Semi-decidable Synthesis for Triangular Hybrid Systems

Omid Shakernia[1], George J. Pappas[2], and Shankar Sastry[1]

[1] Department of EECS, University of California at Berkeley, Berkeley, CA 94704
{omids,sastry}@eecs.berkeley.edu
[2] Department of EE & CIS, University of Pennsylvania, Philadelphia, PA 19104
pappasg@ee.upenn.edu

Abstract. The algorithmic design of least restrictive controllers for hybrid systems that satisfy reachability specifications has received much attention recently. Despite the importance of algorithmic approaches to controller design for hybrid systems, results that guarantee termination of the algorithms have been limited. In this paper, we extend recent decidability results on controller synthesis for classes of linear hybrid systems to semi-decision procedures for *triangular hybrid systems* which can be used to model nonholonomic systems after a transformation. Our results are then applied to verification of a conflict resolution maneuver from air traffic control.

1 Introduction

Safety criticality in motivating applications [13] of hybrid systems has resulted in much research on computing reachable sets for hybrid systems in order to ensure that these systems avoid unsafe regions of the state space [2,3,4]. Furthermore, much research has recently focused on controller synthesis of hybrid systems where the safety property is ensured by design [1,6,7,12].

The complexity of the motivating applications makes algorithmic approaches to controller synthesis very desirable, whenever possible. However, termination guarantees for algorithmic approaches to synthesis have been limited. In particular, the game theoretic framework for controller synthesis introduced in [6] was only recently shown to result in decision procedures for various classes of linear systems [9], and semi-decision procedures for classes of linear hybrid systems [10].

In this paper, we proceed along the same spirit of [9,10] but we increase the complexity of the continuous dynamics to capture *triangular hybrid systems*, which are defined as hybrid control systems whose continuous dynamics in each discrete state are nonlinear with a triangular structure. Triangular nonlinear systems is a rich class of nonlinear systems that capture the so-called *chained systems*, which can be used to model nonholonomic systems after a state transformation. Nonholonomic systems have been very useful kinematic models of aircraft, robots, space robots, etc [5]. In this paper, we consider the following controller synthesis problem: *Given a triangular hybrid system, compute the maximal control invariant set of initial conditions and least restrictive controller*

M.D. Di Benedetto, A. Sangiovanni-Vincentelli (Eds.): HSCC 2001, LNCS 2034, pp. 487–500, 2001.

such that for all disturbances the state will avoid an unsafe set. In particular, we present a semi-decision procedure which, if it terminates, exactly solves the above problem.

The solution of the above problem depends critically on state of the art techniques from controller synthesis of hybrid systems. In particular, we adopt the general framework for controller synthesis of nonlinear hybrid systems [6], while we follow in spirit the approach taken in [9]. In particular, we focus on continuous games for triangular nonlinear systems. Application of the maximum principle leads to bang-bang optimal controls and a triangular structure in the co-state equations. Rather than solving the Hamilton-Jacobi partial differential equations for reachability computations, we abstract the bang-bang nature of the optimal control to a hybrid system. The piece-wise constant nature of the optimal inputs and disturbances, and the triangular structure of the state and co-state dynamics leads to polynomial flows for the states and co-states. This allows us to use quantifier elimination in each discrete state of the abstracted game to perform reachability computations. The above sequence of steps results in a semi-decision procedure for controller synthesis for triangular hybrid systems. However, unlike classes of linear systems where the number of switchings is uniformly finite [9], no such guarantee exists for triangular systems, making very difficult any claims for a decision procedure.

The structure of this paper is as follows: In Section 2 we review the synthesis framework of [6]. In Section 3 we present a semi-decision procedure for reach set computation in triangular nonlinear systems, which is lifted in Section 4 to triangular hybrid systems. These results are then applied in Section 5 to a verification of a conflict resolution maneuver from air traffic control.

2 Controller Synthesis for Nonlinear Hybrid Systems

In this section we review the framework for computing the maximum controlled invariant safe set for general nonlinear hybrid systems [6,12].

Definition 1 (Hybrid system).
A hybrid system H is a collection (X, V, I, f, E, ϕ), with:

- ***State and input variables**: X and V are disjoint collections of state and input variables. We assume that $X = X_D \cup X_C$ and $V = V_D \cup V_C$, where X_C and V_C contain continuous, and X_D and V_D discrete variables. We refer to valuations $x \in \mathbf{X}$ and $v \in \mathbf{V}$ as the state and the input of the hybrid system.*
- ***Initial states**: $I \subseteq \mathbf{X}$ is a set of initial valuations of the state variables.*
- ***Continuous evolution**: $f : \mathbf{X} \times \mathbf{V} \to T\mathbf{X_C}$ is a vector field.*
- ***Discrete transitions**: $E \subseteq \mathbf{X} \times \mathbf{V} \times \mathbf{X}$ is a set of discrete transitions.*
- ***Admissible inputs**: $\phi : \mathbf{X} \to 2^{\mathbf{V}}$ gives the set of admissible inputs at a given state $x \in \mathbf{X}$.*

It is customary to use the notation $(q, x) = (x|_{X_D}, x|_{X_C}) \in \mathbf{X}$. The meaning of the variable x will be clear from the context.

For any input $v = (u, d) \in \mathbf{V}$, define the set:

$$Inv(v) \triangleq \{x \in \mathbf{X} \mid v \in \phi(x) \wedge (x, v, x) \in E\}.$$

For a state $x \in \mathbf{X}$ and input $v = (u, d)$, define:

$$Next(x, v) \triangleq \begin{cases} \{y \in \mathbf{X} \mid (x, v, y) \in E\} & \text{if } v \in \phi(x) \\ \emptyset & \text{if } v \notin \phi(x). \end{cases}$$

$Inv(v)$ is the set of states from which continuous evolution is possible under input v, while $Next(x, v)$ is the set of states that can be reached from x under input v through a discrete transition. For any set $K \subseteq \mathbf{X}$ and input $v = (u, d)$ the *successor* of K under v is given by $Next(K, v) = \bigcup_{x \in K} Next(x, v)$.

For any set $K \subseteq \mathbf{X}$ define the *controllable predecessor* of K, $Pre_u(K)$, and the *uncontrollable predecessor* of K, $Pre_d(K)$, by:

$$Pre_u(K) \triangleq \{x \in \mathbf{X} \mid \exists u \in \mathbf{U}\ \forall d \in \mathbf{D}\ x \notin Inv(v) \wedge\ Next(K, v) \subseteq K\} \cap K,$$
$$Pre_d(K) \triangleq \{x \in \mathbf{X} \mid \forall u \in \mathbf{U}\ \exists d \in \mathbf{D}\ Next(K, v) \cap K^c \neq \emptyset\} \cup K^c.$$

where $v = (u, d)$. $Pre_u(K)$ contains all states in K for which u can force a transition back into K. $Pre_d(K)$ contains all states outside K together with those states for which it is possible to transition outside K regardless of the action of u. Whereas Pre_u and Pre_d capture information about regions of the state space that can be reached through discrete transitions of the system, the following operator [12] captures continuous reachability information.

Definition 2 (Reach-Avoid). *Given a hybrid system H and disjoint sets K, $G \subseteq \mathbf{X}$, the operator $Reach : 2^{\mathbf{X}} \times 2^{\mathbf{X}} \to 2^{\mathbf{X}}$ is defined as:*

$$Reach(K, G) \triangleq \{x_0 \mid \forall u \in \mathcal{U} \exists d \in \mathcal{D} \exists t \geq 0 : x(t) \in K \wedge \forall s \in [0, t]\ x(s) \notin G\},$$

were $\mathcal{U}, \mathcal{D}$ denote the set of piecewise continuous functions from the $\mathbb{R}$ to $\mathbf{U}, \mathbf{D}$ respectively, and $x(\cdot)$ is the unique state trajectory starting from initial condition $x(0) = x_0$ under the input (u, d).

The set $Reach(K, G)$ contains the states from which for all controls there exists a disturbance such that the state trajectory can be driven to K while avoiding the escape set G. The following algorithm uses the *Reach* operator to compute the maximal controlled invariant subset of F (see [12]).

Algorithm 1 (Maximum Controlled Invariant Safe Set)
initialize
$W^0 = F; \quad W^{-1} = \emptyset; \quad i = 0$
while $W^i \neq W^{i-1}$
$W^{i-1} = W^i \setminus Reach(Pre_d(W^i), Pre_u(W^i))$
$i = i - 1$
end while
$W^* := W^i$
end

Algorithm 1 iteratively removes from the safe set F all states for which there is a disturbance which either through continuous evolution or discrete transition can bring the system outside F regardless of the control action. In order to implement Algorithm 1, one needs to encode sets of states, perform set intersection, union, test for emptiness, and *exactly* compute $Reach(\cdot,\cdot)$. If all these conditions hold for a class of systems, then the problem is *semi-decidable* for that class of systems. Even though there is no *guarantee* of termination, if the algorithm terminates, then it exactly computes the unique maximal controlled invariant set W^*. If in addition, Algorithm 1 is guaranteed to terminate after a finite number of iterations for a class of systems, then we say the problem is *decidable* for that class.

The main difficulty in the implementation of Algorithm 1 is the computation of the *Reach* operator. For general nonlinear hybrid systems, the computation of *Reach* relies on the numerical solution of a pair of coupled Hamilton-Jacobi partial differential equations [7,12]. *In this paper, we show that for a certain class of nonlinear hybrid systems with triangular continuous dynamics each step of Algorithm 1 is symbolically computable.* This class is rich enough to capture hybrid systems with chained nonlinear dynamics, which model nonholonomic kinematics for aircraft, cars, and robots.

3 Computing Safe Sets for Triangular Nonlinear Systems

In this section, we address the problem of computing maximal controlled invariant safe sets for a class of nonlinear control systems subject to disturbances. The computation of maximal safe sets is a fundamental step in the least restrictive controller synthesis problem [6]. In this section, we extend the methodology of symbolic controller synthesis for classes linear systems described in [9] to a class of nonlinear systems.

For a differential game $\dot{x} = f(x,u,d)$ between inputs $u \in U \subset \mathbb{R}^{n_u}$ and disturbances $d \in D \subset \mathbb{R}^{n_d}$, the solution to the controller synthesis problem requires the computation of the set of initial states for which there exists a disturbance that can eventually drive the system to some unsafe set regardless of the actions of the control. Therefore the controller synthesis problem for continuous time system requires the computation of the continuous system version of the Reach-Avoid set.

Definition 3 (Reach-Avoid). *Given a differential game $\dot{x} = f(x,u,d)$ and disjoint sets $K, G \subseteq \mathbb{R}^n$, the operator $Reach : 2^{\mathbb{R}^n} \times 2^{\mathbb{R}^n} \to 2^{\mathbb{R}^n}$ is defined as:*

$$Reach(K,G) \triangleq \{x_0 \mid \forall u \in \mathcal{U}\ \exists d \in \mathcal{D}\ \exists t \geq 0\ :\ x(t) \in K \wedge \forall s \in [0,t]\ x(s) \notin G\},$$

where $\mathcal{U}$, $\mathcal{D}$ denote the set of piecewise continuous functions from the $\mathbb{R}$ to U, D respectively, and $x(\cdot)$ is the unique state trajectory of $\dot{x} = f(x,u,d)$ starting from initial condition $x(0) = x_0$ under the input (u,d).

The set $Reach(K,G)$, which is graphically depicted in Figure 1, contains the states from which for all controls there exists a disturbance such that the state

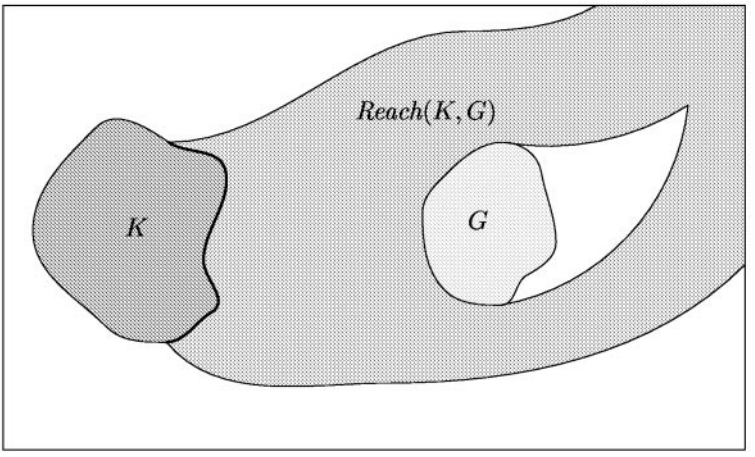


Fig. 1. Showing a graphical depiction of $Reach(K, G)$.

trajectory can be driven to K while avoiding the escape set G. It was shown recently that the computation of *Reach* is decidable for certain classes of linear systems [10]. Here we extend the result to a class of nonlinear systems. As a motivating example, consider the following nonlinear system in so-called *chain form*:

$$\begin{aligned} \dot{x}_j^0 &= u_j && j = 1, \ldots, m \\ \dot{x}_{ij}^1 &= x_i^0 u_j && j = 1, \ldots, m \text{ and } i < j \\ \dot{x}_{ij}^k &= x_{ij}^{k-1} u_j && j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j. \end{aligned} \tag{1}$$

Control systems of the class shown in equation (1) are quite important because they can be used to model many types of nonholonomic and under-actuated systems including unicycles, cars, multi-steering trucks with N-trailers, space robots, etc. [8]. We now apply the symbolic controller synthesis methodology described in [9,10] to this chain form system.

3.1 Computation of Optimal Control

For the chain form system (1), suppose we wish to compute the set of initial conditions $W \subset \mathbb{R}^n$ for which there exists a control $u(\cdot)$, constrained to a compact rectangular feasible control set $U \subset \mathbb{R}^m$, that can steer the state to the goal $G \subset \mathbb{R}^n$ while avoiding states $B \subset \mathbb{R}^n$. This problem is closely related to the problem of nonholonomic motion planning in the presence of obstacles [5] and is equivalent to computing $W = Reach(G, B)$.

To solve the reachability problem, we first introduce the *co-state* $p \in \mathbb{R}^n$ and construct the Hamiltonian:

$$H(x, p, u) = p^T f(x, u) = \sum_{j=1}^{m} \left(p_j^0 + \sum_{i=1}^{j-1} \left(p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1} \right) \right) u_j.$$

The Hamiltonian satisfies the state and co-state differential equations $\dot{x} = \frac{\partial H}{\partial p}$, $\dot{p} = -\frac{\partial H}{\partial x}$. From the Hamiltonian, we compute the co-state dynamics:

$$\begin{array}{ll} \dot{p}_{ij}^{n_j} = 0 & j = 1, \ldots, m \text{ and } i < j \\ \dot{p}_{ij}^{k-1} = -p_{ij}^{k} u_j & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\ \dot{p}_i^0 = -\sum_{j=1}^{m} p_{ij}^1 u_j & i = 1, \ldots, m. \end{array}$$

Notice that the chain structure of the system dynamics is inherited by the co-state dynamics. Next, we initialize the co-state as the inward-pointing normal on the boundary of G and apply the Pontryagin Maximum Principle to compute the optimal control $u^* = \arg\max_{u \in U} H(x, p, u)$. Since the feasible control set is a compact rectangle $U = \prod_{i=1}^{m} [\underline{U}_j, \overline{U}_j] \subset \mathbb{R}^m$, we may decompose the Maximum Principle for each component of the input:

$$u_j^* = \arg\max_{u_j \in [\underline{U}_j, \overline{U}_j]} \left(p_j^0 + \sum_{i=1}^{j-1} \left(p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1} \right) \right) u_j. \tag{2}$$

3.2 Construction of Hybrid System

The Maximum Principle calls for *bang-bang* controls: the optimal controls will always lie on the vertices on the feasible control set U. From equation (2), it is direct to see that u_j^* is either $\underline{U}_j$ or $\overline{U}_j$ depending on the sign of the "switching function" of the state and co-state which multiplies u_j. Thus, as proposed in [9, 10] we can construct a hybrid system which has $2^m + 1$ discrete states: One discrete state for each vertex of the rectangle U, and one discrete state for stopping the reachability computation on the obstacle set B (see [10]). The guards and invariants for the constructed hybrid system are defined by the "switching functions" in the optimal control shown in equation (2).

3.3 Reach Set Computation

For each discrete state of the constructed hybrid system we need to solve a reachability computation for a system of the form:

$$\begin{array}{ll} \dot{x}_j^0 = u_j^* & j = 1, \ldots, m \\ \dot{x}_{ij}^1 = x_i^0 u_j^* & j = 1, \ldots, m \text{ and } i < j \\ \dot{x}_{ij}^k = x_{ij}^{k-1} u_j^* & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\ \dot{p}_{ij}^{n_j} = 0 & j = 1, \ldots, m \text{ and } i < j. \\ \dot{p}_{ij}^{k-1} = -p_{ij}^k u_j^* & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\ \dot{p}_i^0 = -\sum_{j=1}^{m} p_{ij}^1 u_j^* & i = 1, \ldots, m, \end{array} \tag{3}$$

where u_j^* is a constant rational number. It is easily shown that the problem of computing the reachable set of this system is decidable. Indeed, due to the chain form of the state and co-state dynamics, we may iteratively compute the flow of the system by symbolic integration and substitution starting from x_i^0 and

proceeding down the chain. By symbolic integration the flow of this system is computed to be:

$$
\begin{aligned}
x_i^0(t) &= x_i^0(0) + u_i^* t && i = 1, \ldots, m \\
x_{ij}^1(t) &= x_{ij}^1(0) + x_i^0(0) u_j^* t + \tfrac{1}{2} u_i^* u_j^* t^2 && \\
&\vdots && \\
p_{ij}^{n_j}(t) &= p_{ij}^{n_j}(0) && j = 1, \ldots, m \text{ and } i < j \\
p_{ij}^{k}(t) &= \textstyle\sum_{l=0}^{n_j - k} \frac{(-u_j^* t)^l}{l!} p_{ij}^{k+l}(0) && j = 1, \ldots, m \text{ and } i < j \text{ and } k = 1, \ldots, n_j \\
p_i^0(t) &= p_i^0(0) + \textstyle\sum_{l=1}^{n_j - 1} \frac{(-u_j^* t)^l}{l!} p_{ij}^{l}(0) && i = 1, \ldots, m.
\end{aligned}
$$

We use the notation $x(t) = \phi(x_0, u, t)$ to denote the state $x(t)$ which is a result of flowing for t seconds along the dynamics of the system with input u starting at the initial condition $x(0) = x_0$. Since the flow of this system is polynomial, it admits quantifier elimination [11], and hence the computation of the set of points which can reach a semi-algebraic set K, $\{x_0 \in \mathbb{R}^n \mid \exists t > 0 \ : \ \phi(x_0, u_j^*, t) \in K\}$ for each discrete state of the constructed hybrid system is decidable.

The only remaining condition of interest for the constructed hybrid system is an upper bound on the number of switchings between the discrete states. For the case of linear systems with dynamic matrices that are either nilpotent or diagonalizable with real rational eigenvalues, a result of Pontryagin provides that the number of switchings of the optimal control is no greater than the dimension of the system. For these classes of systems, we are able to show decidability of the least restrictive controller synthesis problem [9]. We can make no such claim in the case of chain form systems of the type in equation (1). In general there is no upper bound on the number of switchings on the optimal control defined in (2). Hence we conclude that controller synthesis problem for the class of chain form systems is *semi-decidable*.

3.4 Triangular Systems

Upon examination, we realize that there are essentially two features in the structure of chain form systems that allow the above methodology to work:

1. The vector field has linear terms in u.
   - Thus the Hamiltonian has linear terms in u, and applying the Maximum Principle, we see that the optimal input u^* is piecewise constant on the vertices of the feasible control set.
   - This allows us to construct a hybrid system out of the switching logic of the optimal control, where for each discrete state there is a constant u^*.
2. The time derivative of each state is a polynomial in the input and the *preceding* states of the chain.
   - For a constant u^* the flow can be computed iteratively by symbolic integration and substitution starting from the beginning of the chain.
   - Since u^* is constant and the vector field depends polynomially in states, the flow of the system is polynomial in u^*, t and the state.

– This structure is inherited by the co-state dynamics and hence the flow of the co-state can also be symbolically integrated.

The observation above suggests that the methodology for symbolic reachability computation will also work on the following larger class of *triangular* nonlinear systems.

Definition 4 (Triangular nonlinear system).
A nonlinear system $\dot{x} = f(x,u)$ *is called* triangular *if it can be written as:*

$$\begin{aligned}
\dot{x}_0 &= a + \textstyle\sum_{j=1}^{m} b_j u_j \\
\dot{x}_1 &= f_1(x_0) + \textstyle\sum_{j=1}^{m} g_{1j}(x_0) u_j \\
\dot{x}_2 &= f_2(x_0, x_1) + \textstyle\sum_{j=1}^{m} g_{2j}(x_0, x_1) u_j \\
&\vdots \\
\dot{x}_n &= f_n(x_0, \ldots, x_{n-1}) + \textstyle\sum_{j=1}^{m} g_{nj}(x_0, \ldots, x_{n-1}) u_j,
\end{aligned}$$

where $a,\ b_j \in \mathbb{Q}$ *and* $f_i,\ g_{ij} \in \mathbb{Q}[x_0, \ldots, x_{i-1}]$ *for* $i = 1, \ldots, n$ *and* $j = 1, \ldots, m$.

Moreover, it is direct to see that the methodology is also applicable to the class of triangular *differential games* between inputs $u \in \mathbb{R}^{n_u}$ and disturbances $d \in \mathbb{R}^{n_d}$.

Definition 5 (Triangular differential game).
A differential game $\dot{x} = f(x,u,d)$ *is called* triangular *if it can be written as:*

$$\begin{aligned}
\dot{x}_{0j} &= a_j + \textstyle\sum_{k=1}^{n_u} b_{jk} u_k + \sum_{k=1}^{n_d} c_{jk} d_k \\
\dot{x}_{1j} &= f_{1j}(x_{01}, \ldots, x_{0L}) + \textstyle\sum_{k=1}^{n_u} g_{1jk}(x_{01}, \ldots, x_{0L}) u_j + \\
&\quad \textstyle\sum_{k=1}^{n_d} h_{1jk} d_k(x_{01}, \ldots, x_{0L}) \\
&\vdots \\
\dot{x}_{ij} &= f_{ij}(x_{01}, \ldots, x_{0L}, \ldots, x_{(i-1)1}, \ldots x_{(i-1)L}) + \\
&\quad \textstyle\sum_{k=1}^{n_u} g_{ijk}(x_{01}, \ldots, x_{0L}, \ldots, x_{(i-1)1}, \ldots x_{(i-1)L}) u_j + \\
&\quad \textstyle\sum_{k=1}^{n_d} h_{ijk}(x_{01}, \ldots, x_{0L}, \ldots, x_{(i-1)1}, \ldots x_{(i-1)L}) d_k
\end{aligned}$$

for $j = 1, \ldots, L$, *and* $i = 1, \ldots, n_j$, *and where* $a_j,\ b_{jk},\ c_{jk} \in \mathbb{Q}$ *and* $f_{ij},\ g_{ijk},\ h_{ijk}$ *are polynomials with rational coefficients.*

Theorem 1 (Semi-decidable reach for triangular differential games).
For a triangular differential game $\dot{x} = f(x,u,d)$, *if the inputs and disturbances are constrained to compact rectangles with rational coefficients, then for any disjoint semi-algebraic sets* $K, G \subset \mathbb{R}^n$, *the problem of computing* $Reach(K,G)$ *is* semi-decidable.

Proof. We need to show that the methodology for symbolic reach set computation proposed in [9,10] can be applied to triangular differential games and that each step in the methodology is computable.

1. **Compute Optimal Control.** Since the vector field can be written as $\dot{x} = f_1(x,u) + f_2(x,d)$, the Hamiltonian $H = p^T f(x,u,d)$ is *separable*, which implies that there exists a *saddle solution* (u^*, d^*) of optimal control and disturbance:

$$u^* = \arg\max_{u \in U} p^T f_1(x,u), \qquad d^* = \arg\min_{d \in D} p^T f_2(x,d). \tag{4}$$

   Moreover, since the Hamiltonian has linear terms in u and d, and the sets of feasible controls and disturbances are compact rectangles $U = \prod_{i=1}^{n_u} [\underline{U}_j, \overline{U}_j] \subset \mathbb{R}^{n_u}$, $D = \prod_{i=1}^{n_d} [\underline{D}_j, \overline{D}_j] \subset \mathbb{R}^{n_d}$, we may decompose equation (4) to get:

$$u_j^* = \arg \max_{u_j \in [\underline{U}_j, \overline{U}_j]} s_j^u(x,p)\ u_j, \qquad d_j^* = \arg \max_{d_j \in [\underline{D}_j, \overline{D}_j]} s_j^d(x,p)\ d_j, \tag{5}$$

   where $s_j^u(\cdot)$ and $s_j^d(\cdot)$ are "switching functions" which are polynomial in the state and co-state (x,p). The Maximum Principle calls for *bang-bang* optimal controls and disturbances: Depending on the signs of the switching functions, the optimal controls and disturbances will always lie on a vertex of the feasible control and disturbance set.
2. **Construct Hybrid System.** Construct a hybrid system with 2^{n_u} discrete states for each possible optimal control, 2^{n_d} discrete states for each possible disturbance, and one discrete state for stopping the reachability computation on the avoid set G (see [10]). The switching functions $s_j^u(\cdot)$, $s_j^d(\cdot)$ determine the discrete transitions of the constructed hybrid system, and continuous dynamics are the co-state dynamics $\dot{p} = -\frac{\partial H}{\partial x}$ appended to $\dot{x} = f(x, u^*, d^*)$ where (u^*, d^*) are constant.
3. **Calculate Reach Set.** In each discrete state, the triangular structure of the state dynamics and the fact that the optimal control and disturbance (u^*, d^*) are constant allows the flow of the state dynamics to can be computed by symbolic integration. Moreover, it is direct to check that the co-state dynamics inherit the triangular structure of the state dynamics and that the flow of the co-state dynamics can also be integrated symbolically. Since the flow in each discrete state of the constructed hybrid system is polynomial, we may perform quantifier elimination to compute the reachable set for each discrete state of the hybrid system.

We have constructed a hybrid system for which the problem of computing the reach set of each discrete state is decidable. By initializing the hybrid system with the usable part of the unsafe set K (see [9]), we have a semi-decision procedure for computing $Reach(K, G)$. However, since in general there is no bound on the number of times the switching functions change sign, there is no bound on the number of discrete transitions the hybrid system takes, and hence we cannot guarantee that the reach set computation will terminate. □

4 Controller Synthesis for Triangular Hybrid Systems

The results of the previous section naturally inspire the following definition.

Definition 6 (Triangular hybrid system).
A hybrid system $H = (X, V, I, f, E, \phi)$ is called a triangular *hybrid system if $\forall q \in \mathbf{X}_D$ the set of feasible inputs $\phi(q,x)|_{V_C} = \mathbf{U}_q \times \mathbf{D}_q$, where $\mathbf{U}_q$ and $\mathbf{D}_q$ are compact rectangles with rational vertices, the reset relation $E \subseteq \mathbf{X} \times \mathbf{V} \times \mathbf{X}$ is semi-algebraic, and for each discrete state q the vector field $f(q,x,u,d)$ is triangular with rational coefficients.*

The results of the previous section provide that for each discrete state of the hybrid system, the computation of *Reach* is semi-decidable. Hence if the discrete transition Pre_d and Pre_u are computable (they are when the reset relation $E \subseteq \mathbf{X} \times \mathbf{V} \times \mathbf{X}$ is semi-algebraic), then each iteration of Algorithm 1 is computable, and hence we conclude that the problem of computing the maximum controlled invariant set is *semi-decidable*.

Theorem 2 (Semi-decidable controller synthesis for triangular hybrid systems). *For a triangular hybrid system H and a semi-algebraic safe set F, the problem of computing the maximum controlled invariant set $W^* \subseteq F$ is* semi-decidable.

If the computation of maximal safe set W^* terminates, we would like to provide a least restrictive controller that renders W^* invariant. Since the continuous dynamics of triangular hybrid systems are polynomial, the definition of the least restrictive controller can be written as a quantified first order formula in the theory of reals. Hence the least restrictive controller can be computed by quantifier elimination and is given in the following proposition [10].

Proposition 1 (Least restrictive controller). *Given a triangular hybrid system H and a semi-algebraic maximal controlled invariant set*

$$W^* = \left\{ x \in \mathbb{R}^n \mid \bigvee_{j=1}^{K} \left(\bigwedge_{k=1}^{L_j} h_{j_k}(x) \ \leq \ 0 \right) \right\},$$

the least restrictive controller $g(x) : \mathbf{X} \to 2^{\mathbf{U}}$ that renders W^* invariant is computable and is given by:

$$g(x) = \begin{cases} \{u \in \phi(x)|_U \mid \forall d \in \phi(x)|_D : Next(x,(u,d)) \subseteq W^*\} & \text{if } x \in (W^*)^o \\ \{u \in \phi(x)|_U \mid [\bigvee_{j=1}^{K} (\bigwedge_{k=1}^{L_j} (h_{j_k}(x) = 0) \Rightarrow \forall d \in \phi(x)|_D : \\ \quad (\frac{\partial h_{j_k}(x)}{\partial x})^T f(x,(u,d)) \leq 0) \wedge x \in Inv(u,d)] \vee \\ \quad [\forall d \in \phi(x)|_D : Next(x,(u,d)) \subseteq W^* \wedge x \notin Inv(u,d)]\}, & \text{if } x \in \partial W^* \\ \phi(x)|_U, & \text{if } x \in (W^*)^c. \end{cases}$$

Triangular hybrid systems is the first known class of nonlinear hybrid systems which has a semi-decidable controller synthesis problem. In the following section we apply our methodology to a conflict resolution example from air traffic control.

5 Conflict Resolution Example

In this section we present an application of our methodology towards verification of maneuvers for multi-agent hybrid systems. As an example application we verify a conflict resolution maneuver for air traffic control similar to the one described in [13]. Consider the following conflict resolution maneuver for two aircraft:

1. Cruise until aircraft are α_1 miles apart;
2. Change heading by $\Delta\phi$; fly until lateral displacement of d miles achieved;
3. Change to original heading; fly until aircraft are α_2 miles apart;
4. Change heading by $-\Delta\phi$; fly until lateral displacement of $-d$ miles achieved;
5. Change to original heading.

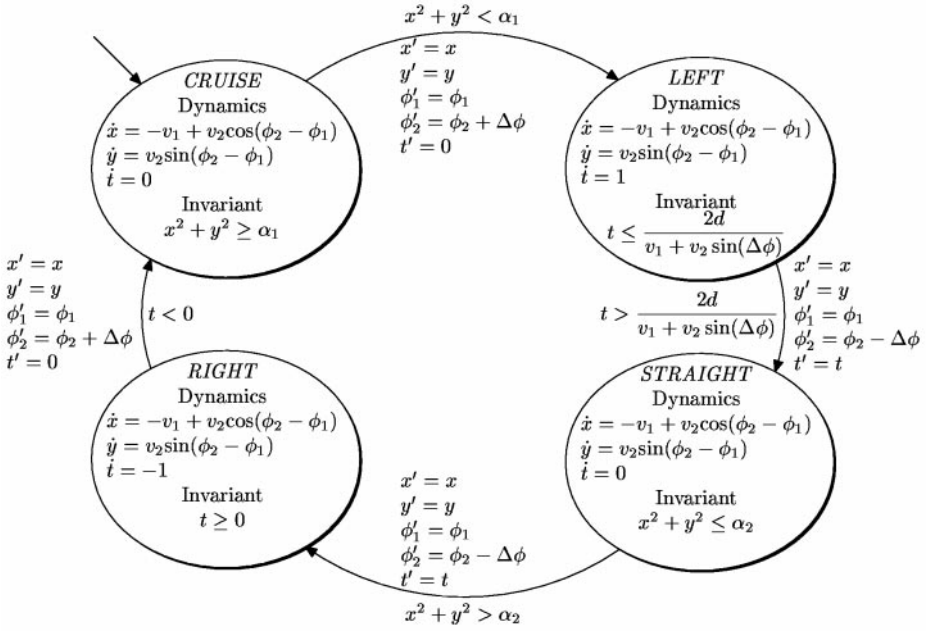


Fig. 2. Hybrid system model of aircraft conflict resolution maneuver.

The hybrid automaton modeling this maneuver has discrete states {*CRUISE, LEFT, STRAIGHT, RIGHT*} and is depicted in Figure 2. The continuous dynamics in each discrete state is the relative flow of the aircraft given a fixed velocity and heading, (v_i is the velocity and ϕ_i is the heading of aircraft i). The aircraft are considered to be at a safe distance if they are at least 5 miles apart. In the relative coordinate frame, the *unsafe* set is given by $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 5\}$.

Aircraft 1 is assumed to fly at a fixed velocity v_i and heading ϕ_1, while aircraft 2 can switch "modes" and rotate left or right a fixed angle of $\pm\Delta\phi$. It is clear that the hybrid automaton modeling the conflict resolution maneuver belongs to the class of triangular hybrid systems described in the previous sections.

Using the quantifier elimination package of MATHEMATICA 4.0, we computed the minimal unsafe sets for each discrete state of the automaton for the scenario where two aircraft are approaching each other with velocities $v_1 = 4,\ v_2 = 5$, with initial heading difference of $\phi_2 - \phi_1 = \frac{\pi}{2}$, and aircraft 2 allowed to change directions at an angle of $\pm\Delta\phi$ such that $\sin(\pm\Delta\phi) = \pm\frac{4}{5}$. Equations (6)-(8) show the results of the computation.

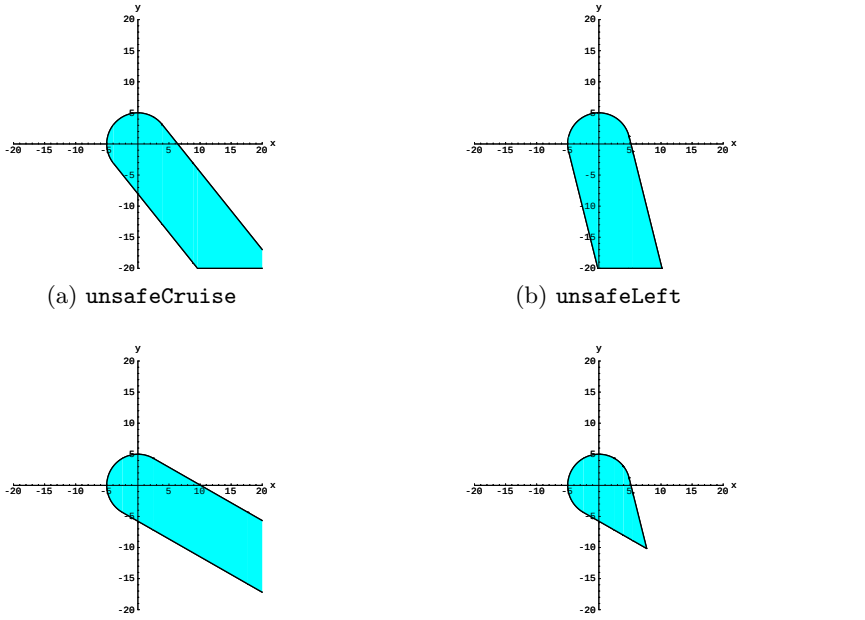
$$
\begin{aligned}
& v_1 = 4; v_2 = 5; \lambda = 0 \\
\texttt{unsafeCruise} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2} v_2 t)^2 \leq 25\right] \\
&= \left(y < -\tfrac{20}{\sqrt{41}} \wedge -\sqrt{41} - \tfrac{4y}{5} \leq x \leq \sqrt{41} - \tfrac{4y}{5}\right) \vee \\
&\quad \left(y = -\tfrac{20}{\sqrt{41}} \wedge -\sqrt{41} - \tfrac{4y}{5} < x \leq \sqrt{41} - \tfrac{4y}{5}\right) \vee \\
&\quad \left(y = \tfrac{20}{\sqrt{41}} \wedge -\sqrt{25 - y^2} < x < \sqrt{41} - \tfrac{4y}{5}\right) \vee \\
&\quad \left(\tfrac{20}{\sqrt{41}} \leq y < 5 \wedge -\sqrt{25 - y^2} < x < \sqrt{25 - y^2}\right) \vee \\
&\quad \left(-\tfrac{20}{\sqrt{41}} < y < \tfrac{20}{\sqrt{41}} \wedge -\sqrt{25 - y^2} < x \leq \sqrt{41} - \tfrac{4y}{5}\right)
\end{aligned}
\tag{6}
$$

$$
\begin{aligned}
& v_1 = 4; v_2 = 5; \lambda = \tfrac{3}{5} \\
\texttt{unsafeLeft} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2} v_2 t)^2 \leq 25\right] \\
&= \left(y < -\tfrac{5}{\sqrt{17}} \wedge -\tfrac{5\sqrt{17}}{4} - \tfrac{y}{4} \leq x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \\
&\quad \left(y = -\tfrac{5}{\sqrt{17}} \wedge -\tfrac{5\sqrt{17}}{4} - \tfrac{y}{4} < x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \\
&\quad \left(y = \tfrac{5}{\sqrt{17}} \wedge -\sqrt{25 - y^2} < x < \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \\
&\quad \left(\tfrac{5}{\sqrt{17}} < y < 5 \wedge -\sqrt{25 - y^2} < x < \sqrt{25 - y^2}\right) \vee \\
&\quad \left(-\tfrac{5}{\sqrt{17}} < y < \tfrac{5}{\sqrt{17}} \wedge -\sqrt{25 - y^2} < x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right)
\end{aligned}
\tag{7}
$$

$$
\begin{aligned}
& v_1 = 4; v_2 = 5; \lambda = -\tfrac{3}{5} \\
\texttt{unsafeRight} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2} v_2 t)^2 \leq 25\right] \\
&= \left(y < -7\sqrt{\tfrac{5}{13}} \wedge -\tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4} \leq x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \\
&\quad \left(y = -7\sqrt{\tfrac{5}{13}} \wedge -\tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4} < x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \\
&\quad \left(y = 7\sqrt{\tfrac{5}{13}} \wedge -\sqrt{25 - y^2} < x < \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \\
&\quad \left(7\sqrt{\tfrac{5}{13}} < y < 5 \wedge -\sqrt{25 - y^2} < x < \sqrt{25 - y^2}\right) \vee \\
&\quad \left(-7\sqrt{\tfrac{5}{13}} < y < 7\sqrt{\tfrac{5}{13}} \wedge -\sqrt{25 - y^2} < x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right)
\end{aligned}
\tag{8}
$$

Since the relative heading and velocity of the two aircraft is same for the *CRUISE* and *STRAIGHT* flight modes, then `unsafeCruise`=`unsafeStraight`.

The result of the symbolic computation of the minimal unsafe sets is shown in Figure 3. The set `unsafeCruise`$\setminus$`unsafeLeft` contains the set of states which are made safe by the aircraft turning left, and the set `unsafeCruise` $\setminus$ `unsafeRight` contains the set of states which are made safe by the aircraft turning right. The set `unsafeCruise` $\setminus$ (`unsafeLeft` $\cup$ `unsafeRight`) contains the states which are made safe by turning either left or right, and the set `unsafeCruise` $\cap$ `unsafeLeft` $\cap$ `unsafeRight` shown in Figure 3(d) is the set of states which is unsafe regardless of the action the aircraft takes.



(a) `unsafeCruise` (b) `unsafeLeft`

(c) `unsafeRight` (d) `unsafeCruise` $\wedge$ `unsafeLeft` $\wedge$ `unsafeRight`

Fig. 3. Showing minimal unsafe sets for each discrete state of maneuver automaton.

6 Conclusion

In this paper, we have presented the first class of nonlinear hybrid systems with a semi-decidable controller synthesis problem. This class of *triangular hybrid systems* is rich enough to capture hybrid models that include kinematic models of aircraft, robots, and cars. Our results were illustrated on a conflict resolution example from air traffic control.

Acknowledgments. The work by O. Shakernia was supported by ONR under grants N00014-97-1-0946 and N00014-00-1-0621, and by DARPA under grant

F33615-98-C-3614. The work of G. J. Pappas was partially supported by DARPA Grant F33615-00-C-1707, and the University of Pennsylvania Research Foundation.

References

1. E. Asarin, O. Bournez, T. Dang, O. Maler, and A. Pnueli. Effective controller synthesis of switching controllers for linear systems. *Proceedings of the IEEE*, 88(7):1011–1025, July 2000.
2. A. Chutinam and B. Krogh. Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations. In *Hybrid Systems : Computation and Control*, volume 1569 of *LNCS*. Springer Verlag, 1999.
3. T. Dang and O. Maler. Reachability analysis via face lifting. In *Hybrid Systems : Computation and Control*, volume 1386 of *LNCS*, pages 96–109. Springer Verlag, Berlin, 1998.
4. G. Lafferriere, G. J. Pappas, and S. Yovine. A new class of decidable hybrid systems. In *Hybrid Systems : Computation and Control*, volume 1569 of *Lecture Notes in Computer Science*, pages 137–151. Springer Verlag, 1999.
5. Z. Li and J.F. Canny, editors. *Nonholonomic Motion Planning*. Kluwer Academic Publishers, 1993.
6. J. Lygeros, C. Tomlin, and S.S. Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349–370, March 1999.
7. I. Mitchell and C. Tomlin. Level set methods for computation in hybrid systems. In *Proceedings of Hybrid Systems: Computation and Control*, LNCS 1790, pages 310–323. Springer-Verlag, March 2000.
8. R.M. Murray, Z. Li, and S.S. Sastry. *A Mathematical Introduction to Robotic Manipulation*. CRC Press, 1994.
9. O. Shakernia, G. Pappas, and S. Sastry. Decidable controller synthesis for classes of linear systems. In *Hybrid Systems: Computation and Control*, LNCS 1790, pages 407–420. Springer-Verlag, March 2000.
10. O. Shakernia, G. Pappas, and S. Sastry. Semidecidable controller synthesis for classes of linear hybrid systems. In *Proceedings of the 39th IEEE Conference on Decision and Control*, Sydney, AU, December 2000.
11. A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, second edition, 1951.
12. C. Tomlin, J. Lygeros, and S. Sastry. Computing controllers for nonlinear hybrid systems. In *Proceedings of Hybrid Systems: Computation and Control*, LNCS 1569. Springer-Verlag, March 1999.
13. C. Tomlin, G. J. Pappas, and S. Sastry. Conflict resolution for air traffic management : A study in muti-agent hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):509–521, April 1998.