Formally Verified Timing Computation for Non-deterministic Horizontal Turns During Aircraft Collision Avoidance Maneuvers

Yanni Kouskoulas[1(✉)], T. J. Machado[1,2], and Daniel Genin[1]

[1] The Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA
{yanni.kouskoulas,daniel.genin}@jhuapl.edu
[2] Department of Mathematics, New Mexico State University, Las Cruces, NM, USA
tjm@nmsu.edu

Abstract. We develop a library of proofs to support rigorous mathematical reasoning about horizontal aircraft turning maneuvers, and apply it to formally verify a timing computation for use during mixed horizontal and vertical aircraft collision avoidance maneuvers. We consider turns that follow non-deterministic circular turn-to-bearing horizontal motion, formalizing path-length and timing properties. These kinematics are the building blocks for Dubins trajectories, and can be used to formalize a variety of techniques, including those that contain non-determinism. The timing computation establishes, for intersecting trajectories, the exact bounds of time intervals when the horizontal position of the aircraft might coincide, and during which they must be at different altitudes to avoid collision.

1 Introduction

Autonomous and semi-autonomous systems that control ground vehicles, boats, and aircraft all need to reason about horizontal turns in order to create plans for future motion that meet system objectives.

We are motivated by aircraft collision avoidance maneuvers that combine vertical and horizontal advice to ensure multi-aircraft encounters are safely separated. These maneuvers advise aircraft to turn at the same time they change vertical velocity – the objective being to keep the aircraft separated in altitude during periods when their positions might coincide horizontally. This requires correctly computing the time interval that describes when in the future both aircraft might come into horizontal conflict.

This paper develops a formalization of *non-deterministic* turn-to-bearing motion, where a vehicle turns following a circular arc until reaching a certain bearing, and then follows a straight path thereafter. Turn-to-bearing motion is the building block for Dubins trajectories used in many different techniques in the literature (see Sect. 2), but here we consider that the parameters that

M. H. ter Beek and D. Ničković (Eds.): FMICS 2020, LNCS 12327, pp. 113–129, 2020.
https://doi.org/10.1007/978-3-030-58298-2_4

describe our future path are non-deterministic and uncertain. The formalization is embodied in a library of proofs that are detailed descriptions of these kinematics, and are machine-checked to guarantee correctness. Each theorem in the text corresponds to proofs in the formalization.[1] We believe that the library can serve as a foundation for formal reasoning about horizontal turns in the Coq proof assistant, supporting the development of insight and correct reasoning for a wide variety of path planning and collision avoidance algorithms. Further, we hope that it helps guarantee a high level of correctness and robustness for robotic systems' horizontal motion, and that it provides the basis for certification artifacts (proofs) that can be used to establish system algorithm and software correctness.

Most importantly, we created these proofs because we wanted to formally verify a collision avoidance algorithm and were unable to find the necessary lemmas in the Coq standard library. We apply these lemmas to a pointwise computation for horizontal conflict intervals, appropriate for use with [8], which can handle analysis of aircraft collision avoidance advice that requires turning horizontally while simultaneously accelerating towards a target vertical velocity.

The contributions of this paper are: the development of a Coq library for reasoning about non-deterministic Dubins-style paths; an additional Coq library defining a variety of two-argument arctangent functions with different branch cuts that are each sensitive to the quadrant and sign of their arguments; a new expression for computing the appropriate angle necessary for connecting Dubins paths to a destination waypoint[2]; insight into the timing characteristics of horizontal turns following circular arc segments; and a simple, efficient, piecewise approach to calculating collision timing of horizontal conflict intervals based on this insight.

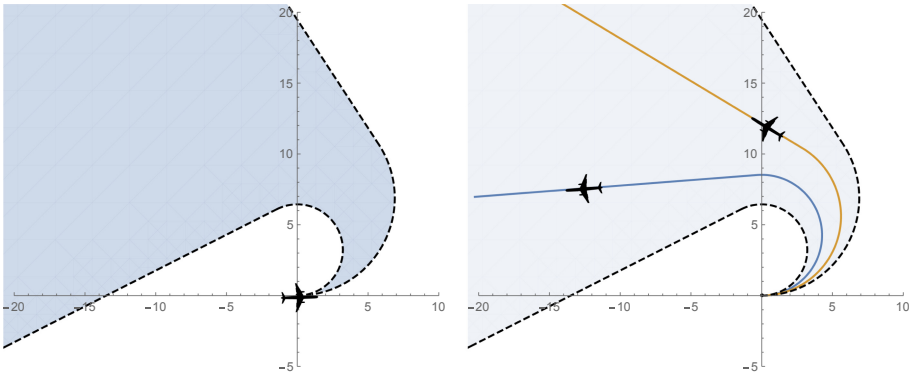
1.1 Non-deterministic Turn-to-Bearing Kinematics

We define *non-deterministic one-turn-to-bearing* motion as a set of trajectories representing a range of future motion possibilities that might be followed by the vehicle. We characterize this motion with a tuple that represents the set future trajectories that are possible $(x_0, y_0, \theta_0, r_\alpha, r_\beta, \theta_\alpha, \theta_\beta, s_\alpha, s_\beta)$ where: (x_0, y_0) and θ_0 are initial position and orientation of the vehicle; r_α, r_β, θ_α, θ_β are bounds on the turn radius and change in orientation after completing the turn, respectively; and s_α, s_β are bounds on the speed throughout the encounter, which unlike the other parameters, is assumed to vary continuously as a function of time. We adopt the convention of using positive radii and bearing offsets to represent counterclockwise (left) turns, and negative radii and bearing offsets to represent clockwise (right) turns. Left turns are represented by $0 < r_\alpha \leq r_\beta$ and $0 < \theta_\alpha < \theta_\beta < 2\pi$, while right turns by $r_\alpha \leq r_\beta < 0$ and $-2\pi < \theta_\alpha < \theta_\beta < 0$. In all cases, we assume $0 < s_\alpha \leq s_\beta$.

[1] Coq proofs are at https://bitbucket.org/ykouskoulas/ottb-foundation-proofs.

[2] There exist alternate expressions for this angle, but to our knowledge, the formulation in this paper is new.

Realization of a specific future trajectory requires drawing from this sample space. Each possibility in the set has parameters $r, \theta_c, s(t)$ satisfying the constraint predicate $\chi(r, \theta_c, s) = \theta_c \in [\theta_\alpha, \theta_\beta] \wedge r \in [r_\alpha, r_\beta] \wedge (\forall u, s(u) \in [s_\alpha, s_\beta])$ which represents a path with initial turn that we model using a circular arc of radius r, followed by a linear path tangent to the turn whose bearing is offset by θ_c from θ_0. The path is traversed with continuously varying speed $s(t)$. Figure 1 plots a visualization of turn-to-bearing envelopes and paths for $(x_0, y_0, \theta_0, r_\alpha, r_\beta, \theta_\alpha, \theta_\beta, s_\alpha, s_\beta) = (0, 0, 0, 3.22, 6.89, 2.41, 3.62, 1, 2)$.



(a) Shaded area is reachable in the future. **(b)** Paths show two possible trajectories.

Fig. 1. Vizualizing turn-to-bearing motion.

Components of the vehicle's trajectory for these kinematics are given by

$$J_x(t) = \begin{cases} r \sin\left(\frac{d(t)}{r} + \theta_0\right) - r\sin(\theta_0) + x_0 & d(t) \leq r\theta_c \\ (d(t) - r\theta_c)\cos(\theta_c + \theta_0) + r\sin(\theta_c + \theta_0) - r\sin(\theta_0) + x_0 & d(t) > r\theta_c \end{cases} \tag{1}$$

$$J_y(t) = \begin{cases} -r \cos\left(\frac{d(t)}{r} + \theta_0\right) + r\cos(\theta_0) + y_0 & d(t) \leq r\theta_c \\ (d(t) - r\theta_c)\sin(\theta_c + \theta_0) - r\cos(\theta_c + \theta_0) + r\cos(\theta_0) + y_0 & d(t) > r\theta_c \end{cases} \tag{2}$$

for overall trajectory $J(t) = J_x(t)\hat{x} + J_y(t)\hat{y}$. The distance traveled on the path is related to speed during the trajectory in the usual way, $d(t) = \int_0^t s(\gamma)d\gamma$.

2 Literature Review

A number of efforts have gone on to formalize horizontal motion and prove properties about it, but all have characteristics that distinguish them from the present work. For instance [7] develops an approach for maneuvering and coordinating

vehicles following Dubins paths utilizing Kripke models which is verified via a model checker. They don't incorporate non-determinism in their turning models, and don't deal with timing characteristics of the turns. In [2], they use differential dynamic logic with KeYmaera X to model collision avoidance in automobiles with skidding, but unlike the present work they are concerned mainly with geometric properties of paths and do not consider timing. The work in [11] is an excellent treatment of collision avoidance in a wide variety of uncertain turning scenarios for ground robots. It assumes obstacles characterized by maximum velocity bounds, is not focused on timing analysis, and is not tailored for use in mixed vertical and horizontal collision avoidance.

Closely related to this work is [13], which considers curved, horizontal aircraft avoidance manuevers, but without combining them with vertical maneuvers; and [6], which considers vertical maneuvers, but with straight-line horizontal kinematics, and does not allow combination with horizontal maneuvers.

Also closely related to this work is [8], which analyzes vertical maneuvers, but contains timing parameters that can be set to ensure safety for simultaneous horizontal manuevers. It is this work upon which we build in this paper, as our timing computation can be used to set parameters that safely compose turn-to-bearing horizontal maneuvers with arbitrary bounded-acceleration vertical maneuvers.

Dubins paths, constructed of circular arc segments and straight lines, are used to model horizontal motion in many path planning and collision avoidance algorithms, such as [4,5,9,10,14,15]. These examples are not formally verified, and although some are created with aircraft in mind, not designed for timing analysis nor the adversarial collision avoidance assumptions in our work.

Many years of work have gone into the tools and libraries that we used for our development, including the Coq proof assistant [1] and the Coquelicot extensions for its real library [3]. Our libraries are intended to contribute to this toolbox.

We develop a new expression for calculating allowable tangents to a turn; an alternate solution to this problem is reported in [12].

3 Reasoning Foundations for Turn-to-Bearing Maneuvers

The following sections describe the development of a library for reasoning about turn-to-bearing trajectories, and the application of this library to compute timing characteristics for safe maneuvering of simultaneously turning aircraft.

We first had to develop some definitions and trigonometric properties that were not available in our environment. We were then able to create a library for reasoning about turn-to-bearing paths.

3.1 Library Interface

The library we have developed is organized around the representation of a path in $\mathbb{R}^2$ and a predicate

$$\text{path\_segment}(D, f_x(d), f_y(d), (x_0, y_0), (x_1, y_1)) \tag{3}$$

which when true asserts: that $f_x(d)$ and $f_y(d)$ are parameterized functions describing the x and y positions of the path in the coordinate plane; that the resulting path is continuous and integrable; and that $f_x(d)$ and $f_y(d)$ are parameterized by the path distance, i.e. $\int_0^d \sqrt{(f'_x(\alpha))^2 + (f'_y(\alpha))^2} d\alpha = d$; that $(f_x(0), f_y(0)) = (x_0, y_0)$; and that $(f_x(D), f_y(D)) = (x_1, y_1)$. Parameterizing our path representation by path distance creates a canonical representation of the geometry for each path, isolating it from timing considerations associated with variations in speed during the maneuver, and allowing us to analyze each aspect separately and combine them in the end.

Note that although the turn-to-bearing paths in the library have a starting and ending point separated by distance D, the paths continue indefinitely.

The library also contains piecewise functions parameterizing the x and y positions for turn-to-bearing paths $H_x(r, \theta_0, x_0, \theta_c, rtp, d)$ and $H_y(r, \theta_0, y_0, \theta_c, rtp, d)$, meant to be used with the path_segment predicate. The functions are equivalent to Eqs. 1 and 2, differing only in that they are parameterized by distance d instead of time t. The functions are curried before being used in path_segment, instantiated with starting point (x_0, y_0), initial orientation θ_0, the turn radius r, and the angular offset for the final bearing θ_c. They also require an argument named rtp, which must be a proof object showing that $0 < r\theta_c < 2\pi|r|$, ensuring the signs of r and θ_c to be identical, and enforcing an upper bound on θ_c. The files *ttyp.v* and *tdyn.v* define the path_segment predicate, the parameterized turn-to-bearing paths, and prove lemmas about path continuity, differentiability, and path-length parameterization of H_x and H_y so they can be used with the path_segment predicate. Along with the parameterization, the library contains predicates straight and turning which indicate whether the parameters describing a path reach the final destination point while traveling in a straight line, or turning on a circular arc, respectively.

The rest of the library has: trigonometric definitions and identities that are missing from the Coq standard library (*atan2.v*, *strt.v* and *strt2.v*); lemmas that help the user introduce turn-to-bearing path_segment predicates into the context (*tlens.v*); lemmas that help derive consequences and mathematical relationships from turn-to-bearing path_segment assumptions (*tlens.v*); lemmas about timing intervals (*ttim.v*); and theorems about the computation of timing properties based on pathlength (*dtlen.v*). The size of the development is significant, around 40k lines of proof scripts.

Because Coq allows expression in a higher order logic, it permits quantification over any variable. This means we can hold the starting and ending points of the path fixed and quantify over the other parameters to reason about waypoints; or fix ranges of parameters and quantify over the radii and angles to reason about ranges of non-deterministic possibilities in turn radius and final bearing.

In this paper, for clarity, we present lemmas from the library in a standard position and orientation such that $(x_0, y_0) = (0, 0)$, $\theta_0 = 0$, and $(x_1, y_1) = (x, y)$. To analyze intersecting paths that are oriented and positioned arbitrarily with respect to one another, the more general form can be recovered by assuming that

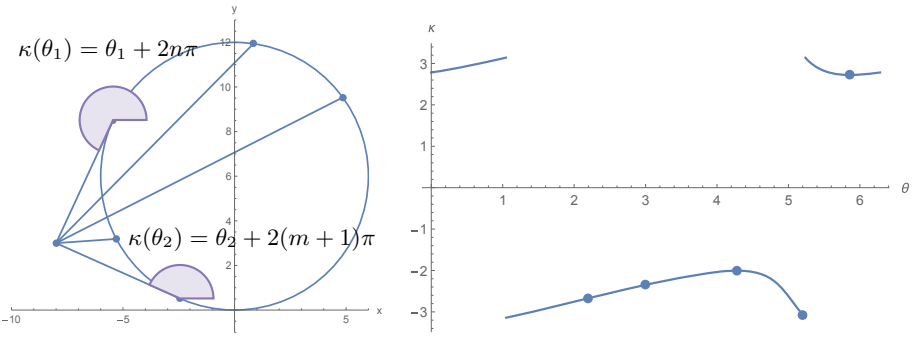
$$x = (x_1 - x_0)\cos(\theta_0) + (y_1 - y_0)\sin(\theta_0) \tag{4}$$
$$y = -(x_1 - x_0)\sin(\theta_0) + (y_1 - y_0)\cos(\theta_0) \tag{5}$$

The library itself contains the translations and rotations to allow full generality when working with more than one path.

3.2 Trigonometric Properties

Geometric intuition which might seem simple does not always translate naturally to formal analysis in a proving environment.

First we needed to encode in our proving environment a basic understanding of the way circular turns may be combined with straight paths that exit the turns on a tangent. There are two tangent lines to a circle that arrive at any particular point outside the circle (see Fig. 2). One of the tangents is not useful because



(a) Angle of each line segment is κ **(b)** Discontinuous κ_2; $\kappa' = 0$ points are tangent

Fig. 2. If we parameterize positions on a circular path using the angle associated with the tangent at each point, $\kappa(\theta)$ – not necessarily a tangent itself – is the angle of the line connecting the point on the circle to a point (x, y) outside the circle.

for counter-clockwise turns, it always results in a path with a discontinuous derivative. This is geometrically obvious to a human by inspection, but somewhat challenging to formalize in Coq.

Using a chord lemma from geometry we can infer that a vehicle approaching (x, y) from a circular turn will do so at an angle of $\theta_m = 2\,\text{atan}_2(y, x)$ and that the radius required to reach it will be $r_m = (x^2 + y^2)/(2y)$. We find that decreasing the radius of the turn decreases the angle, while increasing it makes (x, y) unreachable via a tangent line. Thus θ_m defines an upper bound on the approach angle. From inspection, we can see that the angle of the second tangent exceeds this boundary.

In order to formalize this geometric intuition, we define a function which given the orientation θ of the vehicle on a turning path of radius r would return the angle from the vehicle to the point (x, y).

$$\kappa(\theta) = \operatorname{atan}\left(\frac{y - r(1 - \cos(\theta))}{x - r\sin(\theta)}\right) \tag{6}$$

Both by construction, and by the periodicity of sin and cos, we note that κ is periodic with period 2π. For the remainder of this section we will restrict the domain of κ to $(0, 2\pi)$ for $r > 0$, and $(-2\pi, 0)$ for $r < 0$. As illustrated in Fig. 2b, the function κ is not continuous for all values of the destination point (x, y).

We define a series of functions based on a two-argument arctangent and different branch cuts, which have distinct, overlapping, and complementary domains upon which (x, y) yields a continuous function.

$$\kappa_2(\theta) = \operatorname{atan}_2\left(y - r(1 - \cos(\theta)), x - r\sin(\theta)\right) \tag{7}$$

$$\kappa_3(\theta) = \operatorname{atan}_2\left(-(y - r(1 - \cos(\theta))), -(x - r\sin(\theta))\right) + \pi \tag{8}$$

$$\kappa_4(\theta) = \operatorname{atan}_2\left(-(x - r\sin(\theta)), y - r(1 - \cos(\theta))\right) + \pi/2 \tag{9}$$

Henceforth, when we refer to properties of κ, we are choosing a variant with the branch cut oriented so that there is no discontinuity for the given destination point (x, y).

When κ is continuous, we show that the unique maximum and minimum values $\kappa(\theta_1)$ and $\kappa(\theta_2)$ correspond to the angles of the correct and incorrect tangent lines respectively (for $r > 0$, if $r < 0$ the maxima and minima are reversed). We prove that $\kappa(\theta) = \frac{\theta_m}{2}$ implies that $\theta = 0$ or $\theta = \theta_m$. Since $\frac{\theta_m}{2}$ is a value that κ takes on, it must be that $\kappa(\theta_1) \geq \frac{\theta_m}{2} \geq \kappa(\theta_2)$.

Our choice of domain ensures that 0 is not between θ_1 and θ_2, so we can use the Intermediate Value Theorem to show that θ_m is in-between θ_1 and θ_2 in the domain. Because θ_m is a limiting value of the approach angle, we can eliminate θ_2, which is always outside of the allowable range, leaving θ_1 as the angle of approach that ensures path continuity.

We calculate extremal values of κ, θ_1 and θ_2, by setting the derivative of κ to zero, and solving for the argument. Fortunately, each variant of the κ function for which the destination point (x, y) yields a continuous function has the same derivative

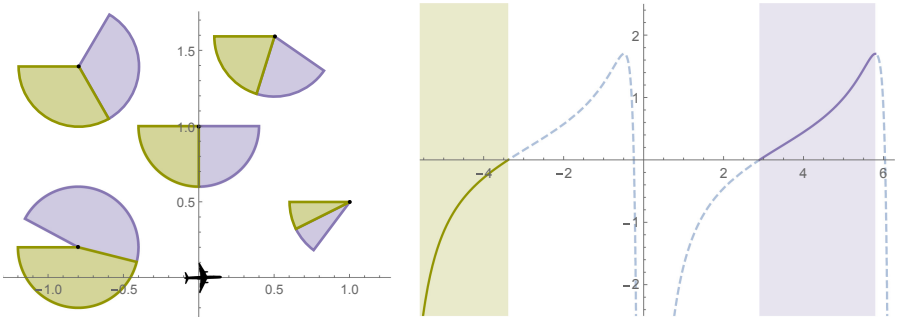
$$\kappa'(\theta) = \frac{r((2r - y)(\tan(\theta/2))^2 - 2x\tan(\theta/2) + y)}{(2(1 - \cos(\theta))/(\sin(\theta))^2) \cdot ((y - r(1 - \cos(\theta)))^2 + (x - r\sin(\theta))^2)} \tag{10}$$

for $\theta \notin \{0, \pi\}$. The sign of the denominator is always positive, and so the sign of κ' is directly related to the sign of the quadratic function in the numerator; the task of calculating the maximum and minimum is reduced to the problem of solving a quadratic in $\tan(\theta/2)$. The solution associated with the maximum value of κ is given in Eq. 14.

Reasoning about the continuity of the κ variants, handling their derivatives as the angle crosses the branch cut, and ordering of roots and angles to establish what "in-between" means in an angular domain that is a clock system is contained within the file *strt.v* and its corresponding documentation.

3.3 Turn-to-Bearing Path Properties

Parameters for turn-to-bearing trajectories must be selected in a way that the radius and angle of departure from the turn lead from the starting point to the ending point, and so that the distance is consistent with the path. In this section we state basic results about paths, and select a few proofs about which we provide some details in order to give a flavor of the reasoning in the library.



(a) Approaches for different points. **(b)** r vs. θ for a single point $(-.8, .2)$.

Fig. 3. Relationship between allowable angle of approach and required radius to achieve that angle. Choosing angular ranges of approach also entails a turn direction; left turns are marked with violet and right turns marked with green. (Color figure online)

We can construct a turn-to-bearing trajectory by choosing an angle of approach θ for a point (x, y), and computing the turn radius required to arrive there with that orientation. The angle of approach is constrained because of the initial position and angle of the aircraft and the required kinematics, as in Fig. 3.

Theorem 1 (Turn-to-bearing dependent radius). *A vehicle following a turn-to-bearing trajectory can approach point* (x, y) *with a chosen angle* θ *when*

$$\begin{aligned}(0 < \theta_m \wedge (\theta_m/2 < \theta \leq \theta_m \vee -2\pi < \theta < \theta_m/2 - 2\pi)) \vee \\ (\theta_m < 0 \wedge (\theta_m \leq \theta < \theta_m/2 \vee \theta_m/2 + 2\pi < \theta < 2\pi))\end{aligned} \tag{11}$$

using radius

$$R(x, y, \theta) = \frac{x \sin(\theta) - y \cos(\theta)}{1 - \cos(\theta)} \tag{12}$$

We can also construct a turn-to-bearing trajectory by choosing a turn radius r, and computing the angle of approach that the radius entails when we arrive at (x, y). The choice of radius is constrained if the target point is on the same side as the direction of the turn, because the turn must be rapid enough to orient the aircraft in the direction of the target point before it has passed it.

Theorem 2 (Turn-to-bearing dependent approach angle). *A vehicle following a turn-to-bearing trajectory can approach point* (x, y) *using a turn with chosen radius* r *when*

$$\left(0 < y \wedge r \leq \frac{x^2 + y^2}{2y}\right) \vee (y = 0 \wedge x < 0) \vee \left(y < 0 \wedge \frac{x^2 + y^2}{2y} \leq r\right) \tag{13}$$

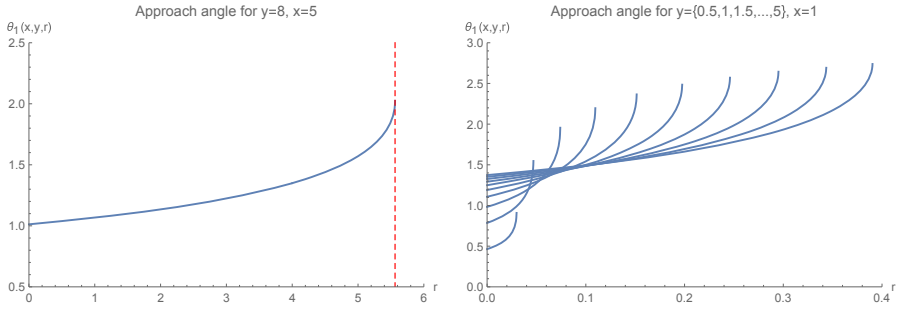
and the angle of approach is

$$\Theta(x, y, r) = \begin{cases} 2\,\mathrm{atan}\left(\frac{x - \sqrt{x^2 - (2r - y)y}}{(2r - y)}\right) + P(x, y, r) & 2r - y \neq 0 \\ 2\,\mathrm{atan}\left(\frac{y}{2x}\right) & 2r - y = 0 \wedge x > 0 \\ \pi\ \mathrm{sign}\ (r) & 2r - y = 0 \wedge x \leq 0 \end{cases} \tag{14}$$

where P *is a phase correction given by*

$$P(x, y, r) = \begin{cases} 0 & (0 < r \wedge ((0 < x \wedge 0 < y) \vee x \leq 0 \wedge 2r < y)) \\ & \vee\ (r < 0 \wedge ((x < 0 \wedge y < 0) \vee y < 2r)) \\ 2\pi & 0 < r \wedge (0 \leq x \wedge y < 0 \vee x < 0 \wedge y < 2r)) \\ -2\pi & r < 0 \wedge (0 \leq x \wedge 0 < y \vee x < 0 \wedge 2r < y). \end{cases} \tag{15}$$

It is not unexpected that for fixed (x, y), the first piece of $\Theta(x, y, r)$ is not differentiable or even always defined at $r = r_m$. What is surprising is that even if we define the endpoint to ensure the value of the function is finite, its rate of change is unbounded at the end of the interval. This is illustrated in Fig. 4, and made formalizing the relationship between the length of circular arc path segments and the rest of the turn-to-bearing kinematics interesting.



(a) Varying r for a single (x, y). **(b)** Varying r for a sequence of points.

Fig. 4. Plot of the first piece of $\Theta(x, y, r)$ from Eq. 14

This geometry appears in a variety of contexts, including [12] at the bottom of p. 19:15, which has another expression that may be used to solve for the angle. We leave it to the interested reader to show the equivalence between the result we have proved, and alternate formulations. We also find a simplification for the tangent path length:

Theorem 3 (Straight path segment expression). *For a turn-to-bearing trajectory given by* $(r, \Theta(x, y, r))$*, that starts at the origin with* $\theta_0 = 0$ *and passes through* (x, y)*, the square of the distance traveled on a straight line before we arrive at* (x, y) *is given by*

$$(x - r\sin(\Theta(x, y, r)))^2 + (y - r(1 - \cos(\Theta(x, y, r))))^2 = x^2 - (2r - y)y \quad (16)$$

4 Reasoning About the Timing of Intersecting Turns

This section describes our approach to analyzing the future safety of two vehicles following non-deterministic turn-to-bearing horizontal kinematics. The problem can be divided into computing the intersection of reachable envelopes where collisions might occur (geometry), and when they might occur (timing).

The geometry of the reachable envelope for a turn, such as the one pictured in Fig. 1a, is bounded by edges that are combinations of circular arcs and straight lines; the intersection of these areas may be computed in a straightforward manner. The rest of our discussion is focused on evaluating the timing of potential collisions at different points in space where the turns intersect.

4.1 Pointwise Collision Timing

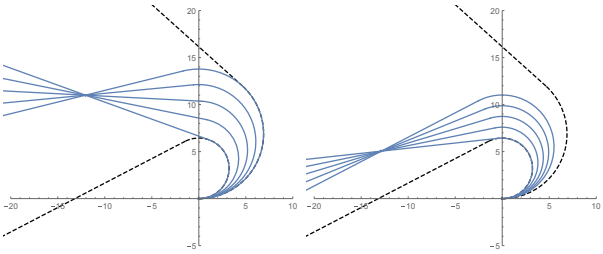
We define the reachable envelope

$$E = \{p \,|\exists\ \theta_c, r, s, u \text{ s.t. } \chi(r, \theta_c, s) \wedge u > 0 \wedge J(u) = p\} \quad (17)$$

for a vehicle to be the set of points that are reachable over the range of possible future trajectories. For any point in the reachable envelope $p \in E$, there is a set of trajectories $\mathcal{T}(p) = \{J(t) \,|\exists\ \theta_c, r, s, u \text{ s.t. } \chi(r, \theta_c, s) \wedge u > 0 \wedge J(u) = p\}$ that can reach that point. Each trajectory $J \in \mathcal{T}(p)$ corresponds with a different choice of radius and final bearing (which determine the path), and future ground speed $s(t)$. Figures 5a and b illustrate two different points in the reachable envelope of the ownship from Fig. 1 and a set of paths followed by trajectories taken from the family of possibilities that would reach each point.

There is a corresponding set of arrival times $I(p) = \{t_a \,|J \in \mathcal{T}(p) \wedge J(t_a) = p\}$ during which that vehicle can arrive at p. The earliest and latest arrival time at point p for a single vehicle are given by $t_e(p) = \inf I(p)$ and $t_l(p) = \sup I(p)$, where $J(t)$ is the position of the aircraft following trajectory J at time t.

To analyze relative timing between two aircraft and determine whether collision is possible, we can look pointwise at the earliest and latest arrival times for each. We first define four logical predicates that express whether the earliest and latest arrival time at point p in the reachable area occur when the other vehicle may also be located at that point. Each time variable t in the subsequent equations has a subscript indicating whether the time is earliest possible $(_e)$ or latest possible $(_l)$ time of arrival, and a superscript indicating which aircraft timing is referenced, ^{i} for intruder or ^{o} for ownship.



(a) **(b)**

Fig. 5. Paths from the set of possible turn-to-bearing trajectories that reach two example points in space. The reachable envelope is shown as a set of dashed lines for a non-deterministic left turn; any point in the reachable envelope is reachable via these kinematics.

$$W_e^i(p) = t_e^o(p) \leq t_e^i(p) \leq t_l^o(p) \tag{18}$$
$$W_l^i(p) = t_e^o(p) \leq t_l^i(p) \leq t_l^o(p) \tag{19}$$
$$W_e^o(p) = t_e^i(p) \leq t_e^o(p) \leq t_l^i(p) \tag{20}$$
$$W_l^o(p) = t_e^i(p) \leq t_l^o(p) \leq t_l^i(p) \tag{21}$$

We combine these to define two predicates to evaluate safety, one using the earliest arrival time, and the other using the latest arrival time,

$$W_e(p) = W_e^i(p) \vee W_e^o(p) \tag{22}$$
$$W_l(p) = W_l^i(p) \vee W_l^o(p) \tag{23}$$

For two aircraft we define a conflict area $C = E^o \cap E^i$ to reflect the geometry of the intersection of future paths without timing considerations. We prove

Theorem 4 (Leading Lagging Equivalence). *For all points $p \in C$, predicates $W_e(p) = W_l(p)$, so we can drop the subscript.*

Theorem 5 (Pointwise Safety). *$W(p)$ correctly establishes safety at point p: when it is true, there exist circumstances that lead to collision at p, and when it is not there are no circumstances that lead to collision at p.*

Theorem 6 (Collision Timing). *For all points $p \in C \wedge W(p)$, a collision may only occur in the time interval $[\max\left(t_e^i(p), t_e^o(p)\right), \min\left(t_l^i(p), t_l^o(p)\right)]$, and under the assumptions, no collision may occur outside this time interval.*

Consequently the earliest and latest collision times in an area C are given by

$$t_e = \inf_{p \in C \wedge W(p)} \max\left(t_e^i(p), t_e^o(p)\right) \tag{24}$$
$$t_l = \sup_{p \in C \wedge W(p)} \min\left(t_l^i(p), t_l^o(p)\right) \tag{25}$$

We can directly relate timing of a trajectory between two points to the range of path lengths for different possible paths connecting the points. The earliest arrival time to reach a point p, $t_e(p)$ is achieved by the trajectory following the shortest path and the highest ground speed, i.e. $\inf I(p) = \frac{d_{\min}(p)}{s_\beta}$, where $d_{\min}(p)$ is the length of the shortest path from the starting point to p. The latest arrival time is achieved by the trajectory following the longest path with the slowest ground speed, i.e. $\sup I(p) = \frac{d_{\max}(p)}{s_\alpha}$, where $d_{\max}(p)$ is the length of longest path from the starting point to p. In this way, we convert the problem of computing collision timing into a problem computing the range of possible path lengths between two points.

4.2 Path Length Properties

We can define a function that computes the distance of the path for a deterministic, left-turning turn-to-bearing trajectory starting from the origin with orientation $\theta_0 = 0$, passing through (x, y) with orientation θ, using a turn of radius r:

$$L(x, y, \theta, r) = r\theta + \|(x, y) - r(\sin\theta, 1 - \cos\theta)\| \tag{26}$$

Turn-to-bearing kinematics constrain the parameters for L, i.e. its arguments cannot all be chosen independently. Assume we fix the point we wish to reach, (x, y). We can independently choose the angle we approach our final point with, θ, and that determines the turn radius of the maneuver. Alternatively, we can choose the radius of our turn, and compute the angle of approach to the second point.

A central insight here is that for paths with the same starting and ending points, the path with a larger angle of approach will have a larger radius; and the path with a larger radius will be longer. More precisely:

Theorem 7 (Approach angle orders turn-to-bearing path radii). *Given two turn-to-bearing paths, (r_1, θ_1) and (r_2, θ_2) that pass through the same point (x, y), if $\theta_1 > \theta_2 > 0$, then the radius of the first path r_1 is longer than the radius of the second path r_2, i.e. $r_1 > r_2$:*

$$\theta_1 > \theta_2 > 0 \rightarrow R(x, y, \theta_1) > R(x, y, \theta_2) \tag{27}$$

Theorem 8 (Radius orders turn-to-bearing path lengths). *Given two turn-to-bearing paths, (r_1, θ_1) and (r_2, θ_2) that pass through the same point (x, y), if $r_1 > r_2 > 0$, then the first path length L_1 is greater than the second path length L_2, i.e. $L_1 > L_2$:*

$$r_1 > r_2 > 0 \rightarrow L(x, y, \Theta(x, y, r_1), r_1) > L(x, y, \Theta(x, y, r_2), r_2) \tag{28}$$

Maximum and Minimum Path Lengths. At each point in the reachable area, we can use the ordering of path lengths implied by Theorems 7 and 8 to find the minimum and maximum length path possible for uncertain turn-to-bearing motion constrained by non-deterministic bounds.

Theorem 9 (Minimum bearing-constrained path length). *For turn-to-bearing kinematics, given interval constraints on final bearing* $[\theta_\alpha, \theta_\beta]$ *and turn radius* $[r_\alpha, r_\beta]$ *where* $0 < r_\alpha$ *and* $0 < \theta_\alpha$*, and a reachable point* (x, y)*, the minimum path length is given by*

$$d_{min}(x,y) = \begin{cases} L(x,y,\Theta(x,y,r_\alpha),r_\alpha) & \theta_\alpha \leq \Theta(x,y,r_\alpha) \leq \theta_\beta \\ L(x,y,\theta_\alpha,R(x,y,\theta_\alpha)) & \theta_\alpha < \theta_m \wedge \Theta(x,y,r_\alpha) < \theta_\alpha \\ L(x,y,\theta_m,r_m) & r_\alpha \leq r_m \leq r_\beta \wedge \theta_m \leq \theta_\alpha \end{cases} \tag{29}$$

Theorem 10 (Maximum bearing-constrained path length). *For turn-to-bearing kinematics, given interval constraints on final bearing* $[\theta_\alpha, \theta_\beta]$ *and turn radius* $[r_\alpha, r_\beta]$ *where* $0 < r_\alpha$ *and* $0 < \theta_\alpha$*, and a reachable point* (x, y)*, the maximum path length is given by*

$$d_{max}(x,y) = \begin{cases} L(x,y,\Theta(x,y,r_\beta),r_\beta) & r_m > r_\beta \wedge \theta_\alpha \leq \Theta(x,y,r_\beta) \leq \theta_\beta \\ L(x,y,\theta_\beta,R(x,y,\theta_\beta)) & \theta_\beta < \theta_m \wedge \theta_\beta < \Theta(x,y,r_\beta) \\ L(x,y,\theta_m,r_m) & r_\alpha \leq r_m \leq r_\beta \wedge \theta_m \leq \theta_\beta \end{cases} \tag{30}$$

Right and Uncertain Turns. So far we have looked only at left turns, where the circle that defines our turn radius is positioned to the left of the vehicle, and the change in bearing is a relative angle in radians, positive according to the usual counter-clockwise convention. For non-deterministic left turns, $0 < r_\alpha \leq r_\beta$ and $0 \leq \theta_\alpha \leq \theta_\beta$.

We can handle other types of turns via symmetry. For right turns, we choose the convention of identifying turning trajectories using radii with negative numbers, and giving relative bearing with negative numbers as well. We describe non-deterministic right turns using parameters such that $r_\alpha \leq r_\beta < 0$ and $\theta_\alpha \leq \theta_\beta < 0$. For this convention, the path length for right turns is given by:

$$L^{\text{right}}(x,y,\theta,r) = L(x,-y,-\theta,-r) \tag{31}$$

The function that determines the maximum and minimum distance for right turns is related to that for left turns in the following way:

$$d^{\text{right}}(x,y,\theta_\alpha,\theta_\beta,r_\alpha,r_\beta) = d(x,-y,-\theta_\beta,-\theta_\alpha,-r_\beta,-r_\alpha) \tag{32}$$

for both minimum and maximum distance.

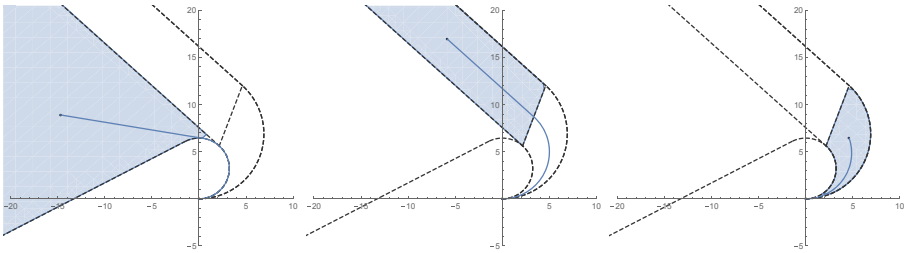
We can compute the distances associated with non-deterministic forward motion that might include either a left or a right turn, by requiring $r_\beta < 0 < r_\alpha$

and $\theta_\alpha \leq 0 \leq \theta_\beta$. The distance function then relates to the left and right distance functions:

$$d^{\text{either}}(x, y, \theta_\alpha, \theta_\beta, r_\alpha, r_\beta) = \begin{cases} d(x, y, 0, \theta_\beta, r_\alpha, \infty) & y > 0 \\ d^{\text{right}}(x, y, \theta_\alpha, 0, -\infty, r_\beta) & y < 0 \\ x & y = 0 \end{cases} \tag{33}$$

4.3 Exact Timing Wavefront

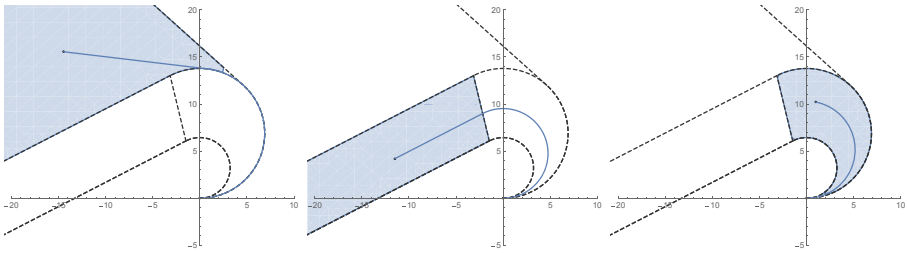
The observations in Theorems 9–10 allow us to subdivide the reachable envelope into different areas, using a piecewise function to describe its timing. Figures 6 and 7 illustrate, for a single vehicle and a particular choice of parameters, the different strategies that maximize and minimize path length, and the areas associated with each strategy. The bounding areas that enclose uniform strategies are shown with dashed lines that illustrates the limits where each strategy is appropriate for finding minimum and maximum length. For turns with different parameters, these shapes would change accordingly.



(a) $r = r_\alpha$ **(b)** $\theta_c = \theta_\alpha$ **(c)** $r = r_m \wedge \theta_m \leq \theta_c$

Fig. 6. Strategies described by Eq. 29 for minimum distance turn-to-bearing trajectories from the origin for each of three possible regions. Example trajectories illustrate the strategy for a single point in each region.

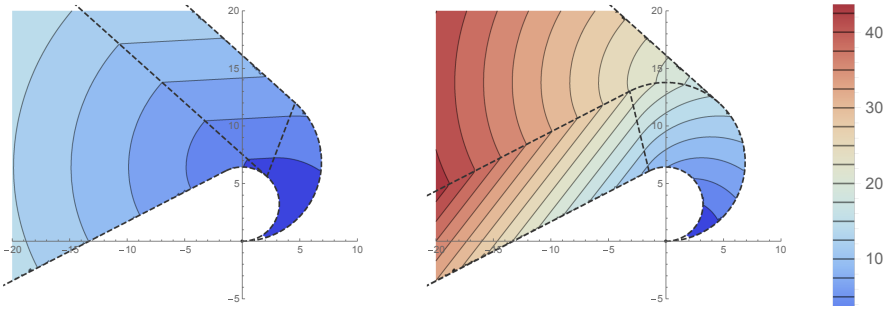
This means that if we want to find the longest and shortest paths to a point, we first consider paths with the greatest and smallest radii, r_α and r_β. Figures 6(a) and 7(a) illustrate individual trajectories that have minimum and maximum length for our example maneuver, constructed by using the minimum and maximum radii allowed. For some points, the most extreme turns could not produce trajectories that arrive at p, because the final bearings required by such trajectories are outside the parameters we have set for our motion, or because the points are inside the turning circle. Figures 6(b) and 7(b) illustrate individual trajectories that have minimum and maximum length for our example maneuver in this case. These are constructed by choosing radii that lead to most extreme values of bearing, so that the trajectory both reaches p, and does so



(a) $r = r_\beta$ **(b)** $\theta_c = \theta_\beta$ **(c)** $r = r_m \wedge \theta_m \leq \theta_c$

Fig. 7. Strategies described by Eq. 30 for maximum distance turn-to-bearing trajectories from the origin for each of three possible regions. Example trajectories illustrate the strategy for a single point in each region.

with an orientation that is allowed by the parameters of our turn. Finally, there are points in the reachable envelope that are reachable as part of the initial turn. For these points, this initial turn is the maximum-length path. If the bearing at point p is outside the allowable range, then this is also the minimum-length path. Figures 6(c) and 7(c) illustrate individual trajectories that have maximum and minimum length for our example maneuver, that must be constructed as circular arcs.



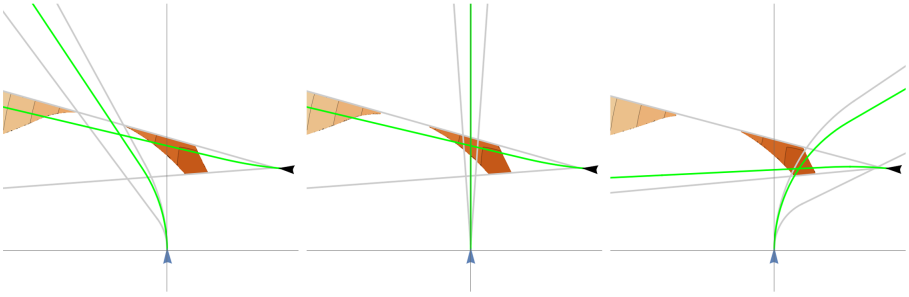
(a) Minimum time to arrive, $t_e(p)$. **(b)** Maximum time to arrive, $t_l(p)$.

Fig. 8. Contour plot describing timing for a left turn with parameters used in Fig. 1. Each (x, y) position in the Cartesian plane is associated with a time to arrive at that position starting from $(0, 0)$ with orientation $\theta_0 = 0$, following turn-to bearing kinematics.

In Fig. 8 we use the parameters of our example maneuver in Fig. 1, combining all of the results from Theorems 9–10 together into a single contour plot of the earliest and latest times to reach each point in the reachable area. The contour lines plotted in Fig. 8a and b can be thought of as the outer and inner boundaries (respectively) of the irregular annulus at the instant corresponding to the value

of the contour. As time progresses, this annulus expands, so we can treat this like a propagating wave that expresses location over time within the reachable area. The contours of equal timing for the minimum and maximum arrival times represent the shape of the leading and trailing edge of this wave, respectively. In addition to modeling and analyzing ranges of possibilities for turn-to-bearing kinematics, we will find that adding non-determinism also allows us to evaluate timing safety for small perturbations of turn-to-bearing – types of motion whose combination of trajectory and speed is sufficiently close, but not exactly the same.

Figure 9 shows how the timing computation can be used to analyze timing safety during a two-aircraft encounter. We analyze three different horizontal maneuvers for the aircraft at the origin, assuming a non-deterministic range of possibilities for forward motion of the other aircraft.



(a) Left turn **(b)** No turn **(c)** Right turn

Fig. 9. Computing timing possibilities for three different pilot maneuvers during a two-aircraft encounter. The shaded area shows the timing of collision possibilities at each horizontal position, indicating the timing required for vertical separation to ensure safety; darker shading indicates earlier collision possibility. The green trajectories show one possible realization from the range of non-deterministic possibilities for each motion model.

5 Conclusion

In this work, we have created a library that describes turn-to-bearing kinematics and allows us to reason about them without approximation. The representation allows non-determinism in all turn parameters by quantifying over state variables.

We have applied the library to compute timing intervals during which intersecting turns might collide, so they can be used to determine when aircraft must be vertically separated. We compute time intervals without approximation, for a given point where the turns intersect that account for arbitrary, non-deterministic bounds for speed during the horizontal maneuvers for each aircraft.

These computations are useful for correctly analyzing the safety of simultaneous horizontal and vertical maneuvers for collision avoidance.

References

1. The coq proof assistant. https://coq.inria.fr. Accessed 24 May 2020
2. Abhishek, A., Sood, H., Jeannin, J.-B.: Formal verification of braking while swerving in automobiles. In: Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control, HSCC 2020. Association for Computing Machinery, New York (2020)
3. Boldo, S., Lelay, C., Melquiond, G.: Coquelicot: a user-friendly library of real analysis for Coq. Math. Comput. Sci. **9**(1), 41–62 (2015). https://doi.org/10.1007/s11786-014-0181-1
4. Cons, M.S., Shima, T., Domshlak, C.: Integrating task and motion planning for unmanned aerial vehicles. Unmanned Syst. **02**(01), 19–38 (2014)
5. Isaiah, P., Shima, T.. A task and motion planning algorithm for the Dubins travelling salesperson problem. IFAC Proc. Vol. **47**(3), 9816–9821 (2014). 19th IFAC World Congress
6. Jeannin, J.-B., et al.: A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system. STTT **19**(6), 717–741 (2017)
7. Jeyaraman, S., Tsourdos, A., żbikowski, R., White, B.A.: Formal techniques for the modelling and validation of a co-operating UAV team that uses Dubins set for path planning. In: Proceedings of the 2005, American Control Conference, 2005, vol. 7, pp. 4690–4695 (2005)
8. Kouskoulas, Y., Genin, D., Schmidt, A., Jeannin, J.-B.: Formally verified safe vertical maneuvers for non-deterministic, accelerating aircraft dynamics. In: Ayala-Rincón, M., Muñoz, C.A. (eds.) ITP 2017. LNCS, vol. 10499, pp. 336–353. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66107-0_22
9. Ma, X., Castanon, D.A.: Receding horizon planning for Dubins traveling salesman problems. In: Proceedings of the 45th IEEE Conference on Decision and Control, pp. 5453–5458, December 2006
10. McGee, T.G., Hedrick, J.K.: Path planning and control for multiple point surveillance by an unmanned aircraft in wind. In: 2006 American Control Conference, p. 6, June 2006
11. Mitsch, S., Ghorbal, K., Vogelbacher, D., Platzer, A.: Formal verification of obstacle avoidance and navigation of ground robots. Int. J. Robot. Res. **36**(12), 1312–1340 (2017)
12. Platzer, A.: Differential hybrid games. ACM Trans. Comput. Log. **18**(3), 19:1–19:44 (2017)
13. Platzer, A., Clarke, E.M.: Formal verification of curved flight collision avoidance maneuvers: a case study. In: Cavalcanti, A., Dams, D.R. (eds.) FM 2009. LNCS, vol. 5850, pp. 547–562. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-05089-3_35
14. Song, X., Hu., S.: 2D path planning with Dubins-path-based A⋆ algorithm for a fixed-wing UAV. In: 3rd IEEE International Conference on Control Science and Systems Engineering (ICCSSE), Beijing, China, pp. 69–73 (2017)
15. Zhao, Z., Yang, J., Niu, Y., Zhang, Y., Shen, L.: A hierarchical cooperative mission planning mechanism for multiple unmanned aerial vehicles. Electronics **8**, 443 (2019)