Reachability Analysis of Hybrid Systems Using Bisimulations

Gerardo Lafferriere†, George J. Pappas‡, Shankar Sastry‡
†Department of Mathematical Sciences, Portland State University, Portland, OR 97207.
‡Department of EECS, University of California at Berkeley, Berkeley, CA 94720.
gerardo@mth.pdx.edu; gpappas,sastry@eecs.berkeley.edu

Abstract

A unified approach to decidability questions for the verification of hybrid systems is obtained by the construction of a bisimulation. These are finite state quotients whose reachability properties are equivalent to those of the original infinite state system. This approach has had some success in the reachability analysis of timed automata and linear hybrid automata. In this paper, we use results from stratification theory, subanalytic sets and model theory of fields in order to extend earlier results on the existence of bismimulations for certain classes of analytic vector fields.

1 Introduction

Hybrid systems consist of finite state machines interacting with differential equations. Various modeling formalisms, analysis, design and control methodologies, as well as applications, can be found in [2, 3, 4, 8, 13]. Formal verification is one of the main approaches for analyzing properties of hybrid systems. The system is first modeled as a hybrid automaton, and the property to be analyzed is expressed using a formula from some temporal logic. Then, model checking or deductive algorithms are used to guarantee that the system model indeed satisfies the desired property.

Generally, a hybrid automaton has both discrete and continuous variables. The discrete variables correspond to a discrete set of locations and evolve according to transitions called jumps. The continuous variables correspond to points in Euclidean space (or more generally on differentiable manifolds) and evolve according to differential equations. In a typical hybrid automaton model, like the one shown in Figure 1, each discrete location has an associated differential equation according to which the continuous variables evolve. If the continuous variables enter a region, called a *guard*, then the transition between locations is enabled and may be taken. If the solution exits a region called an *invariant*, then a discrete transition is forced. The discrete transitions may reinitialize the continuous variables which

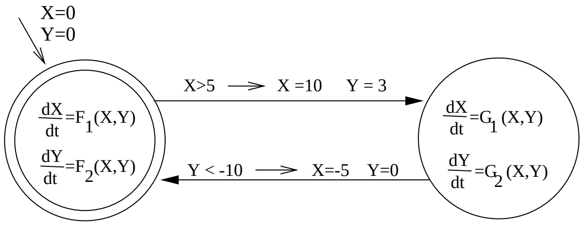

Figure 1: A typical hybrid automaton

now evolve according to the dynamics of the new location. All trajectories of the hybrid automaton originate from an initial region and may be required to avoid certain unsafe regions. Verification algorithms are essentially reachability algorithms which check whether trajectories of the hybrid system can reach the undesirable regions of the state space.

Decidability results for analyzing hybrid systems consider *bisimulations* [9]. Bisimulations are reachability preserving quotient systems in the sense that checking a property on the quotient system is *equivalent* to checking the property on the original system. If an infinite state hybrid automaton has a finite state (decidable) bisimulation then the analysis and verification procedure is decidable. Since the discrete dynamics are already finite, decidability results for hybrid systems depend mainly on obtaining finite bisimulations for continuous dynamics. In this paper, we consider the problem of constructing finite state bisimulations for purely continuous systems. More precisely, *given an analytic vector field on an analytic manifold and a finite family of sets (describing initial conditions, guards, invariants, unsafe regions), we would like to construct a finite state transition system such that checking reachability on the finite graph is equivalent to checking reachability of the original continuous system.*

To tackle this problem we need to restrict the class of sets in our description. A very rich class is provided by the subanalytic sets [5, 16]. Subanalytic sets have many desirable "finiteness" properties. Using the theory of subanalytic sets we present an algorithm for constructing bisimulations of analytic systems. We show that the algorithm terminates for various classes of vector fields on $\mathbb{R}^2$. Moreover, we show how recent results in logic model theory provide a suitable framework for these studies.

In Section 2 we review the notion of bisimulations and the algorithm for computing bisimulations for transition systems. Section 3 presents some basic facts about subanalytic sets which are used in Section 4 to construct bisimulations of analytic vector fields. In Section 5 we present results in model theory which are used in Section 6 to obtain classes of systems for which the bisimulation algorithm terminates.

2 Bisimulations

A more detailed exposition of the material described in this section can be found in [9]. A transition system $H = (Q, \Sigma, \rightarrow, Q_O, Q_F)$ consists of a (not necessarily finite) set Q of states, an alphabet Σ of events, a transition relation $\rightarrow \subseteq Q \times \Sigma \times Q$, a set $Q_O \subseteq Q$ of initial states, and a set $Q_F \subseteq Q$ of final states. The transition system is finite if the cardinality of Q is finite and it is infinite otherwise. A region is a subset $R \subseteq Q$. Given $\sigma \in \Sigma$ we define $Pre_\sigma(R)$ and $Pre(R)$ as

$$Pre_\sigma(R) = \{q \in Q \mid \exists p \in R \text{ and } (q, \sigma, p) \in \rightarrow\}$$

$$Pre(R) = \bigcup_{\sigma \in \Sigma} Pre_\sigma(R).$$

Given an equivalence relation $\sim \subseteq Q \times Q$ on the state space one can define a quotient transition system as follows. Let $Q/\sim$ denote the quotient space. A $\sim$-block is a union of equivalence classes. For a region R we denote by $R/\sim$ the smallest $\sim$-block that contains R. Thus, $Q_O/\sim$ and $Q_F/\sim$ are $\sim$-blocks containing the initial and final states respectively. The transition relation $\rightarrow_\sim$ on the quotient space is defined as follows: for $Q_1, Q_2 \in Q/\sim$, $(Q_1, \sigma, Q_2) \in \rightarrow_\sim$ iff there exist $q_1 \in Q_1$ and $q_2 \in Q_2$ such that $(q_1, \sigma, q_2) \in \rightarrow$. The quotient transition system is then $H/\sim = (Q/\sim, \Sigma, \rightarrow_\sim, Q_0/\sim, Q_F/\sim)$.

The quotient system $H/\sim$ is a *bisimulation* of H iff for all $\sigma \in \Sigma$ and all $\sim$-blocks R, the region $Pre_\sigma(R)$ is a $\sim$-block. A bisimulation is called finite if it has a finite number of equivalence classes. Bisimulations are very important because bisimilar transition systems generate the same language. Therefore, checking properties on the bisimilar quotient is equivalent to checking properties of the original transition system. This is very useful in reducing the complexity of various verification algorithms where Q is finite but very large. In addition, if H is infinite and $H/\sim$ is a finite bisimulation, then verification algorithms for infinite systems (for example, hybrid systems) are guaranteed to terminate. A successful application of this approach for timed automata can be found in [1]. It should be noted that the notion of bisimulation is very similar to the notion of dynamic consistency [6].

Two states $p, q \in Q$ are bisimilar denoted $p \approx q$ iff there exists a bisimulation $\sim$ such that $p \sim q$. It can be shown that if $p \approx q$ then

B1 $p \in Q_F$ iff $q \in Q_F$

B2 if $(p, \sigma, p') \in \rightarrow$ then there exists q' such that $(q, \sigma, q') \in \rightarrow$ and $p' \approx q'$

Based on the above characterization, given a transition system H, the following algorithm computes increasingly finer partitions of the state space Q (alternatively, it defines successive equivalence relations with the old equivalence classes being $\sim$-blocks relative to the newer equivalence class). If the algorithm terminates, then the resulting quotient transition system is a (finite) bisimulation. The state space $Q/\sim$ is called a bisimilarity quotient. At each step we define the transitions for the associated quotient system as described earlier.

Algorithm (Bisimilarity for transition systems)

Set $Q/\sim = \{Q_F, Q \setminus Q_F\}$

while $\exists\ R, R' \in Q/\sim$ and $\sigma \in \Sigma$ such that $\emptyset \neq R \cap Pre_\sigma(R') \neq R$, **do**

refine $Q/\sim = (Q/\sim \setminus \{R\}) \cup \{R \cap Pre_\sigma(R'), R \setminus Pre_\sigma(R')\}$

end while

3 Subanalytic Sets and Stratifications

In this section we describe some fundamental properties of *subanalytic sets* (see [5, 15, 16] for more detailed descriptions and proofs). Let M and N be real analytic manifolds (i.e. manifolds with real analytic transition maps between coordinate charts) and let $C^\omega(M, N)$ denote the set of analytic functions from M into N. Given an analytic manifold U, we denote by $\Sigma(C^\omega(U, \mathbb{R}))$ the Boolean algebra generated by the sets of the form $\{x : f(x) = 0\}$ or $\{x : f(x) > 0\}$, where $f \in C^\omega(U, \mathbb{R})$.

Definition 3.1 Let M be a real analytic manifold. A subset A of M is *semianalytic in* M if for every $p \in M$, there is an open neighborhood U of p in M such that $U \cap A \in \Sigma(C^\omega(U, \mathbb{R}))$. If $A \subset M$ is semianalytic in M we write $A \in \mathrm{SMAN}(M)$. Define $\mathrm{SBAN}_{rc}(M)$ and $\mathrm{SBAN}(M)$ by

1. $A \in \mathrm{SBAN}_{rc}(M)$ if and only if there is (N, f, A^*) such that N is a real analytic manifold, $f \in C^\omega(N, M)$, $A^* \in \mathrm{SMAN}(N)$, A^* is relatively compact and $A = f(A^*)$;
2. $A \in \mathrm{SBAN}(M)$ if and only if A is a locally finite union of members of $\mathrm{SBAN}_{rc}(M)$.

We say that A is *subanalytic in M* if $A \in \mathrm{SBAN}(M)$. The class $\mathrm{SBAN}(M)$ is closed under set complementation and under locally finite unions and intersections. It is also closed under inverse images by analytic functions, and under forward images by proper analytic functions. (A function f is *proper* if $f^{-1}(K)$ is compact whenever K is.) A subanalytic set has a locally finite number of connected components, each of which is subanalytic. This last property is critical for our constructions.

Example 3.1 Points are subanalytic, and so is any locally finite union of points, for example $\mathbb{Z}^n$ as subset of $\mathbb{R}^n$. Let a, $b \in \mathbb{R}$, $a < b$, then $[a,b]$, $[a,b)$, $(a,b]$ and (a,b) are subanalytic in $\mathbb{R}$. The open ball $B(p,r)$ centered at p of radius r in $\mathbb{R}^n$ is in $\mathrm{SBAN}(\mathbb{R}^n)$.

Definition 3.2 Let M be a real analytic manifold. An *analytic (C^ω) stratification* of M is a partition $\mathcal{S}$ of M with the following properties: (1) each $S \in \mathcal{S}$ is a connected, real analytic, embedded submanifold of M, (2) $\mathcal{S}$ is locally finite (i.e. every compact subset of M intersects at most finitely many sets in $\mathcal{S}$), and (3) given two sets $S, P \in \mathcal{S}$, $P \neq S$, such that $S \cap \overline{P} \neq \emptyset$ then $S \subset \overline{P}$ and $\dim S < \dim P$. (We denote by $\overline{P}$ the closure of P.) The sets in a stratification are called *strata*.

The central result on stratifications for our analysis is the following. For a proof see [15].

Theorem 3.1 *Let $\mathcal{A}$ be a locally finite family of nonempty subanalytic subsets of a real analytic manifold M. For each $A \in \mathcal{A}$, let $F(A)$ be a finite set of real analytic vector fields on M. Then there exists a subanalytic stratification $\mathcal{S}$ of M, compatible with $\mathcal{A}$, and having the property that, whenever $S \in \mathcal{S}$, $S \subset A$, $A \in \mathcal{A}$, $X \in F(A)$, then either (i) X is everywhere tangent to S or (ii) X is nowhere tangent to S. ($\mathcal{S}$ is compatible with $\mathcal{A}$ is every set in $\mathcal{A}$ is a union of sets in $\mathcal{S}$.)*

The following proposition illustrates some of the good "finite" intersection properties that analytic curves have with subanalytic sets.

Proposition 3.1 *Let I be an open interval, M a real analytic manifold and $\gamma\colon I \to M$ a real analytic function. Let $\mathcal{S}$ be a C^ω stratification of M by subanalytic sets (that is, $S \in \mathcal{S} \Rightarrow S \in \mathrm{SBAN}(M)$). If $[a,b] \subset I$ then there exists a finite partition $\{x_1, \ldots, x_n\}$ of $[a,b]$ with the property that for each $i = 1, \ldots, n-1$ there exists a stratum $S_i \in \mathcal{S}$ such that $\gamma((x_i, x_{i+1})) \subseteq S_i$.*

Example 3.2 The assumption of subanalyticity in the proposition can not be dropped. Consider the stratification of $\mathbb{R}^2$ by the following five sets:

$$\begin{aligned}
S_1 &= \{(0,0)\} \\
S_2 &= \left\{(x,y)\colon x > 0 \ \wedge \ y = x \sin\frac{1}{x}\right\} \\
S_3 &= \left\{(x,y)\colon x < 0 \ \wedge \ y = x \sin\frac{1}{x}\right\} \\
S_4 &= \left\{(x,y)\colon x \neq 0 \ \wedge \ y > x \sin\frac{1}{x}\right\} \bigcup \{(0,y)\colon y > 0\} \\
S_5 &= \left\{(x,y)\colon x \neq 0 \ \wedge \ y < x \sin\frac{1}{x}\right\} \bigcup \{(0,y)\colon y < 0\}
\end{aligned}$$

Notice that S_1, S_2 and S_3 form the graph of the function $f(x) = x \sin\frac{1}{x}$ ($f(0) = 0$), while S_4 and S_5 denote the region above and the below the graph, respectively. Each set is a C^ω, embedded submanifold of $\mathbb{R}^2$ and they clearly satisfy the condition on the dimensions. Finally, consider the constant vector field $X = \frac{\partial}{\partial x}$. Then the integral curve γ of X through $(0,0)$ is the x-axis (parameterized by x itself). Therefore, the image under γ of any interval containing 0 intersects both S_4 and S_5 an infinite number of times.

4 Bisimulations of Analytic Vector Fields

We assume that we are given a real analytic vector field X on a connected real analytic manifold M as well as a finite family $\mathcal{A}$ of relatively compact subanalytic sets. These sets may describe initial conditions M_0, final conditions M_F, guards, invariants or undesirable regions of the continuous evolution within a discrete location of a hybrid automaton. To start the partitioning process we invoke Theorem 3.1 (here there is a single vector field on each stratum) to obtain a stratification $\mathcal{S}$ of M by subanalytic sets which is compatible with $\mathcal{A}$ and such that on each $S \in \mathcal{S}$ either: (1) for all q in S, X is tangent to S at q, or (2) for all q in S, X is not tangent to S at q. We want to define a transition between two sets of the partition if there is an integral curve of X which leaves one and "immediately" enters the other. For this we need a more precise definition of what we mean by *entering* and *leaving* a stratum. We will write γ_q to denote the integral curve of X which passes through q at time 0, i.e. with $\gamma_q(0) = q$.

Definition 4.1 Given two subsets S, T of M, and a real analytic curve $\gamma : I \to M$ (I an open interval), we say that γ *leaves S through T* (or *enters T from S*) if one of the following exiting conditions is satisfied:

E1 there exist $a, b \in I$, $a < b$, such that $\gamma(t) \in S$ for all $t \in (a,b)$ and $\gamma(b) \in T$

E2 there exist $a, b \in I$, $a < b$, such that $\gamma(a) \in S$ and $\gamma(t) \in T$ for all $t \in (a,b)$.

When $q \in S$ we say that γ_q leaves S trough T if either **E1** or **E2** holds with $a = 0$.

Proposition 4.1 *Let $S \in \mathcal{S}$ and γ be as above. If there exists $t_0, t_1 \in I$ such that $\gamma(t_0) \in S$ and $\gamma(t_1) \notin S$ then there is a stratum T such that either* **E1** *or* **E2** *holds.*

To M, $\mathcal{S}$ and X we associate a transition system $(H, \Sigma, \rightarrow_{\mathcal{S}}, \mathcal{S})$, where $H = \mathcal{S}$, Σ contains one symbol t, and $(S, t, T) \in \rightarrow_{\mathcal{S}}$ iff an integral curve of X leaves S through T. The family $\mathcal{S}$ plays the role of the initial and final sets, and allows more flexibility for the study of reachability questions. We can identify $\rightarrow_{\mathcal{S}}$ with a subset of $\mathcal{S} \times \mathcal{S}$, and we will do so from now on. To obtain a bisimulation we need the stratification $\mathcal{S}$ to satisfy the following two conditions (compare to **B2** of Section 2)

1. if an integral curve of X starting at a point of the stratum S does not exit S, then no other integral curve starting in S leaves S,
2. whenever an integral curve of X which starts in S leaves the stratum through T, then all other integral curves which start in S leave the stratum through T.

To satisfy those conditions we will refine the stratification further according to exit features of the integral curves. This is captured by the following definition of the *Pre* operator (compare to the definition of $Pre(R)$ for transition systems given in Section 2).

Definition 4.2 For each $x \in M$ let $S(x)$ denote the unique set in $\mathcal{S}$ which contains x. Then define

$$Pre(R) = \{x \in M : \gamma_x \text{ leaves } S(x) \text{ through } R\}$$

The set $Pre(R)$ is well defined when $R \in \mathcal{S}$. We now describe the bisimulation algorithm (compare to the one in Section 2). If the algorithm terminates we obtain the desired finite bisimulation.

Algorithm (Bisimilarity for vector fields)

Set $M/\!\sim\; = \mathcal{S}$

Set $\rightarrow_B\; = \rightarrow_{\mathcal{S}}$

while $\exists\, R, R' \in M/\!\sim$ such that $\emptyset \neq R \cap Pre(R') \neq R$, **do**

> **Set** $R_1 = R \cap Pre(R')$; $R_2 = R \setminus Pre(R')$
> **refine** $M/\!\sim\; = (M/\!\sim \setminus \{R\}) \cup \{R_1, R_2\}$
> **update** $\rightarrow_B = (\rightarrow_B \setminus \{(R, R')\}) \cup \{(R_1, R')\} \cup \{(R_2, T) : T \neq R' \;\; (R, T) \in \rightarrow_B\}$

end while

The following proposition says that the notion of transition induced by the vector field is preserved by the construction.

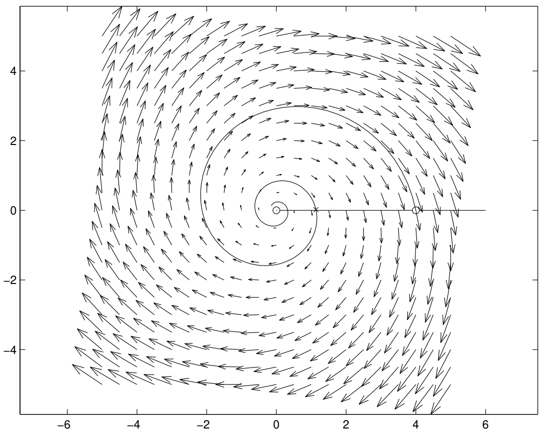

Figure 2: Process does not terminate

Proposition 4.2 *A new pair (U, V) is in $\rightarrow_B$ iff γ leaves U through V.*

Example 4.1 We show that the algorithm need not terminate. Let $M = \mathbb{R}^2$ and X be the linear vector field $\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \mathbf{x}$. Assume the stratification consists of the following five strata: $S_1 = \{(0,0)\}$, $S_2 = \{(4,0)\}$, $S_3 = \{(x,0) : 0 < x < 4\}$, $S_4 = \{(x,0) : x > 4\}$, and $S_5 = \mathbb{R}^2 \setminus \cup_{i=1}^4 S_i$. The integral curves of X are spirals moving away from the origin. Successive computations of the *Pre* operation starting with S_2 will require that we include in H (an increasing number of) pieces of the spiral through S_2 and the (infinitely many) points of intersection of that spiral with S_3. Clearly, the process will not terminate (see Figure 2).

5 Model Theory

To obtain finiteness results, we will utilize model theoretic concepts from mathematical logic. Model theory studies structures through properties of their definable sets (see [10] for general background). The basic structures of interest for this paper are that of the real numbers as a complete ordered field, symbolized by $(\mathbb{R}, +, -, \times, <, 0, 1)$, and its extensions. Each such structure L has associated a language $\mathcal{L}$. The (first order) formulas over $\mathcal{L}$ are the well-formed logical expressions obtained by using logical connectives, quantifiers $\exists\, \forall$, integer numbers as constants, the operations of additions and multiplication, and the relations $<$ and $=$ (quantification is allowed over variables). All formulas will be interpreted over the real numbers. A *definable set* in the language $\mathcal{L}$ (or of the structure L) is a subset of $\mathbb{R}^n$ (for some n) of the form $\{(a_1, \ldots, a_n) \in \mathbb{R}^n : \Phi(a_1, \ldots, a_n)\}$, where $\Phi(x_1, \ldots, x_n)$ is a formula in $\mathcal{L}$ and $x_1, \ldots, x_n$ are free (i.e. not quantified) variables in Φ. A function f is definable if its graph is a definable set. We consider only structures over the real numbers.

Definition 5.1 The theory of $\mathcal{L}$ is *o-minimal* ("order minimal") if every definable subset of $\mathbb{R}$ is a finite union of points and intervals (possibly unbounded).

Tarski was interested in the extension of the theory of the real numbers by the exponential function, $(\mathbb{R}, +, -, \times, <, 0, 1, \exp)$ (i.e., there is an additional symbol in the language for the exponential function). We denote this structure by $\mathbb{R}_{\exp}$. While such theory does not admit elimination of quantifiers, Wilkie showed in [18] that such theory is model complete, which in turns implies that it is o-minimal. Another important extension is obtained as follows. Assume f is a (real-)analytic function in a neighborhood of the cube $[-1,1]^n \subset \mathbb{R}^n$. Let $\hat{f}\colon \mathbb{R}^n \to \mathbb{R}$ be the function defined by

$$\hat{f}(x) = \begin{cases} f(x) & \text{if } x \in [-1,1]^n \\ 0 & \text{otherwise} \end{cases}$$

We call such functions *restricted analytic functions.* The structure $\mathbb{R}_{\text{exp,an}} = (\mathbb{R}, +, -, \times, <, 0, 1, \exp, \{\hat{f}\})$ is then an extension of $\mathbb{R}_{\exp}$ where there is a symbol for each restricted analytic function. One reason this structure is relevant for this paper is that all relatively compact subanalytic sets are definable in $\mathbb{R}_{\text{exp,an}}$. Moreover, if X is a linear vector field in $\mathbb{R}^n$ with real eigenvalues, then the trajectories of X are definable in $\mathbb{R}_{\text{exp,an}}$. In [17], it was shown that $\mathbb{R}_{\text{exp.an}}$ is also o-minimal. Finally, there are a few consequences of o-minimality that are crucial for our results. The proofs are contained in the various references mentioned above.

Proposition 5.1 *Assume L is an o-minimal structure. Then*

1. *Any definable set has a finite number of connected components, each of which is a definable set.*

2. *If A is definable, then so is its (topological) closure. Moreover, $\dim Fr(A) < \dim A$, where $Fr(A) = \overline{A} \setminus A$ is the frontier of A and the dimension of a set $B \subset \mathbb{R}^n$ is the maximum integer d for which there is an embedded C^1 manifold of $\mathbb{R}^n$ contained in B.*

3. *Given definable sets $A_1, \ldots, A_k$ in $\mathbb{R}^n$ (and for any integer p), there is a finite C^p stratification of $\mathbb{R}^n$ compatible with $\{A_1, \ldots, A_k\}$. In fact, for the structure $\mathbb{R}_{exp,an}$ the strata are definable (real) analytic manifolds.*

6 Finiteness Results

In this section we use the model theoretic tools of Section 5 in order to obtain classes of system for which the Bisimulation Algorithm of Section 4 terminates. The following theorem was proved in [12] but we will give the sketch of a simpler proof using model theoretic machinery.

Theorem 6.1 *Let $M = \mathbb{R}^2$, X be the linear vector field Ax and assume that the eigenvalues of A are either real or purely imaginary. Let K be a compact set and define $\mathcal{S}_K = \{S \in \mathcal{S} : S \cap K \neq \emptyset\}$ (which is therefore finite). Then the bisimulation algorithm applied to $\mathcal{S}_K$ terminates.*

Proof: Consider first the case when the eigenvalues are real. We will consider the case when the origin is the only equilibrium of X. (The other cases require minor modifications.) We assume without loss of generality that $\{(0,0)\} \in \mathcal{S}_{\mathcal{K}}$. Let $\{q_1\}, \ldots, \{q_l\}$ be the 0-dimensional strata of $\mathcal{S}_{\mathcal{K}}$. For each $i = 1, \ldots, l$ define

$$S_i = \{x \in \mathbb{R}^2 : (\exists T)\ \gamma_x(T) = q_i\}.$$

Also define $S_* = \{x \in \mathbb{R}^2 : (\forall \varepsilon > 0)(\forall T)(\exists T' > T)\ \|\gamma_x(T')\|^2 < \varepsilon^2\}$ ($\|\cdot\|$ denotes the Euclidean norm). Notice that if $S_i \cap S_j \neq \emptyset$ then $S_i = S_j$. Also, if $S_i \cap S_* \neq \emptyset$ then $S_i \subset S_*$. We assume then that we have excluded the redundancies in the sets S_i and define $S_0 = S_* \setminus \cup S_i$. Each of these (finitely many) sets, as well as the sets in $\mathcal{S}_{\mathcal{K}}$ are definable in $\mathbb{R}_{\text{exp,an}}$. For each set $R \in \mathcal{S}_{\mathcal{K}}$ and each $i = 0, \ldots, l$ the sets $R \cap S_i$ and $R \setminus \cup S_i$ are definable in $\mathbb{R}_{\text{exp,an}}$. Therefore, by o-minimality, we get that each has a finite number of connected components. Let $\tilde{\mathcal{S}}$ denote the (finite) collection of all such connected components. The collection $\tilde{\mathcal{S}}$ is then a partition of $\mathbb{R}^2$ compatible with $\mathcal{S}$ (every set of $\mathcal{S}$ is a union of sets in $\tilde{\mathcal{S}}$). The proof of the theorem follows once we establish the following claim:

Claim: At each step of the bisimilarity algorithm, $\tilde{\mathcal{S}}$ is compatible with $M/\sim$.

The claim shows that $\tilde{\mathcal{S}}$ is finer than all partitions obtained at each step. Since $\tilde{\mathcal{S}}$ is finite this clearly shows that the algorithm terminates. The details of the proof of the claim will appear in [11]. The proof for the case of imaginary eigenvalues is, a special case of Theorem 6.2 below. ■

Theorem 6.2 *If X is an analytic vector field in $\mathbb{R}^2$ which admits an analytic family of first integrals, then the bisimilarity algorithm terminates. (Here, by an analytic family of first integrals we mean an (real) analytic function $f\colon \mathbb{R}^2 \to \mathbb{R}$ such that for each trajectory γ of X the function $f(\gamma(t))$ is constant.)*

This theorem includes the case of the Hamiltonian systems on the plane with an analytic Hamiltonian. The ultimate issue of decidability is still quite open. It is not even known if the theory of $\mathbb{R}_{\exp}$ is decidable. Some special cases are suggested by our approach. For example, if all the relevant sets are semialgebraic (for example if X is a Hamiltonian vector field on the plane with a polynomial Hamiltonian and the initial conditions, guards, etc., are semialgebraic), then they are definable in $(\mathbb{R}, +, -, \times, <, 0, 1)$ for which there are effective decision procedures (see [7] for a related result).

7 Conclusions

We presented an algorithm for obtaining bisimulations of analytic vector fields. Termination is guaranteed for a class of vector fields on the plane. Bisimulations of hybrid systems can still be considered in the framework of subanalytic stratifications and o-minimal structures by allowing multiple vector fields as well as reset maps. However, the reset maps must be in some sense compatible with the flows for the procedure to terminate.

The main results of this paper are existential. For certain restricted classes of vector fields the algorithm can be made constructive (when all relevant sets are semialgebraic). Furthermore, if the bisimulation algorithm does not terminate (or is not computable), it may be useful to consider system over-approximations, or abstractions [14], for which the algorithm would terminate (or can be computed).

Acknowledgment: This work is supported by the Army Research Office under grants DAAH 04-95-1-0588 and DAAH 04-96-1-0341.

References

[1] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.

[2] R. Alur, T.A. Henzinger, and E.D. Sontag, editors. *Hybrid Systems III*. Springer-Verlag, 1996.

[3] P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors. *Hybrid Systems II*. Springer-Verlag, 1995.

[4] P Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors. *Hybrid Systems IV*. Springer-Verlag, 1997.

[5] Edward Bierstone and Pierre D. Milman. Semianalytic and subanalytic sets. *Inst. Hautes Études Sci. Publ. Math.*, 67:5–42, 1988.

[6] P.E. Caines and Y.J. Wei. Hierarchical hybrid control systems: A lattice theoretic formulation. *IEEE Transactions on Automatic Control : Special Issue on Hybrid Systems*, 43(4), April 1998.

[7] Karlis Cerans and Juris Viksna. Deciding reachability for planar multi-polynomial systems. In R. Alur, T. Henzinger, and E.D. Sontag, editors, *Hybrid Systems III*, volume 1066 of *Lecture Notes in Computer Science*, pages 389–400. Springer Verlag, Berlin, Germany, 1996.

[8] R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors. *Hybrid Systems*. Springer-Verlag, 1993.

[9] T.A. Henzinger. Hybrid automata with finite bisimulations. In Z. Fülöp and F. Gécseg, editors, *ICALP 95: Automata, Languages, and Programming*, pages 324–335. Springer-Verlag, 1995.

[10] W. Hodges. *A Shorter Model Theory*. Cambridge University Press, 1997.

[11] Gerardo Lafferriere, George J. Pappas, and Shankar Sastry. Hybrid systems with finite bisimulations. In P. Antsaklis, W. Kohn, M. Lemmon, A. Nerode, and S. Sastry, editors, *Hybrid Systems V*, Lecture Notes in Computer Science. Springer Verlag, New York, 1998. To appear.

[12] Gerardo Lafferriere, George J. Pappas, and Shankar Sastry. Subanalytic stratifications and bisimulations. In T. Henzinger and S. Sastry, editors, *Hybrid Systems : Computation and Control*, volume 1386 of *Lecture Notes in Computer Science*, pages 205–220. Springer Verlag, Berlin, 1998.

[13] O. Maler, editor. *Hybrid and Real-Time Systems*. Springer-Verlag, 1997.

[14] George J. Pappas and Shankar Sastry. Towards continuous abstractions of dynamical and control systems. In P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, editors, *Hybrid Systems IV*, volume 1273 of *Lecture Notes in Computer Science*, pages 329–341. Springer Verlag, Berlin, Germany, 1997.

[15] Héctor J. Sussmann. Subanalytic sets and feedback control. *Journal of Differential Equations*, 31(1):31–52, January 1979.

[16] Héctor J. Sussmann. Real-analytic desingularization and subanalytic sets: An elementary approach. *Transactions of the American Mathematical Society*, 317(2):417–461, February 1990.

[17] Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel Journal of Mathematics*, 85:19–56, 1994.

[18] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted pfaffian functions and the exponential function. *Journal of the AMS*, 9(4):1051–1094, Oct 1996.