NASA/TM-2009-215726

Formally Verified Practical Algorithms For Recovery From Loss of Separation

Ricky W. Butler
Langley Research Center, Hampton, Virginia

César A. Muñoz
National Institute of Aerospace, Hampton, Virginia

June 2009

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-2009-215726

Formally Verified Practical Algorithms For Recovery From Loss of Separation

Ricky W. Butler
Langley Research Center, Hampton, Virginia

César A. Muñoz
National Institute of Aerospace, Hampton, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

June 2009

Available from:

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

Abstract

In this paper, we develop and formally verify practical algorithms for recovery from loss of separation. The formal verification is performed in the context of a criteria-based framework. This framework provides rigorous definitions of horizontal and vertical *maneuver correctness* that guarantee divergence and achieve horizontal and vertical separation. The algorithms are shown to be independently correct, that is, separation is achieved when only one aircraft maneuvers, and implicitly coordinated, that is, separation is also achieved when both aircraft maneuver. In this paper we improve the horizontal criteria over our previous work. An important benefit of the criteria approach is that different aircraft can execute different algorithms and implicit coordination will still be achieved, as long as they all meet the explicit criteria of the framework. Towards this end we have sought to make the criteria as general as possible. The framework presented in this paper has been formalized and mechanically verified in the Prototype Verification System (PVS).

Contents

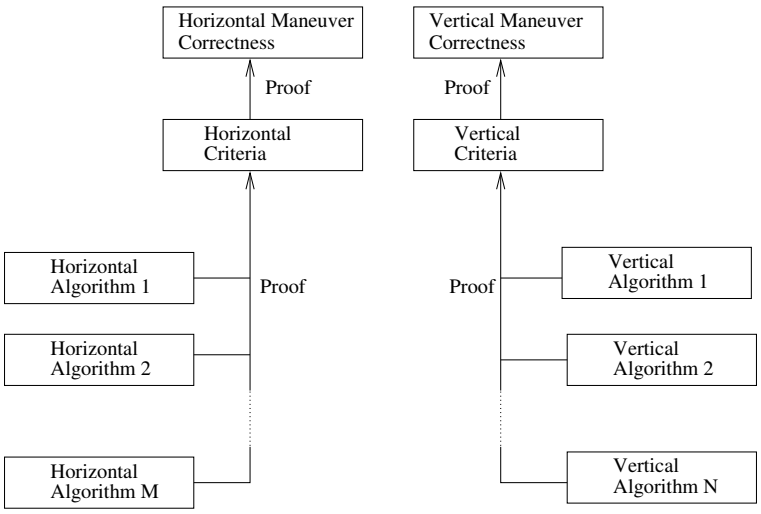


Figure 1. Criteria-based algorithm verification

1 Introduction

As the density of the national airspace increases, conflicts involving multiple aircraft will also increase. Inevitably there will be situations where even the tactical state-based conflict detection algorithms will not be able to prevent a loss of separation (LoS). Although algorithms have been developed that have been formally verified to provide coordinated and independent solutions, e.g., [2, 3], these proofs assume that there are at most two aircraft in conflict. Furthermore, these proofs make other idealistic assumptions: (1) that aircraft state data is perfectly known, (2) the translation of the mathematical algorithms into executable programs is without error, (3) the pilots execute the maneuvers as directed by the software and do so within a suitable amount of time, and (4) the aircraft have adequate performance to achieve the recommended solutions before a loss of separation occurs. It is therefore essential that robust algorithms for recovery from LoS be designed and verified.

In our previous work [1], we developed a criteria-based framework for reasoning about LoS algorithms. We first developed a formal specification of what it means for an algorithm to be correct. Then, rather than proceed immediately to an algorithm that satisfies the correctness property, we proposed an intermediate level called the *criteria level*. The verification process is thereby decomposed into two steps: (1) the criteria to correctness proof and (2) the algorithm to criteria proof. The first step is accomplished once and for all, while the second step is performed for each new algorithm that is developed. This approach is illustrated in Figure 1.

We have separate concepts of correctness and, therefore, separate criteria for the horizontal and vertical dimensions. There is a formal proof that the horizontal criteria satisfies the horizontal correctness property and a formal proof that the vertical criteria satisfies the vertical correctness property. Many different algorithms can then be shown to satisfy the criteria and thereby inherit the correctness asso-

ciated properties. One interesting consequence is that all possible combinations of the algorithms that meet the criteria will all have coordinated solutions. We believe that this is a very powerful enabler for distributed conflict detection and resolution. Each aircraft can execute its own algorithm as long as it satisfies the criteria. This is in stark contrast to the approach used in TCAS II where every aircraft is mandated to execute exactly the same algorithm. Another goal of this endeavor was to push most of the verification burden into the criteria-to-correctness proof so as to simplify the individual proofs of the algorithms. We were able to achieve this goal in the previous work for the vertical case only. In this paper we revise the criteria for the horizontal case in a manner that we believe achieves this goal for the horizontal case as well. We then proceed to develop a horizontal algorithm that satisfies the revised criteria.

2 Basic Concepts

As typical of state-based approaches, our framework is centered around the idea of modeling aircraft trajectories as linear functions of time into a 3-dimensional vector space with coordinates `x`, `y`, and `z`.

The theory is concerned with only two aircraft at a time. We will refer to one as the *ownship* and the other as the *traffic aircraft*. Position and velocity vectors for the ownship are denoted $\mathbf{s_o}$ and $\mathbf{v_o}$, respectively. Traffic vectors are referenced by i, e.g., $\mathbf{s_i}$ and $\mathbf{v_i}$, and new velocity vectors are denoted by primed variables, e.g., $\mathbf{v'_o}$ and $\mathbf{v'_i}$. It is often convenient to use a relative coordinate system where the traffic aircraft is located at the origin of the system and is motionless. The relative position and velocity vectors of the ownship are denoted $\mathbf{s}$ and $\mathbf{v}$, respectively, where $\mathbf{s} = \mathbf{s_o} - \mathbf{s_i}$ and $\mathbf{v} = \mathbf{v_o} - \mathbf{v_i}$. Note that vector variables are written in boldface and their components are referenced by sub-indices, e.g., v_x, v_y, and v_z.

If D and H are, respectively, the minimum horizontal and vertical separation, the predicates that test if the aircraft are horizontally or vertically separated are defined in the relative coordinate system as follows

$$\texttt{horizontal\_separation?}(\mathbf{s}) \equiv s_x^2 + s_y^2 \geq D^2,$$
$$\texttt{vertical\_separation?}(\mathbf{s}) \equiv |s_z| \geq H,$$
$$\texttt{separation?}(\mathbf{s}) \equiv \texttt{horizontal\_separation?}(\mathbf{s})\ \texttt{OR}\ \texttt{vertical\_separation?}(\mathbf{s}).$$

Note that within the translated frame of reference, the concept of *protected zone* can be defined as a cylinder of radius D and height $2H$ centered at the traffic aircraft.

From these predicates, we define *loss of separation* as follows

$$\texttt{loss\_of\_separation?}(\mathbf{s}) \equiv \texttt{NOT separation?}(\mathbf{s}).$$

Therefore, the condition that the aircraft have lost separation can be simply expressed as $\texttt{loss\_of\_separation?}(\mathbf{s})$, where $\mathbf{s} = \mathbf{s_o} - \mathbf{s_i}$.

In our previous work on loss of separation [1], we proposed a concept of correctness for both horizontal and vertical resolutions in the loss of separation situation.

A resolution vector $\mathbf{v_o}$ is *horizontally correct* with respect to the relative position $\mathbf{s}$ and the traffic's velocity vector $\mathbf{v_i}$ if and only if

- `xy_divergent?`$(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i})$, and
- `horizontal_separation?`$(\mathbf{s} + T_h(\mathbf{v_o} - \mathbf{v_i}))$.

where horizontal divergence is defined as follows:

$$\texttt{xy\_divergent?}(\mathbf{s}, \mathbf{v}) \equiv \forall t : t > 0 \implies ||\mathbf{s}|| < ||\mathbf{s} + t\mathbf{v}||.$$

where the norms are two dimensional over the x and y components. The parameter T_h specifies a maximum time to recover in the horizontal dimension. A resolution vector $\mathbf{v_o}$ is *vertically correct* with respect to the relative position $\mathbf{s}$ and the traffic's velocity vector $\mathbf{v_i}$ if and only if

- `z_divergent?`$(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i})$, and
- `vertical_separation?`$(\mathbf{s} + T_v(\mathbf{v_o} - \mathbf{v_i}))$.

where

$$\texttt{z\_divergent?}(\mathbf{s}, \mathbf{v}) \equiv \forall t : t > 0 \implies |s_z| < |s_z + v_z t|.$$

3 Revised Horizontal Criteria

In our previous work on loss of separation [1] our criteria was built around a predicate called `dot_prop` which was defined as $\texttt{dot\_prop}(\mathbf{s}, \mathbf{v}) \equiv \mathbf{s} \cdot \mathbf{v} \geq 0$. The horizontal criteria proposed was

$$\begin{aligned}
&\texttt{criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v_o'}) \equiv \\
&\quad \mathbf{v_o'} \neq \mathbf{v_i} \ \texttt{AND} \\
&\quad \texttt{dot_prop?}(\mathbf{s}, \mathbf{v_o'} - \mathbf{v_i}) \ \texttt{AND} \\
&\quad \texttt{dot_prop?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i}) \implies \\
&\qquad (\mathbf{v_o} \neq \mathbf{v_i} \ \texttt{AND} \ \texttt{dot_prop?}(\mathbf{s}, \mathbf{v_o'} - \mathbf{v_o}) \\
&\qquad \ \texttt{OR} \\
&\qquad (\mathbf{v_o} = \mathbf{v_i} \ \texttt{AND} \ \mathbf{s} \cdot (\mathbf{v_o'} - \mathbf{v_o}) > 0)).
\end{aligned}$$

In this paper, we offer a revision of this criteria that is much simpler:

$$\begin{aligned}
&\texttt{criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v_o'}) \equiv \\
&\qquad \mathbf{s} \cdot (\mathbf{v_o'} - \mathbf{v_i}) > 0 \ \texttt{AND} \\
&\qquad \mathbf{s} \cdot (\mathbf{v_o'} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}).
\end{aligned} \tag{1}$$

Our original criteria only dealt with the sign of the dot product while our new criteria involves the size of the dot product. The rationale for this criteria is clear now that it has been cast in this form. The first conjunction $\mathbf{s} \cdot (\mathbf{v_o'} - \mathbf{v_i}) > 0$ insures divergence when the aircraft are originally convergent (see lemma `dot_pos_divergent` below).

But when the aircraft are already divergent, then some additional logic is needed to achieve coordination. We discovered that if we merely required that the dot product of the new velocity vector is greater than or equal to the current dot product then coordination is achieved. But this is ideal because there is no reason to allow a maneuver where the dot product is smaller, because that would only increase the time to exit. A key insight is that the time to exit is related to the magnitude of the dot product.

We will now develop the formal mathematics. For convenience we define a predicate `dot_pos?`:

$$\texttt{dot\_pos?}(\mathbf{s}, \mathbf{v}) \equiv \mathbf{s} \cdot \mathbf{v} > 0.$$

We then relate this predicate to divergence as follows:

Theorem 3.1 (`dot_pos_divergent`)**.**

$$\begin{aligned} &\texttt{dot\_pos?}(\mathbf{s}, \mathbf{v}) \\ &\iff \texttt{xy\_divergent?}(\mathbf{s}, \mathbf{v}). \end{aligned}$$

Proof. The distance between two aircraft at time t is given by

$$||\mathbf{s} + t\mathbf{v}||, \tag{2}$$

where $\mathbf{v} = \mathbf{v'_o} - \mathbf{v_i}$. The distance achieves a minimum where its square is a minimum, so we can work with the square of the distance:

$$\begin{aligned} &||\mathbf{s} + t\mathbf{v}||^2 = \\ &(\mathbf{s} + t\mathbf{v}) \cdot (\mathbf{s} + t\mathbf{v}) = \\ &t^2 v^2 + 2t(\mathbf{s} \cdot \mathbf{v}) + s^2 \end{aligned} \tag{3}$$

where we use the abbreviation $v^2 = ||\mathbf{v}||^2 = \mathbf{v} \cdot \mathbf{v}$. This achieves a minimum where its derivative with respect to t is zero, or where

$$2tv^2 + 2(\mathbf{s} \cdot \mathbf{v}) = 0. \tag{4}$$

That is, the minimum is achieved at time τ:

$$\tau = -\frac{\mathbf{s} \cdot \mathbf{v}}{v^2}. \tag{5}$$

From $\texttt{dot\_pos?}(\mathbf{s}, \mathbf{v})$ we have $\mathbf{s} \cdot \mathbf{v} > 0$, so the time of closest approach τ is negative, i.e., in the past. Therefore, the aircraft are diverging. The proof works in the reverse direction as well. □

The following is an immediate corollary:

Theorem 3.2 (`criteria_independent`)**.**

$$\begin{aligned} &\texttt{criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v'_o}) \\ &\implies \texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i}). \end{aligned}$$

Proof. The premise $\texttt{criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v'_o})$ gives us $\mathbf{s}\cdot(\mathbf{v'_o}-\mathbf{v_i}) > 0$. We instantiate $\mathbf{v}$ in lemma `dot_pos_divergent` (3.1) with $\mathbf{v'_o}-\mathbf{v_i}$ and obtain the desired conclusion. □

Lemma 3.3 (`backbone`)**.** *If the aircraft are originally in a divergent situation and* $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) \leq K$*, then for all non-negative* K*:*

$$\begin{aligned} &\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq K \ \texttt{AND} \\ &-\mathbf{s} \cdot (\mathbf{v'_i} - \mathbf{v_o}) \geq K \\ &\implies \mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v'_i}) \geq K. \end{aligned}$$

Proof. From the premises we have

$$\begin{aligned} &\mathbf{s} \cdot \mathbf{v_o} - \mathbf{s} \cdot \mathbf{v_i} \leq K, \\ &\mathbf{s} \cdot \mathbf{v'_o} - \mathbf{s} \cdot \mathbf{v_i} \geq K, \\ &-\mathbf{s} \cdot \mathbf{v'_i} + \mathbf{s} \cdot \mathbf{v_o} \geq K, \end{aligned}$$

or

$$\begin{aligned} &\mathbf{s} \cdot \mathbf{v_o} - \mathbf{s} \cdot \mathbf{v_i} < K, \\ &-\mathbf{s} \cdot \mathbf{v'_o} + \mathbf{s} \cdot \mathbf{v_i} \leq -K, \\ &+\mathbf{s} \cdot \mathbf{v'_i} - \mathbf{s} \cdot \mathbf{v_o} \leq -K, \end{aligned}$$

Adding these inequalities yields:

$$-\mathbf{s} \cdot \mathbf{v'_o} + \mathbf{s} \cdot \mathbf{v'_i} < -K,$$

or, equivalently,

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v'_i}) > K.$$

□

Theorem 3.4 (`criteria_coordinated`)**.**

$$\begin{aligned} &\texttt{criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v'_o}) \ \texttt{AND} \\ &\texttt{criteria?}(-\mathbf{s}, \mathbf{v_i}, \mathbf{v_o})(\mathbf{v'_i}) \\ &\implies \texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i}). \end{aligned}$$

Proof. The two premises give us:

$$\begin{aligned} &\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}). \\ &-\mathbf{s} \cdot (\mathbf{v'_i} - \mathbf{v_o}) \geq -\mathbf{s} \cdot (\mathbf{v_i} - \mathbf{v_o}). \end{aligned}$$

Case 1: $\texttt{dot\_pos?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i})$. Applying Lemma 3.3 with $K = \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$, we get

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v'_i}) \geq K = \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}).$$

From the case assumption we have $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) > 0$ so $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v'_i}) > 0$ and thus from Lemma `dot_pos_divergent` (3.1) we have the desired conclusion.

Case 2: NOT dot_pos?($\mathbf{s}, \mathbf{v_o} - \mathbf{v_i}$). In this case we have:

$$\begin{aligned}
&\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) \leq 0, \\
&\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq 0, \\
&-\mathbf{s} \cdot (\mathbf{v'_i} - \mathbf{v_o}) \geq 0. \\
&\quad \Longrightarrow \texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i}).
\end{aligned}$$

Expanding these, we obtain

$$\begin{aligned}
-s_x v_{ox} - s_y v_{oy} + s_x v_{ix} + s_y v_{iy} &> 0, \\
s_x v'_{ox} + s_y v'_{oy} - s_x v_{ix} - s_y v_{iy} &\geq 0, \\
-s_x v'_{ix} - s_y v'_{iy} + s_x v_{ox} + s_y v_{oy} &\geq 0.
\end{aligned}$$

Adding these equations together yields

$$s_x v'_{ox} + s_y v'_{oy} - s_x v'_{ix} - s_y v'_{iy} > 0,$$

or, more succinctly,

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v'_i}) > 0,$$

which is dot_pos?($\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i}$). From Lemma dot_pos_divergent (3.1), we have the desired conclusion. □

4 Horizontal Maneuvers for Loss of Separation Recovery

In the previous paper [1], we proposed criteria that guaranteed divergence and a time to exit that was bounded. But we were never able to prove a suitable horizontal theorem for coordination under that criteria. Our new criteria is much simpler and lends itself to some simple algorithms.

Our algorithms are based upon the idea that the time to exit the protection zone can be controlled by seeking solutions that solve $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J$. The larger the value of J, the smaller the time to exit. We will present the mathematical theory and then discuss methods for selecting a suitable value of J.

4.1 Ground Speed Only

4.1.1 Theory

We are concerned with the situation where a loss of separation has already occurred. So we have:

$$||\mathbf{s}|| < D.$$

We seek solutions where

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J. \tag{6}$$

and

$$\mathbf{v_o'} = k\,\mathbf{v_o},$$

in 2 dimensions. Substituting this last equation into the first, we have

$$\mathbf{s} \cdot (k\,\mathbf{v_o} - \mathbf{v_i}) = J.$$

Solving for k:

$$k = \frac{J + (\mathbf{s} \cdot \mathbf{v_i})}{\mathbf{s} \cdot \mathbf{v_o}}, \tag{7}$$

as long as $\mathbf{s} \cdot \mathbf{v_o} \neq 0$.

4.1.2 Algorithm

The algorithm computes a new ground speed using equation (7). If this value is positive a solution is returned, otherwise a zero vector is returned. Note also that the calculation is guarded by a test on $\mathbf{s} \cdot \mathbf{v_o} \neq 0$ to prevent a division by zero.

```
los_gspd(s, v_o, v_i, J) : Vect2 =
        IF s · v_o ≠ 0 THEN
            k = (s · v_i + J) / (s · v_o)
            IF k > 0 THEN
                k v_o
            ELSE
                (0, 0)
            ENDIF
        ELSE
            (0, 0)
        ENDIF
```

The horizontal LoS criteria requires that

$$\mathbf{s} \cdot (\mathbf{v_o'} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}).$$

This is trivially true when the aircraft are originally convergent because $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$ is negative and $J > 0$. When the aircraft are already divergent some additional

logic is needed:

$$
\begin{array}{l}
\texttt{los\_gs}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, J) : \texttt{Vect2} = \\
\quad \mathbf{v'_o} = \texttt{los\_gspd}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, J) \\
\quad \texttt{IF } \mathbf{v'_o} = (0,0) \texttt{ THEN} \\
\qquad (0,0) \\
\quad \texttt{ELSIF } \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) > 0 \texttt{ THEN} \\
\qquad \texttt{IF } \mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) > \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) \texttt{ THEN} \\
\qquad\quad \mathbf{v'_o} \\
\qquad \texttt{ELSE} \\
\qquad\quad \mathbf{v_o} \\
\qquad \texttt{ENDIF} \\
\quad \texttt{ELSE} \\
\qquad \mathbf{v'_o} \\
\quad \texttt{ENDIF}
\end{array}
$$

Coordinated divergence is guaranteed for all values of J. But how should we choose a good value for J? The larger J, the more drastic the maneuver will be. We would like to define a normalized version of this parameter that takes on a value between 0 and 1. To do this we must calculate a maximum value of the dot product $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i})$ as $\mathbf{v'_o}$ is varied. But as the ground speed is increased, the value of this dot product will monotonically increase or decrease because $\mathbf{v'_o} = c\,\mathbf{v_o}$ and $\mathbf{s} \cdot (c\,\mathbf{v_o} - \mathbf{v_i}) = c\,(\mathbf{s} \cdot \mathbf{v_o}) - (\mathbf{s} \cdot \mathbf{v_i})$ which is a linear function. Therefore, we will assume a maximum operational ground speed, say `max_gs`. Then, we calculate a maximum value of the dot product as follows:

$$
\begin{array}{l}
\texttt{maxDot}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}) : \texttt{posreal} = \\
\quad c = \dfrac{\texttt{max\_gs}}{||\mathbf{v_o}||} \\
\quad m = \mathbf{s} \cdot (c\,\mathbf{v_o} - \mathbf{v_i}) \\
\quad \texttt{IF } m \neq 0 \texttt{ THEN } |m| \\
\quad \texttt{ELSE } |\mathbf{s} \cdot (0.99\,c\,\mathbf{v_o} - \mathbf{v_i})| \\
\quad \texttt{ENDIF}
\end{array}
$$

The `ELSE` expression is included for the rare case where $m = 0$. It is easy to show that if $m = 0$, then $|\mathbf{s} \cdot (0.99\,c\,\mathbf{v_o} - \mathbf{v_i})| \neq 0$ assuming that $\mathbf{s} \cdot \mathbf{v_o} \neq 0$, which will always be the case here. The final form is

$$
\begin{array}{l}
\texttt{los\_gs\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}) : \texttt{Vect2} = \\
\quad j_0 = \eta_{gs}\,\dfrac{D - ||\mathbf{s}||}{D} \\
\quad \texttt{IF } \mathbf{s} \cdot \mathbf{v_o} = 0 \texttt{ THEN } (0,0) \\
\quad \texttt{ELSE los\_gs}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, j_0 * \texttt{maxDot}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})) \\
\quad \texttt{ENDIF}
\end{array}
$$

Note that the factor eta_{gs} is a constant between 0 and 1. It effectively decreases the maximum value of J. We will refer to this parameter as an aggressiveness parameter because it limits the severity of the manuevers.

4.1.3 Correctness

Lemma 4.1 (`los_gs_alg_crit`)**.** *If* $\mathbf{v'_o} = \texttt{los\_gs\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, then* $\texttt{criteria?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i})(\mathbf{v'_o})$.

Proof. We must show that `los_gs_alg` satisfies the horizontal criteria (Formula 1). The algorithm `los_gs_alg` calls `los_gs` with a value of $J = \eta_{gs} \frac{D - ||\mathbf{s}||}{D}$ which is positive in the loss of separation case. We then note that `los_gs` calls `los_gspd` with this same positive value of J. If `los_gspd` returns a non-zero vector $\mathbf{v'_o}$ then we know that we have $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J > 0$ (Formula 6) which satisfies the first condition of the criteria. The second condition of the criteria

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$$

is guaranteed by the presence of precisely this test in the `los_gs` function. Note that whenever $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$ is negative, this condition is true because $J > 0$. When this test fails `los_gs` sets $\mathbf{v'_o} = \mathbf{v_o}$, which trivially satisfies this condition. □

Theorem 4.2 (`los_gs_alg_independent`)**.** *If* $\mathbf{v'_o} = \texttt{los\_gs\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, then* $\texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i})$.

Proof. Lemma `los_gs_alg_crit` 4.1 assures us that the value $\mathbf{v'_o}$ returned by `los_gs_alg` satisfies the horizontal criteria. Then by lemma `criteria_independent` (3.2) we have the needed result. □

Theorem 4.3 (`los_gs_alg_coordinated`)**.** *If* $\mathbf{v'_o} = \texttt{los\_gs\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, and* $\mathbf{v'_i} = \texttt{los\_gs\_alg}(-\mathbf{s}, \mathbf{v_i}, \mathbf{v_o})$ *is non-zero, then* $\texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i})$.

Proof. Lemma `los_gs_alg_crit` 4.1 assures us that both $\mathbf{v'_o}$ and $\mathbf{v'_i}$ satisfy the horizontal criteria. Then the premises of lemma `criteria_coordinated` (3.4) are satisfied and we have the desired result. □

4.2 Track Only Solutions

4.2.1 Theory

We are concerned with the situation where a loss of separation has already occurred. So we have:

$$||\mathbf{s}|| < D.$$

We seek solutions where

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J \tag{8}$$

and

$$||\mathbf{v'_o}|| = ||\mathbf{v_o}||,$$

in 2 dimensions.

$$\begin{aligned}
&\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J, \\
&\mathbf{s} \cdot \mathbf{v'_o} = \mathbf{s} \cdot \mathbf{v_i} + J, \\
&s_x v'_{ox} + s_y v'_{oy} = \mathbf{s} \cdot \mathbf{v_i} + J, \\
&s_y v'_{oy} = \mathbf{s} \cdot \mathbf{v_i} + J - s_x v'_{ox}.
\end{aligned}$$

We will seek solutions to this equation by squaring both sides

$$(s_y v'_{oy})^2 = (\mathbf{s} \cdot \mathbf{v_i} + J - s_x v'_{ox})^2.$$

We will get two solutions from this quadratic equation from which we will only use the solution where $\texttt{sign}(s_y v'_{oy}) = \texttt{sign}(\mathbf{s} \cdot \mathbf{v_i} + J - s_x v'_{ox})$. For a track only solution we also need to constrain the solution by

$$||\mathbf{v'_o}|| = ||\mathbf{v_o}||$$

or

$$(v'_{oy})^2 = v_o^2 - (v'_{ox})^2. \tag{9}$$

Substituting we have

$$s_y^2(v_o^2 - (v'_{ox})^2) = (\mathbf{s} \cdot \mathbf{v_i} + J - s_x v'_{ox})^2.$$

Rearranging

$$s^2(v'_{ox})^2 - 2(\mathbf{s} \cdot \mathbf{v_i} + J)s_x(v'_{ox}) + (\mathbf{s} \cdot \mathbf{v_i} + J)^2 - s_y^2 v_o^2 = 0. \tag{10}$$

which is a quadratic equation in v'_{ox} with

$$\begin{aligned}
&a = s^2, \\
&b = -2s_x(\mathbf{s} \cdot \mathbf{v_i} + J), \\
&c = (\mathbf{s} \cdot \mathbf{v_i} + J)^2 - s_y^2 v_o^2.
\end{aligned} \tag{11}$$

The other component v'_{oy} can be obtained from Equation (9) as follows

$$\begin{aligned}
&\epsilon = \texttt{sign}(s_y)\,\texttt{sign}(-s_x\, v'_{ox} + (\mathbf{s} \cdot \mathbf{v_i}) + J), \\
&v'_{oy} = \epsilon\sqrt{v_o^2 - (v'_{ox})^2}.
\end{aligned} \tag{12}$$

4.2.2 Algorithm

The algorithm just solves the quadratic equation (10). If the discriminant of the equation is non-negative, then a solution is provided, otherwise a zero vector is returned:

$$
\begin{array}{l}
\texttt{los\_trk\_only}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, \rho, J) : \texttt{Vect2} = \\
\qquad a = s^2 \\
\qquad b = -2s_x\,(\mathbf{s} \cdot \mathbf{v_i} + J), \\
\qquad c = (\mathbf{s} \cdot \mathbf{v_i} + J)^2 - s_y^2(\mathbf{v_o} \cdot \mathbf{v_o}) \\
\qquad \texttt{IF discr}(a, b, c) \geq 0 \texttt{ THEN} \\
\qquad\qquad v'_{ox} = \texttt{root}(a, b, c, \rho), \\
\qquad\qquad \epsilon_y = \texttt{sign}(s_y)\,\texttt{sign}(-s_x\,v'_{ox} + (\mathbf{s} \cdot \mathbf{v_i}) + J) \\
\qquad\qquad \texttt{wv} = v_o^2 - (v'_{ox})^2 \\
\qquad\qquad \texttt{IF wv} > 0 \texttt{ THEN} \\
\qquad\qquad\qquad (v'_{ox}, \epsilon_y\sqrt{\texttt{wv}}) \\
\qquad\qquad \texttt{ELSE} \\
\qquad\qquad\qquad (0, 0) \\
\qquad\qquad \texttt{ENDIF} \\
\qquad \texttt{ELSE} \\
\qquad\qquad (0, 0) \\
\qquad \texttt{ENDIF}
\end{array}
$$

where $\texttt{root}(a, b, c, \rho)$ is defined as

$$\frac{-b + \rho\sqrt{b^2 - 4ac}}{2a}.$$

There are two solutions for $\rho = \pm 1$. The horizontal LoS criteria requires that

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}).$$

This is trivially true if the aircraft are convergent, but when the aircraft are already divergent, i.e., when $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) > 0$, some additional logic is needed:

$$
\begin{array}{l}
\texttt{los\_to}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, \rho, J) : \texttt{Vect2} = \\
\quad \mathbf{v'_o} = \texttt{los\_trk\_only}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, \rho, J) \\
\quad \texttt{IF } \mathbf{v'_o} = (0,0) \texttt{ THEN } (0,0) \\
\quad \texttt{ELSIF } \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) > 0 \texttt{ THEN} \\
\qquad \texttt{IF } \mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) > \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i}) \texttt{ THEN} \\
\qquad\quad \mathbf{v'_o} \\
\qquad \texttt{ELSE} \\
\qquad\quad \mathbf{v_o} \\
\qquad \texttt{ENDIF} \\
\quad \texttt{ELSE} \\
\qquad \mathbf{v'_o} \\
\quad \texttt{ENDIF}
\end{array}
$$

Coordinated divergence is guaranteed for all values of J. But how should we value for J that gives us good performance? The larger J, the more drastic the maneuver is. We would like to define a normalized version of this parameter to take on a value between 0 and 1. To do this we must calculate a maximum value of the dot product $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i})$ as $\mathbf{v'_o}$ is varied. The maximum value of the dot product occurs when the track angle is at the same angle as $\mathbf{s}$. This follows because

$$
\begin{array}{l}
\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = \\
\mathbf{s} \cdot \mathbf{v'_o} - \mathbf{s} \cdot \mathbf{v_i} = \\
||\mathbf{s}||\,||\mathbf{v'_o}||\cos\theta - \mathbf{s} \cdot \mathbf{v_i}
\end{array}
$$

where θ is the angle between the vectors. The cosine achieves a maximum when $\mathbf{v'_o}$ is parallel to $\mathbf{s}$.

We can then calculate a maximum value of the dot product as follows:

$$
\begin{array}{l}
\texttt{maxdot}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}) : \texttt{posreal} = \\
\quad \mathbf{w} = \dfrac{||\mathbf{v_o}||}{||\mathbf{s}||}\mathbf{s} \\
\quad \texttt{IF } \mathbf{s} \cdot (\mathbf{w} - \mathbf{v_i}) = 0 \texttt{ THEN } 1 \\
\quad \texttt{ELSE } |\mathbf{s} \cdot (\mathbf{w} - \mathbf{v_i})| \\
\quad \texttt{ENDIF}
\end{array}
$$

In the rare case where the maximum dot product is 0, i.e., when $\mathbf{s} \cdot (\mathbf{w} - \mathbf{v_i}) = 0$, the returned value of 1 will result in a quadratic equation with no solution, and a zero vector will be returned.

The `los_to` function returns two possible vectors, one for each value of ρ. The following function chooses the one that results in the smallest change from the

current velocity vector as follows:

$$\begin{aligned}
&\texttt{los_to_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}) : \texttt{Vect2} = \\
&\qquad j_0 = \texttt{maxdot}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})\, \eta_{to}\, \frac{D - ||\mathbf{s}||}{D} \\
&\qquad \mathbf{v_1} = \texttt{los_to}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, -1, j_0) \\
&\qquad \mathbf{v_2} = \texttt{los_to}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, +1, j_0) \\
&\qquad \texttt{IF } ||\mathbf{v_1} - \mathbf{v_o}|| \leq ||\mathbf{v_2} - \mathbf{v_o}|| \texttt{ THEN } \mathbf{v_1} \\
&\qquad \texttt{ELSE } \mathbf{v_2} \\
&\qquad \texttt{ENDIF}
\end{aligned}$$

The aggressiveness of the maneuver is determined by the parameter η_{to} and the distance between the aircraft: $\frac{D-||\mathbf{s}||}{D}$.

4.2.3 Correctness

Lemma 4.4 (`los_to_crit`). *If* $\mathbf{v'_o} = \texttt{los\_to}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, \rho, J)$ *is non-zero and* $J > 0$, *then* $\texttt{criteria?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i})(\mathbf{v'_o})$.

Proof. We must show that `los_to` satisfies the horizontal criteria (formula 1). The algorithm `los_to` calls `los_trk_only` with this same positive value of J. The function `los_trk_only` sets v'_{ox} to the root of the quadratic equation (formula 10) when the discriminant is positive. Otherwise it returns a zero vector. It sets $v_{oy} = \epsilon_y \sqrt{v_o^2 - (v'_{ox})^2}$. Together these insure that $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J > 0$ and $||\mathbf{v'_o}|| = ||\mathbf{v_o}||$. Thus, if `los_trk_only` returns a non-zero vector $\mathbf{v'_o}$ then we know that we have $\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) = J > 0$ (formula 8) which satisfies the first condition of the criteria. The second condition of the criteria

$$\mathbf{s} \cdot (\mathbf{v'_o} - \mathbf{v_i}) \geq \mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$$

is guaranteed by the presence of precisely this test in the `los_to` function. Note that whenever $\mathbf{s} \cdot (\mathbf{v_o} - \mathbf{v_i})$ is negative, this condition is true because $J > 0$. When this test fails `los_to` sets $\mathbf{v'_o} = \mathbf{v_o}$, which trivially satisfies this condition. □

Lemma 4.5 (`los_to_alg_crit`). *If* $\mathbf{v'_o} = \texttt{los\_to\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, then* $\texttt{criteria?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i})(\mathbf{v'_o})$.

Proof. The algorithm `los_to_alg` calls `los_to` twice for the two possible values of ρ. We end up with two vectors `v1` and `v2` both of which meet the horizontal criteria by lemma `los_to_crit` (4.4). The function `lost_to_alg` returns one of these values, so we have the desired result. □

Theorem 4.6 (`los_to_alg_independent`). *If* $\mathbf{v'_o} = \texttt{los\_to\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, then* $\texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i})$.

Proof. Lemma `los_to_alg_crit` (4.5) assures us that the value $\mathbf{v'_o}$ returned by `los_to_alg` satisfies the horizontal criteria. Then by lemma `criteria_independent` (3.2) we have the needed result. □

Theorem 4.7 (`los_to_alg_coordinated`). *If* $\mathbf{v'_o} = \texttt{los\_to\_alg}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})$ *is non-zero, and* $\mathbf{v'_i} = \texttt{los\_to\_alg}(-\mathbf{s}, \mathbf{v_i}, \mathbf{v_i})$ *is non-zero, then* $\texttt{divergent?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i})$.

Proof. Lemma `los_to_alg_crit` assures us that both $\mathbf{v'_o}$ and $\mathbf{v'_i}$ satisfy the horizontal criteria. Then the premises of lemma `criteria_coordinated` (3.4) are satisfied and we have the desired result. □

4.3 Timeliness of Recovery

In our first paper, the concept of horizontal correctness included a parameter that specified a maximum time to exit T_h:

$$\begin{aligned}&\texttt{xy\_correct?}[T_h](\mathbf{s}, \mathbf{v_i})(\mathbf{v_o}) = \\ &\quad \texttt{xy\_divergent?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i})\ \texttt{AND} \\ &\quad \texttt{horizontal\_separation?}(\mathbf{s} + T_h(\mathbf{v_o} - \mathbf{v_i})).\end{aligned}$$

The hope was that each aircraft could independently calculate new vectors $\mathbf{v'_o}$ and $\mathbf{v'_i}$ such that

$$\begin{aligned}T_h &\geq \texttt{tteh}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i}), \\ T_h &\geq \texttt{tteh}(-\mathbf{s}, \mathbf{v'_i} - \mathbf{v_o}),\end{aligned}$$

and that together these would be sufficient to establish

$$T_h \geq \texttt{tteh}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v'_i}),$$

which is the needed coordinated result. Unfortunately this was not the case.

We now propose an alternative approach that exploits the aggressiveness parameters η_{gs} and η_{to}. The idea is to achieve timeliness via iterative update. The first execution of the algorithm will result in a divergent solution but the divergence rate may be too slow. This can be determined by calculating the time to exit using the new vectors

$$\begin{aligned}\texttt{tteh}(\mathbf{s}, \mathbf{v'_o}, \mathbf{v'_i}) &= \texttt{Theta\_D}(\mathbf{s}, \mathbf{v'_o}, \mathbf{v'_i}) \\ &= \frac{-b + \sqrt{b^2 - 4ac}}{2a}.\end{aligned}$$

where a, b, c are coefficients of a quadratic equation:

$$\begin{aligned}\mathbf{v} &= \mathbf{v'_o} - \mathbf{v'_i}, \\ a &= (\mathbf{v} \cdot \mathbf{v}), \\ b &= 2(\mathbf{s} \cdot \mathbf{v}), \\ c &= (\mathbf{s} \cdot \mathbf{s}) - D^2,\end{aligned}$$

If the time to exit is less than the desired time, i.e., T_h, the values of η_{gs} and η_{to} can be increased by 5%. Of course, the iterative update should only occur after the aircraft has achieved the previously commanded velocity vectors. This iterative increase of η_{gs} and η_{to} can continue until the desired value is reached or the maximum values of these parameters are reached.

4.4 Numerical Instability

The calculation of the discriminant for the quadratic equation (11) for the track only algorithm was found to be numerically unstable in our Java implementations. The straight forward calculation

$$b^2 - 4ac,$$

where

$$\begin{aligned} a &= s^2, \\ b &= -2s_x(\mathbf{s} \cdot M), \\ c &= M^2 - s_y^2 v_o^2, \\ M &= \mathbf{s} \cdot \mathbf{v_i} + J \end{aligned}$$

results in the following subtraction

$$4M^2 s_x^2 - 4M^2 s^2.$$

Since $M >> 1$ this can lead to a massive loss of precision when s_x^2 is nearly equal to s^2. This occurs when s_y is zero or near to zero.

The instability manifested itself in practice in a scenario where the theoretical value of the discriminant was zero, i.e., $s_y = 0$. As the intruder's initial velocity vector ($\mathbf{v_i}$) was varied, the value of M changed. The `los_to_alg` failed to produce a solution in some cases because the calculated value of the discriminant was a small negative number rather than 0. As the heading of the intruder was changed, the `los_to_alg` would alternate between producing a solution and not.

The massive cancellation can be reduced by changing the order of calculation as follows

$$4M^2(s_x^2 - s^2).$$

Another solution is possible. In Section 4.2.1, the solution vector was obtained by first solving for v'_{ox} and then v'_{oy} was obtained from the constraint $||\mathbf{v'_o}|| = ||\mathbf{v_o}||$. The opposite approach can also be used: first solve for v'_{oy} via the quadratic equation $a(v'_{oy})^2 + b(v'_{oy}) + c = 0$ where

$$\begin{aligned} a &= s^2, \\ b &= -2s_y(\mathbf{s} \cdot \mathbf{v_i} + J), \\ c &= (\mathbf{s} \cdot \mathbf{v_i} + J)^2 - s_x^2 v_o^2, \end{aligned} \tag{13}$$

then obtain v'_{ox} using the norm constraint as follows

$$\begin{aligned} \epsilon_x &= \texttt{sign}(s_x)\,\texttt{sign}(-s_y\, v'_{oy} + (\mathbf{s} \cdot \mathbf{v_i}) + J), \\ v'_{ox} &= \epsilon_x \sqrt{v_o^2 - (v'_{oy})^2}. \end{aligned} \tag{14}$$

So a practical approach is use the v_{ox} quadratic (equation 10) when $|s_x| < |s_y|$ and use the v_{oy} quadratic (equation 13) otherwise.

5 Vertical Maneuvers for Loss of Separation Recovery

We have not altered the vertical correctness properties or criteria from the original paper. We reproduce these here for the convenience of the reader

5.1 Correctness Definition and Vertical Criteria

$$\begin{aligned}&\texttt{z\_correct?}[T_v](\mathbf{s}, \mathbf{v_i})(\mathbf{v_o}) = \\ &\quad \texttt{z\_divergent?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i}) \ \texttt{AND} \\ &\quad \texttt{vertical\_separation?}(\mathbf{s} + T_v(\mathbf{v_o} - \mathbf{v_i}),\end{aligned}$$

where

$$\begin{aligned}&\texttt{z\_divergent?}(\mathbf{s}, \mathbf{v}) = \\ &\forall t : t > 0 \implies |s_z| < |s_z + tv_z|,\end{aligned}$$

and

$$\texttt{vertical\_separation?}(\mathbf{s}) = |s_z| \geq H.$$

The parameter T_v specifies a maximum time to recover in the vertical dimension. The vertical criteria is

$$\begin{aligned}&\texttt{z\_criteria?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i})(\mathbf{v'_o}) = \\ &\quad (v'_{oz} - v_{iz}) \neq 0 \ \texttt{AND} \\ &\quad \texttt{z\_prop?}(\mathbf{s}, \mathbf{v'_o} - \mathbf{v_i}) \ \texttt{AND} \\ &\quad (\texttt{z\_prop?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i}) \implies \\ &\qquad ((v'_{oz} - v_{iz}) \neq 0 \ \texttt{AND} \ \texttt{sign}(v'_{oz} - v_{iz})\,(v'_{oz} - v_{iz}) \geq 0) \ \texttt{OR} \\ &\qquad ((v'_{oz} - v_{iz}) = 0 \ \texttt{AND} \ \texttt{break\_vz\_symm}(\mathbf{s})\,(v'_{oz} - v_{iz}) > 0),\end{aligned}$$

where `z_prop?` is defined as

$$\texttt{z\_prop?}(\mathbf{s}, \mathbf{v}) = s_z v_z \geq 0,$$

and `sign` is the two-valued sign function:

$$\texttt{sign}(x) = \texttt{IF} \ x \geq 0 \ \texttt{THEN} \ 1 \ \texttt{ELSE} \ -1 \ \texttt{ENDIF}$$

The `break_vz_symm` function is used in the rare situation where $(v'_{oz} - v_{iz}) = 0$ to overcome the symmetry. It can be any function which satisfies the following two properties:

$$\begin{aligned}&\mathbf{s} \neq 0 \implies \texttt{break\_vz\_symm}(-\mathbf{s}) = -\texttt{break\_vz\_symm}(\mathbf{s}), \\ &s_z \neq 0 \implies \texttt{break\_vz\_symm}(\mathbf{s}) = \texttt{sign}(s_z).\end{aligned}$$

5.2 Vertical Algorithm

The vertical LoS algorithm is

$$
\begin{array}{l}
\texttt{z\_recovery}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, t) = \\
\quad \texttt{nvz} = \dfrac{\texttt{sign\_vz}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i})H - s_z}{t} \\
\quad \texttt{IF z\_prop?}(\mathbf{s}, \mathbf{v_o} - \mathbf{v_i}) \texttt{ AND } |v_z| \geq |\texttt{nvz}| \texttt{ THEN} \\
\quad\quad (v_{ox}, v_{oy}, v_{oz}) \\
\quad \texttt{ELSE} \\
\quad\quad (v_{ox}, v_{oy}, \texttt{nvz} + v_{iz}) \\
\quad \texttt{ENDIF}
\end{array}
$$

where `sign_vz` is

$$
\begin{array}{l}
\texttt{sign\_vz}(\mathbf{s}, \mathbf{v}) = \\
\quad \texttt{IF z\_prop?}(\mathbf{s}, \mathbf{v}) \texttt{ AND } v_z \neq 0 \texttt{ THEN} \\
\quad\quad \texttt{sign}(v_z) \\
\quad \texttt{ELSE} \\
\quad\quad \texttt{break\_vz\_symm}(\mathbf{s}) \\
\quad \texttt{ENDIF}
\end{array}
$$

The `break_vz_symm` function is defined as follows:

$$
\begin{array}{l}
\texttt{break\_vz\_symm}(\mathbf{s}) = \\
\quad \texttt{IF } s_z > 0 \texttt{ OR } (s_z = 0 \texttt{ AND } s_x < 0) \texttt{ OR } (s_z = 0 \texttt{ AND } s_x = 0 \texttt{ AND } s_y < 0) \\
\quad \texttt{THEN} \\
\quad\quad 1 \\
\quad \texttt{ELSE} \\
\quad\quad -1 \\
\quad \texttt{ENDIF}
\end{array}
$$

5.3 Correctness Theorems

The vertical correctness theorems are

$$
\begin{array}{l}
\texttt{z\_criteria\_tr?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, T_v)(\mathbf{v_o'}) \\
\quad \Longrightarrow \\
\texttt{z\_correct?}[T_v](\mathbf{s}, \mathbf{v_i})(\mathbf{v_o'})
\end{array}
$$

and

$$
\begin{array}{l}
\texttt{z\_criteria\_tr?}(\mathbf{s}, \mathbf{v_o}, \mathbf{v_i}, T_v)(\mathbf{v_o'}) \texttt{ AND} \\
\texttt{z\_criteria\_tr?}(-\mathbf{s}, \mathbf{v_i}, \mathbf{v_o}, T_v)(\mathbf{v_i'}) \\
\quad \Longrightarrow \\
\texttt{z\_correct?}[T_v](\mathbf{s}, \mathbf{v_i'})(\mathbf{v_o'}).
\end{array}
$$

The reader is referred to [1] for the proofs of correctness.

6 Future Work

6.1 Coordination in the Presence of Errors

In the analysis developed in this paper we have implicitly assumed that each aircraft has perfect knowledge of its own and traffic aircraft locations and velocities. We believe that this is an appropriate first step because certainly if one does not understand a system under ideal conditions, its behavior under realistic conditions will be unfathomable. There are two aspects of data inaccuracies that we must be concerned with. First, errors can accumulate over time and small inaccuracies can grow into large ones. Second, critical decisions are often made on the basis of specific values of input data. For example, the system is designed to change mode if a specified threshold is exceeded. In the presence of data errors, it is possible for the *measured* system state to oscillate around this threshold while the true value remains below the threshold. If the decision is a coordinated decision, and the system is at the boundary of the decision point, the presence of data errors can destroy the coordination.

The first aspect can be handled with straight-forward calculations which naturally should be checked using a theorem prover. These calculations provide a formal basis for slightly enlarged protection zones, e.g., 5.1 miles rather than 5 miles, which can largely eliminate this problem. Furthermore, if the algorithms are run iteratively with a short period, e.g., 1 second, then the error accumulation will be negligible. The error accumulation problem can be more significant in a centralized approach to recovery where solutions are computed on the ground and delivered to the aircraft.

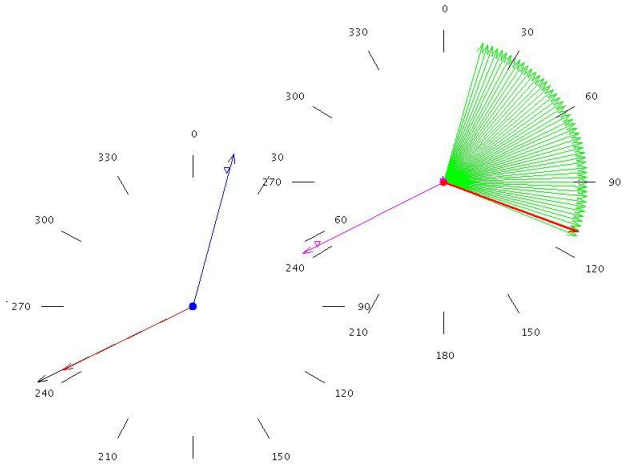
The second aspect is the more serious problem in the distributed execution environment. In fact there is no complete theoretical solution to this problem. The use of filters and dead bands can greatly reduce the impact of this problem, but not eliminate it entirely. However, there exist solutions where the algorithm can alert the pilot (or higher layers of the system) when the filtering strategy has failed. In this case, preplanned emergency maneuvers can be deployed. The centralized implementation is not subject to this problem because it computes the coordinated maneuvers for all of the aircraft. It is more vulnerable to the first aspect, because the computation of conflict-free trajectories for the N aircraft, i.e., NxN potential conflicts, is inherently slower. Iteration rates of 30 seconds or more is not unlikely. We will defer further consideration of these issues to future work.

6.2 Iterative Stability

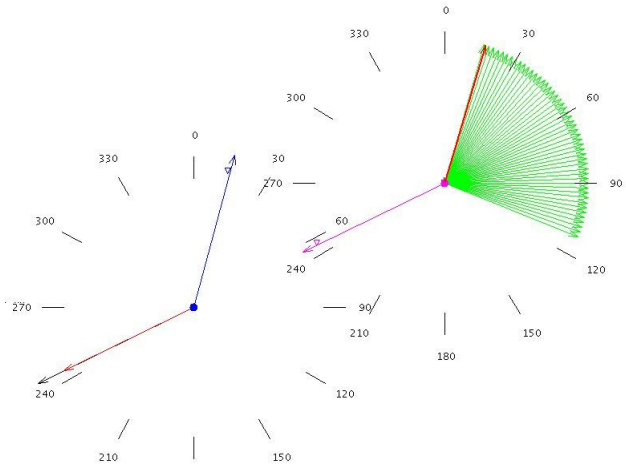
In this paper we have not analyzed the iterative stability of the algorithms. Even with no inaccuracies in the data, it is theoretically possible for poor algorithms to exhibit unacceptable discontinuous behavior as the algorithm is iteratively executed. In other words, it is possible that relatively small changes in the input values could result in resolutions that are far apart. If the algorithms are deployed in a one-shot

manner, this is not an issue. In this case, each aircraft computes its resolution only once. It make take several seconds for the aircraft to achieve the computed resolutions, but since the resolutions are not recomputed in the intermediate states, there is no real problem here. But if the algorithm is executed iteratively, it is important that there are not large changes in the resolutions.

The algorithms presented in this paper have not yet been formally verified to be free of such problems. However, we have not witnessed any serious issues in our simulations except for one special case, the direct head-on case: The magenta aircraft with heading 243 has a track only resolution of 110 degrees



while a small change of heading to 244 results in a track only resolution of 17 degrees.



Here we must use a dead band of a few degrees to prevent oscillations from occurring. It is also essential that data errors be properly handled for special cases such as this. See discussion in section 6.1.

6.3 Completeness

It is possible to satisfy the correctness properties by always returning a zero vector, since we use a zero vector to indicate the absence of a solution. The correctness properties only address non-zero values (See sections 4.1.3, 4.2.3). Our algorithms clearly do not just return a zero vector, but whether the algorithm misses some important cases is an important question. To answer the question the analyst must explore the conditions under which a zero vector is returned. For example, the `los_gs_alg` returns a zero vector when $\mathbf{s} \cdot \mathbf{v_o} = 0$. See section 4.1.2. It also returns a zero vector when $K = \frac{\mathbf{s} \cdot \mathbf{v_i} + J}{\mathbf{s} \cdot \mathbf{v_o}} < 0$. How often do these cases arise? These questions can be examined experimentally or formally in the context of *completeness* theorems. This type of formal analysis will be deferred to future work.

6.4 Investigation of Appropriate Times To Exit

In this paper we introduced two parameters that specify maximum times to exit the protection zone horizontally or vertically:

- T_h specifies a maximum time to recover horizontally.
- T_v specifies a maximum time to recover vertically.

We did not provide any guidelines about appropriate values for these parameters. The divergence aspect of the correctness properties insures that the immediate danger will be over once the recovery algorithm has been executed, but divergence can be slow when the recovery trajectories are nearly parallel. Suitable values for these parameters must be determined within the context of a more fully defined operational concept. Human in the loop experiments could be performed to determine exit times that pilots would be comfortable with. In section 4.3, we argued that the recovery algorithms could be executed iteratively while making small changes to the J parameter to achieve the desired time to exit. Future work will investigate the behavior of these algorithms as they are iterated to insure that very small changes in J result in small changes in the recovery trajectories.

7 Conclusion

In this paper we have developed loss of separation algorithms for both the horizontal and vertical dimensions. The algorithms provide solutions for the track-only, ground speed only, and vertical-speed only cases. A theoretical framework for analyzing these algorithms was developed and used to establish correctness properties about the proposed algorithms. The correctness properties require divergence and a timely exit from the protection zone. Central to the framework is the idea of an intermediate criteria which decomposes the verification process into two steps. The first step establishes that the criteria is sufficient to meet the correctness properties. This verification step has been completed in this paper. The second step shows that a particular algorithm meets the criteria. This must be accomplished for each new

algorithm that is developed. We have completed these proofs for our algorithms as well.

Our correctness properties include requirements for both independent and coordinated correctness. Independent correctness requires that an algorithm recovers from loss of separation if only one of the aircraft maneuvers. The coordinated correctness property requires that an algorithm recovers from loss of separation when both aircraft maneuver. This requires a proof that all possible combinations of maneuvers result in divergence and a timely exit from the protection zone.

The formal proofs were conducted using the PVS theorem prover. Several idealistic assumptions were made in these proofs: (1) input data contains no errors, (2) the computations were performed with infinite precision, i.e., mathematical real numbers, (3) the resolution maneuvers can be performed instantaneously, and (4) pilots implement the prescribed maneuvers. Each of these assumptions can be relaxed by performing additional analysis, which we hope to do in the future.

References

1. Ricky W. Butler and Cesar A. Muñoz. A formal framework for the analysis of algorithms that recover from loss of separation. Technical Report NASA/TM-2008-215356, NASA Langley Research Center, NASA LaRC,Hampton VA 23681-2199, USA, Oct 2008.

2. G. Dowek, A. Geser, and C. Muñoz. Tactical conflict detection and resolution in a 3-D airspace. In *Proceedings of the 4th USA/Europe Air Traffic Management R&DSeminar, ATM 2001*, Santa Fe, New Mexico, 2001. A long version appears as report NASA/CR-2001-210853 ICASE Report No. 2001-7.

3. G. Dowek, C. Muñoz, and V. Carreño. Provably safe coordinated strategy for distributed conflict resolution. In *Proceedings of the AIAA Guidance Navigation, and Control Conference and Exhibit 2005, AIAA-2005-6047*, San Francisco, California, 2005.

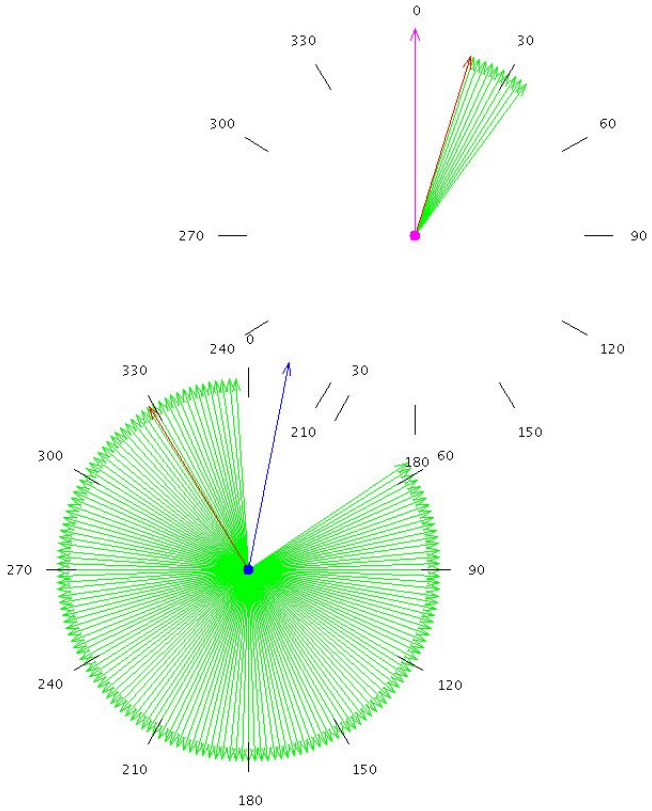
Appendix A

Horizontal Criteria Visualization

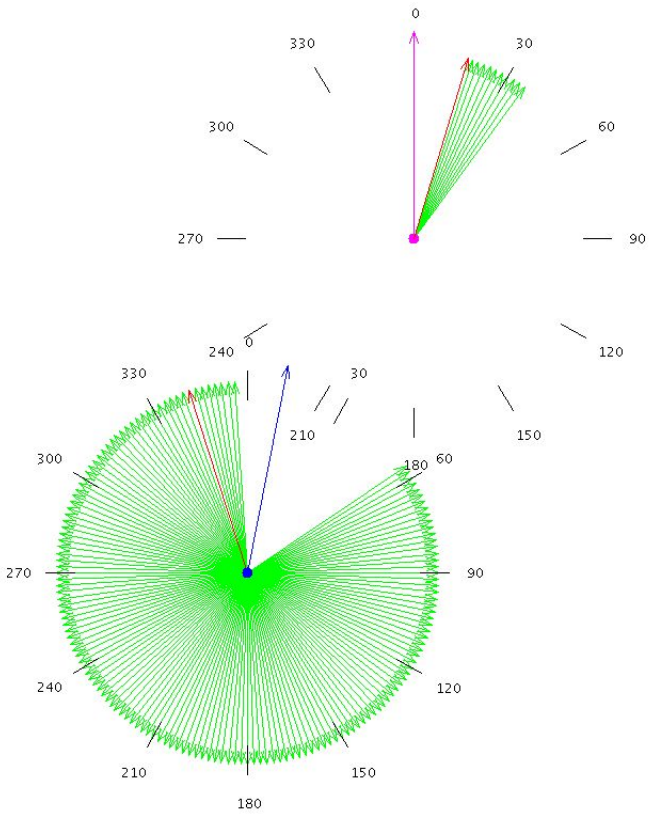
The original ownship vector is displayed in blue and the original traffic vector is displayed in magenta.

$$\mathbf{s}_o = (0\ \texttt{nm}, 0\ \texttt{nm}, 25000\ \texttt{ft})$$
$$\mathbf{s}_i = (1\ \texttt{nm}, 2\ \texttt{nm}, 25000\ \texttt{ft})$$
$$\mathbf{v}_o = (60\ \texttt{kts}, 300\ \texttt{kts}, 0)$$
$$\mathbf{v}_i = (0\ \texttt{kts}, 300\ \texttt{kts}, 0)$$

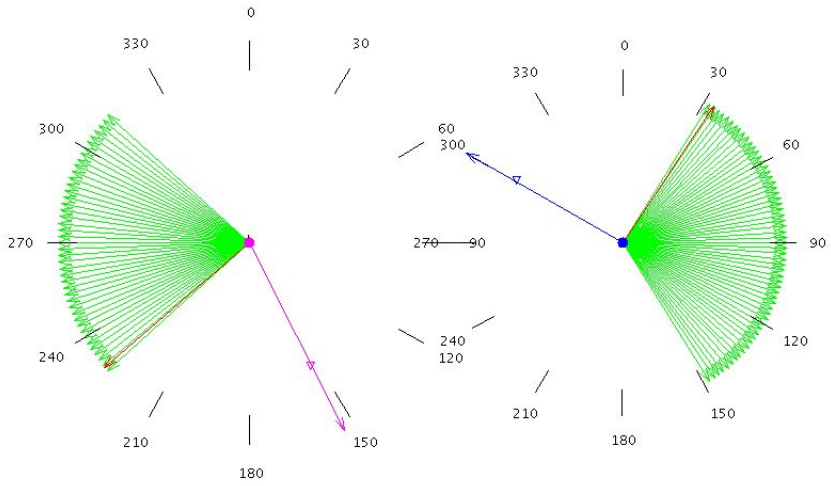
In this scenario, the track-only velocity vectors allowed by the criteria are shown in green. The red vectors are the `los_to_alg` solutions with an aggressiveness factor $\eta_{to} = 1/3$.



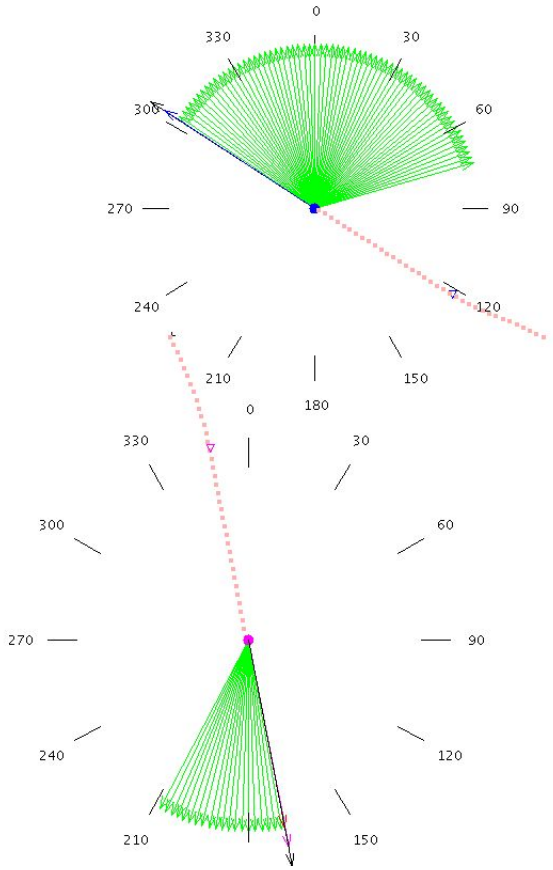
If $\eta_{to} = 1/6$, we obtain:



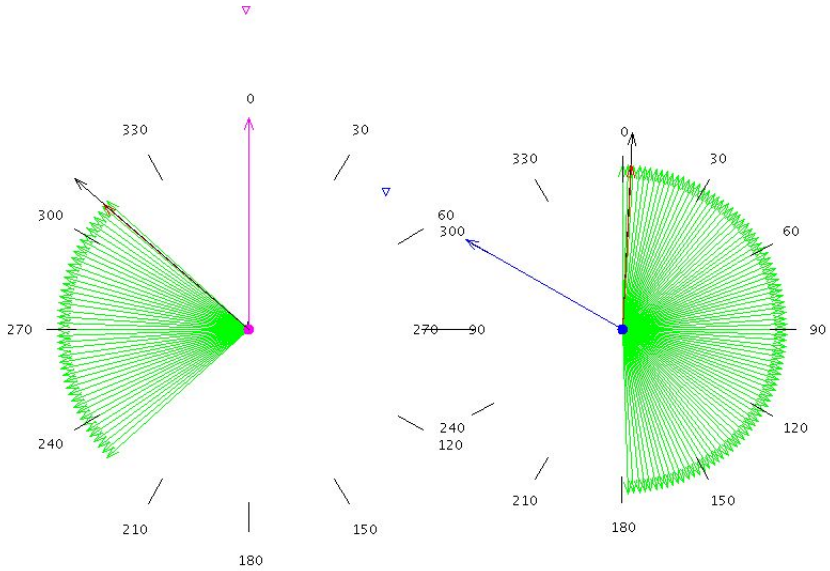
In the following illustration, the ownship track = 300, ground speed = 300 kts, and the traffic track = 150 and ground speed = 350 kts. The separation between the aircraft is 4.21 nm and the vertical speed is 0 for both.



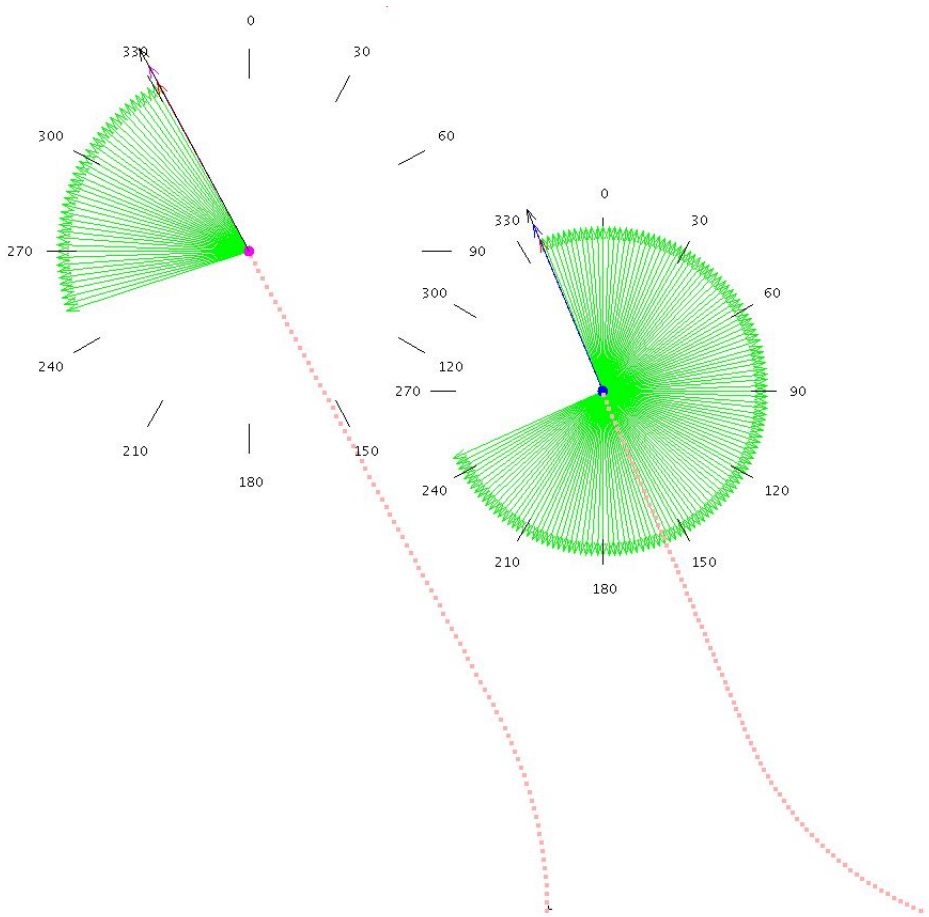
The aggressiveness factor $\eta_{to} = 1/3$. This scenario requires more aggressive maneuvers. The trace that arises from stepping the algorithm iteratively once per second is illustrated below:



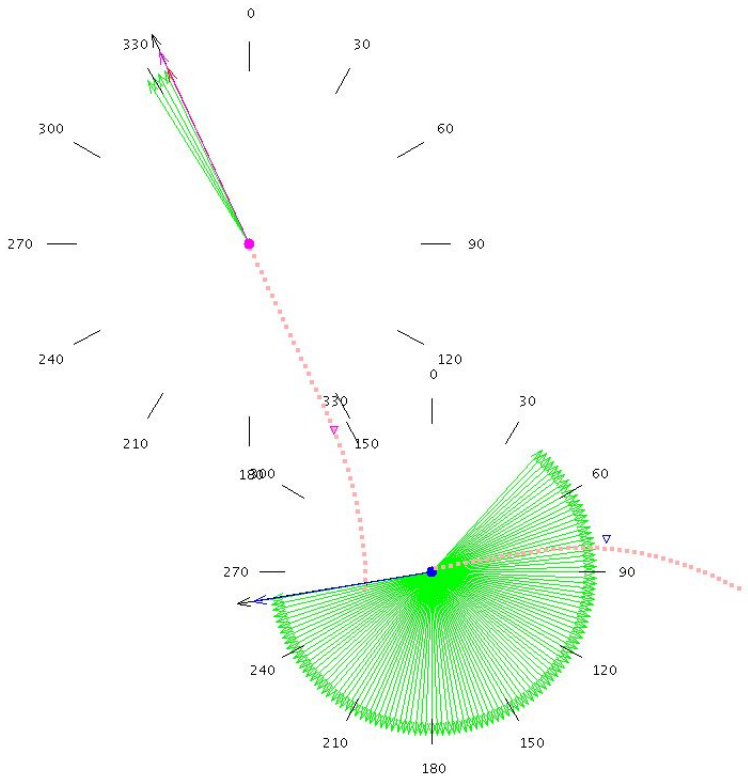
The maneuver executed was limited by a maximum turn rate corresponding to a bank angle of 20^o. The algorithm is re-executed every iteration. Changing the traffic track angle to 360^o, results in



The trace resulting from a 1 second step interval is



The nearly parallel lines of recovery results in a 95+ seconds time to exit. This indicates that an iterative increase in the J value may be needed in a situation such as this. Increasing the aggressiveness factor to 0.5, decreased the time to exit to about 60 seconds. Interestingly, changing the aggressiveness factor to 0.7 resulted in a major change in the ownship trajectory:



and a short 20 second recovery time. The behavior is very different if the algorithm is not recomputed at each iteration step.

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 - 2009	Technical Memorandum	

4. TITLE AND SUBTITLE
Formally Verified Practical Algorithms For Recovery From Loss of Separation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Butler, Ricky W.; and Muñoz, César A.

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-19586

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-2009-215726

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 61
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In this paper, we develop and formally verify practical algorithms for recovery from loss of separation. The formal verification is performed in the context of a criteria-based framework. This framework provides rigorous definitions of horizontal and vertical maneuver correctness that guarantee divergence and achieve horizontal and vertical separation. The algorithms are shown to be independently correct, that is, separation is achieved when only one aircraft maneuvers, and implicitly coordinated, that is, separation is also achieved when both aircraft maneuver. In this paper we improve the horizontal criteria over our previous work. An important benefit of the criteria approach is that different aircraft can execute different algorithms and implicit coordination will still be achieved, as long as they all meet the explicit criteria of the framework. Towards this end we have sought to make the criteria as general as possible. The framework presented in this paper has been formalized and mechanically verified in the Prototype Verification System (PVS).

15. SUBJECT TERMS
Formal methods; Conflict detection and resolution; Separation assurance; Loss of separation; Verification; Software safety

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	36	(443) 757-5802