Composing Semi-Algebraic O-Minimal Automata ⋆

A. Casagrande[1,2], P. Corvaja[1], C. Piazza[1], and B. Mishra[3,4]

[1] DIMI, Università di Udine, Via delle Scienze, 206, 33100 Udine, Italy
[2] Istituto di Genomica Applicata, Via J.Linussio, 51, 33100 Udine, Italy
[3] Courant Institute of Mathematical Science, NYU, New York, U.S.A.
[4] NYU School of Medicine, 550 First Avenue, New York, 10016 U.S.A.

Abstract. This paper addresses questions regarding the decidability of hybrid automata that may be constructed hierarchically and in a modular way, as is the case in many exemplar systems, be it natural or engineered. Since the basic fundamental step in such constructions is a product operation, an essential property that would be desired is that the reachability property of the product hybrid automaton be decidable, provided that the component hybrid automata belong to a suitably restricted family of automata. Somewhat surprisingly, the product operation does not assure a closure of decidability for the reachability problem. Nonetheless, this paper establishes the decidability of the reachability condition over automata which are obtained by synchronizing two semi-algebraic o-minimal systems.

1 Introduction

Classically two disparate mathematical traditions have incongruously coexisted, while studying the same natural phenomena and their dynamics using two different elementary mechanistic representations. In one setting, the systems remain unchanged during a resting period, interrupted discretely and intermittently by modification of its current state to a non-neighboring distant state. In the other, the system only makes continuous changes, while meticulously avoiding any perceptibly significant changes over any infinitesimally small time interval. Common sense and intuition dictate that neither of the approaches should suffice to capture the substantial details of natural phenomena in one or the other representation, and perhaps, a higher fidelity is to be sought through better hybrid representations combining both discrete and continuous evolutions. Since their introduction (see, e.g., [2]) hybrid automata have initiated a new tradition, in the process, promising powerful tools for modeling and reasoning about complex systems: e.g., embedded and real time systems, or computational biology, where the resulting analyses are providing many new insights. Unfortunately, in their flexibility in capturing dynamics, resides also

⋆ This work is developed within the HYCON Network of Excellence, contract number FP6-IST-511368 and partially supported by the project PRIN 2005 project 2005015491. B.M. is supported by funding from two NSF ITR grants and one NSF EMT grant.

their flaws and limitations: many undecidability results proved for general hybrid automata [13] cast doubt on its suitability as a general tool that can be algorithmized and efficiently implemented. On the other hand, if these representations are further restricted, as in the powerful family of *o-minimal* systems [14], one could hope to still enjoy a fidelity of representation that far surpasses either that of a finite automata or a decidable system of differential equations, and yet avoid the curse of undecidability. In particular, the reachability problem has been shown decidable for semi-algebraic o-minimal hybrid automata [14], and their extensions: *SaCoRe* automata which allow inclusion dynamics [7] and *IDA* automata which introduce in some cases identity resets [6].

In order to build a theoretical framework that can also use these hybrid representations in a natural manner, one must shift one's attention to the description of large and complex hybrid systems that can be described in a compositional manner, built out of many elemental modules at many different levels of hierarchy. Since the basic fundamental step in a compositional construction is through a product operation, yielding a new product hybrid automaton by combining two simpler component hybrid automata, an essential desideratum of this new theoretical framework is that the reachability property of the product hybrid automaton be decidable, provided that the component hybrid automata belong to a suitably restricted decidable family of automata, e.g., one in the class of o-minimal automata. In general, the product operation does not assure a closure of decidability property for reachability condition. Nonetheless, in this paper we establish decidability of the reachability condition considering a synchronized product operation, where the elementary component automata are restricted to the decidable class of semi-algebraic o-minimal systems. Such automata appear in biological modeling, and hence could find many practical applications, particularly, when one is interested in understanding complex biological systems that have evolved from many smaller self-organizing systems.

The decidability of the reachability problem over semi-algebraic o-minimal automata can be proved by first translating the problem into a decidability problem over semi-algebraic first-order formulæ [7], since the formulæs decidability follows directly from a classical result of Tarski in [17]. Interestingly, when the translation is extended to synchronized products the presence of cycles in the component automata introduces variables ranging over the naturals. Roughly speaking the formulæ we get are linear Diophantine equations whose coefficients are algebraic reals symbolically represented by first-order formulæ. When at least one coefficient ranges over an interval the existence of a solution is easy to check. On the other hand, when all the coefficients range over finite sets of points more sophisticated methods, based on computational algebraic number theory results, are necessary.

The paper is organized as follows: Section 2 introduces the problem together with all the necessary notations; Section 3 presents our decidability result; Section 4 proves the impossibility of achieving decidability via simulation quotienting techniques and finally, Section 5 concludes with a brief discussion on possible applications as well as further research directions.

All the proofs of the results presented in this paper can be found in [5].

2 Hybrid Automata and Synchronized Product

We start by introducing some basic notions about directed graphs which are used as discrete components in hybrid automata.

Definition 1 (Labeled Directed Graph). *A* labeled directed graph *is a pair* $\langle \mathcal{V}, \mathcal{E} \rangle$ *where* $\mathcal{V}$ *is a finite set of* vertices *and* $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{L} \times \mathcal{V}$ *is a finite set of* edges *such that if* $\left\langle v_1, \lambda_1, v_1' \right\rangle$ *and* $\left\langle v_2, \lambda_2, v_2' \right\rangle$ *are two different edges in* $\mathcal{E}$*, then* $\lambda_1 \neq \lambda_2$*. If* $e = \langle v, \lambda, v' \rangle \in \mathcal{E}$ *is an edge, then we say that* $Source(e) = v$*,* $Dest(e) = v'$*, and* $Label(e) = \lambda$ *are the* source*, the* destination*, and the* label *of* e*, respectively.*

By an abuse of notation, we will also refer to them as directed graphs, when the meaning is clear from the context.

A path is nothing but a successive sequence of edges. A cycle is a path in which the first and the last edges coincide.

Definition 2 (Path and (Simple) Cycle). *Let* $G = \langle \mathcal{V}, \mathcal{E} \rangle$ *be a graph. A* path ph from $v \in \mathcal{V}$ to $v' \in \mathcal{V}$ in G *is either the vertex* v*, only if* $v = v'$*, or a sequence of edges* '$e_1, \ldots, e_n$' *such that, for all* $i \in [1, n-1]$*,* $Source(e_{i+1}) = Dest(e_i)$*,* $Source(e_1) = v$*, and* $Dest(e_n) = v'$*. In the former case, we say that* ph has length $|ph| = 0$ *and, in the latter, that* ph has length $|ph| = n$.

A path $p =$ '$e_1, \ldots, e_n$' *is a* cycle *if* $e_1 = e_n$*. Moreover, if* $e_i \neq e_j$ *for all* $i, j \in [1, n-1]$ *with* $i \neq j$*, then we say that* p *is a* simple cycle.

The standard definition of cycle requires that the first node coincides with the last one, while in our definition we impose that the first and the last edges are identical. A similar difference occurs in the definition of simple cycle. The two definitions are obviously not equivalent. However, also with our definition it is easy to see that a graph has only a finite number of simple cycles.

Before defining hybrid automata, we present some notations and conventions. Capital letters Z_m, Z_m', where $m \in \mathbb{N}$, denote variables ranging over $\mathbb{R}$. Analogously, Z denotes the vector of variables $\langle Z_1, \ldots, Z_k \rangle$ and Z' denotes the vector $\langle Z_1', \ldots, Z_k' \rangle$; and Z^n denotes the vector $\langle Z_1^n, \ldots, Z_k^n \rangle$. The temporal variables T and T' model time and range over $\mathbb{R}_{\geq 0}$. We use the small letters p, q, r, s, … to denote k-dimensional vectors of real numbers. Occasionally, we may use the notation $\varphi[X_1, \ldots, X_m]$ to stress the fact that the set of free variables of the first-order formula φ is included in the set of variables $\{X_1, \ldots, X_m\}$. Analogous notation is used over vectors of variables. Given a formula $\varphi[X^1, \ldots, X^i, \ldots, X^n]$ and a vector p of the same dimension as the vector X^i, the formula obtained by replacing X^i with p is denoted by $\varphi[X^1, \ldots, X^{i-1}, p, X^{i+1}, \ldots, X^n]$.

We are now ready to formally introduce hybrid automata. For each node of a graph we have an invariant condition and a dynamic law. The 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 activation and reset conditions.

Definition 3 (Hybrid Automata - Syntax). *A* hybrid automaton $H = (Z, Z', \mathcal{V}, \mathcal{E}, Inv, \mathcal{F}, Act, Res)$ *of dimension k consists of the following components:*

1. *$Z = \langle Z_1, \ldots, Z_k \rangle$ and $Z' = \langle Z'_1, \ldots, Z'_k \rangle$ are two vectors of reals variables;*
2. *$\langle \mathcal{V}, \mathcal{E} \rangle$ is a graph; the vertices, $\mathcal{V}$, are called* locations*;*
3. *Each vertex $v \in \mathcal{V}$ is labeled by the formula $Inv(v)[Z]$;*
4. *$\mathcal{F}$ is a function assigning to each vertex $v \in \mathcal{V}$ a continuous vector field over $\mathbb{R}^k$; we will use $f_v : \mathbb{R}^k \times \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}^k$ to indicate the solution of the vector field $\mathcal{F}(v)$; $Dyn(v)[Z, Z', T] \stackrel{def}{=} Z' = f_v(Z, T)$;*
5. *Each edge $e \in \mathcal{E}$ is labeled by the two formulæ $Act(e)[Z]$ and $Res(e)[Z, Z']$; $\overline{Res}(e)[Z'] \stackrel{def}{=} \exists Z\, Res(e)[Z, Z']$.*

For the sake of simplicity in notation we will write $\mathcal{I}(v)$, $\mathcal{A}(e)$, and $\mathcal{R}(e)$ to denote the sets of points that satisfy $Inv(v)$, $Act(e)$, and $\overline{Res}(e)$, respectively.

Definition 4 (Hybrid Automata - Semantics). *A* state *ℓ of H is a pair $\langle v, r \rangle$, where $v \in \mathcal{V}$ is a location and $r = \langle r_1, \ldots, r_k \rangle \in \mathbb{R}^k$ is an assignment of values for the variables of Z. A state $\langle v, r \rangle$ is said to be* admissible *if $Inv(v)[r]$ is true.*

The continuous reachability transition relation *$\xrightarrow{t}_C$, where $t > 0$ is the transition elapsed time, between admissible states is defined as follows:*

$$\langle v, r \rangle \xrightarrow{t}_C \langle v, s \rangle \iff \text{It holds that } s = f_v(r, t) \text{, and for each } t' \in [0, t] \text{ the formula } Inv(v)[f_v(r, t')] \text{ is true.}$$

The discrete reachability transition relation *$\rightarrow_D$ between admissible states is defined as follows:*

$$\langle v, r \rangle \xrightarrow{\langle v,\lambda,u \rangle}_D \langle u, s \rangle \iff \text{It holds that } \langle v, \lambda, u \rangle \in \mathcal{E} \text{ and the formulæ } Act(\langle v, \lambda, u \rangle)[r] \text{ and } Res(\langle v, \lambda, u \rangle)[r, s] \text{ are true.}$$

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

Building upon a combination of both continuous and discrete transitions, we can formulate a notion of *trace* as well as a resulting notion of *reachability*.

Definition 5 (Hybrid Automata - Reachability). *Let I be either $\mathbb{N}$ or an initial finite interval of $\mathbb{N}$. A* trace *of H is a sequence of admissible states $\ell_0, \ell_1, \ldots, \ell_i, \ldots$, with $i \in I$, such that $\ell_{i-1} \rightarrow \ell_i$ holds for each $i \in I$ greater than zero.*

The automaton H reaches *a point $s \in \mathbb{R}^k$ (in time t) from a point $r \in \mathbb{R}^k$ if there exists a trace $tr = \ell_0, \ldots, \ell_n$ of H such that $\ell_0 = \langle v, r \rangle$ and $\ell_n = \langle u, s \rangle$, for some $v, u \in \mathcal{V}$ (and t is the sum of the continuous transitions elapsed times).*

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

Definition 6 (Corresponding Path). *Let H be a hybrid automaton and tr be a trace of H. A* corresponding path *of tr is a path ph of $\langle \mathcal{V}, \mathcal{E} \rangle$ obtained by considering the discrete transitions occurring in tr.*

In this paper we are interested in the reachability problem for hybrid automata, namely, given a hybrid automaton H, an initial set of points $I \subseteq \mathbb{R}^k$, and a final set of points $F \subseteq \mathbb{R}^k$ we wish to decide whether there exists a point in I from which a point in F is reachable. A common approach in deciding reachability of hybrid automata is that of discretizing the automata using either equivalence relations (see, e.g., [14]) or abstractions (see, e.g., [1]). Since, as we will show later, the class investigated in this paper does not have a finite (bi)simulation quotient in general, we study reachability of hybrid automata by translating the reachability problem into first-order formulæ over the reals. The formulæ obtained by the translation include the formulæ occurring in the hybrid automata. Hence, it is necessary to select a suitable ambient theory upon which the automata of interest are to be built. A well-known class of hybrid automata is the class of *o-minimal hybrid automata* [14, 4], defined by using formulæ taken over an ambient o-minimal theory and by imposing the constraints of constant resets at discrete transitions, i.e., the resets do not depend on the point from which the edge is crossed. In the case of o-minimal automata defined by a decidable theory, reachability can be decided through bisimulation [14]. A theory which is both o-minimal and decidable is the first-order theory of $(\mathbb{R}, 0, 1, +, *, <)$ [17], also known as the theory of semi-algebraic sets. In this paper we focus on semi-algebraic o-minimal hybrid automata, i.e., o-minimal hybrid automata built over the theory of $(\mathbb{R}, 0, 1, +, *, <)$.

In order to study the reachability problem over the synchronized product of two semi-algebraic o-minimal hybrid automata we will exploit a characterization of the reachability problem over hybrid automata based on first-order formulæ over the reals (see [7, 5]).

Lemma 1. *Let H be an automaton and let ph be a path in $\langle \mathcal{V}, \mathcal{E} \rangle$. Consider the first-order formula $Reach(H)(ph)[Z, Z', T]$ defined in [5]. It holds that a point $r \in \mathbb{R}^k$ reaches a point $s \in \mathbb{R}^k$ in time t through a trace tr having ph as a corresponding path if and only if $Reach(H)(ph)[r, s, t]$ holds.*

Thus we have reduced the reachability problem over a path to that of deciding the satisfiability of an existentially quantified semi-algebraic formula. In the case of o-minimal automata, the constant resets allow to turn this result into a first-order characterization for reachability [7, 5]. As far as the complexity of this problem is concerned, the procedure proposed by Collins in [9] has a double-exponential complexity. Later Hoon Hong, using many practical heuristics, created the first popular quantifier elimination software `Qepcad`. Alternative methods have been proposed Grigorév [11] and Renegar [16] that are double-exponential in the number of quantifier alternations rather than in the number of variables. New approaches have been proposed by Basu [3]. More importantly, symbolic algebraic geometry holds many other powerful tools such as Gröbner bases and characteristic sets in its arsenal, whose utility is just beginning to be examined.

The simultaneous evolution of two or more automata with distinct continuous variables is captured by the notion of *synchronized product of hybrid automata*, also known as *parallel composition* (see, e.g., [12, 15]).

Definition 7 (Synchronized Product). *Let* $H_1 = (Z1, Z1', \mathcal{V}_1, \mathcal{E}_1, Inv_1, \mathcal{F}_1, Act_1, Res_1)$ *and* $H_2 = (Z2, Z2', \mathcal{V}_2, \mathcal{E}_2, Inv_2, \mathcal{F}_2, Act_2, Res_2)$ *be hybrid automata over distinct variables and let* ϵ *be a label not occurring in* $\mathcal{E}_1 \cup \mathcal{E}_2$*. The* synchronized product *of* H_1 *and* H_2 *is the hybrid automaton* $H_1 \otimes H_2 = (Z, Z', \mathcal{V}, \mathcal{E}, Inv, \mathcal{F}, Act, Res)$*, where:*

1. Z *(*Z'*) is the vector obtained by concatenating* $Z1$ *and* $Z2$ *(*$Z1'$ *and* $Z2'$*, respectively);*
2. $\mathcal{V} = \mathcal{V}_1 \times \mathcal{V}_2$ *and* $\mathcal{E} = \mathcal{E}_x \cup \mathcal{E}^1 \cup \mathcal{E}^2$*, where:*
   - $\mathcal{E}_x = \{e_{e_1,e_2} = \langle\langle v_1, v_2\rangle, \langle\lambda_1, \lambda_2\rangle, \langle u_1, u_2\rangle\rangle \mid e_1 = \langle v_1, \lambda_1, u_1\rangle \in \mathcal{E}_1$ *and* $e_2 = \langle v_2, \lambda_2, u_2\rangle \in \mathcal{E}_2\}$,
   - $\mathcal{E}^1 = \{e_{e,v} = \langle\langle u, v\rangle, \langle\lambda, \epsilon\rangle, \langle w, v\rangle\rangle \mid e = \langle u, \lambda, w\rangle \in \mathcal{E}_1$ *and* $v \in \mathcal{V}_2\}$, *and*
   - $\mathcal{E}^2 = \{e_{v,e} = \langle\langle v, u\rangle, \langle\epsilon, \lambda\rangle, \langle v, w\rangle\rangle \mid v \in \mathcal{V}_1$ *and* $e = \langle u, \lambda, w\rangle \in \mathcal{E}_2\}$.
3. $Inv(\langle v_1, v_2\rangle)[Z] \stackrel{def}{=} Inv(v_1)[Z1] \wedge Inv(v_2)[Z2]$*;*
4. $Dyn(\langle v_1, v_2\rangle)[Z, Z', T] \stackrel{def}{=} Dyn(v_1)[Z1, Z1', T] \wedge Dyn(v_2)[Z2, Z2', T]$*;*
5. $$Act(e_{a,b})[Z] \stackrel{def}{=} \begin{cases} Act(a)[Z1] \wedge Act(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}_x \\ Act(a)[Z1] & \text{if } e_{a,b} \in \mathcal{E}^1 \\ Act(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}^2 \end{cases}$$
6. $$Res(e_{a,b})[Z, Z'] \stackrel{def}{=} \begin{cases} Res(a)[Z1] \wedge Res(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}_x \\ Res(a)[Z1] \wedge Z2' = Z2 & \text{if } e_{a,b} \in \mathcal{E}^1 \\ Z1' = Z1 \wedge Res(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}^2 \end{cases}$$

Example 1 (Product of automata). Given the automata H_a and H_b depicted in Figure 1, their synchronized product $H_\otimes = H_a \otimes H_b$ is described in Figure 2.

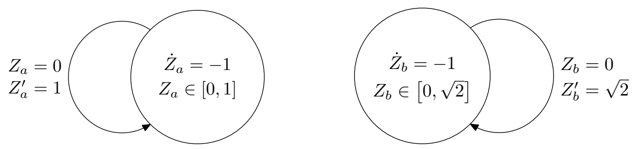

Fig. 1. The automata H_a (left) and H_b (right).

As far as reachability is concerned, we will study the reachability problem over $H_1 \otimes H_2$, where H_1 and H_2 are hybrid automata of dimensions k_1 and k_2, respectively, considering only sets of points of the form $I = I_1 \times I_2$ and $F = F_1 \times F_2$, where $I_1, F_1 \subseteq \mathbb{R}^{k_1}$ and $I_2, F_2 \subseteq \mathbb{R}^{k_2}$. This simplification will allow us to work on H_1 and H_2 quite independently. In the general case our results can be used to both under-estimate and over-estimate reachability. Unfortunately, even with this assumption, one may not always be able to ascertain the closure of reachability condition under composition; namely, starting from a set I_1 it may be possible to reach a set F_1 in the automaton H_1 and similarly, starting from a set I_2 it may be possible to reach a set F_2 in H_2, and yet starting from $I_1 \times I_2$ in $H_1 \otimes H_2$ it may not be possible to reach $F_1 \times F_2$. Moreover, the decidability of

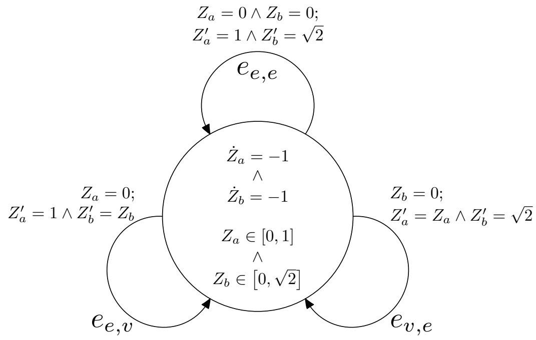

Fig. 2. The hybrid automaton $H_\otimes$ of Example 1.

reachability is not always preserved under product operation i.e., it is possible that reachability is decidable over two classes C_1 and C_2 of hybrid automata, but not over the product class $C_1 \otimes C_2 = \{H_1 \otimes H_2 \mid H_1 \in C_1 \text{ and } H_2 \in C_2\}$ (see [15]).

3 Reachability in the Synchronized Product

To construct a decidable characterization for reachability over synchronized products, we exploit the existance of a canonical path decomposition: namely, given a semi-algebraic o-minimal hybrid automaton, from any cyclic path of the automaton, we can extract both an acyclic part, by removing all the cycles occurring in it, and a set of simple cycles. The global time necessary to cover the path is then equal to the sum of the time necessary to cover the acyclic part plus multiples of the times we can spend over the simple cycles. What is important is that in the case of o-minimal automata the time we can spend over a cycle does not depend on the starting and ending point.

We define the operation which allows us to add a simple cycle to a path.

Definition 8 (Path Augmentability). *Let ph, ph' be two paths. We say that ph' is* augmentable *to ph if ph' is a simple cycle starting and ending with the edge e and ph is a path involving the edge e. If ph' is augmentable to ph we denote by $ph \oplus ph'$ the path obtained by inserting ph' in ph over the first occurrence of their common edge e, i.e., if $ph' = `e, ph'_1, e'$ and $ph = `e_1, \dots, e_{i-1}, e, e_{i+1} \dots, e_n'$ where we explicitly identify the first occurrence of e, then $ph \oplus ph' = `e_1, \dots, e_{i-1}, e, ph'_1, e, e_{i+1} \dots, e_n'$*

Let PH' be a set of (simple cyclic) paths we say that PH' is augmentable to a path ph if either $\mathsf{PH}' = \emptyset$ or there exists an ordering $ph_1, \dots, ph_m$ of the elements of PH' such that for each $i \in [1, m]$ either ph_i is augmentable to ph or there exists $j < i$ such that ph_i is augmentable to ph_j.

Notice that if ph' is augmentable to ph, then it is augmentable to $ph \oplus ph'$ too. Moreover, it is easy to see that if ph is a cyclic path, then there exist $ph_1, \dots, ph_n$, simple cyclic and acyclic, such that $ph = ph_1 \oplus \dots \oplus ph_n$.

Let H be an o-minimal hybrid automaton, $ph = `e_1, \ldots, e_m'$ be a path of H, and $Reach(H)(ph)[Z, Z', T]$ be the formula of Lemma 1 (see also [7, 5]). We define the following formula

$$\begin{aligned}\widetilde{Reach}(H)(ph)[Z, Z', T] \stackrel{\text{def}}{=} \exists \overline{Z}, \overline{Z'} \Big(& Reach(H)(e_1)[Z, \overline{Z}, 0] \wedge \\ & Reach(H)(`e_2, \ldots, e_{m-1}')[\overline{Z}, \overline{Z'}, T] \wedge \\ & Reach(H)(e_m)[\overline{Z'}, Z', 0] \Big)\end{aligned}$$

It is easy to see that the above formula characterizes all the trajectories, corresponding to ph, which start and end with a discrete transition. Because of the constant reset condition imposed on o-minimal automata, the following lemma holds.

Lemma 2. *Let H be an o-minimal automaton and ph be a path over H. If the formula $\widetilde{Reach}(H)(ph)[a, b, t] \wedge \widetilde{Reach}(H)(ph)[c, d, t']$ holds, then $\widetilde{Reach}(H)(ph)[a, b, t']$ holds.*

It follows that, if H is an o-minimal automaton, then we can use the formula $\widetilde{Reach}(H)(ph)[Z, Z', T]$ to define the set of time instants $Time(ph)$ in which ph can be covered, i.e., $Time(ph) \stackrel{\text{def}}{=} \{t \mid \exists Z, Z' \widetilde{Reach}(H)(ph)[Z, Z', t] \text{ holds}\}$. Notice that, since H is o-minimal by hypothesis, for each path ph of H the set $Time(ph)$ is o-minimal. It is easy to see the if a path ph' is augmentable to a path ph and t is the time needed to evolve through ph then the automaton can elapse a time $t + t'$, where $t' \in Time(ph')$, to evolve through $ph \oplus ph'$. The following result characterizes, the existence of a trace which elapses time t.

Lemma 3. *Let H be an o-minimal hybrid automaton of dimension k, let $r, s \in \mathbb{R}^k$ and let $t \in \mathbb{R}_{\geq 0}$. There exists a path ph such that $Reach(H)(ph)[r, s, t]$ holds if and only if there exist a path ph_0 and a set of paths PH such that:*

1. *ph_0 is acyclic;*
2. *$\mathsf{PH} = \{ph_1, \ldots ph_n\}$ is augmentable to ph_0;*
3. *we can choose both t_0 such that $Reach(H)(ph_0)[r, s, t_0]$ holds and for each ph_i two finite non empty sets $\{t_i^0, \ldots, t_i^{m_i}\} \subseteq Time(ph_i)$ and $\{k_i^0, \ldots, k_i^{m_i}\} \subseteq \mathbb{N}_{>0}$ such that $t = t_0 + \sum_{i=1}^{n} \sum_{j=0}^{m_j} k_i^j * t_i^j$.*

In the above lemma the natural number k_i^j represents the number of iterations over the cycle ph_i which are covered in time t_i^j. Intuitively, we impose $k_i^j > 0$ since if there exists ph_p which is augmentable to ph_i only, then it is necessary to cover ph_i at least once, in order to reach ph_p.

The above result suggests a verification technique for o-minimal automaton time reachability. Exploiting such result, we can propose a characterization of synchronized product reachability.

Theorem 1. *Let H_1 and H_2 be two o-minimal automata of dimensions k_1 and k_2, respectively, and $I_1, F_1 \subseteq \mathbb{R}^{k_1}$ and $I_2, F_2 \subseteq \mathbb{R}^{k_2}$ be characterized by the first-order semi-algebraic formulæ $\mathcal{I}_1[Z]$, $\mathcal{F}_1[Z]$, $\mathcal{I}_2[Z]$, and $\mathcal{F}_2[Z]$. The automaton $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ if and only if there exist two acyclic paths ph_1 and ph_2 and two sets of paths $\mathsf{PH}_1 = \{ph^1_1, \dots, ph^1_{n_1}\}$ and $\mathsf{PH}_2 = \{ph^2_1, \dots, ph^2_{n_2}\}$ augmentable to ph_1 and ph_2, respectively, such that for each $h \in \{1, 2\}$ it holds that there exists t_h satisfying $\exists Z, Z'(Reach(H_h)(ph_h)[Z, Z', T] \wedge \mathcal{I}_h[Z] \wedge \mathcal{F}_h[Z])$ and for each ph^h_i there exist two finite non empty sets $\{t^0_{(i,h)}, \dots, t^{m_{(i,h)}}_{(i,h)}\} \subseteq Time(ph^h_i)$ and $\{k^0_{(i,h)}, \dots, k^{m_{(i,h)}}_{(i,h)}\} \subseteq \mathbb{N}_{>0}$ such that*

$$\sum_{i=1}^{n_1} \sum_{j=0}^{m_{(i,1)}} k^j_{(i,1)} * t^j_{(i,1)} - \sum_{i=1}^{n_2} \sum_{j=0}^{m_{(i,2)}} k^j_{(i,2)} * t^j_{(i,2)} = t_2 - t_1$$

We introduce the following definition based on the above theorem.

Definition 9. *Let H_1 and H_2 be two o-minimal automata. Let ph_1, ph_2 be two paths over H_1 and H_2, respectively. Let PH_1 and PH_2 be two sets of paths augmentable to ph_1 and ph_2, respectively. We say that* $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ through $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ *if the hypothesis of Theorem 1 with respect to $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ are satisfied.*

We will spend the remaining part of this section to show that the characterization provided by Theorem 1 is decidable.

First of all, we assume that H_1 and H_2 are two semi-algebraic o-minimal automata of dimensions k_1 and k_2, respectively, and that $I_1, F_1 \subseteq \mathbb{R}^{k_1}$ and $I_2, F_2 \subseteq \mathbb{R}^{k_2}$ are characterized by the first-order semi-algebraic formulæ $\mathcal{I}_1[Z]$, $\mathcal{F}_1[Z]$, $\mathcal{I}_2[Z]$, and $\mathcal{F}_2[Z]$. Furthermore, we assume that the paths ph_1 and ph_2 and the sets of paths PH_1 and PH_2 augmentable to ph_1 and ph_2, respectively, are given and we study the reachability problem with respect to these paths.

Since, as noticed above, $Time(ph)$ is an o-minimal set, either it contains an interval or it consists of a finite number of time points. Given a set PH of paths we will say that PH is *time-empty* if either $\mathsf{PH} = \emptyset$ or for each $ph \in \mathsf{PH}$ it holds that $Time(ph) = \{0\}$. We distinguish three cases:

(0) both PH_1 and PH_2 are time-empty;
(1) either PH_1 or PH_2 is not time-empty and there exists a simple cycle ph^h_i such that $Time(ph^h_i)$ contains an interval;
(2) either PH_1 or PH_2 is not time-empty and for each simple cycle ph^h_i the set $Time(ph^h_i)$ consists of a finite number of points.

Let us consider case **(0)**. Theorem 1 tells us that, in this case, the synchronized product reachability can be tested by verifying whether the intersection of $Time(ph_1)$ and $Time(ph_2)$ is not empty. This can be done simply by deciding whether the semi-algebraic formula

$$\exists T_1 \geq 0 \exists T_2 \geq 0 \exists Z_1, Z'_1, Z_2, Z'_2 \Big(\mathcal{I}_1[Z_1] \wedge Reach(H_1)(ph_1)[Z_1, Z'_1, T_1] \wedge \mathcal{F}_1[Z'_1] \wedge \\ \mathcal{I}_2[Z_2] \wedge Reach(H_2)(ph_2)[Z_2, Z'_2, T_2] \wedge \mathcal{F}_2[Z'_2] \wedge 0 = T_1 - T_2\Big)$$

holds. Hence, from Tarski's result, we can deduce the following theorem.

Theorem 2 (Case 0). *Verifying whether $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ through ph_1, PH_1, ph_2, PH_2, where both PH_1 and PH_2 are time-empty, is decidable.*

As far as case **(1)** is concerned we can further split it as follows: **(1.a)** both PH_1 and PH_2 are not time-empty; **(1.b)** either PH_1 or PH_2 is time-empty.

In case **(1.a)** the decidability of reachability will be a consequence of density of the time interval. In particular, if there exist two simple cycle $ph^1 \in \mathsf{PH}_1$ and $ph^2 \in \mathsf{PH}_2$ such that $Time(ph^1)$ contains an interval (t_a, t_b) and $t_2 \in Time(ph^2)$, with $t_2 > 0$, then there exists a number n_1 of iterations over ph^1 and a number n_2 of iterations over ph^2 such that H_1 and H_2 can elapse the same amount of time over ph^1 and ph^2, respectively i.e., $n_1 * t_1 = n_2 * t_2$.

Theorem 3 (Case 1.a). *If both PH_1 and PH_2 are not time-empty and there is $ph_i^h \in \mathsf{PH}_1 \cup \mathsf{PH}_2$ such that $Time(ph_i^h)$ contains an open non empty interval, then verifying whether $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ through $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ is decidable.*

We cannot use the decision technique proposed by Theorem 3 for case **(1.b)** because either PH_1 or PH_2 is time-empty. However, if $Time(ph_1^1)$, with $ph_1^1 \in \mathsf{PH}_1$, contains an interval (t_a, t_b) and PH_2 is time-empty, then either $t_a = 0$ or $t_a > 0$. In the former case H_1 can spend any wanted time t by cycling on ph_1^1. In the latter, the number of cycles elapsing a time $t \in \mathbb{R}$ is upper bounded. Since the problem is symmetric with respect to H_1 and H_2, we analyze the case in which PH_2 is time-empty.

Theorem 4 (Case 1.b). *If there exists $ph_i^1 \in \mathsf{PH}_1$ such that $Time(ph_i^1)$ contains a non empty interval and PH_2 is time-empty, then the problem of verifying whether $H_1 \times H_2$ reaches $F_1 \times F_2$ from $I_1 \otimes I_2$ through $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ is decidable.*

To get the decidability of both case **(0)** and case **(1)**, we simply exploit Tarski's result and the density of $\mathbb{R}$. In particular, case **(0)** and case **(1.a)** have been reduced to a decidability problem for a semi-algebraic formula over the reals, while case **(1.b)** has been mapped into a decidability problem for a semi-algebraic formula with a bounded integer parameter. To decide case **(2)**, we must apply a different technique. For all $h \in \{1, 2\}$ and $i \in [1, n_h]$, we know how to characterize the time elapsed along every single cycle ph_i^h. In particular, this step can be effectively performed by exploiting a formula $\psi_i^h[T]$. We wish to known whether there exist both a set of natural numbers $\{n_i^h\}$ and a set of time $\{t_i^h\}$ such that $\psi_i^h[t_i^h]$ and $\sum_{i\in[1,n_1]} n_i^1 * t_i^1 - \sum_{i\in[1,n_2]} n_i^2 * t_i^2 = t$, where t is the time needed to reach the ending point from the starting point.

The above formula is neither a semi-algebraic formula, since it involves natural numbers, nor a "standard" linear Diophantine equation, since the coefficients t_i^h are solutions of semi-algebraic formulæ. However, this problem can be solved combining computational algebraic number theory algorithms (see, e.g., [8]) with linear Diophantine equation algorithms (see, e.g., [10]).

Theorem 5 (Case 2). *If $\mathsf{PH}_1 \cup \mathsf{PH}_2$ is not time-empty and for each $ph_i^h \in \mathsf{PH}_1 \cup \mathsf{PH}_2$ it holds that $Time(ph_i^h)$ is a finite set of points, then the problem of verifying whether $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ through $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ is decidable.*

From the above theorems, since a graph has only a finite number of acyclic paths and a finite number of simple cycles, we obtain the following result.

Corollary 1. *Let H_1 and H_2 be semi-algebraic o-minimal automata of dimensions k_1 and k_2, respectively. Let $I_1, F_1 \subseteq \mathbb{R}^{k_1}$ and $I_2, F_2 \subseteq \mathbb{R}^{k_2}$ be characterized by first-order semi-algebraic formulæ. Verifying that $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ is decidable.*

4 Simulation in the Synchronized Product

The notion of *simulation* was introduced by Milner as a means to compare programs. Roughly speaking, a hybrid automaton H simulates H', if every behavior of H' can be matched by H. In hybrid automata context, the most interesting type of simulation is the *time-abstract simulation*.

Definition 10 (Time-Abstract Simulation). *Let H and $\overline{H}$ be two automata of dimensions k and $\overline{k}$, respectively, and F be a set of formulæ. A relation R between H and $\overline{H}$ states is a* time-abstract simulation preserving F *if and only if, for each pair of states $q = \langle v, r\rangle$ and $\tilde{q}$ of H and for each state $q' = \langle v', r'\rangle$ of $\overline{H}$, if $(q, q') \in R$ then:*

- *$\varphi[r]$ holds if and only if $\varphi[r']$ for all $\varphi[Z] \in F$;*
- *for each edge e of H such that $q \xrightarrow{e}_D \tilde{q}$ in H there exist an edge e' and a state $\tilde{q}'$ such that $Label(e) = Label(e')$, $q' \xrightarrow{e'}_D \tilde{q}'$ in $\overline{H}$, and $(\tilde{q}, \tilde{q}') \in R$;*
- *if $q \rightarrow_C \tilde{q}$ in H, then there exists a state $\tilde{q}'$ such that $q' \rightarrow_C \tilde{q}'$ in $\overline{H}$ and $(\tilde{q}, \tilde{q}') \in R$.*

If there exist two time-abstract simulations R and R' preserving F such that $(q, q') \in R$ and $(q', q) \in R'$ then q and q' are *simulation equivalent with respect to F*, denoted by $q \simeq_F q'$. For any hybrid automaton H, the relation $\simeq_F$ between states of H is an equivalence relation. Hence, we can consider the $\simeq_F$'s equivalence classes $[q]_{\simeq_F}$ and the quotient set $\left(\mathcal{V} \times \mathbb{R}^k\right) / \simeq_F$ where $\mathcal{V} \times \mathbb{R}^k$ is the set of states of H. It has been proved that, given a hybrid automaton H, there exists an unique transition relation $\rightarrow_{\simeq_F}$ such that $| \rightarrow_{\simeq_F} |$ is minimal and H and the transition system $H/\simeq_F = \langle \mathcal{V} \times \mathbb{R}^k / \simeq_F, \mathcal{L}, \rightarrow_{\simeq_F}\rangle$ are simulation equivalent with respect to F. Such a transition system is said *simulation quotient preserving F* of H and it maintains some of the properties of H. In particular, $[q_j]_{\simeq_F}$ is reachable from $[q_i]_{\simeq_F}$ in $H/\simeq_F$ if and only if there exist two states $\tilde{q}_i$ and $\tilde{q}_j$ of H such that $\tilde{q}_i \in [q_i]_{\simeq_F}$, $\tilde{q}_j \in [q_j]_{\simeq_F}$, and $\tilde{q}_i$ reaches $\tilde{q}_j$. We say that an automaton H has a *finite simulation quotient* if, for all set of formulæ F, H has a finite simulation quotient preserving F. A *bisimulation* is a symmetric simulation. If a hybrid automaton admits a finite bisimulation quotient, then it also admits a finite simulation quotient.

Even if in [14] it has been proved that every o-minimal automaton admits a finite bisimulation quotient, in this section we prove that there exist semi-algebraic o-minimal automata whose synchronized product does not admit a finite simulation quotient. In particular, we prove that the automaton $H_\otimes$ of Example 1, which can be easily proved to be semi-algebraic, does not admit a finite simulation. To prove this fact, we show that there exists an infinite succession of states $(q_i)_{i\in\mathbb{N}}$ such that q_i reaches q_{i+1} in $H_\otimes$ and $[q_i]_{\simeq_\emptyset} \neq [q_j]_{\simeq_\emptyset}$, for all simulation equivalences between $H_\otimes$'s states $\simeq$ and all $i \neq j \in \mathbb{N}$.

Let us consider the succession $S(i)$ defined as $S(i) \stackrel{\text{def}}{=} i - \left\lfloor \frac{i}{\sqrt{2}} \right\rfloor \sqrt{2}$ with $i \in \mathbb{N}$.

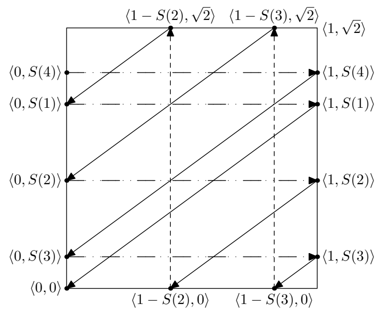

Fig. 3. Infinite states which are not similar in the automaton $H_\otimes$ of Example 1.

As intuitively shown in Figure 3 there is an infinite number of states of the form $(\langle v, \langle 0, S(i)\rangle\rangle)$ which are not simulation equivalent.

Theorem 6. *Consider the automaton $H_\otimes$ of Example 1. Let $R \subseteq \left(\mathcal{V}_\otimes \times \mathbb{R}^2\right) \times \left(\mathcal{V}_\otimes \times \mathbb{R}^2\right)$ be a time-abstract simulation. If $(\langle v, \langle 0, S(i)\rangle\rangle, \langle v, \langle 0, S(j)\rangle\rangle) \in R$, then $i = j$.*

As a direct consequence of the preceding result, we have proven that $H_\otimes$ does not admit a finite simulation quotient.

Corollary 2. *There exist synchronized products of semi-algebraic o-minimal automata, which possess an infinite simulation quotient.*

5 Applications and Conclusions

In this paper we studied the behavior of two semi-algebraic o-minimal automata evolving concurrently. In particular, we showed that the reachability problem for synchronized product of semi-algebraic o-minimal hybrid automata is decidable. To achieve such a result we exploited Tarski's decidability result on semi-algebraic theory, density results over the reals, algorithms to solve the membership problems over algebraic fields, and algorithms for solving systems of linear Diophantine equations. The combination of these techniques allowed us to prove the decidability of particular formulæ involving both real and integer variables. Moreover, we were able to reduce the reachability problem of synchronized product of semi-algebraic o-minimal hybrid automata to a decidability problem over such formulæ and in the process proving the decidability of the reachability problem itself. Since we showed that the studied automaton class does not admit a finite simulation quotient, we also proved that such a result cannot be achieved using finite quotient techniques.

To illustrate the utility of the theoretical frameworks we have proposed, we next sketch two examples, both taken from the field of system biology. First example concerns a ubiquitous motif in biochemical pathways, composed of mutually repressing pair of proteins A and B, operating as a bistable switch. Analyzing the concentration traces of A, we will soon observe that we can approximate its behaviors with a semi-algebraic o-minimal hybrid automaton, relatively accurately. This assumption is quite reasonable, since the dynamics can be approximated through Taylors method with polynomials and the constant resets can safely approximate a certain level of uncertainty. Symmetrically, we can draw an analogous automaton for B. We can now exploit the new methodology for product automata to study the nature of their interaction and examine what other unstable or metastable states that can be reached when the proteins interact. For instance, since A is a repressor for B and vice-versa, then in the product of the two automata from a region near the maximum value of A and the minimum of B it should be possible to reach a region near the minimum of A and the maximum of B and vice-versa.

A more complex example concerns multiple clock-like dynamics that coexist within a cell, and are speculated to play a role in temporal multiplexing of biological processes. As noticed in [18, 19] the set of metabolic reactions executed in a cell follow an ultradian clock dynamics, since they must coordinate those reactions, which are incompatible as well as others, which produce toxic by-products. Hence, it is important to understand the exact details of the mechanisms, which have evolved in order that the cell can avoid dangerous situations. Spatial compartmentalization is not always able to explain these phenomena. Temporal compartmentalization (or multiplexing) better models the repeated temporal segregations of metabolic processes over successive cycles which have been experimentally observed. Many concrete examples have been presented in [18, 19] (e.g., circadian cycle and metabolic cycle in yeast). The synchronized product presented here can be exploited to automatically model the combined cyclic behaviors of different metabolic processes occurring within a cell.

Time-complexity issues limits the applicability of our result. Nevertheless it presents some intriguing theoretical features. First of all, to prove the decidability of synchronized product we take advantage from the decidability of a very simple mixed real-integer language. Such approach mimes in some senses the continuous-discrete behavior described by hybrid systems, but, as far as we know, it has not been investigated yet. We believe that such techniques can be extended to handle more complex languages and, hence, to decide more sophisticated hybrid systems. Moreover, real systems are built by many components which can interact with each other. Unfortunately, models describing such systems may have a number of discrete states exponential with respect to the number of the systems components themselves. This problem is known as the state explosion problem. Different techniques have been developed to address this issue: above all symbolic model checking, abstract model checking, partial order reduction,and equivalence reductions. All such techniques use a top-down approach i.e., starting from the entire system they aim to reduce the state space. This approach faces two important hurdles: it assumes to handle the overall system representation, and this is a strong assumption for many biological systems having hundreds of interacting components; it does not yet exploit the possibility of verifying the decidable parts of the system. For these reasons, we aim to apply the bottom-up approach (i.e., verify each system's component and combine the results). and deciding the reachability problem for synchronized product of o-minimal hybrid automata can be seen as a first step over a hybrid automaton compositional theory. Notice that it is proved in [15] that the decidability problem for synchronized product of four semi-algebraic hybrid automata whose resets are either constant or identity is not decidable. Despite this fact, the decidability of reachability problem for the closure under synchronized product of semi-algebraic o-minimal automata is still an open problem. Moreover, the technique proposed in this paper emphasizes the hardest cases to decide (case **(2)**) an suggests a class of automata whose closure under synchronized product has a reasonably high chance of being decidable.

References

1. Alur, R., Dang, T., and Ivancic, F. Progress on Reachability Analysis of Hybrid Systems Using Predicate Abstraction. In *Proc. of Hybrid Systems: Computation and Control (HSCC'03)* (2003), vol. 2623 of *LNCS*, Springer, pp. 4–19.
2. Alur, R., Henzinger, T. A., and Ho, P.-H. Automatic Symbolic Verification of Embedded Systems. In *IEEE Real-Time Systems Symposium '93* (1993), IEEE Computer Society Press, pp. 2–11.
3. Basu, S. An Improved Algorithm for Quantifier Elimination Over Real Closed Fields. In *IEEE Symposium on Foundations of Computer Science (FOCS'97)* (1997), pp. 56–65.
4. Brihaye, T., Michaux, C., Rivière, C., and Troestler, C. On O-Minimal Hybrid Systems. In *Proc. of Hybrid Systems: Computation and Control (HSCC'04)* (2004), R. Alur and G. J. Pappas, Eds., vol. 2993 of *LNCS*, Springer, pp. 219–233.
5. Casagrande, A., Corvaja, P., Piazza, C., and Mishra, B. Synchronized Product of Semi-Algebraic O-Minimal Hybrid Automata. Tech. rep., University of Udine, 2006. Available at http://fsv.dimi.uniud.it/papers/synchro.pdf.
6. Casagrande, A., Mysore, V., Piazza, C., and Mishra, B. Independent dynamics hybrid automata in systems biology. In *Proc. of the First International Conference on Algebraic Biology (AB'05)* (2005), Universal Academy Press, Inc., pp. 61–73.
7. Casagrande, A., Piazza, C., and Mishra, B. Semi-Algebraic Constant Reset Hybrid Automata - SACoRe. In *Proc. of the 44rd Conference on Decision and Control (CDC'05)* (2005), IEEE Computer Society Press, pp. 678–683.
8. Cohen, H. *A Course in Computational Algebraic Number Theory*, vol. 138 of *Graduate Texts in Mathematics*. Springer, 1993.
9. Collins, G. E. Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition. In *Proceedings of GI Conference on Automata Theory and Formal Languages* (1975), vol. 33 of *LNCS*, Springer, pp. 134–183.
10. Contejean, E., and Devie, H. An Efficient Incremental Algorithm for Solving Systems of Linear Diophantine Equations. *Information and Computation 113*, 1 (1994), 143–172.
11. Grigorév, D. Complexity of Deciding Tarski Algebra. *Journal of Symbolic Computation 5* (1988), 65–108.

12. Henzinger, T. A. The Theory of Hybrid Automata. In *Proc. of IEEE Symposium on Logic in Computer Science (LICS'96)* (1996), IEEE Computer Society Press, pp. 278–292.
13. Henzinger, T. A., Kopke, P. W., Puri, A., and Varaiya, P. What's decidable about hybrid automata? In *Proc. of ACM Symposium on Theory of Computing (STOCS'95)* (1995), pp. 373–382.
14. Lafferriere, G., Pappas, G. J., and Sastry, S. O-minimal Hybrid Systems. *Mathematics of Control, Signals, and Systems 13* (2000), 1–21.
15. Miller, J. S. Decidability and Complexity Results for Timed Automata and Semi-linear Hybrid Automata. In *Proc. of Hybrid Systems: Computation and Control (HSCC'00)* (2000), vol. 1790 of *LNCS*, Springer, pp. 296–309.
16. Renegar, J. On the Computational Complexity and Geometry of the First-order Theory of the Reals, parts I-III. *Journal of Symbolic Computation 13* (1992), 255–352.
17. Tarski, A. *A Decision Method for Elementary Algebra and Geometry*. Univ. California Press, 1951.
18. Tu, B. P., Kudlicki, A., Rowicka, M., and McKnight, S. L. Logic of the Yeast Metabolic Cycle: Temporal Compartmentalization of Cellular Processes. *Science 310* (2005), 1152–1158.
19. Tu, B. P., and McKnight, S. L. Metabolic cycles as an underlying basis of biological oscillations. *Nature Reviews - Molecular Cell Biology 7* (2006), 696–701.