Reachability Problems on Extended O-Minimal Hybrid Automata

Raffaella Gentilini

Università di Udine (DIMI), Via Le Scienze 206, 33100 Udine - Italy
gentilin@dimi.uniud.it

Abstract. Within hybrid systems theory, o-minimal automata are often considered on the border between decidability and undecidability. In such classes of hybrid automata, the constraint of having only *constant reset* upon discrete jumps is a strong limitation for their applicability: hence, an important issue for both theoreticians and practitioners, is that of relaxing the above constraint, while not fall into undecidability.

In this paper we start considering the problem of *timed-bounded* reachability on o-minimal automata. This can be seen either as a reachability problem paired with time-constraints or as a classical reachability problem for a class of hybrid automata which properly extends the o-minimal one, with an extra variable representing time. Then, we directly face the problem of extending o-minimal automata by allowing some variables to retain their values upon a discrete jump, without crossing the undecidability border.

1 Introduction

Hybrid automata [10] allow formal modeling and reasoning on systems in which continuous and discrete dynamics mutually interact. A fundamental task, underlying automatic verification of hybrid systems, consists in solving a reachability problem i.e. in checking whether the hybrid systems trajectories can evolve to some (bad) region of the (infinite) state-space. The reachability problem is known to be undecidable for a great variety of hybrid automata families [10, 11, 2]. Indeed, the analysis of the border between decidability and undecidability stands as one of the major questions in hybrid systems theory. So far, the results in literature suggest that decidability can follow only from the imposition of strict constraints, either to the continuous flow or to the discrete transitions of systems [2, 11, 1, 9, 13]. To this purpose, the recently introduced family of o-minimal hybrid automata [13] is significant in that, on the one hand, it admits a great variety of possible continuous evolutions but, on the other hand, it imposes a very restrictive constraint on discrete transitions. Basically, upon each discrete jump of an o-minimal system, all continuous variables must be (non deterministically) reset to a constant. Stated in an other way, continuous and discrete dynamics are completely decoupled. In [13], the entire family of o-minimal systems was shown to admit finite bisimulation, and various classes of o-minimal automata were proved decidable, being the corresponding bisimulation algorithm computable.

P. Pettersson and W. Yi (Eds.): FORMATS 2005, LNCS 3829, pp. 162–176, 2005.

Because of the above positive results o-minimal systems are a family of hybrid automata having a great interest from a theoretical point of view; however, their application is rather limited since any continuous variable is never admitted to "remember" its value upon discrete transition.

Starting from the above considerations, in the first part of this paper we consider a variant of reachability problem for o-minimal systems: the *time-bounded reachability problem* (is a region reachable within a maximum time t?). Such a problem can be seen either as a reachability problem paired with time-constraints, or it can be reduced to a classical reachability problem for a class of hybrid automata which properly extends the o-minimal one, with an extra variable representing time. In order to show the decidability of our extended reachability problem, we use the first of the two above characterizations, and we introduce a proof technique that does not require the construction of a (finite) bisimulation abstraction. Basically, we build and solve an equivalent minimum-path problem on a suitable weighted-graph.

In the second part of the paper, we directly face the problem of adjoining o-minimal automata with variables that can maintain their value upon a discrete jump. To this purpose we introduce the class of *relaxed o-minimal automata* that we show to admit finite bisimulation. Finally, we rely on techniques introduced in the first part of the paper to study and prove decidability for a further extension of o-minimal automata, that we call *MasterSlaves o-minimal automata.* For space sake, we include complete proofs of the claims in this paper in [8].

2 Preliminaries

We introduce here the basic notions and the notation we will need in the sequel.

Definition 1 (Hybrid Automata [2]). *An* Hybrid Automata *is a tuple* $H = (L, E, X, Init, Inv, F, G, R)$ *with the following components:*

- *a finite set of* locations*,* L*;*
- *a finite set of* continuous variables*,* $X = \{x_1, \dots x_n\}$*, that take value on* $\mathbb{R}$*;*
- *a finite set of* discrete transitions *(or* jumps*)* $E \subseteq L \times L$*;*
- $F : L \times \mathbb{R}^n \mapsto \mathbb{R}^n$*, assigning to each location* $\ell \in L$ *a vector field* $F(\ell, \cdot)$ *that defines the evolution of continuous variables within* ℓ*;*
- *an initial set of conditions:* $Init \subseteq L \times \mathbb{R}^n$*;*
- Inv*:* $L \mapsto 2^{\mathbb{R}^n}$*, the* Invariant location labelling*;*
- $G : E \mapsto 2^{\mathbb{R}^n}$*, the* Guard edge labelling*;*
- $R : E \times \mathbb{R}^n \mapsto 2^{\mathbb{R}^n}$*, the* Reset edge labelling.

We use the notation $\mathbf{v}$ to represent a valuation, $(v_1, \dots, v_n) \in \mathbb{R}^n$, of the variables' vector $\mathbf{x} = (x_1, \dots, x_n)$. $||\mathbf{x}||$ represents the usual euclidean vector norm, whereas $\dot{\mathbf{x}}$ denotes the first derivatives of the variables in $\mathbf{x}$. A *state* in H is a pair $s = (\ell, \mathbf{v})$, where $\ell \in L$ is called the *discrete component* of s and $\mathbf{v}$ is called the *continuous component* of s. An execution of $H = (L, E, X, Init, Inv, f, G, R)$, starts at any $(\ell, \mathbf{v}) \in Init$ and consists of continuous evolutions (within a location) and discrete transitions (between two locations). Formally, an execution of H is a path in the *timed transition system* of H (cfr. Definition 2, below), alternating discrete and continuous steps.

Definition 2. *The* timed transition system, *T_H^t, of the hybrid automata $H = (L, E, X, Init, Inv, F, G, R)$ is the labeled transition system $T_H^t = (Q, Q_0, \Sigma, \rightarrow)$, with $Q \subseteq L \times \mathbb{R}^n, Q_0 \subseteq Q, \Sigma = \mathbb{R}^+ \cup E$, where:*

- *$(\ell, \mathbf{v}) \in Q$ if and only if $\mathbf{v} \in Inv(\ell)$ and $(\ell, \mathbf{v}) \in Q_0$ if and only if $\mathbf{v} \in Init(\ell) \cap Inv(\ell)$;*
- *for each $\delta \in \mathbb{R}^+$, there is a continuous transition $(\ell, \mathbf{v}) \rightarrow_\delta (\ell, \mathbf{v}')$, if and only if there is a differentiable function $f : [0, \delta] \rightarrow \mathbb{R}^n$, with the first derivative $\dot{f} : [0, \delta] \rightarrow \mathbb{R}^n$ such that:*
  1. *$f(0) = \mathbf{v}$ and $f(\delta) = \mathbf{v}'$;*
  2. *for all $\varepsilon \in (0, \delta)$, $f(\varepsilon) \in Inv(\ell)$, and $\dot{f}(\varepsilon) = F(\ell, f(\varepsilon))$.*
- *there is a discrete transition $(\ell, \mathbf{v}) \rightarrow_e (\ell', \mathbf{v}')$ if and only if $e = (\ell, \ell') \in E$, $\mathbf{v} \in G(\ell)$ and $\mathbf{v}' \in R((\ell, \ell'), \mathbf{v})$*

A run of H will be denoted by the sequence (of continuous and discrete steps) $r = (\ell_0, \mathbf{v_0}) \xrightarrow{t_0} (\ell_0, \mathbf{w_0}) \rightarrow (\ell_1, \mathbf{v_1}) \xrightarrow{t_1} (\ell_1, \mathbf{w_1}) \rightarrow \ldots (\ell_n, \mathbf{v_n}) \xrightarrow{t_n} (\ell_n, \mathbf{w_n})$, where $\sum_{i=0}^n t_i$ will be said the *duration* of r.

The *time abstract transition system* of H is the labeled transition system $T_H = (Q, Q_0, \Sigma \rightarrow)$, where $\Sigma = E \cup \{\tau\}$, that is obtain from T_H^t by replacing each label $\delta \in \mathbb{R}^+$ with the label τ.

A fundamental tool for resizing transition systems, while preserving crucial properties (such as reachability) is *bisimulation reduction*, that we introduce below. Consider a labeled transition system $T = (Q, Q_0, Q_F, \Sigma, \rightarrow)$, where Q_F denotes the set of final states, and let $\sim_{\mathcal{B}}$ to be an equivalence relation on Q.

Definition 3. *$\sim_{\mathcal{B}}$ is a* bisimulation *of $T = (Q, Q_0, Q_F, \Sigma, \rightarrow)$ if and only if:*

- *both Q_0 and Q_F are $\sim_{\mathcal{B}}$ blocks (i.e. union of $\sim_{\mathcal{B}}$ classes);*
- *for each $\sim_{\mathcal{B}}$ block, B, for each label $a \in \Sigma$, the region $Pre_a(B) = \{q \in Q \mid \exists p \in B \quad \wedge \quad q \rightarrow_a p\}$ is a $\sim_{\mathcal{B}}$-block.*

2.1 O-Minimal Theories and O-Minimal Hybrid Automata

In this paper we consider a class of hybrid automata called *o-minimal automata* [13, 14]. O-minimal theories, introduced below, play a central role in the definition of o-minimal automata. We refer to [19, 18, 20] for a more comprehensive introduction to o-minimal theories.

Definition 4. *A theory of the reals is o-minimal if and only if every definable subset of $\mathbb{R}$ is a finite union of points and intervals (possibly unbounded).*

The class of o-minimal theories over the reals is quite rich: the theories $\mathsf{Li}(\mathbb{R}) = (\mathbb{R}, <, +, -, 0, 1)$ and $\mathsf{OF}(\mathbb{R}) = (\mathbb{R}, <, +, -, *, 0, 1)$ are both o-minimal. The extension of the above theories obtained by admitting, in the underlying language, a symbol for the exponential function, $\mathsf{OF}_{\mathsf{exp}}(\mathbb{R}) = (\mathbb{R}, <, +, -, *, exp, 0, 1)$, is also o-minimal. Another important extension is obtained by introducing, in the underline language, a symbol for each *restricted analytic functions* and more extensions are discussed in [13]. By Definition 6, below, such a variety of o-minimal theories (over the reals) ensures that o-minimal automata is a large and important family of hybrid automata, admitting powerful continuous evolutions. In the following definitions, we will use the notation adopted in [13].

Definition 5. *Let $F : \mathbb{R}^n \mapsto \mathbb{R}^n$ a smooth vector field on $\mathbb{R}^n$. For each $\mathbf{v} \in \mathbb{R}^n$, let $\gamma_{\mathbf{v}}(t)$ to denote the integral curve of F which passes through $\mathbf{v}$ at $t = 0$, that is $\dot{\gamma}_{\mathbf{v}}(t) = F(\gamma_{\mathbf{v}}(t))$ and $\gamma_{\mathbf{v}}(0) = \mathbf{v}$. We say that F is* complete *if, for each $\mathbf{v} \in \mathbb{R}^n$, $\gamma_{\mathbf{v}}(t)$ is defined for all times t. For such an F, the* flow *of F is the function $\phi : \mathbb{R}^n \times \mathbb{R} \mapsto \mathbb{R}^n$, given by $\phi(\mathbf{v}, t) = \gamma_{\mathbf{v}}(t)$.*

Definition 6 (O-Minimal Hybrid Automata [13]). *The hybrid automaton $H = (L, E, X, \mathrm{Init}, \mathrm{Inv}, F, G, R)$ is said an* o-minimal automata *if and only if:*

- *for each $\ell \in L$ the smooth vector field $F(\ell, \cdot)$ is complete;*
- *for each $(\ell, \ell') \in E$, the reset function $R : E \mapsto \mathbb{R}^n$ does not depend on continuous variables (*constant resettings*);*
- *for each $\ell \in L$ and $(\ell, \ell') \in E$, the sets $Inv(\ell)$, $R(\ell, \ell')$, $G(\ell)$, $Init(\ell)$, and the flow of $F(\ell, \cdot)$ are definable in the same o-minimal theory*

Given an o-minimal theory, $\mathcal{T}$, we denote by o-minimal($\mathcal{T}$) automata the class of o-minimal automata induced by $\mathcal{T}$.

3 Related Work

The *reachability problem* for an hybrid automaton H, consists in the problem of determinimg, given a location ℓ and $V \subseteq \mathbb{R}^n$, if there exists a run of H ending at $(\ell, \mathbf{v})$ with $\mathbf{v} \in V$. In general, the latter problem is not decidable [11, 10]. So far, according to the results in the litterature, it seems that its decidability can be obtained only by imposing strict constraints either on the discrete transitions, or on the continuous evolution of hybrid automata [2, 11].

In *timed automata* [1] and *multirate automata* [11, 12], for example, the flow of continuous variables must be of constant slope one and general constant slope, respectively. In both cases, the reachability problem is decidable because the corresponding time-abstract transition systems can be (algorithmically) reduced to finite by *bisimulation* reduction [11]. *Initialized rectangular automata* [12] allow to specify derivatives of the continuous variables flows by means of a conjunction of inequality of the form $\dot{x} \approx c$, where $\approx \in \{<, >, =\}$ and $c \in \mathbb{Q}$. Moreover they impose an *initialization constraint* on discrete transitions. Given a discrete transition (ℓ, ℓ'), all the variables that have a different flow in ℓ and ℓ' must be reset to an interval over $\mathbb{R}$; The reachability problem is decidable for initialized rectangular automata, since the corresponding time abstract transition systems can be (algorithmically) reduced to finite by *simulation* reduction [9, 11].

O-minimal hybrid systems [13] are considered on the border between decidability and undecidability for the reachability problem. If H is an o-minimal automata, then T_H admits finite bisimulation [13, 14, 7]. This result does not guarantee the decidability of the entire family [14], because the bisimulation reduction is not computable, in general, for o-minimal automata. In order to decide reachability relying on bisimulation reduction, it is necessary to effectively:

1. represent sets of states;
2. perform set intersection, set complement, and check set emptiness;
3. given a set of states, Y, compute the set of states that can reach an element in Y following a discrete/continuous step.

The computability of the above operations depends on the o-minimal theory in which the flow of the hybrid automata, the *Inv* sets, the *Guard* sets, the *Reset* sets, and the *Initial* conditions are defined. In [14] it is proved the decidability of o-minimal($\mathsf{OF}(\mathbb{R})$) automata. Decidability depends on the fact that the theory ($\mathsf{OF}(\mathbb{R})$) *admits quantifier elimination* [17, 4] i.e. each formula in the theory is equivalent to a quantifier free one that can be algorithmically determined. Thus, for example, checking set emptiness corresponds to first performing quantifier elimination, and then checking if the resulting formula is equivalent to *false.* The results in [13, 14] show that o-minimal($\mathsf{OF}(\mathbb{R})$) automata constitute a class of decidable hybrid systems admitting powerful coupled continuous dynamics. For example, the flow of continuous variables whose first derivatives is given by $\dot{\mathbf{x}} = A\mathbf{x}$, with A nilpotent (that is $\exists n\ A^n = 0$), is $\mathsf{OF}(\mathbb{R})$ definable [13]. On the converse, o-minimal($\mathsf{OF}(\mathbb{R})$) automata define the class of decidable hybrid systems with the strongest constraints on discrete transition: each variable must be nondeterministically reset to a constant upon each location switch.

In the next section we show how the above constraints on discrete transitions leave open the following decidability question for o-minimal automata.

Is it possible to decide if a region is reachable within a time interval?

The answer of such a question is positive for the other families of decidable hybrid automata (timed, multirate and initialized rectangular automata). We enclose the circle giving a positive answer also for o-minimal($\mathsf{OF}(\mathbb{R})$) automata. The construction we will give is interesting in itself, because it allows establishing an alternative proof that reachability is decidable for o-minimal($\mathsf{OF}(\mathbb{R})$) automata. Such a proof does not make use of bisimulation or simulation reduction and, in our opinion, allows to better understand the link relating the constraints defining both discrete and continuous components, in o-minimal automata, and the decidability of the reachability problem. Moreover, our proof is constructive and gives, as a free byproduct, an *optimal* reachability run i.e. a run whose duration is minimal. The problem of determining optimal runs, assuming both time constraints and discrete switches costs has been previously considered for the class of timed automata in [16, 5, 3].

We conclude this section citing the works in [15, 6] where the issue of extending o-minimal automata relaxing the constant reset constraint is taken into consideration, and some extensions leading to undecidability are presented.

4 Time Bounded Reachability Problem and O-Minimal Hybrid Automata

We start by formally defining the *time bounded reachability problem* on hybrid automata.

Definition 7. *The* timed bounded reachability problem *for an hybrid automata H, consists in determining, given a location ℓ, $V \subseteq \mathbb{R}^n$, and a time value $t \in \mathbb{Q}$, if there exists a run of H having duration $t' \leq t$ and ending at $(\ell, \mathbf{v})$, with $\mathbf{v} \in V$.*

For most families of decidable hybrid automata (but not for classes of o-minimal systems), the above problem can be reduced to a classical reachability problem on an augmented automata of the same family. In fact, assume for example to work with a timed, a multirate, or an initialized rectangular automata, H, and suppose that you want to state if the region (ℓ, V) is reachable within time $t \in \mathbb{Q}$. You can obtain a new automata of the same family, H', by augmenting the set of continuous variables with a new (time) variable x_t, where $\dot{x_t} = 1$ in all locations and $R(v_t) = v_t$ for all discrete transitions. Trivially, (ℓ, V) is reachable within the time t in H if and only if $(\ell, V \times \{t' \mid t' \leq t\})$ is reachable in H'. The construction does not work for o-minimal($\mathsf{OF}(\mathbb{R})$) automata, since o-minimal automata do not allow a variable to always maintain the same value upon a discrete transition.

In order to prove that time bounded reachability is still decidable for o-minimal($\mathsf{OF}(\mathbb{R})$) automata, we shall define an equivalent weighted graph minimum-path problem. The graph manipulated will be a labelling of the control graph of H, instead of a simulation or a bisimulation abstraction of T_H. The following lemma establishes a general property of o-minimal systems and will be central in the correctness of the encoding.

Lemma 1. *For each run of H,*
$r = (\ell_0, \mathbf{v_0}) \xrightarrow{t_0} (\ell_0, \mathbf{w_0}) \rightarrow (\ell_1, \mathbf{v_1}) \ldots \xrightarrow{t_{n-1}} (\ell_{n-1}, \mathbf{w_{n-1}}) \rightarrow (\ell_n, \mathbf{v_n})$,
there is a run of H,
$r^* = (\ell'_0, \mathbf{v'_0}) \xrightarrow{t_0} (\ell'_0, \mathbf{w'_0}) \rightarrow (\ell'_1, \mathbf{v'_1}) \ldots \xrightarrow{t_{m-1}} (\ell'_{m-1}, \mathbf{w'_{m-1}}) \rightarrow (\ell'_m, \mathbf{v'_m})$, *where:*

- $\ell_0 = \ell'_0$, $\mathbf{v_0} = \mathbf{v'_0}$, $\ell_n = \ell'_m$, *and* $\mathbf{v_n} = \mathbf{v'_m}$
- $\forall\, 0 \leq i, j < m$, *it holds* $(i \neq j) \rightarrow (\langle \ell'_i, \ell'_{i+1} \rangle) \neq (\langle \ell'_j, \ell'_{j+1} \rangle)$
- *the duration of r^* is less or equal to the duration of r.*

Lemma 1 can be used to build, given an o-minimal automata H, an o-minimal automata H' with the following property: (ℓ, V) is reachable in H if and only if V is reachable (in a suitable location of H') through a path that passes *at most once* on each H'-location. More precisely, we define the *guard-expansion* of an o-minimal automata H, as below:

Definition 8. *The* guard-expansion *of* $H = (L, E, X, \mathrm{Init}, \mathrm{Inv}, \mathrm{f}, G, R)$ *is the o-minimal automata* $H' = (L', E', X', \mathrm{Init}', \mathrm{Inv}', \mathrm{f}', G', R')$ *where:*

- $L' = \{\ell_i^j \mid (\ell_j, \ell_i) \in E\} \cup \{\ell_i^\sharp \mid \ell_i \in L$ *has not incoming edges*$\}$;
- $(\ell_i^j, \ell_p^i) \in E$ *if and only if* $(\ell_i, \ell_p) \in E$;
- *for all* $\ell_i^j \in L'$ *we have* $\mathrm{Init}'(\ell_i^j)=\mathrm{Init}(\ell_i)$, $\mathrm{Inv}'(\ell_i^j)=\mathrm{Inv}(\ell_i)$, $G(\ell_i^j, \ell_p^i)=G(\ell_i, \ell_p)$, $f'(\ell_i^j, \mathbf{x})=f(\ell_i, \mathbf{x})$;
- *for all* $(\ell_i^j, \ell_p^i) \in E$, $R'(\ell_i^j, \ell_p^i) = R(\ell_i, \ell_p)$.

The result in Lemma 2 follows directly by Definition 8 and by Lemma 1.

Lemma 2. *If* (ℓ_i, V) *is reachable in the o-minimal automata* H *within time* t*, then there exists* j *such that* (ℓ_i^j, V) *is reachable in the guard-expansion of* H*, through a run of duration* $t' \leq t$ *that never pass twice in the same location.*

5 An Algorithm for Time Bounded Reachability on Classes of O-Minimal Hybrid Automata

We prove here the decidability of time bounded reachability for o-minimal(OF ($\mathbb{R}$)) automata. As anticipated, we will make use of the results in Section 4 to map the problem onto a weighted graph minimum-path problem.

Given an o-minimal(OF($\mathbb{R}$)) automata, H, the first step in the construction consists in obtaining the guard-expansion of H (cfr. Definition 8), H'. By Lemma 2, checking if H admits a run to a region R, of duration at most t, is equivalent to checking if there is a suitable acyclic run of duration at most t in H'. We represent in Figure 1 an o-minimal(OF($\mathbb{R}$)) automata and its guard-expansion[1]. In the rest of this section we will use exactly the automata of Figure 1 to illustrate the overall procedure.

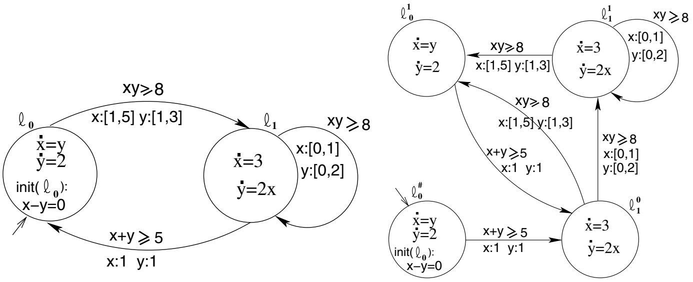

Fig. 1. An o-minimal(OF($\mathbb{R}$)) automaton and its guard-expansion

5.1 Phase 1: Labelling Scheme

Our next task is that of opportunely labeling the control graph of the guard-expansion automata H', obtaining a weighted graph $\mathcal{G}$. The set of nodes in $\mathcal{G}$ consists of the set of locations of H' plus an auxiliary final node F.

[1] Note that the continuous dynamics of the hybrid automata depicted in Figure 1 can be expressed within (OF($\mathbb{R}$)) theory because the matrices involved in the underlying differential equations systems are *nilpotent* (see [14]).

If the target region, in our process, is in the location l_i of H, then F is linked to all the locations of H' into which l_i gets split. Hence, for example, if we would like to check time-bounded reachability of a region in the location ℓ_0, then $\mathcal{G}$ would have the structure depicted in Figure 2.

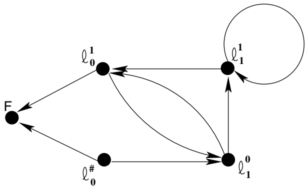

Fig. 2.

The weights in $\mathcal{G}$ are real numbers maintaining as much information as necessary to reduce our time bounded reachability problem to that of detecting a minimum weighted path in $\mathcal{G}$. Such weights are defined relying on the fact that $\mathsf{OF}(\mathbb{R})$ is a decidable theory that admits quantifier elimination. In fact, to label each edge of $\mathcal{G}$, we build a suitable $\mathsf{OF}(\mathbb{R})$ formula and we eliminate its quantifiers. As a byproduct, we obtain a real number that we use as a weight. More in detail, the labeling of $\mathcal{G}$ proceeds as follows:

- For each edge (l_i^j, l_p^i) in $\mathcal{G}$, we build the formula $\psi_{(l_i^j, l_p^i)}(t_0)$, that represents the *greatest lower bound* of the (o-minimal) set of times allowing to pass from a point in the reset region $R(l_j, l_i)$ of H, to a point in the guard region $G(l_i, l_p)$ of H. The formula $\psi_{(l_i^j, l_p^i)}(t_0)$ is given by:

$$\begin{aligned}\psi_{(l_i^j, l_p^i)}(t_0) = \ & (\mathit{Reach}^{\Delta}_{(l_i^j, l_p^i)}(t_0) \vee \mathit{Reach}_{(l_i^j, l_p^i)}(t_0)) \wedge \\ & \wedge \forall t (\mathit{Reach}_{(l_i^j, l_p^i)}(t) \rightarrow t \geq t_0))\end{aligned} \tag{1}$$

In $\psi_{(l_i^j, l_p^i)}(t_0)$, the subformula $\mathit{Reach}^{\Delta}_{(l_i^j, l_p^i)}(t_0)$ characterizes the time-point t_0 as the left extreme of an open interval, $\Delta = (t_0, t_0 + \epsilon)$, such that, for each $t_0 < t < t_0 + \epsilon$, the continuous components of H' can evolve from a value in $R(l_j, l_i)$ to a value in $G(l_i, l_p) \in H$, in time t. Similarly, the subformula $\mathit{Reach}_{(l_i^j, l_p^i)}(t)$ expresses the possibility to reach the guard-set $G(l_i, l_p) \in H$ from the reset-set $R(l_j, l_i) \in H$ in time t. If ϕ denotes the flow of the vector field $F(\ell_i, \cdot)$, then $\mathit{Reach}^{\Delta}_{(l_i^j, l_p^i)}(t_0)$ and $\mathit{Reach}_{(l_i^j, l_p^i)}(t)$ are the following $\mathsf{OF}(\mathbb{R})$ first-order formulas:

$$\mathit{Reach}^{\Delta}_{(l_i^j, l_p^i)}(t_0) = \exists \epsilon \forall t [(t_0 < t \wedge t < \epsilon) \rightarrow \mathit{Reach}_{(l_i^j, l_p^i)}(t)] \tag{2}$$

$$\begin{aligned}\mathit{Reach}_{(l_i^j, l_p^i)}(t) = \exists \mathbf{x}, \mathbf{y}\ & [\mathbf{x} \in R(l_j, l_i) \wedge \mathbf{y} \in G(l_i, l_p) \wedge \phi(\mathbf{x}, t) = \mathbf{y} \wedge \\ & \wedge \forall t' (0 \leq t' \leq t \rightarrow \phi(\mathbf{x}, t') \in \mathit{Inv}(l_i))]\end{aligned} \tag{3}$$

If $\psi_{(l_i^j, l_p^i)}(t_0)$ is satisfiable, then there is a unique value that can be assigned to t_0 to have a true sentence. Hence, by using, for example, Collins cylindric algebraic decomposition algorithm [6] we can eliminate the quantifiers in $\psi_{(l_i^j, l_p^i)}(t_0)$ and obtain a real algebraic number witnessing (the unique) time-value satisfying $\psi_{(l_i^j, l_p^i)}(t_0)$. We use the computed greatest lower bound, say α, to label the edge (l_i^j, l_p^i) in $\mathcal{G}$. We also distinguish the case in which α is the left extreme of an *open* interval of times, from the case in which α is the left extreme of a *closed* interval of times (allowing to pass from $R(l_j, l_i)$ to $G(l_i, l_p)$)[2]. In the first case, we use a dotted edge to connect the vertex l_i^j to the vertex l_p^i in $\mathcal{G}$. Finally, if $\psi_{(l_i^j, l_p^i)}(t_0)$ is not satisfiable, the edge (l_i^j, l_p^i) is labeled with the value $+\infty$, meaning that it is never possible to reach location $l_p^i \in H'$ from $l_i^j \in H'$.

- For each edge $(l_i^{\#}, l_p^i)$ in $\mathcal{G}$, we derive the formula $\psi_{(l_i^{\#}, l_p^i)}(t_0)$, that represents the greatest lower bound on the time required to pass from a point in the initial region of $\ell_i \in H$ to a point in the guard region $G(l_i, l_p)$ of H. The process of construction of formula $\psi_{(l_i^{\#}, l_p^i)}(t_0)$ is equivalent to that of building formula $\psi_{(l_i^j, l_p^i)}(t_0)$, in Equation 1. The only difference is that we should use the initial-set $Init(l_i)$ in place of the reset-set $R(l_j, l_i)$, within the definition of the subformula in Equation 3. The edge $(l_i^{\#}, l_p^i)$ is finally labeled either with $+\infty$ or with the real number resulting from solving the expression derived from quantifier elimination applied to $\psi_{(l_i^{\#}, l_p^i)}(t_0)$.
- We follow an analogous approach to label each edge leading to the node F in $\mathcal{G}$. In this case, however, in place of guard-sets we use the final region V to define the formulae in Equations 1,2,3.

5.2 Phase 2: Time Bounded Acyclic Paths Detection

Since now we have never used the input information about the time bound. This information is necessary in the last phase of our procedure. In such a step we simply apply a classical algorithm for the (multiple sources) minimum-path problem[3] on $\mathcal{G}$, where F plays the role of target node, and the sources are the nodes associated with each initial location, $l_i^{\#}$, in H'. Then, we match the weight, w, of such a minimum path with the time bound, t_{max}. Finally we answer positively to our problem if and only if $w < t_{max}$ or $w = t_{max}$ and the corresponding minimum path does not contain any dotted edge.

Theorem 1. *Time-bounded reachability is decidable for o-minimal(*$\mathsf{OF}(\mathbb{R})$*) hybrid automata.*

6 Generalizing Issues

The strategy discussed in previous sections to answer the time-bounded o-minimal reachability problem can be naturally translated into an approach to decide general reachability problem for o-minimal automata. Such an approach

[2] This can be done by simply checking if the sentence $\exists t_0(Reach_{(l_i^j, l_p^i)}(t_0) \wedge \forall t(Reach_{(l_i^j, l_p^i)}(t) \rightarrow t \geq t_0))$ is equivalent to the free-quantifier sentence *true*.

[3] Note that it is possible to carry on the computation of the overall minimum path algorithm *symbolically*. This means that if α and α' are two edge labelling reals, represented by the two $\mathsf{OF}(\mathbb{R})$ quantifier free formulas $\phi(t)$ and $\phi'(t)$, then $\alpha + \alpha'$ can be obtained by eliminating the quantifiers in $\exists t_1, t_2(\phi(t_1) \wedge \phi'(t_2) \wedge t_1 + t_2 = t_3)$.

is even simpler in the case of general reachability, in the sense that we only need to solve an equivalent connectivity problem on a directed (unlabeled) graph $\mathcal{G}$. Moreover, building the edges of $\mathcal{G}$ involves the definition and evaluation of $\mathsf{OF}(\mathbb{R})$ sentences simpler than the formulas in Equations 1, 2, 3. More in detail, consider again the o-minimal automata in Figure 1 and the problem of detecting the reachability of an $\mathsf{OF}(\mathbb{R})$ definable set of states within location ℓ_0. The directed unlabeled graph built to solve such problem has exactly the same set of nodes of the graph in Figure 2 (built for time-bounded reachability). The rule for defining the set of edges in $\mathcal{G}$, instead, changes: in particular, for each edge (l_i^j, l_p^i) in the guard expansion H', we build a corresponding edge $(l_i^j, l_p^i) \in \mathcal{G}$ if and only if the following sentence is equivalent to the quantifier free sentence *true*:

$$\exists \mathbf{x}, \mathbf{y}, t(\mathbf{x} \in R(l_j, l_i) \cap Inv(l_i) \wedge \mathbf{y} \in G(l_i, l_p) \cap Inv(l_i) \wedge$$

$$\wedge \phi(\mathbf{x}, t) = \mathbf{y} \wedge \forall t' \leq t(\phi(\mathbf{x}, t') \in Inv(l_i)) \tag{4}$$

The above sentence simply asserts the possibility of reaching a point in the guard region $G(l_i, l_p)$, from a point in the reset region $R(l_j, l_i)$. Note that, if it is not necessary to specify the invariant sets in our hybrid automata, then the sentence in Equation 4 uses *only* the existential fragment of the underlying theory.

With respect to traditional decision procedures in the litterature [13, 14], for deciding reachability in o-minimal automata, the above sketched strategy does not require to build the whole state-space of the bisimulation abstraction of T_H. Thus, it is valuable with respect to the, often fundamental in the verification field, space-efficiency parameter. Moreover, in our opinion, the outlined decision procedure for reachability *precisely localize* the decidability of o-minimal hybrid automata within the following two parameters:

- the constant resets imposed onto the discrete dynamics;
- the decidability of the (existential fragment) of the theory defining all relevant sets in the automata.

7 Relaxing O-Minimal Automata Constant Resets

7.1 Relaxed O-Minimal Automata

In this section, we directly face the problem of adjoining o-minimal automata with variables that can maintain their values upon a discrete jump. To this aim, Definition 9, below, introduces the class of *relaxed o-minimal automata.* In a relaxed o-minimal hybrid automata, say H, continuous variables can maintain their values along discrete transitions. However, for each cycle in the control graph of H, there must be at least one edge along which all variables are non deterministically reset to a constant. Let $\mathcal{T}$ to be an o-minimal theory:

Definition 9 (Relaxed O-Minimal($\mathcal{T}$) Automata). *A* Relaxed o-minimal ($\mathcal{T}$) Automata *is an hybrid automata* $H = \langle L, E, X, Init, Inv, F, G, R \rangle$ *in which:*

- *$L, E, X, Init, Inv, F, G$ are defined as in o-minimal hybrid automata, inside the same o-minimal theory $\mathcal{T}$;*
- *the reset function $R = R_1 \times \ldots \times R_{n=|X|} : E \times \mathbb{R}^n \times 2^{\mathbb{R}^n}$ is defined as follows:*
  1. *for each edge $e \in E$, for each $1 \leq i \leq n$, $R_i(e, \cdot)$ is either equal to the identity function $id : \mathbb{R} \mapsto \mathbb{R}$, or it is a constant function mapping each value of the continuous variable x_i to an interval over $\mathbb{R}$;*
  2. *for each cycle $(\ell_1 \ldots \ell_k = \ell_1)$ in the control graph of H, $\mathcal{G} = (L, E)$, there exists an edge $e = (\ell_i, \ell_{i+1})$ upon which the reset function $R = R_1 \times \ldots \times R_n$ is composed only by constant functions.*

Consider a (general) hybrid automata $H = \langle L, E, X, Init, Inv, F, G, R \rangle$ and let $T_H = \langle Q, Q_0, Q_F, \Sigma, \rightarrow \rangle$, were Q_F is a set of final states, to be the time-abstract transition system of H. We represent in Figure 3 a well known partition-refinement computational approach to determine the maximum bisimulation over T_H. The procedure in Figure 3 successively refines a partition onto Q coarser than the bisimulation quotient, iterating until a (finite) partition stable with respect to $\rightarrow = (\bigcup_{e \in E} \rightarrow_e) \cup \rightarrow_\tau$ is determined. It follows that Bisim(H) computes the bisimilation quotient of T_H if and only if T_H admits a finite bisimulation. Theorem 2, at the end of this section, shows exactly that this is the case for the time abstract transition systems of relaxed o-minimal automata.

We start by observing that, in order to show bisimulation finiteness for o-minimal hybrid automata in [13], Pappas et al. used a partition refinement bisimulation algorithm simpler than the general one presented in Figure 3. Such an algorithm is depicted in Figure 4, and reduces to perform only the first for-loop of Bisim, splitting independently the state-space associated with each location $\ell \in L$. This, in turn, means that the discrete transitions are never considered within the splitting process. The correctness of the algorithm depends on the fact that o-minimal systems are constrained to *constant resets*. More precisely, if $G(e)$

```
Bisim($H$)

Let $\mathcal{P}$ be the coarsest partition of $L \times \mathbb{R}^n$ compatible with respect to each block
  $\{\ell\} \times Z$, where $\ell \in L$, $Z \in \mathcal{A}_\ell$ and $\mathcal{A}_\ell = \{Inv(\ell), Init(\ell), Final(\ell)\}$
Repeat
  $old\mathcal{P} \leftarrow \mathcal{P}$
  for each $(\ell \in L)$
    while $(\exists B, B' \in \mathcal{P}$ such that $\emptyset \neq B \cap Pre_\tau(B') \neq B)$
      $B_1 \leftarrow B \cap Pre_\tau(B'); B_2 \leftarrow B \setminus Pre_\tau(B')$
      $\mathcal{P} \leftarrow (\mathcal{P} \setminus \{B\}) \cup \{B_1, B_2\}$
  for each $(e = (\ell, \ell') \in E)$
    for each $(\ell' \times V' = B' \in \mathcal{P}, \ell \times V = B \in \mathcal{P}$ such that $\emptyset \neq B \cap Pre_e(B') \neq B)$
      $B_1 \leftarrow B \cap Pre_e(B'); B_2 \leftarrow B \setminus Pre_e(B')$
      $\mathcal{P} \leftarrow (\mathcal{P} \setminus \{B\}) \cup \{B_1, B_2\}$
until $(\mathcal{P} = old\mathcal{P})$
```

Fig. 3. The partition refinement bisimulation algorithm for general hybrid automata

```
BisimLoc($H$)

define $\mathcal{A}_\ell = \{Inv(\ell), Init(\ell), Final(\ell)\} \cup \{G(\ell,\ell'), R(\ell,\ell') \mid (\ell,\ell' \in E)\}$
Let $\mathcal{P}$ be the coarsest partition of $L \times \mathbb{R}^n$ compatible with respect
to each block $\{\ell\} \times Z$, where $\ell \in L$, $Z \in \mathcal{A}_\ell$
  for each $(\ell \in L)$
    while $(\exists B, B' \in \mathcal{P}$ such that $\emptyset \neq B \cap Pre_\tau(B') \neq B)$
      $B_1 \leftarrow B \cap Pre_\tau(B'); B_2 \leftarrow B \setminus Pre_\tau(B')$
      $\mathcal{P} \leftarrow (\mathcal{P} \setminus \{B\}) \cup \{B_1, B_2\}$
```

Fig. 4. The partition refinement bisimulation algorithm for o-minimal automata in [13]

and $R(e)$ are classes in the initial partition $\mathcal{P}_0$, for each edge e, constant resets ensure that discrete transitions do not cause any partition refinement since:

$$Pre_e(B) = \begin{cases} \emptyset, & \text{if } B \cap R(e) = \emptyset; \\ G(e), & \text{otherwise.} \end{cases}$$

On the other hand, the *termination* of the refinement process within the bisimulation procedure used by [13] in Figure 4, only depends on the form of the following two components:

- the initial partition, which is a *finite* and composed by *classes definable in the o-minimal theory of H* ;
- the smooth and complete vector field that defines the relation of the transition system, whose flow is definable in the o-minimal theory of H.

The above facts will be used within the following Lemmas, preliminary to the main Theorem 2. Note that, since relaxed o-minimal automata allow identity resets, the procedure in Figure 4 [13] does not allow to define a bisimulation over the corresponding time-abstract transition systems. Consider a relaxed o-minimal automata, H, and let $\mathcal{P}_0$ to be the partition built in the initialization phase of Bisim(H).

Lemma 3. *Each execution of the first for-loop within* Bisim *terminates leading to a finite partition which refines $\mathcal{P}_0$.*

Theorem 2. *Relaxed o-minimal hybrid automata admit finite bisimulation.*

The corollary below, follows immediately from Theorem 2 and from the fact that the o-minimal theory $\mathsf{OF}(\mathbb{R})$ admits quantifier elimination.

Corollary 1. *The reachability problem is decidable for Relaxed o-minimal(*OF *($\mathbb{R}$)) automata.*

7.2 MasterSlaves O-Minimal Automata

In Section 5, we exploited Tarski quantifier elimination to obtain a real value that is a lower bound onto the time necessary to move among regions, within one o-minimal automaton location. Here we build up on this idea to define a further extension of o-minimal automata which does not cross the undecidability border, while relaxing the condition of having only constant reset on discrete jumps.

Briefly, this is achieved by endowing our automata with *two* classes of continuous variables. Precisely, *MasterSlaves* o-minimal hybrid automata will be endowed with a set of variables that we call *constant reset* variables (or *slaves variables*) plus a further variable that we call *free variable* (or *master variable*). We impose the continuous evolution of the master variable, say x^f, to be independent from slaves variables[4]: x^f is allowed to maintain its value upon a discrete transition if its flow does not change with the corresponding switch to a new location. Otherwise, the free variable must be reset to a constant. As far as slaves variables is concerned, we impose their discrete dynamics to be always constrained to constant reset.

Given a location ℓ, it is possible to define a $\mathcal{T}$ formula representing the set of times allowing to traverse[5] ℓ, using exactly the same techniques adopted in Section 5. We guarantee that such a set admits a *strictly positive* lower bound for MasterSlaves o-minimal automata. The above fact, together with *closed bounded invariant sets* (cfr. condition *f*) in Definition 10, below), is strongly related to the decidability results stated in Theorems 3 and 4, at the end of this section.

To equip the reader of some more intuition, before formally introducing MasterSlaves automata, we anticipate that conditions *f*), *g*) in Definition 10, and the form of continuous dynamics, allow to ensure the following properties:

1. $\forall \ell \in L$ there exists a *strictly positive* lower bound to the time required to traverse ℓ;
2. there exists a finite *upper bound* on the time that the free variable can spend evolving according to a given vector field, F^f, and subject to identity resetting, without violating invariants.

Definition 10 (MasterSlaves O-Minimal($\mathcal{T}$) Automata). *A* MasterSlaves o-minimal($\mathcal{T}$) Automata *is an Hybrid Automata* $H = (L, E, X, \text{Init}, \text{Inv}, F, G, R)$ *with:*

continuous dynamics

a) $X = X^c \cup \{x^f\}$, $x^f \notin X^c$. $X^c = \{x^c_1, \ldots, x^c_m\}$, $m \geq 1$, *is said the set of* constant reset variables *(or* slaves variables*), whereas* x^f *is said the* free variable *(or* master variable*);*

b) $\forall \ell \in L$, $F(\ell, \cdot) : \mathbb{R}^{m+1} \mapsto \mathbb{R}^{m+1}$ *is a complete smooth vector field whose flow is* $\mathcal{T}$*-definable.*

c) $\forall \ell \in L$, *the continuous evolution of the free variables does not depend on* X^c, *i.e. it can be represented as the solution of a complete smooth vector field,* $F^f(\ell) : \mathbb{R} \mapsto \mathbb{R}$. *Moreover, if* $v \in Inv(\ell) \mid_{x^f}$, *then* $||F^f(v)|| \neq 0$.

[4] In other words, for each location of a MasterSlaves automata, the flow of the free variable can be represented as the solution of a smooth vector field $F^f : \mathbb{R} \mapsto \mathbb{R}$.

[5] i.e. to reach a guard region in ℓ departing from any guard region associated to a discrete edge mapping to ℓ.

discrete dynamics

d) $\forall(\ell,\ell') \in E$, $R(\ell,\ell') = R^f \times R^c$, *where* $R^f(\ell,\ell')$ *can be the identity function* $id : \mathbb{R} \mapsto \mathbb{R}$ *only if* $F^f(\ell) = F^f(\ell')$ *and* $Inv(\ell)|_{x^f} = Inv(\ell')|_{x^f}$*; otherwise* $R^f(\ell,\ell')$ *is a constant* $\mathcal{T}$*-definable function mapping to* $2^{\mathbb{R}}$. $R^c(\ell,\ell') : \mathbb{R}^m \mapsto 2^{\mathbb{R}^m}$ *is a constant* $\mathcal{T}$*-definable function;*

relevant sets

e) $\forall(\ell,\ell') \in E, \ell \in L$, *the guard-set* $G(l,l')$*, the invariant-set* $Inv(\ell)$*, and (if any) the initial set* $Init(\ell)$ *are definable within* $\mathcal{T}$*;*

f) $\forall\ell \in L$, $Inv(\ell)$ *is a* closed *and* bounded *set;*

g) $\forall\ell \in L$, *there exists a strict positive constant* $d > 0$ *such that:*
- $*$ *for each* $\mathbf{v} \in \bigcup_{\ell'|(\ell',\ell)\in E} R(\ell',\ell)(G(\ell',\ell)) \cup Init(\ell)$
- $*$ *for each* $\mathbf{w} \in \bigcup_{\ell''|(\ell,\ell'')\in E} G(\ell,\ell'')$

the distance between $\mathbf{v}$ *and* $\mathbf{w}$ *is at least* d*, i.e.* $||\mathbf{v} - \mathbf{w}|| \geq d$.

Lemma 4 states that it is possible to solve a reachability problem on a given MasterSlave o-minimal automata, by checking only runs that traverse at most k edges, where k is a proper constant. The proof of Lemma 4 is based exactly on the two properties discussed before formalizing our automata.We rely on the same properties, and on the o-minimality of the theory underlying the definition of our systems, to prove Theorem 3, stating that MasterSlaves o-minimal automata admit finite bisimulation.

Lemma 4. *Let* H *be a partitioned o-minimal. There is a constant* k *such that for each state of* H*,* $(\ell,\mathbf{w})$*,* $(\ell,\mathbf{w})$ *is reachable in* H *if and only if* H *admits a run traversing at most* k *discrete edges and leading to* $(\ell,\mathbf{w})$*.*

Theorem 3. *MasterSlaves o-minimal automata admit finite bisimulation.*

The decidability of the reachability problem for MasterSlaves($\mathsf{OF}(\mathbb{R})$) automata follows directly from Theorem 3 (or, equivalently from Lemma 4) and from decidability of o-minimal $\mathsf{OF}(\mathbb{R})$ theory.

Theorem 4. *The reachability problem is decidable for MasterSlaves(*$\mathsf{OF}(\mathbb{R})$*) o-minimal automata.*

8 Conclusions

In this paper we study a number of problems related both to the understanding and to the extension of the border between hybrid systems decidability and undecidability . Our starting point was the family of o-minimal automata, which is largely considered layering on such a border. In particular, we develop some not bisimulation-based proof techniques for showing decidability of (timed-bounded) reachability problems for classes of o-minimal systems. We finally analyze the possibility to explicitly introduce identity resetting variables in o-minimal automata, without crossing the undecidability border.

Acknowledgements. We thank prof. A. Policriti for many useful discussions.

References

1. R. Alur and D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.
2. R. Alur, T.A. Henzinger, G. Lafferriere, and G.J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88:971–984, 2000.
3. R. Alur, S. La Torre, and G. J. Pappas. Optimal paths in weighted timed automata. In *Proceedings of the 4th International Workshop on Hybrid Systems*, pages 49–62. Springer-Verlag, 2001.
4. D. S. Arnon, G. E. Collins, and S. McCallum. Cylindrical algebraic decomposition i: the basic algorithm. *SIAM J. Comput.*, 13(4):865–877, 1984.
5. G. Behrmann, A. Fehnker, T. Hune, K. G. Larsen, P. Pettersson, J. Romijn, and F. Vaandrager. Minimum-cost reachability for priced timed automata. In *Proceedings of the 4th International Workshop on Hybrid Systems*, pages 147–161. Springer-Verlag, 2001.
6. T. Brihaye, C. Michaux, C. Rivire, and C. Troestler. On o-minimal hybrid systems. In *Proceedings of the 7-th International Workshop on Hybrid Systems*, pages 219–233, 2004.
7. J.M. Davoren. Topologies, continuity and bisimulations. *Theoretical Informatics and Applications*, 33(4/5):357–381, 1999.
8. R. Gentilini. Reachability problems on extended o-minimal hybrid automata. RR 07-05, Dep. of Computer Science, University of Udine, Italy, 2005.
9. M. R. Henzinger, T. A. Henzinger, and P. W. Kopke. Computing simulations on finite and infinite graphs. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, page 453. IEEE, 1995.
10. T.A. Henzinger. The theory of hybrid automata. In M.K. Inan and R.P. Kurshan, editors, *Verification of Digital and Hybrid Systems*, NATO ASI Series F: Computer and Systems Sciences 170, pages 265–292. Springer-Verlag, 2000.
11. T.A. Henzinger, P.W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *Proceedings of the 27th Annual Symposium on Theory of Computing*, pages 373–382. ACM Press, 1995.
12. P.W. Kopke. *The Theory of Rectangular Hybrid Automata.* PhD thesis, Cornell University, 1996.
13. G. Lafferriere, G. Pappas, and S. Sastry. O-minimal hybrid systems. *Mathematics of Control, Signals, and Systems*, 13:1–21, 2000.
14. G. Lafferriere, J.G. Pappas, and S. Yovine. A new class of decidable hybrid systems. In *Proceedings of the Second International Workshop on Hybrid Systems*, pages 137–151. Springer-Verlag, 1999.
15. J.S. Miller. Decidability and complexity results for timed automata and semi-linear hybrid automata. In *Proceedings of the Third International Workshop on Hybrid Systems*, pages 296–309, 2000.
16. C. Courcoubetis R. Alur and T. A. Henzinger. Computing accumulated delays in real-time systems. *Formal Methods in System Design*, 11:137–156, 1997.
17. A. Tarski. A decision method for elementary algebra and geometry. 1951.
18. L. van den Dries. O-minimal structures. In W. Hodges, editor, *Logic: From Foundations to Applications*, pages 99–108. Clarendon Press, 1996.
19. L. van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1998.
20. A. J. Wilkie. Schanuel conjecture and the decidability of the real exponential field. *Algebraic Model Theory*, pages 223–230, 1997.