Invariant Synthesis for Hybrid Systems.

Sriram Sankaranarayanan
University of Colorado, Boulder, CO.

November 2, 2011.

Talk Outline

1. Invariant Synthesis
2. Algebraic Invariants
3. Results

Example #1: Square Root Calculation

Example: Compute $\lceil \sqrt{n} \rceil$, for $n \geq 0$.

```
int computeSqrt ( int n )
    @Pre: n ≥ 0
1:  int i, j = (0, 0);
2:  while ( j ≤ n ) {        ⟵  j = i², n ≥ 0, j ≤ n + 1, j ≤ n − 2i − 1
3:      i := i + 1;
4:      j := j + 2 ∗ i − 1;
5:  }
    @Post: i² ≥ n ∧ (i − 1)² ≤ n
```

Verification Problem: Is this program *correct*?

Yes: Automatically synthesized invariant.

Example # 2: Hamiltonian System

$$\begin{aligned} \frac{dp_1}{dt} &= -2q_1q_2^2, \\ \frac{dp_2}{dt} &= -2q_1^2q_2, \\ \frac{dq_1}{dt} &= 2p_1, \\ \frac{dq_2}{dt} &= 2p_2 \end{aligned}$$

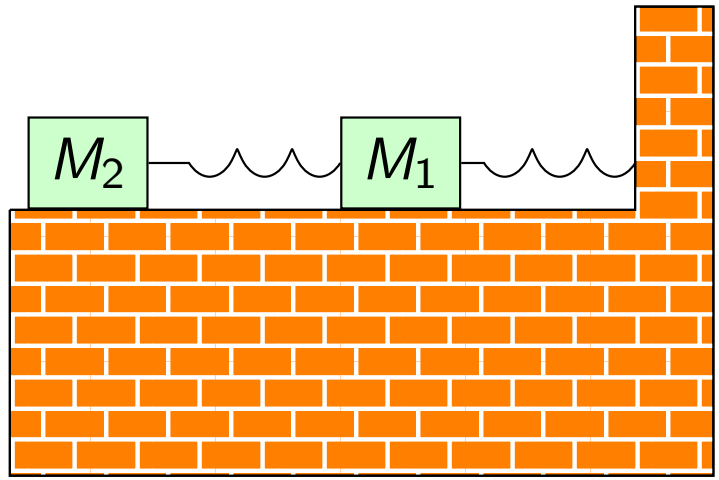
Initial condition:

$$V_0 : \{\vec{x} : (p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q^2 - 1 = 0, q_2 = 0\}.$$

Invariant: $p_1^2 + p_2^2 + q_1^2q_2^2 = 4$.

Example #3: Two Masses connected by Spring

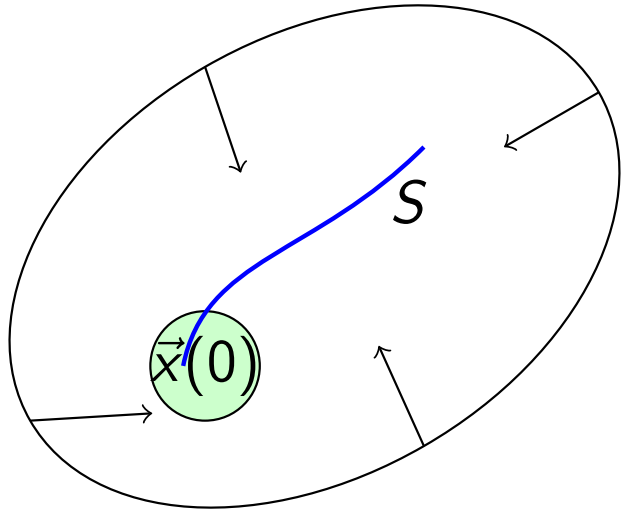
$$
\begin{array}{rcl}
\frac{dx_1}{dt} & = & v_1, \\
\frac{dx_2}{dt} & = & v_2, \\
\frac{dv_1}{dt} & = & -kx_1 - \frac{k}{5}(x_1 - x_2), \\
\frac{dv_2}{dt} & = & k(x_1 - x_2), \\
\frac{dk}{dt} & = & 0
\end{array}
$$



$$V_0 : x_1 = x_2 = 0, v_1 = 1, v_2 = -1, k \in R$$

$$
\begin{array}{rcl}
p_1 & : & 576 + 1200v_1^2 + 625v_1^4 + 2880v_1v_2 + 3000v_1^3v_2 + \\
 & & 528v_2^2 + 4150v_1^2v_2^2 + 1320v_1v_2^3 + 121v_2^4 \\
 & & -1860kx_2^2 + 2750kv_1^2x_2^2 + 1600kv_1v_2x_2^2 \\
 & & +710kv_2^2x_2^2 + 525k^2x_2^4 = 0, \\
p_2 & : & 240x_1 + 250v_1^2x_1 + 600v_1v_2x_1 + 110v_2^2x_1 \\
 & & +396x_2 - 525v_1^2x_2 - 260v_1v_2x_2 - 131v_2^2x_2 - 105kx_2^3 = 0, \\
p_3 & : & 24 + 25v_1^2 + 60v_1v_2 + 11v_2^2 + 50kx_1x_2 + 5kx_2^2 = 0 \\
p_4 & & -21 + 25v_1^2 + 10v_1v_2 + 6v_2^2 + 25kx_1^2 + 5kx_2^2 = 0
\end{array}
$$

What is an invariant?



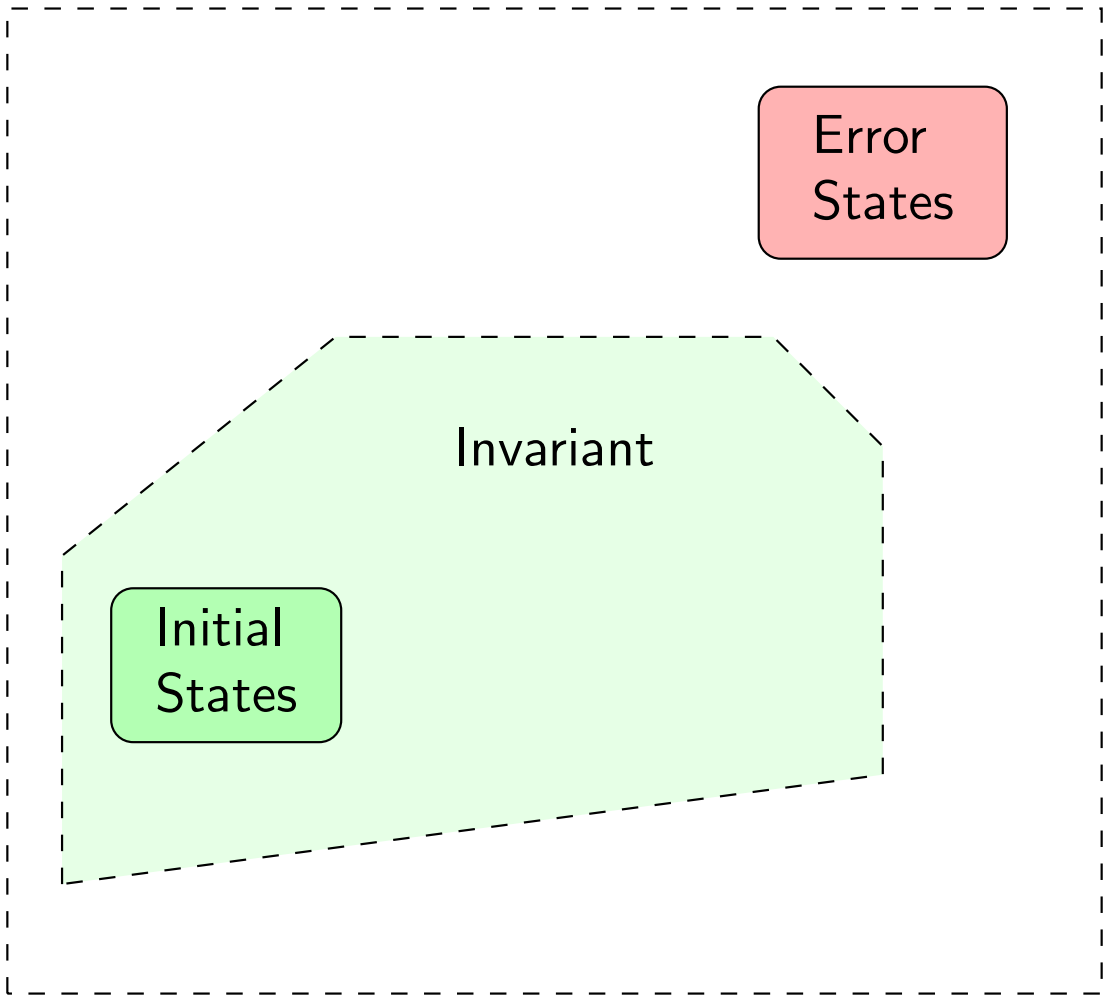
Set of states S is invariant for system $\mathcal{T}$ iff

$$\forall\ \vec{x}(0) \in S,\ \mathcal{T}(\vec{x}(0), t) \in S\,.$$

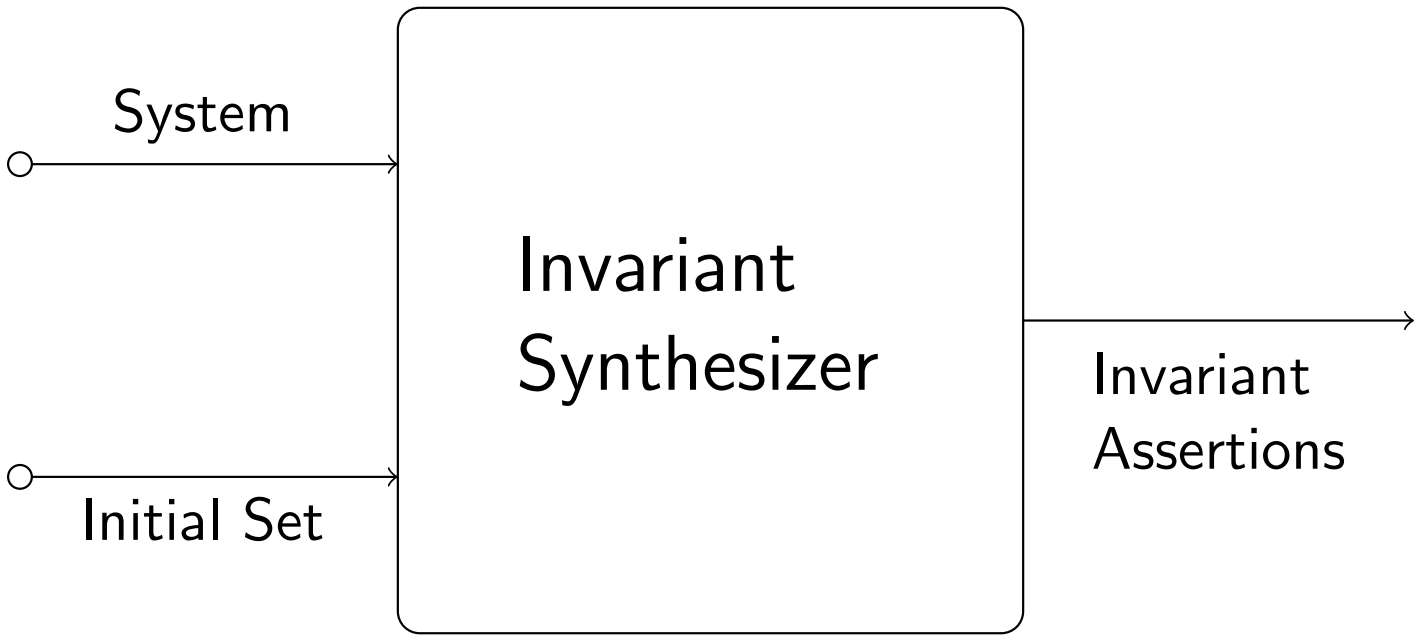
Initial cond. inside set $S \Rightarrow$ entire trajectory inside S.

Why Invariants?

Goal: Prove "unreachability" of error states.



Invariant Synthesis



Invariant Synthesis Techniques for Programs.

- 40+ years of research.
- Floyd'68,Hoare'69, King'69, Manna+Katz'75, Cousot+Cousot'77,Cousot+Halbwachs'78, Mine'02, Sank.+Others'03'05, Gulwani'07,...

Applications:

- Astreé project: Runtime error freedom in Airbus A380 command & control systems (Airbus inc.)
- Absint: Timing verification in real-time systems.
- Polyspace: Verification of control systems (Mathworks inc.).
- F-Soft: C/C++ systems program verification (NEC labs).
- Clousot: .net verification (Microsoft Research).
- ...

Beyond "Just" Programs..

Programs that interact with physical world around us.

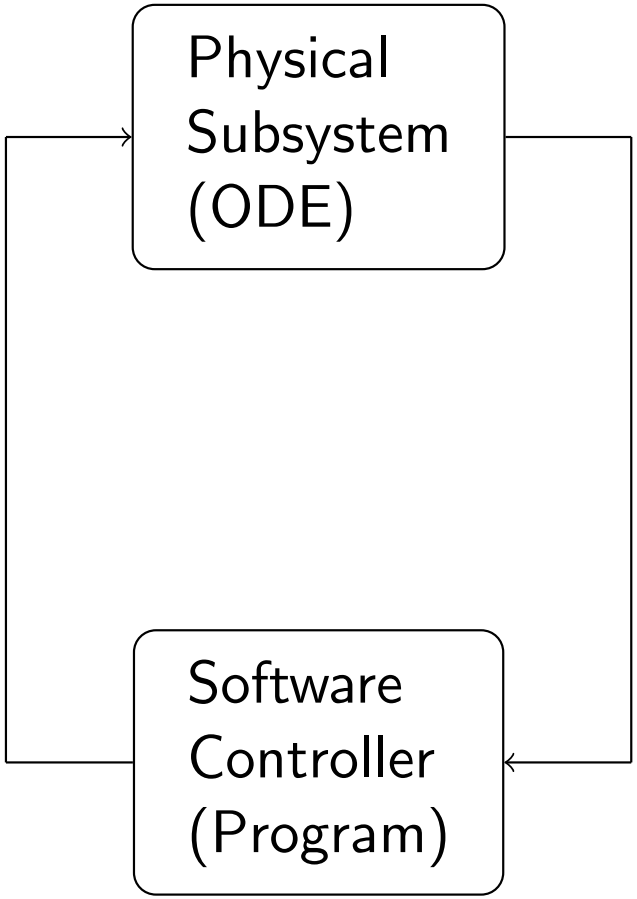
Anti-lock braking
Engine Control
Stability Control
Airbag deployment
Powertrain

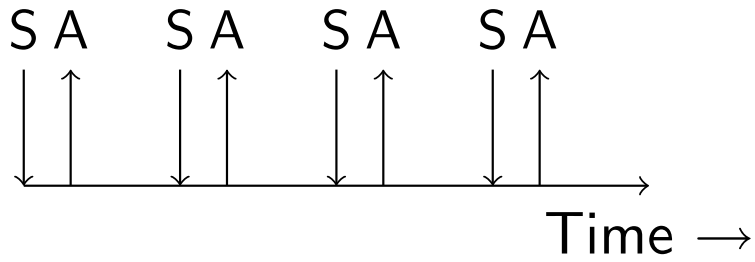
Autopilot
Navigation
Fly-by-wire

Emergency shutdown
Instrumentation

Anesthesia Machines
Ventilators
Infusion Pumps

Software Enabled Control

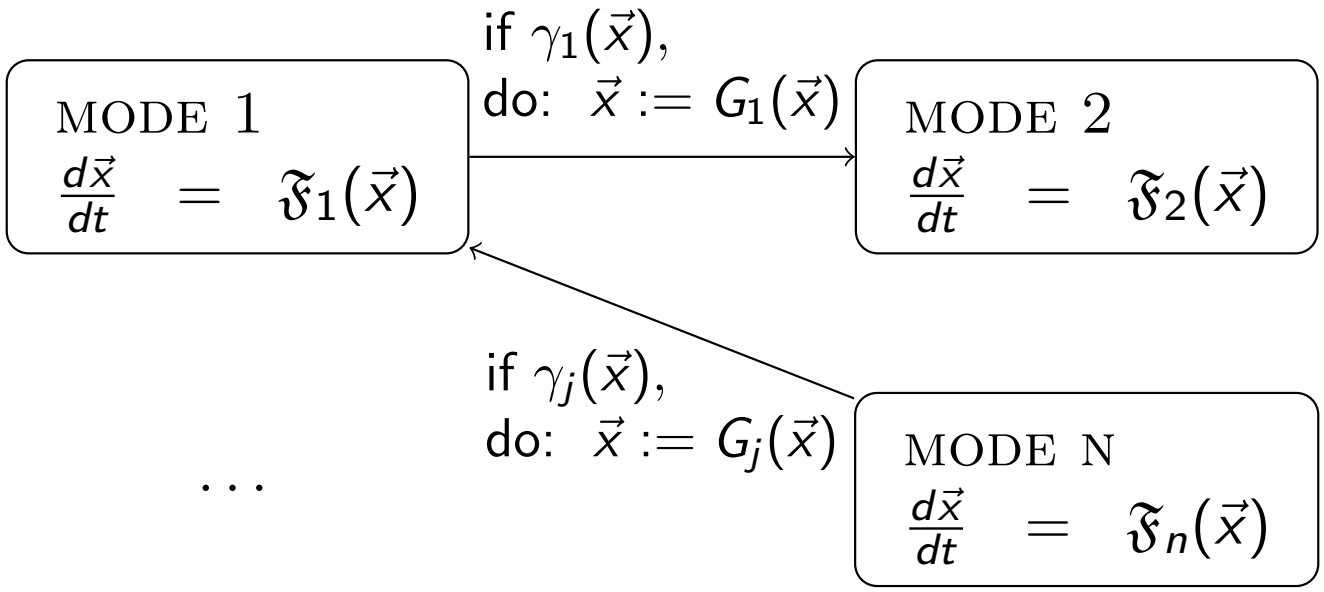




S: Sense, A: Actuate

Hybrid Automaton

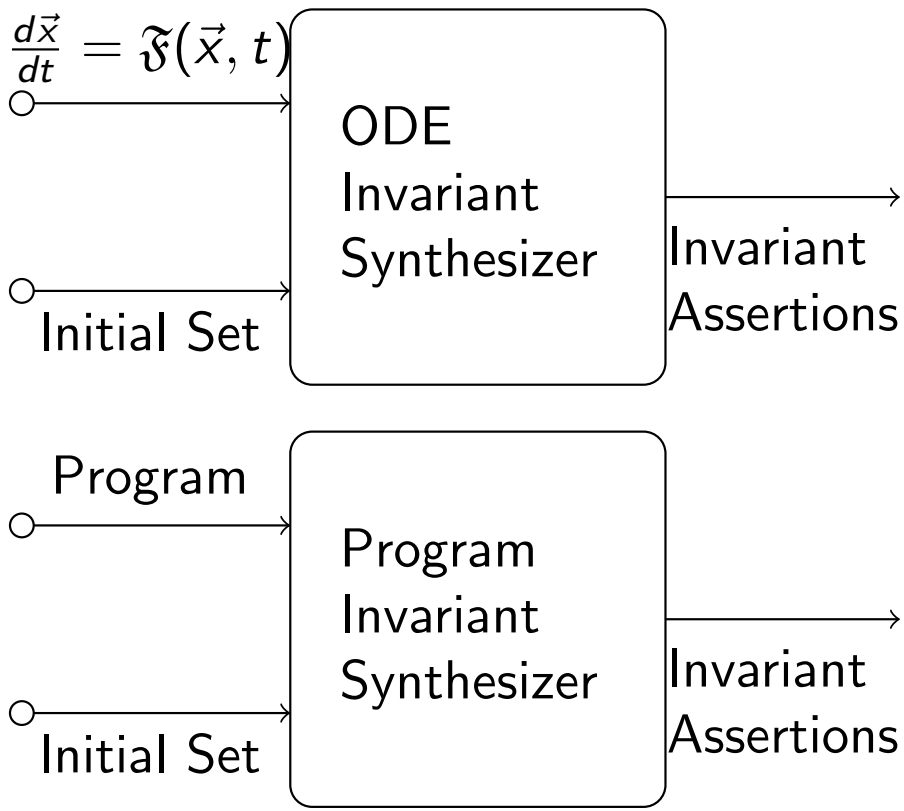
[Alur et al.'96; Sastry et al. '98]



- Finite set of *modes*. $Q : \{q_1, \ldots, q_N\}$
- Continuous state variables. $\vec{x} : (x_1, \ldots, x_n)$.
- Dynamics for each mode.
- Discrete Transitions between modes.

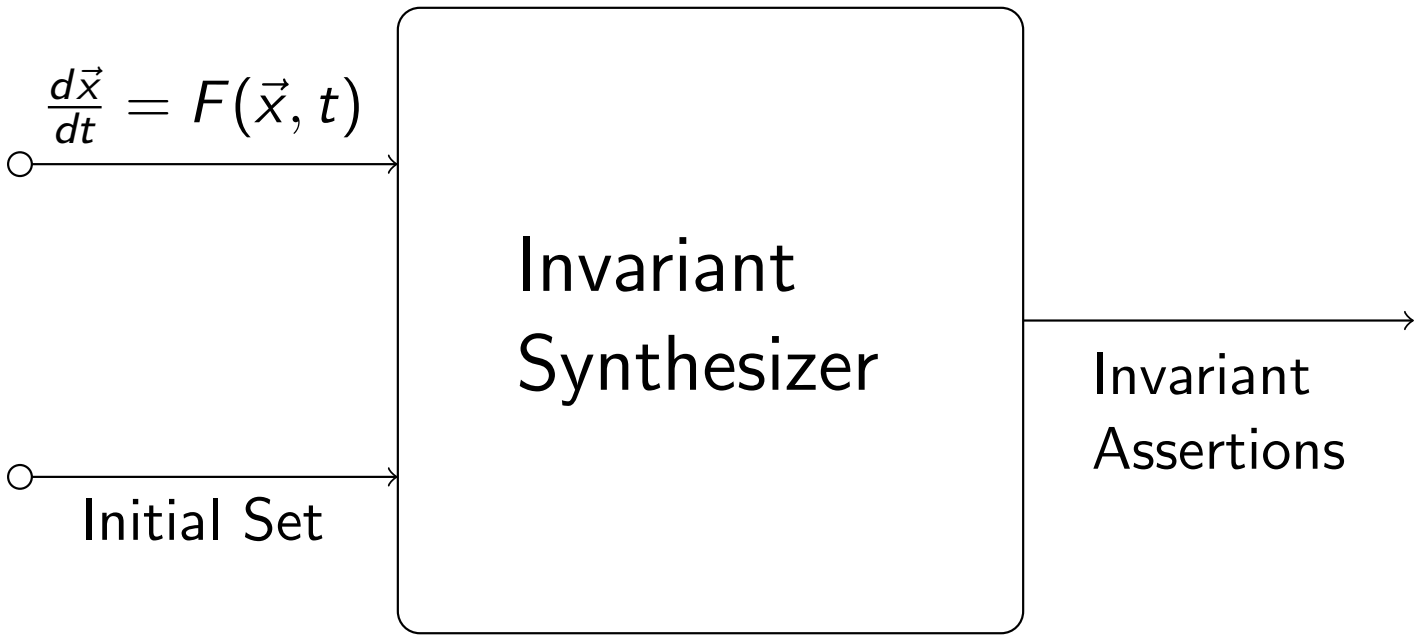
Invariant Synthesis for Hybrid Systems

Goal: Combine invariant synthesis for discrete and continuous subsystems.

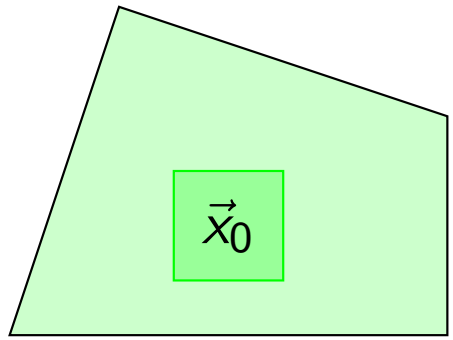


Challenge: Invariants *for Differential Equations*.

Invariant Synthesis for ODEs



Affine ODEs: Polyhedral Invariant Generation.



Affine dynamics:

$$\frac{d\vec{x}}{dt} = A\vec{x} + \vec{b}\,.$$

- Polyhedra [Halbwachs'94, Henzinger et al.'96, Sank.et al.'06]
- Zonotopes. [Girard'05]
- (Linear) Support Functions. [Girard'09,'10]
- Templatized Polyhedra. [Sank.et al.'08,'09]

- Tools: PHaver, Mattisse, TimePass,...

Non-Linear ODE

Algebraic ODE:

$$\frac{d\vec{x}}{dt} = p(\vec{x}, t)$$

p is a polynomial over the variables in $\vec{x}$ and time t.

Initial condition:

$$q_1(\vec{x}) = 0 \ \wedge \ q_2(\vec{x}) = 0 \ \wedge \ \cdots \wedge \ q_m(\vec{x}) = 0\,.$$

Goal: Algebraic invariants.

$$p_1(\vec{x}) = 0 \ \wedge \ \cdots \ \wedge \ p_m(\vec{x}) = 0$$

Example: Hamiltonian System

$$\begin{array}{rclrcl} \frac{dp_1}{dt} & = & -2q_1q_2^2 & \frac{dq_1}{dt} & = & 2p_1, \\ \frac{dp_2}{dt} & = & -2q_1^2q_2 & \frac{dq_2}{dt} & = & 2p_2 \end{array}$$

$$V_0 = \{(p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q_1^2 - 1 = 0, q_2 = 0\}$$

Claim Invariant: $p_1^2 + p_2^2 + q_1^2q_2^2 = 4$.

Example: Hamiltonian System

$$\begin{array}{lcllcl} \frac{dp_1}{dt} & = & -2q_1q_2^2 & \frac{dq_1}{dt} & = & 2p_1, \\ \frac{dp_2}{dt} & = & -2q_1^2q_2 & \frac{dq_2}{dt} & = & 2p_2 \end{array}$$

$$V_0 = \{(p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q_1^2 - 1 = 0, q_2 = 0\}$$

Claim Invariant: $p_1^2 + p_2^2 + q_1^2q_2^2 = 4$.

1. Initial conditions satisfy invariant:

$$(p_1^2 + p_2^2 - 4 = 0,\ q_1^2 - 1 = 0, q_2 = 0) \models p_1^2 + p_2^2 + q_1^2q_2^2 = 4\,.$$

Example: Hamiltonian System

$$\begin{array}{lcllcl} \frac{dp_1}{dt} & = & -2q_1q_2^2 & \frac{dq_1}{dt} & = & 2p_1, \\ \frac{dp_2}{dt} & = & -2q_1^2q_2 & \frac{dq_2}{dt} & = & 2p_2 \end{array}$$

$$V_0 = \{(p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q_1^2 - 1 = 0, q_2 = 0\}$$

Claim Invariant: $p_1^2 + p_2^2 + q_1^2q_2^2 = 4$.

1. Initial conditions satisfy invariant:

$$(p_1^2 + p_2^2 - 4 = 0,\ q_1^2 - 1 = 0, q_2 = 0) \models p_1^2 + p_2^2 + q_1^2q_2^2 = 4\,.$$

2. Lie derivative vanishes (zero everywhere):

$$\begin{array}{lcl} \frac{d(p_1^2+p_2^2+q_1^2q_2^2-4)}{dt} & = & 2p_1(\frac{dp_1}{dt}) + 2p_2(\frac{dp_2}{dt}) + 2q_1q_2^2(\frac{dq_1}{dt}) + 2q_2q_1^2(\frac{dq_2}{dt}) \\ & = & 0 \end{array}$$

Example: Hamiltonian System

$$\begin{aligned}
\frac{dp_1}{dt} &= -2q_1q_2^2, \\
\frac{dp_2}{dt} &= -2q_1^2q_2, \\
\frac{dq_1}{dt} &= 2p_1, \\
\frac{dq_2}{dt} &= 2p_2
\end{aligned}$$

Initial condition:

$$V_0 : \{(p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q^2 - 1 = 0, q_2 = 0\}.$$

Invariant: $p_1^2 + p_2^2 + q_1^2q_2^2 = 4$.

Challenge: How do we discover invariants like this?

without assuming special structure on ODEs.

Using an Ansatz

Ansatz: Polynomial with unknown coefficients.

$$\underline{a_1} p_1^2 + \underline{a_2} p_2^2 + \underline{a_3} p_1 p_2 + \underline{a_4} p_1 + \underline{a_5} p_2 + \underline{a_6} = 0$$

Goal: Discover values of $a_1, \ldots, a_6$ s.t. the ansatz is an invariant.

Approach: Encode invariance of ansatz into
system of constraints over $a_1, \ldots, a_6$.

Encoding Invariance

1. Initial Conditions:

$$\underbrace{\left(\begin{array}{l} p_1^2 + p_2^2 - 4 = 0, \\ q^2 - 1 = 0, \\ q_2 = 0 \end{array}\right)}_{\text{Initial}} \models \underbrace{a_1 p_1^2 + a_2 p_2^2 + \cdots + a_6 = 0}_{\text{Ansatz}}.$$

2. Invariance:

$$\underbrace{\frac{d(a_1 p_1^2 + a_2 p_2^2 + a_3 p_1 p_2 + a_4 p_1 + a_5 p_2 + a_6)}{dt}}_{\text{Lie Derivative}} = 0$$

3. Detailed approach: [Sank.+Sipma+Manna'04,'08]
   - Use elementary computational algebraic techniques.
   - Derive linear equations involving $a_1, \ldots, a_6$.

Example

$$\begin{aligned} \frac{dp_1}{dt} &= -2q_1q_2^2, \\ \frac{dp_2}{dt} &= -2q_1^2q_2, \\ \frac{dq_1}{dt} &= 2p_1, \\ \frac{dq_2}{dt} &= 2p_2 \end{aligned}$$

Initial condition:

$$V_0 : \{\vec{x} : (p_1, q_1, p_2, q_2) \mid p_1^2 + p_2^2 - 4 = 0,\ q^2 - 1 = 0, q_2 = 0\}\,.$$

Ansatz: generic degree 4 polynomial 126 unknowns.

Invariant found with ansatz:

$$p_1^2 + p_2^2 + q_1^2q_2^2 = 4\,.$$

Simple Invariant Discovery

Challenge # 1: Size of ansatz can be large.

$$\left[\begin{array}{r} \#\text{ variables } = n, \\ \text{degree } = d \end{array}\right] \Rightarrow \text{ ansatz has } \binom{n+d}{d} \text{ unknowns}.$$

Solution: Ansatz discovery technique (prune monomials).

Simple Invariant Discovery

Challenge # 1: Size of ansatz can be large.

$$\left[\begin{array}{r} \#\text{ variables } = n, \\ \text{degree } = d \end{array}\right] \Rightarrow \text{ ansatz has } \binom{n+d}{d} \text{ unknowns}.$$

Solution: Ansatz discovery technique (prune monomials).

Challenge #2: No invariant exists

1. Satisfying $\frac{dp}{dt} = 0$ and
2. Fitting ansatz.

Solution: More sophisticated invariance rules.

Our Approach

1. A series of invariance principles:
   - "Standard" Invariant: $\frac{dp}{dt} = 0$.
   - Constant Scale Invariant: $\frac{dp}{dt} = \lambda p,\ \lambda \in \mathbb{R}$.
   - Polynomial Scale Invariant: $\frac{dp}{dt} = gp,\ g \in \mathbb{R}[\vec{x}]$.
   - Invariant ideal: $\frac{dp_i}{dt} = \sum_{j=1}^{n} g_{ij} p_i,\ i \in [1, n]$.

2. "Ansatz-Free" methods: Using computer algebra.

Constant Scale Invariant

Polynomial $p = 0$ is constant scale invariant iff

1. Initial condition entailment:

$$\vec{x} \in V_0 \models p(\vec{x}) = 0$$

2. Constant scale rule:

$$(\exists\, \lambda \in \mathbb{R})\ \frac{dp}{dt} = \lambda p\,.$$

Example # 2

$$\begin{aligned} \frac{dx}{dt} &= 2xy^2 - 3x + 2y \\ \frac{dy}{dt} &= 2x^2y + 3y + 2x \end{aligned}$$

We can prove that $p = x^2 - y^2 = 0$ is a constant scale.

$$\frac{d(x^2 - y^2)}{dt} = -6(x^2 - y^2)$$

Note: $(x^2 - y^2)e^{-6t}$ satisfies standard invariance condition.

Constant Scale Invariant

1. Const. scale $p = 0 \quad \Rightarrow \quad$ all trajectories satisfy $p = 0$.
2. Const. scale $p = 0 \quad \Rightarrow \quad pe^{-\lambda t}$ is a (standard) invariant.

Constant Scale Invariant

1. Const. scale $p = 0 \quad \Rightarrow \quad$ all trajectories satisfy $p = 0$.

2. Const. scale $p = 0 \quad \Rightarrow \quad pe^{-\lambda t}$ is a (standard) invariant.

Advantage: However, $e^{-\lambda t}$ is not needed in the Ansatz.

Constant Scale Invariant

1. Const. scale $p = 0 \quad \Rightarrow$ all trajectories satisfy $p = 0$.

2. Const. scale $p = 0 \quad \Rightarrow \quad pe^{-\lambda t}$ is a (standard) invariant.

Advantage: However, $e^{-\lambda t}$ is not needed in the Ansatz.

Invariant Synthesis: Two possible approaches.

1. Ansatz-based approach yields non-square eigenvalue problems. [Sank.+Sipma+Manna'04,'08]
2. Generalization using vector-space approaches. [Sank.'11]

Polynomial Scale Invariant

Polynomial $p = 0$ is constant scale invariant iff

1. Initial condition entailment:

$$\vec{x} \in V_0 \models p(\vec{x}) = 0$$

2. Polynomial scale:

$$(\exists g \in \mathbb{R}[\vec{x}]) \frac{dp}{dt} = gp\,.$$

Lie derivative of p scaled by polynomial factor.

Example: Polynomial Scale

$$\begin{aligned} \frac{dx}{dt} &= y^2 + 3x \\ \frac{dy}{dt} &= x^2 + 3y \end{aligned}$$

Consider $p = x - y$:

$$\frac{dp}{dt} = \frac{d(x-y)}{dt} = (y + x + 3)(x - y) = gp$$

Conclusion: $x = y$ is a (polynomial scale) invariant of the ODE.

Polynomial Scale: Properties

1. Poly. scale $p = 0 \quad \Rightarrow \quad$ all trajectories satisfy $p = 0$.
2. Poly. scale $p = 0 \quad \Rightarrow \quad f(\vec{x}, t) = 0$ (standard) invariant.

Polynomial Scale: Properties

1. Poly. scale $p = 0 \quad \Rightarrow$ all trajectories satisfy $p = 0$.

2. Poly. scale $p = 0 \quad \Rightarrow \quad f(\vec{x}, t) = 0$ (standard) invariant.

Advantage: However, f may not be known in a closed form.

Polynomial Scale: Properties

1. Poly. scale $p = 0 \quad \Rightarrow$ all trajectories satisfy $p = 0$.

2. Poly. scale $p = 0 \quad \Rightarrow \quad f(\vec{x}, t) = 0$ (standard) invariant.

Advantage: However, f may not be known in a closed form.

Invariant Synthesis:

1. Ansatz-based approach using morphisms. [Matringe+Others'09]
2. Generalization using ideal fixed points. [Sank.'10]

Further Generalization

Thus far, single polynomial invariant $p = 0$.

$$\frac{dp}{dt} = g \cdot p$$

Generalization: $k > 0$ polynomials $p_1, \ldots, p_k$.

$$\begin{aligned} \frac{dp_1}{dt} &= g_{11}p_1 + g_{12}p_2 + \cdots + g_{1k}p_k \\ &\vdots \\ \frac{dp_k}{dt} &= g_{k1}p_1 + g_{k2}p_2 + \cdots + g_{kk}p_k \end{aligned}$$

Further Generalization

Thus far, single polynomial invariant $p = 0$.

$$\frac{dp}{dt} = g \cdot p$$

Generalization: $k > 0$ polynomials $p_1, \ldots, p_k$.

$$\begin{aligned} \frac{dp_1}{dt} &= g_{11}p_1 + g_{12}p_2 + \cdots + g_{1k}p_k \\ &\vdots \\ \frac{dp_k}{dt} &= g_{k1}p_1 + g_{k2}p_2 + \cdots + g_{kk}p_k \end{aligned}$$

Result: If initially $p_1(0) = \cdots = p_k(0) = 0$ then

$$(\forall\ t)p_1(t) = \cdots = p_k(t) = 0\,.$$

Further Generalization

Generalization: $k > 0$ polynomials $p_1, \ldots, p_k$.

$$\begin{aligned} \frac{dp_1}{dt} &= g_{11}p_1 + g_{12}p_2 + \cdots + g_{1k}p_k \\ &\vdots \\ \frac{dp_k}{dt} &= g_{k1}p_1 + g_{k2}p_2 + \cdots + g_{kk}p_k \end{aligned}$$

Challenge: Synthesize invariants of form above.

1. k is not known *a priori*.
2. Need ansatz for $p_1, \ldots, p_k$ and $g_{11}, \ldots, g_{k1}$.
3. Constraints on unknowns are non-linear.

Further Generalization

Generalization: $k > 0$ polynomials $p_1, \ldots, p_k$.

$$\begin{aligned} \frac{dp_1}{dt} &= g_{11}p_1 + g_{12}p_2 + \cdots + g_{1k}p_k \\ &\vdots \\ \frac{dp_k}{dt} &= g_{k1}p_1 + g_{k2}p_2 + \cdots + g_{kk}p_k \end{aligned}$$

Challenge: Synthesize invariants of form above.

1. k is not known *a priori*.
2. Need ansatz for $p_1, \ldots, p_k$ and $g_{11}, \ldots, g_{k1}$.
3. Constraints on unknowns are non-linear.

Contribution: Ansatz-free technique.

Ansatz-Free Synthesis of Invariants

Basic Ideas: Invariants = fixed point of monotone operator over lattice of ideals in polynomial ring.

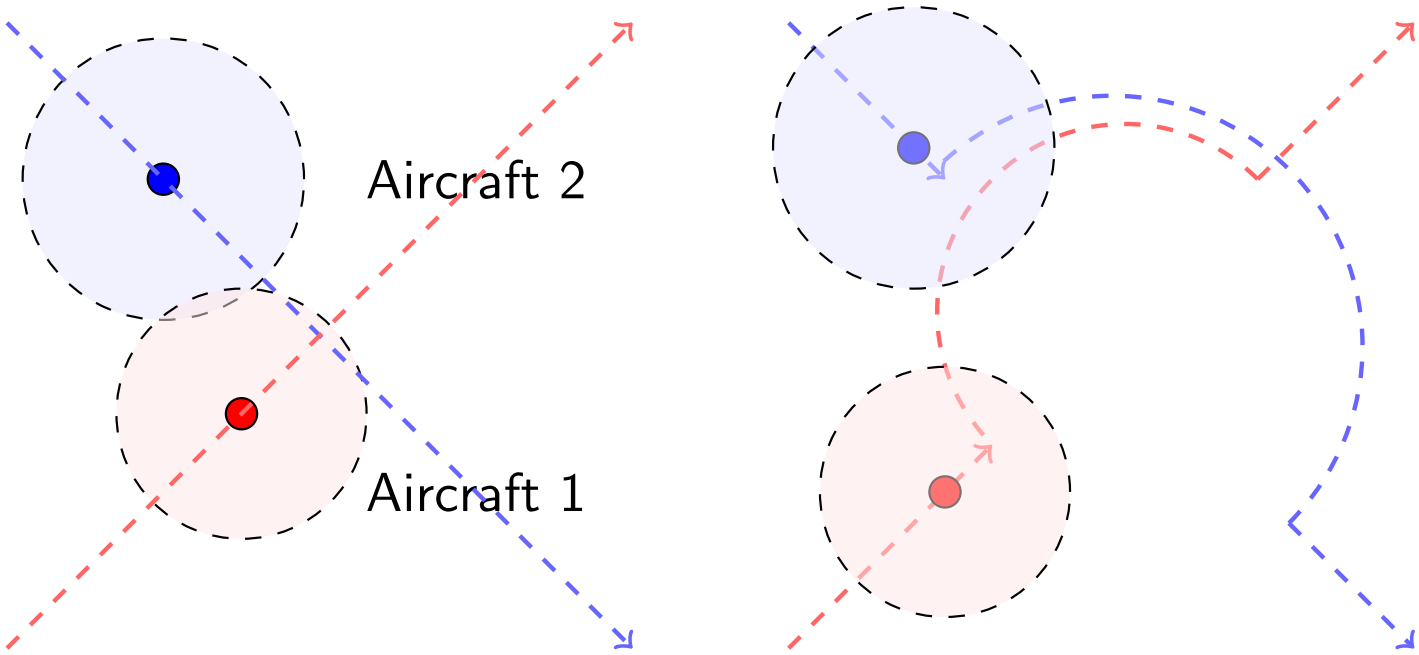
1. Construct monotone operator over polynomial ideals.
2. Construction realized using standard algebra operations.
3. Iterative fixed point computation procedure.
4. Force convergence by embedding inside a vector space.

Tedious Details:

Sank., *Automatic Invariant Generation for Algebraic Systems using Ideal Fixed Points*, Hybrid Systems: Computation and Control, 2010 (journal version under preparation)

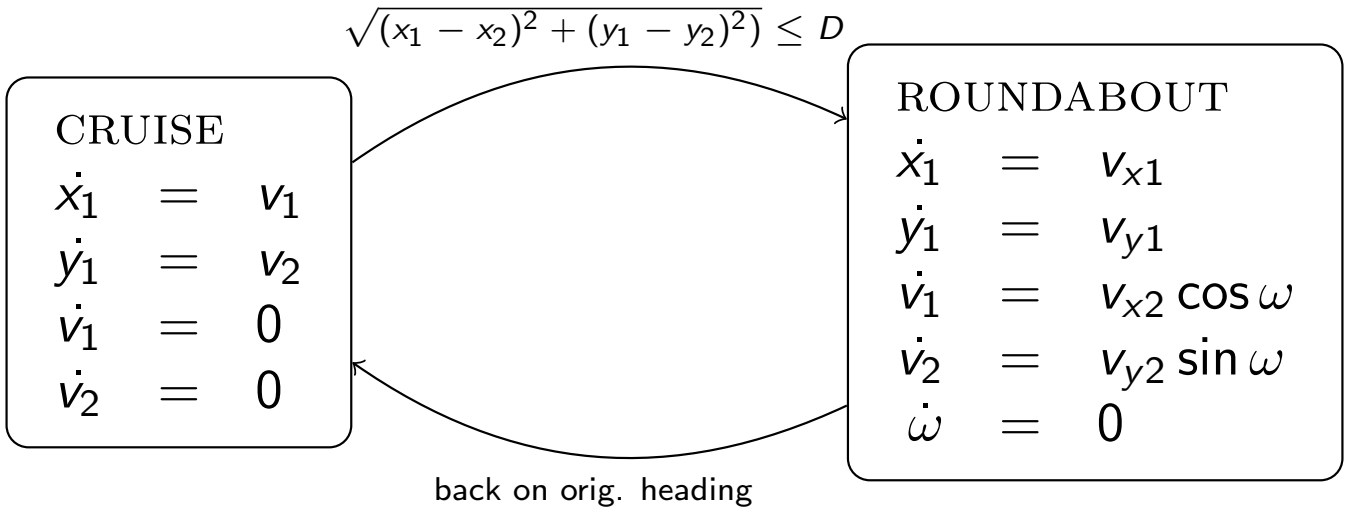
Application: Conflict Resolution Maneuvers

Conflict resolution protocol. [Tomlin et al.'98, Platzer et al.'09]



Collision Avoidance Model

Hybrid automaton for each aircraft:



Aircraft Collision Avoidance

Vector Field:

$$\begin{array}{cccc} x_1' = d_1 & x_2' = d_2 & d_1' = -\omega d_2 & d_2' = \omega d_1 \\ y_1' = e_1 & y_2' = e_2 & e_1' = -\theta e_2 & e_2' = \theta e_1 \\ a' = 0 & b' = 0 & r_1' = 0 & r_2' = 0 \end{array}$$

Initial set

$$\left[\begin{array}{c} x_1 = y_1 = r_1 \ \wedge \ x_2 = y_2 = r_2 \ \wedge \ d_1 = a \ \wedge \\ d_2 = 0 \ \wedge \ e_1 = b \ \wedge \ e_2 = 0 \end{array} \right]$$

Collision Avoidance Protocol

Invariant Set Obtained:

$$
\begin{aligned}
\mathbf{p_1} &: \underline{e_1^2 + e_2^2 - b^2}, \\
\mathbf{p_2} &: \underline{d_1^2 + d_2^2 - a^2} \\
\mathbf{p_3} &: e_1 - r_2\theta + \theta y_2, \\
\mathbf{p_4} &: -a + d_1 - r_2\omega + \omega x_2 \\
\mathbf{p_5} &: b - e_2 - r_1\theta + \theta y_1, \\
\mathbf{p_6} &: -br_1 + by_1 + e_1 r_2 - e_1 y_2 - e_2 r_1 + e_2 y_1 \\
\mathbf{p_7} &: br_2 - by_2 - e_1 r_1 + e_1 y_1 - e_2 r_2 + e_2 y_2 \\
\mathbf{p_8} &: -d_2 - r_1\omega + \omega x_1 \\
\mathbf{p_9} &: ad_2 r_2 - ad_2 x_2 + d_1 d_2 r_2 - d_1 d_2 x_2 - r_1 d_2^2 r_1 + d_2^2 x_1 \\
\mathbf{p_{10}} &: ar_1 - ax_1 - d_1 r_1 + d_1 x_1 - d_2 r_2 + d_2 x_2
\end{aligned}
$$

Risk Analysis in Infusion Pumps

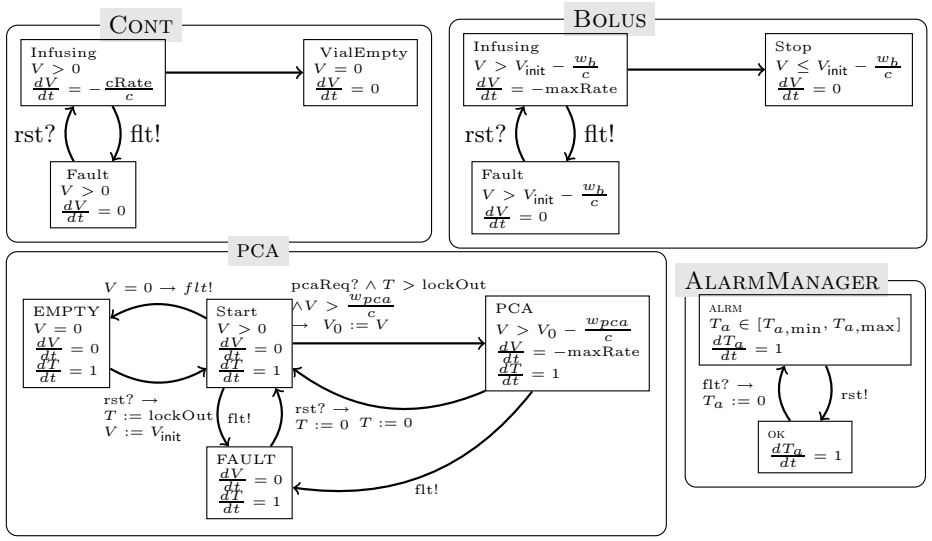


Fig. 3. Pump model for continuous, bolus, PCA infusion modes and the alarm manager component.

Goal: Analyze effect faults during drug infusion.

1. Analgesic infusion pump. [Sank.+Homaei+Lewis'11]
2. Insulin infusion pumps (ongoing).

Ongoing Work

- Polynomial inequality invariants:
  - Refinement over cones of semi-definite (psd) polynomials.
  - Using *sum-of-squares* relaxation and semi-definite programming. [Shor'87, Parillo'03]

Ongoing Work

- Polynomial inequality invariants:
  - Refinement over cones of semi-definite (psd) polynomials.
  - Using *sum-of-squares* relaxation and semi-definite programming. [Shor'87, Parillo'03]
- Study $F-$ related vector fields.
  - Similar to *topological semi-conjugacy*.
  - Algorithm for computing *linearizing maps*.
  - Encouraging results. [Sank.HSCC '11]

Thanks and Questions!

Acknowledgments: Henny Sipma (Kestrel Inst.) and Zohar Manna (Stanford University).

US National Science Foundation.