Formal Verification of Next-Generation Airborne Collision Avoidance System with Adversarial Intruder Behavior

Rachel Cleaveland

Advisor: André Platzer

Background

- **Mid-air aircraft collisions** are increasing in likelihood as air space gets more congested.
  - Collision avoidance maneuvers must be performed as a last resort when two aircraft are on a collision course.
- It is imperative to **formally verify the safety of these maneuvers** in advance under all reasonable flight circumstances to ensure that no collisions happen.
- **ACAS X** is a collision-avoidance system developed by the Federal Aviation Association (FAA) [1].
  - Tracks the position and velocity of an ownship and intruders in its vicinity and uses this data in its collision avoidance advisories.
  - An advisory asks the pilot to maintain their vertical speed, or accelerate towards a new vertical speed.
  - Advisories only apply to the aircraft's climb rate in the vertical direction (not horizontal)

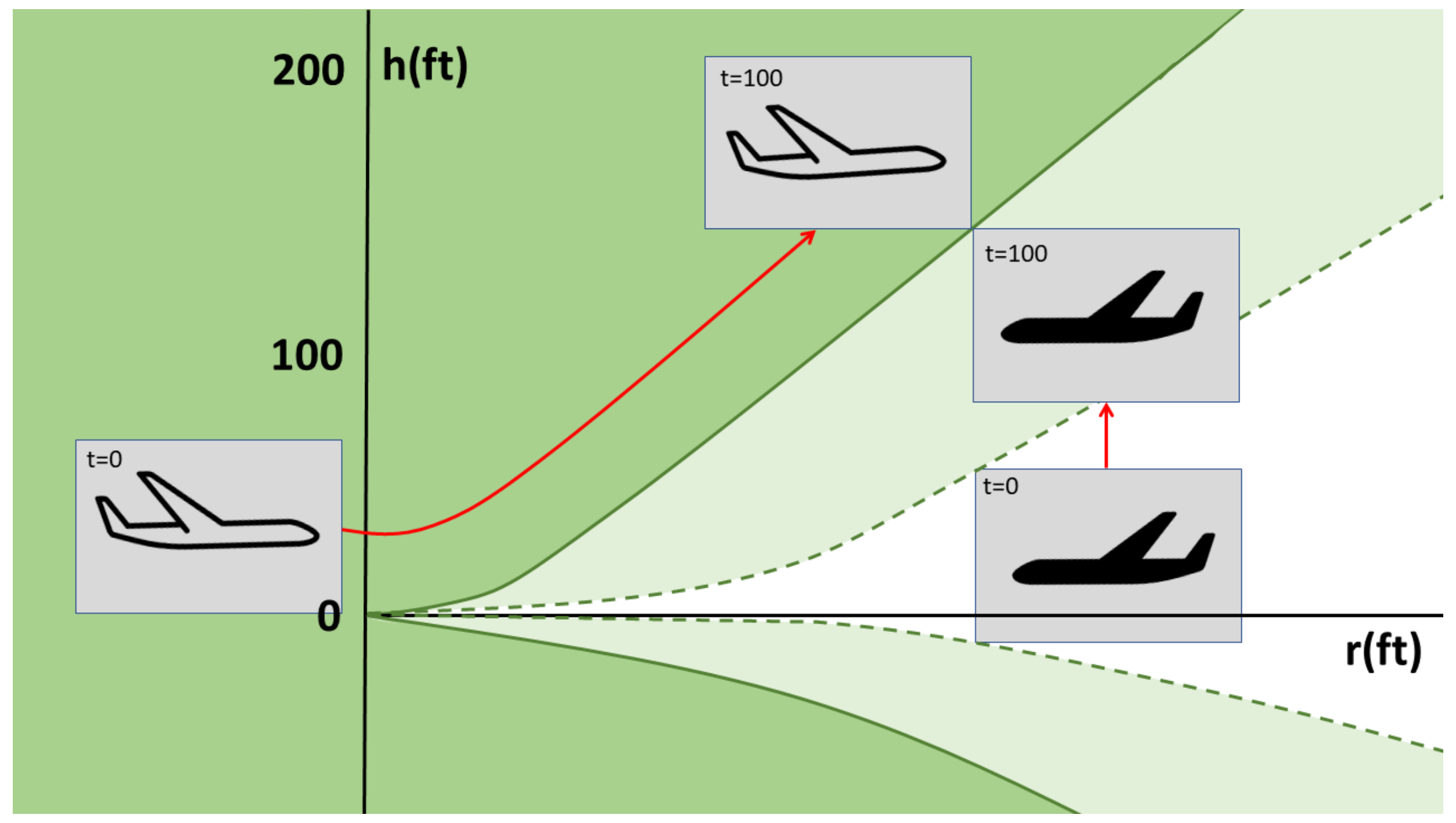

Figure 1: Safe region (dark green) and minimally compliant trajectory (red) with a vertically maneuvering intruder. The region that would be safe without intruder maneuverability is shown in light green.

Introduction

- **Previous work has assumed severe restrictions on the intruder's maneuverability** in their formal verification of ACAS X, limiting their safety guarantees in real-world collision scenarios.
- Our previous work [2] used hybrid systems in its verification and introduced the idea of *safe regions.*
  - A region is safe if for all possible ownship positions and velocities within the region, a near mid-air collision (NMAC) will never occur (Fig. 1).
  - If ACAS X issues an advisory, and following this advisory always keeps the ownship within a safe region, then this advisory is guaranteed to be safe.
  - This work assumed that the intruder aircraft is approaching at a constant velocity, both horizontally and vertically.

Contribution

- My work represents aircraft encounters with Differential Game Logic (dGL) [3] as opposed to the Differential Dynamic Logic [4] of our previous work.
  - dGL allows for the **modeling of an intruder aircraft that can change its flight path and velocity** as the encounter is evolving.
  - Hybrid games apply perfectly to collision-avoidance because the intruder may act adversarially, and the ownship must have a **strategy to overcome any sequence of intruder maneuvers**.
- This is the first work that we know of to apply hybrid games to the problem of collision-avoidance.

```
1  $\text{init}() \land R(r,h,v,\text{advisory} = (w, v_{lo})) \rightarrow$
2  $[(\quad (\text{advisory} := (w, v_{lo}); ?R(r,h,v,\text{advisory} = (w, v_{lo})); )$
3          $(a_o := \text{ownship}(\text{advisory}); )^d$
4          $(\boldsymbol{a_i := \textbf{intruder}}\ \ ;$
5              $\{\text{motion}(a_o, a_i) \quad \& \quad \text{EDC}(v, v_{lo}, a, a_{lo})\}$
6          $)^*$
7  $)^*](\neg\text{NMAC})$
```

Figure 2: high-level model showing the general structure of the models developed in this work

Model Overview

- Formula P → [α]Q (Fig. 2) says that all executions of hybrid program α starting in a state satisfying logical formula P end up in a state satisfying Q.
- Preconditions require ownship to be in a *safe region* R(r, h, v, advisory=(w,v_{lo})) for initial advisory (w,v_{lo}).
- Lines 2-4 encode the discrete choices of the advisory, followed by the ownship and intruder accelerations
  - Intruder choice (line 4) is omitted from models that do not allow for intruder maneuverability.
- **Ownship choice (line 3) is contained in the (^{d}) operator, which differentiates choices made by the ownship and intruder.**
  - All choices in the program (^{d}) are resolved by our helpful player, so we need only show that the pilot *can* strategically pick her acceleration such that for *any* advisory satisfying the safe region and *any* set of intruder actions, a collision does not occur.
- Motion equations (line 5) are followed for any duration of time, as long as the evolution domain constraint (EDC(v,a)) is true.
- Final * operator means that the program can be repeated any number of times.
  - Postcondition guarantees that *any sequence* of advisories satisfying our safe region will be safe.

Results

- **Developed and proved seven hybrid game models** verifying under appropriate assumptions that the ownship can always maneuver to safety.
- Each model was developed and verified using the theorem prover KeYmaera X.
- Model categories
  - **Infinite-horizon**
    - Requires advisories to be safe indefinitely
      - While the system can issue follow-up advisories, the aircraft must avoid collision *whether or not* a new advisory is issued.
    - This is a rigid definition of safety: in some scenarios it is better to follow an unsafe advisory for limited time, followed by an advisory that is safe indefinitely
  - **Finite-horizon**
    - Proves safety of advisories only up to Ɛ-time
    - No liveness: does not give formal safety guarantees after Ɛ-time
    - Stepping-stone to the safeable models
  - **Safeable**
    - An advisory is *safeable* if and only if it is safe or can still be made safe in the future, if necessary, via subsequent advisories.
    - Proves Ɛ-time safety with liveness: advisories are safe after Ɛ-time if there exists a follow-up advisory which is safe indefinitely
    - Example shown in Fig. 3
- Infinite-horizon models
  - Model 1: non-maneuvering intruder
  - Model 2: vertically-maneuvering intruder
  - Model 3: horizontally-maneuvering intruder
- Finite-horizon models
  - Model 4: non-maneuvering intruder
  - Model 5: vertically-maneuvering intruder
- Safeable models
  - Model 6: non-maneuvering intruder
  - Model 7: vertically-maneuvering intruder

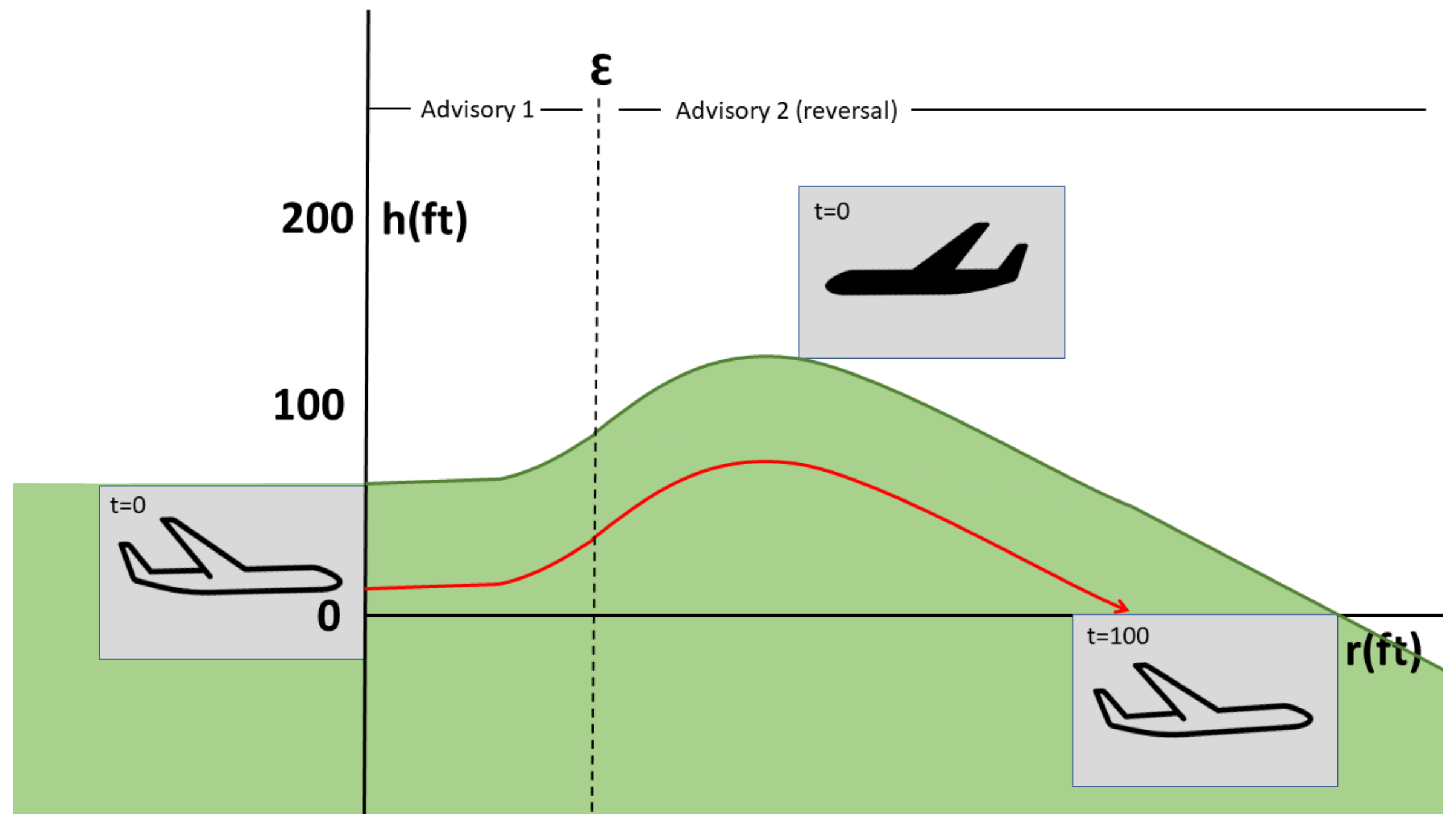

Figure 3: safe region (green) of an ownship following Advisory 1 for Ɛ-time and Advisory 2 afterwards

Conclusion

- This work applied hybrid games to the verification of ACAS X
  - Proved that against an intruder with limited maneuverability, an ownship given a safe ACAS X advisory can always find a verifiably safe path.
- Challenges
  - Development of an ownship strategy
    - Ownship does not know intruder actions in advance, only the broad limitations of the intruder's maneuvering capabilities.
    - Strategy must ensure safety no matter what the intruder chooses to do.
  - Correct assignment of responsibility for each action
    - Positive outcomes of one actor act as negative outcomes for the other.
    - Vital to the correctness of the model that the discrete choices be resolved by the correct actor to prevent any unfair advantages.
    - Previous model iterations incorrectly allowed the choice of advisory to be resolved by the ownship, allowing the ownship to choose an *optimal* advisory instead of proving safety of *all possible* advisories.

Future Work

- Develop and prove bounded-time and safeable models in which the intruder has horizontal maneuverability
- Develop models for an intruder which can simultaneously maneuver horizontally and vertically
- Ownship collision-avoidance maneuvers are currently limited to the vertical direction
  - Expand ownship maneuverability to the horizontal direction

References

1. Federal Aviation Administration TCAS Program Office: Algorithm design descrip-tion for the surveillance and tracking module of ACAS X (2014). Run12
2. Jeannin, J., et al.: A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system. STTT **19**(6), 717–741 (2017).
3. Platzer, A.: Differential game logic for hybrid games. Technical Report CMU-CS-12-105, School of Computer Science, Carnegie Mellon University,Pittsburgh, PA(2012).
4. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas.41(2),143–189 (2008).