Differential Radical Invariants: Safety Verification and Design of Correct Hybrid Systems

Khalil Ghorbal PI: André Platzer
Computer Science Departement Carnegie Mellon University
kghorbal@cs.cmu.edu

6 - 7 Nov, 2014
Arlington, VA

1. *Hybrid Systems Theorem Proving*

Context
[Hybrid Program]

```
Init
⟶
[(
 Sensing: read data from sensors
 Control: actuate
 Plant: evolve ◀ ◀ ◀ ◀ ◀
)*]
Safety
```

Focus
[Ordinary Differential Equations]

- No closed form solution exists in general
- Transcendental functions are oftem involved
- Alternatives
  - Local approximations (Taylor series) [Lanotte et al. 2005]
  - Inductive (differential) Invariants [Maths, ThPhy 1870-] [Control 1900-] [FM 2001-]

Challenges
[Characterizing Invariant Varieties]

Invariant Checking

- Given $\dot{\boldsymbol{x}} = \boldsymbol{f}$, and $\boldsymbol{x}(0)$ such that $p(\boldsymbol{x}(0)) = 0$, is $p(\boldsymbol{x}(t)) = 0$ for all t ?

Invariant Generation

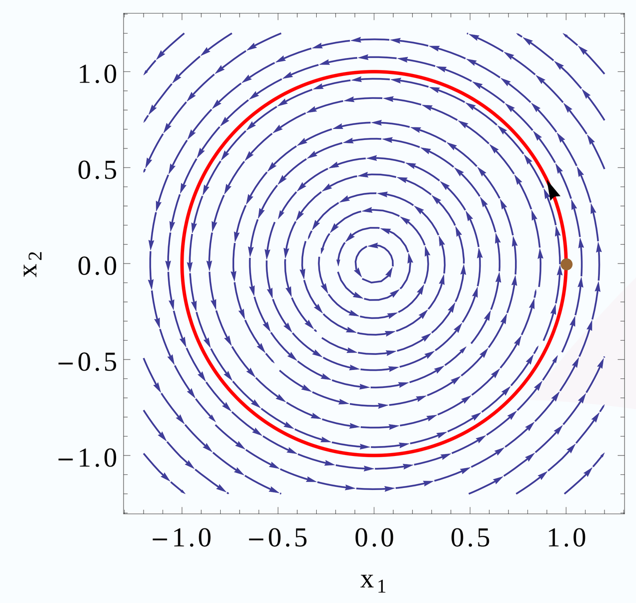
- Given $\dot{\boldsymbol{x}} = \boldsymbol{f}$, how to generate p such that $p(\boldsymbol{x}(t)) = 0$?

Contributions
[DRI Related Publications]

- [TACAS 2014] *Characterizing algebraic invariants by differential radical invariants*
- [SAS 2014] *Invariance of conjunctions of polynomial equalities for algebraic differential equations*
- [JAIS 2014] *Hybrid theorem proving of aerospace systems: Applications and challenges*
- [VMCAI 2015] *A Hierarchy of Proof Rules for Checking Differential Invariance of Algebraic Sets*

2. *Algebraic Invariant Equations*

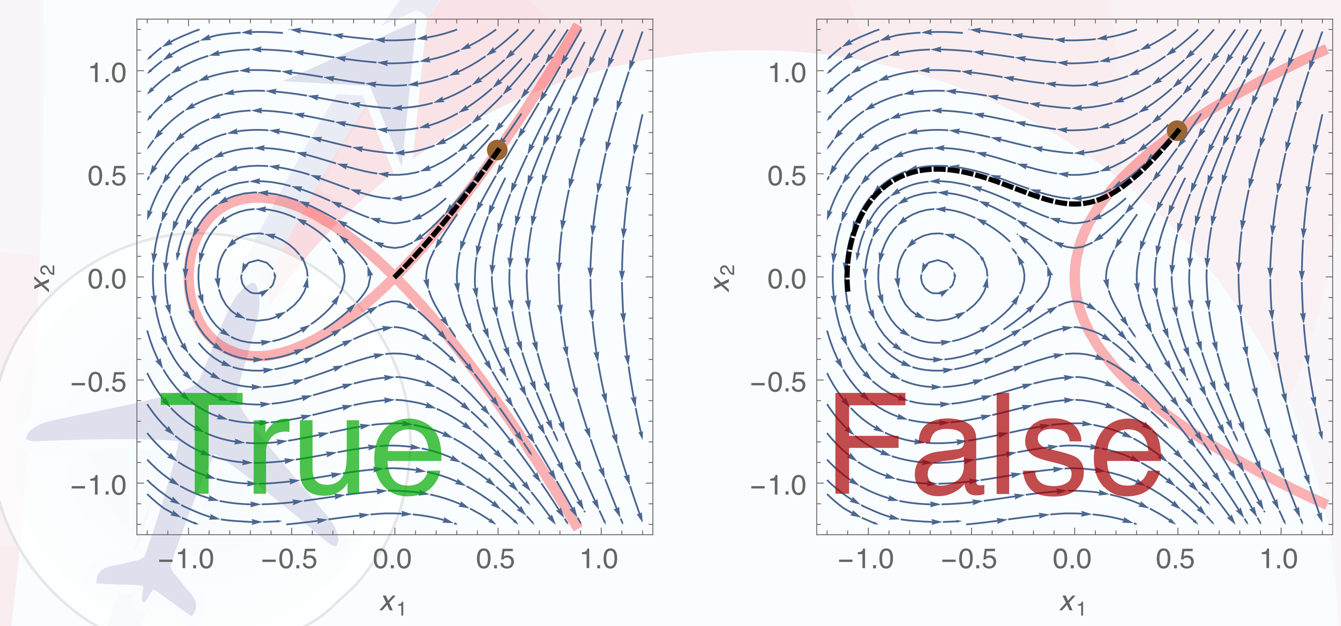
$(\dot{x}_1, \dot{x}_2) = (-x_2, x_1)$



Algebraic Invariant Equation

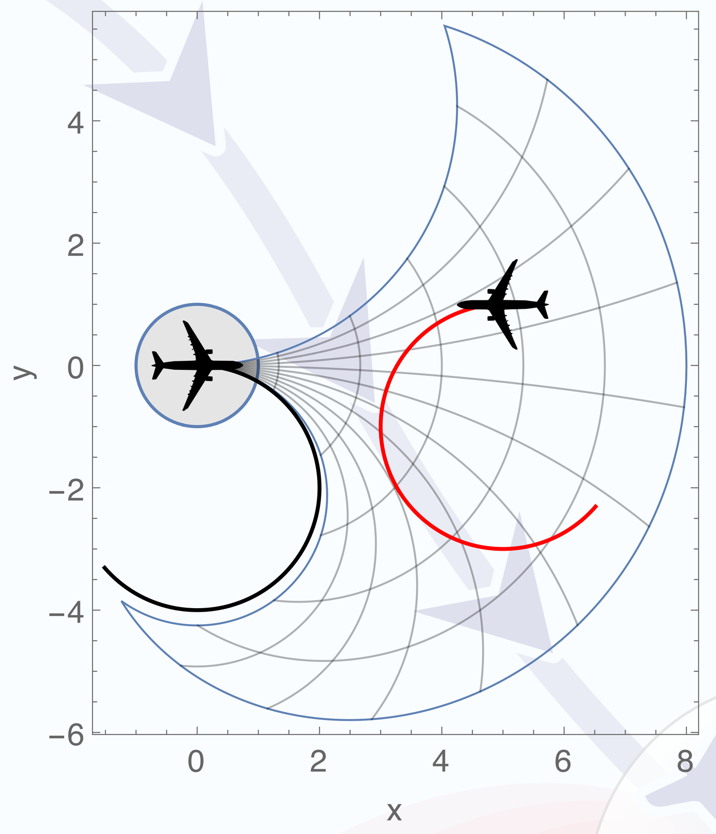
The solution for $\boldsymbol{x}(0) = (1, 0)$ respects $\boxed{x_1(t)^2 + x_2(t)^2 - 1 = 0}$ $\forall t$

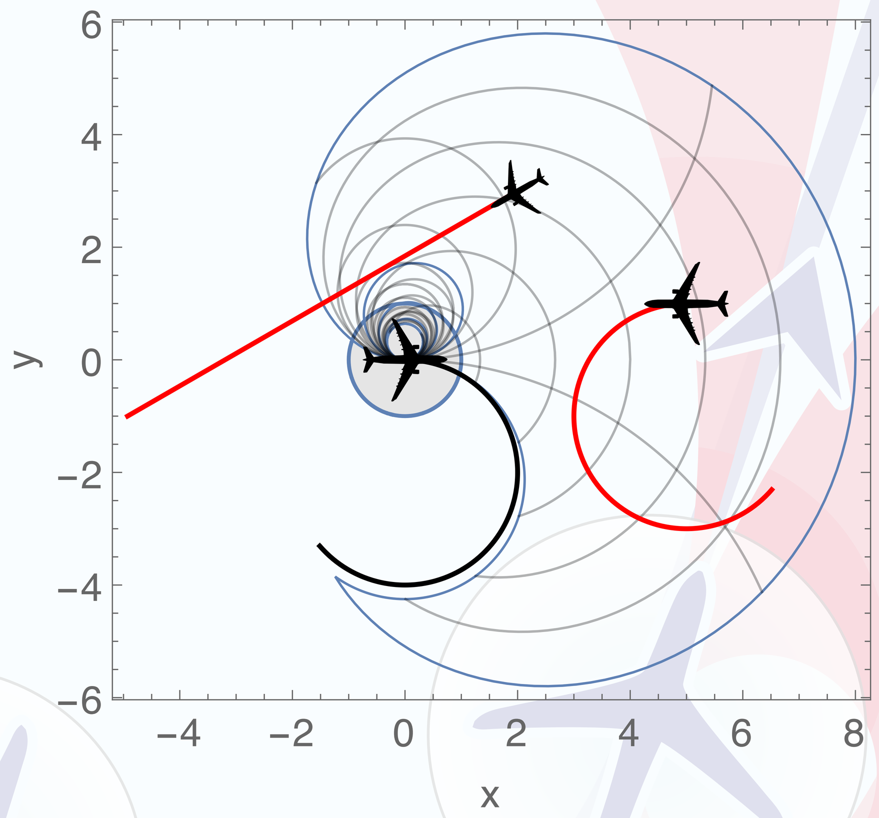
$(\dot{x}_1, \dot{x}_2) = (-2x_2, -2x_1 - 3x_1^2)$



$x_1^2 + x_1^3 - x_2^2 = 0$ $\qquad$ $x_1 - x_2^2 = 0$

3. *Safe-By-Design Collision Avoidance System with Curved, Fully Flighable Trajectories*





- **Differential Equations**

$$\dot{x} = v_2 \cos\theta - v_1 + \omega_1 y$$
$$\dot{y} = v_2 \sin\theta - \omega_1 x$$
$$\dot{\theta} = \omega_2 - \omega_1$$

- **Safety Conditions**

$$\texttt{monitor} \equiv \begin{array}{l} (\omega_1, \omega_2) = (0,0) \longrightarrow I_1(0) > p(v_1 + v_2) \wedge \\ (\omega_1, \omega_2) \neq (0,0) \longrightarrow I_2(0) > 2v_1v_2 + 2p(v_2|\omega_1| + v_1|\omega_2|) + p^2|\omega_1\omega_2| \end{array}$$

- **Generated Invariants**

$$I_1(t) = (v_2 \sin\theta(0))x(t) - (v_2\cos\theta(0) - v_1)y(t)$$
$$I_2(t) = -\omega_1\omega_2\big(x(t)^2 + y(t)^2\big) + 2v_2\omega_1 \sin\theta(t)x(t) + 2(v_1\omega_2 - v_2\omega_1\cos\theta(t))y(t) + 2v_1v_2\cos\theta(t)$$

4. *Differential Radical Characterization* [TACAS 2014]

➙ N_p is **finite** $\rightsquigarrow$ The problem is **<u>decidable</u>**

$$✓\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle \ \wedge \ p = 0 \to \mathfrak{D}^{(N_p-1)}(p) = 0 ✓$$
$$\vdots$$
$$✗\mathfrak{D}^{(3)}(p) \in \langle p, \mathfrak{D}(p), \mathfrak{D}^{(2)}(p)\rangle \ \wedge \ p = 0 \to \mathfrak{D}^{(2)}(p) = 0 ✓$$
$$✗\mathfrak{D}^{(2)}(p) \in \langle p, \mathfrak{D}(p)\rangle \ \wedge \ p = 0 \to \mathfrak{D}(p) = 0 ✓$$
$$\frac{✗\mathfrak{D}(p) \in \langle p\rangle \ (\exists\lambda \in \mathbb{R}[\boldsymbol{x}] : \mathfrak{D}(p) = \lambda p)}{(p = 0) \to [\dot{\boldsymbol{x}} = \boldsymbol{f}](p = 0)}$$

▶ ▶ ▶ ▶ ▶ ◀ ◀ ◀ ◀ ◀

Generating Invariant Equations

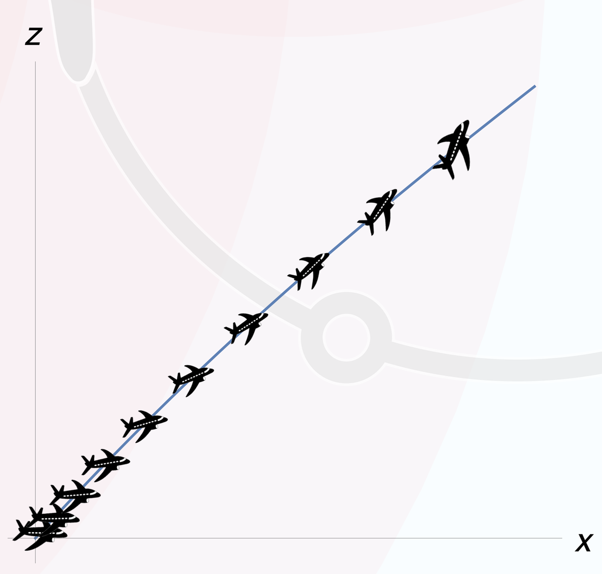
$$\mathfrak{D}^{(N_p)}(p) \in \langle p, \ldots, \mathfrak{D}^{(N_p-1)}(p)\rangle$$

if and only if

$$\exists\lambda_i \in \mathbb{R}[\boldsymbol{x}], \boxed{\mathfrak{D}^{(N_p)}(p) = \sum_{i=0}^{N_p-1} \lambda_i \mathfrak{D}^{(i)}(p)}$$

➙ Equivalent to the <u>MinRank Problem</u>: **Symbolic Linear Algebra**
at least **NP-hard** but in **PSPACE** [Buss et al. 1999]

5. *Longitudinal Motion of Aircraft*



Longitudinal Dynamics of an Airplane

$\dot{u} = \frac{X}{m} - g\sin(\theta) - qw$	u : axial velocity
$\dot{w} = \frac{Z}{m} + g\cos(\theta) + qu$	w : vertical velocity
$\dot{x} = \cos(\theta)u + \sin(\theta)w$	x : range
$\dot{z} = -\sin(\theta)u + \cos(\theta)w$	z : altitude
$\dot{q} = \frac{M}{I_{yy}}$	q : pitch rate
$\dot{\theta} = q$	θ : pitch angle

Automatically Generated Invariant Functions

$$I_1 = \frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta)$$
$$I_2 = \frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta)$$
$$I_3 = -q^2 + \frac{2M\theta}{I_{yy}}$$