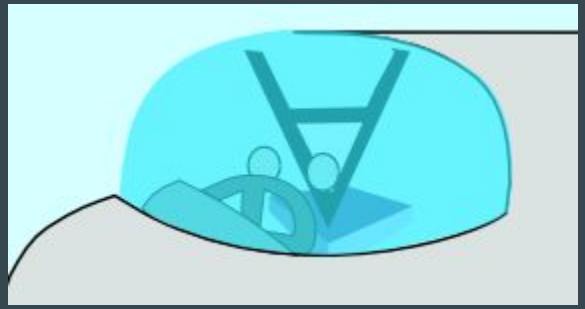


Proofs in the Pilot's Seat

...

Toward Verified Simultaneous Maneuvers in the Next-Generation Airborne Collision Avoidance System

Brandon Bohrer (bbohrer@cs.cmu.edu)

Who Came Here By Plane?

...

Want to Get Home Alive?

...

Background: Collision Avoidance

- Onboard collision avoidance offers last-minute advice to pilots
- Aircraft remains under human control
- Current Generation: TCAS
- Next Generation: ACAS X
  - Enable denser airspace by reducing spurious alerts
  - Improve safety beyond levels achieved by TCAS

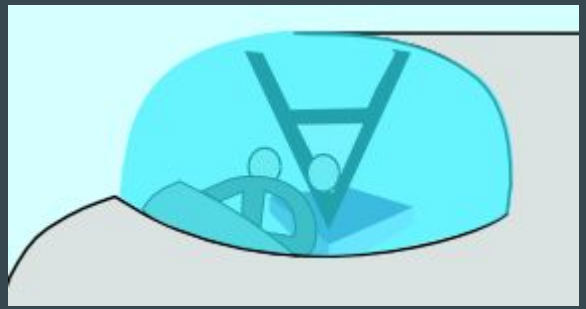
Image Source: FlySafe Project - http://www.eu-flysafe.org/Project/Aviation-Hazards/Air-Traffic/current-systems.html

Background: ACAS X Verification

- ACAS X implementation extremely large
  - Lookup table with millions of states
- ACAS X *output* extremely simple
  - One of twelve maneuvers
- Idea: Verify correctness of *output*, not *implementation*.
- Verification approach:
  - Exhaustive testing (cover entire lookup table)
  - Compute safe maneuvers for each state
  - Compare with ACAS X output
  - **Verify correctness of "safe maneuvers" computation**

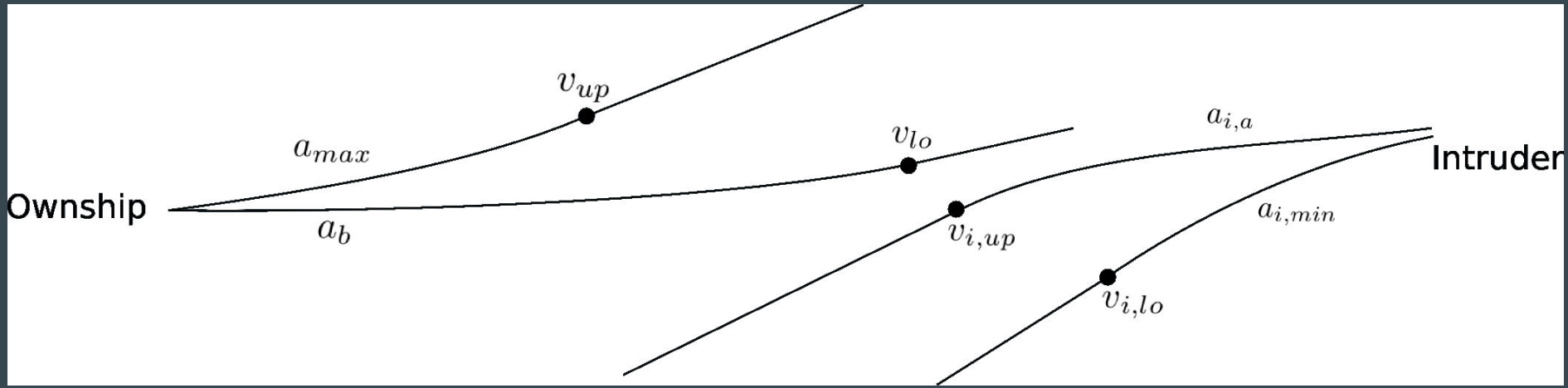
Using Verification in the Implementation

- **Problem:** Not all ACAS X bugs easily fixed by changing lookup table
- **Solution:** Use safety analysis *in production* to provide safer advice
- Compare ACAS X result with list of safe maneuvers
- If given unsafe maneuver when safe one exists, **change it!**
- **Problem:** *Really* need to trust the safety analysis
- Need to generalize previous verification results



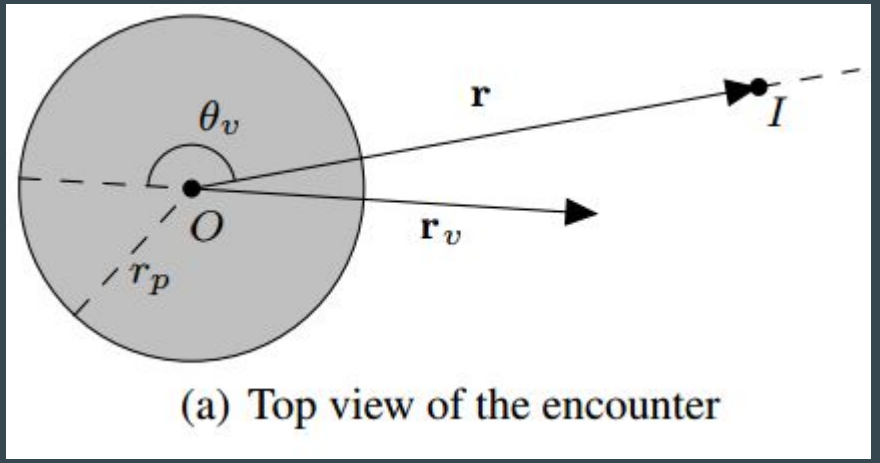
Project: Verified Simultaneous Maneuvers

- **Prior work (by others):** Assumes intruder aircraft moves in straight line.
- What if both aircraft are equipped with ACAS X?
- What if intruder aircraft makes evasive maneuvers?
- What if intruder aircraft behaves randomly?
- **Solution:** Model encounters where both aircraft maneuver



Modeling: Dynamics

- Assumption: Aircraft flying head-on
- Assumption:
  Constant horizontal velocity
- Vertical acceleration changes discretely
- Vertical trajectory:
  Sequence of parabolas
- Differential Equation:
  - r' = -vr,
    h' = v, v' = a,
    hi' = vi, vi' = ai

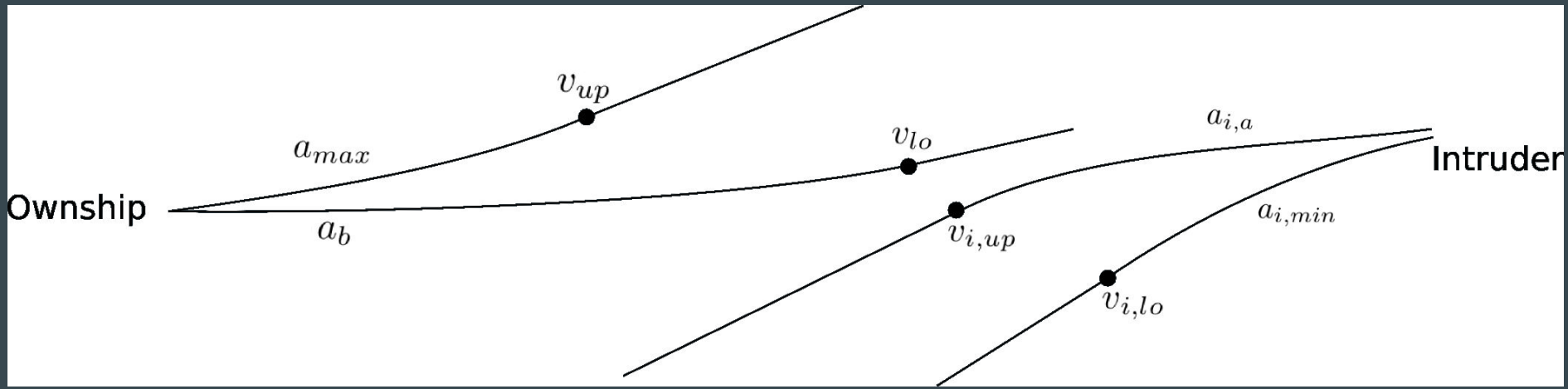


(a) Top view of the encounter

Image Source: [JBJ2105]

(Prior Work) Modeling: Maneuvers

- Bounds a_min <= a <= a_max obeyed at all times
- Target velocity range v_min <= v <= v_max
- Accelerate with acceleration a_a or a_b to achieve desired velocity



Contribution: Safe Regions

- Maneuver safe iff ownship is *always above* or *always below* intruder
- Compute acceleration lower bound a_lo
  - “Is the aircraft forced to accelerate upward?”
- Compute acceleration upper bound a_up in {a_max, a_a}
  - “Is the aircraft forced to accelerate downward?”
- At all points in trajectory, ownship and intruder bounds separated

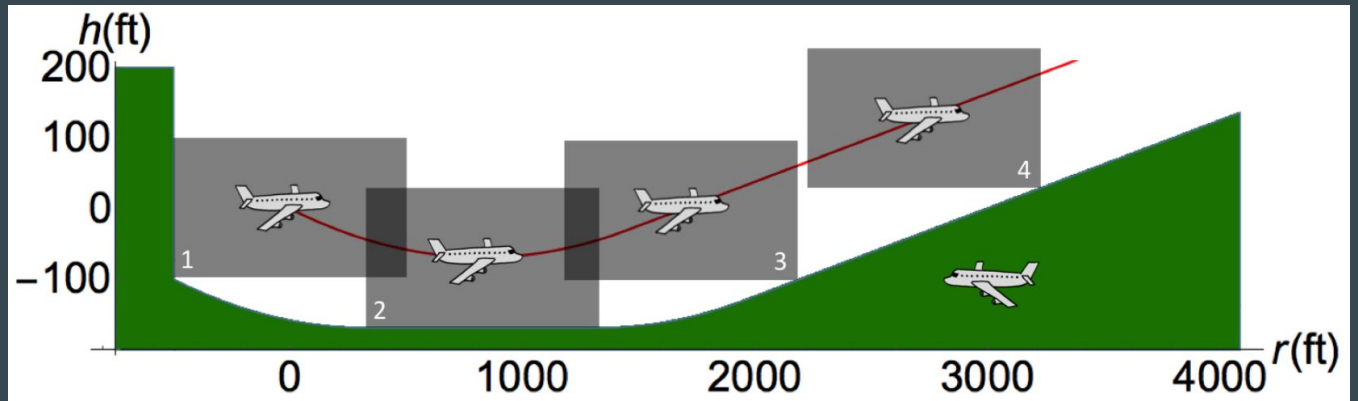


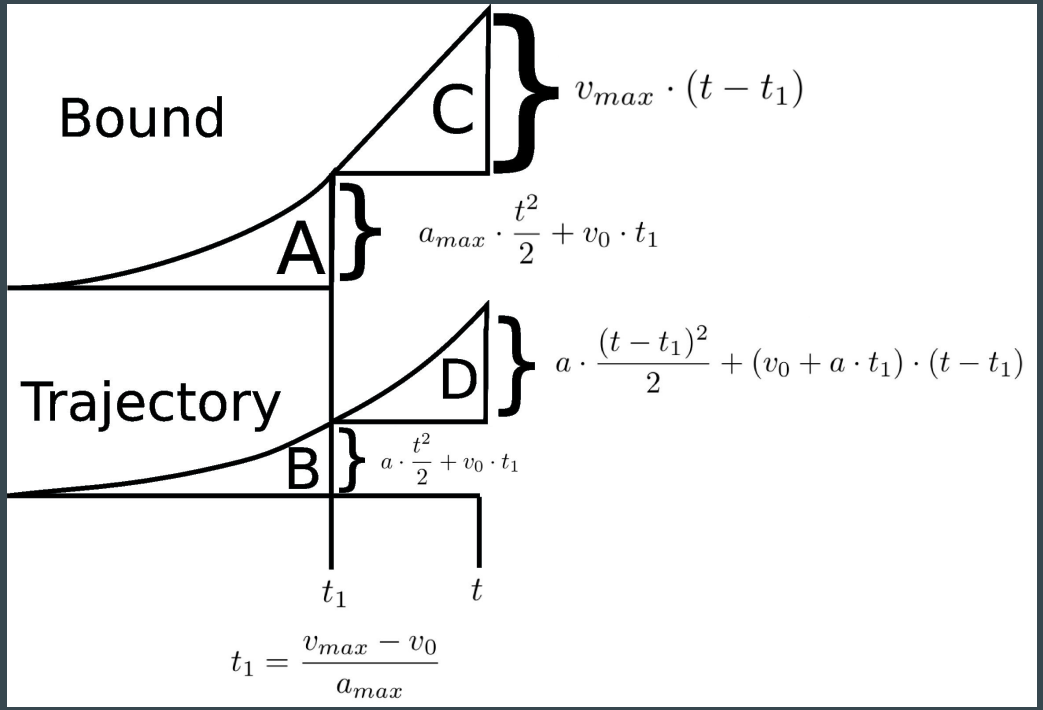
Fig. 1 Nominal trajectory of the ownship (red) and safe region for the intruder (green), immediate response

Image Source: [JBJ2105]

Contribution: Proof

- Always above intruder vs. always below intruder (2 cases)
- Constraints on a_lo, a_up? (4 cases)
- Is each trajectory quadratic or linear? (4 cases)
- In total: 2 * 2 * 4 = 32 cases
- Each case: First-order arithmetic problems
- Use custom tactic library for arithmetic proofs
- **Current progress:** 2 - epsilon cases (this proof is hard)
    - Third case somewhat harder
    - Many other cases are symmetric

Proof Example: Linear-Quadratic Case



1. $B + D \leq A + C$
2. $a \leq a_{max}$
3. $$\begin{aligned} & A \cdot \frac{t - t_1}{2} + (v_0 + a \cdot t_1) \\ \leq & v_0 + a \cdot (t_1 + (t - t_1)) \\ = & v \\ \leq & v_{max} \end{aligned}$$

References

- A Formally Verified Hybrid System for Safe Advisories in the Next-Generation Airborne Collision Avoidance System. Jean-Baptiste Jeannin, et. al. Manuscript, November 2015
- Yanni Kouskoulas, et. al. Safe advisories for ACAS X in the presence of curved trajectories and non-deterministic intruder behavior. Unpublished Work (in progress), 2016.
- Mykel J. Kochenderfer and James P. Chryssanthacopoulos. Robust airborne collision avoidance through dynamic programming. Project Report ATC-371, MIT Lincoln Laboratory, 2011.