NASA/TM-2010-216706

Formal Verification of Air Traffic Conflict Prevention Bands Algorithms

Anthony J. Narkawicz and César A. Muñoz
Langley Research Center, Hampton, Virginia

Gilles Dowek
Ecole polytechnique, France

June 2010

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at 443-757-5803

- Phone the NASA STI Help Desk at 443-757-5802

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/TM-2010-216706

Formal Verification of Air Traffic Conflict Prevention Bands Algorithms

Anthony J. Narkawicz and César A. Muñoz
Langley Research Center, Hampton, Virginia

Gilles Dowek
Ecole polytechnique, France

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

June 2010

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Abstract

In air traffic management, a pairwise conflict is a predicted loss of separation between two aircraft, referred to as the ownship and the intruder. A conflict prevention bands system computes ranges of maneuvers for the ownship that characterize regions in the airspace that are either conflict-free or "don't go" zones that the ownwhip has to avoid. Conflict prevention bands are surprisingly difficult to define and analyze. Errors in the calculation of prevention bands may result in incorrect separation assurance information being displayed to pilots or air traffic controllers. This paper presents provably correct 3-dimensional prevention bands algorithms for ranges of track angle, ground speed, and vertical speed maneuvers. The algorithms have been mechanically verified in the Prototype Verification System (PVS). The verification presented in this paper extends in a non-trivial way that of previously published 2-dimensional algorithms.

Contents

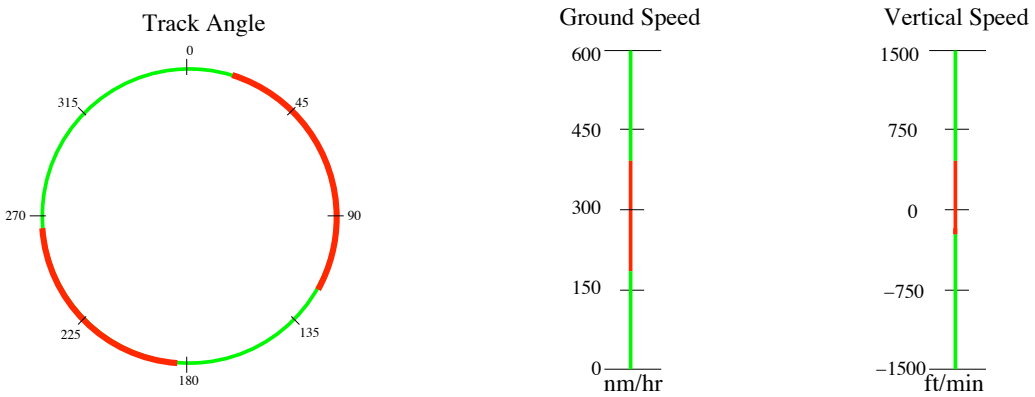

Figure 1. A graphical display of prevention bands algorithms for track angle, ground speed, and vertical speed

1 Introduction

In air traffic management, a *(pairwise) conflict* is a predicted loss of separation between two aircraft within a lookahead time. One of the aircraft is called the *ownship* and the other aircraft, which represents an arbitrary traffic aircraft, is called the *intruder*.

A *conflict prevention* system consists of algorithms that sense traffic aircraft and characterize ranges of maneuvers for the ownship that are either conflict-free or that lead to conflict. The maneuvers are typically constrained to those where only one parameter of the ownship's velocity is varied at a time: track angle, vertical speed, or ground speed.

More precisely, a *(pairwise) prevention bands* algorithm, for a given parameter such as track angle, ground speed, or vertical speed, has as input the state information of the ownship and intruder aircraft, i.e., their 3-dimensional position and velocity vectors. It returns a list of regions, called *bands*, consisting of values for the specified parameter. There is a natural way to associate a color, either red or green, to each band. *Red bands* specify "don't go" zones, i.e., parameter values that the ownship has to avoid because they lead to conflict. Conversely, the *green bands* specify parameter values for the ownship that yield conflict-free maneuvers.

Figure 1 illustrates in a graphical display prevention bands for the ownship for track angle, ground speed, and vertical speed maneuvers. Given the current position and velocity vectors of the aircraft, the displayed bands in Figure 1 indicate that the aircraft will be in conflict if, for instance, the ownship maneuvers to a track angle of 45^o, to a ground speed of 300 knots, or to a vertical speed of 0 feet per min. On the other hand, if the ownship maneuvers to any value in the green regions the aircraft will be conflict-free.

A pairwise prevention bands algorithm is *correct* if every possible value for the chosen parameter is either contained in a band or is a boundary point of one of the bands, and if the colors of the bands characterize conflict as follows. For all bands B and parameter values $x \in B$, the ownship's maneuver corresponding to the value x

is in conflict with the traffic aircraft if and only if the color of B is red. Equivalently, the ownship's maneuver corresponding to x is not in conflict if and only if the color of B is green.

Conflict prevention bands are surprisingly difficult to define and analyze [1]. The formal verification of a prevention bands algorithm for horizontal conflicts was described in [2]. Three-dimensional prevention bands algorithms were presented, without correctness proofs, in [3]. The 3-dimensional algorithms presented in that paper compute incorrect bands for some special cases. This paper presents *correct* versions of the prevention bands algorithms originally proposed in [3]. The correctness properties of these new algorithms have been formally verified in the Prototype Verification Systems (PVS) [4].

This paper focuses on pairwise algorithms, i.e., it considers only one traffic aircraft: the intruder. Prevention bands algorithms for an arbitrary number of traffic aircraft can be obtained from a pairwise algorithm by simply letting the red region for n-aircraft be the union of the red regions computed for the ownship and each individual traffic aircraft. The green regions can be computed as the complement of the red ones. The correctness of the algorithms for n-aircraft can be easily derived from the correctness of the pairwise prevention bands algorithms.

Notation

The mathematical development presented in this paper has been fully formalized in PVS.[1] However, for readability, this paper uses standard mathematical notation instead of PVS syntax.

Vector variables are written in **boldface** letters and can denoted by their components. For example, if $\mathbf{w} \in \mathbb{R}^3$ and $\mathbf{u} \in \mathbb{R}^2$, then $\mathbf{w} = (\mathbf{w}_x, \mathbf{w}_y, \mathbf{w}_z)$ and $\mathbf{u} = (\mathbf{u}_x, \mathbf{u}_y)$. The notation $\mathbf{w}_{(x,y)}$ denotes the projection of $\mathbf{w}$ in the horizontal plane, i.e.,[2]

$$\mathbf{w}_{(x,y)} \equiv (\mathbf{w}_x, \mathbf{w}_y),$$

and the notation $\mathbf{u}$ `with` $[z \leftarrow r]$ denotes the 3-dimensional vector whose projection to $\mathbb{R}^2$ is $\mathbf{u}$ and whose z-coefficient is $r \in \mathbb{R}$, i.e.,

$$\mathbf{u} \texttt{ with } [z \leftarrow r] \equiv (\mathbf{u}_x, \mathbf{u}_y, r).$$

As usual, the notation $\|\mathbf{w}\|$ refers to the norm of the vector $\mathbf{w}$ and the notation $\mathbf{w} \cdot \mathbf{w}'$ refers to the dot product of the vectors $\mathbf{w}$ and $\mathbf{w}'$. The expression $\mathbf{0}$ represents the zero vector, e.g., the vector whose components are 0.

If $\mathbf{u} \in \mathbb{R}^2$, then $\mathbf{u}^\perp$ denotes the (right) perpendicular vector:

$$\mathbf{u}^\perp \equiv (\mathbf{u}_y, -\mathbf{u}_x).$$

From this definition, it can be easily proven that $\mathbf{u} \cdot \mathbf{u}^\perp = 0$. Furthermore, if $\mathbf{u}$ is nonzero, then the vector $\mathbf{w} \in \mathbb{R}^2$ can be written as a linear combination of $\mathbf{u}$ and $\mathbf{u}^\perp$ in the following way:

$$\mathbf{w} = \frac{1}{\|\mathbf{u}\|^2}((\mathbf{u} \cdot \mathbf{w})\,\mathbf{u} + (\mathbf{u}^\perp \cdot \mathbf{w})\,\mathbf{u}^\perp). \tag{1}$$

[1] Electronically avaialable from http://shemesh.larc.nasa.gov/people/cam/ACCoRD.

[2] The symbol $\equiv$ is used in this paper to introduce mathematical definitions.

The function sign: $\mathbb{R} \mapsto \{-1, 1\}$ is defined such that $\text{sign}(x) = 1$ if $x \geq 0$ and $\text{sign}(x) = -1$ otherwise. As usual in mathematics, $\iota = \pm 1$ denotes the fact that an integer ι belongs to the set $\{-1, 1\}$. Moreover, $\neg$, $\implies$, $\iff$ denote logical negation, implication, and equivalence, respectively.

Finally, by convention, names of predicates and functions used in the specification of the problem are written in *italics*. Functions that represent algorithms to be implemented in a programming language are written in `typewriter` font.

2 Statement of the Problem

The prevention bands algorithms discussed here only use state-based information for the two aircraft, i.e., constant position and velocity vectors that are elements of the 3-dimensional Euclidean space $\mathbb{R}^3$. Aircraft dynamics are represented by a point moving at constant linear speed. These approximations of real aircraft behavior are valid for short lookahead times (typically less than 5 minutes). The current state of the ownship and traffic aircraft are denoted by the following vectors.

$\mathbf{s}_o \in \mathbb{R}^3$	Initial position of the ownship aircraft
$\mathbf{v}_o \in \mathbb{R}^3$	Initial velocity of the ownship aircraft
$\mathbf{s}_i \in \mathbb{R}^3$	Initial position of the traffic aircraft
$\mathbf{v}_i \in \mathbb{R}^3$	Initial velocity of the traffic aircraft

In the airspace system, the separation criterion for two aircraft is specified as a minimum horizontal separation D and a minimum vertical separation H. A conflict between the ownship and the intruder occurs when there is a time in the future, within a lookahead time T, such that the horizontal distance between the aircraft is less than D, and the vertical distance is less than H. Typically, D is 5 nautical miles, H is 1000 feet, and T is 5 minutes.

For the remainder of the paper, it is assumed that the ground speeds of the ownship and intruder aircraft are not zero, i.e., both $\|\mathbf{v}_{o(x,y)}\| \neq 0$ and $\|\mathbf{v}_{i(x,y)}\| \neq 0$ hold, and that the aircraft are not in loss of separation, i.e., either $\|\mathbf{s}_{o(x,y)} - \mathbf{s}_{i(x,y)}\| \geq D$ or $|\mathbf{s}_{oz} - \mathbf{s}_{iz}| \geq H$ hold. Therefore,

$$\begin{aligned} \mathbf{v}_{o(x,y)} &\neq \mathbf{0}, \\ \mathbf{v}_{i(x,y)} &\neq \mathbf{0}, \\ \mathbf{s}_o - \mathbf{s}_i &\neq \mathbf{0}. \end{aligned}$$

As noted in the introduction, the possible maneuvers considered for the ownship are constrained to those where only one parameter of the ownship's velocity vector is varied, e.g., track angle, ground speed, or vertical speed.

2.1 Conflicts

The ownship and the intruder aircraft are in conflict if there exists $t \in [0, T]$ such that, at time t, vertical separation is lost, i.e,

$$|((\mathbf{s}_o + t\,\mathbf{v}_o) - (\mathbf{s}_i + t\,\mathbf{v}_i))_z| < H,$$

and horizontal separation is lost, i.e.,

$$\|(\mathbf{s}_o + t\,\mathbf{v}_o)_{(x,y)} - (\mathbf{s}_i + t\,\mathbf{v}_i)_{(x,y)}\| < D.$$

Since $(\mathbf{s}_o+t\,\mathbf{v}_o)-(\mathbf{s}_i+t\,\mathbf{v}_i) = (\mathbf{s}_o-\mathbf{s}_i)+t\,(\mathbf{v}_o-\mathbf{v}_i)$, the predicate that characterizes conflict can be defined on $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$, the relative position and velocity vector, respectively, of the ownship with respect to the intruder.

That is, conflict can be viewed as a predicate of two vectors $\mathbf{s}$ and $\mathbf{v}$ rather than a predicate of four vectors $\mathbf{s}_o$, $\mathbf{v}_o$, $\mathbf{s}_i$, and $\mathbf{v}_i$, a result that greatly simplifies the notation. Thus, the predicate *conflict?* can be formally defined as follows.

$$\begin{aligned} \textit{conflict?}(\mathbf{s},\mathbf{v}) \equiv \exists t \in [0,T] : |(\mathbf{s}+t\,\mathbf{v})_z| < H \text{ and} \\ \|\mathbf{s}_{(x,y)} + t\,\mathbf{v}_{(x,y)}\| < D. \end{aligned} \tag{2}$$

For the remainder of this paper, the relative position and velocity vectors, $\mathbf{s}$ and $\mathbf{v}$, will be used in place of $\mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v}_o - \mathbf{v}_i$, respectively.

The separation criterion can be understood as an imaginary cylinder of height H and diameter D around each aircraft and a conflict between two aircraft as a future overlapping of these cylinders. In this paper, an alternative but equivalent view is considered where the intruder is surrounded by a cylinder, called *protected zone*, of half-height H and radius D. From this perspective, a conflict between these two aircraft is equivalent to the existence of a time $t \in [0,T]$ at which the ownship is in the interior of the intruder's protected zone.

2.2 Track Angle, Ground Speed, and Vertical Speed Maneuvers

A *maneuver* for the ownship is a new velocity vector $\mathbf{v}'_o$ that is implemented by the aircraft in zero time. Track angle, ground speed, and vertical speed maneuvers are formally defined as follows.

- A *track angle maneuver* for the ownship is a velocity vector $\mathbf{v}'_o$ such that $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$ and $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$. In this case, there exists a function $\texttt{track}\colon \mathbb{R}^3 \mapsto \mathbb{R}$ that computes a real number $\alpha = \texttt{track}(\mathbf{v}'_o)$, called the *track angle* of $\mathbf{v}'_o$, such that

  $$\mathbf{v}'_{o(x,y)} = (\|\mathbf{v}_{o(x,y)}\| \sin\alpha, \|\mathbf{v}_{o(x,y)}\| \cos\alpha).$$

  The function `track` is easily defined using the arc tangent function and the signs of $\mathbf{v}'_{ox}$ and $\mathbf{v}'_{oy}$.

- A *ground speed maneuver* for the ownship is a velocity vector $\mathbf{v}'_o$ such that $\mathbf{v}'_{o(x,y)}$ and $\mathbf{v}_{o(x,y)}$ are parallel (have the same track angle) and $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$. In this case, there exists a real number p with the property that

  $$\mathbf{v}'_o = (\frac{p}{\|\mathbf{v}_{o(x,y)}\|}\mathbf{v}_{ox}, \frac{p}{\|\mathbf{v}_{o(x,y)}\|}\mathbf{v}_{oy}, \mathbf{v}_{oz}).$$

  The number p is the *ground speed* of $\mathbf{v}_o$, i.e., $\|\mathbf{v}'_{o(x,y)}\| = p$.

- A *vertical speed maneuver* for the ownship is a velocity vector $\mathbf{v}'_o$ such that $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$, i.e., the horizontal velocity vectors are equal. In this case, there exists a real number r, called the *vertical speed* of $\mathbf{v}'_o$ such that

$$\mathbf{v}'_o = (\mathbf{v}_{ox}, \mathbf{v}_{oy}, r).$$

The functions $\nu_{\text{trk}}, \nu_{\text{gs}}, \nu_{\text{vs}} \colon \mathbb{R} \mapsto \mathbb{R}^3$, implicitly parametrized by $\mathbf{v}_o$, are defined as follows.

$$\nu_{\text{trk}}(\alpha) \equiv (\|\mathbf{v}_{o(x,y)}\| \sin\alpha, \|\mathbf{v}_{o(x,y)}\| \cos\alpha, \mathbf{v}_{oz}), \tag{3}$$

$$\nu_{\text{gs}}(p) \equiv (\frac{p}{\|\mathbf{v}_{o(x,y)}\|}\mathbf{v}_{ox}, \frac{p}{\|\mathbf{v}_{o(x,y)}\|}\mathbf{v}_{oy}, \mathbf{v}_{oz}), \tag{4}$$

$$\nu_{\text{vs}}(r) \equiv (\mathbf{v}_{ox}, \mathbf{v}_{oy}, r), \tag{5}$$

These functions assign to each track angle $\alpha \in \mathbb{R}$, ground speed $p \in \mathbb{R}$, and vertical speed $r \in \mathbb{R}$, respectively, the corresponding velocity vector for the ownship. Important properties of the functions ν_{trk}, ν_{gs}, and ν_{vs} are:

$$\|\nu_{\text{trk}}(\alpha)_{(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|, \tag{6}$$

$$\|\nu_{\text{gs}}(p)_{(x,y)}\| = p, \tag{7}$$

$$\nu_{\text{vs}}(r)_z = r. \tag{8}$$

The constructions in this paper will restrict ground speed maneuvers to those where the ground speed p is positive.

2.3 Conflict Detection Algorithm

A *conflict detection* algorithm `cd` is a function that takes as parameters the relative position of the aircraft $\mathbf{s}$ and the velocity vectors $\mathbf{v}_o$, $\mathbf{v}_i$, and returns a Boolean value, i.e., `True` or `False`.

Definition 1. *The algorithm* `cd` *is* correct *if it holds that*

$$\textit{conflict?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) \implies \texttt{cd}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i).$$

It is `cd` *is* complete *if it holds that*

$$\texttt{cd}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i) \implies \textit{conflict?}(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i).$$

In other words, a conflict detection algorithm is correct if it does not have missed alerts, i.e., it detects all conflicts, and it is complete if it does not have false alerts, i.e., it only detects actual conflicts. Note that a conflict detection algorithm $\texttt{cd}_\texttt{T}$ that always returns `True` is correct and an algorithm $\texttt{cd}_\texttt{F}$ that always returns `False` is complete. However, $\texttt{cd}_\texttt{T}$ is not complete and $\texttt{cd}_\texttt{F}$ is not correct. An example of a correct *and* complete conflict detection algorithm is `cd3d` (see Appendix in [3]).

2.4 Prevention Bands Algorithms

Given a function $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$ and a closed interval $I = [I_1, I_2]$, a *prevention bands algorithm* for ν over I is a function with parameters $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$ that returns a finite, ordered sequence L_ν of elements of I, such that $I_1 \in L_\nu$ and $I_2 \in L_\nu$. Each consecutive pair A and B of entries in L_ν determines an open interval (A, B), which is called a *band* (for the parameter represented by ν).

By abuse of notation, the syntax $(A, B) \in L_\nu$ will denote that (A, B) is a band in L_ν, i.e., A and B are consecutive entries in L_ν.

Definition 2. *Given a function $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$ and a closed interval $I \subset \mathbb{R}$, a prevention bands algorithm for ν over I is* correct *if for any band (A, B) in L_ν and real numbers $x, y \in (A, B)$, it holds that*

$$\textit{conflict?}(\mathbf{s}, \nu(x) - \mathbf{v}_i) \iff \textit{conflict?}(\mathbf{s}, \nu(y) - \mathbf{v}_i).$$

The definition above states that all the points in a band computed by a correct prevention bands algorithm have the same conflict property, e.g., either all the points yield conflict-free maneuvers or all the points yield maneuvers that lead to conflict. Typically, ν will be one of the functions ν_{trk}, ν_{gs}, or ν_{vs} defined in formulas (3), (4), and (5). The boundaries I_1 and I_2, of the interval I, are minimum and maximum values for the argument of ν. For $\nu = \nu_{\text{trk}}$, the standard values are $I_1 = 0$ and $I_2 = 2\pi$. For $\nu = \nu_{\text{gs}}$ and $\nu = \nu_{\text{vs}}$, I_1 and I_2 are typically the minimum and maximum ground or vertical speeds for the ownship, respectively.

To each band (A, B) in L_ν, a color is associated as follows:

$$\begin{aligned}
&\texttt{color}(\mathbf{s}, \mathbf{v}_i, A, B) \equiv \\
&\quad \texttt{if cd}(\mathbf{s}, \nu(\frac{A+B}{2}), \mathbf{v}_i)\ \texttt{then} \\
&\qquad \texttt{Red} \\
&\quad \texttt{else} \\
&\qquad \texttt{Green} \\
&\quad \texttt{endif}
\end{aligned} \tag{9}$$

where `cd` is any correct conflict detection algorithm, such as `cd3d`.

The following theorem can be easily proven from Definition 2.

Theorem 1. *Given a function $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$ and a closed interval $I \subset \mathbb{R}$, a prevention bands algorithm for ν is correct if and only if for any band (A, B) in L_ν,*

$$\texttt{color}(\mathbf{s}, \mathbf{v}_i, A, B) = \texttt{Red} \iff \forall y \in (A, B) : \textit{conflict?}(\mathbf{s}, \nu(y) - \mathbf{v}_i), \textit{and} \tag{10}$$

$$\texttt{color}(\mathbf{s}, \mathbf{v}_i, A, B) = \texttt{Green} \iff \forall y \in (A, B) : \neg\textit{conflict?}(\mathbf{s}, \nu(y) - \mathbf{v}_i). \tag{11}$$

The relation between a graphical display such as in Figure 1 and the output of a prevention bands algorithm can be illustrated by considering the track angle display, that is, where $\nu = \nu_{\text{trk}}$ and $I = [0, 2\pi]$. A prevention bands algorithm for track angle will return a finite, ordered sequence $L_{\nu_{\text{trk}}}$ of track angles in the interval $[0, 2\pi]$. This sequence will contain both of the angles 0 and 2π. If the algorithm is correct, then each consecutive pair, α and β, of track angles in this sequence defines a band, i.e., an open interval (α, β), with the property that either

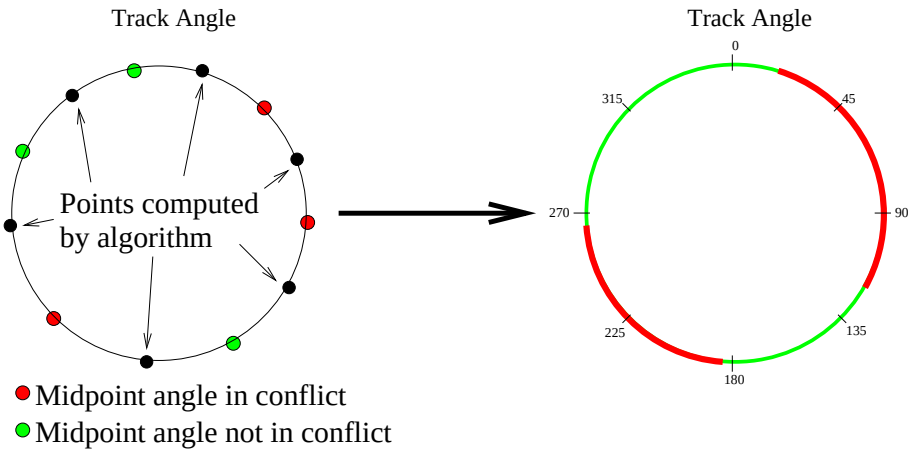

Figure 2. Relation between track angle prevention bands algorithm and graphical display

1. all track angles between α and β result in conflict, or

2. all track angles between α and β do not result in conflict.

If the track angles between α and β all result in conflict, the region between α and β is colored red. Otherwise, this region is colored green. The color of each such region is determined by conflict information at the midpoint $\frac{\alpha+\beta}{2}$. This is illustrated by Figure 2.

2.5 Proving Correctness of a Prevention Bands Algorithm

This section provides a general strategy that can be followed to formally verify that a given prevention bands algorithm is correct. Subsequent sections will describe the use of this strategy in the formal verification of prevention bands algorithms for track angle, ground speed, and vertical speed.

Recall that a prevention bands algorithm depends on a function $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$, (e.g. $\nu = \nu_{\text{trk}}$), and a closed interval $I = [I_1, I_2]$. Thus, a real-valued argument x of the function ν is understood as a parameter of the ownship's velocity vector, and the value $\nu(x)$ is the corresponding velocity vector for that parameter. The following theorem can be used to verify the correctness of a prevention bands algorithm for ν over I.

Theorem 2. *Let L_ν be a finite sequence computed by a prevention bands algorithm for ν over an interval I and let $\Omega_\nu\colon \mathbb{R} \mapsto \mathbb{R}$ be a* continuous *function, implicitly parametrized by* $\mathbf{s}$ *and* $\mathbf{v}_i$*, such that*

1. *Ω_ν characterizes conflict? in the following way:*

$$\Omega_\nu(x) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu(x) - \mathbf{v}_i), \textit{ and} \tag{12}$$

2. *L_v is Ω_ν-complete: For all real value $x \in I$,*

$$\Omega_\nu(x) = 1 \implies x \in L_\nu, \tag{13}$$

then the algorithm that computes L_ν is correct.

Proof. By Theorem 1, it suffices to prove that Formulas (10) and (11) hold. Let (A, B) be a band in L_ν.

- Suppose that $\texttt{color}(\mathbf{s}, \mathbf{v}_i, A, B) = \texttt{Red}$ and let y be a real number in the open interval (A, B). Suppose, by reduction to absurdity, that $\neg \mathit{conflict?}(\mathbf{s}, \nu(y) - \mathbf{v}_i)$. By Hypothesis 1, $\Omega_\nu(y) \geq 1$. However, by Hypothesis 2, since $(A, B) \in L_\nu$ and y is equal to neither A nor B, it follows that $\Omega_\nu(y) > 1$. By the definition of the function `color` given in Equation (9), it holds that $\mathit{conflict?}(\mathbf{s}, \nu(x) - \mathbf{v}_i)$, where $x = \frac{A+B}{2}$. Again by Hypothesis 1, $\Omega_\nu(x) < 1$. Since Ω_ν is continuous, the intermediate value theorem implies that there exists some z between x and y such that $\Omega_\nu(z) = 1$. Since z is therefore in the interval (A, B), A and B are consecutive in L_ν, and the algorithm computes all points where Ω_ν realizes a value of 1, this is a contradiction.

- Similar reasoning can be used to show that if $\texttt{color}(\mathbf{s}, \mathbf{v}_i, A, B) = \texttt{Green}$, then any y in (A, B) satisfies $\neg \mathit{conflict?}(\mathbf{s}, \nu(y) - \mathbf{v}_i)$.

□

3 The Function Ω

Using Theorem 2 to verify that a prevention bands algorithm is correct for track angle, ground speed, or vertical speed maneuvers, i.e., for the functions ν_{trk}, ν_{gs}, and ν_{vs}, will require finding three separate instantiations of the function Ω_ν that satisfies all the hypotheses of the theorem. This section proposes the definition of a function Ω that can be used to define Ω_ν for any $\nu \colon \mathbb{R} \mapsto \mathbb{R}^3$, where some of these hypotheses can be discharged once and for all.

Let $\Omega \colon \mathbb{R}^3 \mapsto \mathbb{R}^3$ be a continuous function, implicitly parametrized by $\mathbf{s}$ $(= \mathbf{s}_o - \mathbf{s}_i)$, that characterizes *conflict?* in the following way:

$$\Omega(\mathbf{v}) < 1 \iff \mathit{conflict?}(\mathbf{s}, \mathbf{v}). \tag{14}$$

For any continuous function ν, a continuous function $\Omega_\nu \colon \mathbb{R} \mapsto \mathbb{R}$ that satisfies Equation (12) can be defined as follows:

$$\Omega_\nu(x) \equiv \Omega(\nu(x) - \mathbf{v}_i). \tag{15}$$

Therefore, since functions ν_{trk}, ν_{gs}, and ν_{vs} are continuous, Formula (15) can be used to construct continuous functions $\Omega_{\nu_{\text{trk}}}$, $\Omega_{\nu_{\text{gs}}}$, and $\Omega_{\nu_{\text{vs}}}$ that satisfy Equation (12) in Theorem 2.

Given such a function Ω, the verification of correctness of a track angle, ground speed, and vertical speed prevention bands algorithms over an interval I can be

reduced to proving that L_ν, i.e., the sequence returned by each algorithm, is Ω_ν-complete, i.e., it contains all $x \in I$ where the function Ω_ν attains a value of 1. Since each of the algorithms will compute a sequence of values in a distinct way, a special proof of Ω_ν-completeness will be required for each algorithm that computes L_ν. The function Ω will be of use in this step as well. Indeed, the function Ω will be defined such that vectors $\mathbf{v}$ where $\Omega(\mathbf{v}) = 1$ have particular forms. The proof that L_ν is Ω_ν-complete, for $\nu \in \{\nu_{\text{trk}}, \nu_{\text{gs}}, \nu_{\text{vs}}\}$, will be done by proving that $x \in L_\nu$ if and only if the vector $\nu(x)$ has one of these forms.

The rest of this section concerns the definition of such a function Ω.

3.1 Cylindrical Distance

Recall from Section 2.1 that the protected zone is a cylinder around the intruder aircraft that has half-height H and radius D. In order to define the function Ω that satisfies Equation (14), a notion of cylindrical distance is needed.

Definition 3. *The* cylindrical length *of a vector* $\mathbf{w} \in \mathbb{R}^3$ *is the quantity*

$$\|\mathbf{w}\|_{cyl} \equiv \max\left(\frac{\|\mathbf{w}_{(x,y)}\|}{D}, \frac{|\mathbf{w}_z|}{H}\right).$$

Definition 4. *The* cylindrical distance *between two vectors,* $\mathbf{w}_1$ *and* $\mathbf{w}_2$*, is the quantity* $\|\mathbf{w}_1 - \mathbf{w}_2\|_{cyl}$.

Cylindrical distance is a metric on $\mathbb{R}^3$, in the sense of real analysis [5], and $\mathbb{R}^3$ is a metric space with this metric. In particular, this means that the triangle inequality holds for any $\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2 \in \mathbb{R}^3$:

$$\|\mathbf{w}_0 - \mathbf{w}_2\|_{\text{cyl}} \leq \|\mathbf{w}_0 - \mathbf{w}_1\|_{\text{cyl}} + \|\mathbf{w}_1 - \mathbf{w}_2\|_{\text{cyl}}. \tag{16}$$

The key property of cylindrical distance, as it relates to loss of separation of aircraft, is stated in the following theorem.

Theorem 3. *Two aircraft are in loss of separation if and only if* $\|\mathbf{s}\|_{cyl} < 1$*, where, as in Section 1,* $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ *is the relative position vector of the aircraft.*

3.2 The Definition of Ω

By Theorem 3, the ownship and the intruder aircraft are in conflict if and only if there exists some $t \in [0, T]$ such that $\|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} < 1$. Thus, for $\mathbf{s}$ such that $\|\mathbf{s}\|_{\text{cyl}} \neq 1$, i.e., for $\mathbf{s}$ not on the boundary of the protected zone, the function $\Omega(\mathbf{v})$ is defined as

$$\Omega(\mathbf{v}) \equiv \min_{t \in [0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}}. \tag{17}$$

Two important remarks on the definition of the function Ω given by Formula (17) are in order. First, the function Ω is well-defined since the quantity $\|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}}$ actually attains a minimum as t ranges over the interval $[0, T]$. That is, there exists some $\tau \in [0, T]$ such that $\|\mathbf{s}+\tau\,\mathbf{v}\|_{\text{cyl}} \leq \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}}$ for all $t \in [0, T]$. Indeed, when the vectors $\mathbf{s}$ and $\mathbf{v}$ are fixed, the function $d_{cyl}\colon [0, T] \mapsto \mathbb{R}$ defined by $d_{cyl}(t) = \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}}$

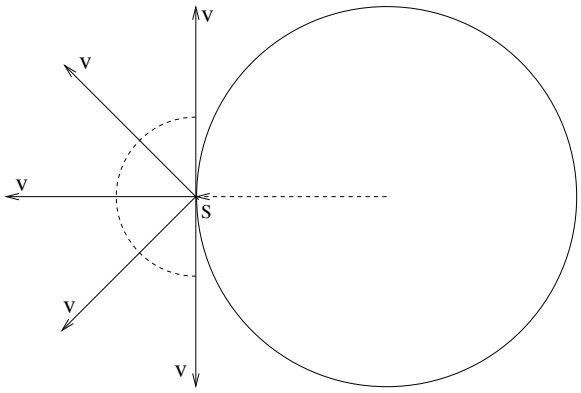

Figure 3. Infinite many places where $\min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} = 1$

is continuous, and every continuous function on a closed interval attains a minimum on that interval. The function d_{cyl} is continuous because it is the maximum of two functions, d_{horiz} and d_{vert}, defined by

$$d_{horiz}(t) \equiv \frac{\|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\|}{D},$$
$$d_{vert}(t) \equiv \frac{|(\mathbf{s} + t\,\mathbf{v})_z|}{H},$$

both of which are continuous.

Second, Formula (17) does not define Ω when $\|\mathbf{s}\|_{|cyl} = 1$. If $\|\mathbf{s}\|_{\text{cyl}} = 1$, in which case $\mathbf{s}$ is on the boundary of the cylinder, then any $\mathbf{v}$ which points outward from the cylinder will satisfy $\min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} = 1$. This is because the minimum is attained at $t = 0$ for any such $\mathbf{v}$. This is illustrated in Figure 3 in the case where $\|\mathbf{s}_{(x,y)}\| = D$ and $|\mathbf{s}_z| < H$. Therefore, if $\|\mathbf{s}\|_{\text{cyl}} = 1$, there is an infinite number of vectors $\mathbf{v}$ such that $\min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} = 1$. Defining Ω in this case using Formula (17) would make the proof that L_ν is Ω_ν-complete impossible, as by definition of a prevention bands algorithm the sequence L_ν is *finite*.

While this shows that some care is needed when defining Ω on the boundary of the cylinder, it is possible to define Ω so that

1. it satisfies Equation (12),
2. it is continuous, and
3. it is suitable for showing that a sequence L_ν is Ω_ν-complete.

$$\Omega(\mathbf{v}) \equiv \begin{cases} \mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} & \text{if } \|\mathbf{s}_{(x,y)}\| = D \text{ and } |\mathbf{s}_z| < H \\ \mathbf{s}_z \mathbf{v}_z & \text{if } \|\mathbf{s}_{(x,y)}\| < D \text{ and } |\mathbf{s}_z| = H \\ \max(\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)}, \mathbf{s}_z \mathbf{v}_z) & \text{if } \|\mathbf{s}_{(x,y)}\| = D \text{ and } |\mathbf{s}_z| = H \\ \min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} & \text{otherwise, i.e., if } \|\mathbf{s}\|_{\text{cyl}} \neq 1 \end{cases} \tag{18}$$

The following theorem is a basic exercise in vector algebra.

Theorem 4. *conflict?*$(\mathbf{s}, \mathbf{v}) \iff \Omega(\mathbf{v}) < 1$.

The formal proof that Ω is continuous requires more work and it is explained in the rest of this section. Section 4 provides a classification theorem for Ω, which is used then used in sections 5-7 to show that the sequences L_ν, for $\nu \in \{\nu_{\text{trk}}, \nu_{\text{gs}}, \nu_{\text{vs}}\}$, computed by the proposed prevention bands algorithms, are Ω_ν-complete.

3.3 Continuity of Ω

Since the if-statements in the definition of Ω do not depend on $\mathbf{v}$, Ω is continuous if and only if each of the quantities $\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)}$, $\mathbf{s}_z \mathbf{v}_z$, $\max(\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)}, \mathbf{s}_z \mathbf{v}_z)$, and $\min_{t\in[0,T]} \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}}$ are continuous functions of $\mathbf{v}$. Only one of these four statements is nontrivial, that the minimum $\min_{t\in[0,T]} \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}}$ is continuous in $\mathbf{v}$. This can be proved with standard techniques from real analysis [5]. In fact, it follows from a generalization of the Heine-Cantor theorem, which says that a continuous function on a closed interval is uniformly continuous. In particular, the following theorem has been proved.

Theorem 5. *If A and B are real numbers with $A < B$ and $f\colon [A,B] \times \mathbb{R}^n \mapsto \mathbb{R}$ is continuous, then the function $g\colon \mathbb{R}^n \mapsto \mathbb{R}$ defined by $g(\mathbf{v}) \equiv \min_{t\in[A,B]} f(t,\mathbf{v})$ is continuous.*

The formal proof of this theorem required the development of a vector analysis library in PVS, which is now part of the PVS NASA Libraries.[3]

The continuity of Ω is a direct consequence of Theorem 5, when $A = 0$, $B = T$, and $f(t,\mathbf{v}) = \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}}$.

Theorem 6. *The function Ω is continuous.*

The purpose for constructing the function Ω was to provide a definition for $\Omega_\nu\colon \mathbb{R} \mapsto \mathbb{R}$ for every function $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$. The following corollaries follow directly from theorems 4 and 6.

Corollary 7. *For any $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$, the function Ω_ν, defined in Equation (15), satisfies $\Omega_\nu(x) < 1$ if and only if conflict?$(\mathbf{s}, \nu(x) - \mathbf{v}_i)$.*

Corollary 8. *If $\nu\colon \mathbb{R} \mapsto \mathbb{R}^3$ is continuous, then the function Ω_ν is continuous.*

Since functions ν_{trk}, ν_{gs}, and ν_{vs} are continuous, corollaries 7 and 8 hold for $\Omega_{\nu_{\text{trk}}}$, $\Omega_{\nu_{\text{gs}}}$, and $\Omega_{\nu_{\text{vs}}}$.

4 Classification of Critical Vectors

To verify the correctness of a prevention bands algorithm for ν over a closed interval I, it must be shown that the computed sequence L_ν is finite and includes all points $x \in I$ such that $\Omega(\nu(x) - \mathbf{v}_i) = 1$. Vectors $\mathbf{v}$ that satisfy $\Omega(\mathbf{v}) = 1$ are called *critical vectors*. This section shows that critical vectors can be analytically classified in a finite way.

[3]The PVS NASA Libraries are available from http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html.

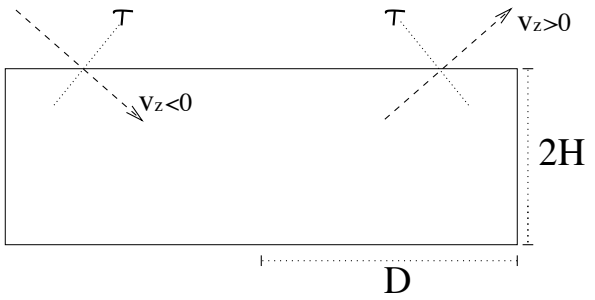

Figure 4. Case $\mathbf{v}_z \neq 0$, $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| < D$

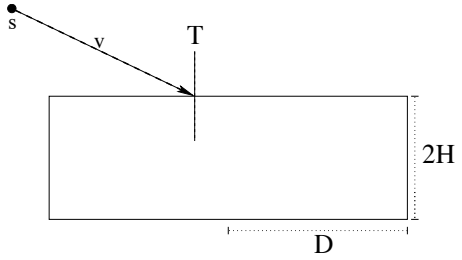

Figure 5. Case $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + T\,\mathbf{v})_{(x,y)}\| < D$

Consider a relative position vector $\mathbf{s}$ that satisfies $\|\mathbf{s}\|_{\text{cyl}} \neq 1$ and a critical vector $\mathbf{v}$. Since $\Omega(\mathbf{v}) = 1$, it holds that $\min_{t\in[0,T]} \|\mathbf{s}+t\,\mathbf{v}\|_{\text{cyl}} = 1$. This minimum is attained at a real number $\tau \in [0, T]$. Since $\|\mathbf{s}\|_{\text{cyl}} \neq 1$, it follows that $\tau \neq 0$. Thus, either $\tau = T$ or $0 < \tau < T$. If it holds that $\mathbf{v}_z \neq 0$, $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + \tau\mathbf{v})_{(x,y)}\| < D$, then it can be shown that $\min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} < 1$. That is, there is a time near τ where the aircraft will be in loss of separation. This is illustrated in Figure 4.

If the same conditions hold, but with $\mathbf{v}_z = 0$, then τ is not unique, and it can also be shown that a particular τ can be chosen so that $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$.

Since, $1 = \Omega(\mathbf{v}) = \|\mathbf{s} + \tau\,\mathbf{v}\|_{\text{cyl}} = \max(\frac{\|(\mathbf{s}+\tau\,\mathbf{v})_{(x,y)}\|}{D}, \frac{|\mathbf{s}_z+\tau\,\mathbf{v}_z|}{H})$, this leaves the following cases.

1. Case $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + T\,\mathbf{v})_{(x,y)}\| < D$.
2. Case $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| < H$, and $\|(\mathbf{s} + T\,\mathbf{v})_{(x,y)}\| = D$.
3. Case $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$ and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$.
4. Case $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| < H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$.

These four cases are illustrated in figures 5, 6, 7, and 8, respectively.

These cases will be formalized using four predicates: *vertical_case?* (Section 4.1), *circle_case_2D?* (Section 4.2), *circle_case_3D?* (Section 4.3), and *line_case?* (Section 4.4). It will be shown in Section 4.5 that these four predicates are sufficient to classify solutions to the equation $\Omega(\mathbf{v}) = 1$, even in the case where $\|\mathbf{s}\|_{\text{cyl}} = 1$.

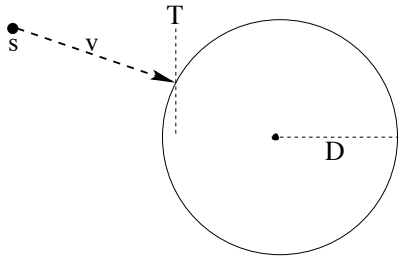

Figure 6. Case $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| < H$, and $\|(\mathbf{s} + T\,\mathbf{v})_{(x,y)}\| = D$

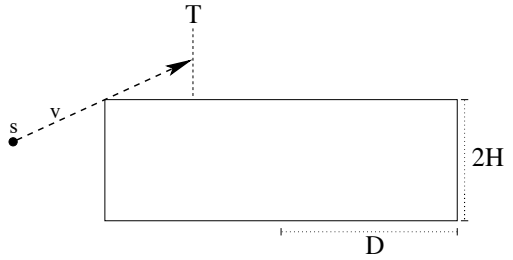

Figure 7. Case $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$

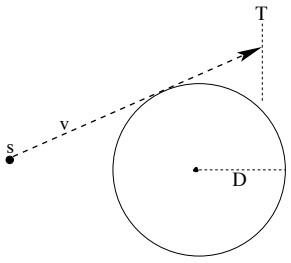

Figure 8. Case $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| < H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$

4.1 Vertical Case

Consider the case 1 where $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| = H$, and $\|(\mathbf{s}+T\,\mathbf{v})_{(x,y)}\| < D$, which is illustrated by Figure 5. In this case, if $(\mathbf{s}_z + T\,\mathbf{v}_z)\,\mathbf{v}_z > 0$, it can be formally proven that there is some $t \in (0, T)$ such that $\|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} < 1$, which is a contradiction. This motivates the definition of the following predicate on $\mathbf{s}_z$, $\mathbf{v}_z$, a real number t, and an integer $\iota = \pm 1$.

$$\begin{aligned} \textit{vertical\_case?}(\mathbf{s}_z, \mathbf{v}_z, t, \iota) \equiv |\mathbf{s}_z + t\,\mathbf{v}_z| = H \text{ and} \\ \iota\ (\mathbf{s}_z + t\,\mathbf{v}_z)\,\mathbf{v}_z \geq 0. \end{aligned} \tag{19}$$

Intuitively, the number ι can be thought of as direction, with $\iota = -1$ corresponding to entry into the protected zone at time t, and $\iota = 1$ corresponding to exit.

Case 1 corresponds to *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$. The condition

$$\|(\mathbf{s} + T\,\mathbf{v})_{(x,y)}\| < D$$

is explicitly not included in this predicate, because the more general form is useful when classifying other types of critical vectors. It is important to note that if $|\mathbf{s}_z + T\,\mathbf{v}_z| = H$, then *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, \iota)$ holds for some $\iota = \pm 1$.

Vectors $\mathbf{v}$ that satisfy the predicate *vertical_case?* are called *vertical solutions*.

4.2 Circle Case 2D

Consider the case 2 where $\tau = T$, $|\mathbf{s}_z + T\,\mathbf{v}_z| < H$, and $\|(\mathbf{s}+T\,\mathbf{v})_{(x,y)}\| = D$, which is illustrated by Figure 6. If $(\mathbf{s}_{(x,y)} + T\,\mathbf{v}_{(x,y)}) \cdot \mathbf{v}_{(x,y)} > 0$, then it can be formally proven that there is some $t \in (0, T)$ such that $\|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} < 1$, which is a contradiction. This motivates the definition of the following predicate on $\mathbf{s}$, $\mathbf{v}$, a real number t, and $\iota = \pm 1$.

$$\begin{aligned} \textit{circle\_case\_2D?}(\mathbf{s}, \mathbf{v}, t, \iota) \equiv \|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\| = D \text{ and} \\ \iota\ (\mathbf{s}_{(x,y)} + t\,\mathbf{v}_{(x,y)}) \cdot \mathbf{v}_{(x,y)} \geq 0. \end{aligned} \tag{20}$$

Case 2 corresponds to *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, T, -1)$. The condition

$$|\mathbf{s}_z + T\,\mathbf{v}_z| < H$$

is not included in this predicate, because it will be used, along with *vertical_case?*, to classify other types of critical vectors. As for the predicate *vertical_case?* above, an important property of *circle_case_2D?* is that $\|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\| = D$ implies that *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$ holds for some $\iota = \pm 1$.

Vectors $\mathbf{v}$ that satisfy the predicate *circle_case_2D?* are called *2D circle solutions*.

4.3 Circle Case 3D

Consider the case 3 where $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$ and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$, which is illustrated by Figure 7. It follows from the definitions of *vertical_case?* and *circle_case_2D?* that there exists ι_1, ι_2, each equal to -1 or 1, such that *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, \tau, \iota_1)$ and *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, \tau, \iota_2)$. If τ is positive and $\iota_1 = \iota_2$, it can be proven that either

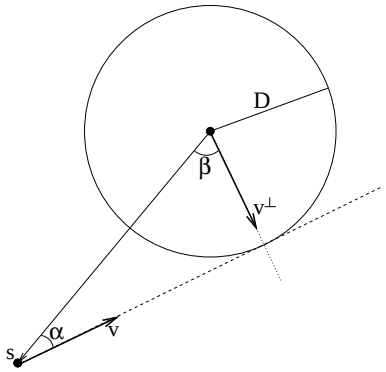

Figure 9. Line case: $\mathbf{v}$ is tangent to the circle

vertical_case?$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$ or $\Omega(\mathbf{v}) < 1$. In classifying the solutions to the equation $\Omega(\mathbf{v}) = 1$, the case where *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$ is true is handled separately. Since it holds that $\Omega(\mathbf{v}) = 1$, a requirement for the case where $|\mathbf{s}_z + \tau\,\mathbf{v}_z| = H$ and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$ is therefore that $\iota_1 = -\iota_2$. This motivates the definition of the following predicate. Similar to the predicate *circle_case_2D?*, this predicate depends on $\mathbf{s}$, $\mathbf{v}$, $\iota = \pm 1$, and a real number t.

$$\begin{aligned} \textit{circle\_case\_3D?}(\mathbf{s}, \mathbf{v}, t, \iota) \equiv\ & t > 0 \text{ and} \\ & \textit{circle\_case\_2D?}(\mathbf{s}, \mathbf{v}, t, \iota) \text{ and} \\ & \textit{vertical\_case?}(\mathbf{s}_z, \mathbf{v}_z, t, -\iota). \end{aligned} \tag{21}$$

Vectors $\mathbf{v}$ that satisfy the predicate *circle_case_3D?* are called *3D circle solutions.*

4.4 Line Case

Consider the case 4 where $0 < \tau < T$, $|\mathbf{s}_z + \tau\,\mathbf{v}_z| < H$, and $\|(\mathbf{s} + \tau\,\mathbf{v})_{(x,y)}\| = D$, which is illustrated by Figure 8. As Figure 9 indicates, the fact that τ satisfies $\min_{t\in[0,T]} \|\mathbf{s} + t\,\mathbf{v}\|_{\text{cyl}} = \|\mathbf{s} + \tau\,\mathbf{v}\|_{\text{cyl}}$ can be used to show that the trajectory from $\mathbf{s}_{(x,y)}$ along $\mathbf{v}_{(x,y)}$ is tangent to the circle of radius D around the origin. In this figure, the vector $\mathbf{v}^\perp$ is the vector $(v_y, -v_x, \mathbf{v}_z)$.

It is immediately clear from Figure 9 that the angle α can be no greater than $\pi/2$. Since $\mathbf{s}_{(x,y)} \cdot -\mathbf{v}_{(x,y)} = \|\mathbf{s}_{(x,y)}\|\|\mathbf{v}_{(x,y)}\| \cos\alpha \geq 0$, it follows that $\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} \leq 0$. In addition, $\cos\beta = \frac{D}{\|\mathbf{s}_{(x,y)}\|}$. Thus,

$$\begin{aligned} \mathbf{s}_{(x,y)} \cdot \mathbf{v}^\perp{}_{(x,y)} &= \|\mathbf{s}_{(x,y)}\|\|\mathbf{v}_{(x,y)}\| \cos\beta \\ &= D\|\mathbf{v}_{(x,y)}\|. \end{aligned} \tag{22}$$

This construction depends on a vector $\mathbf{v}_{(x,y)}$ that is tangent to the right side of the circle. The analogous construction for a vector $\mathbf{v}_{(x,y)}$ that is tangent to the left side of the circle would use $-\mathbf{v}^\perp$ in the place of the vector $\mathbf{v}^\perp$. This motivates

the definition of the following predicate, which depends on $\mathbf{s}$, $\mathbf{v}$, and a parameter ε, which is equal to either -1 for a right-tangent, or 1 for a left-tangent.

$$\begin{aligned} \textit{line\_case?}(\mathbf{s}, \mathbf{v}, \varepsilon) \equiv \mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} \leq 0 \text{ and} \\ -\varepsilon\ (\mathbf{s}_{(x,y)} \cdot \mathbf{v}^{\perp}{}_{(x,y)}) = D\|\mathbf{v}_{(x,y)}\|. \end{aligned} \tag{23}$$

Vectors $\mathbf{v}$ that satisfy the predicate *line_case?* are called *line solutions.*

4.5 The Classification Theorem

Critical vectors can be classified according to the following theorem.

Theorem 9. *If $\Omega(\mathbf{v}) = 1$, then one of the following conditions holds.*

1. $\|\mathbf{s}_{(x,y)}\| \geq D$ *and* *line_case?*$(\mathbf{s}, \mathbf{v}, \iota)$ *holds for some* $\iota = \pm 1$.
2. $|\mathbf{s}_z + T\,\mathbf{v}_z| < H$ *and* *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, T, -1)$
3. *There exists a real number* $t > 0$ *such* *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$ *holds for some* $\iota = \pm 1$.
4. $\|\mathbf{s}_{(x,y)} + T\,\mathbf{v}_{(x,y)}\| \leq D$ *and* *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$

This theorem can be used to show that a sequence L_ν computed by a prevention bands algorithm is Ω_ν-complete by proving that L_ν contains all the vectors that have one of the four forms. It follows from this that L_ν contains all points $x \in I$ such that $\Omega_\nu(x) = 1$. When applying this technique to the case of track angle, ground speed, and vertical speed bands, it is still possible to find a few special cases where there are infinitely many points in I at which Ω_ν attains a value of 1. These cases are handled separately by defining special versions of Ω_ν that avoid this problem.

Section 4.6 defines functions Θ_H and Θ_D that compute the times where the aircraft lose vertical separation and horizontal separation, respectively, and illustrates the relation between these times and the four cases in the classification theorem (Theorem 9). The functions Θ_D and Θ_H will be used to define prevention bands algorithms for track angle, ground speed, and vertical speed maneuvers in sections 5, 6, and 7, respectively.

4.6 Entry and Exit Times

In Figure 5, the time t at which the trajectory from $\mathbf{s}$ along $\mathbf{v}$ enters the protected zone vertically, i.e., where $(\mathbf{s}+t\,\mathbf{v})_z = \pm H$, is precisely T. In Figure 6, the trajectory first touches the circle of radius D around the origin at time T. In Figure 7, the time at which this trajectory enters the circle is precisely the time where its z-component exits the interval $[-H, H]$. In Figure 8, the trajectory is tangent to the circle, so the time where the trajectory first touches the circle is equal to the time where the trajectory last touches the circle.

All this indicates that there are relationships between the predicates defined in sections 4.1 to 4.4 and the following quantities:

- the times where the z-component of the trajectory from $\mathbf{s}$ along $\mathbf{v}$ enters and exits the interval $[-H, H]$, and
- the times where the 2-dimensional trajectory from $\mathbf{s}_{(x,y)}$ along $\mathbf{v}_{(x,y)}$ enters and exits the circle of radius D around the origin.

This section gives precise definitions of mathematical functions that compute these times and gives a variant of Theorem 9 that uses them.

The times where the z-component of the trajectory from $\mathbf{s}$ along $\mathbf{v}$ enters and exits the interval $[-H, H]$ are real numbers t such that $|\mathbf{s}_z + t\,\mathbf{v}_z| = H$. This motivates the definition of the following function.

$$\Theta_H(\mathbf{s}_z, \mathbf{v}_z, \iota) \equiv \frac{\iota\ sign(\mathbf{v}_z)\,H - \mathbf{s}_z}{\mathbf{v}_z}, \text{ for } \mathbf{v}_z \neq 0, \tag{24}$$

where the number ι is ± 1. It is easy to check that $|\mathbf{s}_z + \Theta_H(\mathbf{s}_z, \mathbf{v}_z, \iota)\,\mathbf{v}_z| = H$. In addition,

$$\Theta_H(\mathbf{s}_z, \mathbf{v}_z, -1) < \Theta_H(\mathbf{s}_z, \mathbf{v}_z, 1). \tag{25}$$

Intuitively, the times $\Theta_H(\mathbf{s}_z, \mathbf{v}_z, -1)$ and $\Theta_H(\mathbf{s}_z, \mathbf{v}_z, 1)$ are the times at which the z-component of the trajectory from $\mathbf{s}$ along $\mathbf{v}$ enters and exits the interval $[-H, H]$, respectively. It can be proved from definitions that $\iota\,(\mathbf{s}_z + \Theta_H(\mathbf{s}_z, \mathbf{v}_z, \iota)\,\mathbf{v}_z)\,\mathbf{v}_z \geq 0$ for $\mathbf{v}_z \neq 0$ and $\iota = \pm 1$.

Lemma 10. *If $\mathbf{v}_z \neq 0$, then $|(\mathbf{s} + t\,\mathbf{v})_z| = H$ if and only if $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_z, -1)$ or $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_z, 1)$.*

Corollary 11. *If $\mathbf{v}_z \neq 0$ and $\iota = \pm 1$, then vertical_case?$(\mathbf{s}_z, \mathbf{v}_z, t, \iota)$ if and only if $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_z, \iota)$.*

Lemma 12. *If $\mathbf{v}_z \neq 0$, then $|(\mathbf{s} + t\,\mathbf{v})_z| < H$ if and only if $\Theta_H(\mathbf{s}_z, \mathbf{v}_z, -1) < t < \Theta_H(\mathbf{s}_z, \mathbf{v}_z, 1)$.*

A similar construction can be used to find the times at which the trajectory from $\mathbf{s}_{(x,y)}$ along $\mathbf{v}_{(x,y)}$ enters and exits the circle of radius D around the origin. These times are real numbers t such that $\|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\|^2 = D^2$. This is a quadratic equation in t:

$$\|\mathbf{v}_{(x,y)}\|^2 t^2 + 2\,(\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)})\,t + (\|\mathbf{s}_{(x,y)}\|^2 - D^2) = 0. \tag{26}$$

The roots of this quadratic equation are therefore given by the following function, where $\iota = \pm 1$.

$$\Theta_D(\mathbf{s}, \mathbf{v}, \iota) \equiv \frac{-\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} + \iota \sqrt{(\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)})^2 - \|\mathbf{v}_{(x,y)}\|^2(\|\mathbf{s}_{(x,y)}\|^2 - D^2)}}{\|\mathbf{v}_{(x,y)}\|^2}. \tag{27}$$

For this function to return a real number, it is required that the 2-dimensional vector $\mathbf{v}_{(x,y)}$ be nonzero and that discriminant of the quadratic equation (26) is nonnegative. That is, $\Delta(\mathbf{s}, \mathbf{v}) \geq 0$, where

$$\Delta(\mathbf{s}, \mathbf{v}) \equiv (\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)})^2 - \|\mathbf{v}_{(x,y)}\|^2(\|\mathbf{s}_{(x,y)}\|^2 - D^2). \tag{28}$$

The discriminant of the polynomial is given by $4\Delta(\mathbf{s},\mathbf{v})$. If $\Delta(\mathbf{s},\mathbf{v}) \geq 0$, then

$$\Theta_D(\mathbf{s},\mathbf{v},1) - \Theta_D(\mathbf{s},\mathbf{v},-1) = \frac{2\sqrt{(\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)})^2 - \|\mathbf{v}_{(x,y)}\|^2(\|\mathbf{s}_{(x,y)}\|^2 - D^2)}}{\|\mathbf{v}_{(x,y)}\|^2}.$$

Thus, $\Theta_D(\mathbf{s},\mathbf{v},-1) \leq \Theta_D(\mathbf{s},\mathbf{v},1)$, and these two numbers are equal if and only if there is only one solution to the quadratic equation (26), which is equivalent to the statement that the line with direction $\mathbf{v}$ that passes through $\mathbf{s}$ is tangent to the circle of radius D around the origin. It has been formally proved that $\iota\,(\mathbf{s}_{(x,y)} + \Theta_D(\mathbf{s},\mathbf{v},\iota)\,\mathbf{v}_{(x,y)}) \cdot \mathbf{v}_{(x,y)} \geq 0$ for $\Delta(\mathbf{s},\mathbf{v}) \geq 0$, $\mathbf{v}_{(x,y)} \neq 0$, and $\iota = \pm 1$.

Lemma 13. *If $\mathbf{v}_{(x,y)} \neq 0$, then $\|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\| = D$ if and only if $\Delta(\mathbf{s},\mathbf{v}) \geq 0$ and $t = \Theta_D(\mathbf{s},\mathbf{v},-1)$ or $t = \Theta_D(\mathbf{s},\mathbf{v},1)$.*

Corollary 14. *If $\Delta(\mathbf{s},\mathbf{v}) \geq 0$ and $\mathbf{v}_{(x,y)} \neq 0$, then circle_case_2D?$(\mathbf{s},\mathbf{v},t,\iota)$ if and only if $t = \Theta_D(\mathbf{s},\mathbf{v},\iota)$.*

Lemma 15. *If $\mathbf{v}_{(x,y)} \neq 0$, then $\|(\mathbf{s} + t\,\mathbf{v})_{(x,y)}\| < D$ if and only if $\Delta(\mathbf{s},\mathbf{v}) > 0$ and $\Theta_D(\mathbf{s},\mathbf{v},-1) < t < \Theta_D(\mathbf{s},\mathbf{v},1)$.*

The next result follows directly from corollaries 11 and 14.

Corollary 16. *If $\Delta(\mathbf{s},\mathbf{v}) \geq 0$, $\mathbf{v}_{(x,y)} \neq 0$, and $\mathbf{v}_z \neq 0$, then circle_case_3D?$(\mathbf{s},\mathbf{v},t,\iota)$ if and only if $t > 0$ and the following string of equalities holds:*

$$t = \Theta_D(\mathbf{s},\mathbf{v},\iota) = \Theta_H(\mathbf{s}_z,\mathbf{v}_z,-\iota).$$

Finally, the predicate defined in Section 4.4, *line_case?*, can also be be written in terms of the function Θ_D. It is clear from definitions that $\Theta_D(\mathbf{s},\mathbf{v},-1) = \Theta_D(\mathbf{s},\mathbf{v},1)$ is equivalent to the statement that the 2 dimensional trajectory from $\mathbf{s}_{(x,y)}$ along $\mathbf{v}_{(x,y)}$ is tangent to the circle of radius D around the origin. This statement is made precise in the following corollary, which can be formally proven.

Corollary 17. *If $\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} \leq 0$ and $\mathbf{v}_{(x,y)} \neq 0$, then line_case?$(\mathbf{s},\mathbf{v},-1)$ or line_case?$(\mathbf{s},\mathbf{v},1)$ holds if and only if $\Delta(\mathbf{s},\mathbf{v}) \geq 0$ and $\Theta_D(\mathbf{s},\mathbf{v},-1) = \Theta_D(\mathbf{s},\mathbf{v},1)$.*

It follows from algebraic manipulations that if $\|\mathbf{s}_{(x,y)}\| \geq D$ and $\Omega(\mathbf{v}) = 1$, then $\mathbf{s}_{(x,y)} \cdot \mathbf{v}_{(x,y)} \leq 0$.

5 Track Angle Prevention Bands

This section presents a formally verified algorithm, namely `track_bands`, for track angle prevention bands over the closed interval $[0, 2\pi]$, for the function $\nu_{\text{trk}} \colon \mathbb{R} \mapsto \mathbb{R}^3$, defined by Equation (3) in Section 2.2. Given vectors $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$, this algorithm computes track angle maneuvers, i.e., vectors $\mathbf{v}'_o$ that satisfy $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$ and $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$.

The definition of `track_bands` depends on the algorithms `track_line`, `track_circle_2D`, and `track_circle_3D`, which compute track angle maneuvers that are line solutions,

2D circle solutions, and 3D circle solutions, respectively. These three algorithms are proved to be *complete*, i.e., they compute all vectors that satisfy their respective predicate, and *correct*, i.e., only vectors that satisfy their respective predicate are computed. The correctness of `track_bands` depends on the completeness of `track_line`, `track_circle_3D`, and `track_circle_2D`.

5.1 A Special Version of $\Omega_{\nu_{\mathbf{trk}}}$

For $\nu = \nu_{\text{trk}}$, the function Ω_ν, defined in Equation (15) of Section 3, characterizes conflict in the sense of Corollary 7 (Section 3.3). In this section, ν will refer exclusively to the track angle function ν_{trk}. To prove the correctness of a track angle prevention bands algorithm, it must be shown that the finite sequence L_ν returned by the algorithm contains all track angles $\alpha \in [0, 2\pi]$ such that $\Omega_\nu(\alpha) = 1$. An obvious requirement is that there be only finitely many track angles in the interval $[0, 2\pi]$ for which this equation holds. As it turns out, there are several special cases where this equation has infinitely many solutions for track angles $\alpha \in [0, 2\pi]$. Thus, a variant of Ω_ν, namely Ω^*_{trk}, must be defined for these special cases.

Suppose that $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$ satisfy $\mathbf{s}_{(x,y)} = T\ \mathbf{v}_{i(x,y)}$, $\|\mathbf{v}_{o(x,y)}\|^2 = \frac{D^2}{T^2}$, and $|\mathbf{s}_z + T\ \mathbf{v}_z| < H$, where $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$. In this case,

$$\begin{aligned} \|\mathbf{s}_{(x,y)} + T\ \mathbf{v}_{(x,y)}\| &= \|T\ \mathbf{v}_{i(x,y)} + T\ (\mathbf{v}_{o(x,y)} - \mathbf{v}_{i(x,y)})\| \\ &= \|T\ \mathbf{v}_{o(x,y)}\| \\ &= T\|\mathbf{v}_{o(x,y)}\| \\ &= D. \end{aligned} \tag{29}$$

In addition, if $\alpha \in [0, 2\pi]$ is any track angle, then $\|\nu_{\text{trk}}(\alpha)_{(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, and therefore this equality hold if $\mathbf{v}_o$ is replaced with the vector $\nu_{\text{trk}}(\alpha)$. It follows immediately that for any α, $\Delta(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i) \geq 0$. Lemma 13 in Section 4.6 implies that T is equal to $\Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, \iota)$ for some $\iota = \pm 1$. If $\|\mathbf{s}_{(x,y)}\| > 1$, there are infinitely many track angles α such that $T = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, -1)$, in which case Lemma 15 in Section 4.6 implies that the minimum $\min_{t \in T} \|\mathbf{s} + t\ (\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)\|_{\text{cyl}}$ is attained at $t = T$. Thus, if $\|\mathbf{s}_{(x,y)}\| > 1$, then the function $\Omega_\nu(\alpha) \equiv \Omega(\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$ intersects the line at 1 at infinitely many points between 0 and 2π. This special case is specified by the following predicate and illustrated in Figure 10.

$$\begin{aligned} \textit{track\_spc?}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t) \equiv \mathbf{s}_{(x,y)} = t\mathbf{v}_{i(x,y)} \text{ and} \\ \|\mathbf{v}_{o(x,y)}\|^2 = \frac{D^2}{T^2}. \end{aligned} \tag{30}$$

An appropriate replacement Ω^*_{trk} for Ω_ν in this case would have to satisfy the following two properties.

$$\begin{aligned} \Omega^*_{trk}(\alpha) < 1 &\iff \Omega_\nu(\alpha) < 1. \\ \Omega^*_{trk}(\alpha) \geq 1 &\iff \Omega_\nu(\alpha) \geq 1. \end{aligned}$$

In addition, the function Ω^*_{trk} should allow only finitely many solutions to the equation $\Omega^*_{trk}(\alpha) = 1$ for $\alpha \in [0, 2\pi]$. If *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T)$ holds as above, then

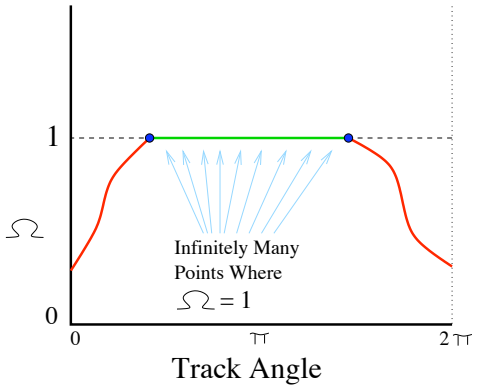

Figure 10. A graph of $\Omega_\nu(\alpha) = \Omega(\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$

the track angles α such that $T = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, -1)$ are precisely those angles α such that $\Omega_\nu(\alpha) \geq 1$, and the angles α such that $T = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, 1)$ are precisely those angles such that $\Omega_\nu(\alpha) < 1$. Thus, it is easy to see that $\Omega^*_{trk}(\alpha) = 1$ should imply that the following two equalities hold.

$$T = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, -1) = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, 1).$$

By Corollary 14 and the definition of the predicate *circle_case_2D?*, it follows that

$$(\mathbf{s}_{(x,y)} + T(\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)_{(x,y)}) \cdot (\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)_{(x,y)} = 0.$$

Replacing $\mathbf{s}_{(x,y)}$ with $T\mathbf{v}_{i(x,y)}$ and factoring out T, this is equivalent to the statement that

$$\begin{aligned} 0 &= \nu_{\text{trk}}(\alpha)_{(x,y)} \cdot (\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)_{(x,y)} \\ &= \|\nu_{\text{trk}}(\alpha)_{(x,y)}\|^2 - \nu_{\text{trk}}(\alpha)_{(x,y)} \cdot \mathbf{v}_{i(x,y)} \\ &= \|\mathbf{v}_{o(x,y)}\|^2 - \nu_{\text{trk}}(\alpha)_{(x,y)} \cdot \mathbf{v}_{i(x,y)} \\ &= \frac{D^2}{T^2} - \nu_{\text{trk}}(\alpha)_{(x,y)} \cdot \mathbf{v}_{i(x,y)}. \end{aligned}$$

This motivates the following definition of the function $\Omega^*_{trk} \colon \mathbb{R} \mapsto \mathbb{R}^3$, which depends on the explicit parameters $\mathbf{v}_o$, $\mathbf{v}_i$, $t \in \mathbb{R}$, and $\iota = \pm 1$.

$$\Omega^*_{trk}(\mathbf{v}_o, \mathbf{v}_i, t, \iota)(\alpha) \equiv \iota \ (\nu_{\text{trk}}(\alpha)_{(x,y)} \cdot \mathbf{v}_{i(x,y)} - \frac{D^2}{T^2}) + 1. \tag{31}$$

Identical reasoning to that above can be used to prove that if *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$ holds and $\Omega^*_{trk}(\mathbf{v}_o, \mathbf{v}_i, t, \iota)(\alpha) = 1$, then the following equalities hold.

$$t = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, -1) = \Theta_D(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, 1).$$

In particular, the following theorem can be formally proved using Corollary 17 in Section 4.6.

Theorem 18. *If track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$ *holds and* $\Omega^*_{trk}(\mathbf{v}_o, \mathbf{v}_i, t, \iota)(\alpha) = 1$, *then line_case?*$(\mathbf{s}, \nu_{trk}(\alpha) - \mathbf{v}_i, \varepsilon)$ *holds for some* $\varepsilon = \pm 1$.

When proving the correctness of the track angle prevention bands algorithm presented in the next sections, the function Ω^*_{trk} will be used in the place of Ω_ν when *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T)$ holds. Thus, it is necessary to prove that Ω^*_{trk} characterizes conflict in some special cases.

Theorem 19. *If track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$*, then the equivalence*

$$\Omega^*_{trk}(\mathbf{v}_o, \mathbf{v}_i, t, \iota)(\alpha) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu_{trk}(\alpha) - \mathbf{v}_i)$$

holds in each of the following three cases.

1. $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, \iota)$, *and* $0 < t < T$.
2. $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, $\iota = 1$, $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, 1)$, *and* $t = T$.
3. $\iota = 1$, $t = T$, *and* $|\mathbf{s}_z + T\ (\mathbf{v}_{oz} - \mathbf{v}_{iz})| < H$.

5.2 Line Solutions For Track Angle Maneuvers

The algorithm `track_line`, defined in this section, takes as parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, t, $\varepsilon = \pm 1$, and $\iota = \pm 1$. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ that is either the zero vector or is equal to $\nu_{\text{trk}}(\alpha)$ for some $\alpha \in [0, 2\pi)$ such that the relative velocity vector $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$ is tangent to the circle, i.e., it satisfies *line_case?*$(\mathbf{s}, \mathbf{v}', \varepsilon)$. The main theorem in this section states that `track_line` is correct and complete for line solutions that are track angle maneuvers.

The definition of `track_line` requires the definition an auxiliary function, namely `tangent_line`, that takes as parameter a relative position vector $\mathbf{s} \in \mathbb{R}^3$ such that $\|\mathbf{s}_{(x,y)}\| \geq D$ and a number $\varepsilon = \pm 1$, and returns a vector in $\mathbb{R}^3$ that is tangent to the protected zone.

$$\begin{array}{l}
\texttt{tangent_line}(\mathbf{s}, \varepsilon) \equiv \\
\quad \texttt{if}\ \ \|\mathbf{s}_{(x,y)}\| = D\ \ \texttt{then} \\
\quad\quad \varepsilon\ \mathbf{s}^\perp \\
\quad \texttt{else} \\
\quad\quad \texttt{let}\ \ d = \|\mathbf{s}_{(x,y)}\|^2\ \ \texttt{in} \\
\quad\quad\quad (\dfrac{D^2}{d} - 1)\,\mathbf{s} + \dfrac{\varepsilon\, D\sqrt{d - D^2}}{d}\,\mathbf{s}^\perp \\
\quad \texttt{endif}
\end{array} \tag{32}$$

The proofs of the following lemmas rely on standard vector algebra.

Lemma 20. *If* $\|\mathbf{s}_{(x,y)}\| \geq D$ *and* $\varepsilon = \pm 1$*, then line_case?*$(\mathbf{s}, \textit{tangent\_line}(\mathbf{s}, \varepsilon), \varepsilon)$ *holds.*

Lemma 21. *If* $\|\mathbf{s}_{(x,y)}\| \geq D$*, then line_case?*$(\mathbf{s}, \mathbf{v}, \varepsilon)$ *holds if and only if there exists* $k \geq 0$ *such that*

$$\mathbf{v}_{(x,y)} = k\ \textit{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)}.$$

If $\mathbf{v}'_o \in \mathbb{R}^3$ is a track angle maneuver for the ownship such that *line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ holds, then it holds that

$$\|\mathbf{v}_{o(x,y)}\|^2 = \|k \ \texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)} + \mathbf{v}_{i(x,y)}\|^2. \tag{33}$$

Equation (33) has the form $\|\mathbf{v}_{o(x,y)}\|^2 = \|k\ \mathbf{u} + \mathbf{v}_{i(x,y)}\|^2$, where $\mathbf{u} \in \mathbb{R}^2$. Since it will be necessary in later sections to solve similar equations of this form, a function is needed that explicitly solves this equation for $k \in \mathbb{R}$.

It follows from the equation $\|\mathbf{v}_{o(x,y)}\|^2 = \|k\ \mathbf{u} + \mathbf{v}_{i(x,y)}\|^2$ that

$$\begin{aligned} 0 &= (k\ \mathbf{u} + \mathbf{v}_{i(x,y)}) \cdot (k\ \mathbf{u} + \mathbf{v}_{i(x,y)}) - \|\mathbf{v}_{o(x,y)}\|^2 \\ &= \|\mathbf{u}\|^2 k^2 + (2\,\mathbf{v}_{i(x,y)} \cdot \mathbf{u})k + (\|\mathbf{v}_{i(x,y)}\|^2 - \|\mathbf{v}_{o(x,y)}\|^2). \end{aligned} \tag{34}$$

This is a quadratic equation in k. If $\iota = \pm 1$, then $\frac{-b+\iota\sqrt{b^2-4ac}}{2a}$ is a root of this equation, where

$$\begin{aligned} a &= \|\mathbf{u}\|^2, \\ b &= 2\,\mathbf{v}_{i(x,y)} \cdot \mathbf{u}, \\ c &= \|\mathbf{v}_{i(x,y)}\|^2 - \|\mathbf{v}_{o(x,y)}\|^2. \end{aligned} \tag{35}$$

Thus, if $b^2 - 4ac \geq 0$ and $k = \frac{-b+\iota\sqrt{b^2-4ac}}{2a}$ is nonnegative, then the unique vector $\mathbf{v}'_o$ such that $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$ and $\mathbf{v}'_{o(x,y)} = k\ _{(x,y)} + \mathbf{v}_{i(x,y)}$ satisfies both $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$ and *line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$. This motivates the definition of the function `track_only_line`, which returns a real number.

$$\begin{array}{l} \texttt{track\_only\_line}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i, \iota) \equiv \\ \quad \texttt{let} \\ \quad\quad a = \|\mathbf{u}\|^2, \\ \quad\quad b = 2\,\mathbf{v}_{i(x,y)} \cdot \mathbf{u}, \\ \quad\quad c = \|\mathbf{v}_{i(x,y)}\|^2 - \|\mathbf{v}_{o(x,y)}\|^2 \\ \quad \texttt{in} \\ \quad\quad \texttt{if}\ \ b^2 - 4ac \geq 0\ \ \texttt{then} \\ \quad\quad\quad \dfrac{-b + \iota\sqrt{b^2 - 4ac}}{2a} \\ \quad\quad \texttt{else} \\ \quad\quad\quad 0 \\ \quad\quad \texttt{endif} \end{array} \tag{36}$$

The next lemma states that the algorithm `track_only_line` computes solutions for k to the equation $\mathbf{v}'_{o(x,y)} = k\ \mathbf{u} + \mathbf{v}_{i(x,y)}$, where $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$.

Lemma 22. *If* $\mathbf{u} \neq \mathbf{0}$*, then* $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$ *and* $k\ \mathbf{u} = \mathbf{v}'_{o(x,y)} - \mathbf{v}_{i(x,y)}$ *if and only if*

$$k = \textit{track\_only\_line}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i, \iota),$$

for some $\iota = \pm 1$.

Using `track_only_line`, the algorithm `track_line`, which computes track angle maneuvers $\mathbf{v}'_o \in R^3$ that satisfy *line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ for $\varepsilon = \pm 1$, can be defined as follows.

$$
\begin{array}{l}
\texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota) \equiv \\
\quad \texttt{let} \\
\quad\quad k \;\; = \texttt{track\_only\_line}(\texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)}, \mathbf{v}_o, \mathbf{v}_i, \iota), \\
\quad\quad \mathbf{v}'_o = (k\ \texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)} + \mathbf{v}_{i(x,y)})\ \texttt{with}\ [z \leftarrow \mathbf{v}_{oz}] \\
\quad \texttt{in} \\
\quad\quad \texttt{if}\ k \geq 0\ \texttt{then} \\
\quad\quad\quad \mathbf{v}'_o \\
\quad\quad \texttt{else} \\
\quad\quad\quad \mathbf{0} \\
\quad\quad \texttt{endif}
\end{array}
\tag{37}
$$

The correctness and completeness of `track_line` follow from its definition and Lemma 22.

Theorem 23 (Correctness and completeness of `track_line`)**.** *If* $\|\mathbf{s}_{(x,y)}\| \geq D$ *and* $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$*, then* $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$*,* $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$*, and line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ *holds if and only if*

$$\mathbf{v}'_o = \textit{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota),$$

for some $\iota = \pm 1$*.*

5.3 2D Circle Solutions For Track Angle Maneuvers

The algorithm `track_circle_2D`, defined in this section, takes as parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, t, $\iota = \pm 1$, and $\varepsilon = \pm 1$. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ that is either the zero vector or is equal to $\nu_{\text{trk}}(\alpha)$ for some $\alpha \in [0, 2\pi)$ such that the relative velocity vector $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$ satisfies *circle_case_2D?*$(\mathbf{s}, \mathbf{v}', t, \iota)$. The main theorems in this section state that `track_circle_2D` is correct and complete for 2D circle solutions that are track angle maneuvers.

If *circle_case_2D?*$(\mathbf{s}, \mathbf{v}', t, \iota)$ holds, then the vector $\mathbf{v}'_o$ must satisfy $\|\mathbf{s}_{(x,y)} + t\mathbf{v}'_{(x,y)}\|^2 = D^2$. If $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, then algebraic manipulations can be used to show that

$$\|\mathbf{s}_{(x,y)} + t\mathbf{v}'_{(x,y)}\|^2 = \|\mathbf{s}_{(x,y)}\|^2 + t^2\|\mathbf{v}_{o(x,y)}\|^2 + 2t(s_{(x,y)} - t\mathbf{v}_{i(x,y)}) \cdot \mathbf{v}'_{(x,y)} - t^2\|\mathbf{v}_{i(x,y)}\|^2.$$

Thus, if $t > 0$, then

$$(\mathbf{s}_{(x,y)} - t\mathbf{v}_{i(x,y)}) \cdot \mathbf{v}'_{(x,y)} = \frac{1}{2t}(D^2 - \|\mathbf{s}_{(x,y)}\|^2 - t^2(\|\mathbf{v}_{o(x,y)}\|^2 - \|\mathbf{v}_{i(x,y)}\|^2)). \tag{38}$$

This equation has the form $\mathbf{u} \cdot \mathbf{v}'_{(x,y)} = j$, where $\mathbf{u} = \mathbf{s}_{(x,y)} - t\mathbf{v}_{i(x,y)}$ and

$$j = \frac{1}{2t}(D^2 - \|\mathbf{s}_{(x,y)}\|^2 - t^2(\|\mathbf{v}_{o(x,y)}\|^2 - \|\mathbf{v}_{i(x,y)}\|^2)).$$

Since it will be necessary in later sections to solve similar equations of the form $\mathbf{u} \cdot \mathbf{v}'_{(x,y)} = j$, a function is needed that explicitly solves this equation for $\mathbf{v}'_o$ when $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$.

Assuming $\mathbf{u} \neq \mathbf{0}$, Equation (1) yields

$$\begin{aligned}\mathbf{v}'_{(x,y)} &= \frac{1}{\|\mathbf{u}\|^2}((\mathbf{u} \cdot \mathbf{v}'_{(x,y)})\mathbf{u} + (\mathbf{u}^\perp \cdot \mathbf{v}'_{(x,y)})\mathbf{u}^\perp) \\ &= \frac{1}{\|\mathbf{u}\|^2}(j\mathbf{u} + k\mathbf{u}^\perp),\end{aligned}$$

where $k = \mathbf{u}^\perp \cdot \mathbf{v}'_{(x,y)}$. Lemma 22 in Section 5.2 can be used to prove that

$$k = \texttt{track\_only\_line}(\mathbf{u}^\perp{}_{(x,y)}, \mathbf{v}_o, \mathbf{v}_i + \frac{j}{\|\mathbf{u}_{(x,y)}\|^2}\mathbf{u}, \iota),$$

for some $\iota = \pm 1$.

It follows from this that for $\mathbf{u} \neq 0$, the function `track_only_dot`, defined below, solves the equation $\mathbf{u} \cdot (\mathbf{v}'_{o(x,y)} - \mathbf{v}_{i(x,y)}) = j$ for $\mathbf{v}'_o$, when $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$.

$$\begin{aligned}&\texttt{track\_only\_dot}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i, j, \iota) \equiv \\ &\quad \texttt{let } k = \texttt{track\_only\_line}(\mathbf{u}^\perp, \mathbf{v}_o, \mathbf{v}_i + \frac{j}{\|\mathbf{u}_{(x,y)}\|^2}\mathbf{u}, \iota) \texttt{ in} \\ &\qquad (k\mathbf{u}^\perp + \mathbf{v}_{i(x,y)} + \frac{j}{\|\mathbf{u}_{(x,y)}\|^2}\mathbf{u}) \texttt{ with } [z \leftarrow \mathbf{v}_{oz}]\end{aligned} \tag{39}$$

Lemma 24. *If* $\mathbf{u} \neq \mathbf{0}$ *and* $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$*, then* $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$*,* $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$*, and* $\mathbf{u} \cdot (\mathbf{v}'_{o(x,y)} - \mathbf{v}_{i(x,y)}) = j$ *if and only if*

$$\mathbf{v}'_o = \textit{track\_only\_dot}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i, j, \iota),$$

for some $\iota = \pm 1$.

The function `track_only_dot` is used to solve Equation (38) when $\mathbf{v}_i \neq \mathbf{0}$ and $t > 0$. Using `track_only_dot`, the algorithm `track_circle_2D`, which computes track angle maneuvers $\mathbf{v}'_o \in R^3$ that satisfy *circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ for $\iota = \pm 1$, can be defined as follows.

$$
\begin{array}{l}
\texttt{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon) \equiv \\
\quad \texttt{let} \\
\quad\quad \mathbf{u} = (\mathbf{s} - t\mathbf{v}_i)_{(x,y)}, \\
\quad\quad j = \dfrac{1}{2t}(D^2 - \|\mathbf{s}_{(x,y)}\|^2 - t^2(\|\mathbf{v}_{o(x,y)}\|^2 - \|\mathbf{v}_{i(x,y)}\|^2)) \\
\quad \texttt{in} \\
\quad\quad \texttt{if } \mathbf{u} \neq \mathbf{0} \texttt{ then} \\
\quad\quad\quad \texttt{let} \\
\quad\quad\quad\quad \mathbf{v}'_o = \texttt{track\_only\_dot}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i, j, \varepsilon) \\
\quad\quad\quad \texttt{in} \\
\quad\quad\quad\quad \texttt{if } \iota\ (\mathbf{s} + t\ (\mathbf{v}'_o - \mathbf{v}_i)) \geq 0 \texttt{ then} \\
\quad\quad\quad\quad\quad \mathbf{v}'_o \\
\quad\quad\quad\quad \texttt{else} \\
\quad\quad\quad\quad\quad \mathbf{0} \\
\quad\quad\quad\quad \texttt{endif} \\
\quad\quad \texttt{else} \\
\quad\quad\quad \mathbf{0} \\
\quad\quad \texttt{endif}
\end{array}
\tag{40}
$$

The correctness and completeness of `track_circle_2D` follow from its definition and Lemma 24.

Theorem 25 (Correctness of `track_circle_2D`)**.** *If* $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$ *and*

$$\mathbf{v}'_o = \textit{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon),$$

then $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$, *and circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ *holds.*

Theorem 26 (Completeness of `track_circle_2D`)**.** *If* $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$, *and circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ *holds, then either track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$ *holds or*

$$\mathbf{v}'_o = \textit{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon)$$

for some $\varepsilon = \pm 1$.

5.4 3D Circle Solutions For Track Angle Maneuvers

Theorems 25 and 26 imply that the algorithm `track_circle_2D` can be used to compute vectors $\mathbf{v}'_o$ such that *circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ holds, where $t > 0$. By the definition of the predicate *circle_case_3D?* in Section 4.3, this algorithm can be used to compute vectors $\mathbf{v}'_o$ such that *circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ holds when $\Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota) > 0$. This motivates the definition of the algorithm `track_circle_3D`, which takes as a parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, $\iota = \pm 1$, and $\varepsilon = \pm 1$. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ that is either the zero vector or is equal

to $\nu_{\text{trk}}(\alpha)$ for some $\alpha \in [0, 2\pi)$ such that the relative velocity vector $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$ satisfies *circle_case_3D?*$(\mathbf{s}, \mathbf{v}', \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$.

```
track_circle_3D(s, v_o, v_i, ι, ε) ≡
   if v_oz = v_iz then
      0
   else
      let t = Θ_H(s_z, v_oz − v_iz, −ι) in
         if t > 0 then                                          (41)
            track_circle_2D(s, v_o, v_i, t, ι, ε)
         else
            0
         endif
   endif
```

The following theorems state that `track_circle_3D` is correct and complete for 3D circle solutions that are track angle maneuvers. These properties follow from theorems 25 and 26, and properties of the function Θ_H presented in Section 4.6.

Theorem 27 (Correctness of `track_circle_3D`)**.** *If* $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$ *and*

$$\mathbf{v}'_o = \textit{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon),$$

then $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$, *and circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ *holds.*

Theorem 28 (Completeness of `track_circle_3D`)**.** *If* $\|\mathbf{v}'_{o(x,y)}\| = \|\mathbf{v}_{o(x,y)}\|$, $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, *and circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ *holds, then either track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota)))$ *holds or*

$$\mathbf{v}'_o = \textit{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon),$$

for some $\varepsilon = \pm 1$.

5.5 A Prevention Bands Algorithm For Track Angle Maneuvers

Using the functions defined in the previous section, the prevention bands algorithm `track_bands` for the function $\nu_{\text{trk}} \colon \mathbb{R} \mapsto \mathbb{R}^3$ can be defined as follows, where V is a sequence of vectors, $|V|$ is its length, $\mathcal{L}$ is a set of real numbers, and `sort` is a function that takes as parameter a set of real numbers and returns the sequence of elements in the set that is sorted by increasing order.[4]

[4]For readability, the algorithm is written using pseudo-code including assignment and bounded loop constructions. The PVS development provides a functional version of this code.

$$
\begin{array}{l}
\texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i) \equiv \\
\quad V_0 \ \texttt{:=}\ \texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, -1); \\
\quad V_1 \ \texttt{:=}\ \texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, 1); \\
\quad V_2 \ \texttt{:=}\ \texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, -1); \\
\quad V_3 \ \texttt{:=}\ \texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, 1); \\
\quad \texttt{if}\ \|\mathbf{s}_{(x,y)}\| \geq D\ \texttt{then} \\
\quad\quad V_4 \ \texttt{:=}\ \texttt{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, -1, -1); \\
\quad\quad V_5 \ \texttt{:=}\ \texttt{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, -1, 1); \\
\quad\quad V_6 \ \texttt{:=}\ \texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, -1); \\
\quad\quad V_7 \ \texttt{:=}\ \texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, 1); \\
\quad\quad V_8 \ \texttt{:=}\ \texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, -1); \\
\quad\quad V_9 \ \texttt{:=}\ \texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, 1); \\
\quad \texttt{endif} \\
\quad \mathcal{L} = \{0, 2\pi\}; \\
\quad \texttt{for}\ i = 1\ \texttt{to}\ |V|\ \texttt{do} \\
\quad\quad \texttt{if}\ V_{i(x,y)} \neq \mathbf{0}\ \texttt{then} \\
\quad\quad\quad \mathcal{L}\ \texttt{:=}\ \mathcal{L} \cup \{\texttt{track}(V_i)\}; \\
\quad\quad \texttt{endif} \\
\quad \texttt{endfor} \\
\quad L_{\nu_{\text{trk}}}\ \texttt{:=}\ \texttt{sort}(\mathcal{L});
\end{array}
\tag{42}
$$

The finite, ordered sequence $\text{Ł}_{\nu_{\text{trk}}}$returned by `track_bands` is computed using every possible instantiation of the parameters ε and ι, both of which can be ± 1, in the functions `track_line`, `track_circle_2D`, and `track_circle_3D`. For each vector $\mathbf{v}'_o$ returned by one of these three algorithms for $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$ with the property that $\mathbf{v}'_{o(x,y)} \neq 0$, the track angle of $\mathbf{v}'_o$ is an element of the sequence returned by `track_bands`.

Theorem 29 (Correctness of `track_bands`)**.** *The track angle prevention bands algorithm* ***`track_bands`*** *is correct for ν_{trk} over the interval $[0, 2\pi]$.*

Proof. By Theorem 2 in Section 2.5, it suffices to find a continuous function $\Omega_\nu : \mathbb{R} \mapsto \mathbb{R}$, parameterized by $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$, that satisfies the following two properties.

1. For all $\alpha \in [0, 2\pi]$,

$$\Omega_\nu(\alpha) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i).$$

2. For all $\alpha \in [0, 2\pi]$,

$$\Omega_\nu(\alpha) = 1 \implies \alpha \in \texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i).$$

In most cases, the function Ω_ν, where $\nu = \nu_{\text{trk}}$, defined in Equation (15) of Section 3, will suffice. However, in some special cases, the function Ω^*_{trk}, defined in Equation (31) of Section 5.1, will be used. The latter case is considered first.

Suppose that *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$, where $t > 0$, and that one of the following conditions holds.

1. $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, \iota)$, and $0 < t < T$.
2. $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, $\iota = 1$, $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, 1)$, and $t = T$.
3. $\iota = 1$, $t = T$, and $|\mathbf{s}_z + T\ (\mathbf{v}_{oz} - \mathbf{v}_{iz})| < H$.

By Theorem 19 in Section 5.1,

$$\Omega^*_{trk}(\mathbf{v}_o, \mathbf{v}_i, t, \iota)(\alpha) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$$

holds for any $\alpha \in \mathbb{R}$. Thus, all that is required to complete the proof in this special case is to prove that for all $\alpha \in [0, 2\pi]$, $\Omega^*_{trk}(\alpha) = 1$ implies

$$\alpha \in \texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i).$$

If $\Omega^*_{trk}(\alpha) = 1$, then Theorem 18 implies that *line_case?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, \varepsilon)$, for some $\varepsilon = \pm 1$. By the completeness of the algorithm `track_line` (Theorem 23 in Section 5.2), if $\|\mathbf{s}_{(x,y)}\| \geq D$, then $\nu_{\text{trk}}(\alpha)$ is equal to $\texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota)$, for some $\iota = \pm 1$. Thus, $\alpha = \texttt{track}(\nu_{\text{trk}}(\alpha))$ is equal to $\texttt{track}(\texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota))$, which, by definition, is an element of $\texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i)$. If $\|\mathbf{s}_{(x,y)}\| < D$, then it must be true that the third condition holds: $\iota = 1$, $t = T$, and $|\mathbf{s}_z + T\ (\mathbf{v}_{oz} - \mathbf{v}_{iz})| < H$. In this case, it is easy to prove that for any $\alpha \in \mathbb{R}$, *conflict?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$, and therefore $\Omega^*_{trk}(\alpha) < 1$. This completes the proof in the case where one of the three conditions above holds.

Now suppose that the second condition above holds, but where $\iota = 1$ is replaced with $\iota = -1$. That is, suppose that $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$, $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -1)$, $t = T$, and *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T)$. Since $\nu_{\text{trk}}(\alpha)_z = \mathbf{v}_{oz}$ for any $\alpha \in \mathbb{R}$, Lemma 12 of Section 4.6 can be used to show that *conflict?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$ does not hold for any $\alpha \in \mathbb{R}$. In this case, the correctness of the algorithm `track_bands` is trivial.

The proof has now been reduced to the case where neither of the following conditions hold.

1. $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$ and there exists $\iota = \pm 1$ such that *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t)$ and $0 < t \leq T$, where $t = \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, \iota)$.
2. *track_spc?*$(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T)$ and $|\mathbf{s}_z + T\ (\mathbf{v}_{oz} - \mathbf{v}_{iz})| < H$.

By Corollary 7 of Section 3.3, the function Ω_ν, where $\nu = \nu_{\text{trk}}$, characterizes conflict. Suppose that $\alpha \in [0, 2\pi]$ and $\Omega_\nu(\alpha) = 1$. Since $\Omega_\nu(\alpha) = \Omega(\nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$, Theorem 9 in Section 4.5 implies that one of the following conditions holds, where $\mathbf{v} = \nu_{\text{trk}}(\alpha) - \mathbf{v}_i$.

- $\|\mathbf{s}_{(x,y)}\| \geq D$ and either *line_case?*$(\mathbf{s}, \mathbf{v}, \varepsilon)$, for some $\varepsilon = \pm 1$.

- $|\mathbf{s}_z + T\mathbf{v}_z| < H$ and *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, T, -1)$.
- There is some real number $t > 0$ such that *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$, for some $\iota = \pm 1$.
- $\|\mathbf{s}_{(x,y)} + T\mathbf{v}_{(x,y)}\| \leq D$ and *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$.

These cases are now considered individually.

- Suppose first that $\|\mathbf{s}_{(x,y)}\| \geq D$ and *line_case?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, \varepsilon)$, for some $\varepsilon = \pm 1$. By completeness of `track_line` (Theorem 23), $\nu_{\text{trk}}(\alpha)$ is equal to $\texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota)$, for some $\iota = \pm 1$. Thus, $\alpha = \texttt{track}(\nu_{\text{trk}}(\alpha))$ is equal to $\texttt{track}(\texttt{track\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon, \iota))$, which, by definition, is an element of $\texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i)$.
- Suppose that $|\mathbf{s}_z + T\mathbf{v}_z| < H$ and *circle_case_2D?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i, T, -1)$. By completeness of the algorithm `track_circle_2D` (Theorem 26), $\nu_{\text{trk}}(\alpha)$ is equal to $\texttt{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon)$, for some $\iota = \pm 1$ and $\varepsilon = \pm 1$. Thus, $\alpha = \texttt{track}(\nu_{\text{trk}}(\alpha)) = \texttt{track}(\texttt{track\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon))$. Hence, α is an element of $\texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i)$.
- Suppose that there is a real number $t > 0$ such that *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$, where $\iota = \pm 1$. Assume that $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$. By completeness of `track_circle_3D` (Theorem 28), $\nu_{\text{trk}}(\alpha) = \texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon)$ for some $\iota = \pm 1$ and $\varepsilon = \pm 1$. Thus, as above,

  $$\alpha = \texttt{track}(\nu_{\text{trk}}(\alpha)) = \texttt{track}(\texttt{track\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon)).$$

  Hence, α is an element of $\texttt{track\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i)$. The case where $\mathbf{v}_{oz} = \mathbf{v}_{iz}$ can be equally discharged.
- Finally, suppose that $\|\mathbf{s}_{(x,y)} + T\mathbf{v}_{(x,y)}\| \leq D$ and *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$. In this case, the fact that $\nu_{\text{trk}}(\alpha)_z = \mathbf{v}_{oz}$ implies that *conflict?*$(\mathbf{s}, \nu_{\text{trk}}(\alpha) - \mathbf{v}_i)$ does not hold for any $\alpha \in \mathbb{R}$. From there, the correctness of the algorithm `track_bands` is trivial.

□

6 Ground Speed Prevention Bands

This section presents a formally verified algorithm, namely `gs_bands`, for ground speed prevention bands over an arbitrary interval $[gsmin, gsmax]$ for the function $\nu_{\text{gs}} \colon \mathbb{R} \mapsto \mathbb{R}^3$, defined by Equation (4) in Section 2.2. The boundaries of the interval, $gsmin$ and $gsmax$, represent (postitive) minimum and maximum ground speeds for the ownship aircraft, respectively. Given vectors $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$, this algorithm computes ground speed maneuvers, i.e., vectors $\mathbf{v}'_o$ that satisfy $\mathbf{v}'_{o(x,y)} = \ell\, \mathbf{v}_{o(x,y)}$, for some $\ell > 0$, and $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$.

The definition of `gs_bands` depends on the algorithms `gs_line`, `gs_circle_2D`, and `gs_circle_3D`, which compute ground speed maneuvers that are line solutions,

2D circle solutions, and 3D circle solutions, respectively. These three algorithms are proved to be complete and correct for ground speed maneuvers that satisfy their respective predicate. The correctness of `gs_bands` depends on the completeness of `gs_line`, `gs_circle_3D`, and `gs_circle_2D`.

If $\mathbf{v}'_o$ is a ground speed maneuver for the ownship, then there is some positive $p \in \mathbb{R}$ such that $\nu_{\text{gs}}(p) = \mathbf{v}'_o$. Therefore, $\mathbf{v}'_{o(x,y)} = \ell\, \mathbf{v}_{o(x,y)}$, where $\ell = \frac{p}{\|\mathbf{v}_{o(x,y)}\|}$ and $\ell > 0$.

6.1 Line Solutions For Ground Speed Maneuvers

The algorithm `gs_line`, defined in this section, takes as parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, t, and $\varepsilon = \pm 1$. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ that is either the zero vector or is equal to $\nu_{\text{gs}}(p)$ for some $p \in \mathbb{R}$ such that the relative velocity vector $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$ is tangent to the circle, i.e., it satisfies *line_case?*$(\mathbf{s}, \mathbf{v}', \varepsilon)$. The main theorem in this section states that `gs_line` is correct and complete for line solutions that are ground speed maneuvers.

Suppose $\|\mathbf{s}_{(x,y)}\| \geq D$ and that $\mathbf{v}'_o$ is a vector in $\mathbb{R}^3$ such that $\mathbf{v}'_{o(x,y)} = \ell\, \mathbf{v}_{o(x,y)}$. Suppose further that *line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ holds for some $\varepsilon = \pm 1$. By Lemma 21 of Section 5.2, there is some $k \geq 0$ such that $\ell\, \mathbf{v}_{o(x,y)} = k\, \texttt{tangent\_line}(\mathbf{s}, \varepsilon) + \mathbf{v}_{i(x,y)}$. This equation has the form

$$\ell\, \mathbf{v}_{o(x,y)} = k\, \mathbf{u} + \mathbf{v}_{i(x,y)}, \tag{43}$$

where $\mathbf{u} \in \mathbb{R}^3$. Functions can be defined that explicitly solve this equation for k and ℓ. It is easily proved that

$$(\mathbf{v}_{i(x,y)} \cdot \mathbf{u}^\perp)\, \mathbf{v}_{o(x,y)} - (\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp)\, \mathbf{v}_{i(x,y)} = (\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_o^\perp{}_{(x,y)})\, \mathbf{u}.$$

Thus, if $\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp \neq 0$, then

$$k = \frac{\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_o^\perp{}_{(x,y)}}{\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp}, \tag{44}$$

$$\ell = \frac{\mathbf{v}_{i(x,y)} \cdot \mathbf{u}^\perp}{\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp}. \tag{45}$$

This motivates the definition of the algorithms `gs_line_k` and `gs_line_l`, which solve Equation (43) for k and l.

$$\begin{array}{l}
\texttt{gs_line_k}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i) \equiv \\
\quad \texttt{if } \mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp \neq 0 \texttt{ then} \\
\quad\quad \dfrac{\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_o^\perp{}_{(x,y)}}{\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^\perp} \\
\quad \texttt{else} \\
\quad\quad 0 \\
\quad \texttt{endif}
\end{array} \tag{46}$$

$$
\begin{array}{l}
\texttt{gs\_line\_l}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i) \equiv \\
\quad \texttt{if } \mathbf{v}_{o(x,y)} \cdot \mathbf{u}^{\perp} \neq 0 \texttt{ then} \\
\qquad \max\left(\dfrac{\mathbf{v}_{i(x,y)} \cdot \mathbf{u}^{\perp}}{\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^{\perp}}, 0\right) \\
\quad \texttt{else} \\
\qquad 0 \\
\quad \texttt{endif}
\end{array}
\tag{47}
$$

Lemma 30. *If $\ell > 0$ and either $\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_{o\,(x,y)}^{\perp} \neq 0$ or $\mathbf{v}_{o(x,y)} \cdot \mathbf{u}^{\perp} \neq 0$, then Equation (43) holds if and only if $k =$ gs_line_k$(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i)$ and $\ell =$ gs_line_l$(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i)$.*

Using gs_line_k and gs_line_l, the algorithm gs_line, which computes ground speed maneuvers $\mathbf{v}'_o \in R^3$ that satisfy *line_case?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ for $\varepsilon = \pm 1$, can be defined as follows.

$$
\begin{array}{l}
\texttt{gs\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon) \equiv \\
\quad \texttt{let} \\
\qquad \mathbf{u} = \texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)} \\
\qquad k = \texttt{gs\_line\_k}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i) \\
\qquad \ell = \texttt{gs\_line\_l}(\mathbf{u}, \mathbf{v}_o, \mathbf{v}_i) \\
\quad \texttt{in} \\
\qquad \texttt{if } k \geq 0 \texttt{ then} \\
\qquad\quad \ell\, \mathbf{v}_{o(x,y)} \texttt{ with } [z \leftarrow \mathbf{v}_{oz}] \\
\qquad \texttt{else} \\
\qquad\quad \mathbf{0} \\
\qquad \texttt{endif} \\
\quad \texttt{endif}
\end{array}
\tag{48}
$$

The correctness and completeness of gs_line follow from its definition and Lemma 30.

Theorem 31 (Correctness and completeness of gs_line)**.** *If $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$, and either $\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_{o\,(x,y)}^{\perp} \neq 0$ or $\mathbf{v}_{o(x,y)} \cdot$ tangent_line$(\mathbf{s}, \varepsilon)^{\perp}{}_{(x,y)} \neq 0$, then $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$, $\mathbf{v}'_{o(x,y)} = \ell\, \mathbf{v}_{o(x,y)}$ for some $\ell > 0$, and line_case?$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \varepsilon)$ holds if and only if*

$$\mathbf{v}'_o = \textit{gs\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \varepsilon).$$

This theorem does not hold if $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_{o\,(x,y)}^{\perp} = 0$, and $\mathbf{v}_{o(x,y)} \cdot$ tangent_line$(\mathbf{s}, \varepsilon)^{\perp}{}_{(x,y)} = 0$. This case has to be handled separately in the verification of correctness of the ground speed prevention bands algorithm.

6.2 2D Circle Solutions For Ground Speed Maneuvers

The algorithm `gs_circle_2D`, defined in this section, takes as parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, t, $\iota = \pm 1$, and $\varepsilon = \pm 1$. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ such that $\mathbf{v}'_o$ is either the zero vector or is equal to $\nu_{\text{gs}}(p)$ for some $p > 0$ such that the relative velocity vector $\mathbf{v} = \mathbf{v}'_o - \mathbf{v}_i$ satisfies *circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$. The main theorems in this section state that `gs_circle_2D` is correct and complete for 2D circle solution that are ground speed maneuvers.

If *circle_case_2D?*$(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, t, \iota)$ holds, then the vector $\mathbf{v}'_o$ must satisfy

$$\|\mathbf{s}_{(x,y)} + t\,(\mathbf{v}'_{o(x,y)} - \mathbf{v}_{i(x,y)})\|^2 = D^2.$$

If $\mathbf{v}'_{o(x,y)} = \ell\,\mathbf{v}_{o(x,y)}$, then simple algebraic manipulation can be used to show that $a\ \ell^2 + b\ \ell + c = 0$, where

$$\begin{aligned} a &= t^2\,\|\mathbf{v}_{o(x,y)}\|^2, \\ b &= 2t\,(\mathbf{s} - t\,\mathbf{v}_i)_{(x,y)} \cdot \mathbf{v}_{o(x,y)}, \\ c &= \|(\mathbf{s} - t\mathbf{v}_i)_{(x,y)}\|^2 - D^2. \end{aligned}$$

This is a quadratic equation in ℓ, which can be solved using the quadratic formula. Note that if $\mathbf{v}'_o$ represents a ground speed maneuver for the ownship, then ℓ must be positive, since $\mathbf{v}'_{o(x,y)} = \ell\,\mathbf{v}_{o(x,y)}$. This motivates the following definition of the algorithm `gs_circle_2D`, which computes ground speed maneuvers $\mathbf{v}'_o \in R^3$

that satisfy *circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ for $\iota = \pm 1$.

$$
\begin{array}{l}
\texttt{gs\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon) \equiv \\
\quad \texttt{let} \\
\qquad a = t^2 \, \|\mathbf{v}_{o(x,y)}\|^2 \\
\qquad b = 2t \, (\mathbf{s} - t \, \mathbf{v}_i)_{(x,y)} \cdot \mathbf{v}_{o(x,y)} \\
\qquad c = \|(\mathbf{s} - t\mathbf{v}_i)_{(x,y)}\|^2 - D^2 \\
\quad \texttt{in} \\
\qquad \texttt{if } b^2 - 4ac \geq 0 \texttt{ then} \\
\qquad\quad \texttt{let} \\
\qquad\qquad \ell = \dfrac{b^2 + \varepsilon \sqrt{b^2 - 4ac}}{2a} \\
\qquad\qquad \mathbf{v}'_o = \max(\ell, 0) \, \mathbf{v}_{o(x,y)} \texttt{ with } [z \leftarrow \mathbf{v}_{oz}] \\
\qquad\quad \texttt{in} \\
\qquad\qquad \texttt{if } \iota \, (\mathbf{s} + t \, (\mathbf{v}'_o - \mathbf{v}_i))_{(x,y)} \cdot (\mathbf{v}'_o - \mathbf{v}_i)_{(x,y)} \geq 0 \texttt{ then} \\
\qquad\qquad\quad \mathbf{v}'_o \\
\qquad\qquad \texttt{else} \\
\qquad\qquad\quad \mathbf{0} \\
\qquad\qquad \texttt{endif} \\
\qquad \texttt{else} \\
\qquad\quad \mathbf{0} \\
\qquad \texttt{endif}
\end{array}
\tag{49}
$$

The correctness and completeness of `gs_circle_2D` follow from its definition and the correctness and completeness of the quadratic formula, which has been proved in PVS.

Theorem 32 (Correctness of `gs_circle_2D`)**.** *If* $\mathbf{v}_{o(x,y)} \neq 0$ *and*

$$\mathbf{v}'_o = \textit{gs\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon),$$

then circle_case_2D?$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ *holds,* $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$*, and* $\mathbf{v}'_{o(x,y)} = \ell \, \mathbf{v}_{o(x,y)}$ *for some* $\ell > 0$*.*

Theorem 33 (Completeness of `gs_circle_2D`)**.** *If* $\mathbf{v}'_{o(x,y)} = \ell \mathbf{v}_{o(x,y)}$*,* $\ell > 0$*,* $\mathbf{v}'_{oz} - \mathbf{v}_{oz}$*, and circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ *holds, then*

$$\mathbf{v}'_o = \textit{gs\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \iota, \varepsilon),$$

for some $\varepsilon = \pm 1$*.*

6.3 3D Circle Solutions For Ground Speed Maneuvers

Theorems 32 and 33 imply that the algorithm `gs_circle_2D` can be used to compute vectors $\mathbf{v}'_o$ such that *circle_case_2D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ holds, where $t > 0$. By the

definition of the predicate *circle_case_3D?* in Section 4.3, this algorithm can be used to compute vectors $\mathbf{v}'_o$ such that *circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(s_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ holds when $\Theta_H(s_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota) > 0$. This motivates the definition of the algorithm `gs_circle_3D`, which takes as a parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, ι, and ε. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ such that the relative velocity vector $\mathbf{v}' = \mathbf{v}'_o - \mathbf{v}_i$ satisfies *circle_case_3D?*$(\mathbf{s}, \mathbf{v}', \Theta_H(\mathbf{s}_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$.

```
gs_circle_3D(s, v_o, v_i, ι, ε) ≡
    if v_oz = v_iz then
        0
    else
        let
            t = Θ_H(s_z, v_oz − v_iz, −ι)
        in
            if t > 0 then
                gs_circle_2D(s, v_o, v_i, t, ι, ε)
            else
                0
            endif
    endif
```
(50)

The following theorems state that `gs_circle_3D` is correct and complete for 3D circle solutions that are ground speed maneuvers. These properties follow from theorems 32 and 33, and properties of the function Θ_H presented in Section 4.6.

Theorem 34 (Correctness of `gs_circle_3D`)**.** *If* $\mathbf{v}'_{o(x,y)} \neq \mathbf{0}$ *and*

$$\mathbf{v}'_o = \textit{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon),$$

then circle_case_3D?$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(s_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ *holds,* $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$*, and* $\mathbf{v}'_{o(x,y)} = \ell\, \mathbf{v}_{o(x,y)}$ *for some* $\ell > 0$*.*

Theorem 35 (Completeness of `gs_circle_3D`)**.** *If* $\mathbf{v}'_{o(x,y)} = \ell \mathbf{v}_{o(x,y)}$*,* $\ell > 0$*,* $\mathbf{v}'_{oz} = \mathbf{v}_{oz}$*,* $\mathbf{v}_{oz} \neq \mathbf{v}_{iz}$*, and circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, \Theta_H(s_z, \mathbf{v}_{oz} - \mathbf{v}_{iz}, -\iota), \iota)$ *holds, then*

$$\mathbf{v}'_o = \textit{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, \iota, \varepsilon),$$

for some $\varepsilon = \pm 1$*.*

6.4 A Prevention Bands Algorithm For Ground Speed Maneuvers

The prevention bands algorithm `gs_bands` for the function $\nu_{\text{gs}} \colon \mathbb{R} \mapsto \mathbb{R}^3$ that computes a sorted sequence $L_{\nu_{\text{gs}}}$ is defined in a similar way to algorithm `track_bands` in Section 5.5.

$$
\begin{array}{l}
\texttt{gs\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i) \equiv \\
\quad V_0 \ \texttt{:=}\ \texttt{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, -1); \\
\quad V_1 \ \texttt{:=}\ \texttt{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1, 1); \\
\quad V_2 \ \texttt{:=}\ \texttt{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, -1); \\
\quad V_3 \ \texttt{:=}\ \texttt{gs\_circle\_3D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, 1, 1); \\
\quad \texttt{if}\ \|\mathbf{s}_{(x,y)}\| \geq D\ \texttt{then} \\
\quad\quad V_4 \ \texttt{:=}\ \texttt{gs\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, -1, -1); \\
\quad\quad V_5 \ \texttt{:=}\ \texttt{gs\_circle\_2D}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, -1, 1); \\
\quad\quad V_6 \ \texttt{:=}\ \texttt{gs\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1); \\
\quad\quad V_7 \ \texttt{:=}\ \texttt{gs\_line}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, -1); \\
\quad \texttt{endif} \\
\quad \mathcal{L} = \{gsmin, gsmax\}; \\
\quad \texttt{for}\ i = 1\ \texttt{to}\ |V|\ \texttt{do} \\
\quad\quad \texttt{if}\ V_{i(x,y)} \neq \mathbf{0}\ \texttt{and}\ gsmin \leq \|V_{i(x,y)}\| \leq gsmax\ \texttt{then} \\
\quad\quad\quad \mathcal{L}\ \texttt{:=}\ \mathcal{L} \cup \{\|V_{i(x,y)}\|\}; \\
\quad\quad \texttt{endif} \\
\quad \texttt{endfor} \\
\quad L_{\nu_{\text{gs}}}\ \texttt{:=}\ \texttt{sort}(\mathcal{L});
\end{array}
\tag{51}
$$

Theorem 36 (Correctness of `gs_bands`)**.** *The ground speed prevention bands algorithm* ***`gs_bands`*** *is correct for ν_{gs} over the interval $[gsmin, gsmax]$.*

Proof. The first step in the proof is to consider the special case where $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_o^{\perp}{}_{(x,y)} = 0$, and $\mathbf{v}_{o(x,y)} \cdot \texttt{tangent\_line}(\mathbf{s}, \varepsilon)^{\perp}{}_{(x,y)} = 0$. This case is handled separately because it is explicity excluded from the hypotheses of Theorem 31. In this case, it can be proved that the vectors $\texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)}$, $\mathbf{v}_{o(x,y)}$, and $\mathbf{v}_{i(x,y)}$ are all co-linear.

To prove correctness of the algorithm for the special case, it suffices to show that if $p \in [gsmin, gsmax]$, then *conflict?*$(\mathbf{s}, \nu_{\text{gs}}(p) - \mathbf{v}_i)$ does not hold. Since $\nu_{\text{gs}}(p)$ is a ground speed maneuver of $\mathbf{v}_o$, both vectors point in the same direction. Therefore, $\nu_{\text{gs}}(p)_{(x,y)} - \mathbf{v}_{i(x,y)}$ is also co-linear with $\texttt{tangent\_line}(\mathbf{s}, \varepsilon)_{(x,y)}$. The trajectory from $\mathbf{s}_{(x,y)}$ along $\nu_{\text{gs}}(p)_{(x,y)} - \mathbf{v}_{i(x,y)}$ is therefore tangent to the circle of radius D around the origin and is never in horizontal conflict.

In the general case, suppose that it is not true that $\|\mathbf{s}_{(x,y)}\| \geq D$, $\mathbf{v}_{i(x,y)} \cdot \mathbf{v}_o^{\perp}{}_{(x,y)} = 0$, and $\mathbf{v}_{o(x,y)} \cdot \texttt{tangent\_line}(\mathbf{s}, \varepsilon)^{\perp}{}_{(x,y)} = 0$. In this case, by Theorem 2 in Section 2.5, it suffices to prove that the function Ω_ν, where $\nu = \nu_{\text{gs}}$, satisfies the following two properties.

1. For all ground speeds $p \in [gsmin, gsmax]$,

$$\Omega_\nu(p) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu_{\text{gs}}(p) - \mathbf{v}_i).$$

2. For all ground speeds $p \in [gsmin, gsmax]$,

$$\Omega_\nu(p) = 1 \implies p \in \texttt{gs\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i).$$

The first of these properties follows immediately from Corollary 7 in Section 3.3. All that is left to verify is the second property, the proof of which is identical in form and substance to the general case of the proof of Theorem 29 in Section 5.5. □

7 Vertical Speed Prevention Bands

This section presents a formally verified algorithm, namely `vs_bands`, for vertical speed prevention bands over an arbitrary interval $[vsmin, vsmax]$ for the function $\nu_{\text{vs}}\colon \mathbb{R} \to \mathbb{R}^3$, defined by Equation (5) in Section 2.2. The boundaries of the interval, $vsmin$ and $vsmax$, represent minimum and maximum vertical speeds for the ownship aircraft, respectively. Given vectors $\mathbf{s}$, $\mathbf{v}_o$, and $\mathbf{v}_i$, this algorithm computes vertical speed maneuvers, i.e., vectors $\mathbf{v}'_o$ that satisfy $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$.

The definition of `vs_bands` depends on the algorithm `vs_circle`, which computes vertical speed maneuvers that are 3D circle solutions and vertical solutions. This algorithm is proved to be complete for vertical speed maneuvers. The correctness of `vs_bands` depends on the completeness of `vs_circle`.

By the definition of *circle_case_3D?* in Equation (21), *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$ implies *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, t, -\iota)$ and *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$ for any $t \in \mathbb{R}$ and $\iota = \pm 1$. Thus, an algorithm for computing 3D circle solutions for vertical speed maneuvers will also compute vertical solutions and 2D circle solutions. If *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, t, -\iota)$ holds, then $|\mathbf{s}_z + t\,\mathbf{v}_z| = H$, and therefore there is some $\varepsilon = \pm 1$ such that $\mathbf{s}_z + t\,\mathbf{v}_z = \varepsilon\,H$. The function `vs_at`, defined below, takes as parameters $\mathbf{s}_z$, a nonzero real number t, and $\varepsilon = \pm 1$. It returns the real number $\mathbf{v}_z$ such that $\mathbf{s}_z + t\mathbf{v}_z = \varepsilon\,H$.

$$\texttt{vs\_at}(\mathbf{s}_z, t, \varepsilon) \equiv \frac{\varepsilon\,H - \mathbf{s}_z}{t}. \tag{52}$$

Lemma 37. *If $\mathbf{v}_z$ is a real number, then $\mathbf{s}_z + t\mathbf{v}_z = \varepsilon\,H$ if and only if*

$$\mathbf{v}_z = \mathit{vs\_at}(\mathbf{s}_z, t, \varepsilon).$$

The next lemma states that the function `vs_at` can be used to compute vertical solutions. The proof follows from Equation (19) and Lemma 37.

Lemma 38. *If $t > 0$ and vertical_case?$(\mathbf{s}_z, \mathbf{v}_z, t, -1)$ holds, then*

$$\mathbf{v}_z = \mathit{vs\_at}(\mathbf{s}_z, t, \mathit{sign}(\mathbf{s}_z))$$

.

7.1 3D Circle and Vertical Solutions For Vertical Speed Maneuvers

The algorithm `vs_circle`, defined in this section, takes as parameters $\mathbf{s}$, $\mathbf{v}_o$, $\mathbf{v}_i$, t, and $\varepsilon = \pm 1$. It returns a vector $\mathbf{v}'_o$ that is either the zero vector or is equal

to $\nu_{\text{vs}}(r)$ for some $r \in \mathbb{R}$ such that the relative vector $\mathbf{v} = \mathbf{v}'_o - \mathbf{v}_i$ satisfies *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$. The main theorems in this section state that `vs_circle` computes all 3D circle solutions and all vertical solutions that are vertical speed maneuvers.

Suppose that $\Delta(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i) > 0$ and *circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t, \iota)$ holds, where $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$ and $\mathbf{v}'_{oz} = r$. It is easy to prove that $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) > 0$ implies $\mathbf{v}_{o(x,y)} \neq \mathbf{v}_{i(x,y)}$. Since $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) = \Delta(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i)$, Corollary 14 in Section 4.6 implies that $t = \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota)$. Since *vertical_case?*$(\mathbf{s}_z, (r - \mathbf{v}_{iz}), t, -\iota)$ holds, there is some $\varepsilon = \pm 1$ such that

$$\mathbf{s}_z + \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota)\,(r - \mathbf{v}_{iz}) = \varepsilon\, H. \tag{53}$$

Since $\Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota) > 0$, the following equivalence holds.

$$r = \mathbf{v}_{iz} \iff H = \varepsilon\, \mathbf{s}_z.$$

Suppose that $H \neq \varepsilon\, \mathbf{s}_z$. Multiplying both sides of Equation (53) by ε and applying the fact that $\varepsilon^2 = 1$ yields

$$\varepsilon\, \mathbf{s}_z + \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota)\, \varepsilon\, (r - \mathbf{v}_{iz}) = H.$$

Since $\Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota) > 0$, it follows that

$$-\operatorname{sign}(\varepsilon\,(r - \mathbf{v}_{iz})) = \operatorname{sign}(\varepsilon\, \mathbf{s}_z \;-\; H). \tag{54}$$

Since *vertical_case?*$(\mathbf{s}_z, (r - \mathbf{v}_{iz}), \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota), -\iota)$ holds,

$$-\iota\,(\mathbf{s}_z + \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota)(r - \mathbf{v}_{iz}))\,(r - \mathbf{v}_{iz}) \;\geq 0.$$

It therefore follows from Equation (53) that $-\iota\, \varepsilon\, H\,(r - \mathbf{v}_{iz}) \geq 0$. Since $H > 0$ and $r \neq \mathbf{v}_{iz}$, basic arithmetic manipulations can be used to deduce that

$$-\operatorname{sign}(\varepsilon\,(r - \mathbf{v}_{iz})) = \iota. \tag{55}$$

Putting equations (54) and (55) together, the following equality holds.

$$\operatorname{sign}(\varepsilon\, \mathbf{s}_z \;-\; H) = \iota \tag{56}$$

This equation is used to select the appropriate choice of ι in the algorithm `vs_circle`, defined below in Equation (52), even in the case where $\varepsilon\, \mathbf{s}_z = H$. It follows from Lemma 37 that

$$r = \mathbf{v}_{iz} + \texttt{vs\_at}(\mathbf{s}_z, \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota), \varepsilon). \tag{57}$$

This equation also appears in the definition of `vs_circle`, which is given below. It returns a vector $\mathbf{v}'_o \in \mathbb{R}^3$ such that either $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$ or $\mathbf{v}'_o = \mathbf{0}$.

$$
\begin{array}{l}
\texttt{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \varepsilon) \equiv \\
\quad \texttt{if } \Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) \leq 0 \texttt{ then} \\
\quad\quad \texttt{if } \varepsilon\, \mathbf{s}_z \geq H \texttt{ and } t > 0 \texttt{ then} \\
\quad\quad\quad \mathbf{v}_{o(x,y)} \texttt{ with } [z \leftarrow \mathbf{v}_{iz} + \texttt{vs\_at}(\mathbf{s}_z, t, \varepsilon)] \\
\quad\quad \texttt{else} \\
\quad\quad\quad \mathbf{0} \\
\quad\quad \texttt{endif} \\
\quad \texttt{else} \\
\quad\quad \texttt{let} \\
\quad\quad\quad \Theta_{-1} = \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, -1), \\
\quad\quad\quad \Theta_{+1} = \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1), \\
\quad\quad\quad \tau_{min} = \min(t, \Theta_D(s, \mathbf{v}_o - \mathbf{v}_i, 1)) \\
\quad\quad \texttt{in} \\
\quad\quad\quad \texttt{if } \varepsilon\, \mathbf{s}_z < H \texttt{ and } \|\mathbf{s}_{(x,y)}\| > D \texttt{ then} \\
\quad\quad\quad\quad \mathbf{v}_{o(x,y)} \texttt{ with } [z \leftarrow \mathbf{v}_{iz} + \texttt{vs\_at}(\mathbf{s}_z, \Theta_{-1}, \varepsilon)] \\
\quad\quad\quad \texttt{elsif } \varepsilon\, \mathbf{s}_z \geq H \texttt{ and } \tau_{min} > 0 \texttt{ then} \\
\quad\quad\quad\quad \mathbf{v}_{o(x,y)} \texttt{ with } [z \leftarrow \mathbf{v}_{iz} + \texttt{vs\_at}(\mathbf{s}_z, \tau_{min}, \varepsilon)] \\
\quad\quad\quad \texttt{else} \\
\quad\quad\quad\quad \mathbf{0} \\
\quad\quad\quad \texttt{endif} \\
\quad \texttt{endif}
\end{array}
\tag{58}
$$

The completeness of `vs_circle` for 3D circle and vertical solutions follows from its definition, Lemma 38, and properties of the function Θ_D presented in Section 4.6.

Theorem 39 (Completeness of `vs_circle` for 3D Circle Solutions)**.** *If* $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$*,* $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) > 0$*,* $\iota = \pm 1$*,* $t > 0$*, circle_case_3D?*$(\mathbf{s}, \mathbf{v}'_o - \mathbf{v}_i, t', \iota)$*, for some* $t' \in \mathbb{R}$*, and either* $\iota = -1$ *or* $\Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1) \leq t$*, then*

$$\mathbf{v}_o = \textit{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \varepsilon),$$

for some $\varepsilon = \pm 1$*.*

Theorem 40 (Completeness of `vs_circle` for Vertical Solutions)**.** *If* $\mathbf{v}'_{o(x,y)} = \mathbf{v}_{o(x,y)}$*, vertical_case?*$(\mathbf{s}_z, \mathbf{v}'_{oz} - \mathbf{v}_{iz}, t, -1)$*, and either* $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) \leq 0$ *or* $t \leq \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1)$*, then*

$$\mathbf{v}'_o = \textit{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, t, \varepsilon),$$

for some $\varepsilon = \pm 1$*.*

7.2 A Prevention Bands Algorithm For Vertical Speed Maneuvers

The prevention bands algorithm `vs_bands` for the function $\nu_{\rm vs}\colon \mathbb{R} \mapsto \mathbb{R}^3$ that computes a sorted sequence $L_{\nu_{\rm vs}}$ is defined in a similar way to the previous algorithms `track_bands` in Section 5.5 and `gs_bands` in Section 6.4.

$$
\begin{array}{l}
\texttt{vs\_bands}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i) \equiv \\
\quad V_0 \ \texttt{:=}\ \texttt{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, -1); \\
\quad V_1 \ \texttt{:=}\ \texttt{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, 1); \\
\quad \mathcal{L} = \{vsmin, vsmax\}; \\
\quad \texttt{for}\ i = 1\ \texttt{to}\ |V|\ \texttt{do} \\
\qquad \texttt{if}\ V_{i(x,y)} \neq \mathbf{0}\ \texttt{and}\ vsmin \leq V_{i_z} \leq vsmax\ \texttt{then} \\
\qquad\quad \mathcal{L}\ \texttt{:=}\ \mathcal{L} \cup \{V_{iz}\}; \\
\qquad \texttt{endif} \\
\quad \texttt{endfor} \\
\quad L_{\nu_{\rm vs}}\ \texttt{:=}\ \texttt{sort}(\mathcal{L});
\end{array}
\tag{59}
$$

Theorem 41 (Correctness of `vs_bands`)**.** *The vertical speed prevention bands algorithm* ***`vs_bands`*** *is correct for ν_{vs} over the interval $[vsmin, vsmax]$.*

Proof. By Theorem 2 in Section 2.5, it suffices to prove that the function Ω_ν, where $\nu = \nu_{\rm vs}$, satisfies the following two properties.

1. For all vertical speeds $r \in [vsmin, vsmax]$,

$$\Omega_\nu(r) < 1 \iff \textit{conflict?}(\mathbf{s}, \nu_{\rm vs}(r) - \mathbf{v}_i).$$

2. For all vertical speeds $r \in [vsmin, vsmax]$,

$$\Omega_\nu(r) = 1 \implies r \in \texttt{vs\_bands}(\mathbf{s}, T, \mathbf{v}_o, \mathbf{v}_i).$$

The first of these properties follows immediately from Corollary 7 in Section 3.3. To prove the second property, suppose that $r \in [vsmin, vsmax]$ and $\Omega_\nu(r) = 1$, where $\nu = \nu_{\rm vs}$. Since $\Omega_\nu(r) = \Omega(\mathbf{s}, \nu_{\rm vs}(r) - \mathbf{v}_i)$, Theorem 9 implies that one of the following conditions holds, where $\mathbf{v} = \nu_{\rm vs}(r) - \mathbf{v}_i$.

- $\|\mathbf{s}_{(x,y)}\| \geq D$ and either *line_case?*$(\mathbf{s}, \mathbf{v}, -1)$ or *line_case?*$(\mathbf{s}, \mathbf{v}, 1)$.
- $|\mathbf{s}_z + T\mathbf{v}_z| < H$ and *circle_case_2D?*$(\mathbf{s}, \mathbf{v}, T, -1)$.
- There is some real number $t > 0$ such that either *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$, for some $\iota = \pm 1$.
- $\|\mathbf{s}_{(x,y)} + T\mathbf{v}_{(x,y)}\| \leq D$ and *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$.

In either of the first two cases, it can easily be shown that *conflict?*$(\mathbf{s}, \nu_{\rm vs}(x) - \mathbf{v}_i)$ does not hold for any $x \in \mathbb{R}$. In this case, by Definition 2 in Section 2.4, it follows that the prevention bands algorithm `vs_bands` is correct for $\nu_{\rm vs}$ over $[vsmin, vsmax]$.

The latter two cases are considered individually. For the rest of the proof, it is assumed that $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) > 0$. The proof in the case where $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) \leq 0$ is left to the reader. Since $\Delta(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i) > 0$, it is easy to prove that $\mathbf{v}_{o(x,y)} \neq \mathbf{v}_{i(x,y)}$.

Suppose that there is some real number $t > 0$ such that *circle_case_3D?*$(\mathbf{s}, \mathbf{v}, t, \iota)$, where $\iota = \pm 1$. By the definition of *circle_case_3D?* (Equation (21) in Section 4.3) and Corollary 14 in Section 4.6, it follows that $t = \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota)$. By Theorem 39 in Section 7.1 (completenes of `vs_circle` for 3D circle solutions), if either $\iota = -1$ or $\Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, \iota) \leq T$, then $\nu_{\text{vs}}(r)$ is equal to $\texttt{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, \varepsilon)$, for some $\varepsilon = \pm 1$. Thus, $r \in \texttt{vs\_bands}(\mathbf{s}, T, \mathbf{v}_o, vi)$. Alternatively, if $\iota = 1$ and $\Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1) > T$, it can be proved from the definition of the function Ω_ν that $\Omega_\nu(r) > 1$, a contradiction.

Finally, suppose that $\|\mathbf{s}_{(x,y)} + T\mathbf{v}_{(x,y)}\| \leq D$ and *vertical_case?*$(\mathbf{s}_z, \mathbf{v}_z, T, -1)$. The proof in this case is similar to the case above. By Theorem 40 in Section 7.1 (completeness of `vs_circle` for vertical solutions), if $T \leq \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1)$, then $\nu_{\text{vs}}(r)$ is equal to $\texttt{vs\_circle}(\mathbf{s}, \mathbf{v}_o, \mathbf{v}_i, T, \varepsilon)$, for some $\varepsilon = \pm 1$. Thus, it holds that $r \in \texttt{vs\_bands}(\mathbf{s}, T, \mathbf{v}_o, vi)$. Alternatively, if $T > \Theta_D(\mathbf{s}, \mathbf{v}_o - \mathbf{v}_i, 1)$, it can be proved that $\Omega_\nu(r) > 1$, a contradiction. □

8 Conclusion

In [3], Maddalon et al. present, without verification, 3D algorithms for track angle, ground speed, and vertical speed prevention bands. Formal verification of horizontal versions of these algorithms was presented in [2]. This paper provides correct versions of the algorithms presented in [3], namely `track_bands` (Section 5.5), `gs_bands` (Section 6.4), and `vs_bands` (Section 7.2). The correctness of these algorithms has been formally verified using the PVS theorem prover.

Although this paper focuses on track angle, ground speed, and vertical speed prevention bands, the techniques presented here applied to arbitrary conflict prevention bands algorithms that are based on state information. More precisely, given a function $\nu\colon \mathbb{R} \to \mathbb{R}^3$ and an interval $I \subset \mathbb{R}$, Section 2.5 describes a general strategy that can be followed to prove that a given prevention bands algorithm is correct. In fact, Section 3 develops the theory of a universal function Ω that can be used as a tool in the verification of prevention bands algorithms for many different choices of ν.

References

1. Ricky Butler, George Hagen, Jeffrey Maddalon, César Muñoz, Anthony Narkawicz, and Gilles Dowek. How formal methods impels discovery: A short history of an air traffic management project. In César Muñoz, editor, *Proceedings of the Second NASA Formal Methods Symposium (NFM 2010), NASA/CP-2010-216215*, pages 34–46, Langley Research Center, Hampton VA 23681-2199, USA, April 2010. NASA.

2. Jeffrey Maddalon, Ricky Butler, César Muñoz, and Gilles Dowek. A mathematical analysis of conflict prevention information. In *Proceedings of the AIAA 9th Aviation, Technology, Integration, and Operations Conference, AIAA-2009-6907*, Hilton Head, South Carolina, USA, September 2009.

3. Jeffrey Maddalon, Ricky Butler, César Muñoz, and Gilles Dowek. Mathematical basis for the safety analysis of conflict prevention algorithms. Technical Memorandum NASA/TM-2009-215768, NASA, Langley Research Center, Hampton VA 23681-2199, USA, June 2009.

4. Sam Owre, John Rushby, and Natarajan Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *Proceeding of the 11th International Conference on Automated Deductioncade*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752. Springer, June 1992.

5. Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill, third edition, 1976.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 06 - 2010	Technical Memorandum	

Formal Verification of Air Traffic Confict Prevention Bands Algorithms

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Narkawicz, Anthony J.; Muñoz, César A.; Dowek, Gilles

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
411931.02.51.07.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L-19881

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM-2010-216706

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In air traffic management, a pairwise conflict is a predicted loss of separation between two aircraft, referred to as the ownship and the intruder. A conflict prevention bands system computes ranges of maneuvers for the ownship that characterize regions in the airspace that are either conflict-free or `don't go' zones that the ownwhip has to avoid. Conflict prevention bands are surprisingly difficult to define and analyze. Errors in the calculation of prevention bands may result in incorrect separation assurance information being displayed to pilots or air traffic controllers. This paper presents provably correct 3-dimensional prevention bands algorithms for ranges of track angle, ground speed, and vertical speed maneuvers. The algorithms have been mechanically verified in the Prototype Verification System (PVS). The verification presented in this paper extends in a non-trivial way that of previously published 2-dimensional algorithms.

15. SUBJECT TERMS
Air traffic; Avoidance; Conflict; Detection; Prevention; Resolution

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	50	(443) 757-5802