A geometric approach to bisimulation and verification of hybrid systems

Mireille Broucke

Deparment of Electrical Engineering and Computer Sciences, University of California,
Berkeley CA 94720, USA,
mire@eecs.berkeley.edu

Abstract. An approximate verification method for hybrid systems in which sets of the automaton are over-approximated, while leaving the vector fields intact, is presented. The method is based on a geometrically-inspired approach, using tangential and transversal foliations, to obtain bisimulations. Exterior differential systems provide a natural setting to obtain an analytical representation of the bisimulation, and to obtain the bisimulation under parallel composition. We define the symbolic execution theory and give applications to coordinated aircraft and robots.

1 Introduction

We consider a hybrid system which is viewed as a two level system with a finite automaton at the top level and a dynamical system corresponding to each location at the lower level. Former approaches to reachability problems for hybrid systems have taken the view that the initial and final regions, and the enabling conditions and reset conditions are fixed by the problem specification. To obtain a computationally tractable algorithm, a bisimulation is formed with respect to these constraints. Here we are interested in obtaining bisimulations for verification of the safety problem for multiple autonomous agents modeled by their kinematics.

A primary focus of research is to extend the class of hybrid systems that have a finite bisimulation. Two fundamental and potentially compelling questions are: *can a bisimulation of a hybrid system be found analytically?* and, *what geometric structure should the continuous dynamics of the hybrid system possess in order to have a finite bisimulation?* We provide some results on these questions, but our approach is, in general, approximate. In particular, the initial and final regions, enabling conditions, and reset conditions will be approximated so that they are compatible with the bisimulation. This work has been inspired by the papers by Caines [2, 3] and the groundbreaking paper of Alur and Dill [1].

1.1 Notation

x' refers to the updated value of a variable x after a transition is taken, and $\dot{x}$ refers to the time derivative. d_H is the Hausdorff metric. $\overline{\sigma} \in \Sigma^*$ refers to a finite string of events $\sigma_i \in \Sigma$. All manifolds, vector fields, curves and maps are of class C^∞. Manifolds are assumed to be connected, paracompact, and Hausdorff. $C^\infty(M)$, $\mathcal{X}(M)$, and $\Omega^k(M)$ denote the sets of smooth real-valued functions, smooth vector fields, and k-forms defined on a manifold M. The wedge product of $\alpha, \beta \in \Omega(M)$ is denoted $\alpha \wedge \beta$. $\Omega(M) = \oplus_{k=0}^{\infty} \Omega^k(M)$ with the wedge product is the exterior algebra on M. $d : \Omega^k(M) \to \Omega^{k+1}(M)$ is the exterior derivative. $\omega \in \Omega^k(M)$ is *exact* if there exists an $\alpha \in \Omega^{k-1}(M)$ such that $\omega = d\alpha$.

2 Hybrid automata

A hybrid automaton is a system $A = (Q, \Sigma, D, Q^0, I, E, J, Q^f)$ consisting of the following components:

State space $Q = L \times M$ consists of a finite set L of control locations and n continuous variables $x \in M$, where M is an n-dimensional differentiable manifold.

Events Σ is a finite observation alphabet.

Vector fields $D : L \to \mathcal{X}(M)$ is a function assigning an autonomous vector field to each location. We will use the notation $D(l) = f_l$. For location l, the dynamics are given by $\dot{x} = f_l(x), f_l \in \mathcal{X}(M)$.

Initial conditions $Q^0 : L \to 2^M$ is a function assigning an initial set of states for each location. If the automaton is started in location l, then $x \in Q^0(l)$ at $t = 0$. We assume $Q^0(l) \subseteq I(l)$.

Invariant conditions $I : L \to 2^M$ is a function assigning for each location an invariant condition on the continuous states. The invariant condition $I(l) \subset M$ restricts the region on which the continuous states can evolve for location l.

Control switches E is a set of control switches. $e = (l, \sigma, l')$ is a directed edge between a source location l and a target location l' with observation $\sigma \in \Sigma$.

Jump conditions $J : E \to G \times R$ is a function assigning to each edge a guard condition and a reset condition. G is the set of guard conditions g on the continuous states, where $g \subset M$ is compact. R is the set of reset conditions r where $r : M \to 2^M$ is a compact set-valued map. We use the notation $G(e) = g_e$ and $R(e) = r_e$, and we assume for each $e = (l, \sigma, l') \in E$, $g_e \subseteq I(l)$, $r_e(g_e) \subseteq I(l')$.

Final condition $Q^f \subset Q$ is a set of final states. We will assume there is one final location so that $Q^f = \{l^f\} \times X^f, X^f \subset M$, and we assume $X^f \subseteq I(l^f)$.

Semantics A state is a pair (l, x) satisfying $x \in I(l)$. The invariant can be used to enforce edges from location l. In location l the continuous state evolves according to the vector field f_l. $\Sigma(l)$ will denote the set of events possible at $l \in L$ and $E(l)$ will denote the set of edges possible at $l \in L$. An edge is enabled when the discrete location is l and the continuous state satisfies $x \in g_e$, for $e \in E(l)$. When the transition $e = (l, \sigma, l')$ is taken, the event σ is recorded, the discrete location becomes l', and the continuous state is reset (possibly nondeterministically) to $x' := r_e(x)$.

For $\sigma \in \Sigma$ a *σ-step* is a tuple $\xrightarrow{\sigma} \subset Q \times Q$ and we write $q \xrightarrow{\sigma} q'$. Define $\phi_t^l(x)$ to be a trajectory of f_l at l, starting from x and evolving for time t. For $t \in \mathbb{R}^+$, define a *t-step* to be the tuple $\xrightarrow{t} \subset Q \times Q$. We write $(l, x) \xrightarrow{t} (l', x')$ iff (1) $l = l'$, (2) at $t = 0, x' = x$, and (3) for $t \geq 0$, $x' = \phi_t^l(x)$, where $\dot{\phi}_t^l(x) = f_l(\phi_t^l(x))$. We will use the label λ to represent a t-step with an arbitrary time passage.

A *trajectory* π of A is a finite or infinite sequence of the form $\pi : q_0 \xrightarrow{\tau_0} q_1 \xrightarrow{\tau_1} q_2 \xrightarrow{\tau_2} \ldots$ where $q_0 \in Q^0$, and for all $i \geq 0$, $q_i \in Q, \tau_i \in \Sigma \cup \mathbb{R}^+$. We assume throughout a *non-zeno* condition: every trajectory of A admits a finite number of σ-steps in any bounded time interval. Finally, given a set of initial states $Q^0 \subseteq Q$, the *reach set* of A, $Reach_A$, is the set of states that can be reached by any trajectory of A.

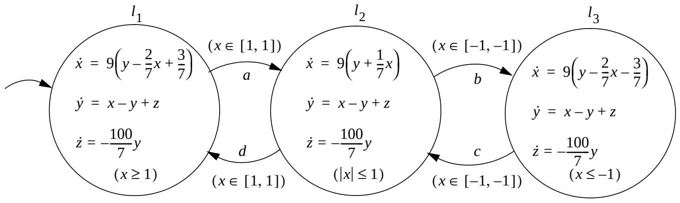
l_1
l_2
l_3
$\dot{x} = 9\left(y - \frac{2}{7}x + \frac{3}{7}\right)$
$\dot{y} = x - y + z$
$\dot{z} = -\frac{100}{7}y$
$(x \geq 1)$
$(x \in [1, 1])$
a
d
$(x \in [1, 1])$
$\dot{x} = 9\left(y + \frac{1}{7}x\right)$
$\dot{y} = x - y + z$
$\dot{z} = -\frac{100}{7}y$
$(|x| \leq 1)$
$(x \in [-1, -1])$
b
c
$(x \in [-1, -1])$
$\dot{x} = 9\left(y - \frac{2}{7}x - \frac{3}{7}\right)$
$\dot{y} = x - y + z$
$\dot{z} = -\frac{100}{7}y$
$(x \leq -1)$

Fig. 1. Double scroll hybrid automaton.

Example 1. Consider the hybrid automata of Figure 1. The invariants for locations l_1, l_2, l_3 are $x \geq 1, |x| \leq 1, x \leq -1$, respectively. The dynamics in each location are either affine linear or linear. It has been shown that this hybrid automaton has a homoclinic orbit and by Shilnikov's theorem the system has a Smale horseshoe implying the existence of a chaotic attractor [4].

Bisimulation A *bisimulation* of A is a binary relation $\simeq \subset Q \times Q$ satisfying the condition that for all states $p, q \in Q$, if $p \simeq q$ and $\sigma \in \Sigma \cup \{\lambda\}$, then
(1) if $p \xrightarrow{\sigma} p'$, then there exists q' such that $q \xrightarrow{\sigma} q'$ and $p' \simeq q'$, and
(2) if $q \xrightarrow{\sigma} q'$, then there exists p' such that $p \xrightarrow{\sigma} p'$ and $p' \simeq q'$.

3 Verification

In this section we develop an approach to verification that approximates the enabling, reset, initial and final conditions, but leaves the vector fields intact. An equivalence relation that gives a bisimulation is defined, and its existence for a vector field will be shown, in a local sense.

Let K be a subset of an n-dimensional manifold M homeomorphic to the closed, unit n-cube in $\mathbb{R}^n$. For each $l \in L$ we construct a finite cover of K, denoted C_l, consisting of a finite collection of compact n-dimensional cells c_i such that $K = \cup_i^m c_i$. The boundary of each cell consists of a set of $2n$ faces of dimension $(n-1)$ and a collection of edges of dimension $n-2$ to 1 and a set of 2^n vertices. We require $int(c_i) \neq \emptyset$ and $int(c_i) \cap int(c_j) = \emptyset, \forall i \neq j, c_i, c_j \in C_l$.

Let C be such a cover of K. The diameter of $c \in C$ is $\rho(c) = \sup\{d(x,y) | x, y \in c\}$, where d is a Riemannian metric defined on M. The *mesh* of C is $\mu(C) = \sup\{\rho(c) | c \in C\}$. The *resolution* α of C is $\alpha(C) = \inf\{\rho(c) | c \in C\}$. A cover C' *refines*[1] cover C if $\mu(C') < \alpha(C)$.

Fact *If C has a resolution $\alpha(C) > 0$, then there exists a refinement of C, denoted C' with $\alpha(C') > 0$.*

If V is a closed subset of K, we say $(V)_\mu$ is a *μ-approximation of V with respect to C with mesh μ*, given by

$$(V)_\mu = \{c \in C \mid c \cap V \neq \emptyset, \mu(C) = \mu\}.$$

If $P = \{l\} \times U \subset Q$, then we write $(P)_\mu = \{l\} \times (U)_\mu$.

Fact $d_H(V, (V)_\mu) \leq \mu$.

Let $\mathcal{C}(K) = \{C_l \mid l \in L\}$ be the set of covers of K for automaton A. $\mathcal{C}(K)$ induces an equivalence relation $\simeq$ on Q. We say $q \simeq q'$, where $q = (l, x)$ and $q' = (l', x')$ iff
(1) $l = l'$,
(2) $x \notin K$ iff $x' \notin K$,
(3) if $x, x' \in K$, then $x \in c$ iff $x' \in c$, $\forall c \in C_l$.

We say cover C_l of K at l is a *stable partition of the flow* if for all l, x, x', y and $t \geq 0$, if $(l, x) \simeq (l, x')$ and $y = \phi_t(x)$, then there exists a y' and $t' \geq 0$ such that $y' = \phi_{t'}(x')$ and $(l, y) \simeq (l, y')$.

Suppose we are given a collection of stable partitions $\mathcal{C}(K)$ of $K \subset M$ for hybrid automaton A. We write $\mathcal{C}(K, \mu)$ if $\mu(C_l) = \mu > 0$ for all $l \in L$. We define the approximate hybrid automaton

$$A_\mu = (Q, \Sigma, D, Q^0_\mu, I_\mu, E, J_\mu, Q^f_\mu).$$

Q, Σ, D, and E are unchanged. Q^0_μ, I_μ, J_μ, and Q^f_μ are the μ-approximations of the respective sets. That is,

$$\begin{aligned} Q^0_\mu(l) &= (Q^0(l) \cap K)_\mu, \\ I_\mu(l) &= (I(l) \cap K)_\mu, \\ J_\mu(e) &= ((g_e \cap K)_\mu, (r_e)_\mu) \\ Q^f_\mu &= l^f \times (X^f \cap K)_\mu. \end{aligned}$$

Let $e = (l, \sigma, l')$ and $m(x)$ be the number of cells having non-empty intersection with the point x. We define O_x to be the set of points that lie in the same intersection of cells as x. That is,

$$O_x = \Big\{ y \in \bigcap_{i=1}^{m(x)} c_i \;\Big|\; \forall c_i \in C_l \,.\, x \in c_i \Big\}. \tag{1}$$

[1] We use a nonstandard definition of refinement of covers.

The set-valued map $(r_e)_\mu$ is defined point-wise by

$$(r_e)_\mu(x) = (r_e(O_x) \cap K)_\mu.$$

The modified reset map ensures that the points of O_x are "indistinguishable" after the reset. This operation introduces extra non-determinacy in the approximated model because the identity map is not preserved, in general.

We will say A_μ is an *over-approximation* of A on K if the following additional conditions are satisfied: (1) $Q^0(l) \subseteq K$, each $l \in L$, (2) $g_e, r_e(g_e) \subseteq K$, each $e \in E$, (3) $X^f \subseteq K$, and (4) $I(l) \subseteq K$.

Fact *If A_μ is an over-approximation of A on K, then $Reach_A\big|_K \subseteq Reach_{A_\mu}\big|_K$.*

Approximate Verification Problem:
Given hybrid automaton A, $\mathcal{C}(K, \mu)$ with $\mu > 0$, and $P \subset L \times K$, determine if $(P)_\mu \cap Reach_{A_\mu} = \emptyset$.

Remarks:

1. If $(P)_\mu \cap Reach_{A_\mu} = \emptyset$ and A_μ is an over-approximation of A on K, then $P \cap Reach_A = \emptyset$. However, if either $(P)_\mu \cap Reach_{A_\mu} \neq \emptyset$ or A_μ is not an over-approximation of A on K, we have no conclusive answer about the original safety problem.
2. If $(P)_\mu \cap Reach_{A_\mu} = \emptyset$ for $\mu > 0$ then for all $\delta < \mu, (P)_\delta \cap Reach_{A_\delta} = \emptyset$. Therefore, we can find a coursest μ-approximation A_{μ^*} which verifies that the original system is safe.

Theorem 1 (Stable Partitions). *Given hybrid automaton A and $K \subset M$ homeomorphic to the closed, unit n-cube, suppose there exists $\mathcal{C}(K, \mu)$, a collection of stable partitions of K. Then $\simeq$ is a bisimulation for A_μ.*

Proof. Consider first a t-step. Suppose $(l, x) \simeq (l, y)$. Suppose there exists $t_1 \geq 0$ such that $x' = \phi_{t_1}(x)$. By the stability of C_l, there exists $t_2 \geq 0$ and y' such that $y' = \phi_{t_2}(y)$ and $(l, x') \simeq (l, y')$. Next consider a σ-step. Let (l, x) be a state satisfying $x \in (g_e)_\mu$ for some $e = (l, \sigma, l') \in E(l)$ and suppose $(l, x) \simeq (l, y)$. After the σ-step x is reset to some $x' \in (r_e(O))_\mu$. $(l, x) \simeq (l, y)$ implies $y \in (g_e)_\mu$ and $O_y = O_y$. In particular, letting $y' = x'$, we have $y \xrightarrow{\sigma} y'$ and $(l', x') \simeq (l', y')$. Reversing the data in the above two steps provides the converse statements.

3.1 Local existence

Consider a point $q = (l, x), l \in L, x \in M$. We say q is a *regular point* of A if (1) $f_l(x) \neq 0$, and (2) $x \notin \partial g_e, \forall e \in E(l)$. For such a point we can show that "locally" a stable partition for A exists. That is, at regular point q, we can find $\{l\} \times U, U \subset M$, a neighborhood of q, and a partition C_l of $\{l\} \times U$ that gives a bisimulation on $L \times M$. Almost all the interesting behavior of the hybrid system is excluded here, but the intent is to show that locally vector fields have the right structure for bisimulation, and to give the reader a flavor of the more substantial result to come later.

A *first integral* of $\dot{x} = f(x), x \in M$ is a function $g : M \to \mathrm{I\!R}$ satisfying $L_f g = 0$, where $L_f g$ is the Lie derivative of g along f. One can see that that if $\phi : I \to M$ is an integral curve, then $g \circ \phi = c$, $c \in \mathrm{I\!R}$; that is, integral curves stay on level sets of g.

A bisimulation $\simeq$ of automaton A is said to be a *local bisimulation on $P \subset L \times M$ if $p \notin P$ and $p' \notin P$ together imply $p \simeq p'$.*

Theorem 2 (Local Existence). *Let $q = (l, x_0)$ be a regular point of hybrid automaton A. Then there exists $\{l\} \times U$, a neighborhood of q, with $U \subset M$ closed, such that if A satisfies*
1) $Q^0 \subseteq \{l\} \times U$,
2) any trajectory of A that leaves $\{l\} \times U$ never returns to it, unless it is reset, then there exists a local bisimulation of A on $\{l\} \times U$.

Proof. By the Flow Box Theorem [9], there exists a closed neighborhood U of x_0 and a diffeomorphism $h : U \to V \subset \mathrm{I\!R}^n$, where $V = [-1, 1]^n$, such that $\dot{x} = f_l(x)$ expressed in $y = h(x)$ coordinates is

$$\dot{y}_1 = 0, \dot{y}_2 = 0, ...\dot{y}_n = 1. \tag{2}$$

There exist $n - 1$ independent functions $y_1 = c_1, \ldots, y_{n-1} = c_{n-1}$ that are first integrals of (2), and they define $(n-1)$ mutually transverse submanifolds, passing through each $y = (c_1, \ldots, c_{n-1}, y_n)$. A submanifold transverse to the flow of (2) is given by $y_n = c_n$. Fix $N \in \mathbb{Z}^+$ and define $\Delta = \frac{1}{N} > 0$. Take the subcollection of submanifolds $y_1 = w_1, \ldots, y_n = w_n$, where $w_i \in \{0, \pm\Delta, \pm 2\Delta, \ldots, \pm 1\}$. Call this collection of submanifolds $S = \{s_\alpha\}$ and let $\overline{U} = U \setminus \cup_\alpha \{s_\alpha\}$. $\overline{U}$ is the union of $(2N)^n$ disjoint open sets $\{c_\beta\}$. Let $\tilde{s}_\alpha = h^{-1}(s_\alpha)$ and $\tilde{c}_\beta = h^{-1}(c_\beta)$.

We can define the equivalence relation $\simeq$ on $L \times M$. For $p = (l, x)$ and $q = (l', x')$, we say $p \simeq q$ iff
1) $l = l'$,
2) $x \notin U$ iff $x' \notin U$,
3) if $x, x' \in U$, then $x \in \tilde{s}_\alpha$ iff $x' \in \tilde{s}_\alpha$ and $x \in \tilde{c}_\beta$ iff $x' \in \tilde{c}_\beta$, $\forall \alpha, \beta$.

$\simeq$ is clearly a local bisimulation on U, using the fact that no trajectories of A enter U without either being initialized there or being reset there. Finally, $\simeq$ by construction, has a finite number of equivalence classes.

4 Construction of bisimulations

In this section we elaborate on the geometric construction suggested in the previous section to show how to derive an analytical representation of the bisimulation. The main geometric tool is foliations. The reader is referred to [7], [12] for background.

Given an n-dimensional manifold M a smooth *foliation* of dimension p or codimension $q = n - p$ is a collection of disjoint connected subsets $F = \{s_\alpha\}$ whose disjoint union forms a partition of M. The foliation satisfies the property that each point of M has a neighborhood U and a system of coordinates y :

$U \to \mathbb{R}^p \times \mathbb{R}^q$ such that for each s_α, the (connected) components of $(U \cap s_\alpha)$ are given by $y_{p+1} = c_1, \ldots, y_{p+q} = c_q$, where $c_i \in \mathbb{R}$. Each connected subset is called a *leaf* of the foliation. We are interested in foliations whose leaves are regular submanifolds of dimension p in M, and we construct the foliations using submersions. A foliation globally defined by a submersion is called *simple.*

Let $f \in \mathcal{X}(M)$. We will define two types of simple co-dimension one foliations with respect to f, called tangential and transversal foliations. For this we require a notion of transversality of foliations.

A map $h : M \to N$ is *transverse* to foliation F of N if either $h^{-1}(F) = \emptyset$, or if for every $x \in h^{-1}(F)$, $h_* T_x M + T_{h(x)} F = T_{h(x)} N$. A submanifold P on M is *transverse* to foliation F of M if the inclusion map $i : P \to M$ is transverse to F. A foliation F' is said to be *transverse* to F if each leaf of F' is transverse to F. A foliation in general does not admit a transversal foliation, but a local submanifold Σ_x of M such that Σ_x intersects every leaf in at most one point (or nowhere) and $T_x \Sigma_x + T_x F = T_x M$ can be found.

A *tangential foliation* F of M is a co-dimension one foliation that satisfies $f(x) \in T_x F, \forall x \in M$; that is, f is a cross-section of the tangent bundle of F. A *transversal foliation* $F_\perp$ of M is a co-dimension one foliation that satisfies $f(x) \notin T_x F, \forall x \in M$. A tangential foliation is therefore an invariant of the flow, whereas integral curves hit the leaves of a transversal foliation transversally.

We construct a collection F_i of $n-1$ tangential foliations on $K \subset M$ and one transversal foliation $F_n := F_\perp$ on K. Additionally, we require a regularity condition on this collection of n foliations: *each pair of foliations* $(F_i, F_j), i \neq j$ *is transverse.* If the foliations are constructed via submersions, the following lemma provides an algebraic test for regularity.

Lemma 1. *Let M be an n-dimensional manifold and define $h_i : M \to \mathbb{R}, i = 1, \ldots n$, a collection of submersions on M. If dh_i are linearly independent on $K \subset M$, then the foliations defined by $h^{-1}(\mathbb{R})$ are mutually transverse on K.*

We will not use all of the leaves of a foliation, but only some finite subset of them. We *discretize* a simple co-dimension one foliation as follows. Let $h : M \to \mathbb{R}$ be the submersion of a simple co-dimension one foliation F. Given an interval $[a, b]$, a gridsize $\Delta = \frac{b-a}{N} > 0$ with $N \in \mathbb{Z}^+$, define the finite collection of points $W = \{a, a + \Delta, \ldots, b\}$. Then, $h^{-1}(W)$ is the discretization of F on $h^{-1}([a, b])$.

A bisimulation can be constructed using foliations by elaborating the following steps:

1. Find $(n-1)$ simple co-dimension one tangential foliations on $K \subset M$, for each $f_l, l \in L$.
2. Construct either a local or global (on K) transversal foliation for each f_l.
3. Check the regularity condition for mutual transversality on K.
4. Discretize the foliations to obtain a cover C_l with mesh μ, for each $l \in L$.
5. Construct the approximate system A_μ by approximating the enabling and reset conditions, and the initial and final regions using C_l for each l.

Theorem 3 (Foliations). *Given hybrid automaton A, $\mu > 0$, and an open $U \subset M$ on which, $\forall l \in L$, $f_l \in \mathcal{X}(M)$ is non-vanishing, suppose there exists a* *set of $n-1$ simple, mutually transversal co-dimension one tangential foliations on U. Then there exists $K \subset M$ homeomorphic to the closed, unit n-cube and a collection of stable partitions on K such that A_μ has a finite bisimulation.*

Proof. Suppose that the collection of tangential foliations for each l is denoted $\{F_i\}^l_{i=1,\ldots,n-1}$ and the associated submersions are $h^l_i, i = 1, \ldots, n-1$. We can find a closed set $K \subset U$ such that (1) $h_i(K) = [-1,1]$ (by rescaling h_i, if needed), and (2) there exists h^l_n independent of $h^l_i, i = 1, \ldots, n-1$, for each $l \in L$. Define the coordinates $y_1 = h_1, \ldots, y_n = h_n$. Fix $N \in \mathbb{Z}^+$ and define $\Delta = \frac{1}{N} > 0$. Take the subcollection of submanifolds $y_1 = w_1, \ldots, y_n = w_n$, where $w_i \in \{0, \pm\Delta, \pm 2\Delta, \ldots, \pm 1\}$. Call this collection of submanifolds $S = \{s_\alpha\}$ and let $\overline{K} = K \setminus \cup_\alpha \{s_\alpha\}$. $\overline{K}$ is the union of $(2N)^n$ disjoint open sets $\{c_\beta\}$. Let $\tilde{s}_\alpha = h^{-1}(s_\alpha)$ and $\tilde{c}_\beta = h^{-1}(c_\beta)$.

As in the Local Existence theorem, we can define the equivalence relation $\simeq$ on $L \times M$. For $p = (l, x)$ and $q = (l', x')$, we say $p \simeq q$ iff
1) $l = l'$,
2) $x \notin K$ iff $x' \notin K$,
3) if $x, x' \in K$, then $x \in \tilde{s}_\alpha$ iff $x' \in \tilde{s}_\alpha$ and $x \in \tilde{c}_\beta$ iff $x' \in \tilde{c}_\beta$, $\forall \alpha, \beta$.

$\simeq$ defines a stable partition on K with a finite number of equivalence classes, so we can invoke the Stable Partitions Theorem to obtain the bisimulation of A_μ.

Example [Timed automata] A timed automaton has dynamics, in Pfaffian form (see section 5), given by $\{dx_1 - dt, \ldots, dx_n - dt\}$. There are $n-1$ independent tangential foliations defined by the submersions: $x_1 - x_2 = c_1, \ldots, x_{n-1} - x_n = c_{n-1}$, where $c_i \in \mathbb{R}$. A transversal foliation is $x_n = d_n$ though the partition of [1] uses more transversal foliations because of the nature of the enabling and reset conditions: $x_1 = d_1, \ldots, x_n = d_n$. Each of the leaves of the transversal foliations are transverse to every integral curve. The partition for timed automata is exact, in the sense that it is not necessary to over-approximate regions.

Example [Brunovsky normal form] Consider the Brunovsky normal form for linear systems in $\mathbb{R}^4$ given by

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= x_3 \\ \dot{x}_3 &= x_4 \\ \dot{x}_4 &= u. \end{aligned}$$

The three tangential foliations are

$$\begin{aligned} x_1 - \frac{x_2 x_4}{u} + \frac{x_3 x_4^2}{2u^2} - \frac{x_4^4}{8u^3} &= c_1 \\ x_2 - \frac{x_3 x_4}{u} + \frac{x_4^3}{3u^2} &= c_2 \\ x_3 - \frac{1}{2u} x_4^2 &= c_3. \end{aligned}$$

A transversal foliation is $x_4 = c_4$. We confirm the regularity condition on the foliations by checking the rank of the matrix:

$$Dh = \begin{bmatrix} 1 & -\frac{x_4}{u} & \frac{x_4^2}{2u^2} & -\frac{x_2}{u} + \frac{x_3 x_4}{u^2} - \frac{x_4^3}{2u^3} \\ 0 & 1 & -\frac{x_4}{u} & -\frac{x_3}{u} + \frac{x_4^2}{u^2} \\ 0 & 0 & 1 & -\frac{x_4}{u} \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

This matrix is full rank for all $u \neq 0$; therefore, the partition is defined on all $\mathbb{R}^4$.

4.1 Topological conjugacy

Two vector fields f and g are *topologically conjugate* if there exists a homeomorphism $h : M \to N$, and h takes integral curves ϕ_t of f to integral curves ψ_t of g while preserving the parameter t. In particular, $h \circ \phi_t(x) = \psi_t(h(x))$ and $g = h_* f$. Suppose we have constructed a set of tangential and transversal foliations $\{F_1, \ldots, F_{n-1}, F_n = F_\perp)$ of $K \subset M$ for f.

Theorem 4. *Suppose f and g are topologically conjugate vector fields with homeomorphism $h : M \to N$ and the set of foliations $\{F_i\}$ defines a stable partition on $l \times K, K \subset M$ for f. Then there exists a stable partition on $l \times h(K), h(K) \subset N$ for g.*

Proof. Suppose each foliation F_i is constructed by submersion $\xi_i : M \to \mathbb{R}$. Define the set of foliations $\{G_i\}$ constructed by submersions $\eta_i = \xi_i \circ h^{-1} : N \to \mathbb{R}$. Then note that $L_g \eta_i = d(\xi_i \circ h^{-1})(h_* f) = d\xi_i \cdot f = L_f \xi_i$. Therefore, η_i form $(n-1)$ tangential foliations and one transverse foliation for g, and if ξ_i are independent, then so are η_i. Finally, the homeomorphism h maps fixed points of f to fixed points of g, so a stable partition defined on K for f non-vanishing on K, is well-defined for $h(K)$ and g is non-vanishing on $h(K)$.

5 Exterior differential systems

Tangential foliations of a vector field can be found using first integrals. A natural setting for finding first integrals is provided by exterior differential systems. The reader is referred to [10, 12] for background.

A set of independent one-forms $\omega^1, \ldots, \omega^q$ generates a Pfaffian system $I = \{\omega^1, \ldots, \omega^q\} = \{\sum f_k \omega^k | f_k \in C^\infty(M)\}$. The Frobenius theorem says that if I satisfies the Frobenius condition $d\omega^k \wedge \omega^1 \wedge \cdots \wedge \omega^q = 0$, for $k = 1, \ldots, q$, then it admits coordinates $h_1, \ldots, h_q$ such that $I = \{dh_1, \ldots, dh_q\}$. In this case the Pfaffian system is said to be *completely integrable* and the h_i are the first integrals of I. We adapt the proof of the Frobenius theorem to obtain our main result on existence of bisimulations.

Theorem 5 (First Integrals). *Given hybrid automaton A, $\mu > 0$, and an open $U \subset M$ on which, $\forall l \in L$, $\quad f_l \in \mathcal{X}(M)$ is non-vanishing, there exists $K \subset M$ homeomorphic to the closed, unit n-cube and a collection of stable partitions such that A_μ has a finite bisimulation.*

Proof. The approach is to find a codistribution of one-forms $\{w^2, \ldots, w^n\}$ such that $w^i = dh_i = 0$. Then we will show that the $n-1$ independent functions $h_i : K \to \mathbb{R}$ are submersions and by construction first integrals. They will provide $n-1$ simple, co-dimension one tangential foliations, so we can invoke the Foliations theorem to show existence of a bisimulation.

Fix l, and let $f_1 = f_l$. On some open $V \subset U$ we can find $n-1$ smooth complementary vector fields $f_2, \ldots, f_n$ such that $span\{f_1, \ldots, f_n\} = \mathbb{R}^n$ at each $x \in V$ and $\{f_1, \ldots, f_n\}$ is clearly involutive on V. Let $\phi_t^i(x)$ be the flow of f_i. Fix $x^0 \in V$. There exists W, a neighborhood of 0 in $\mathbb{R}^n$ such that the map $G : W \to V$ given by

$$(a_1, \ldots, a_n) \mapsto \phi^1_{a_1} \circ \cdots \circ \phi^n_{a_n}(x^0).$$

is well defined. Since the ϕ's commute, we can change the order of integration

$$\begin{aligned}\left(\frac{\partial G}{\partial a_i}\right)_0 &= \frac{\partial}{\partial a_i}\phi^i_{a_i} \circ \phi^1_{a_1} \circ \cdots \circ \phi^{i-1}_{a_{i-1}} \circ \phi^{i+1}_{a_{i+1}} \circ \cdots \circ \phi^n_{a_n}(x^0) \\ &= f_i(x^0).\end{aligned}$$

Since the f_i's are independent, $\frac{\partial G}{\partial a_i}$ is nonsingular, so G^{-1} exists locally on $V' \subset V$ by the Inverse Function Theorem. Let $[h_1(y), \ldots, h_n(y)]^T = G^{-1}(y), y \in V'$. By definition

$$\left[\frac{\partial G^{-1}}{\partial y}\right] \cdot \left[\frac{\partial G}{\partial a}\right] = I.$$

In particular,

$$\frac{\partial h_i}{\partial y} \cdot f_1 = 0$$

for $i = 2, \ldots, n$. So $h_2, \ldots, h_n$ are the desired functions. Since $G^{-1}(y)$ has rank n, the h_i are independent submersions.

Remark: The map G is nonsingular everywhere that $\{f_i\}$ are a complementary, involutive collection of vector fields, and V' is as large as the range of G.

5.1 Parallel composition

Bisimulation for hybrid systems is, in general, not closed under parallel composition of automata. Here we give a sufficient condition on the Pfaffian form of the continuous dynamics of each control location so that if two hybrid automata have a finite bisimulation, then so does their parallel composition. We refer the reader to [6] for the definition of composition of hybrid automata.

Theorem 6 (Parallel Composition). *Given hybrid automata* $A_1 = (L_1 \times M_1^n, \Sigma_1, D_1, Q_1^0, I_1, E_1, J_1, Q_1^f)$ *and* $A_2 = (L_2 \times M_2^m, \Sigma_2, D_2, Q_2^0, I_2, E_2, J_2, Q_2^f)$*, suppose there exist* $K_1 \subset M_1, K_2 \subset M_2$ *such that, via the First Integrals theorem, bisimulations for* $A_{1\mu}$ *and* $A_{2\mu}$ *exist. If for each pair* $(l, l'), l \in L_1, l' \in L_2$ *there exists a one-form of the Pfaffian system at* l

$$h(dx_1, \ldots, dx_n) - dt = 0,$$

and a one-form of the Pfaffian system at l'

$$h'(dx_{n+1}, \ldots, dx_{n+m}) - dt = 0,$$

such that the one-form

$$h(dx_1, \ldots, dx_n) - h'(dx_{n+1}, \ldots, dx_{n+m}) = d\alpha$$

is exact, and α *is independent of the first integrals on* K_1 *and* K_2 *of the vector fields at* l *and* l'*, respectively, then a bisimulation of* $(A_1 \times A_2)_\mu$ *exists.*

Proof. From the First Integrals theorem, we have $n-1$ first integrals for each $f_l, l \in L_1$ and $m-1$ first integrals for each $f_{l'}, l' \in L_2$, giving $n+m-2$ first integrals for the vector field $f = [f_l \quad f_{l'}]^T$. But we require $n+m-1$ first integrals to construct the bisimulation. The missing first integral is provided by the exact form α. Using the fact that $h(dx_1, \ldots, dx_n)$ has the form $\frac{dx_i}{f_i(x)}$ for some $i = 1, \ldots, n$, and similarly for h', it can be verified that α satisfies $L_f\alpha = 0$.

6 Applications

A domain of models that we wish to apply this theory to is kinematic models of rigid bodies. The symmetry in kinematics allows first integrals to be constructed. We demonstrate the ideas with several examples.

Example [Planar Aircraft] Consider the coordination problem of two aircraft A and B flying at a fixed altitude near an airport [11]. Each aircraft is modeled by a hybrid system in which an automaton location corresponds to an atomic maneuver performed with constant control inputs. The control inputs are changed instantaneously upon switching control locations. The state is $g \in SE(2)$ and X is an element of the Lie algebra $se(2)$. Assuming the aircraft does not exercise it's pitch control, the kinematic dynamics of aircraft A are given by $\dot{g} = gX$ where

$$g = \begin{bmatrix} \cos\phi & -\sin\phi & x \\ \sin\phi & \cos\phi & y \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$X = \begin{bmatrix} 0 & -u_1 & u_2 \\ u_1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

ϕ is the yaw angle, and the inputs u_1, u_2 control the yaw and velocity, respectively, of the aircraft. There are two tangential foliations given by equations

$$\begin{aligned} u_1 x - u_2 \sin\phi &= c_x \\ u_1 y + u_2 \cos\phi &= c_y \end{aligned}$$

and a transversal foliation given by $\phi = c_\phi$. Letting the state variables and inputs of aircraft B be ϕ_B, x_B, y_B, u_{1B}, and u_{2B}, analogous expressions for the tangential and transversal foliations are obtained for aircraft B. An additional tangential foliation is found for the parallel composition of the two systems given by

$$u_{1B}\phi_A - u_{1A}\phi_B = c_{AB}.$$

We check the regularity condition on the five tangential foliations and either of the two transversal foliations. Namely,

$$Dh = \begin{bmatrix} u_{1A} & 0 & -u_{2A}\cos\phi_A & 0 & 0 & 0 \\ 0 & u_{1A} & -u_{2A}\sin\phi_A & 0 & 0 & 0 \\ 0 & 0 & u_{1B} & 0 & 0 & -u_{1A} \\ 0 & 0 & 0 & u_{1B} & 0 & -u_{2B}\cos\phi_B \\ 0 & 0 & 0 & 0 & u_{1B} & -u_{2B}\sin\phi_B \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

This matrix has full rank so long as $u_{1A}, u_{1B} \neq 0$, so the partition is defined globally on $\mathbb{R}^4 \times \mathbb{T}^2$. If, in addition, $\frac{u_{1A}}{u_{1B}}$ is rational, a finite bisimulation on $K \times \mathbb{T}^2$, for compact $K \subset \mathbb{R}^4$, exists.

Example [Mobile robot] Consider the coordination problem of two mobile robots A and B, operating in a closed workspace. The robots are modeled using hybrid automata, with each control location corresponding to an atomic maneuver, such as “move forward”, or “change direction”. Each location of the automaton has a kinematic model of the associated maneuver using constant control inputs. The control input changes instantaneously upon switching locations. The kinematic model for each robot, converted to chained form [8] is the following:

$$\begin{aligned} \dot{x}_1 &= u_1 \\ \dot{x}_2 &= u_2 \\ \dot{x}_3 &= x_2 u_1 \\ \dot{x}_4 &= x_3 u_1. \end{aligned}$$

There are three tangential foliations given by the equations

$$\begin{aligned} x_2 - \frac{u_2}{u_1} x_1 &= c_2 \\ x_3 - \frac{u_1}{2u_2} x_2^2 &= c_3 \\ x_4 + \frac{1}{3}\left(\frac{u_1}{u_2}\right)^2 x_2^3 - \frac{u_1}{u_2} x_2 x_3 &= c_4. \end{aligned}$$

and a transversal foliation given by: $x_1 = c_1$.

To show these foliations define a bisimulation for each robot, we must check the regularity condition:

$$Dh = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\frac{u_2}{u_1} & 1 & 0 & 0 \\ 0 & -\frac{u_1}{u_2}x_2 & 1 & 0 \\ 0 & -\frac{u_1}{u_2}x_3 + \left(\frac{u_1}{u_2}\right)^2 x_2^2 & -\frac{u_1}{u_2}x_2 & 1 \end{bmatrix}.$$

This matrix has full rank so long as $u_1 \neq 0$ and $u_2 \neq 0$. Thus, the partition for each robot is defined globally on $\mathrm{I\!R}^4$.

When we take their parallel composition, an extra tangential foliation is introduced:

$$u_{1B}x_{1A} - u_{1A}x_{1B} = c_{AB}.$$

A calculation similar to the previous example shows that a bisimulation for the parallel composition exists.

Example [Linear systems] Finally, we consider a hybrid automaton in which each location of the automaton contains an affine linear system. The dynamics of each location are given by:

$$\dot{x_i} = \lambda_i x_i + b_i, \quad i = 1, \ldots, n$$

where $\lambda_i, b_i \in \mathrm{I\!R}$. We assume for each i that λ_i, b_i are not both zero. The tangential folations are

$$\frac{1}{\lambda_1}\ln|\lambda_1 x_1 + b_1| - \frac{1}{\lambda_2}\ln|\lambda_2 x_2 + b_2| = c_1$$

$$\vdots$$

$$\frac{1}{\lambda_{n-1}}\ln|\lambda_{n-1}x_{n-1} + b_{n-1}| - \frac{1}{\lambda_n}\ln|\lambda_n x_n + b_n| = c_{n-1}.$$

A transversal foliation is given by

$$\frac{1}{2\lambda_1}|\lambda_1 x_1 + b_1|^2 + \frac{1}{2\lambda_2}|\lambda_2 x_2 + b_2|^2 + \cdots + \frac{1}{2\lambda_n}|\lambda_n x_n + b_n|^2 = c_n.$$

We check the regularity condition as follows:

$$Dh = \begin{bmatrix} \frac{1}{|\lambda_1 x_1 + b_1|} & -\frac{1}{|\lambda_2 x_2 + b_2|} & 0 & \cdots & 0 \\ 0 & \frac{1}{|\lambda_2 x_2 + b_2|} & -\frac{1}{|\lambda_3 x_3 + b_3|} & \cdots & 0 \\ 0 & 0 & & & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & & \frac{1}{|\lambda_{n-1}x_{n-1} + b_{n-1}|} & -\frac{1}{|\lambda_n x_n + b_n|} \\ |\lambda_1 x_1 + b_1| & |\lambda_2 x_2 + b_2| & \cdots & |\lambda_{n-1}x_{n-1} + b_{n-1}| & |\lambda_n x_n + b_n| \end{bmatrix}.$$

After some algebraic manipulation, we can show this matrix has full rank so long as $x_1 \neq -\frac{b_1}{\lambda_1}, \ldots, x_n \neq -\frac{b_n}{\lambda_n}$; that is, we avoid a set of hyperplanes. This divides $\mathrm{I\!R}^n$ into quadrants where the bisimulation can be constructed.

7 Symbolic execution theory

In this section we consider the implementation of the theory of approximate verification in a symbolic model checking algorithm.

A theory $\mathcal{T}$ of A is a set of predicates that are assigned truth values by the states of A. We write $[p] \in Q$ for the set of states that satisfy predicate p. $\langle R \rangle$ denotes the set of formulas of $\mathcal{T}$ that define a region $R \subset Q$. A theory is *decidable* if it can be decided for each predicate p of $\mathcal{T}$ whether $[p]$ is empty. The theory $\mathcal{T}$ permits the symbolic analysis of A if (1) $\mathcal{T}$ is decidable, (2) $\mathcal{T}$ is closed under boolean operations and *Pre* and *Post* operations, and (3) $\langle Q^f \rangle \in \mathcal{T}$, $\langle Q^0(l) \rangle \in \mathcal{T}$, $l \in L$.

Suppose the tangential and transversal foliations on K for each $l \in L$ are defined by submersions $h_i^l(x) = c_i$. Let $\mathcal{S}$ be the class of formulas

$$h_i^l(x) \ \% \ c_i$$

with $c_i \in \mathrm{I\!R}$, $\% = \{\leq, <, =, >, \geq\}$, $l \in L$, $i = 1, \ldots, n$, and all finite conjunctions and disjunctions of these expressions. A finite automaton with its symbolic execution theory is said to be *effectively presented* [5].

Theorem 7. *A_μ with the theory $\mathcal{S}$ is effectively presented.*

Proof. $\mathcal{S}$ is a symbolic execution theory of A_μ. For (1) the regions Q_μ^0, I_μ, J_μ, and Q_μ^f in $L \times K$ can be represented by formulas in $\mathcal{S}$, (2) $\langle Pre(R) \rangle \in \mathcal{S}$ and $\langle Post(R) \rangle \in \mathcal{S}$ for $\langle R \rangle \in \mathcal{S}$ by construction, and (3) $\mathcal{S}$ is decidable. Consider an atomic formula $\psi(x)$ for a closed region: $\exists x.(c_1 \leq h_1(x) \leq d_1) \wedge \cdots \wedge (c_n \leq h_n(x) \leq d_n)$. $\psi(x)$ is equivalent to the quantifier free expression $(c_1 \leq d_1) \wedge \cdots \wedge (c_n \leq d_n)$.

8 Critique and future work

This paper opens up avenues for applying model checking algorithms to the verification of safety problems for hybrid systems consisting of coordinating autonomous agents, and especially hybrid systems where the continuous level is a kinematic model. Model checking may provide a vast improvement in efficiency over simulation-based approaches for validating hybrid system performance, though potential gains may not be as great as those reported for model checking of circuit designs and protocols.

There are some limitations and obstacles to be overcome. First, it is likely that model checking will still be a computationally expensive tool. Initially, the number of autonomous agents will be small and the continuous dynamics will be low- dimensional, at least until further breakthroughs appear on this frontier. The approach becomes more interesting when more of the "burden of control" can be placed at the logic level. Some work that remains to be done is obtaining the approximate automaton automatically, given the analytical representation of its bisimulation.

The paper suggests some areas for future investigation. First, the paper develops a local geometric theory of bisimulation. A global theory is needed. The most promising approach is to use symmetry to obtain global first integrals. Also, a theory of robustness of hybrid systems is needed in light of the approximations that are introduced to complete the verification. We plan to report on these directions in future papers.

Acknowledgements The author is grateful to André de Carvalho, Tom Henzinger, and Charles Pugh, for their insights and many valuable discussions, and to Peter Caines, whose talks at Berkeley initiated this investigation.

References

1. R. Alur and D. L. Dill. Automata for modeling real-time systems. In *"Proc. 17th ICALP: Automata, Languages and Programming*, LNCS 443, Springer-Verlag, 1990.
2. P. Caines and Y. Wei. The hierarchical lattices of a finite machine. *Systems and Control Letters*, vol. 25, no. 4, pp. 257-263, July, 1995.
3. P. Caines and Y. Wei. On dynamically consistent hybrid systems. In P. Antsaklis, W. Kohn, A. Nerode, eds., *Hybrid Systems II*, pp. 86-105, Springer-Verlag, 1995.
4. L.O. Chua, M. Komuro, and T. Matsumoto. The double scroll family - part I: rigorous proof of chaos. *IEEE Transactions on Circuits and systems* vol. 33, no. 11, pp. 1072-1097, November, 1986.
5. T. Henzinger. Hybrid automata with finite bisimulations. In *"Proc. 22nd ICALP: Automata, Languages and Programming*, LNCS 944, pp. 324-335, Springer-Verlag, 1995.
6. T. Henzinger. The theory of hybrid automata. In *Proc. 11th IEEE Symposium on Logic in Computer Science*, pp. 278-292, New Brunswick, NJ, 1996.
7. H. B. Lawson. The Quantitative theory of foliations. *Regional Conference Series in Mathematics*, no. 27. American Mathematical Society, Providence, 1977.
8. R. Murray and S. Sastry. Nonholonomic motion planning: steering using sinusoids. *IEEE Transactions on Automatic Control*, vol.38, no.5, pp. 700-16, May, 1993.
9. J. Palis and W. de Melo. *Geometric Theory of Dynamical Systems: an Introduction.* Springer-Verlag, New York, 1982.
10. W. Sluis. *Absolute Equivalence and its Applications to Control Theory.* Ph.D. thesis, University of Waterloo, 1992.
11. C. Tomlin, G. Pappas, J. Lygeros, D. Godbole, and S. Sastry. Hybrid Control Models of Next Generation Air Traffic Management. In P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, eds., *Hybrid Systems IV*, LNCS 1273, pp. 378-404, Springer-Verlag, 1997.
12. F. Warner. *Foundations of Differential Manifolds and Lie Groups.* Springer-Verlag, New York, 1983.