The Image Computation Problem in Hybrid Systems Model Checking*

André Platzer[1] and Edmund M. Clarke[2]

[1] University of Oldenburg, Department of Computing Science, Germany
platzer@informatik.uni-oldenburg.de
[2] Carnegie Mellon University, Computer Science Department, Pittsburgh, PA
emc@cs.cmu.edu

Abstract. In this paper, we analyze limits of approximation techniques for (non-linear) continuous image computation in model checking hybrid systems. In particular, we show that even a single step of continuous image computation is not semidecidable numerically even for a very restricted class of functions. Moreover, we show that symbolic insight about derivative bounds provides sufficient additional information for approximation refinement model checking. Finally, we prove that purely numerical algorithms can perform continuous image computation with arbitrarily high probability. Using these results, we analyze the prerequisites for a safe operation of the *roundabout maneuver* in air traffic collision avoidance.

Keywords: model checking, hybrid systems, image computation.

1 Introduction

The fundamental operation in model checking [1] is *image computation*, i.e., determining the set of states reachable from some (initial) set of states by following all transitions of the system. Verifying safety amounts to checking whether a bad state can be reached by repeating image computation from the initial states until convergence or a bound is reached. Today, the primary challenge for verification of industrial hybrid systems is to improve (*a*) scalability by building model checkers that are able to deal with higher-dimensional continuous state-spaces, and (*b*) modeling capabilities by providing verification techniques for systems having richer continuous dynamics. In this paper, we focus on (*b*) using approximation techniques and delineate the borderline of decidability of the image computation

* This research was sponsored by a fellowship of the German Academic Exchange Service (DAAD), by the German Research Council (DFG) under grant SFB/TR 14 AVACS, the National Science Foundation under grant nos. CNS-0411152, CCF-0429120, CCR-0121547, and CCR-0098072, the US Army Research Office under grant no. DAAD19-01-1-0485, and the Office of Naval Research under grant no. N00014-01-1-0796. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution, government or other entity.

A. Bemporad, A. Bicchi, and G. Buttazzo (Eds.): HSCC 2007, LNCS 4416, pp. 473–486, 2007.

problem for hybrid systems model checking. In particular, we show that even a *single step* of continuous image computation is not semidecidable.

In this paper we analyze techniques for approximating image computation for hybrid systems having non-linear continuous flows. First-order real arithmetic is among the most expressive theories for continuous values that is known to be decidable [2]. It is used successfully in hybrid system verification [3, 4, 5, 6]. We thus investigate approximations of system flows using real arithmetic, including polynomial and spline approximations. For verification, we argue that uniform approximations, i.e., approximations with a uniform global error bound, are crucial, since verification is about making sure that the system is well-behaved even in worst-case scenarios. For this, we analyze the conditions required to guarantee that uniform approximations of flows can be constructed computationally. In addition, we study approximation-based model checking for hybrid systems with flows that are given implicitly as numerical solutions of differential equations.

Throughout the paper, we observe that numerical algorithms need additional knowledge about the system behavior to be successful in model checking. We show a strong undecidability result about the purely numerical treatment of even the basic operation of image computation in hybrid systems to support this observation.

The distinguishing feature of *numerical algorithms* in this context is that they compute their output with specific real values or rational approximations like 1.421. In contrast, *symbolic algorithms* are capable of computing with symbolic terms like $x^2 + 2xy$ that involve variable symbols to obtain results that are valid for *all* instantiations of x and y with real values. However, all terms that occur during the symbolic computation need to have a common representation that is effective. Further, numerical computations are generally more scalable to higher dimensions. See [7] for details on machine models for numerical computations; see [8] for symbolic computation and symbolic representations.

Model checking depends on image computation of *sets* of states. As they operate on concrete values, numerical algorithms can only compute images at a finite number of individual points in bounded time. Thus, the primary challenge in using numerical methods for verification is caused by the need for such a finite mesh of points on which solutions are computed numerically. This imposes two primary causes for errors: (a) there is only limited knowledge about the behavior in between the finite mesh, and (b) the numerical computations themselves introduce errors. For proper verification, these errors have to be controlled computationally to make sure the system is safe under *all* circumstances.

While the certainty required for verification is impossible to obtain by numerical means alone, we additionally show that numerical methods can provide a stochastic understanding of system safety. The probability of a wrong verification result can be made arbitrarily small under fairly mild assumptions.

We use our techniques to obtain results about *roundabout maneuvers for collision avoidance* in air traffic management (ATM) [9,10]. We show that a classical collision avoidance maneuver is unsafe for more realistic model assumptions. To overcome this limitation, we propose a modified roundabout maneuver that uses

adaptive flight paths following a tangential geometric construction. Since the image computation techniques presented in this paper are suitable for automation, they have impact on improving verification tools like HyTech [11], CheckMate [12], or PHAVer [13] to cover more complicated dynamics. Supporting more general dynamics is important for verifying hybrid systems, for instance, in ATM [9, 10, 14] and for systems biology [6].

Structure of this Paper. After giving the basics of model checking in Sect. 2, we present the roundabout maneuver in Sect. 3. In Sect. 4, we present the framework for approximation refinement model checking. We analyze flow approximation techniques in Sect. 5. In addition, we cover flows that are specified implicitly as solutions of differential equations in Sect. 6. Experimental results of our preliminary model checker for *roundabout maneuvers* are presented in Sect. 7. Related work is discussed in Sect. 8.

2 Preliminaries

For model checking to be effective, both representing sets of states and computing images of sets of states under transitions have to be computable. Hybrid systems have two kinds of transitions: discrete jumps in the state space caused by mode switches, and continuous evolution along flows within a mode; see [6, 11].

Definition 1 (Hybrid Automata). *A* hybrid automaton *A consists of*

- *a continuous state space* $\mathbf{R}^n$*;*
- *a directed graph with vertices* Q *(as modes) and edges* E *(control switches);*
- flows φ_v*, where* $\varphi_v(t; x) \in \mathbf{R}^n$ *is the state reached after staying in mode* v *for time* $t \geq 0$ *when continuous evolution starts in state* $x \in \mathbf{R}^n$*;*
- *invariant conditions* $inv_v \subseteq \mathbf{R}^n$ *for* $v \in Q$*;*
- *jump relations* $jump_e \subseteq \mathbf{R}^n \times \mathbf{R}^n$ *for edges* $e \in E$*;*

where $jump_e$ *and* inv_v *are definable in first-order real arithmetic [2]. Typically, the jump relation* $jump_e$ *contains transition guards and variable resets as in [6].*

To simplify the formal machinery, we define the semantics of hybrid automata in terms of image computation (see, e.g. [6, 15, 11] for details on the relationship to trace semantics). Numerical algorithms typically work within a compact domain. For simplicity, we assume that all flows share the same domain of relevance $D \subseteq \mathbf{R} \times \mathbf{R}^n$, which comprises all relevant states and observation times. In (1) of Fig. 1, the *post-image* for automaton A is defined in terms of its discrete and continuous transitions: $Post_A(Y)$ is the set of states reachable from $Y \subseteq Q \times \mathbf{R}^n$ in one step. The post-image under the continuous flow φ_v restricted to D is defined in (2). For discrete jumps along edge $e \in E$ from $v \in Q$ to $w \in Q$, the post-image is defined in (3). Reachability in an arbitrary number of steps is defined by the least fixpoint equation (4). The *pre-image* $Pre_A(Y)$ is defined accordingly. Model checking reachability of bad states $B \subseteq Q \times \mathbf{R}^n$ from the initial set of states $I \subseteq Q \times \mathbf{R}^n$ amounts to checking emptiness of $Post_A^*(I) \cap B$.

$$Post_A(Y) := \bigcup_{v\in Q} Post_{\varphi_v|_D}(Y) \cup \bigcup_{e\in E} Post_{jump_e}(Y) \quad (1)$$

$$Post_{\varphi_v|_D}(Y) := \{(v,\varphi_v(t;x)) \in Q\times\mathbf{R}^n : (v,x)\in Y, (t,x)\in D \text{ for some } t\geq 0 \text{ and } \varphi_v(t';x)\in inv_v \text{ for all } 0\leq t'\leq t\} \quad (2)$$

$$Post_{jump_e}(Y) := \{(w,y)\in Q\times\mathbf{R}^n \;:\; (x,y)\in jump_e \text{ for some } (v,x)\in Y \text{ and } y\in inv_w \text{ where } e=(v,w)\} \quad (3)$$

$$Post_A^*(Y) := \mu Z.(Y\cup Z\cup Post_A(Z)) \quad (4)$$

Fig. 1. Image computation semantics of hybrid automata

3 Air Traffic Management

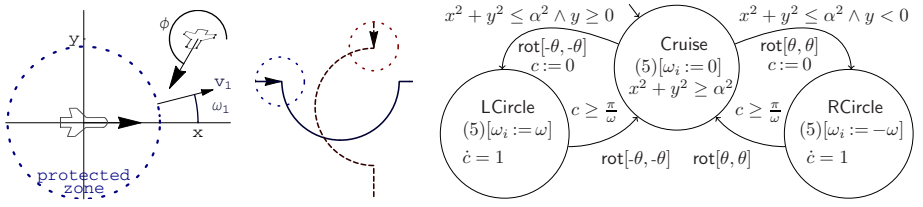
Tomlin et al. [9] presented conflict resolution protocols for air traffic management, which direct two airplanes flying too close to each other to perform collision avoidance maneuvers. Assuming, for simplicity, aircraft remain at the same altitude, a configuration can be described in the special Euclidean group of $\mathbf{R}^2$ [9] and relative coordinates can be used to reduce the state-space dimension. The relative position of aircraft 2 with aircraft 1 at the origin is represented by its (planar) position x, y and orientation ϕ; see Fig. 2a. With linear velocities v_i and angular velocities ω_i (in radians per time unit) of the respective aircraft i, the in-flight dynamics in relative coordinates are as follows (see [9] for details):

$$\dot{x} = -v_1 + v_2\cos\phi + \omega_1 y \qquad \dot{y} = v_2\sin\phi - \omega_1 x \qquad \dot{\phi} = \omega_2 - \omega_1 \;. \quad (5)$$

A configuration is unsafe if there is another aircraft within a 5mi-radius protected zone, i.e., $x^2+y^2<5^2$.

Straight line protocols [9, 10] for collision avoidance are unrealistic. Between straight lines, they assume instant turns, which are impossible in mid-flight. As a more realistic model, we investigate roundabout maneuvers [9], which also contain proper flight curves with $\omega_i\neq 0$, see Fig. 2b. The roundabout maneuver refines several instant turns to realistic curves with more complicated dynamics. For this refinement, we show that the standard maneuvers are unsafe.

Fig. 2c contains the hybrid automaton for *roundabout collision avoidance*, which generalizes the protocols in [9, 10, 14]. This protocol initiates evasive actions when the distance drops to α. The clock c determines when it is safe to turn back into the original direction after a half turn of duration $\frac{\pi}{\omega}$. For a concise presentation, (5)$[\omega_i := s]$ is an abbreviation for the dynamics of equation (5), with ω_1 and ω_2 replaced by s. Further, $\mathsf{rot}[\theta_1,\theta_2]$ denotes the action of the first aircraft turning by θ_1 and the second by θ_2, simultaneously. Typically, the θ_i are chosen as fixed values like $\theta=\pi/2$ [14]. We use $[-r,r]^2\times[0,2\pi]$ with $r=\alpha+8$ as the relevant domain for states (x,y,ϕ) and choose observation times in $[0,400]$. By continuity, other safety-relevant trajectories trespass a point in D.



(a) Configuration. (b) Maneuver. (c) Roundabout maneuver automaton.

Fig. 2. Roundabout collision avoidance maneuver

4 Approximation in Hybrid Systems Model Checking

In this section, we provide the theoretical foundations for flow approximation in model checking hybrid systems and outline the approximation refinement model checking algorithm. Model checking depends on image computation of *sets* of states, which is particularly crucial for infinite-state systems. Yet, computing the image of a set under complicated flows is not possible in general. Hence, our guiding principle is to first approximate complicated dynamics using simpler flows (Sect. 4.2) and then compute images of sets under simple flows (Sect. 4.3).

4.1 Approximation Refinement Model Checking

For approximate set operations, we define the distance between sets $X \subseteq \mathbf{R}^n$ and $Y \subseteq \mathbf{R}^n$ as $d(X,Y) := \inf_{x \in X, y \in Y} \|x - y\|$, and $d(x,Y) := d(\{x\},Y)$ for a point $x \in \mathbf{R}^n$. Further, for an $\epsilon > 0$, let $\mathcal{U}_\epsilon(Y) := \{x \in \mathbf{R}^n : d(x,Y) < \epsilon\}$ be the ϵ-*neighborhood* of $Y \subseteq \mathbf{R}^n$. For convenience, we define $\mathcal{U}_0(Y) := Y$. Finally, let $S[x,y] \subseteq \mathbf{R}^n$ be the *line segment* connecting $x \in \mathbf{R}^n$ and $y \in \mathbf{R}^n$.

Image computation for discrete transitions is as usual in model checking [1]. Hence, we focus on a treatment of continuous evolutions that combines well with techniques for handling discrete image computation. Since the mode does not change during a continuous flow, we drop modes from $Post_{\varphi|_D}(Y)$.

We handle complicated dynamics by approximating flows and we conservatively over-approximate the resulting images. For an approximation of error $\leq\epsilon$, safety proofs require that all states reachable in this approximation have a distance $>\epsilon$ to B. This is captured formally in the following decision problem.

Problem 1 (Approximate reachability in image computation). Given an *arbitrarily effective* function $\varphi \in C^k(D \subseteq \mathbf{R}^n, \mathbf{R}^m)$, i.e., for rational input x, the value $\varphi(x)$ can be computed up to arbitrary precision, and given effective representations of $B \subseteq \mathbf{R}^m$ and of a compact closure D of an open set, decide the following problem with tolerance $\epsilon \geq 0$: "$\mathcal{U}_\epsilon(Post_{\varphi|_D}(Y)) \cap B = \emptyset$?"

Exact image computation is retained with $\epsilon = 0$. Extensions to $Post_A^*(Y)$ are defined inductively using approximate flow images $\mathcal{U}_\epsilon(Post_{\varphi|_D}(Y))$ in Fig. 1.

Safety of an approximation with tolerance ϵ implies safety of the actual system by monotonicity of image computation. If the over-approximation is unsafe,

```
choose initial δ > 0
while true do
    Ã := approx(δ, A); ε := errorbound(Ã)
    reachable := check(U_ε(Post*_Ã(I)) ∩ B ≠ ∅)
    if not reachable then
        return 'A is safe'
    else if ε ≪ 1
        return 'A is unsafe with fragility ε'
    else δ := δ/2
```

Fig. 3. Approximation Refinement Model Checking (AMC)

however, counterexamples can be *spurious*. This happens if the approximation is too coarse because the current guaranteed error bound, ϵ, is still too large and permits behavior that is impossible in reality. Hence, refining the approximation tolerance is necessary [16] until the system is (a) proven safe after closer analysis, or (b) the system is considered *fragile* [3,14] because it is unsafe for a sufficiently small value of ϵ (below the stability advised by general engineering principles). An approximation refinement algorithm (AMC) exploiting those circumstances for Problem 1 is depicted in Fig. 3. It is parametric in a procedure approx for approximating the flows of the hybrid automaton A with a means to determine a uniform error bound. Techniques for this will be examined in Sect. 5–6 using the theory in Sect. 4.2. AMC further depends on the ability to check reachability by image computation in the approximation $\tilde{A}$, which we investigate in Sect. 4.3.

In order to support approximations with posterior error bound reporting, our algorithm distinguishes the refinement tolerance δ from the resulting error bound ϵ. The required assumption to ensure convergence is that ϵ decreases with δ and converges to zero when δ does. Modes can be split into modes that apply for different subregions by partitioning D (using the techniques in [13]) to keep refinements of δ local to smaller parts of the state space. As a further improvement, it is simple to extend AMC to stop if a counterexample has been found that reaches a bad state with a distance $>\epsilon$ to good states (beyond the approximation error). In that case, the concrete system is unsafe without fragility.

4.2 Image Approximation

As a theoretical framework for flow approximations in approx to solve Problem 1 with AMC, we present the following result. It shows that continuous flows support uniform approximation of images with polynomials on compact domains.

Proposition 1 (Weierstraßian flows). *Let $\varphi \in C(D, \mathbf{R}^n)$ on a compact closure $D \subset \mathbf{R}\times\mathbf{R}^n$ of an open set. Then, $\forall \epsilon > 0$ $\exists p \in \mathbf{R}[t, x_1, \ldots, x_n]^n$ $\forall Y \subseteq \mathbf{R}^n$*

$$Post_{\varphi|_D}(Y) \subseteq \mathcal{U}_\epsilon(Post_{p|_D}(Y)) \tag{6}$$

$$Pre_{\varphi|_D}(Y) \subseteq Pre_{p|_D}(\mathcal{U}_\epsilon(Y)) \ . \tag{7}$$

Proof. For any $\epsilon > 0$, let p be a vector of polynomials approximating φ on D with uniform error $<\epsilon$ according to the generalized Weierstraß theorem [17]. Equation (6) is a consequence of the following representation (case (7) is similar):

$$\mathcal{U}_\epsilon(Post_{p|_D}(Y)) = \{z \in \mathbf{R}^n \ : \ \exists x \in Y \ \ \exists t \ \ (t,x) \in D \, , \, \|z - p(t,x)\| < \epsilon\} \ .$$

Let $z \in Post_{\varphi|_D}(Y)$, i.e., let $(t,x) \in D, x \in Y$ with $z = \varphi(t;x)$. The Weierstraß theorem implies $z \in \mathcal{U}_\epsilon(Post_{p|_D}(Y))$, as $\|z - p(t,x)\| = \|\varphi(t;x) - p(t,x)\| < \epsilon$.

This result shows that image computation can be split into approx, i.e., finding a uniform approximation p of φ that satisfies (7), and check, i.e., computing the right-hand side of (7). Further, it proves the existence of an approximation p.

4.3 Polynomial Image Computation and Beyond

In this section, we present classes of flows that support exact image computation of sets of states for the procedure check. These are adequate choices for functions with which approx can approximate more complicated dynamics. Beyond polynomial flows, we generalize exact image computation to piecewise polynomials and rational functions—in particular to multivariate rational splines.

Proposition 2 (Decidability of polynomial image computation). *Given definable Y and D, the right-hand sides of* (6) *and* (7) *in Proposition 1 are definable in first-order real arithmetic, hence decidable by Tarski's theorem [2].*

Proof. Let F_D and F_Y define D and Y, respectively. Then, $z \in \mathcal{U}_\epsilon(Post_{p|_D}(Y))$ is definable by: $\exists x \, \exists t \, (F_Y(x) \wedge F_D(t,x) \wedge \|z - p(t,x)\| < \epsilon)$. As the square function increases strictly monotonically on $[0,\infty)$ and $\epsilon \geq 0$, the Euclidean norm can in turn be defined by: $\|z\| < \epsilon \equiv \sum_{i=1}^n z_i^2 < \epsilon^2$. With this, we can implement check.

Proposition 3. *Piecewise polynomials are definable in first-order arithmetic.*

Proof. Let $s : D \to \mathbf{R}$ be a function consisting of polynomial pieces $P_i : D_i \to \mathbf{R}$ for disjoint domains D_i with $D = D_1 \cup \cdots \cup D_n$ that are definable in first-order real arithmetic. Then, the following equivalence defines the piecewise function s:

$$s(x) = t \quad \equiv \quad \bigvee_{i=1}^n (x \in D_i \wedge p_i(x) = t) \ .$$

The image computation corresponding to (6) follows from the decomposition

$$Post_{s|_D}(Y) \ = \ \bigcup_{i=1}^n Post_{p_i|_{D_i}}(Y) \quad \text{and} \ \ \mathcal{U}_\epsilon(X \cup Y) \ = \ \mathcal{U}_\epsilon(X) \cup \mathcal{U}_\epsilon(Y) \ . \quad (8)$$

Due to their piecewise definitions, splines provide a better approximation with lower degree than polynomials do. Hence, we propose to use splines for image computation, and solve a multitude of simpler polynomial problems as opposed to using a single high-degree polynomial problem. For this, splines in (8) split into a disjoint set of polynomial reachability problems of lower degree. For a result on uniform approximation with multivariate splines, we refer to [18, 19]. Even rational approximations can be used, but AMC does not yet apply them:

Proposition 4. *Tarski's theorem [2] can be extended from semialgebraic sets formed with polynomials over real-closed fields to rational functions.*

Proof. In first-order formulas of real arithmetic with rational expressions, the following equivalences reduce rational (in-)equalities to polynomial formulas:

$$\begin{aligned} p(x)/q(x) = 0 &\equiv p(x) = 0 \wedge q(x) \neq 0 \\ p(x)/q(x) > 0 &\equiv (p(x) > 0 \wedge q(x) > 0) \vee (p(x) < 0 \wedge q(x) < 0) \ . \end{aligned}$$

By using the fact that the field of fractions of $\mathbf{Q}[X_1, \ldots, X_n]$ is a field, all atomic formulas can be reduced to one of the above forms.

5 Flow Approximation

In this section, we analyze which flows can be approximated effectively. In addition to giving an approximation result for bounded flows, we identify the limits of numerical methods for approximating hybrid systems with the certainty that is needed for verification. Further, we show that numerical methods can give sufficient justification of verification in stochastic terms up to arbitrary probability. Throughout the section we assume φ is a flow of a mode of a hybrid system.

Using the results presented so far, we can reduce Problem 1 to the following problem for approx, for which Proposition 1 guarantees the existence of solutions.

Problem 2 (Uniform approximation). Given an arbitrarily effective continuous function $\varphi \in C(D, \mathbf{R}^n)$ on a compact closure $D \subset \mathbf{R} \times \mathbf{R}^n$ of an open set, with an effective representation of D, find an approximation of φ with multivariate splines of uniform error $<\epsilon$.

5.1 Bounded Flow Approximation

In order to turn the theoretical existence result of Proposition 1 into an algorithm approx that solves Problem 2, we need an effective form of Weierstraß approximation. The following result shows that solutions of Problem 2 can be computed effectively when derivatives $\dot{\varphi}$ are continuous and have a known bound.

Proposition 5 (Effective Weierstraß approximation). *If $\varphi \in C^1(D, \mathbf{R}^n)$ and $b := \max_{x \in D} \|\dot{\varphi}(x)\|$ are given, then Problem 2 is computable.*

Proof. Using component-wise approximation and norm properties, we can assume the range of φ is in $\mathbf{R}^1$ rather than $\mathbf{R}^n$. Let $\epsilon > 0, x \in D$. Further, we can assume D is connected (otherwise the problem can be treated separately on each connected component). By premise, φ is arbitrarily effective, i.e., for each $\delta_c > 0$ there is an effective function f_{δ_c} such that for all $y \in D$: $\|\varphi(y) - f_{\delta_c}(y)\| < \delta_c$. Let x_i be a point on a δ_g-grid with distance $\|x - x_i\| < \delta_g$. We assume that $x_i \in D$ and D is convex on the grid cell around x_i. Due to convexity, the mean-value theorem applies and yields a $\xi \in S[x, x_i]$ such that

$$\|\varphi(x) - \varphi(x_i)\| = \|\dot{\varphi}(\xi)(x - x_i)\| = \|\dot{\varphi}(\xi)\| \cdot \|(x - x_i)\| < b\delta_g \ .$$

As φ is arbitrarily effective at the grid point x_i, this inequality implies

$$\|\varphi(x) - f_{\delta_c}(x_i)\| \leq \|\varphi(x) - \varphi(x_i)\| + \|\varphi(x_i) - f_{\delta_c}(x_i)\| < b\delta_g + \delta_c \ .$$

Thus, φ can be approximated by step functions up to precision $b\delta_g + \delta_c$, which can be chosen $<\epsilon$. Such step functions are defined as $f_{\delta_c}(x_i)$ on the $\pm\delta_g/2$ hypercube around x_i (or sufficiently close rational approximations thereof). As step functions are piecewise polynomials there is no need to prove that step functions can be approximated by polynomials (cf. Proposition 3).

5.2 Continuous Image Computation

In this section, we demonstrate a fundamental limitation of numerical approaches to verification of hybrid systems. Despite the fact that Proposition 1 guarantees the existence of a uniform polynomial approximation, effectively constructing such an approximation using numerical computations is impossible without additional symbolic techniques. More generally, we show that even a single step of continuous image computation is not semidecidable using numerical evaluations.

As they require concrete values, numerical algorithms can only evaluate the input function φ *at individual points* but do not have access to its symbolic representation. Even evaluating derivatives of φ at points is not sufficient to obtain decidability:

Proposition 6 (Undecidability of image computation). *Problem 1 is not semidecidable using numerical evaluation of derivatives $\varphi^{(j)}(x)$ for $j \geq 0$ at individual points, even for arbitrarily large tolerable errors $\epsilon > 0$ and arbitrary high degrees of derivatives. This remains true even for smooth functions where all derivatives are effectively known, and when functions are restricted to one-dimensional (effective) smooth polynomial functions with rational coefficients.*

Proof. In Problem 1, choose $n = m = 1$, $D = [0, 1]$, $B = [\epsilon, \infty)$ for the tolerable error $\epsilon > 0$. Assume there is an algorithm $\mathcal{A}$, which solves Problem 1 for this case. Choose a function φ with $\varphi(D) \cap B = \emptyset$, say $\varphi = 0$. Running $\mathcal{A}$ with input φ yields correct output "$=\emptyset$", since $\varphi(x) = 0 < \epsilon$. Tracing the run identifies the set of all points x_i at which $\mathcal{A}$ evaluates at least one of the $\varphi^{(j)}$. Although the set of all x_i is unbounded, it is finite after termination, since $\mathcal{A}$ can only make a finite number of computation steps in a bounded interval of time. After termination, the maximum j where a $\varphi^{(j)}(x_i)$ has been evaluated by $\mathcal{A}$ is finite as well.

Now let $0 < \delta < \min_{i \neq j} \|x_i - x_j\|$, and assume x_2 is not the right-most point, hence $x_2 + \delta \in D$ (otherwise reorder). However, by Hermite interpolation, there is an (effective) polynomial function $g \in C^k(D, \mathbf{R})$ with $g^{(j)}(x_i) = \varphi^{(j)}(x_i) = 0$ and $g(x_2 + \delta) = 2\epsilon > \epsilon$ but $g(D) \cap B \neq \emptyset$. Since φ and g are indistinguishable by the $\varphi^{(j)}(x_i)$ that $\mathcal{A}$ asked about φ, the hypothetical algorithm $\mathcal{A}$ would yield the same output for φ

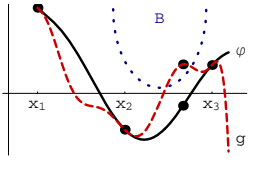


Fig. 4. Indistinguishable

and g, one of which is wrong. Fig. 4 depicts this situation with a more general choice of φ and B that gives better graphics. Moreover, Turing machines choose $x_i \in \mathbf{Q}$, from which $g \in \mathbf{Q}[X]$ can be concluded.

The proof principles of Proposition 6 are highly general and apply for all machine models that only allow a finite number of evaluations of input function φ (and derivatives) at individual points in bounded time. This includes the generalization of "numerical" Turing machines for real values by Blum et al. [7].

As a simple corollary, the same undecidability results apply for Problem 2 using the reduction in Sect. 4. In particular, this shows that the mere presence of a bound is not sufficient if the bound b is not known for Problem 2.

5.3 Probabilistic Model Checking

While Proposition 6 shows that image computation is not semidecidable even in quite robust scenarios with large tolerable errors, increasing the number of points x_i where φ (or its derivatives) are evaluated increases the constraints on the counterexample g, hence—intuitively speaking—increases the likelihood of the reachability problem being answered correctly (when assuming a non-degenerate probability distribution P). If arbitrarily large derivatives are unlikely by system design, model checking algorithms based on purely numerical information can provide stochastic certainty of verification. In that case, the following result shows that such algorithms can perform image computation with arbitrarily high probability by evaluating φ on a sufficiently dense grid.

Proposition 7 (Stochastic model checking). *If $P(\|\dot\varphi\|_\infty > b) \to 0$ when the bound $b \to \infty$, and if D is an open set, then any evaluation of φ on a finite set of points $G \subseteq D$ obtains sufficient information to decide Problem 1 correctly with probability $p \to 1$ as $\|d(\cdot, G)\|_\infty \to 0$.*[1]

Proof. Let (φ, D, B) be a problem instance with tolerance $\epsilon > 0$. Let $G \subseteq D$ be the set of points where φ is evaluated and $\nu := \|d(\cdot, G)\|_\infty$. If $\varphi(x_i) \in \mathcal{U}_\epsilon(B)$ for some $x_i \in G$, the output "$\neq\emptyset$" is correct with tolerance ϵ. Otherwise, we show that the probability of the output "$=\emptyset$" being wrong converges to zero for $\nu \to 0$. Suppose there is an $x \in D$ with $\varphi(x) \in B$. Let $x_i \in G$ have smallest distance to x. Then we can assume $S[x, x_i] \subseteq D$ (otherwise use a $\nu > 0$ such that $\mathcal{U}_\nu(x) \subseteq D$, which exists since D is open). Thus, by mean-value theorem, there is a $\xi \in S[x, x_i]$ such that

$$\epsilon \leq \|\varphi(x) - \varphi(x_i)\| = \|\dot\varphi(\xi)(x - x_i)\| = \|\dot\varphi(\xi)\| \cdot \|x - x_i\| \ . \tag{9}$$

The first inequality holds since $\varphi(x) \in B$ but $\varphi(x_i) \notin \mathcal{U}_\epsilon(B)$. Yet, $\nu \geq \|x - x_i\|$. Thus, dividing (9) by $\nu > 0$ leads to $\frac{\epsilon}{\nu} \leq \|\dot\varphi(\xi)\| \leq \|\dot\varphi\|_\infty$. But this becomes arbitrarily improbable when refining ν, because $P(\|\dot\varphi\|_\infty \geq \frac{\epsilon}{\nu}) \to 0$ for $\nu \to 0$ by premise, as ϵ is a constant independent of ν and $\frac{\epsilon}{\nu} \to \infty$ as $\nu \to 0$.

[1] This result also applies for a compact D by working (separately) on a finite open subcover. $\|d(\cdot, G)\|_\infty = \max_{x \in D} d(x, G)$ corresponds to the "density" of G in D.

6 Differential Flow Approximation

In this section, we investigate how the results of the previous sections can be extended when the flow φ of a mode in a hybrid system is not given to the model checker, but implicitly generated as a numerical solution of a differential equation. For verification, we have to control several sources of errors: (a) initial conditions between the points of the numerical mesh can lead to different behavior of the solutions, (b) observation times t off the mesh lead to interpolation errors, and (c) numerical computations introduce errors. Proposition 6 shows that we have to assume additional knowledge, e.g., a Lipschitz-constant. Note that the undecidability proof of Proposition 6 shows that it is *not* sufficient to assume Lipschitz-continuity without knowledge of the actual Lipschitz-constant.

Proposition 8. *Let $f \in C([a,b] \times \mathbf{R}^n, \mathbf{R}^n)$ be ℓ-Lipschitz-continuous in x, i.e., $\|f(t,x_1) - f(t,x_2)\| \leq \ell\|x_1 - x_2\|$ for all t, x_1, x_2. Then there is a computable set of points sufficient for solving Problem 1 numerically, where φ is a solution of the differential equation $\dot{x}(t) = f(t,x)$.*

Proof. Let $\epsilon > 0$. For t, x_0 let t_2, x_2 be the closest points on a mesh. Then the solution flow $\varphi(t;x_0)$ after time t, with initial value $\varphi(t_0;x_0) = x_0$, is arbitrarily close to the mesh values $\varphi(t_2;x_2)$, which can be approximated numerically:

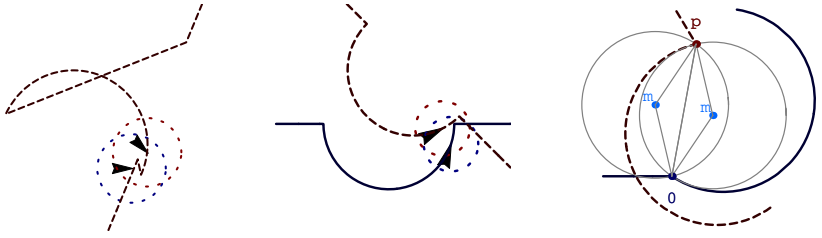
$$\begin{aligned} \|\varphi(t;x_0) - \varphi(t_2;x_2)\| \leq\ & \|\varphi(t;x_0) - \varphi(t;x_2)\| + \|\varphi(t;x_2) - \varphi(t_2;x_2)\| \\ \leq\ & e^{\ell|t-t_0|}\|x_0 - x_2\| + \|\dot{\varphi}(\xi;x_2)\| \cdot |t - t_2| \\ =\ & e^{\ell|t-t_0|}\|x_0 - x_2\| + \|f(\xi,\varphi(\xi;x_2))\| \cdot |t - t_2| \end{aligned} \tag{10}$$

by a consequence of Picard-Lindelöf [20, theorem 7.1.4] and mean-value theorem with a ξ between t and t_2. Further, (10) can be bounded by any $\frac{\epsilon}{2} > 0$ by refining the mesh such that $\|x_0 - x_2\|$ and $|t - t_2|$ are sufficiently small, since the remaining factors are bounded on a compact domain in bounded time and f is Lipschitz-continuous. Moreover, by [20, theorem 7.2.2.3] there are "Lipschitz-continuous one-step methods of order p" (see [20]) that approximate the mesh quantity $\varphi(t_2;x_2)$ with a global discretization error that is bounded by $\frac{\epsilon}{2}$ when refining the mesh. The rate of convergence can be computed from the Lipschitz-constants and p (see [20] for details). Hence, the overall error is bounded by ϵ.

The most crucial influence on the error bound analysis comes from the exponential term in the proof of Proposition 8. Yet, this bound is tight in general: $\dot{x} = \ell x$ is ℓ-Lipschitz-continuous with unique global solution $\varphi(t;x_0) = x_0 e^{\ell t}$ for $t_0 = 0$, hence $\varphi(t;x_0) - \varphi(t;x_2) = e^{\ell t}(x_0 - x_2)$.

7 Experimental Results

Using the results presented in this paper, we have implemented a preliminary approximation refinement model checker for a class of hybrid systems. For a reasonable range of parameter choices (in particular for α, ω, θ), it always produces



(a) Relative CEX. (b) Absolute CEX. (c) Tangential ATM.

Fig. 5. Counterexample flight and adaptive tangential construction

a counterexample to the safety property in Sect. 3 (with distances of ≈0.0016mi, the first after 3 mesh refinements). Fig. 5a contains a counterexample flight in relative coordinates with aircraft 1 fixed at the origin, 5b in absolute coordinates. This counterexample shows that the verification results in [14,10] for roundabout maneuvers starting from orthogonal flight paths do not extend to non-orthogonal initial flight paths. To maintain safe operation for general free flight, we propose the following modified roundabout maneuver with *adaptive tangential rotation*.

Instead of choosing a fixed rotation angle θ as in Sect. 3, we choose rotation angles θ_i for the individual aircraft depending on the current relative position $p = (x, y)$. Let m be the center of any circle of radius α through the plane positions 0 and p (cf. construction in Fig. 5c). Those (gray) circles correspond to worst-case evasive flight curves at maximum angular speed $\omega = v/\alpha$. Actual evasive actions use smaller ω (dark curves). Let γ_1 and γ_2 be the angles of the plane positions 0 and p, respectively, to m according to the following equation system:

$$\alpha^2 = \|m - 0\|^2 \quad \alpha^2 = \|m - p\|^2 \quad \gamma_1 = \angle(m - 0) \quad \gamma_2 = \angle(m - p) \ . \tag{11}$$

We define the angle $\angle(u)$ as the argument of the complex number $u_1 + u_2\imath$. Then, we choose rotation angles (θ_1, θ_2) as $(\gamma_1 - \pi/2, \gamma_2 - \pi/2)$ or $(\gamma_1 + \pi/2, \gamma_2 + \pi/2)$ with all solutions of (11) for γ_j. This rotates the aircraft tangentially to the gray circles such that the aircraft follow the dark curves in circle mode. Among the resulting choices for θ_j, we choose minimal turning angles. Thus, the primary change for the automaton in Fig. 2c is a position-dependent rotation $\mathsf{rot}[\theta_1, \theta_2]$ due to our construction (which happens before the check on $y \geq 0$).

8 Related Work

Several approaches [3,4,5,6] emphasize the importance of quantifier elimination in first-order real arithmetic for hybrid system verification. Our results thus use first-order real arithmetic for approximating more general dynamics.

Piazza et al. [6] propose Taylor series approximation of known flows. For applications in systems biology, they do not handle approximation errors.

Lanotte and Tini [15] propose a syntactic Taylor approximation of hybrid automata with known flows, modified by the maximum error. They use a complicated computation of error bounds from given Lipschitz-constants. Taylor

approximations, though, have a non-uniform and more complicated error distribution, which makes them less useful for verification.

Tomlin et al. [9] derive results for the straight line ATM scenario using Hamilton-Jacobi-Isaacs partial differential equations. Our techniques avoid complicated PDEs and are thus more suitable for automatic model checking.

Massink and Francesco [10] investigate ATM using purely discrete linearized or untimed models. They primarily focus on the straight line protocol but also use coarse over-relaxations to investigate the roundabout maneuver. Massink and Francesco do not investigate the resulting error bounds.

Damm et al. [14] investigate model checking of LTL properties for discrete time robust hybrid systems using interval-constraint solving. They emphasize the importance of robustness in safety-critical control applications and show safety only for a *discrete* roundabout maneuver with orthogonal trajectories.

Asarin et al. [21] approximate non-linear differential equations by piecewise linear differential equations using interpolation. We propose non-linear polynomial and spline approximations of flows and investigate hybrid dynamics.

9 Conclusions and Future Work

We analyzed the image computation problem in hybrid systems model checking with a focus on approximation techniques for continuous dynamics. We presented a model checking algorithm that successively refines flow approximations. It approximates complicated dynamics using simpler flows (approx), and then computes images of sets of states under simple flows (check) taking into account error bounds. Flow approximations are refined when counterexamples are spurious.

Uniform polynomial approximations always exist for continuous functions on compact domains. Despite that, we have shown that the image computation problem for continuous flows is not semidecidable with numerical evaluations even for very restricted dynamics. With a priori knowledge about the system behavior, uniform approximation is effective. We have illustrated that such additional knowledge can either be obtained from information on bounds of flows or differential equations, or from stochastic information about likely system behavior. Definitely, numerical computations are invaluable for verification speed-up. Yet, for the mathematical rigor and certainty that is required in verification, they always have to be accompanied by symbolic analysis.

Additionally, we gave results for the *roundabout maneuver* in air traffic management using our preliminary model checker implementation. For free flight, we show that a classical maneuver is unsafe and propose a solution.

Future work includes improvements of our model checker. For the roundabout maneuver, we want to analyze situations arising from discrepancies in relative position recording of the aircraft, and extend our collision avoidance protocol to full curve dynamics using compositional verification. Finally, we want to investigate the impact of rational spline approximations for hybrid system verification.

References

1. Clarke, E.M., Grumberg, O., Peled, D.A.: Model Checking. MIT Press (1999)
2. Tarski, A.: A Decision Method for Elementary Algebra and Geometry. 2nd edn. University of California Press, Berkeley (1951)
3. Fränzle, M.: Analysis of hybrid systems. In Flum, J., Rodríguez-Artalejo, M., eds.: CSL. Volume 1683 of LNCS., Springer (1999) 126–140
4. Lafferriere, G., Pappas, G.J., Yovine, S.: A new class of decidable hybrid systems. In Vaandrager, F.W., van Schuppen, J.H., eds.: HSCC. Volume 1569 of LNCS., Springer (1999) 137–151
5. Anai, H., Weispfenning, V.: Reach set computations using real quantifier elimination. In Benedetto, M.D.D., Sangiovanni-Vincentelli, A.L., eds.: HSCC. Volume 2034 of LNCS., Springer (2001) 63–76
6. Piazza, C., Antoniotti, M., Mysore, V., Policriti, A., Winkler, F., Mishra, B.: Algorithmic algebraic model checking I: Challenges from systems biology. In Etessami, K., Rajamani, S.K., eds.: CAV. Volume 3576 of LNCS., Springer (2005)
7. Blum, L., Cucker, F., Shub, M., Smale, S.: Complexity and real computation. Springer New York, Inc., Secaucus, NJ, USA (1998)
8. Mora, T.: Solving Polynomial Equation Systems II. Cambridge Univ. Press (2005)
9. Tomlin, C., Pappas, G.J., Sastry, S.: Conflict resolution for air traffic management. IEEE Transactions on Automatic Control **43**(4) (1998) 509–521
10. Massink, M., Francesco, N.D.: Modelling free flight with collision avoidance. In: ICECCS, IEEE Computer Society (2001) 270–280
11. Alur, R., Henzinger, T.A., Ho, P.H.: Automatic symbolic verification of embedded systems. IEEE Trans. Software Eng. **22**(3) (1996) 181–201
12. Silva, B.I., Richeson, K., Krogh, B.H., Chutinan, A.: Modeling and verification of hybrid dynamical system using CheckMate. In: ADPM. (2000)
13. Frehse, G.: PHAVer: Algorithmic verification of hybrid systems past HyTech. [22]
14. Damm, W., Pinto, G., Ratschan, S.: Guaranteed termination in the verification of LTL properties of non-linear robust discrete time hybrid systems. In Peled, D., Tsay, Y.K., eds.: ATVA. Volume 3707 of LNCS., Springer (2005)
15. Lanotte, R., Tini, S.: Taylor approximation for hybrid systems. [22] 402–416
16. Clarke, E.M., Grumberg, O., Jha, S., Lu, Y., Veith, H.: Counterexample-guided abstraction refinement. In Emerson, E.A., Sistla, A.P., eds.: CAV. Volume 1855 of LNCS., Springer (2000) 154–169
17. Stone, M.H.: The generalised Weierstrass approximation theorem. Math Mag **21** (1948) 167–184 and 237–254
18. Bejancu, A.: The uniform convergence of multivariate natural splines. Technical Report NA1997/07, Applied Mathematics, Cambridge, UK (1997)
19. Wang, R.H.: Multivariate Spline Functions and Their Applications. Kluwer (2001)
20. Stoer, J., Bulirsch, R.: Introduction to Numerical Analysis. Springer, NY (2002)
21. Asarin, E., Dang, T., Girard, A.: Reachability analysis of nonlinear systems using conservative approximation. In Maler, O., Pnueli, A., eds.: HSCC. Volume 2623 of LNCS., Springer (2003) 20–35
22. Morari, M., Thiele, L., eds.: HSCC. In Morari, M., Thiele, L., eds.: HSCC. Volume 3414 of LNCS., Springer (2005)