)[s]$$

Hence the formula

$$\exists Z'' \, \exists 0 \leq T' \leq t \, (C\text{-}Reach(H, v)[r, Z'', T'] \wedge C\text{-}Reach(H, v)[Z'', s, t - T'])$$

holds if and only if the following statement holds

$$\exists Z'' \, \exists 0 \leq T' \leq t \, ((((\,(T' > 0 \wedge Dyn(v)[r, Z'', T'] \wedge \psi(H, v)[r, T']) \vee \\ (T' = 0 \wedge r = Z'')\,) \wedge Inv(v)[r] \wedge Inv(v)[Z'']) \\ \wedge \\ (\,(t - T') > 0 \wedge Dyn(v)[Z'', s, t - T'] \wedge \\ \psi(H, v)[Z'', t - T']) \vee ((t - T') = 0 \wedge \\ Z'' = s)\,) \wedge Inv(v)[Z''] \wedge Inv(v)[s]))$$

As noted earlier, we are considering the case in which both $T' \neq t$ and $T' \neq 0$ hold. In this case, it is easy to prove that the above formula is equivalent to

$$\exists Z'' \, \exists 0 \leq T' \leq T \, ((\,(T' > 0 \wedge Dyn(v)[r, Z'', T'] \wedge \psi(H, v)[r, T'] \wedge \\ (t - T') > 0 \wedge Dyn(v)[Z'', s, t - T'] \wedge \\ \psi(H, v)[Z'', t - T']) \wedge Inv(v)[r] \wedge Inv(v)[Z''] \wedge \\ Inv(v)[s])$$

Moreover, by ψ's definition, if the formulæ $\psi(H, v)[Z'', t - T']$, $\psi(H, v)[r, T']$, and $C\text{-}Reach(H, v)[r, Z'', T']$ are satisfiable, then $\psi(H, v)[r, t]$ holds. Hence, since Dyn is transitive, it easily follows that if the formula

$$\exists Z'' \, \exists 0 \leq T' \leq t \, (C\text{-}Reach(H, v)[r, Z'', T'] \wedge C\text{-}Reach(H, v)[Z'', s, t - T'])$$

holds, then $C\text{-}Reach(H, v)[r, s, t]$ holds too. $\square$

Lemma 48 *Let H be a hybrid automaton. Moreover, let $ph = (v_i)_{i\in[0,h]}$ and $ph' = (v'_i)_{i\in[0,h']}$ be two paths in $\langle \mathcal{V}, \mathcal{E}\rangle$ such that $v_h = v'_0$. If Dyn is a transitive dynamics, then $Reach(H, ph'')[r, s, t]$ holds if and only if it holds that*

$$\exists Z''\, \exists 0 \leq T' \leq t\, (Reach(H, ph)[r, Z'', T'] \wedge Reach(H, ph)[Z'', s, t - T'])$$

where $ph'' = ph \cdot ph'$.

PROOF. Let h'' be the length of $ph \cdot ph'$ (i.e., $h'' = |ph \cdot ph'|$) and $ph \cdot ph'$ be the path $(\overline{v}_i)_{i\in[0,h'']}$. By *Reach*'s definition, $Reach(H, ph'')[r, s, t]$ is equivalent to

$$\exists Z^1, \ldots, Z^{2h''}\ \overline{Reach}(H, ph'')[r, Z^1, \ldots, Z^{2h''}, s, t]$$

Hence, by $\overline{Reach}$'s definition, the formula $Reach(H, ph'')[Z^0, Z^{2h''+1}, T]$ is satisfied by (r, s, t) if and only if the following formula is satisfied by (r, s, t)

$$\begin{aligned}
&\exists Z^1, \ldots, Z^{2h''}\, \exists T_0 \geq 0, \ldots, T_{h''} \geq 0 \\
&\qquad \Bigg(T = \sum_{i=0}^{h''} T_i \ \wedge\ C\text{-}Reach(H, \overline{v}_0)[Z^0, Z^1, T_0] \wedge \\
&\qquad\quad \bigwedge_{i\in[0,h''-1]} \Big(D\text{-}Reach(H, \langle \overline{v}_i, \overline{v}_{i+1}\rangle)[Z^{2i+1}, Z^{2i+2}] \wedge \\
&\qquad\qquad C\text{-}Reach(H, \overline{v}_{i+1})[Z^{2i+2}, Z^{2i+3}, T_{i+1}] \Big) \Bigg)
\end{aligned}$$

By Lemma 47, it follows that $Reach(H, ph'')[Z^0, Z^{2h''+1}, T]$ is satisfied by (r, s, t) if and only if the following formula is satisfied by (r, s, t)

$$\begin{aligned}
&\exists Z''\, \exists 0 \leq T' \leq T\ \exists Z^1, \ldots, Z^{2h''}\, \exists T_0 \geq 0\ \ldots \exists T_{h''} \geq 0 \\
&\qquad \exists T'_h \geq 0\, \exists T''_h \geq 0\, T_h = T'_h + T''_h \\
&\qquad \Bigg(T' = T'_h + \sum_{i=0}^{h-1} T_i \ \wedge\ C\text{-}Reach(H, \overline{v}_0)[Z^0, Z^1, T_0] \wedge \\
&\qquad\quad \bigwedge_{i\in[0,h-2]} \Big(D\text{-}Reach(H, \langle \overline{v}_i, \overline{v}_{i+1}\rangle)[Z^{2i+1}, Z^{2i+2}] \wedge \\
&\qquad\qquad C\text{-}Reach(H, \overline{v}_{i+1})[Z^{2i+2}, Z^{2i+3}, T_{i+1}] \Big) \wedge \\
&\qquad\quad D\text{-}Reach(H, \langle \overline{v}_{h-1}, \overline{v}_h\rangle)[Z^{2h-1}, Z^{2h}] \wedge \\
&\qquad\quad C\text{-}Reach(H, \overline{v}_h)[Z^{2h}, Z'', T'_h] \Bigg) \wedge \\
&\qquad \Bigg(T - T' = T''_h + \sum_{i=h+1}^{h''} T_i \wedge \\
&\qquad\quad C\text{-}Reach(H, \overline{v}_h)[Z'', Z^{2h+1}, T''_h] \wedge
\end{aligned}$$

$$\bigwedge_{i\in[h,h''-1]} \Big(D\text{-}Reach(H,\langle\overline{v}_i,\overline{v}_{i+1}\rangle)[Z^{2i+1},Z^{2i+2}]\wedge$$
$$C\text{-}Reach(H,\overline{v}_{i+1})[Z^{2i+2},Z^{2i+3},T_{i+1}]\Big)\Bigg)$$

This last formula is equivalent to

$$\exists Z''\,\exists 0\le T'\le T\ (Reach(H,ph)[Z,Z'',T']\wedge Reach(H,ph')[Z'',Z',T-T'])$$

Hence, the thesis holds. □

Proof of Theorem 43

PROOF. If $\widetilde{\varrho}\,(H,H',\mathtt{E}\,Q_1\mathtt{U}\,Q_2,v)\,[q]$ holds, then there exist two paths $ph\in\overline{P}_{\mathcal{E}}(v)$ and $ph'\in\overline{P}_{\mathcal{E}}(u_{ph})$ such that either

$$\phi_1 \stackrel{\text{def}}{=} \exists Z'\ \exists T\ge 0\ (\forall 0\le T'<T\ \exists Z''\ (Reach(H',ph)[Z,Z'',T']\wedge$$
$$Reach(H,ph')[Z'',Z',T-T']\ \wedge\ \varrho\,(H,Q_2,u_{ph'})\,[Z']))$$

or

$$\phi_2 \stackrel{\text{def}}{=} \exists Z'\ \exists T\ge 0\,(\exists T'>0\ \forall 0<T''\le T'\ \exists Z''\ (Reach(H',ph)[Z,Z',T]\wedge$$
$$Reach(H,ph')[Z',Z'',T'']\ \wedge\ \varrho\,(H,Q_2,u_{ph'})\,[Z'']))$$

holds. If ϕ_1 holds, then there exist a Z' and a $T\ge 0$ such that for all $T'\in[0,T)$ the formula

$$\exists Z''\ (Reach(H',ph)[Z,Z'',T']\wedge$$
$$Reach(H,ph')[Z'',Z',T-T']\ \wedge\ \varrho\,(H,Q_2,u_{ph'})\,[Z'])$$

holds too. Hence, since *Dyn* is transitive by hypothesis, if ϕ_1 holds, then there exist a Z' and a $T\ge 0$ such that the formula $Reach(H',ph\cdot ph')[Z,Z',T]\wedge\varrho\,(H,Q_2,u_{ph\cdot ph'})\,[Z']$ holds by Lemma 48. By Lemma 27 and by *Reach*'s definition, if $m=|ph\cdot ph'|$, there exist a trace $tr=(\langle v_i,r_i\rangle)_{i\in[0,\ldots,2*m-1]}$ of H and a sequence $(f_i:)_{i\in[0,\ldots,m-1]}$ of functions such that $f_i:[0,t_i]\to\mathbb{R}^n$ is $(r_{2*i},r_{2*i+1},v_{2*i})$ admissible in H for all $i\in[0,\ldots,m-1]$ and H reaches $\langle v,Z\rangle$ from $\langle u_{ph\cdot ph'},Z'\rangle$ through tr (i.e., $\langle v,Z\rangle=\langle v_0,r_0\rangle$ and $\langle u_{ph\cdot ph'},Z'\rangle=\langle v_m,r_m\rangle$). Hence, by Theorem 39, $\langle u_{ph\cdot ph'},Z'\rangle\Vdash Q_2$. Moreover, if $\overline{m}=2*|ph|-1$, we can deduce that H' reaches $\langle v,Z\rangle$ from $\langle u_{ph\cdot ph'},Z'\rangle$ through $tr'=\langle v_0,r_0\rangle,\ldots,\langle v_{\overline{m}},r_{\overline{m}}\rangle,\langle u_{ph},Z''\rangle$, f_i is $(r_{2*i},r_{2*i+1},v_{2*i})$ admissible in H' for all $i\in[0,\ldots,\overline{m}-1]$, and $f_{\overline{m}}$ is $(r_{2*\overline{m}},Z'',v_{2*\overline{m}})$ admissible in H'. Hence, by H''s definition and by Theorem 39, $\langle v_{2*i},f_i(t)\rangle\Vdash Q_1$ for all $i\in[0,\ldots,m-1]$ and for all $t\in[0,t_i)$. It follows that $\langle v,q\rangle\Vdash\mathtt{E}\,Q_1\mathtt{U}\,Q_2$. In an analogous way, we can prove the same result if ϕ_2 holds. □