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.
{casa,corvaja,piazza}@dimi.uniud.it, mishra@nyu.edu

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 an important step in such constructions is a product operation, which constructs a new product hybrid automaton by combining two simpler component hybrid automata, 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 composing two semi-algebraic o-minimal systems. The class of semi-algebraic o-minimal automata is not even closed under composition, i.e., the product of two automata of this class is not necessarily a semi-algebraic o-minimal automaton. However, we can prove our decidability result combining the decidability of both semi-algebraic formulæ over the reals and linear Diophantine equations. All the proofs of the results presented in this paper can be found in [1].

1 Semi-algebraic O-Minimal Automata and Composition

Hybrid automata are systems in which discrete and continuous evolutions are mixed. In particular, their discrete nature is usually modeled through *labeled directed graphs* (called graphs in the rest of this paper), i.e., directed graphs with labels on the edges. On this kind of graphs we define: a *path ph* as sequence of edges; a *cycle* as a path in which the first and the last edges coincide; a *simple cycle* as a cycle without other repetitions.

A *hybrid automaton* $H = (Z, Z', \mathcal{V}, \mathcal{E}, \mathit{Inv}, \mathcal{F}, \mathit{Act}, \mathit{Res})$ of dimension k consists of the following components:

* This work is developed within HYCON, contract number FP6-IST-511368 and supported by the projects PRIN 2005 2005015491 and BIOCHECK. B.M. is supported by funding from two NSF ITR grants and one NSF EMT grant.

A. Bemporad, A. Bicchi, and G. Buttazzo (Eds.): HSCC 2007, LNCS 4416, pp. 668–671, 2007.

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 labeled directed graph; the vertices, $\mathcal{V}$, are called *locations*;
3. Each vertex $v \in \mathcal{V}$ is labeled by the formulæ $Inv(v)[Z]$ and $Dyn(v)[Z, Z', T] \stackrel{\text{def}}{=} Z' = f_v(Z, T)$, where f_v is the solution of the continuous vector field $\mathcal{F}$;
4. Each edge $e \in \mathcal{E}$ is labeled by the two formulæ $Act(e)[Z]$ and $Res(e)[Z, Z']$.

A *state* q 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 semantics of hybrid automata is given in terms of *continuous* $\xrightarrow{t}_C$ and *discrete* $\xrightarrow{e}_D$ transitions over asmissible states in the standard way [1]. We use the notation $q \rightarrow q'$ to denote that either $q \xrightarrow{t}_C q'$ or $q \xrightarrow{e}_D q'$. A *trace* $tr = q_0, q_1, \ldots, q_n$is a sequence of admissible states connected through transitions. 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 $tr = q_0, \ldots, q_n$ of H such that $q_0 = \langle v, r \rangle$ and $q_n = \langle u, s \rangle$, for some $v, u \in \mathcal{V}$ (and t is the sum of the continuous transitions elapsed times). Given a trace tr of H we can identify at least one path of $\langle \mathcal{V}, \mathcal{E} \rangle$ underlying tr. We call such paths *corresponding paths* of tr.

A well-known class of hybrid automata is the class of *o-minimal hybrid automata* [2], defined by using formulæ taken over an ambient o-minimal theory [3] and by imposing the constraints of *constant resets at discrete transitions*. In the case of o-minimal automata defined by a decidable theory, reachability can be decided through bisimulation [2]. A theory which is both o-minimal and decidable is the first-order theory of $(\mathbb{R}, 0, 1, +, *, <)$ [4], 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 $(\mathbb{R}, 0, 1, +, *, <)$.

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 *product* (see, e.g., [5,6]) 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 concatenation of $Z1$ 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: $\mathcal{E}_x = \{e_{e_1,e_2} \,|\, e_1 \in \mathcal{E}_1 \text{ and } e_2 \in \mathcal{E}_2\}$, $\mathcal{E}^1 = \{e_{e,v} \mid e\mathcal{E}_1 \text{ and } v \in \mathcal{V}_2\}$, and $\mathcal{E}^2 = \{e_{v,e} \mid v \in \mathcal{V}_1 \text{ and } e \in \mathcal{E}_2\}$.
3. $Inv(\langle v_1, v_2 \rangle)[Z] \stackrel{\text{def}}{=} Inv(v_1)[Z1] \wedge Inv(v_2)[Z2]$;
4. $Dyn(\langle v_1, v_2 \rangle)[Z, Z', T] \stackrel{\text{def}}{=} Dyn(v_1)[Z1, Z1', T] \wedge Dyn(v_2)[Z2, Z2', T]$;
5. $Act(e_{a,b})[Z] \stackrel{\text{def}}{=} \begin{cases} Act(a)[Z1] \wedge Act(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}_x \\ Act(a)[Z1] & \text{if } e_{a,b} \in \mathcal{E}^1 \\ Act(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}^2 \end{cases}$
6. $Res(e_{a,b})[Z, Z'] \stackrel{\text{def}}{=} \begin{cases} Res(a)[Z1] \wedge Res(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}_x \\ Res(a)[Z1] \wedge Z2' = Z2 & \text{if } e_{a,b} \in \mathcal{E}^1 \\ Z1' = Z1 \wedge Res(b)[Z2] & \text{if } e_{a,b} \in \mathcal{E}^2 \end{cases}$

We study the reachability problem over $H_1 \otimes H_2$, where H_1 and H_2 are semi-algebraic o-minimal hybrid automata, considering sets of points of the form $I = I_1 \times I_2$ and $F = F_1 \times F_2$. As noticed in [6] the decidability of reachability is not always preserved under product operations, i.e., it is possible that reachability is decidable over two classes of automata, but not over the product class.

2 Our Results

A common approach in deciding reachability of hybrid automata is that of discretizing the automata using equivalence relations (see, e.g., [2]). A powerfull equivalence reduction preserving reachability is *time-abstract simulation.* Let H and $\overline{H}$ be two automata, a relation R between H and $\overline{H}$ states is a *time-abstract simulation* if and only if, for each pair of states q and $\tilde{q}$ of H and for each state q' of $\overline{H}$, if $(q, q') \in R$ then: 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 $\mathrm{Label}\,(e) = \mathrm{Label}\,(e')$, $q' \xrightarrow{e'}_D \tilde{q}'$ 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 $(\tilde{q}, \tilde{q}') \in R$. We cannot use time-abstract simulation to decide reachability.

Theorem 1. *There exist products of two semi-algebraic o-minimal automata, which possess an infinite simulation quotient.*

In order to study the reachability problem over the product of two semi-algebraic o-minimal automata we exploit a characterization of the reachability problem over hybrid automata based on first-order formulæ over the reals (see [1]): there exists a formula $\mathit{Reach}(H)(ph)[Z, Z', T]$ such that $r \in \mathbb{R}^k$ reaches $s \in \mathbb{R}^k$ in time t through a trace tr having ph as a corresponding path if and only if $\mathit{Reach}(H)(ph)[r, s, t]$ holds. We can also characterize through a first-order formula the set of time instants $Time(ph)$ in which a path ph can be covered starting and ending with discrete transitions. This means that $Time(ph)$ is a finite union of intervals and points. Moreover, we exploit the existence of a canonical path decomposition: given a semi-algebraic o-minimal automaton, from any path we can extract both an acyclic part and a set of simple cycles. In this case we say that the set of simple cycles is *augmentable* to the acyclic part. 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 points.

Theorem 2. *Let H_1 and H_2 be 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 formulæ $\mathcal{I}_1[Z1]$, $\mathcal{F}_1[Z1]$, $\mathcal{I}_2[Z2]$, and $\mathcal{F}_2[Z2]$. 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 $\mathsf{PH}_1 = \{ph^1_1, \ldots, ph^1_{n_1}\}$ and $\mathsf{PH}_2 = \{ph^2_1, \ldots, ph^2_{n_2}\}$ augmentable to ph_1 and ph_2, respectively, such that for each $h \in \{1, 2\}$ it holds that there exists t_h satisfying $\exists Zh, Zh'(\mathit{Reach}(H_h)(ph_h)[Zh, Zh', T] \wedge \mathcal{I}_h[Zh] \wedge \mathcal{F}_h[Zh'])$ and for each ph^h_i there are two finite non empty sets $\{t^0_{(i,h)}, \ldots, t^{m_{(i,h)}}_{(i,h)}\} \subseteq Time(ph^h_i)$ and $\{k^0_{(i,h)}, \ldots, k^{m_{(i,h)}}_{(i,h)}\} \subseteq \mathbb{N}_{>0}$ such that*

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

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 2 are satisfied. Given a set PH of paths we 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 prove the decidability of $H_1 \otimes H_2$ reaches $F_1 \times F_2$ from $I_1 \times I_2$ through $ph_1, \mathsf{PH}_1, ph_2, \mathsf{PH}_2$ by the following case analysis: (0) both PH_1 and PH_2 are time-empty; (1) only PH_1 or PH_2 is not time-empty and there exists a simple cycle ph_i^h such that $Time(ph_i^h)$ contains an interval; (2) both PH_1 and PH_2 are not time-empty and there exists a simple cycle ph_i^h such that $Time(ph_i^h)$ contains an interval; (3) either PH_1 or PH_2 is not time-empty and for each simple cycle ph_i^h the set $Time(ph_i^h)$ consists of a finite number of points. In case (0) the decidability follows from Tarski's result [4]. In case (1) we map our problem into that of deciding a first-order formula with a bounded integer parameter, since, 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. In case (2) the decidability is a consequence of the density of the time interval. In particular, if there exist two simple cycles $ph^1 \in \mathsf{PH}_1$ 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 exist 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. Case (3) requires the use of algorithms to solve membership problems over algebraic fields [7] and algorithms for solving systems of Diophantine equations.

Since graphs have a finite number of acyclic paths and simple cycles, it holds:

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.*

References

1. Casagrande, A., Corvaja, P., Piazza, C., Mishra, B.: Synchronized Product of Semi-Algebraic O-Minimal Hybrid Automata. Technical report, University of Udine (2006) Available at http://fsv.dimi.uniud.it/downloads/synchro.pdf.
2. Lafferriere, G., Pappas, G.J., Sastry, S.: O-minimal Hybrid Systems. Mathematics of Control, Signals, and Systems **13** (2000) 1–21
3. Van den Dries, L.: Tame Topology and O-minimal Structures. Cambridge University Press (1998)
4. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. Univ. California Press (1951)
5. Henzinger, T.A.: The Theory of Hybrid Automata. In: Proc. of IEEE Symp. on Logic in Computer Science (LICS'96), IEEE Computer Society Press (1996) 278–292
6. 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). Volume 1790 of LNCS., Springer (2000) 296–309
7. Cohen, H.: A Course in Computational Algebraic Number Theory. Volume 138 of Graduate Texts in Mathematics. Springer (1993)