Proceedings of the 37th IEEE
Conference on Decision & Control
Tampa, Florida USA • December 1998

A geometric approach to bisimulation and verification of hybrid systems

Mireille Broucke
Department of Electrical Engineering and Computer Science,
University of California, Berkeley CA 94720
mire@eecs.berkeley.edu

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. Hybrid models arise in applications where multiple agents communicating via protocols are operating under feedback control. If there are many agents each executing maneuvers, it is necessary to do a verification of the protocols to ensure desirable properties such as safety, liveness, fairness, and no deadlock. Likewise, control objectives at the planning level can be stated in terms of temporal logic formulas, and these formulas can be checked by formal verification methods (model checking) [9].

We are interested in constructing bisimulations in order to carry out a verification of the safety problem.

Safety problem: *For hybrid system A determine if a set of states P can be reached from an initial set of states Q^0. P is usually the unsafe set to be avoided.*

A primary focus of research is to extend the the class of hybrid systems that have a finite bisimulation. The techniques developed have primarily involved transforming the state variables to obtain a reduction to timed automata [5]. However, the ability to perform this reduction is increasingly difficult as the control location dynamics are allowed to be more general.

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, and only in certain cases is it exact. We will develop techniques for a hybrid system that is "close" to the original system. 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].

2 Definitions

2.1 Notation

x' refers to the updated value of a variable x after a transition is taken, and $\dot{x}$ refers to the time derivative. 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.

2.2 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 $t = 0$.

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

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 σ.

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 will use the notation $G(e) = g_e$ and $R(e) = r_e$.

0-7803-4394-8/98 $10.00 © 1998 IEEE

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

We make the following simplifying assumptions:
1) for each $e = (l, \sigma, l') \in E$, $g_e \subseteq I(l)$, $r_e(g_e) \subseteq I(l')$,
2) $Q^0(l) \subseteq I(l)$, and
3) $X^f \subseteq I(l^f)$.

2.3 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 non-deterministically) 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 $t > 0$, $x' = \phi_t^l(x)$, 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 *timed word* of A is a finite or infinite sequence $\overline{\tau} = \tau_0\tau_1\tau_2\ldots$ of letters from $\Sigma \cup \mathbb{R}^+$; that is, each τ_i is either an observation of A or a non-negative real that denotes a duration of time between observations. The timed word $\overline{\tau}$ is *divergent* if $\overline{\tau}$ is infinite and $\sum\{\tau_i | \tau_i \in \mathbb{R}^+, i \in \mathbb{N}\} = \infty$. 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 $i \geq 0$, we have $q_i \in Q$, $\tau_i \in \Sigma \cup \mathbb{R}^+$. The trajectory π accepts the timed word $\overline{\tau} = \tau_0\tau_1\ldots$ and π is called divergent if $\overline{\tau}$ is divergent. The *w*-language, called $Lang(A)$, is the set of all divergent timed words that are accepted by trajectories of A. A *run* of A is the projection to the discrete part of a trajectory accepted by A, namely, a finite or infinite sequence $l_0, l_1, l_2, \ldots$ of admissible locations. 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 hybrid automaton A, $Reach_A$, is the set of states that can be reached by any trajectory of A.

2.4 Bisimulation

Given a hybrid system $A = (Q, \Sigma, D, Q^0, I, E, J, Q^f)$, 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 $\exists\ q'$ such that $q \xrightarrow{\sigma} q'$ and $p' \simeq q'$, and
(2) if $q \xrightarrow{\sigma} q'$, then $\exists\ p'$ such that $p \xrightarrow{\sigma} p'$ and $p' \simeq q'$.

Let $Q/_\simeq$ be the set of equivalence classes of $\simeq$. A bisimulation is finite if it has a finite number of equivalence classes. Using $\simeq$, a quotient system $A/_\simeq$ can be constructed. If $\simeq$ is finite, the quotient system $A/_\simeq$ is a finite automaton. This quotient system can be used in verification of the safety problem: if $P \cap Reach_{A/_\simeq} = \emptyset$, where P is a set of final states, then $P \cap Reach_A = \emptyset$. If $P \cap Reach_{A/_\simeq} \neq \emptyset$, then no conclusive answer about the safety problem is obtained.

3 Verification

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 $int(c_i) \cap int(c_j) = \emptyset, \forall i \neq j$, for $c_i, c_j \in C_l$.

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

$$\mu(C) = \sup\{\rho(c) | c \in C\}.$$

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

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

If $P = \{l\} \times U \subset L \times M$, then $(P)_\mu = \{l\} \times (U)_\mu$.

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

Let $C(K) = \{C_l \mid l \in L\}$ be the set of covers of K for automaton A. $C(K)$ induces an equivalence relation $\simeq$ on Q. We say $q \simeq q'$, where $q = (l, x)$ and $q' = (l', x')$ if
(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 $t > 0$, if $(l, x) \simeq (l, x')$ and $y = \phi_t(x)$, then there exists a y' and $t' > 0$ such that $y' = \phi_{t'}(x')$ and $(l, y) \simeq (l, y')$.

3.1 Approximate automaton

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

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

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,

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

If $e = (l, \sigma, l')$ and

$$O(x) = \left\{ y \in \bigcap_{i=1}^{m(x)} c_i \mid \forall c_i \in C_l \,.\, x \in c_i \right\} \tag{3.1}$$

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

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

This operation introduces extra non-determinacy in the approximate automaton 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. $X^f \subseteq K$.
4. $I(l) \subseteq K$.

Note that if A_μ is an over-approximation of A on K, then $Reach_A|_K \subset Reach_{A_\mu}|_K$.

Approximate Verification Problem:
Given hybrid automaton A, $C(K, \mu)$ 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 coarsest μ-approximation A_{μ^*} which verifies that the original system is safe.

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

4 Construction of bisimulations

In this section we elaborate a geometric construction in order to derive an analytical representation of the bisimulation. The main geometric tool is foliations. The reader may refer to [6] for background. We are interested in foliations whose leaves are regular submanifolds. By the Pre-Image theorem, regular submanifolds can be constructed by submersions. A foliation globally defined by a submersion is called *simple*.

Let $f \in X(M)$. 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: an integral curve starting on a leaf of the foliation remains on it forever, 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 transversal.* For simple foliations, the following lemma provides an algebraic test for regularity.

Lemma *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 transversal on K.*

We will not use all of the leaves of a foliation, but only some finite subset of them. We *discretize* a simple 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.

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 [Foliations] *Given hybrid automaton A, $\mu > 0$, and an open $U \subset M$ on which, $\forall l \in L$, $f_l \in X(M)$ 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 $h_i^l, i = 1, \ldots, n-1$. 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_n^l independent of $h_i^l, i = 1, \ldots, n-1$, 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 $\tilde{c}_\beta = h^{-1}(c_\beta)$.

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

$$\begin{aligned} \dot{x}_i &= x_{i+1}, \quad i = 1, 2, 3, \\ \dot{x}_4 &= u. \end{aligned}$$

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 $\mathbb{R}^4$.

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. 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 Pfaffian system satisfies the *Frobenius condition* if one of the following equivalent conditions holds:
(1) $d\omega^i$ is a linear combination of $\omega^1, \ldots, \omega^q$,
(2) $d\omega^i \wedge \omega^1 \wedge \cdots \wedge \omega^q = 0, i = 1, \ldots, q$.
(3) $d\omega^i = \sum_{j=1}^q \theta^j \wedge \omega^j$, some θ^j.

We write $d\omega^i \equiv 0 \pmod{\omega^1, \ldots, \omega^q}$ if ω^i satisfies the Frobenius condition.

Theorem [Frobenius] *Let $I = \{\omega^1, \ldots, \omega^q\}$ be a Pfaffian system with one-forms satisfying the Frobenius condition $d\omega^i \equiv 0 \pmod{I}$ for $k = 1, \ldots, q$. Then there exist 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. Thus, the Frobenius theorem is a useful tool that provides local first integrals.

Theorem [First Integrals] *Given hybrid automaton A, $\mu > 0$, and an open $U \subset M$ on which, $\forall l \in L$, $f_l \in X(M)$ 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 $x \in V$. $\{f_1, \ldots, f_n\}$ 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

$$(a_1, \ldots, a_n) \mapsto \phi_{a_1}^1 \circ \cdots \circ \phi_{a_n}^n(x^0).$$

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

$$\left(\frac{\partial G}{\partial a_i}\right)_0 = \frac{\partial}{\partial a_i} \phi_{a_i}^i \circ \phi_{a_1}^1 \circ \cdots \circ \phi_{a_{i-1}}^{i-1} \circ \phi_{a_{i+1}}^{i+1} \circ \cdots \circ \phi_{a_n}^n(x^0) = f_i(x^0).$$

Since the f_i 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. □

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.

Proposition [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 $f = [f_l \;\; f_{l'}]^T$. 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

Planar Aircraft Consider the coordination problem of two aircraft A and B flying at a fixed altitude near an airport [8]. 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

$$g = \begin{bmatrix} \cos\phi & -\sin\phi & x \\ \sin\phi & \cos\phi & y \\ 0 & 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & -u_1 & u_2 \\ u_1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

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 takes the form

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

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.

Mobile robot Consider the coordination problem of two mobile robots A and B, operating in a closed workspace of a factory. 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 the kinematic model of the associated maneuver. We assume in each automaton location, the control inputs are constant, but they are allowed to change instantaneously upon switching locations. The kinematic model for each robot, converted to chained form [7] 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

$$\begin{aligned} x_2 - \frac{u_2}{u_1}x_1 &= c_2 \\ x_3 - \frac{u_1}{2u_2}x_2^2 &= c_3 \\ x_4 + \frac{1}{3}\left(\frac{u_1}{u_2}\right)^2 x_2^3 - \frac{u_1}{u_2}x_2x_3 &= c_4. \end{aligned}$$

and a transversal foliation given by: $x_1 = c_1$. These foliations define the bisimulation for each robot, by checking the regularity condition as follows:

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

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 $\mathbb{R}^4$.

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

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

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

7 Symbolic execution theory

In this section we consider the implementation of the theory of approximate verification in a symbolic model checking algorithm. A symbolic execution theory S of A is a set of predicates assigned truth values by the states of A and satisfying:

1. the emptiness problem for each predicate p of S is decidable,
2. S is closed under boolean operations and Pre and $Post$ operations,
3. $\langle Q^f \rangle \in S$, where $\langle Q^f \rangle$ denotes the set of formulas defining Q^f.

Suppose the tangential and transversal foliations on K for each $l \in L$ are defined by submersions $h_i^l(x) = c_i$. Let S be the class of formulas $h_i^l(x)$ % c_i with % $= \{\leq, <, =, >, \geq\}, l \bullet L, i = 1, \ldots, n$ and all finite conjunctions and disjunctions of these expressions. A finite automaton with its symbolic execution theory is said to be *effectively presented* [4].

Theorem *A_μ with the theory S is effectively presented.*

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 model of the kinematic dynamics. 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, for the performance of model checking is relatively unaffected by the number of states of the automaton. Some work that remains to be done is obtaining the approximate automaton automatically, given the analytical representation of its bisimulation, and to characterize the robustness of the reach set to model variations.

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

References

[1] R. Alur, D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, no. 126, pp. 183-235, 1994.

[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] T. Henzinger. Hybrid automata with finite bisimulations. In *"Proc. 22nd ICALP: Automata, Languages and Programming*, LNCS 944, pp. 324-335, Springer-Verlag, 1995.

[5] T. Henzinger, P. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *Proc. 27th Annual Symp. Theory of Computing Science*, pp. 373-382, ACM Press, 1995.

[6] H. B. Lawson. The Quantitative theory of foliations. *Regional Conference Series in Mathematics*, no. 27. American Mathematical Society, Providence, 1977.

[7] 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.

[8] 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.

[9] M. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification. *Proc. 1st Annual Symposium LICS*, p. 332-344, 1986.