8-2009

Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study

Andre Platzer
Carnegie Mellon University

Edmund M. Clarke
Carnegie Mellon University

Formal Verification of Curved Flight Collision Avoidance Maneuvers: A Case Study

André Platzer **Edmund M. Clarke**

August 2009
CMU-CS-09-147

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

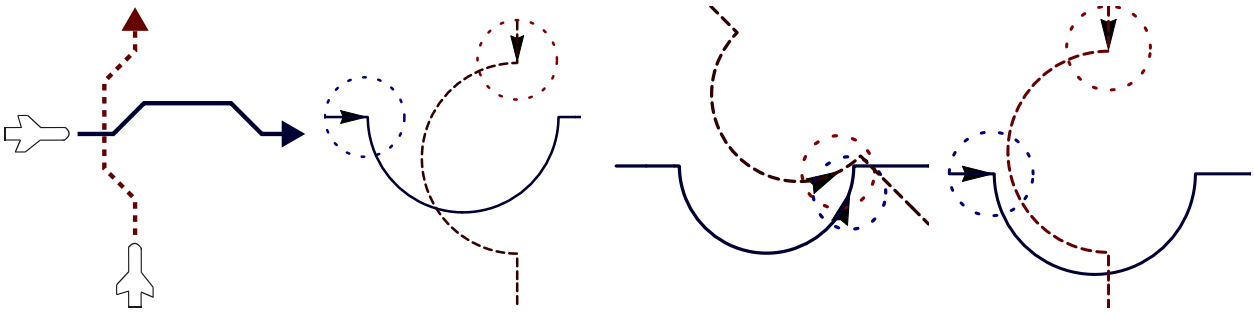
School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA

This research was sponsored by the German Research Council (DFG) under grant SFB/TR 14 AVACS, by the NASA under grant NNG05GF84H, the Berkman Faculty Award, by General Motors and the Carnegie Mellon University-General Motors Collaborative Research Laboratory under grant no. GM9100096UMA, the National Science Foundation (NSF) under grants CCR-0411152, CCF-0429120, CCF-0541245, by the Semiconductor Research Corporation (SRC) under contracts no. 2008TJ1860, and by the Air Force (University of Vanderbilt) under contract no. 18727S3. 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 or government.

Keywords: formal verification of hybrid systems, deduction, air traffic control, logic for hybrid systems

Abstract

Aircraft collision avoidance maneuvers are important and complex applications. Curved flight exhibits nontrivial continuous behavior. In combination with the control choices during air traffic maneuvers, this yields hybrid systems with challenging interactions of discrete and continuous dynamics. As a case study illustrating the use of a new proof assistant for a logic for nonlinear hybrid systems, we analyze collision freedom of roundabout maneuvers in air traffic control, where appropriate curved flight, good timing, and compatible maneuvering are crucial for guaranteeing safe spatial separation of aircraft throughout their flight. We show that formal verification of hybrid systems can scale to curved flight maneuvers required in aircraft control applications. We introduce a fully flyable variant of the roundabout collision avoidance maneuver and verify safety properties by compositional verification.



(a) Linear (b) Circular (c) Counterexample (d) Tangential

Figure 1: Evolution of collision avoidance maneuvers in air traffic control

1 Introduction

In air traffic control, collision avoidance maneuvers [23, 13, 5, 6, 10] are used to resolve conflicting flight paths that arise during free flight. See Fig. 1 for a series of increasingly more realistic—yet also more complicated—aircraft collision avoidance maneuvers. Fig. 1c shows a malfunctioning collision avoidance attempt. Collision avoidance maneuvers are a "last resort" for resolving air traffic conflicts that could lead to collisions. They are important whenever conflicts have not been detected by the pilots during free flight or by the flight directors of the Air Route Traffic Control Centers. Consequently, complicated online trajectory prediction or maneuver planning may no longer be feasible in the short time that remains for resolving the conflict. In the tragic 2002 mid-flight collision in Überlingen [3], the aircraft collided tens of seconds after the on-board traffic alert and collision avoidance system TCAS [13] signalled a traffic alert. Thus, for safe aircraft control we need particularly reliable reactions with maneuvers whose correctness has been established previously by a thorough offline analysis. To ensure correct functioning of aircraft collision avoidance maneuvers under all circumstances, the temporal evolution of the aircraft in space must be analyzed carefully together with the effects that maneuvering control decisions have on their dynamics. This results in complicated superpositions of physical system dynamics with control, which is an example of a hybrid system [7].

Several numerical [23, 11, 2, 9, 10] or optimization-based [11, 2, 8, 10] approaches have been proposed for air traffic control. It is difficult to give sound formal verification results for these approaches due to errors in numerical computations or implicit definition of maneuvers in terms of complicated optimization processes. Formal verification is important to avoid collisions, see Fig. 1c. Formal results have been given by geometrical reasoning [5, 6, 24, 25] in PVS. Yet, one still has to prove by other techniques that the hybrid dynamics of a flight controller actually follows the geometrical shapes. In contrast, we verify the hybrid system dynamics directly using a formally sound approach (assuming sound elementary decision procedures), consider curved flight, and achieve better automation.

Control Challenges Because of the complicated spatio-temporal movement of aircraft, their maneuvers are challenging for verification. Unlike in ground transportation, braking and waiting

is not an option to resolve conflicts. Consequently, aircraft maneuvers have to be coordinated such that the aircraft always respect minimal and maximal lateral and angular speed constraints yet always remain safely separated. Further, angular velocity for curving is the primary means of control, because changes in thrust and linear speed are less efficient for aircraft.

Technical Challenges Complexities in analysis of aircraft maneuvers manifest most prominently in difficulties with analysing hybrid systems for flight equations. General solutions of flight equations involve trigonometric functions that depend on the angular velocity ω and the orientation of the aircraft in space. For straight line flight ($\omega = 0$), the movement in space is just linear so that classical analysis techniques can be used [7]. These include pure straight line maneuvers [23, 14, 5, 6, 10]; see, e.g., Fig. 1a. They have to assume instant turns for heading changes of the aircraft between multiple straight line segments. Instant turns, however, are impossible in mid-flight, because they are *not flyable*: Aircraft cannot suddenly change their flight direction from 0 to 45 degrees discontinuously but need to follow a smooth curve instead, in which they slowly steer towards the desired direction by adjusting the angular velocity ω appropriately. Further the area required by maneuvers for which instant turns could possibly be understood as adequately close approximations of properly curved flight is prohibitively huge. Curved flight is thus an inherent part of real aircraft control.

During curved flight, the angular velocity ω is non-zero. For $\omega \neq 0$, flight equations have transcendental solutions, which generally fall into undecidable classes of arithmetics; see Appendix A.1. Consequently, maneuvers with curves, like in Fig. 1b–1d, are more realistic but also substantially more complicated for verification than straight line maneuvers like that in Fig. 1a. We have recently developed a *sound* verification algorithm that works with differential invariants [17, 20, 22] instead of solutions of differential equations to address this arithmetic. In the associated report [21], we have shown that 3 kinds of properties can be verified with this approach for some phases of curved flight. Now we prove a significant extension and show that, indeed, a full curved flight maneuver is amenable to formal verification and we verify 12 corresponding properties.

In this paper, we introduce and verify the *fully flyable tangential roundabout maneuver (FTRM)*. It refines the non-flyable tangential roundabout maneuver (NTRM) from Fig. 1d, which has discontinuities at the entry and exit points of roundabouts, to a fully flyable curved maneuver. Unlike most previously proposed maneuvers [23, 2, 14, 5, 4, 6, 10], FTRM does not have non-flyable instant turns. It is flyable and smoothly curved. Unlike other approaches emphasizing the importance of flyability [11], we give formal verification results.

Contribution Our main contribution is to show that reality in model design and coverage in formal verification are no longer incompatible desires even for applications as complex as aircraft maneuvers. As a case study illustrating the use of differential dynamic logic for hybrid systems [18], we demonstrate how tricky and nonlinear dynamics can be verified with our verification algorithm [20, 22] in our verification tool KeYmaera. We introduce a fully curved flight maneuver and verify its hybrid dynamics formally. In contrast to previous approaches, we handle curved flight, hybrid dynamics, and produce formal proofs with almost complete automation. Manual

effort is still needed to simplify arithmetical complexity and modularize the proof appropriately. We further illustrate the resulting verification conditions for the respective parts of the maneuver. Finally, we identify the most difficult steps during the verification and present new transformations to handle the enormous computational complexity. To reduce complexity, we still use some of the simplifications assumed in related work, e.g., synchronous maneuvering (i.e. aircraft make simultaneous maneuver choices).

2 Related Work

Lafferriere et al. [12] gave important decidability results for hybrid systems with some classes of linear continuous dynamics but only random discrete resets. These results do not apply to air traffic maneuvers, because these maneuvers have non-trivial resets: the aircraft's position does not just jump randomly when switching modes but, rather, systematically according to the maneuver.

Tomlin et al. [23] analyze competitive aircraft maneuvers game-theoretically using numerical approximations of partial differential equations. As a solution, they propose roundabout maneuvers and give bounded-time verification results for straight-line approximations (Fig. 1a). We verify actual curved roundabout maneuvers with up to 28 variables and use a sound symbolic approach that avoids numerical approximation errors.

Flyability has been identified as one of the major challenges in Košecká et al. [11], where planning based on superposition of potential fields has been used to resolve air traffic conflicts. This planning does not guarantee flyability but, rather, defaults to classical vertical altitude changes whenever a nonflyable path is detected. The resulting maneuver has not yet been verified. The planning approach has been pursued by Bicchi and Pallottino [2] with numerical simulations.

Numerical simulation algorithms approximating discrete-time Markov Chain approximations of aircraft behavior have been proposed by Hu et al. [9]. They approximate bounded-time probabilistic reachable sets for one initial state. We consider hybrid systems combining discrete control choices and continuous dynamics instead of uncontrolled, probabilistic continuous dynamics.

Hwang et al. [10] have presented a straight-line aircraft conflict avoidance maneuver that involves optimization over complicated trigonometric computations, and validate it using random numerical simulation and informal arguments.

The work of Dowek et al. [5] and Galdino et al. [6] is probably closest to ours. They consider straight-line maneuvers and formalize geometrical proofs in PVS.

A few attempts [14, 4] have been undertaken to Model Check discretizations of roundabout maneuvers, which indicate avoidance of orthogonal collisions (Fig. 1b). However, counterexamples found by our Model Checker in previous work [19] show that collision avoidance does not extend to other initial flight paths of the classical roundabout; see Fig. 1c.

Pallottino et al. [16] have presented a spatially distributed pattern for multiple roundabout circles at different positions. They reason manually about desirable properties of the system and estimate probabilistic results as in [9]. Pallottino et al. thus take a view that is complementary to ours: they determine the global compatibility of multiple roundabouts while assuming correct functioning within each local roundabout. We verify that the actual hybrid dynamics of each local roundabout is collision free. Generalizing our approach to verify a spatial pattern of verified local

roundabouts could be interesting future work.

Similarly, the work by Umeno and Lynch [25, 24] is complementary to ours. They consider real-time properties of airport protocols using Timed I/O Automata. We are interested in proving local properties of the actual hybrid system.

Our approach has a very different focus than other complementary approaches:

- Our maneuver directly involves curved flight unlike [23, 9, 5, 6, 10, 25, 24]. This makes our maneuver more realistic but much more difficult to analyze.
- Unlike [11, 9, 10], we do not give results for a finite (sometimes small) number of initial flight positions (simulation). Instead, we verify uncountably many initial states and give unbounded-time horizon verification results.
- Unlike [23, 11, 2, 9, 8, 10], we use symbolic instead of numerical computation so that numerical and floating point errors cannot cause soundness problems.
- Unlike [2, 14, 9, 5, 6, 10, 25, 24], we analyze hybrid system dynamics directly.
- Unlike [11, 23, 2, 9, 10, 14, 16] we produce formal, deductive proofs. Further unlike the formal proofs in [5, 6, 25, 24], our verification is much more automatic.
- In [5, 6, 10, 25, 24], it remains to be proven that the hybrid dynamics and flight equations follow the geometrical thoughts. In contrast, our approach directly works for the hybrid flight dynamics. We illustrate verification results graphically to help understand them, but the figures do not prove anything.
- Unlike [15], we consider collision avoidance maneuvers, not just detection.
- Unlike [2, 8], we do not guarantee optimality of the resulting maneuver.

3 Background: Differential Dynamic Logic

Hybrid Programs We use a *hybrid program* (HP) notation [18] for hybrid systems that include hybrid automata (HA) [7]. Each discrete and continuous transition corresponds to a sequence of statements, with a nondeterministic choice ($\cup$) between these transitions. Line 2 in Fig. 2 represents a continuous transition in a simplistic altitude controller. It tests (denoted by $?q = \mathit{up}$) if the current location q is *up*, and then follows a differential equation restricted to invariant region $z \leq 9$ (conjunction $z' = 1 \wedge z \leq 9$). Line 3 tests guard $z \geq 5$ when in state *up*, resets z by a discrete assignment, and then changes location q to *down*. The * at the end indicates that the transitions of a HA repeat indefinitely. We will build HP directly, which gives more natural programs than HA-translation.

As *terms* we allow polynomials over $\mathbb{Q}$ with variables in a set V. *Hybrid programs (HP)* are built with the statements in Table 1. The effect of $x := \theta$ is an instantaneous discrete jump assigning θ to x. Instead, $x := *$ randomly assigns *any* real value to x by a nondeterministic choice. During a continuous evolution $x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n \wedge \chi$ with terms θ_i, all conjuncts need to hold.

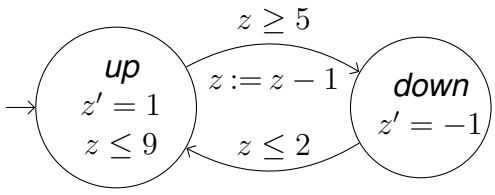
Table 1: Statements and (informal) effects of hybrid programs (HP)

notation	statement	effect
$x := \theta$	discrete assignment	assigns term θ to variable $x \in V$
$x := *$	nondet. assignment	assigns any real value to $x \in V$
$x_1' = \theta_1 \wedge \ldots$ $\ldots \wedge x_n' = \theta_n \wedge \chi$	continuous evolution	diff. equations for $x_i \in V$ and terms θ_i, with formula χ as evolution domain
$?\chi$	state check	test formula χ at current state
$\alpha;\ \beta$	seq. composition	HP β starts after HP α finishes
$\alpha \cup \beta$	nondet. choice	choice between alternatives HP α or β
α^*	nondet. repetition	repeats HP α n-times for any $n \in \mathbb{N}$

Its effect is a continuous transition controlled by the differential equation $x_1' = \theta_1, \ldots, x_n' = \theta_n$ that always satisfies the arithmetic constraint χ (thus remains in the region described by χ). This directly corresponds to a continuous evolution mode of a HA. The effect of state check $?\chi$ is a *skip* (i.e., no change) if χ is true in the current state and that of *abort*, otherwise. Non-deterministic choice $\alpha \cup \beta$ expresses alternatives in the behavior of the hybrid system. Sequential composition $\alpha;\beta$ expresses a behavior in which β starts after α finishes (β never starts if α continues indefinitely). Non-deterministic repetition α^*, repeats α an arbitrary number of times ($\geq$0). If $\mathcal{F}$ is a differential equation system and G is a first-order formula, the operation *do* $\mathcal{F}$ *until* G expresses that the system follows differential equation $\mathcal{F}$ exactly until condition G is true. It is definable by a HP. We define *do* $\mathcal{F}$ *until* G as the HP $\mathcal{F} \wedge (\neg G \vee \partial G);\ ?G$. There $\mathcal{F}$ evolves while $\neg G \vee \partial G$ holds and can only stop when G holds. There ∂G denotes the border of G. For instance, *do* $\mathcal{F}$ *until* $x_1 \geq 0$ is $\mathcal{F} \wedge x_1 \leq 0;\ ?x_1 \geq 0$.

Formulas of dL To express and combine correctness properties of HP, we use a verification logic for HP: The *differential dynamic logic* dL [18] is an extension of first-order logic over the reals with modal formulas like $[\alpha]\phi$, which is true iff all states reachable by following the transitions of HP α satisfy property ϕ (*safety*). Reachability properties are expressible using the dual modality $\langle\alpha\rangle\phi$, which is true iff there is a state satisfying ϕ that α can reach from its initial state. *Formulas of* dL are defined by the following grammar, where θ_1, θ_2 are terms, $\sim \in \{=, \leq, <, \geq, >\}$, ϕ, ψ are formulas, $x \in V$, and α is an HP (Table 1):

$$\text{Formula} \ ::= \ \theta_1 \sim \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi \ .$$



$q := \textit{up};$ /* *initial location is up* */
$\big($ $(?q = \textit{up};\ \ z' = 1 \wedge z \leq 9)$
$\cup\ (?q = \textit{up} \wedge z \geq 5;\ \ z := z - 1;\ \ q := \textit{down})$
$\cup\ (?q = \textit{down};\ \ z' = -1)$
$\cup\ (?q = \textit{down} \wedge z \leq 2;\ \ q := \textit{up};\ \ ?z \leq 9)\big)^*$

Figure 2: Hybrid automaton vs. hybrid program (simplistic altitude control)

A Hoare-triple $\{\psi\}\alpha\{\phi\}$ can be expressed as $\psi \rightarrow [\alpha]\phi$, which is true iff all states reachable by HP α satisfy ϕ when starting from an initial state that satisfies ψ.

The *semantics* of dL and HP is a Kripke semantics over $\mathbb{R}$; see appendix B

4 Curved Flight in Roundabout Maneuvers

4.1 Flight Dynamics

The parameters of two aircraft at (planar) position $x = (x_1, x_2)$ and $y = (y_1, y_2)$ in $\mathbb{R}^2$ flying in directions $d = (d_1, d_2) \in \mathbb{R}^2$ and $e = (e_1, e_2)$ are illustrated in Fig. 3. Their dynamics is determined by their angular speeds $\omega, \varrho \in \mathbb{R}$ and linear velocity vectors d and e, which describe both the linear velocity $\|d\| := \sqrt{d_1^2 + d_2^2}$ and orientation of the aircraft in space. Roundabout maneuvers are horizontal collision avoidance maneuvers so that, like [23, 14, 8, 4, 16, 6, 10], we simplify to planar positions. We denote the flight equations for the aircraft at x and y with angular velocities ω, ϱ by $\mathcal{F}(\omega)$ and $\mathcal{G}(\varrho)$ respectively, see [23] and Appendix A.1:

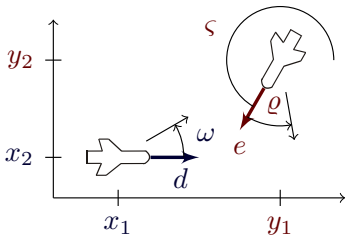


Figure 3: Aircraft flight

$$[x' = d \qquad d' = \omega d^{\perp}] \qquad (\mathcal{F}(\omega))$$
$$[y' = e \qquad e' = \varrho e^{\perp}] \qquad (\mathcal{G}(\varrho))$$

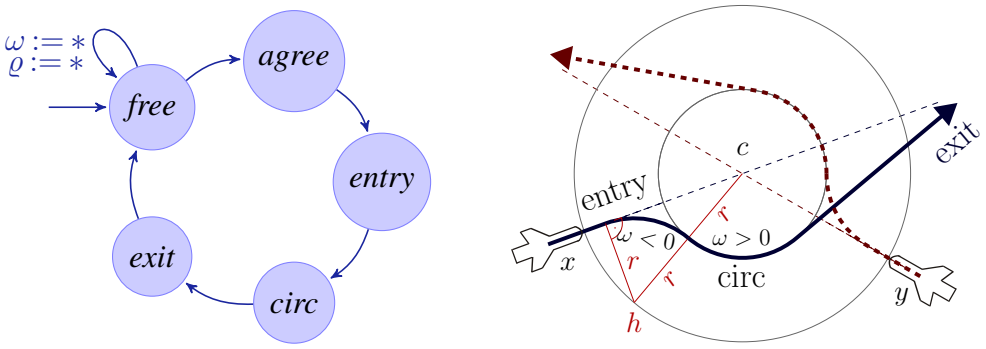
There $d^{\perp} := (-d_2, d_1)$ is the *orthogonal complement* of vector d. Differential equations $\mathcal{F}(\omega)$ express that x is moving in direction d, which is rotating with angular velocity ω, i.e., evolves orthogonal to d. Equations $\mathcal{G}(\varrho)$ are similar for y, e and ϱ. In safe flight configurations, aircraft respect protected zone p. That is, they are separated by at least distance p, i.e., the state satisfies formula $\mathcal{S}(p)$:

$$\mathcal{S}(p) \;\equiv\; \|x - y\|^2 \geq p^2 \;\equiv\; (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2 \quad \text{for } p \in \mathbb{R} \qquad (1)$$

Like all other parameters, we treat p purely symbolically without a specific value. In practice, horizontal separation should be $\geq$5mi, vertical separation $\geq$1000ft.

4.2 Roundabout Maneuver Overview

FTRM consists of the phases in the protocol cycle in Fig. 4a which correspond to the marked flight phases in Fig. 4b. During free flight, the aircraft move without restriction by repeatedly choosing arbitrary new angular velocities ω and ϱ respectively (as indicated by the self loop of phase *free* in Fig. 4a). When the aircraft come too close to one another, they agree on a compatible roundabout maneuver by negotiating a compatible roundabout center $c = (c_1, c_2)$ in coordination phase *agree* by communication. Next, the aircraft approach the actual roundabout circle in a right curve with $\omega < 0$ (*entry* mode) according to Fig. 4b, thereby approaching a tangential configuration around center c. During the *circ* mode, the aircraft follow the circular roundabout maneuver around



(a) Collision avoidance protocol

(b) Maneuver construction

Figure 4: Protocol cycle and construction of flyable roundabout maneuver

the agreed center c with a left curve of common angular velocity $\omega > 0$. Finally, the aircraft leave the circular roundabout in cruise mode ($\omega = 0$) in their original direction (*exit*) and enter free flight again when they have reached sufficient distance (the protocol cycle repeats as necessary). The collision avoidance maneuver is symmetric when exchanging left and right curves.

4.3 Compositional Verification Plan

For verifying safety properties and collision avoidance of FTRM, we decompose the verification problem and pursue the following overall verification plan:

AC1 *Tangential roundabout maneuver cycle*: We prove that the protected zones of aircraft are safely separated at all times during the whole maneuver (including repetitive collision avoidance maneuver initiation and including multiple aircraft) with a simplified but not yet flyable entry operation $entry_n$. Subsequently, we refine this verification result to a flyable maneuver by verifying that we can replace $entry_n$ with its flyable variant *entry*.

AC2 *Bounded control choices for aircraft velocities*: We show that linear speeds remain unchanged during the whole maneuver (the aircraft do not stall).

AC3 *Flyable entry*: We prove that the simplified $entry_n$ procedure can be replaced by a flyable curve *entry* reaching the same position as $entry_n$.

AC4 *Bounded entry duration*: Flyable *entry* procedure succeeds in bounded time, i.e., the aircraft reach the roundabout circle in some bounded time $\leq T$.

AC5 *Safe entry separation*: Most importantly, we prove that the protected zones of aircraft are still respected during the flyable entry procedure.

AC6 *Successful negotiation*: We prove that the negotiation phase (*agree*) satisfies the respective requirements of multiple aircraft simultaneously.

AC7 *Safe exit separation*: We show that, for its bounded duration, the exit procedure cannot produce collisions and that the initial *far separation* for free flight is reached again so that the FTRM cycle repeats safely.

This plan modularizes the proof and allows us to identify the respective safety constraints imposed by the various maneuver phases successively. We present details of these verification tasks in the sequel and summarize the respective verification results into a joint safety property of FTRM in Section 6. The proof and formulation for **AC2** is a simple variation of **AC1** and will not be discussed. It is a consequence of previous results [17].

4.4 Tangential Roundabout Maneuver Cycles (AC1)

First, we analyze roundabouts with a simplified instant entry procedure and without an exit procedure (**AC1**), i.e., the non-flyable NTRM depicted in Fig. 1d. We refine this maneuver and its verification to the flyable FTRM afterwards.

Modular Correctness of Tangential Roundabout Cycles We verify that NTRM safely avoids collisions, i.e., the aircraft always maintain a safe distance $\geq p$ during the curved flight in roundabout. In addition, these results show that arbitrary repetitions of the protocol cycle are always safe when, as a first step, we simplify the entry maneuver. The NTRM model and property are summarized in Fig. 5.

$$
\begin{aligned}
\psi &\equiv \mathcal{S}(p) \rightarrow [\mathit{NTRM}]\,\mathcal{S}(p)\\
\mathit{NTRM} &\equiv (\mathit{free};\ \mathit{agree};\ \mathit{entry}_n;\ \mathit{circ})^*\\
\mathit{free} &\equiv (\omega := *;\ \ \varrho := *;\ \ \mathcal{F}(\omega) \wedge \mathcal{G}(\varrho) \wedge \mathcal{S}(p))^*\\
\mathit{agree} &\equiv \omega := *;\ c := *\\
\mathit{entry}_n &\equiv d := \omega(x-c)^{\perp};\ \ e := \omega(y-c)^{\perp}\\
\mathit{circ} &\equiv \mathcal{F}(\omega) \wedge \mathcal{G}(\omega)
\end{aligned}
$$

Figure 5: Nonflyable tangential roundabout collision avoidance maneuver NTRM

The simplified flight controller in Fig. 5 performs collision avoidance maneuvers by tangential roundabouts and repeats these maneuvers any number of times as needed. During each cycle of the loop of *NTRM*, the aircraft first perform arbitrary free flight (*free*) by choosing arbitrary new angular velocities ω and ϱ (repeatedly as indicated by the loop in *free*). Aircraft only fly freely while they are safely separated, which is expressed by constraint $\mathcal{S}(p)$ in the differential equation for *free*. Then the aircraft agree on an arbitrary roundabout center c and angular velocity ω (*agree*). We model this communication by nondeterministic assignments to the shared variables ω, c. Refinements include all negotiation processes that reach an agreement on common ω, c in bounded time. Next, they perform the simplified non-flyable entry procedure (entry_n) with instant turns (Fig. 1d). This operation identifies the goal state that *entry* needs to reach:

$$\mathcal{R} \equiv d = \omega(x-c)^{\perp} \wedge e = \omega(y-c)^{\perp} \tag{2}$$

It expresses that, at the positions x and y, respectively, the directions d and e are tangential to the roundabout circle at center c and angular velocity ω; see Fig. 6. Finally, the roundabout maneuver itself is carried out in *circ*. The collision avoidance roundabouts can be left again by repeating the

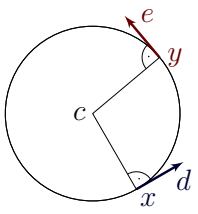


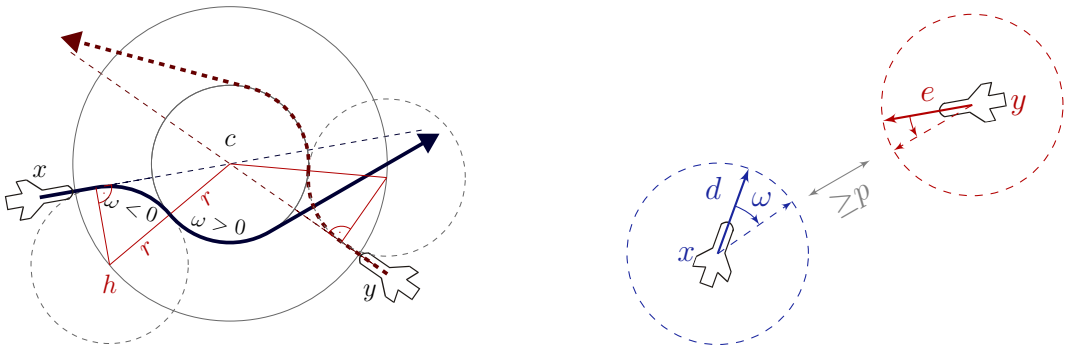
Figure 6: $\mathcal{R}$

loop and entering arbitrary free flight at any time. When further conflicts occur during free flight, the controller in Fig. 5 again enters roundabout conflict resolution maneuvers.

Multiple Aircraft We prove separation for up to 5 aircraft participating in the roundabout at the same time. There, the safety property is mutual collision avoidance, i.e., each aircraft has a safe distance $\geq p$ to every other aircraft, which yields a quadratic number of separation properties that have to be verified. This quadratic increase in the size of the property that actually needs to be proven for a safe roundabout of n aircraft and the increased dimension of the underlying continuous state space increase verification times. Also see Appendix A.2.

4.5 Flyable Entry Procedures (AC3)

For property **AC3** in Section 4.3, we generalize the verification results about NTRM with simplified entry procedures (Fig. 1d) to FTRM (Fig. 4b) by replacing the non-flyable $entry_n$ procedure with flyable curves (called *entry*). This turns the non-flyable NTRM into the flyable FTRM maneuver.



(a) Flyable entry characteristics

(b) Entry separation by overapproximation

Figure 7: Flyable entry maneuver: characteristics and separation

Flyable Entry Properties A flyable entry maneuver that follows the smooth entry curve from Fig. 4b is constructed according to Fig. 7a and specified formally as:

$$(r\omega)^2 = \|d\|^2 \wedge \|x-c\| = \sqrt{3}r \wedge \exists\lambda{\geq}0\,(x+\lambda d = c) \;\wedge\; \|h-c\| = 2r \;\wedge\; d = -\omega(x-h)^{\perp} \\ \rightarrow\; [\mathcal{F}(-\omega) \wedge \|x-c\| \geq r]\,\big(\|x-c\| \leq r \rightarrow d = \omega(x-c)^{\perp}\big) \quad (3)$$

The assumptions in formula (3) express that r is the radius corresponding to speed $\|d\|$ and angular velocity ω ($(r\omega)^2 = \|d\|^2$) and that *entry* starts with distance $\sqrt{3}r$ heading towards c ($\exists\lambda{\geq}0\,(x+\lambda d = c)$). For the construction of the maneuver and positioning in space, we use the auxiliary anchor point $h \in \mathbb{R}^2$ identified in Fig. 7a and line 1 of (3). It is positioned relative to the roundabout center c and the x position at the start of the entry curve (i.e., with x at the right angle indicated in Fig. 7a). The entry curve around h is similar to the roundabout curve around c. Formally, h is characterized by distance r to x, distance $2r$ to c ($\|h-c\| = 2r$) and, further, vector $x-h$ is orthogonal to d and obeys the relative orientation of the curve belonging to $-\omega$ (hence $d = -\omega(x-h)^{\perp}$). The property in (3) specifies that the tangential goal configuration (2) around c is reached by a flyable curve when waiting until aircraft x and center c have distance r, because the domain restriction of the dynamics is $\|x-c\| \geq r$ (line 2) and the postcondition assumes $\|x-c\| \leq r$, which imply $\|x-c\| = r$. The feasibility of choosing anchor point h can be shown by proving an existence property; see Appendix A.3.

Spatial Symmetry Reduction The property in (3) can be verified in a simplified version. We use a new *spatial symmetry reduction* to simplify property (3) computationally. We exploit symmetries to reduce the spatial dimension by fixing variables. Without loss of generality, we recenter the coordinate system with c at position 0. Further, we can assume aircraft x comes from the left by changing the orientation of the coordinate system. Finally, we assume, without loss of generality, linear speed 1 (by rescaling units appropriately). Observe that we *cannot* fix a value for both the linear speed and the angular velocity, because the units are interdependent. In other words, if we fix the linear speed, we need to consider all angular velocities in order to verify the maneuver for each possible radius r of the roundabout maneuver (and corresponding ω). The x position resulting from these symmetry reductions can be determined easily by Pythagoras theorem (i.e., $(2r)^2 = r^2 + x_1^2$ for the triangle enclosed by h, x, c in Fig. 7a):

$$x = (\sqrt{(2r)^2 - r^2}, 0) = (\sqrt{3}r, 0) \;\; . \quad (4)$$

Consequently, we simplify (3) by specializing to the following situation:

$$c := (0,0);\; d := (1,0);\; r := *;\; ?r > 0;\; \omega := 1/r;\; x := (\sqrt{3}r, 0)$$

4.6 Bounded Entry Duration (AC4)

As the first step for showing that the entry procedure finally succeeds at goal (2) and maintains a safe distance all the time, we show that *entry* succeeds in bounded time and cannot take arbitrarily long to succeed (**AC4** in Section 4.3).

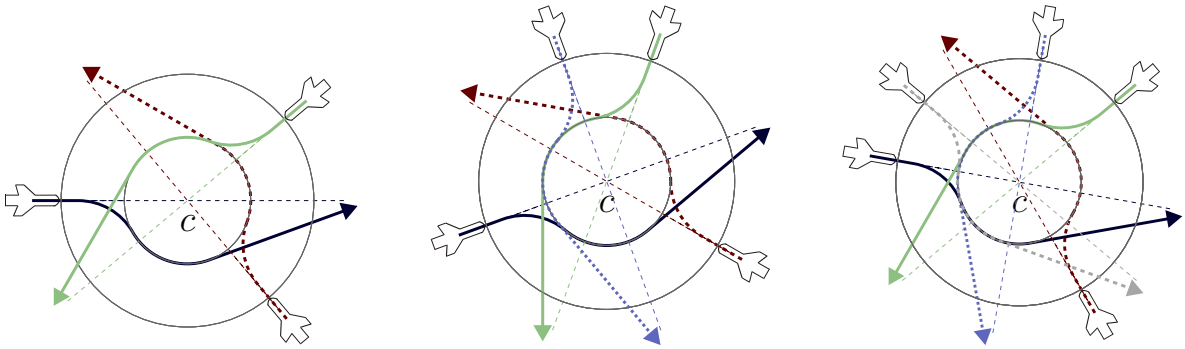


Figure 8: Flyable aircraft roundabout (multiple aircraft)

By a simple consequence of the proof for (3), the entry procedure follows a circular motion around anchor point h, see Fig. 7a. That is, when r is the radius belonging to the angular velocity ω and the linear speed $\|d\|$, the property $\|x - h\| = r$ is an invariant of *entry*; see Appendix A.4. By **AC2**, which can be proven easily, the speed $\|d\|$ is constant during the *entry* procedure. Thus, the aircraft proceeds with nonzero minimum progress rate $\|d\|$ around the circle. The flight duration for a full circle of radius r around h at constant linear speed $\|d\|$ is $\frac{2\pi r}{\|d\|}$, because its arc length is $2\pi r$. From the trigonometric identities underlying equation (4), we can read off that the aircraft completes a $\frac{\pi}{3} = 60°$ arc, see Fig. 7a. Hence, the maximum duration T of the *entry* procedure is:

$$T := \frac{1}{6} \cdot \frac{2\pi r}{\|d\|} = \frac{\pi r}{3\|d\|} \tag{5}$$

Instead of π, which is not definable in first-order real arithmetic, we can use any overapproximation, e.g., 3.1415927 in (5). Roots like $r = \sqrt{3}$, instead, are definable easily via $r^2 = 3 \wedge r \geq 0$.

4.7 Safe Entry Separation (AC5)

In Section 4.5, we have shown that the simplified *entry*$_n$ procedure from NTRM can be replaced by a flyable *entry* maneuver that meets the requirements of approaching tangentially for each aircraft. Unlike in instant turns (*entry*$_n$), we still have to show that the respective flyable entry maneuvers of multiple aircraft do not produce mutually conflicting flight paths, i.e., spatial separation of all aircraft is maintained during the entry maneuvers of multiple aircraft (**AC5**). Fig. 8 illustrates FTRM with multiple aircraft where separation is important.

Bounded Overapproximation We show that entry separation is a consequence of the bounded speed (**AC2**) and bounded duration (**AC4**) of the flyable entry procedure when initiating the negotiation phase *agree* with sufficient distance. We prove that, when following bounded speed for a bounded duration, aircraft only come closer by a bounded distance. Let b denote the overall speed bound during FTRM according to **AC2** and let T be the time bound for the duration of the entry procedure due to **AC4**. We overapproximate the actual behavior during the *entry* phase by arbitrary curved flight (see Fig. 7b). When the *entry* procedure is initiated with sufficient distance $\sqrt{2}(p + 2bT)$, the protected zone $p{\geq}0$ will still be respected after the 2 aircraft follow *any*

curved flight (including the actual choices during the *entry* phase and subsequent *circ* phase) with speed $\|d\| \leq b$ and $\|e\| \leq b$ up to $T \geq 0$ time units (see Fig. 7b):

$$\|x-y\| \geq \sqrt{2}(p+2bT) \wedge p \geq 0 \wedge \|d\|^2 \leq \|e\|^2 \leq b^2 \wedge b \geq 0 \wedge T \geq 0 \\ \rightarrow [\textit{entry}]\,(\|x-y\| \geq p) \quad (6)$$

In Appendix A.5, we show that this property follows from the more general fact that aircraft only make limited progress in bounded time from some initial point z when starting with bounded speeds (even when changing ω arbitrarily):

$$x = z \wedge \|d\|^2 \leq b^2 \wedge b \geq 0 \;\rightarrow\; [\tau := 0;\; \mathcal{F}(\omega) \wedge \tau' = 1]\,(\|x-z\|_\infty \leq \tau b) \quad (7)$$

The maximum distance $\|x-z\|_\infty$ from z depends on clock τ and bound b. To reduce the polynomial degree and the verification complexity, we overapproximate distances from quadratic Euclidean norm $\|\cdot\|$ in terms of linearly definable supremum norm $\|\cdot\|_\infty$, instead, which is

$$\|x\|_\infty \leq c \equiv -c \leq x_1 \leq c \wedge -c \leq x_2 \leq c$$

Far Separation By combining the estimation of the entry duration (5) at speed $\|d\| = b$ with the entry separation property (6), we determine the following magnitude as the *far separation*, i.e., the initial distance which guarantees that the protected zone p is maintained during the full ***FTRM***, including *entry*:

$$f := \sqrt{2}(p+2bT) \overset{(5)}{=} \sqrt{2}\left(p + \frac{2}{3}\pi r\right) \quad (8)$$

5 Synchronization of Roundabout Maneuvers

Following our verification plan in Section 4.3, we show that the various actions of multiple aircraft can be synchronized appropriately to ensure safety of the maneuver. We analyze the negotiation phase and compatible exit procedures.

5.1 Successful Negotiation (AC6)

For negotiation to succeed (**AC6**), we have to show that there is a common choice of the roundabout center c and angular velocity ω (or radius r) so that multiple participating aircraft can satisfy the local requirements of their respective entry procedures simultaneously, i.e., of the property (3) for **AC3**.

We prove that all corresponding choices of *agree* satisfy the mutual requirements of multiple aircraft simultaneously. As one possible option among others: when choosing roundabout center c as the simultaneous intersection (intersection $x + \lambda d = y + \lambda e$ after time λ) of the flight paths of

the aircraft at x and y, the choices for c, r, ω are compatible for multiple aircraft; see Fig. 9a:

$$\begin{aligned}
&\lambda > 0 \wedge x + \lambda d = y + \lambda e \wedge \|d\| = \|e\| \rightarrow \\
&\quad [c := x + \lambda d;\ r := *;\ ?\|x - c\| = \sqrt{3}r;\ ?\|y - c\| = \sqrt{3}r;\ \omega := *;\ ?(r\omega)^2 = \|d\|^2] \\
&\qquad \big(\|x - c\| = \sqrt{3}r \wedge \lambda \geq 0 \wedge x + \lambda d = c \wedge \|y - c\| = \sqrt{3}r \wedge y + \lambda e = c\big) \qquad (9)
\end{aligned}$$

The tests in the dynamics ensure that the *entry* curve starts when x, y and c have appropriate distance $\sqrt{3}r$ identified in Section 4 and that r is the radius belonging to angular velocity ω and linear speed $\|d\|$. This property expresses that, for aircraft heading towards the simultaneous intersection of their flight paths with speed $\|d\| = \|e\|$ (line 1), the intersection of the linear flight paths (line 2) is a safe choice for c satisfying the joint requirements (line 3) identified in Section 4. For an analysis of far separation during negotiation and of the feasibility of these choices, see-Appendix A.6. Other choices of c, ω than Fig. 9a are possible for asymmetric initial positions of aircraft, but computationally more involved.

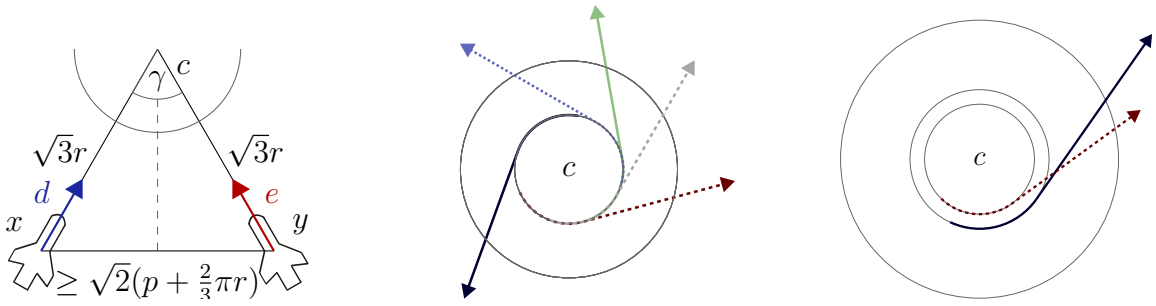
5.2 Safe Exit Separation (AC7)

NTRM (Fig. 1d) does not need an exit procedure for safety, because the maneuver repeats when further air traffic conflicts arise. For FTRM, instead, we need to show that the exit procedure produces safe flight paths until the aircraft are sufficiently separated: When repeating the FTRM maneuver, the *entry* procedure needs far separation (8) not just distance p for safety, see Fig. 4b.

Safe Separation If the aircraft enter simultaneously, they can exit simultaneously. For **AC7**, we first show that aircraft that exit simultaneously (from tangential positions of the roundabout circle) always respect their protected zones:

$$\mathcal{R} \wedge \|x - y\|^2 \geq p^2 \ \rightarrow\ [x' = d \wedge y' = e]\,(\|x - y\|^2 \geq p^2) \qquad (10)$$

This property expresses that safely separated aircraft exiting simultaneously along straight lines from tangential positions ($\mathcal{R}$ by eqn. 2) of a roundabout will always remain safely separated. The



(a) Negotiation separation (b) Exit ray separation (c) Incompatible exit rays

Figure 9: Separation of negotiation and good and bad exit procedure separation

$$
\begin{aligned}
\psi &\equiv \|d\| = \|e\| \wedge r > 0 \wedge \mathcal{S}(f) \rightarrow [\mathit{FTRM}^*]\mathcal{S}(p) \\
\mathcal{C} &\equiv \|x-c\| = \sqrt{3}r \wedge \exists \lambda{\geq}0\, (x + \lambda d = c) \wedge \|y-c\| = \sqrt{3}r \wedge \exists \lambda{\geq}0\, (y + \lambda e = c) \\
\mathit{FTRM} &\equiv \mathit{free}^*;\ \mathit{agree};\ \Pi(\mathit{entry};\ \mathit{circ};\ \mathit{exit}) \\
\mathit{free} &\equiv \omega := *;\ \ \varrho := *;\ \ \mathcal{F}(\omega) \wedge \mathcal{G}(\varrho) \wedge \mathcal{S}(f) \\
\mathit{agree} &\equiv c := *;\ \ r := *;\ ?(\mathcal{C} \wedge r > 0);\ \ ?\mathcal{S}(f); \\
&\qquad \omega := *;\ ?(r\omega)^2 = \|d\|^2;\ \ x_0 := x; d_0 := d; y_0 := y; e_0 := e \\
\mathit{entry} &\equiv \mathit{do}\, \mathcal{F}(-\omega)\ \mathit{until}\ \|x-c\|^2 = r^2 \\
\mathit{circ} &\equiv \mathit{do}\, \mathcal{F}(\omega)\ \mathit{until}\ \exists \lambda{\geq}0\, \exists \mu{>}0\, (x + \lambda d = x_0 + \mu d_0) \\
\mathit{exit} &\equiv \mathcal{F}(0);\ ?\mathcal{S}(f)
\end{aligned}
$$

Figure 10: Flight control with flyable tangential roundabout collision avoidance

proof for (10) uses overapproximations: even the whole exit rays (Fig. 9b–9c) are separated at all times; see Appendix A.7.

Far Separation To show that the aircraft reach arbitrary separation when following the exit procedure long enough, we prove that—due to different exit directions $d \neq e$—the exit procedure will finally separate the aircraft arbitrarily far (starting from tangential configuration (2) of the roundabout):

$$\mathcal{R} \wedge d \neq e \ \rightarrow\ \forall a\, \langle x' = d \wedge y' = e \rangle\, (\|x-y\|^2 > a^2) \tag{11}$$

The proof uses the same ray overapproximations (Fig. 9b–9c), see Appendix A.7.

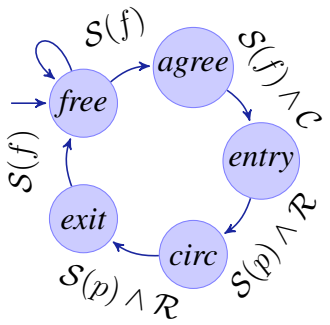
6 Flyable Tangential Roundabout Maneuver

We combine the results about the individual phases of flyable roundabouts into a full model of FTRM that inherits safety modularly. We collect the maneuver phases according to the protocol cycle of Fig. 4 and take care to ensure that the safety prerequisites are met, as identified for the respective phases in Section 4-5.

One possible instance of FTRM is the hybrid program in Fig. 10, which is composed of previously illustrated parts of the maneuver. The technical construction and protocol cycle of the entry procedure have already been illustrated in Fig. 4.

Finally, in FTRM, Π denotes the synchronous parallel product. Using communication, FTRM operates synchronously, i.e., all aircraft make simultaneous mode changes like in [10]. Consequently, the parallel product $\Pi(\mathit{entry}; \mathit{circ}; \mathit{exit})$ of HP simplifies to the conjunction of the respective differential equations in the various modes and can be defined easily as follows (likewise for more aircraft):

$$(\mathit{entry}_x \wedge \mathit{entry}_y)\ ;\ (\mathit{circ}_x \wedge \mathit{circ}_y)\ ;\ (\mathit{exit}_x \wedge \mathit{exit}_y)$$



Decomposed property of system dynamics		See
$\mathcal{S}(f) \rightarrow$	$[\mathit{free}]\,\mathcal{S}(f)$	Fig. 5
$\mathcal{S}(f) \rightarrow$	$[\mathit{agree}](\mathcal{S}(f) \wedge \mathcal{C})$	(9), (19)
$\mathcal{C} \wedge \mathcal{S}(f) \rightarrow$	$[\mathit{entry}]\,\mathcal{S}(p)$	(6)
$\mathcal{C} \wedge \mathcal{S}(f) \rightarrow$	$[\mathit{entry}]\,\mathcal{R}$	(3)
$\mathcal{R} \wedge \mathcal{S}(p) \rightarrow$	$[\mathit{circ}](\mathcal{S}(p) \wedge \mathcal{R})$	Fig. 5
$\mathcal{R} \wedge \mathcal{S}(p) \rightarrow$	$[\mathit{exit}]\,\mathcal{S}(p)$	(10)
$\mathcal{R} \wedge \mathcal{S}(p) \rightarrow$	$[\mathit{exit}]\,\mathcal{S}(f)$	(10), (11)

Figure 11: Composing verification for flyable tangential roundabout maneuvers

where entry_x is the entry procedure of the aircraft at position x, etc. Further Fig. 14 instantiates Fig. 10 with all abbreviations resolved.

To verify this maneuver, we split the proof into the modular properties that we have already shown previously following the verification plan from Section 4.3. Formally, we split the system at its sequential compositions, giving the subproperties depicted in Fig. 11. Formula $\mathcal{R}$ is due to equation (2) and $\mathcal{S}(p)$ by (1).

By combining the results about the FTRM flight phases as summarized in Fig. 11, we conclude that FTRM avoids collisions safely. The modular proof structure in Fig. 11 still holds when replacing any part of the maneuver with a different choice that still satisfies the specification, e.g., for different entry procedures that still succeed in tangential configuration $\mathcal{R}$ within bounded time. This includes roundabouts with *asymmetric positions*, i.e., where the initial distance to c can be different, and with *near conflicts*, where the flight paths do not intersect in one point but in a larger critical region [10]. Most notably, the separation proof in Section 4.7 is by overapproximation and tolerates asymmetric distances to c (Fig. 7b).

Theorem 1 (Safety of flyable tangential roundabout maneuvers) *FTRM is collision free, i.e., the collision avoidance property ψ in Fig. 10 is valid. Even any variation of FTRM with a modified entry procedure that safely reaches tangential configuration $\mathcal{R}$ in some bounded time T is safe, i.e., when the following formula holds, saying that, until time T, the aircraft have safe distance p and will have reached configuration $\mathcal{R}$ at time T with τ as a clock:*

$$\mathcal{S}(f) \;\rightarrow\; [\tau := 0;\, \mathit{agree} \wedge \tau' = 1]\big((\tau \leq T \rightarrow \mathcal{S}(p)) \wedge (\tau = T \rightarrow \mathcal{R})\big) \;.$$

7 Experimental Results

Table 2 summarizes experimental results obtained using the tool KeYmaera[1] for our verification algorithm [20, 22] on a 2.6GHz AMD Opteron with 4GB memory. Rows marked with $*$ indicate a property where simplifications like symmetry reduction have been used to reduce the computational complexity. Table 2 shows that even aircraft maneuvers with challenging hybrid curve

[1]KeYmaera verification tool is available at `http://symbolaris.com/info/KeYmaera.html` experiments are available at `http://symbolaris.com/pub/RCAS-examples.zip`

Table 2: Experimental results for air traffic control

Case study	See	Time(s)	Memory(MB)	Steps	Dimension
tangential roundabout	2 aircraft	10.4	6.8	197	13
tangential roundabout	3 aircraft	253.6	7.2	342	18
tangential roundabout	4 aircraft	382.9	10.2	520	23
tangential roundabout	5 aircraft	1882.9	39.1	735	28
bounded maneuver speed	**AC2**	0.5	6.3	14	4
flyable roundabout entry*	(3)	10.1	9.6	132	8
flyable entry feasible*	(14)	104.5	87.9	16	10
flyable entry circular	(15)	3.2	7.6	81	5
limited entry progress	(7)	1.9	6.5	60	8
entry separation	(16)	140.1	20.1	512	16
mutual negotiation successful	(9)	0.8	6.4	60	12
mutual negotiation feasible*	(17)	7.5	23.8	21	11
mutual far negotiation	(19)	2.4	8.1	67	14
simultaneous exit separation*	(21)	4.3	12.9	44	9
different exit directions	(23)	3.1	11.1	42	11

dynamics can be verified formally. Memory consumption of quantifier elimination is shown in Table 2, excluding the front-end. The dimension of the continuous state space and number of automatic proof steps are indicated. Except for simple manual steps during one property (16), the proofs for Table 2 are 100% automatic.

8 Summary

We have analyzed complex air traffic control applications. Real aircraft can only follow sufficiently smooth flyable curves. Hence, mathematical maneuvers that require instant turns give physically impossible conflict resolution advice. We have developed a new collision avoidance maneuver with smooth, fully flyable curves. Despite its complicated dynamics and maneuvering, we have verified collision avoidance in this flyable tangential roundabout maneuver formally using our verification algorithm for a logic of hybrid systems. Due to the intricate spatio-temporal movement of aircraft in roundabout maneuvers, some of the properties require intricate arithmetic, which we handled by symmetry reduction and degree-based reductions. The proof is automatic except for modularization and arithmetical simplifications to overcome the computational complexity.

While the flyable roundabout maneuver is a highly nontrivial and challenging study, we still use modeling assumptions that should be generalized and relaxed in future work, including synchronous conflict resolution. The proof structure behind Theorem 1 is already sufficiently general, but the computational complexity high. It would be interesting future work to see if the informal robustness studies of Hwang et al. [10] can be carried over to a formal verification result.

References

[1] Alberto Bemporad, Antonio Bicchi, and Giorgio Buttazzo, editors. *Hybrid Systems: Computation and Control, 10th International Conference, HSCC 2007, Pisa, Italy, Proceedings*, volume 4416 of *LNCS*. Springer, 2007.

[2] A. Bicchi and L. Pallottino. On optimal cooperative conflict resolution for air traffic management systems. *IEEE Trans. Intelligent Transportation Systems*, 1(4):221–231, December 2000.

[3] Bundesstelle für Flugunfalluntersuchung. Investigation, May 2004. AX001-1-2/02.

[4] Werner Damm, Guilherme Pinto, and Stefan Ratschan. Guaranteed termination in the verification of LTL properties of non-linear robust discrete time hybrid systems. In Doron Peled and Yih-Kuen Tsay, editors, *ATVA*, volume 3707 of *LNCS*, pages 99–113. Springer, 2005.

[5] Gilles Dowek, César Muñoz, and Víctor A. Carreño. Provably safe coordinated strategy for distributed conflict resolution. In *AIAA-2005-6047*, 2005.

[6] André L. Galdino, César Muñoz, and Mauricio Ayala-Rincón. Formal verification of an optimal air traffic conflict resolution and recovery algorithm. In Daniel Leivant and Ruy de Queiroz, editors, *WoLLIC*, volume 4576 of *LNCS*, pages 177–188. Springer, 2007.

[7] Thomas A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292. IEEE, 1996.

[8] Jianghai Hu, Maria Prandini, and Shankar Sastry. Optimal coordinated motions of multiple agents moving on a plane. *SIAM Journal on Control and Optimization*, 42:637–668, 2003.

[9] Jianghai Hu, Maria Prandini, and Shankar Sastry. Probabilistic safety analysis in three-dimensional aircraft flight. In *CDC*, volume 5, pages 5335 – 5340, 2003.

[10] Inseok Hwang, Jegyom Kim, and Claire Tomlin. Protocol-based conflict resolution for air traffic control. *Air Traffic Control Quarterly*, 15(1):1–34, 2007.

[11] J. Košecká, Claire Tomlin, George Pappas, and Shankar Sastry. 2-1/2D conflict resolution maneuvers for ATMS. In *CDC*, volume 3, pages 2650–2655, Tampa, FL, USA, 1998.

[12] Gerardo Lafferriere, George J. Pappas, and Sergio Yovine. A new class of decidable hybrid systems. In Frits W. Vaandrager and Jan H. van Schuppen, editors, *HSCC*, volume 1569 of *LNCS*, pages 137–151. Springer, 1999.

[13] Carolos Livadas, John Lygeros, and Nancy A. Lynch. High-level modeling and analysis of TCAS. *Proc. IEEE - Special Issue on Hybrid Systems*, 88(7):926–947, 2000.

[14] Mieke Massink and Nicoletta De Francesco. Modelling free flight with collision avoidance. In Sten F. Andler and Jeff Offutt, editors, *ICECCS*, pages 270–280, Los Alamitos, 2001. IEEE.

[15] César Muñoz, Victor Carreño, Gilles Dowek, and Ricky W. Butler. Formal verification of conflict detection algorithms. *STTT*, 4(3):371–380, 2003.

[16] L. Pallottino, V. G. Scordio, E. Frazzoli, and A. Bicchi. Decentralized cooperative policy for conflict resolution in multi-vehicle systems. *IEEE Trans. on Robotics*, 23(6):1170–1183, 2007.

[17] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 2008. To appear.

[18] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reasoning*, 41(2):143–189, 2008.

[19] André Platzer and Edmund M. Clarke. The image computation problem in hybrid systems model checking. In Bemporad et al. [1], pages 473–486.

[20] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

[21] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. Technical Report CMU-CS-08-103, Carnegie Mellon University, 2008.

[22] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. *Form. Methods Syst. Des.*, 35(1):98–120, 2009.

[23] Claire Tomlin, George J. Pappas, and Shankar Sastry. Conflict resolution for air traffic management. *IEEE T. Automat. Contr.*, 43(4):509–521, 1998.

[24] Shinya Umeno and Nancy A. Lynch. Proving safety properties of an aircraft landing protocol using I/O automata and the PVS theorem prover. In Jayadev Misra, Tobias Nipkow, and Emil Sekerinski, editors, *FM*, volume 4085 of *LNCS*, pages 64–80. Springer, 2006.

[25] Shinya Umeno and Nancy A. Lynch. Safety verification of an aircraft landing protocol: A refinement approach. In Bemporad et al. [1], pages 557–572.

A Additional Verification Results for the Flyable Tangential Roundabout Maneuver

In this appendix, we provide additional background and verification results for aircraft.

A.1 Transcendental Functions Make Flight Dynamics Difficult

Solutions of flight equations contain complicated transcendental functions that give undecidable arithmetic. Consider, for instance, the differential equation system for relative positions $x = (x_1, x_2)$ of two aircraft with linear speed v_1 and and v_2 respectively, and angular velocity ω and ϱ, respectively; see [23] for details:

$$x_1' = -v_1 + v_2\cos\vartheta + \omega x_2 \qquad x_2' = v_2\sin\vartheta - \omega x_1 \qquad \vartheta' = \varrho - \omega \tag{12}$$

Differential equation solving in Mathematica produces the solution depicted in Fig. 12. The "solution" (if it is one at all) in Fig. 12 is not suitable for verification purposes. It involves several trigonometric functions and has an undefined singularity at $\omega = 0$. Reachability verification is not possible for trigonometric solutions like in Fig. 12, because the resulting formulas of the form $\forall t{\geq}0\, G(x_1(t), x_2(t), \vartheta(t))$ involve quantified arithmetic over trigonometric functions, which is undecidable.

$$\begin{aligned}
x_1(t) = \frac{1}{\varrho\omega}\big(&x_1\varrho\omega\cos(t\omega) - \omega\sin(\vartheta)v_2\cos(t\omega) + \omega\cos(t\varrho)\sin(\vartheta)v_2\cos(t\omega)\\
&+ \omega\cos(\vartheta)\sin(t\varrho)v_2\cos(t\omega) + x_2\varrho\omega\sin(t\omega) - \varrho\sin(t\omega)v_1\\
&- \omega\cos(\vartheta)\cos(t\varrho)\sin(t\omega)v_2 + \omega\sin(\vartheta)\sin(t\varrho)\sin(t\omega)v_2\\
&- \omega\sqrt{1-\sin(\vartheta)^2}\sin(t\omega)v_2\big)\\
x_2(t) = \frac{1}{\varrho\omega}\big(&\varrho v_1\cos(t\omega)^2 + x_2\varrho\omega\cos(t\omega) - \varrho v_1\cos(t\omega) - \omega\cos(\vartheta)\cos(t\varrho)v_2\cos(t\omega)\\
&+ \omega\sin(\vartheta)\sin(t\varrho)v_2\cos(t\omega) - \omega\sqrt{1-\sin(\vartheta)^2}v_2\cos(t\omega) - x_1\varrho\omega\sin(t\omega)\\
&+ \varrho\sin(t\omega)^2v_1 + \omega\sin(\vartheta)\sin(t\omega)v_2\\
&- \omega\cos(t\varrho)\sin(\vartheta)\sin(t\omega)v_2 - \omega\cos(\vartheta)\sin(t\varrho)\sin(t\omega)v_2\big)\\
\vartheta(t) = \vartheta + t(&\varrho - \omega)
\end{aligned}$$

Figure 12: Formal but useless "solution" of flight equations produced by Mathematica

The flight equations $\mathcal{F}(\omega)$ and $\mathcal{G}(\varrho)$ given in Section 4.1 can be derived from equation (12). These equations $\mathcal{F}(\omega)$ and $\mathcal{G}(\varrho)$ still have just as complicated trigonometric solutions, but the differential equations themselves are polynomials in the state variables, which is crucial for differential invariants [17, 22].

The derivation works as follows. The parameters of two aircraft at the respective (planar) positions $x = (x_1, x_2) \in \mathbb{R}^2$ and $y = (y_1, y_2)$ with angular orientation ϑ and ς are as in Fig. 3 (with $\vartheta = 0$). Following [23], aircraft dynamics is determined by their linear speeds $v, u \in \mathbb{R}$ and angular speeds $\omega, \varrho \in \mathbb{R}$, respectively:

$$x_1' = v\cos\vartheta \quad x_2' = v\sin\vartheta \quad \vartheta' = \omega \quad y_1' = u\cos\varsigma \quad y_2' = u\sin\varsigma \quad \varsigma' = \varrho \tag{13}$$

That is, position x moves with speed v into the direction with angular orientation ϑ, which rotates with angular velocity ω (likewise for y, u, ς, ϱ). To handle the transcendental functions in equation (13), we axiomatize $\sin$ and $\cos$ by differential equations and reparametrize the system using linear velocity vectors

$$d = (d_1, d_2) := (v\cos\vartheta, v\sin\vartheta) \in \mathbb{R}^2 \text{ and } e = (e_1, e_2) := (u\cos\varsigma, u\sin\varsigma) \in \mathbb{R}^2$$

which describe both the linear speed $\|d\| := \sqrt{d_1^2 + d_2^2} = v$ and the orientation of the aircraft in space, see vectors d and e in Fig. 3:

$$\begin{array}{llll} [x_1' = d_1 & x_2' = d_2 & d_1' = -\omega d_2 & d_2' = \omega d_1] \\ [y_1' = e_1 & y_2' = e_2 & e_1' = -\varrho e_2 & e_2' = \varrho e_1\,] \end{array}$$

Using vectorial notation, these polynomial differential equations are the same as the earlier differential equations $\mathcal{F}(\omega)$ and $\mathcal{G}(\varrho)$, respectively. They can be verified using our verification algorithm on the basis of differential invariants [22].

A.2 Non-Flyable Tangential Roundabout Maneuver for Multiple Aircraft (AC1)

Concerning multiple aircraft, Fig. 13 contains the system and separation property specification for the 5-aircraft NTRM. There, property ψ expresses that the 5 aircraft at positions $x, y, z, u, v \in \mathbb{R}^2$, respectively, keep mutual distance $\geq p$.

A.3 Flyable Entry Procedure Proofs (AC3)

For **AC3**, we further prove that the anchor point h can always be chosen as illustrated in Fig. 7a. That is we show feasibility of the assumptions of property (3) by the following existence property:

$$\begin{array}{r} (r\omega)^2 = \|d\|^2 \wedge \|x-c\| = \sqrt{3}r \wedge \exists\lambda{\geq}0\,(x + \lambda d = c) \\ \rightarrow \exists h\,(d = -\omega(x-h)^\perp \wedge \|h-c\| = 2r) \end{array} \tag{14}$$

A.4 Bounded Entry Duration Proof for Circular Flight (AC4)

For **AC4**, we prove constant distance to anchor point h, i.e., that, indeed, $\|x-h\| = r$ is an invariant of *entry* as conjectured in Section 4.6:

$$\begin{array}{r} (r\omega)^2 = \|d\|^2 \wedge \|x-c\| = \sqrt{3}r \wedge \exists\lambda{\geq}0\,(x+\lambda d = c) \wedge d = -\omega(x-h)^\perp \wedge \|h-c\| = 2r \\ \rightarrow\ [\mathcal{F}(-\omega) \wedge \|x-c\| \geq r]\,\big(\|x-h\| = r\big) \end{array} \tag{15}$$

$$
\begin{aligned}
\psi &\equiv \mathcal{S}(p) \rightarrow [\mathit{NTRM}^*]\,\mathcal{S}(p)\\
\mathcal{S}(p) &\equiv (x_1-y_1)^2+(x_2-y_2)^2 \geq p^2 \wedge (y_1-z_1)^2+(y_2-z_2)^2 \geq p^2\\
&\quad \wedge (x_1-z_1)^2+(x_2-z_2)^2 \geq p^2 \wedge (x_1-u_1)^2+(x_2-u_2)^2 \geq p^2\\
&\quad \wedge (y_1-u_1)^2+(y_2-u_2)^2 \geq p^2 \wedge (z_1-u_1)^2+(z_2-u_2)^2 \geq p^2\\
&\quad \wedge (x_1-v_1)^2+(x_2-v_2)^2 \geq p^2 \wedge (y_1-v_1)^2+(y_2-v_2)^2 \geq p^2\\
&\quad \wedge (z_1-v_1)^2+(z_2-v_2)^2 \geq p^2 \wedge (u_1-v_1)^2+(u_2-v_2)^2 \geq p^2\\
\mathit{NTRM} &\equiv \mathit{free};\ \mathit{agree};\ \mathit{entry}_n;\ \mathit{circ}\\
\mathit{circ} &\equiv x_1'=d_1 \wedge x_2'=d_2 \wedge d_1'=-\omega_x d_2 \wedge d_2'=\omega_x d_1\\
&\quad \wedge y_1'=e_1 \wedge y_2'=e_2 \wedge e_1'=-\omega_y e_2 \wedge e_2'=\omega_y e_1\\
&\quad \wedge z_1'=f_1 \wedge z_2'=f_2 \wedge f_1'=-\omega_z f_2 \wedge f_2'=\omega_z f_1\\
&\quad \wedge u_1'=g_1 \wedge u_2'=g_2 \wedge g_1'=-\omega_u g_2 \wedge g_2'=\omega_u g_1\\
&\quad \wedge v_1'=h_1 \wedge v_2'=h_2 \wedge h_1'=-\omega_v h_2 \wedge h_2'=\omega_v h_1\\
\mathit{free} &\equiv (\omega_x := *;\ \omega_y := *;\ \omega_z := *;\ \omega_u := *;\ \omega_v := *;\\
&\quad x_1'=d_1 \wedge x_2'=d_2 \wedge d_1'=-\omega_x d_2 \wedge d_2'=\omega_x d_1\\
&\quad \wedge y_1'=e_1 \wedge y_2'=e_2 \wedge e_1'=-\omega_y e_2 \wedge e_2'=\omega_y e_1\\
&\quad \wedge z_1'=f_1 \wedge z_2'=f_2 \wedge f_1'=-\omega_z f_2 \wedge f_2'=\omega_z f_1\\
&\quad \wedge u_1'=g_1 \wedge u_2'=g_2 \wedge g_1'=-\omega_u g_2 \wedge g_2'=\omega_u g_1\\
&\quad \wedge v_1'=h_1 \wedge v_2'=h_2 \wedge h_1'=-\omega_v h_2 \wedge h_2'=\omega_v h_1 \wedge \mathcal{S}(p))^*\\
\mathit{agree} &\equiv \omega := *;\ c := *\\
\mathit{entry}_n &\equiv d_1 := -\omega(x_2-c_2);\ d_2 := \omega(x_1-c_1);\\
&\quad e_1 := -\omega(y_1-c_1);\ e_2 := \omega(y_2-c_2);\\
&\quad f_1 := -\omega(z_1-c_1);\ f_2 := \omega(z_2-c_2);\\
&\quad g_1 := -\omega(u_1-c_1);\ g_2 := \omega(u_2-c_2);\\
&\quad h_1 := -\omega(v_1-c_1);\ h_2 := \omega(v_2-c_2)
\end{aligned}
$$

Figure 13: Tangential roundabout collision avoidance maneuver (5 aircraft)

A.5 Safe Entry Separation Proof (AC5)

Cartesian Degree Reduction To simplify separation property (6), we use the (linearly definable) supremum norm $\|\cdot\|_\infty$ in place of the (quadratically definable) Euclidean 2-norm $\|\cdot\|_2$, thereby yielding the following provable variant of (6):

$$\|x-y\|_\infty \geq (p+2bT) \wedge p \geq 0 \wedge \|d\|^2 \leq \|e\|^2 \leq b^2 \wedge b \geq 0 \wedge T \geq 0 \\ \rightarrow [\tau := 0; \exists\omega\, \mathcal{F}(\omega) \wedge \exists\varrho\, \mathcal{G}(\varrho) \wedge \tau' = 1 \wedge \tau \leq T](\|x-y\|_\infty \geq p) \quad (16)$$

Here, the angular velocity ω is allowed to change arbitrarily and nondeterministically during the flight, which we indicate by the quantifier $\exists\omega$ in the continuous dynamics.Using standard equivalences of norms, we conclude that the following variant of (16) with Euclidean 2-norms is valid:

$$\|x-y\|_2 \geq \sqrt{2}(p+2bT) \wedge p \geq 0 \wedge \|d\|^2 \leq \|e\|^2 \leq b^2 \wedge b \geq 0 \wedge T \geq 0 \\ \rightarrow [\tau := 0; \exists\omega\, \mathcal{F}(\omega) \wedge \exists\varrho\, \mathcal{G}(\varrho) \wedge \tau' = 1 \wedge \tau \leq T](\|x-y\|_2 \geq p)$$

The extra factor of $\sqrt{2}$ in the separation requirement results from the relaxation of the 2-norm to the ∞-norm. Using **AC4**, it is easy to see that the entry maneuver is a special case refining the above nondeterministic curved flight dynamics. Thus we conclude that property (6) is valid.

A.6 Far Separation during Successful Negotiation (AC6)

Feasible Negotiation Choices We show that the choices for property (9) are feasible for simultaneous flight path intersections, i.e., there always is a mutually agreeable choice:

$$\|d\| = \|e\| \wedge \lambda > 0 \wedge x + \lambda d = y + \lambda e \rightarrow \\ \langle c := x + \lambda d;\ r := *;\ ?\|x-c\| = \sqrt{3}r;\ ?\|y-c\| = \sqrt{3}r;\ \omega := *;\ ?(r\omega)^2 = \|d\|^2\rangle \\ \big(\|x-c\| = \sqrt{3}r \wedge \lambda \geq 0 \wedge x + \lambda d = c \wedge \|y-c\| = \sqrt{3}r \wedge \lambda \geq 0 \wedge y + \lambda e = c\big) \quad (17)$$

The essential difference to (9) is the use of a diamond modality, which expresses existence of a corresponding transition that satisfies all the constraints of the dynamics.

Separation During Negotiation The *entry* procedure has to be initiated while the aircraft are still sufficiently far apart for safety reasons. Otherwise, there may not be sufficient maneuvering space for collision avoidance. Correspondingly, the *agree* procedure will negotiate a roundabout choice while the aircraft have far distance. Thus, the *agree* procedure will have to maintain far separation, i.e., satisfy the property

$$\|x-y\| \geq \sqrt{2}(p + \frac{2}{3}\pi r) \ \rightarrow\ [\mathit{agree}]\left(\|x-y\| \geq \sqrt{2}(p + \frac{2}{3}\pi r)\right) \quad (18)$$

This may seem like a trivial property, because *agree* models the successful completion of the negotiation, so that no time elapses during the dynamics of *agree*, hence the positions x and y

do not even change. Observe, however, that the far separation distance according to equation (8) depends on the protected zone p and the radius r of evasive actions. Unlike p, radius r may change during *agree*, which allows for the flexibility of changing the flight radius r adaptively when repeating the roundabout maneuver loop at different positions. Consequently, the far separation distance $\sqrt{2}(p + \frac{2}{3}\pi r)$ is affected when changing r.

To ensure that the new radius r is chosen such that far separation is still maintained, i.e., property (18) is respected, we add a corresponding constraint to *agree*. Thus, changes of r are only accepted as long as they do not compromise far separation. We show that, when adding a corresponding constraint to property (9), all choices by *agree* maintain far separation of the aircraft at x and y according to (8):

$$\begin{aligned}
&\|d\| = \|e\| \land \lambda > 0 \land x + \lambda d = y + \lambda e \rightarrow \\
&\quad [c := x + \lambda d;\ r := *;\ ?\|x - c\| = \sqrt{3}r;\ ?\|y - c\| = \sqrt{3}r;\ ?\|x - y\| \geq \sqrt{2}(p + \frac{2}{3}\pi r); \\
&\qquad\qquad \omega := *;\ ?(r\omega)^2 = \|d\|^2] \\
&\quad \big(\|x - c\| = \sqrt{3}r \land \lambda \geq 0 \land x + \lambda d = c \land \|y - c\| = \sqrt{3}r \land \lambda \geq 0 \land y + \lambda e = c \\
&\qquad\qquad \land \|x - y\| \geq \sqrt{2}(p + \frac{2}{3}\pi r)\big) \quad (19)
\end{aligned}$$

Finally, we analyze when such choices of *agree* are feasible using a diamond modality:

$$\begin{aligned}
&\|d\| = \|e\| \land \lambda > 0 \land x + \lambda d = y + \lambda e \rightarrow \\
&\qquad \langle c := x + \lambda d;\ r := *;\ ?\|x - c\| = \|y - c\| = \sqrt{3}r\rangle \|x - y\| \geq \sqrt{2}(p + \frac{2}{3}\pi r) \quad (20)
\end{aligned}$$

The corresponding distance constraints on x, y and c for *agree*, respectively, are depicted in Fig. 9a. Using standard trigonometric relations for each half of the triangle, we can compute the resulting distance of x and y as $\|x - y\| = 2\sqrt{3}r \sin\frac{\gamma}{2}$. With Collins-Tarski quantifier elimination and simple evaluation for the remaining trigonometric expressions, we can determine under which circumstances property (20) holds true, i.e., for all protected zones p there is a radius r satisfying the distance requirements:

$$\left(\forall p\, \exists r{\geq}0\ \left(2\sqrt{3}r \sin\frac{\gamma}{2} \geq \sqrt{2}(p + \frac{2}{3}\pi r)\right)\right) \equiv \sin\frac{\gamma}{2} > \frac{1}{3}\sqrt{\frac{2}{3}}\pi \equiv\ \gamma > 117.527^\circ$$

Consequently, corresponding choices are feasible for all protected zones with flight paths that do not intersect with narrow collision angles. The constraint on the flight path intersection angle relaxes to $\gamma > 74.4^\circ$ when removing the extra factor of $\sqrt{2}$ from (8), which results from our computational simplification of cartesian degree reduction in Section 4.7.

Despite the presence of trigonometric expressions, the above formula is a substitution instance of first-order real arithmetic and can thus be handled by our quantifier elimination lifting [18]. Note that the primary difference to trigonometric expressions occurring in the solutions of flight equations for curved flight—which do not support quantifier elimination—is that the argument $\frac{\gamma}{2}$ of $\sin$ is not quantified over, here.

A.7 Safe Exit Separation Proof (AC7)

Safe Separation To reduce the arithmetical complexity, we overapproximate property (10) by showing that even the whole exit rays never cross when the aircraft exit the same roundabout tangentially (see Fig. 9b; the counterexample in Fig. 9c shows that the assumption $\|x-c\|^2 = \|y-c\|^2$ on identical radius is required for this relaxation):

$$\mathcal{R} \wedge \|x-c\|^2 = \|y-c\|^2 \wedge x \neq y \rightarrow [x' = d; y' = e]x \neq y \tag{21}$$

Property (10) clearly refines (21), because every synchronous evolution along the joint differential equation system $x' = d \wedge y' = e$ can be emulated by successive evolutions $x' = d; y' = e$ with two consecutive evolutions of identical duration.

Again the computational complexity of proving this property can be simplified by adding $c_1 := 0 \wedge c_2 := 0$ by symmetry reduction. From this property, the original separation property (10) follows using the geometric fact that, for linearity reasons, rays that never cross cannot come closer than the original distance p. This can be expressed elegantly in $\mathsf{d}\mathcal{L}$:

$$\|x-y\|^2 \geq p^2 \wedge [x' = d \wedge y' = e]x \neq y \rightarrow [x' = d \wedge y' = e](\|x-y\|^2 \geq p^2) \tag{22}$$

Thus, by combining (21) with (22) propositionally (modus ponens) and by the simple fact that the sequential independent ray evolution $x' = d;\ y' = e$ is an overapproximation of the synchronous evolution $x' = d \wedge y' = e$, we conclude that property (10) is valid.

Far Separation To show that the aircraft reach arbitrary separation when following the exit procedure long enough, we prove that aircraft which enter roundabouts in different directions always remain in different directions while following the roundabout:

$$\mathcal{R} \wedge d \neq e \ \rightarrow\ [\mathcal{F}(\omega) \wedge \mathcal{G}(\omega)]\|d-e\|^2 > 0 \tag{23}$$

We combine (23) with the geometric fact that rays into different directions which never cross will be arbitrarily far apart after sufficient time (Fig. 9b):

$$d \neq e \wedge [x' = d \wedge y' = e]x \neq y \ \rightarrow\ \forall a\, \langle x' = d \wedge y' = e\rangle(\|x-y\|^2 > a^2)$$

By combining this geometric fact with (23), we obtain the final separation property by standard propositional reasoning. It says that—due to their different directions—the exit procedure will finally separate the aircraft arbitrarily far. This proves property (11).

$$
\begin{aligned}
\psi \;\equiv\; & d_1^2 + d_2^2 = e_1^2 + e_2^2 \wedge r > 0 \wedge (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq 2\left(p + \frac{2}{3}\pi r\right)^2 \\
& \rightarrow [\mathit{FTRM}^*]\,(x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2 \\
\mathit{FTRM} \;\equiv\; & \Bigg(\Big(\omega := *;\, \varrho := *; \\
\mathit{free}\colon\; & x_1' = d_1 \wedge x_2' = d_2 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1 \\
& \wedge\, y_1' = e_1 \wedge y_2' = e_2 \wedge e_1' = -\varrho e_2 \wedge e_2' = \varrho e_1 \\
& \wedge\, (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq 2\left(p + \frac{2}{3}\pi r\right)^2 \Big)^*; \\
\mathit{agree}\colon\; & c := *;\; r := *;\; ?r > 0;\; ?(x_1 - c_1)^2 + (x_2 - c_2)^2 = 3r^2; \\
& ?\exists \lambda{\geq}0\,(x_1 + \lambda d_1 = c_1 \wedge x_2 + \lambda d_2 = c_2); \\
& ?(y_1 - c_1)^2 + (y_2 - c_2)^2 = 3r^2; \\
& ?\exists \lambda{\geq}0\,(y_1 + \lambda e_1 = c_1 \wedge y_2 + \lambda e_2 = c_2); \\
& ?(x_1 - y_1)^2 + (x_2 - y_2)^2 \geq 2\left(p + \frac{2}{3}\pi r\right)^2; \\
& \omega := *;\; ?(r\omega)^2 = d_1^2 + d_2^2 \\
& x_1^0 := x_1;\; x_2^0 := x_2;\; d_1^0 := d_1;\; d_2^0 := d_2; \\
& y_1^0 := y_1;\; y_2^0 := y_2;\; e_1^0 := e_1;\; e_2^0 := e_2; \\
\mathit{entry}_x \wedge \mathit{entry}_y\colon\; & x_1' = d_1 \wedge x_2' = d_2 \wedge d_1' = -(-\omega) d_2 \wedge d_2' = -\omega d_1 \\
& \wedge\, y_1' = e_1 \wedge y_2' = e_2 \wedge e_1' = -(-\omega) e_2 \wedge e_2' = -\omega e_1; \\
& ?(x_1 - c_1)^2 + (x_2 - c_2)^2 = r^2; \\
\mathit{circ}_x \wedge \mathit{circ}_y\colon\; & x_1' = d_1 \wedge x_2' = d_2 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1 \\
& \wedge\, y_1' = e_1 \wedge y_2' = e_2 \wedge e_1' = -\omega e_2 \wedge e_2' = \omega e_1 \\
& \wedge\, (\neg\big(\exists \lambda{\geq}0\, \exists \mu{>}0\,(x_1 + \lambda d_1 = x_1^0 + \mu d_1^0 \wedge x_2 + \lambda d_2 = x_2^0 + \mu d_2^0) \\
& \quad \wedge\, \exists \lambda{\geq}0\, \exists \mu{>}0\,(y_1 + \lambda e_1 = y_1^0 + \mu e_1^0 \wedge y_2 + \lambda e_2 = y_2^0 + \mu e_2^0)\big) \\
& \vee\, \partial\big(\exists \lambda{\geq}0\, \exists \mu{>}0\,(x_1 + \lambda d_1 = x_1^0 + \mu d_1^0 \wedge x_2 + \lambda d_2 = x_2^0 + \mu d_2^0) \\
& \quad \wedge\, \exists \lambda{\geq}0\, \exists \mu{>}0\,(y_1 + \lambda e_1 = y_1^0 + \mu e_1^0 \wedge y_2 + \lambda e_2 = y_2^0 + \mu e_2^0)\big)\big); \\
& ?\big(\exists \lambda{\geq}0\, \exists \mu{>}0\,(x_1 + \lambda d_1 = x_1^0 + \mu d_1^0 \wedge x_2 + \lambda d_2 = x_2^0 + \mu d_2^0) \\
& \quad \wedge\, \exists \lambda{\geq}0\, \exists \mu{>}0\,(y_1 + \lambda e_1 = y_1^0 + \mu e_1^0 \wedge y_2 + \lambda e_2 = y_2^0 + \mu e_2^0)\big); \\
\mathit{exit}_x \wedge \mathit{exit}_y\colon\; & x_1' = d_1 \wedge x_2' = d_2 \wedge y_1' = e_1 \wedge y_2' = e_2; \\
& ?(x_1 - y_1)^2 + (x_2 - y_2)^2 \geq 2\left(p + \frac{2}{3}\pi r\right)^2 \Bigg)
\end{aligned}
$$

Figure 14: Flight control with FTRM (synchronous instantiation)

B Semantics of Differential Dynamic Logic

The semantics of $\mathsf{d}\mathcal{L}$ [18] is a Kripke semantics in which states of the Kripke model are states of the hybrid system. A state is a map $\nu : V \to \mathbb{R}$; the set of all states is denoted by Sta. We write $\nu \models \phi$ if formula ϕ is true at state ν (Def. 2). Likewise, $[\![\theta]\!]_\nu$ denotes the real *value of term* θ at state ν. The semantics of HP α is captured by the state transitions that are possible by running α. For continuous evolutions, the transition relation holds for pairs of states that can be interconnected by a continuous flow respecting the differential equation and invariant region. That is, there is a continuous transition along $x' = \theta \wedge \chi$ from state ν to state w, if there is a solution of the differential equation $x' = \theta$ that starts in state ν and ends in w and that always remains within the region χ during its evolution. As in [7], we assume non-zeno behavior, for simplicity.

Definition 1 (Transition system of hybrid programs) *The* transition relation, $\rho(\alpha)$, of a hybrid program α*, specifies which state* w *is reachable from a state* ν *by operations of* α *and is defined as follows*

1. $(\nu, w) \in \rho(x := \theta)$ *iff the state* w *is identical to* ν *except that* $w(x) = [\![\theta]\!]_\nu$.
2. $(\nu, w) \in \rho(x := *)$ *iff the state* w *agrees with* ν *except for the value of* x*, which is an arbitrary real value.*
3. $(\nu, w) \in \rho(x_1' = \theta_1 \wedge \ldots \wedge x_n' = \theta_n \wedge \chi)$ *iff for some* $r \geq 0$*, there is a function* $\varphi{:}[0, r] \to \mathrm{Sta}$ *with* $\varphi(0) = \nu, \varphi(r) = w$*, such that,*
   - *The differential equation holds, i.e., for each* x_i *and each time* $\zeta \in [0, r]$*,*
   $$\frac{\mathsf{d}\,[\![x_i]\!]_{\varphi(t)}}{\mathsf{d}t}(\zeta) = [\![\theta_i]\!]_{\varphi(\zeta)} \ .$$
   - *For other variables* $y \notin \{x_1, \ldots, x_n\}$ *and* $\zeta \in [0, r]$*, the value remains constant, i.e.,* $[\![y]\!]_{\varphi(\zeta)} = [\![y]\!]_{\varphi(0)}$.
   - *The invariant is always respected, i.e.,* $\varphi(\zeta) \models \chi$ *for each* $\zeta \in [0, r]$.
4. $\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$
5. $\rho(\alpha; \beta) = \{(\nu, w) : (\nu, z) \in \rho(\alpha), (z, w) \in \rho(\beta)$ *for a state* $z\}$
6. $(\nu, w) \in \rho(\alpha^*)$ *iff there are an* $n \in \mathbb{N}$ *and* $\nu = \nu_0, \ldots, \nu_n = w$ *such that* $(\nu_i, \nu_{i+1}) \in \rho(\alpha)$ *for all* $0 \leq i < n$.

Definition 2 (Interpretation of $\mathsf{d}\mathcal{L}$ formulas) *The* interpretation $\models$ *of a* $\mathsf{d}\mathcal{L}$ *formula with respect to state* ν *uses the standard meaning of first-order logic:*

1. $\nu \models \theta_1 \sim \theta_2$ *iff* $[\![\theta_1]\!]_\nu \sim [\![\theta_2]\!]_\nu$ *for* $\sim \in \{=, \leq, <, \geq, >\}$
2. $\nu \models \phi \wedge \psi$ *iff* $\nu \models \phi$ *and* $\nu \models \psi$*, accordingly for* $\neg, \vee, \rightarrow, \leftrightarrow$

3. $\nu \models \forall x\, \phi$ *iff* $w \models \phi$ *for all* w *that agree with* ν *except for the value of* x

4. $\nu \models \exists x\, \phi$ *iff* $w \models \phi$ *for some* w *that agrees with* ν *except for the value of* x

It extends to correctness statements about a HP α *as follows*

5. $\nu \models [\alpha]\phi$ *iff* $w \models \phi$ *for all* w *with* $(\nu, w) \in \rho(\alpha)$

6. $\nu \models \langle\alpha\rangle\phi$ *iff* $w \models \phi$ *for some* w *with* $(\nu, w) \in \rho(\alpha)$