Formal Verification of Distributed Aircraft Controllers

Sarah M. Loos, David Renshaw, and André Platzer

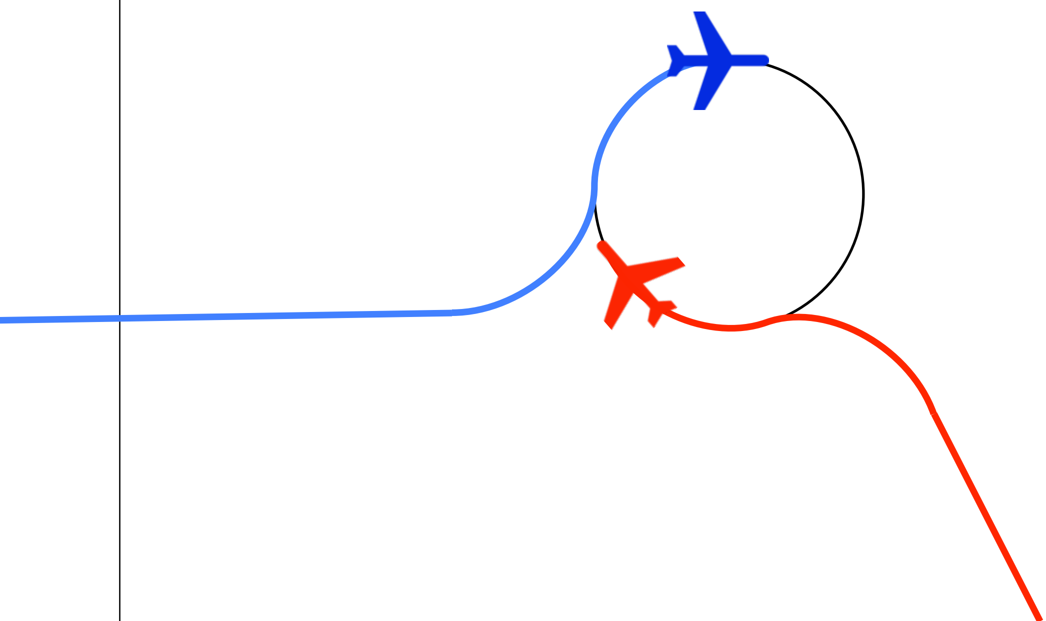
Computer Science Department

Carnegie Mellon University

April 10, 2013

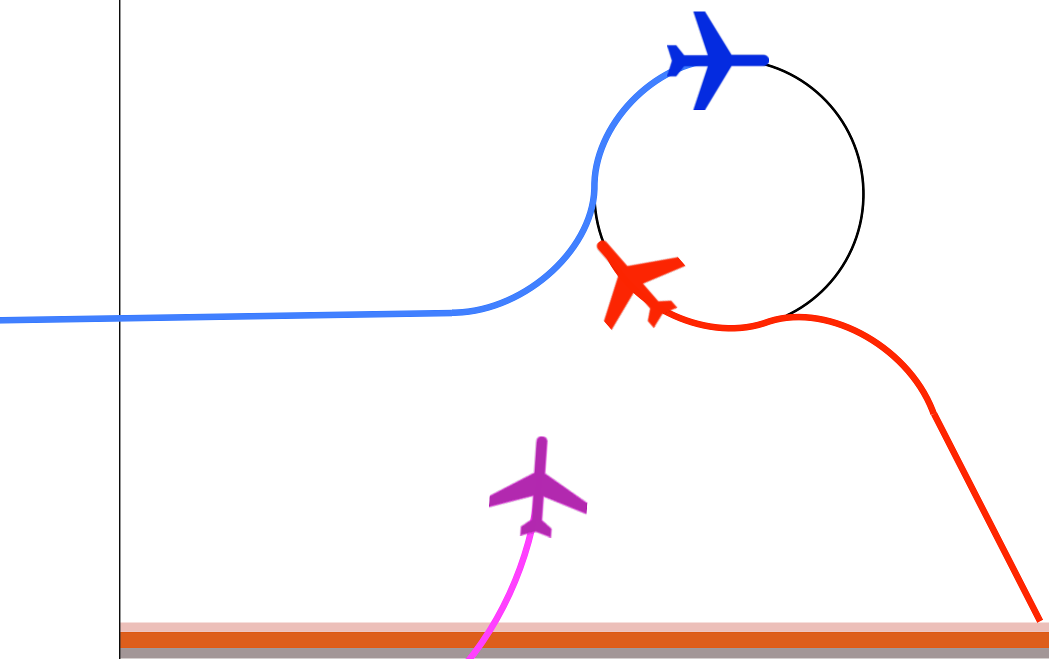
How Can We Prove Distributed Airspace?

How Can We Prove Distributed Airspace?



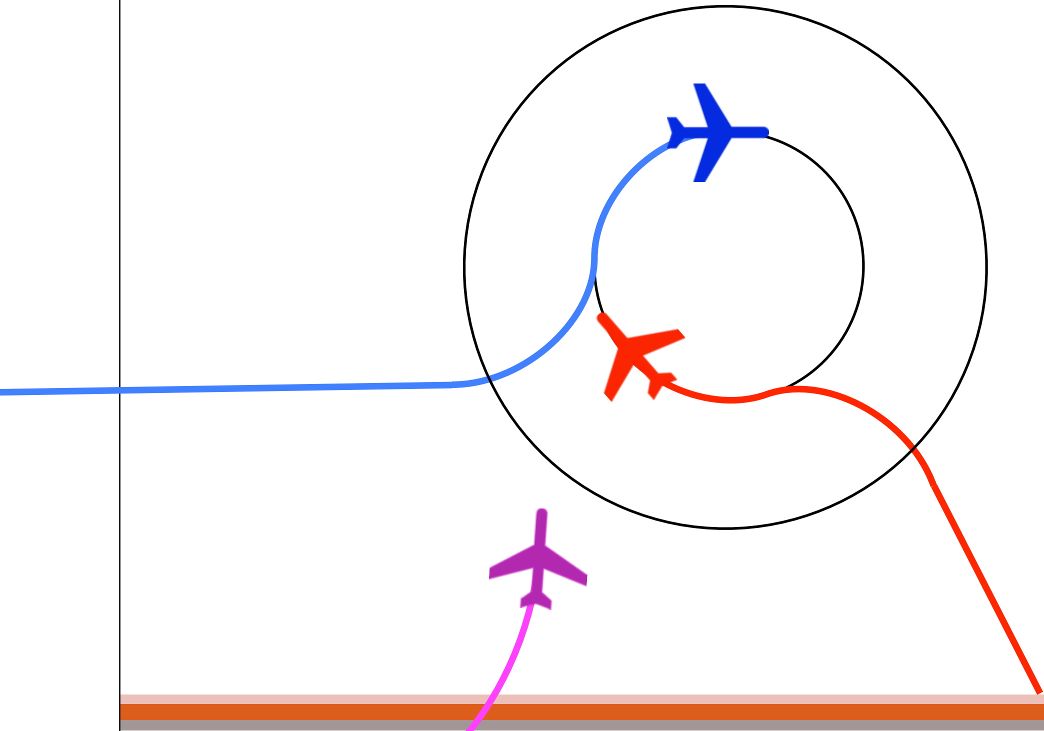
Sensor limits on aircraft are local.

How Can We Prove Distributed Airspace?



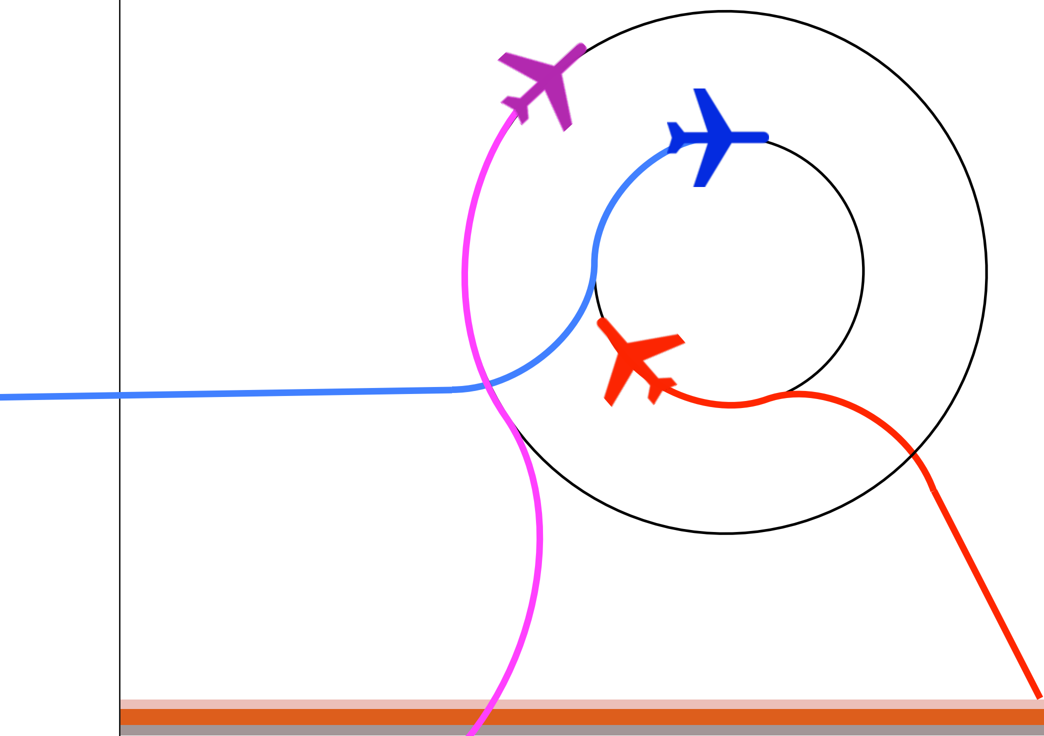
Sensor limits on aircraft are local.

How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

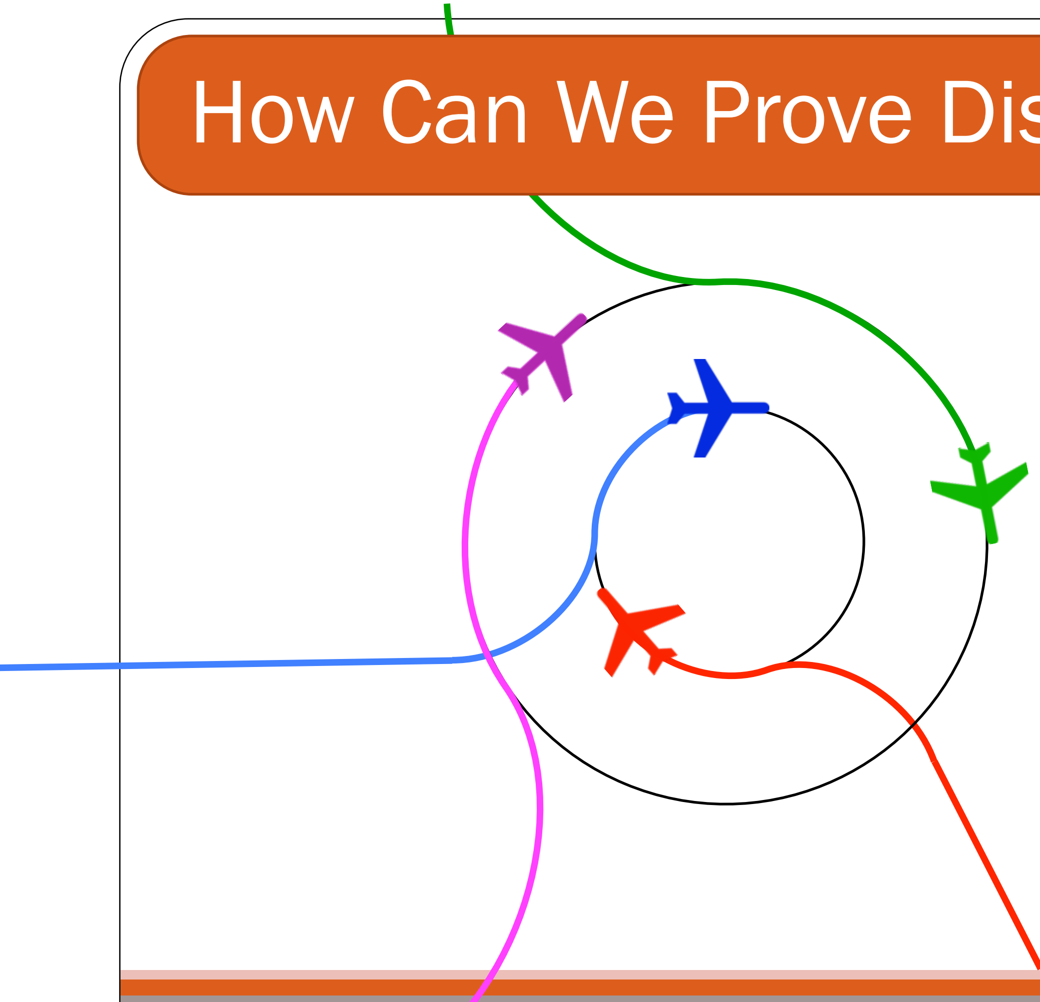
How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

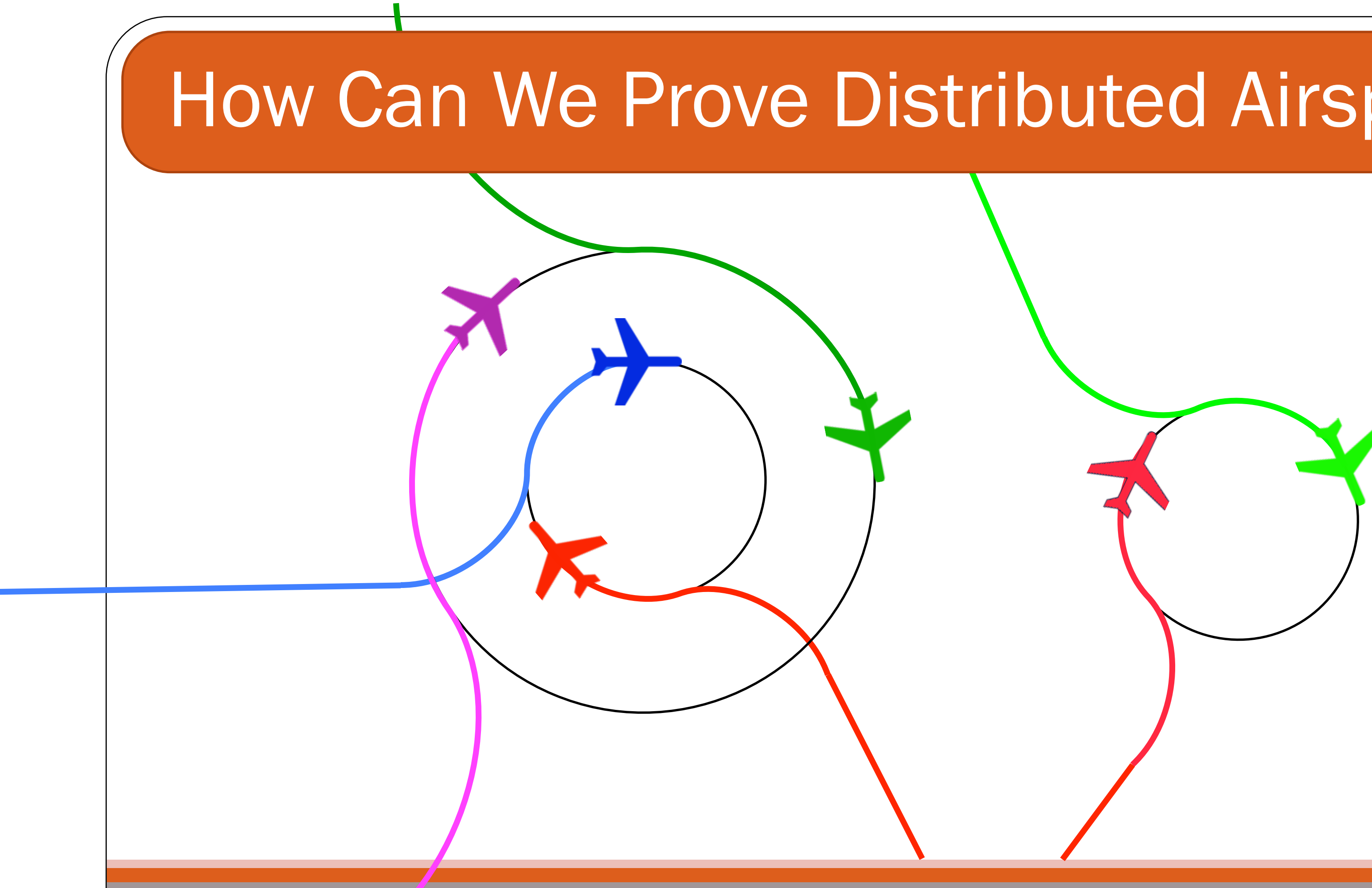
How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

How Can We Prove Distributed Airspace?

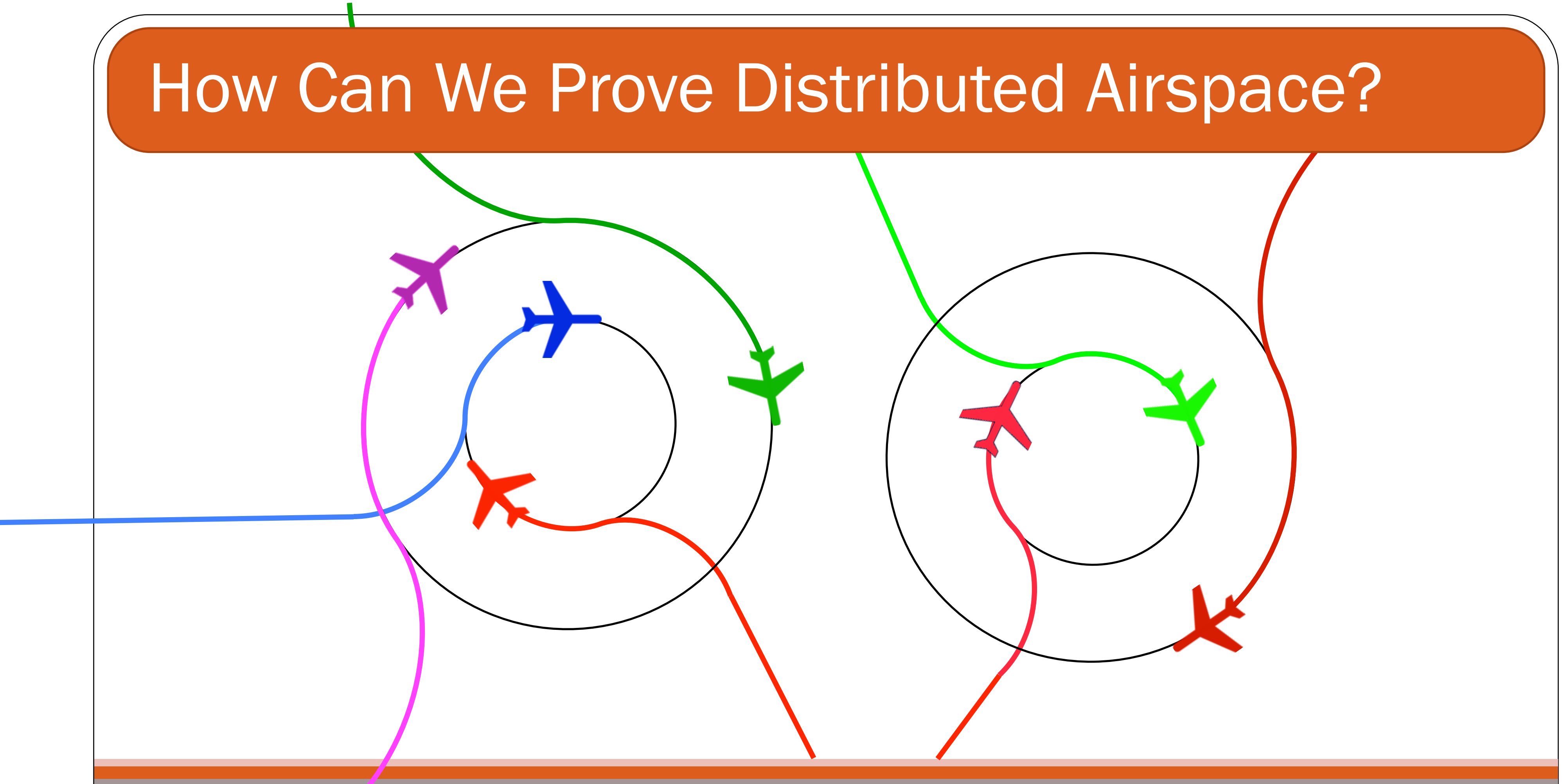


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

But is a terrible idea when implemented globally.

How Can We Prove Distributed Airspace?

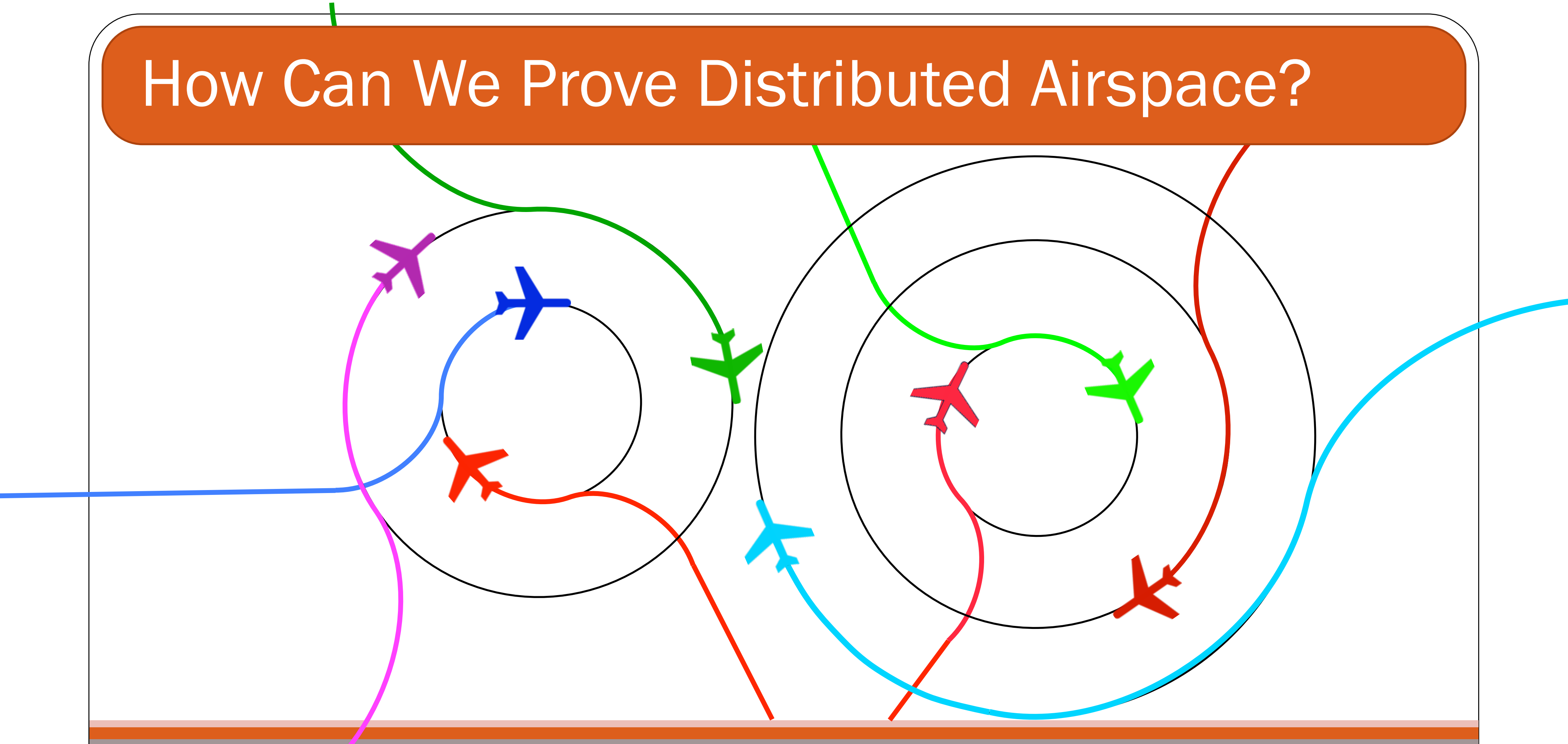


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

But is a terrible idea when implemented globally.

How Can We Prove Distributed Airspace?

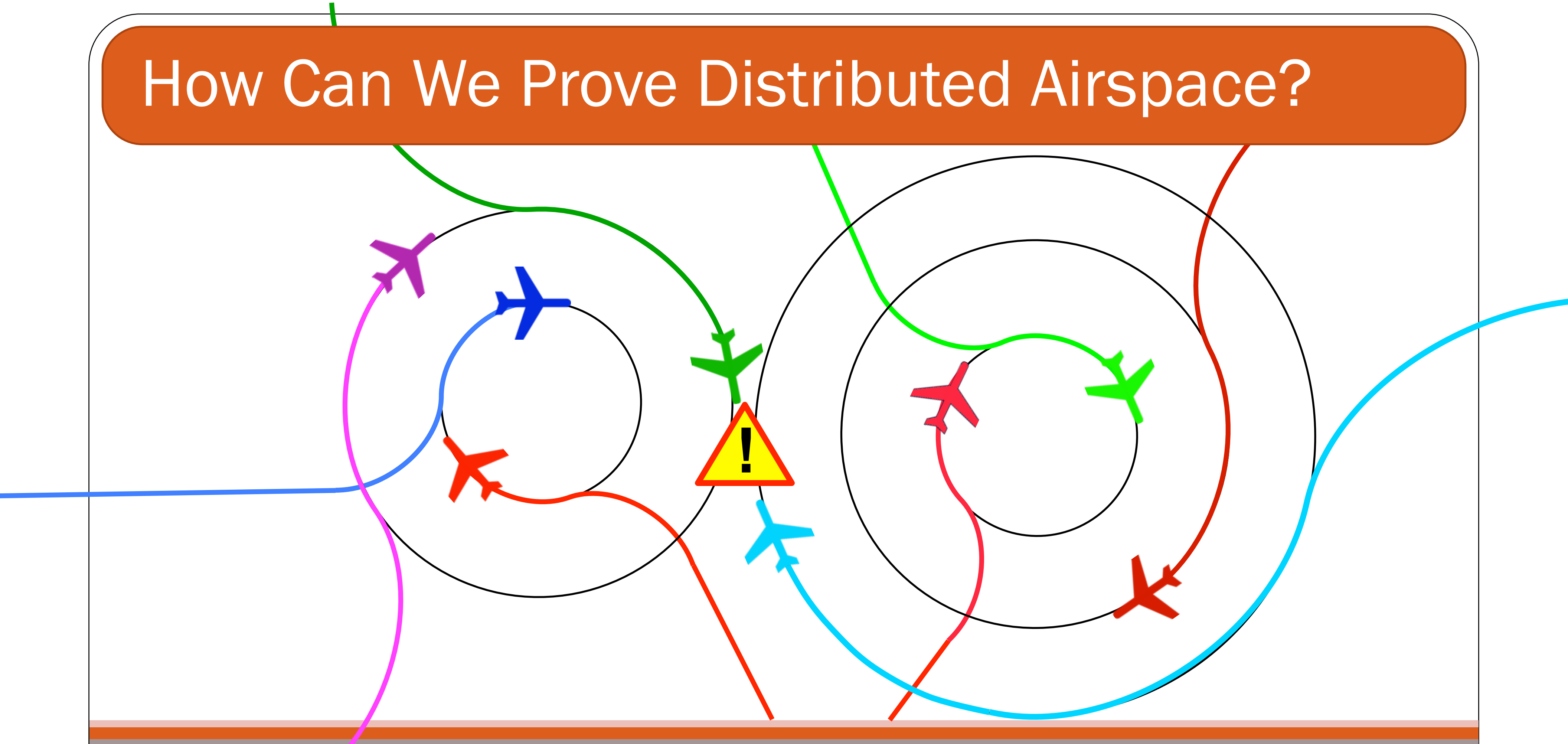


Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

But is a terrible idea when implemented globally.

How Can We Prove Distributed Airspace?



Sensor limits on aircraft are local.

Sometimes a maneuver may look safe locally...

But is a terrible idea when implemented globally.

Assumptions and Requirements

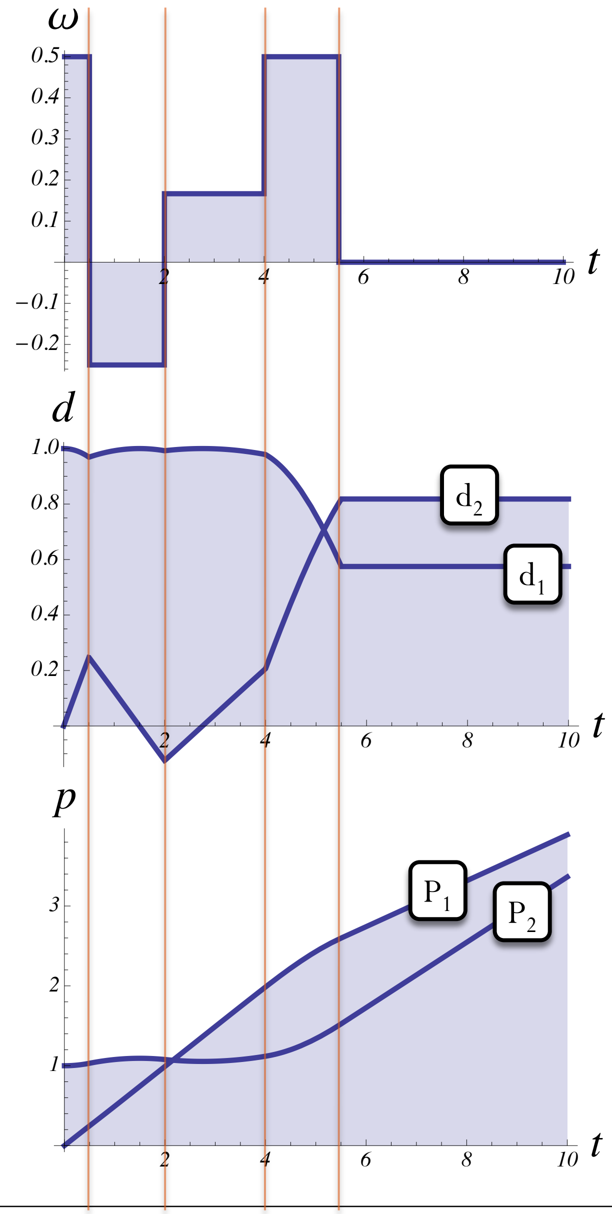
Requirements

- **Safety**: At all times, the aircraft must be separated by distance greater than p.
- Aircraft trajectories must always be **flyable**.
- An **arbitrary number** of aircraft may enter the maneuver at any time.

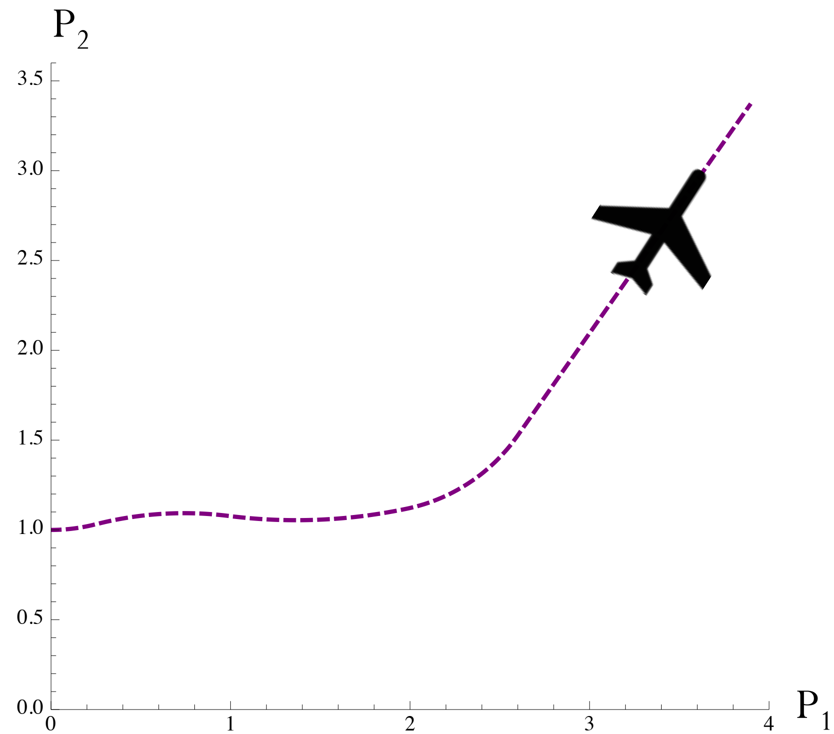
Assumptions

- Aircraft maintain constant velocity.
- Sensors are accurate and have no delay.
- Collision avoidance maneuvers are executed on the 2D plane.

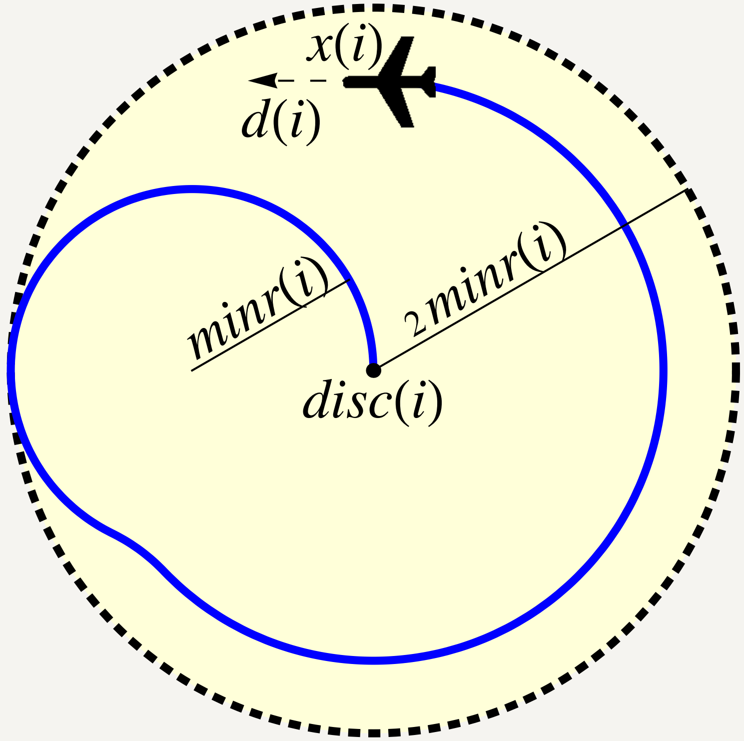
Hybrid Dynamics



Aircraft are controlled by steering, through discrete changes in angular velocity ω.



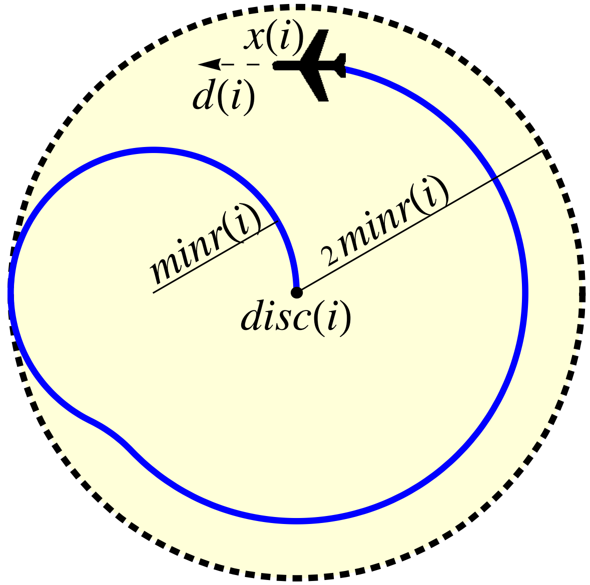
Big Disc Control



- Leaves maneuverability to pilot discretion.
- Requires large buffer disc.
- Requires aircraft to return to the center of the disc before completing avoidance maneuver.

Big Disc Control

$$\texttt{BigDisc} \equiv (\texttt{Control} \cup \texttt{Plant})^*$$
$$\texttt{Control} \equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA})$$
$$\texttt{CA} \equiv ?(ca(k) = 1);\ (\texttt{Steer} \cup \texttt{Exit})$$
$$\texttt{NotCA} \equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter})$$
$$\texttt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k))$$
$$\texttt{Exit} \equiv ?(disc(k) = x(k));\ ca(k) := 0$$
$$\texttt{Enter} \equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1$$
$$\texttt{Flip} \equiv side(k) := -side(k)$$



$$\texttt{Plant} \equiv \forall i : \mathbb{A}\ \Big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},$$
$$disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \texttt{EvDom}\Big)$$

$$\texttt{EvDom} \equiv \forall j : \mathbb{A}$$
$$((j \ne i \wedge (ca(i) = 0 \vee ca(j) = 0)) \to \mathsf{Sep}(i, j)$$
$$\wedge \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\|$$
$$\le minr(i))$$
$$\mathsf{Sep}(i, j) \equiv \|disc(i) - disc(j)\| \ge 2minr(i) + 2minr(j) + p$$

Big Disc Control

$$\texttt{BigDisc} \equiv (\texttt{Control} \cup \texttt{Plant})^*$$

$$\texttt{Control} \equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA})$$

$$\texttt{CA} \equiv ?(ca(k) = 1);\ (\texttt{Steer} \cup \texttt{Exit})$$

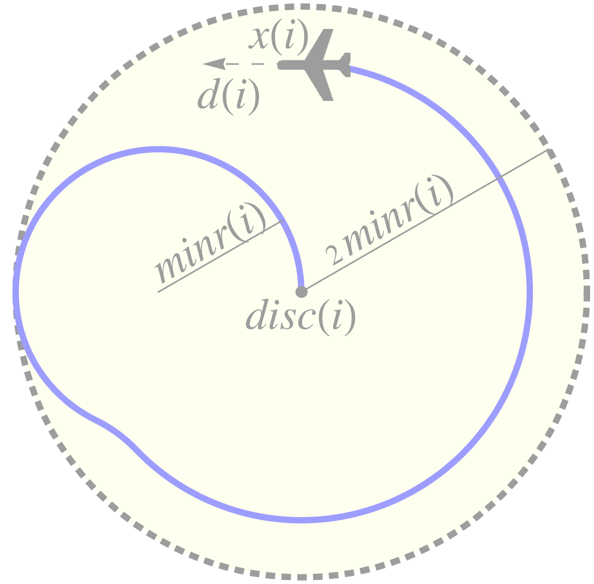
$$\texttt{NotCA} \equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter})$$

$$\texttt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k))$$

$$\texttt{Exit} \equiv ?(disc(k) = x(k));\ ca(k) := 0$$

$$\texttt{Enter} \equiv \omega(k) := side(k) \cdot \Omega(k);\ ca(k) := 1$$

$$\texttt{Flip} \equiv side(k) := -side(k)$$



$$\texttt{Plant} \equiv \forall i : \mathbb{A}\ \big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) \cdot d(i)^{\perp},$$

$$disc(i)' = (1 - ca(i)) \cdot v(i) \cdot d(i)\ \&\ \texttt{EvDom}\big)$$

✔ **Verified in KeYmaeraD**

$$\texttt{EvDom} \equiv \forall j : \mathbb{A}$$

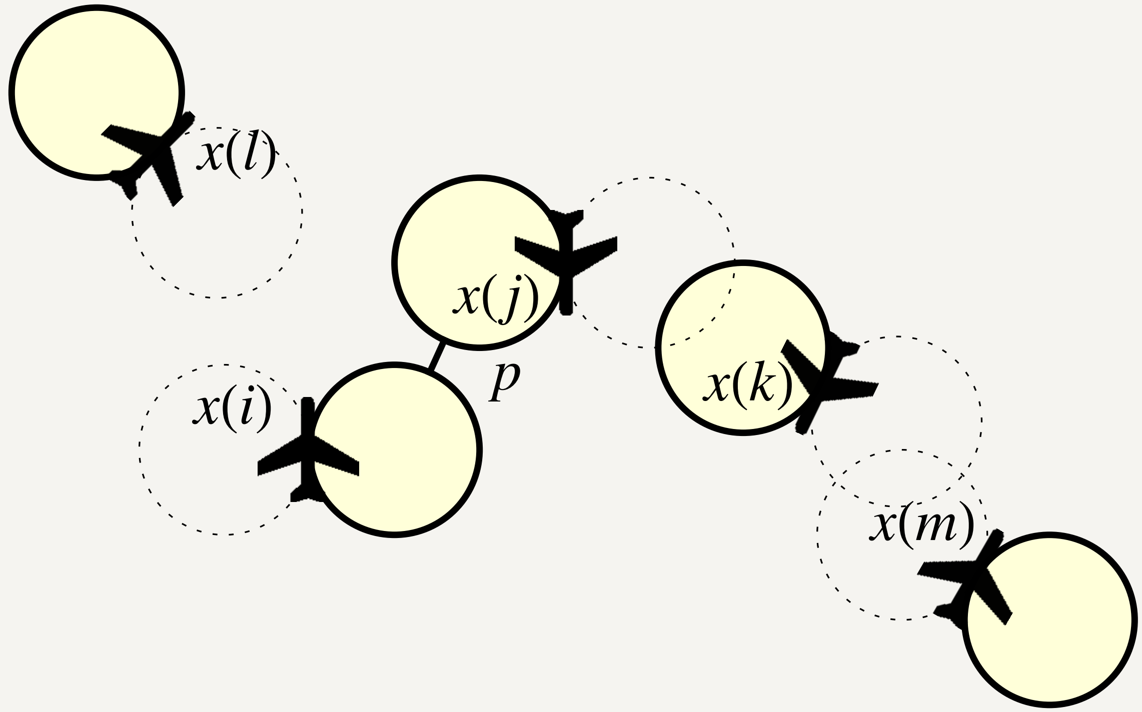
$$((j \ne i \wedge (ca(i) = 0 \vee ca(j) = 0)) \rightarrow \mathsf{Sep}(i, j)$$

$$\wedge\ \|disc(i) - (x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp})\|$$

$$\le minr(i))$$

$$\mathsf{Sep}(i, j) \equiv \|disc(i) - disc(j)\| \ge 2minr(i) + 2minr(j) + p$$

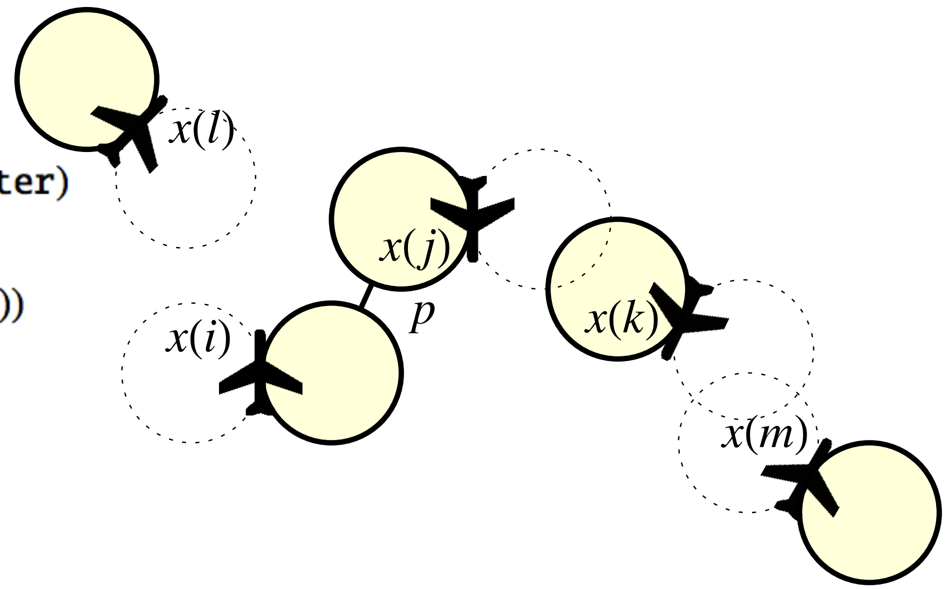
Small Discs Control



- Deterministic control makes it well suited for UAVs.
- Smaller discs allow aircraft to fly closer together.
- Aircraft may exit maneuver as soon as it is safe to do so.

Small Discs Control

$$\begin{aligned}
\texttt{SmallDiscs} &\equiv (\texttt{Control} \cup \texttt{Plant})^* \\
\texttt{Control} &\equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA}) \\
\texttt{CA} &\equiv ?(ca(k) = 1);\ (\texttt{Exit} \cup \texttt{Skip}) \\
\texttt{NotCA} &\equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter}) \\
\texttt{Skip} &\equiv ?true \\
\texttt{Steer} &\equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k)) \\
\texttt{Exit} &\equiv ca(k) := 0 \\
\texttt{Enter} &\equiv (\omega(k) := side(k) \cdot \Omega(k));\ ca(k) := 1 \\
\texttt{Flip} &\equiv ?(\forall j : \mathbb{A}\ (j \ne k \rightarrow \mathsf{FlipSep}(j,k)));\\
&\quad\ side(k) := -side(k) \\
\mathsf{FlipSep}(i,j) &\equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) \\
&\quad - (x(j) - minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \\
&\quad \ge minr(i) + minr(j) + p \\
\texttt{Plant} &\equiv \forall i : \mathbb{A}\ \big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) d(i)^{\perp} \\
&\quad \&\ \forall j : \mathbb{A}\ ((j \ne i \land (ca(i) = 0 \lor ca(j) = 0)) \\
&\qquad \rightarrow \mathsf{Sep}(i,j))\big) \\
\mathsf{Sep}(i,j) &\equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) \\
&\quad - (x(j) + minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \\
&\quad \ge minr(i) + minr(j) + p
\end{aligned}$$



Small Discs Control

$$\texttt{SmallDiscs} \equiv (\texttt{Control} \cup \texttt{Plant})^*$$

$$\texttt{Control} \equiv k := *_{\mathbb{A}};\ (\texttt{CA} \cup \texttt{NotCA})$$

$$\texttt{CA} \equiv ?(ca(k) = 1);\ (\texttt{Exit} \cup \texttt{Skip})$$

$$\texttt{NotCA} \equiv ?(ca(k) = 0);\ (\texttt{Steer} \cup \texttt{Flip} \cup \texttt{Enter})$$

$$\texttt{Skip} \equiv ?true$$

$$\texttt{Steer} \equiv \omega(k) := *_{\mathbb{R}};\ ?(-\Omega(k) \le \omega(k) \le \Omega(k))$$

$$\texttt{Exit} \equiv ca(k) := 0$$

$$\texttt{Enter} \equiv (\omega(k) := side(k) \cdot \Omega(k));\ ca(k) := 1$$

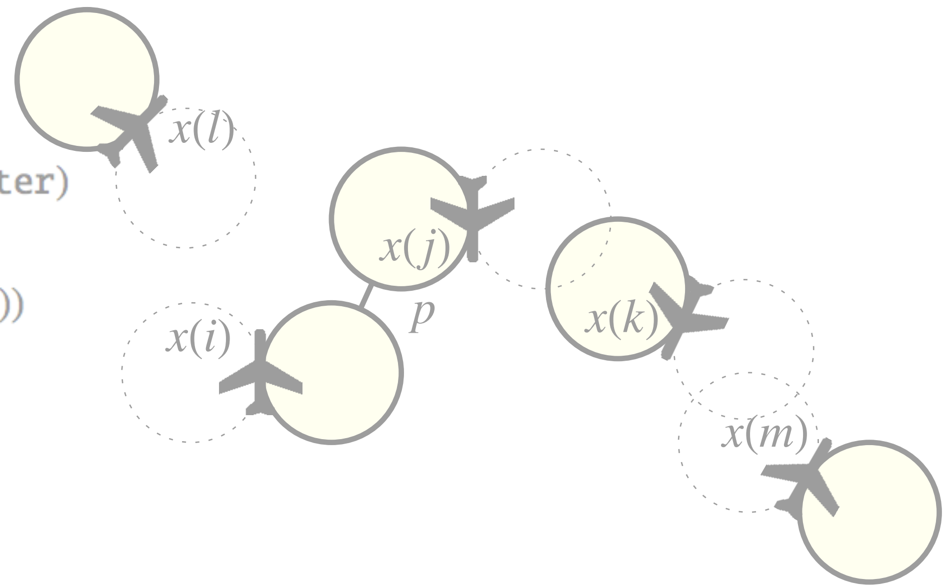
$$\texttt{Flip} \equiv ?(\forall j : \mathbb{A}\ (j \ne k \to \mathsf{FlipSep}(j, k)));\ side(k) := -side(k)$$

$$\mathsf{FlipSep}(i, j) \equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) - (x(j) - minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \ge minr(i) + minr(j) + p$$

✔ Verified in KeYmaeraD

$$\texttt{Plant} \equiv \forall i : \mathbb{A}\ \big(x(i)' = v(i) \cdot d(i),\ d(i)' = \omega(i) d(i)^{\perp}\ \&\ \forall j : \mathbb{A}\ ((j \ne i \wedge (ca(i) = 0 \vee ca(j) = 0)) \to \mathsf{Sep}(i, j))\big)$$

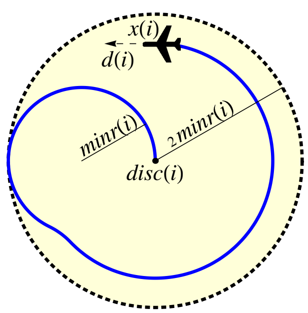
$$\mathsf{Sep}(i, j) \equiv \|(x(i) + minr(i) \cdot side(i) \cdot d(i)^{\perp}) - (x(j) + minr(j) \cdot side(j) \cdot d(j)^{\perp})\| \ge minr(i) + minr(j) + p$$



Conclusions

Challenges

- Infinite, continuous, and evolving state space, $\mathbb{R}^\infty$
- Continuous dynamics
- Discrete control decisions
- Distributed dynamics
- Arbitrary number of aircraft
- Emergent behaviors



Solutions

- Quantifiers for distributed dynamics
- Compositionality – using small problems to solve the big ones
- Hierarchical and modular proofs
- Non-linear flight paths allow flyable maneuvers