Invariant-Based Verification and Synthesis for Hybrid Systems

Naijun Zhan

Institute of Software, Chinese Academy of Sciences

(Joint work with Hengjun Zhao, Jiang Liu, Deepak Kapur, Kim G. Larsen, Liang Zou, etc.)

IFIP WG 2.2 Scientific Meeting, IMS, Singapore

Sept. 12-16, 2016

Outline

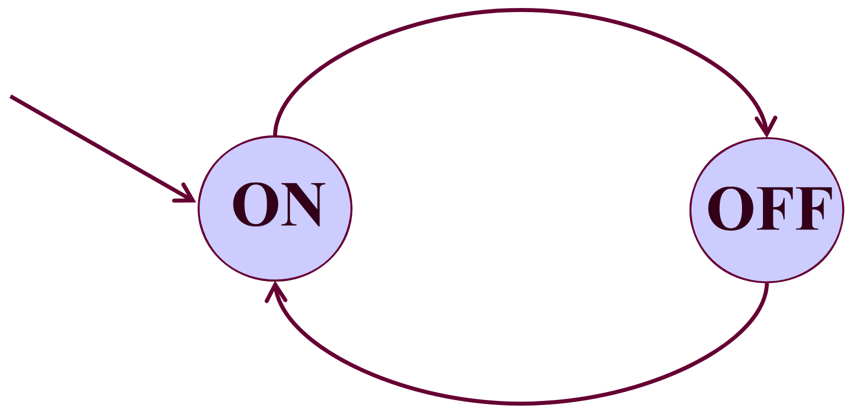
- Background
- Invariant and Verification
- Invariant-Based Synthesis
- Case Studies
- Conclusion

Outline

- **Background**
- **Invariant and Verification**
- **Invariant-Based Synthesis**
- **Case Studies**
- **Conclusion**

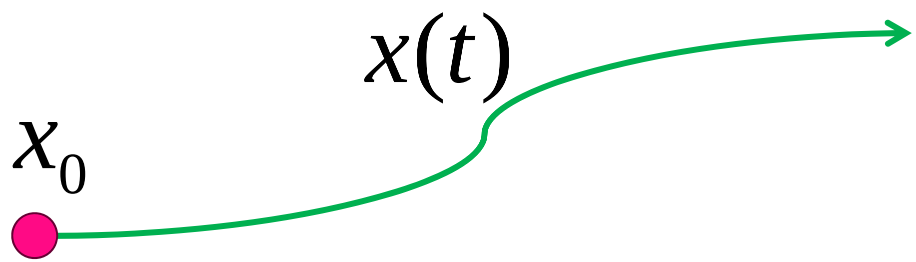
Classification of Dynamical Systems

- **Discrete**



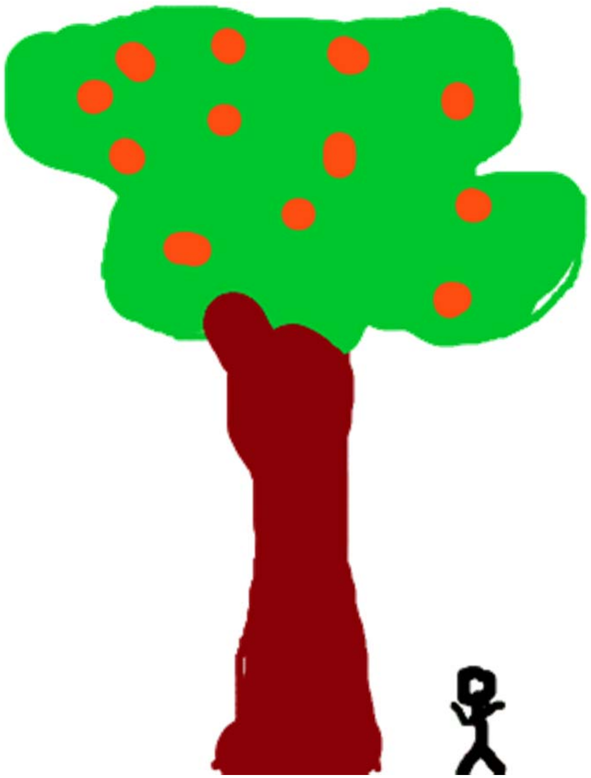
- **Continuous**

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x)$$



Hybrid System

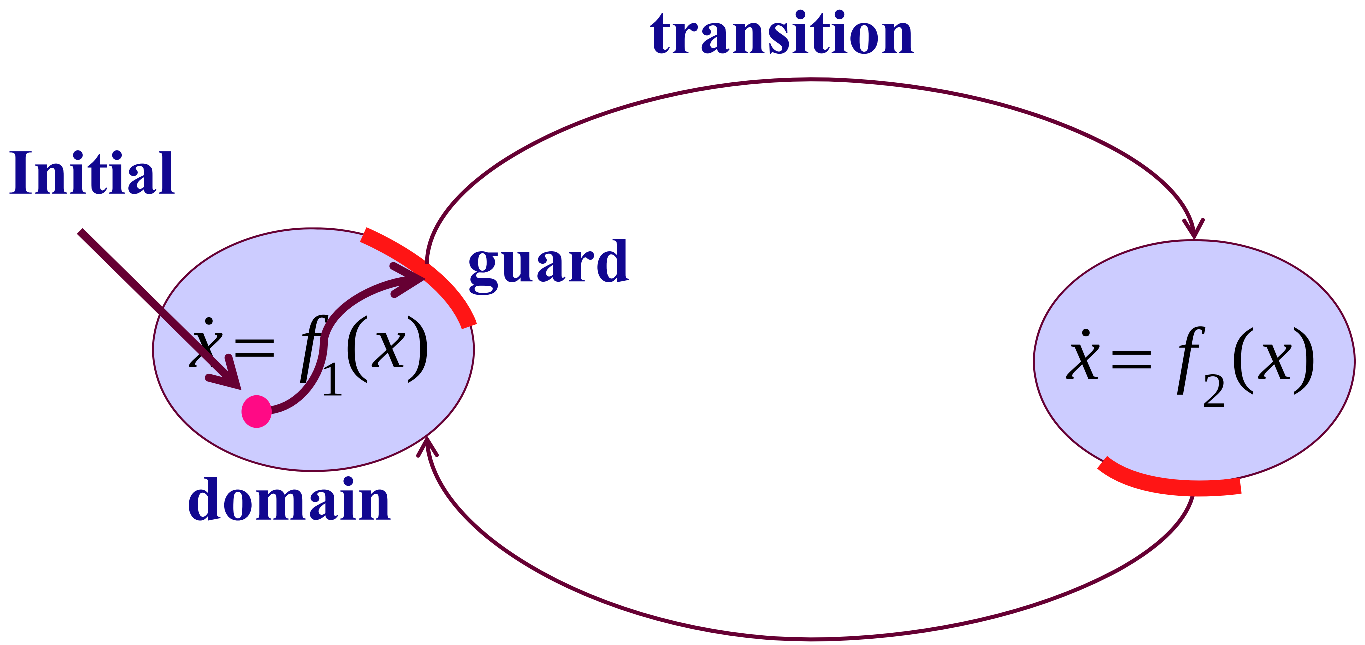
- **Continuous + Discrete**



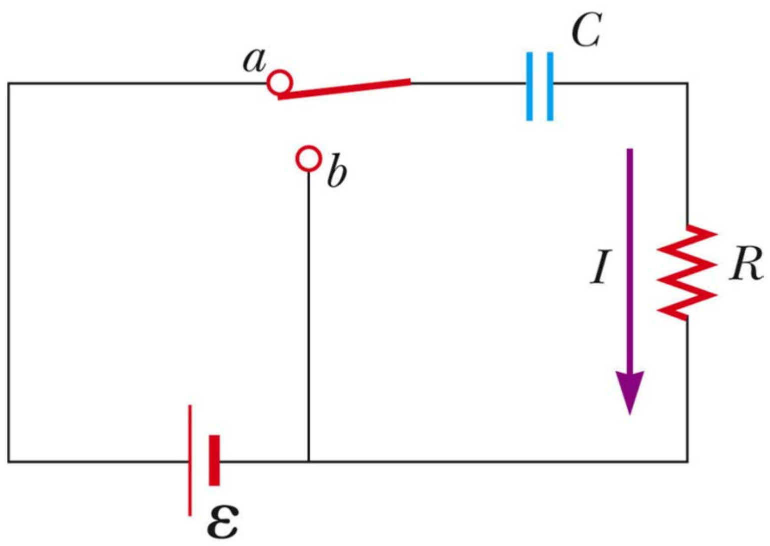
Universal Law of Gravitation

by Heer Rami
http://www.benettonplay.com/toys/flipbookdeluxe/player.php?id=294504

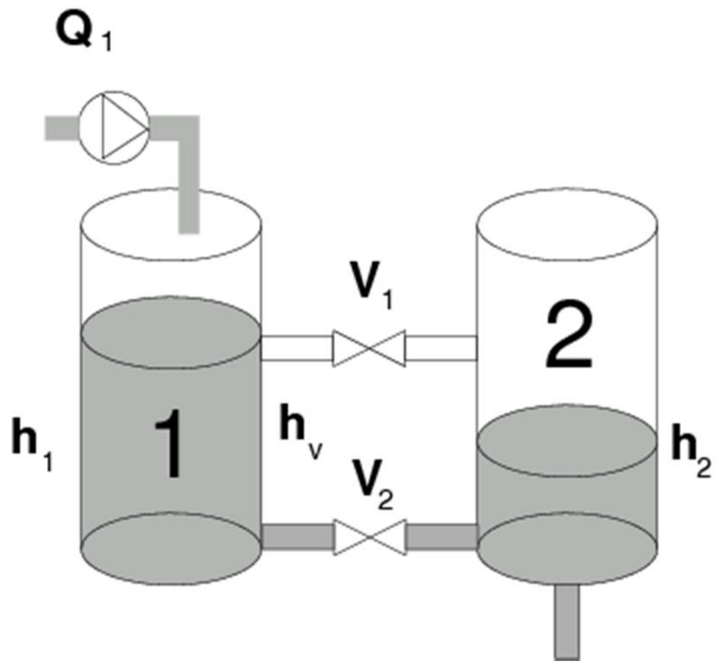
Hybrid Automata



HSs in Engineering



Electrical Circuits



Chemical Process

http://people.ee.ethz.ch/~mpt/2/docs/demos/twotanks.php

Embedded Control Systems

actuator

logic/computation **physical discipline**

sensor

Safety Critical Systems

Motivation

- Develop formal methods for enhancing the trustworthiness of safety critical embedded systems
  - Problems: Verification and Design
  - System Requirements: mainly safety
  - Techniques: symbolic/rigorous computation

Outline

- Background
- **Invariant and Verification**
- Invariant-Based Synthesis
- Case Studies
- Conclusion

Deductive Verification

- **Program**

  x:=1;

  while (x<=1000000000)

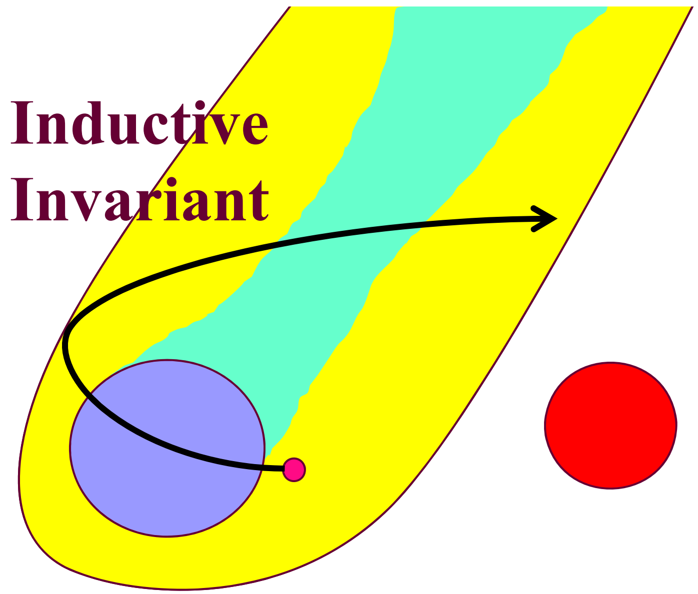
  { x:=x+1; }

  x≦0

- **Inductive Invariant**
  - x=1 ➔ x≧1
  - x≧1 ➔ x+1≧1
  - x≧1 ➔ ¬(x≦0)

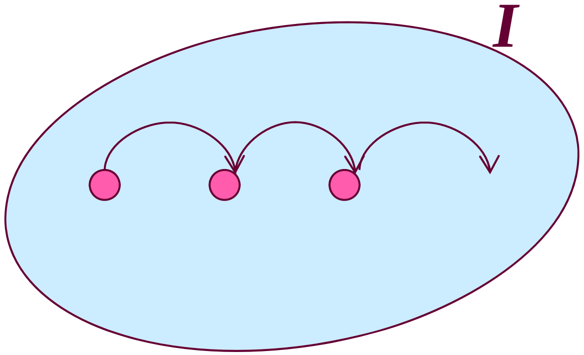
- **Continuous system**

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x)$$



Inductiveness

- **Discrete**



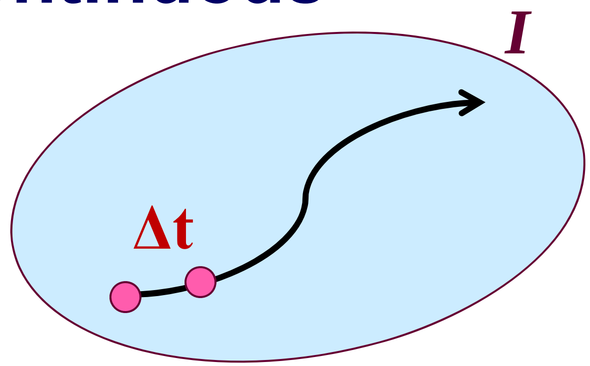
- **Inductiveness**

$$x_k \in I \rightarrow x_{k+1} \in I$$

- **Transition relation**

$$x_{k+1} = \varphi(x_k)$$

- **Continuous**



- **Inductiveness**

$$x(t) \in I \rightarrow x(t + \Delta t) \in I$$

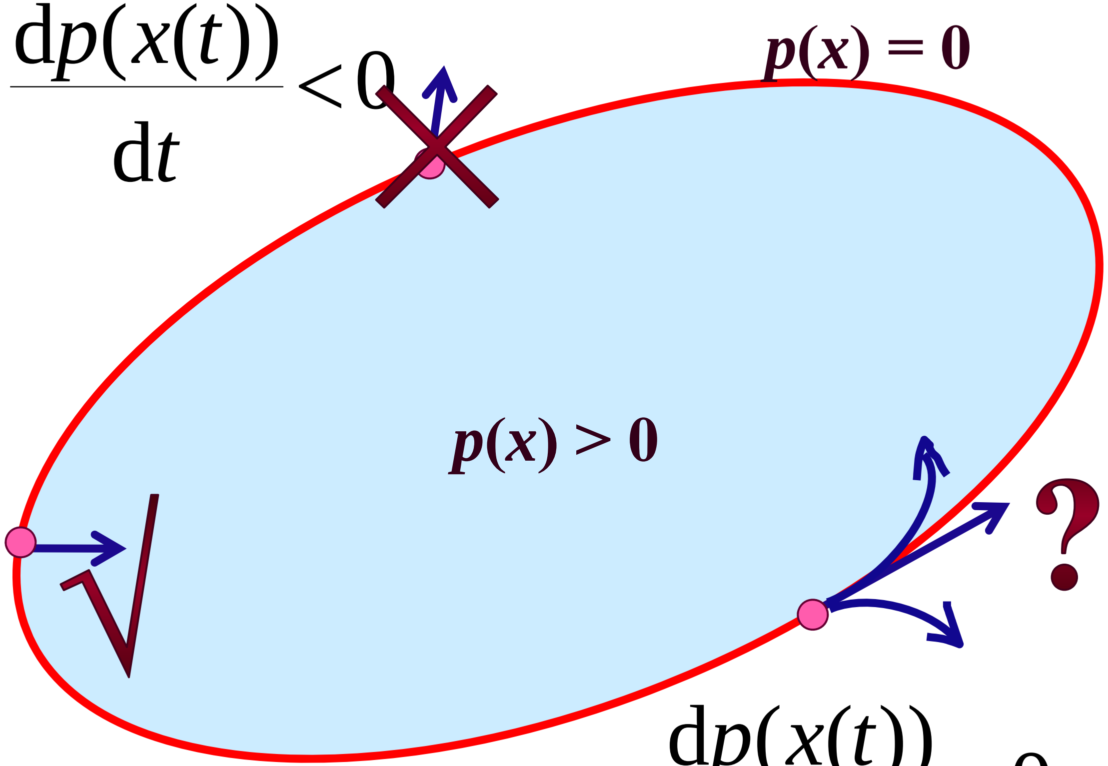
- **Transition relation**

$$x(t + \Delta t) = x(t) + x'(t) \cdot \Delta t$$

Lie Derivatives and Invariant

$$\boxed{\frac{\mathrm{d}x}{\mathrm{d}t} = f(x)}$$

$$\frac{\mathrm{d}p(x(t))}{\mathrm{d}t} < 0$$



$$\frac{\mathrm{d}p(x(t))}{\mathrm{d}t} > 0$$

$$\frac{\mathrm{d}p(x(t))}{\mathrm{d}t} = 0$$

Higher-Order Lie Derivatives

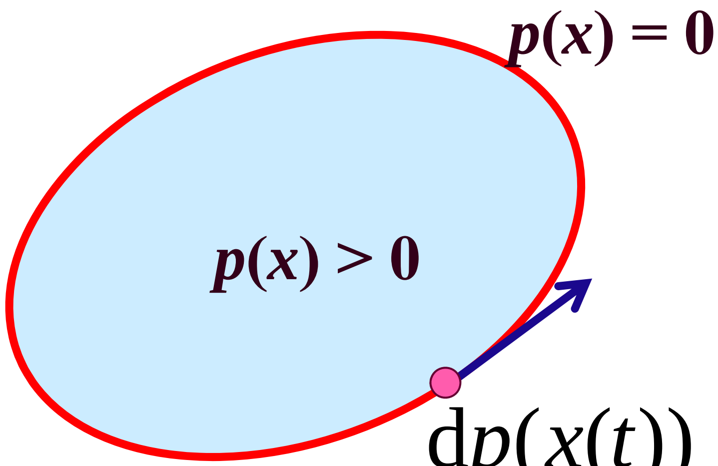
$$\frac{d^1 p}{dt^1} > 0$$

$$\vee \frac{d^1 p}{dt^1} = 0 \wedge \frac{d^2 p}{dt^2} > 0$$

$$\vee \frac{d^1 p}{dt^1} = 0 \wedge \frac{d^2 p}{dt^2} = 0 \wedge \frac{d^3 p}{dt^3} > 0$$

$$\vee \frac{d^1 p}{dt^1} = 0 \wedge \frac{d^2 p}{dt^2} = 0 \wedge \frac{d^3 p}{dt^3} = 0 \wedge \cdots$$

?



$$\frac{dp(x(t))}{dt} = 0$$

Criterion for Invariant

- $f(x)$ and $p(x)$ are polynomials
- Compute an upper bound N s.t.
- $p(x) \geq 0$ is an inductive invariant of $\dfrac{\mathrm{d}x}{\mathrm{d}t} = f(x)$

iff

$$p = 0 \Rightarrow \left(\begin{array}{l} \dfrac{\mathrm{d}^1 p}{\mathrm{d}t^1} > 0 \vee \\ \dfrac{\mathrm{d}^1 p}{\mathrm{d}t^1} = 0 \wedge \dfrac{\mathrm{d}^2 p}{\mathrm{d}t^2} > 0 \vee \\ \cdots \cdots \vee \\ \dfrac{\mathrm{d}^1 p}{\mathrm{d}t^1} = 0 \wedge \dfrac{\mathrm{d}^2 p}{\mathrm{d}t^2} = 0 \wedge \cdots \wedge \dfrac{\mathrm{d}^N p}{\mathrm{d}t^N} \geq 0 \end{array} \right)$$

Main Result

- **Semi-algebraic set**

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} p_{ij}(\mathbf{x}) \triangleright 0, \quad \triangleright \in \{\geq, >\}$$

- **First-order theory of real numbers is decidable**
  - **Quantifier Elimination**

Checking whether a semi-algebraic set is an inductive invariant of a polynomial continuous dynamical systems is decidable

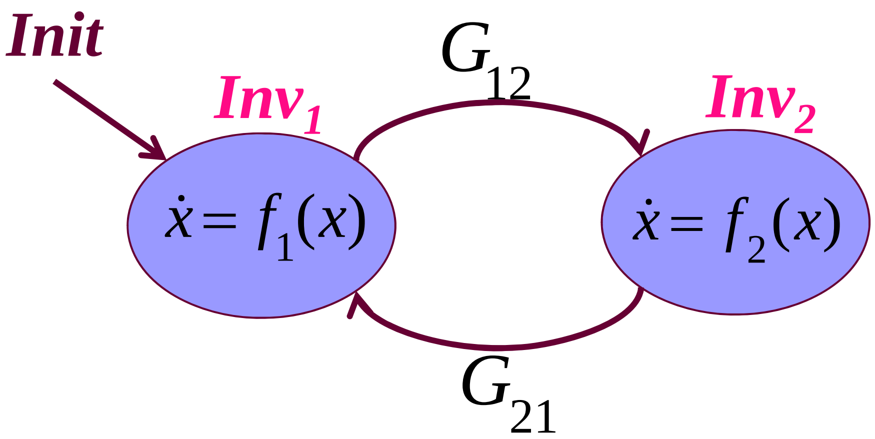
Parametric Case

- **Parametric polynomials *p(u,x)***
- ***p(u,x)* ≥ 0 is an inductive invariant of** $\frac{\mathrm{d}x}{\mathrm{d}t} = f(x)$ **iff *u* satisfies**

$$p(u,x)=0 \Rightarrow \left(\frac{\mathrm{d}^1 p}{\mathrm{d}t^1} > 0 \vee \frac{\mathrm{d}^1 p}{\mathrm{d}t^1} = 0 \wedge \frac{\mathrm{d}^2 p}{\mathrm{d}t^2} > 0 \vee \cdots\cdots \vee \frac{\mathrm{d}^1 p}{\mathrm{d}t^1} = 0 \wedge \frac{\mathrm{d}^2 p}{\mathrm{d}t^2} = 0 \wedge \cdots \wedge \frac{\mathrm{d}^N p}{\mathrm{d}t^N} \geq 0 \right)$$

Use parametric polynomials and quantifier elimination (or other compuation techniques) to automatically discovering inductive invariants

Inductive Invariant of HSs



$$Init \Rightarrow Inv_1$$

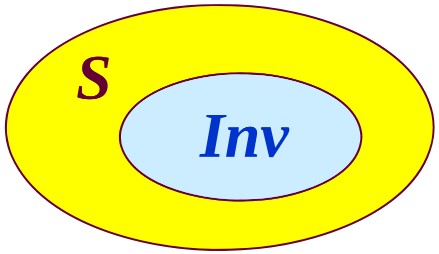
$$Inv_1,\ Inv_2$$

$$Inv_1 \wedge G_{12} \Rightarrow Inv_2$$

$$Inv_2 \wedge G_{21} \Rightarrow Inv_1$$

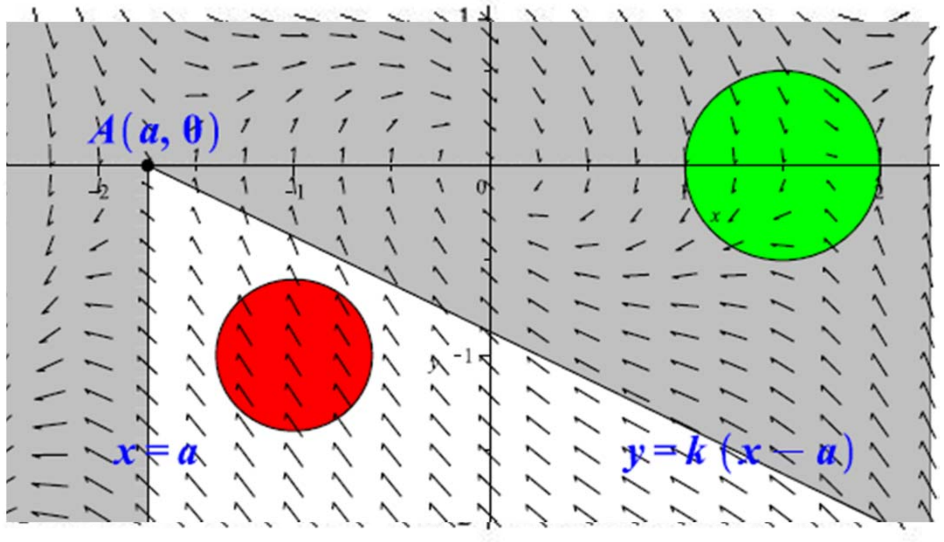
Safety Verification

- **Try to generate an invariant that implies the safety property**



- **Example**

$$\begin{pmatrix}\dot{x}\\ \dot{y}\end{pmatrix} = \begin{pmatrix} y \\ -x + \frac{x^3}{3} - y \end{pmatrix}$$



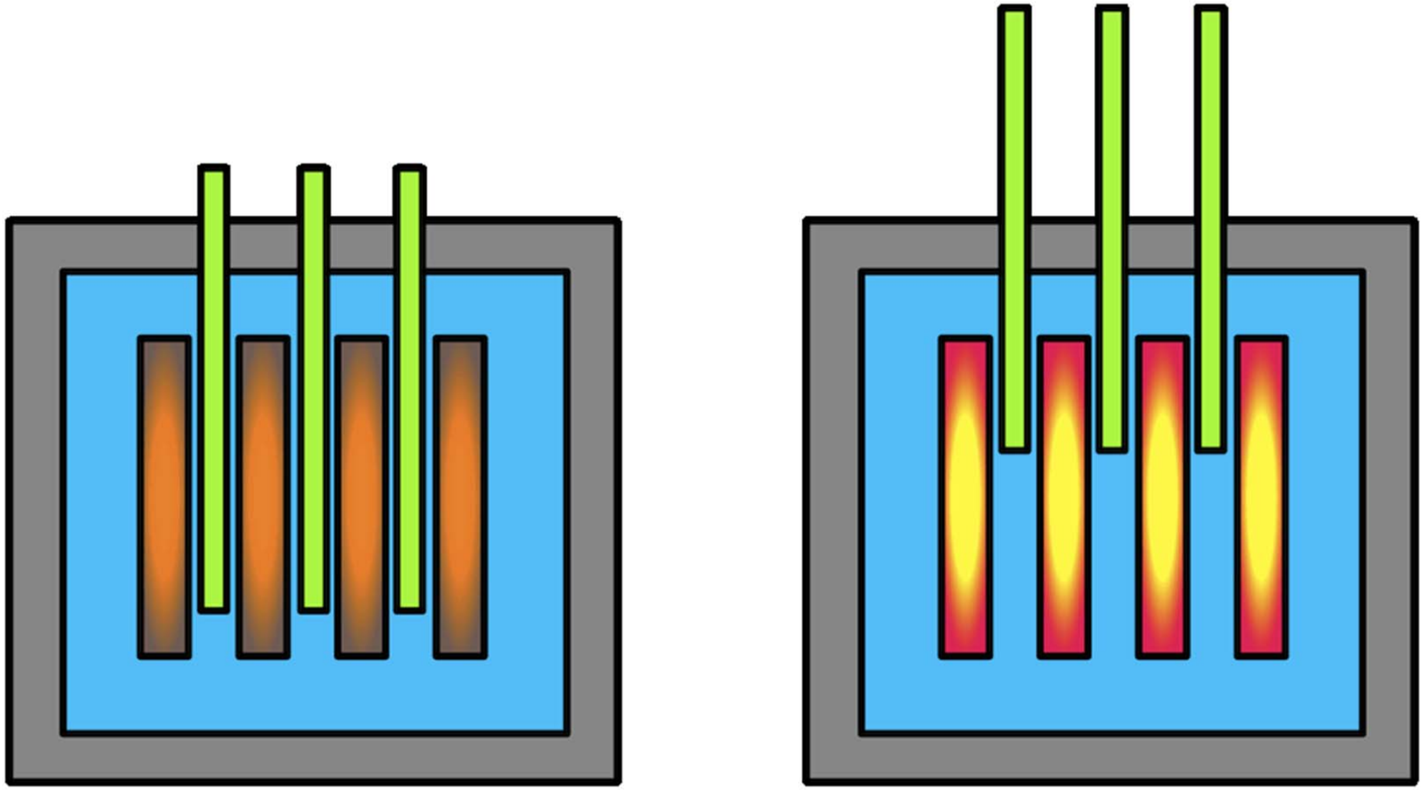
Outline

- Background
- Invariant and Verification
- **Invariant-Based Synthesis**
- Case Studies
- Conclusion

Problem Description

- Given an initial specification of a hybrid system and a safety requirement, construct a refined hybrid system such that the safety requirement is satisfied
  - domains
  - guards

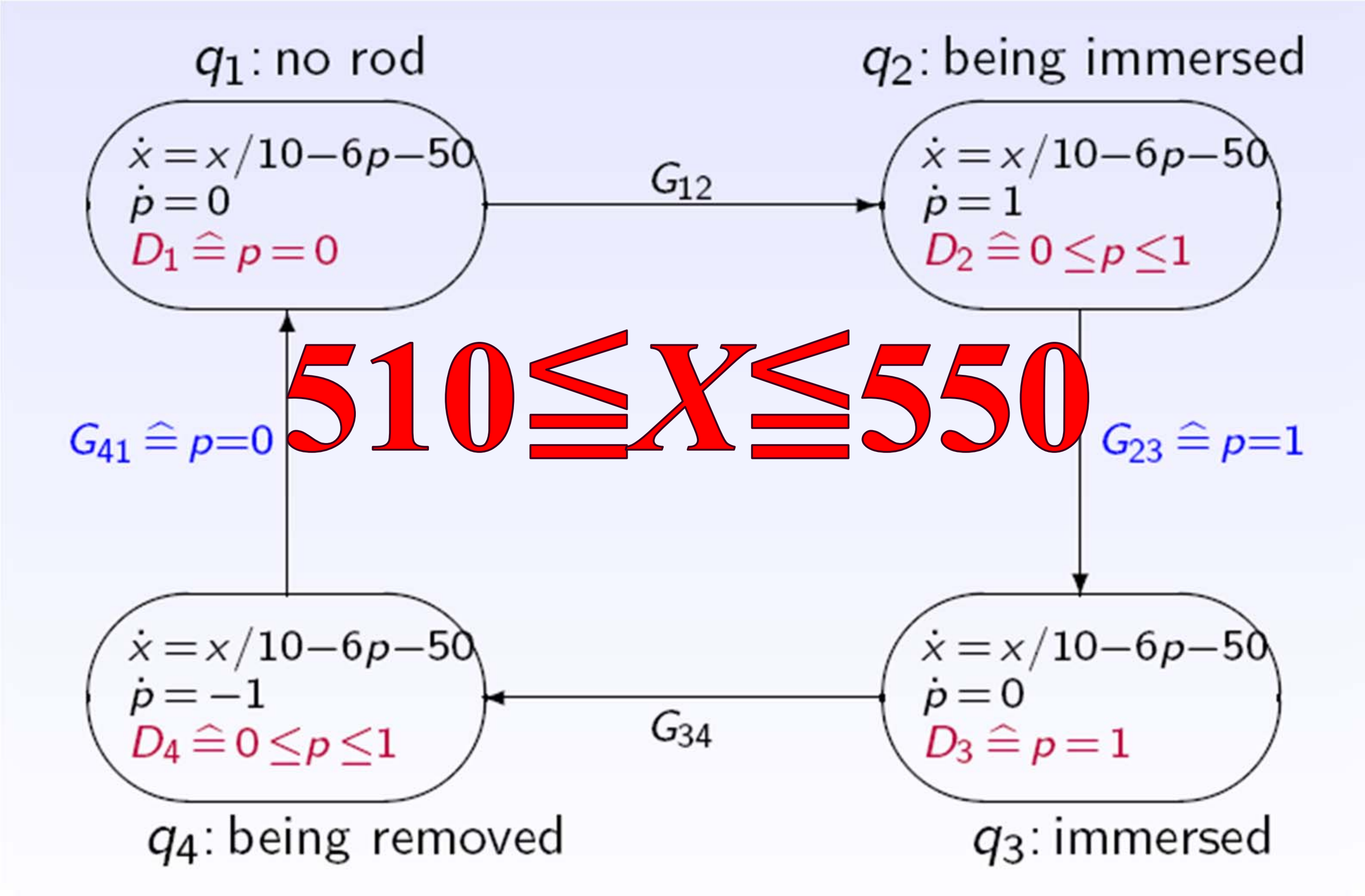
Nuclear Reactor



http://commons.wikimedia.org/wiki/File:Control_rods_schematic.svg

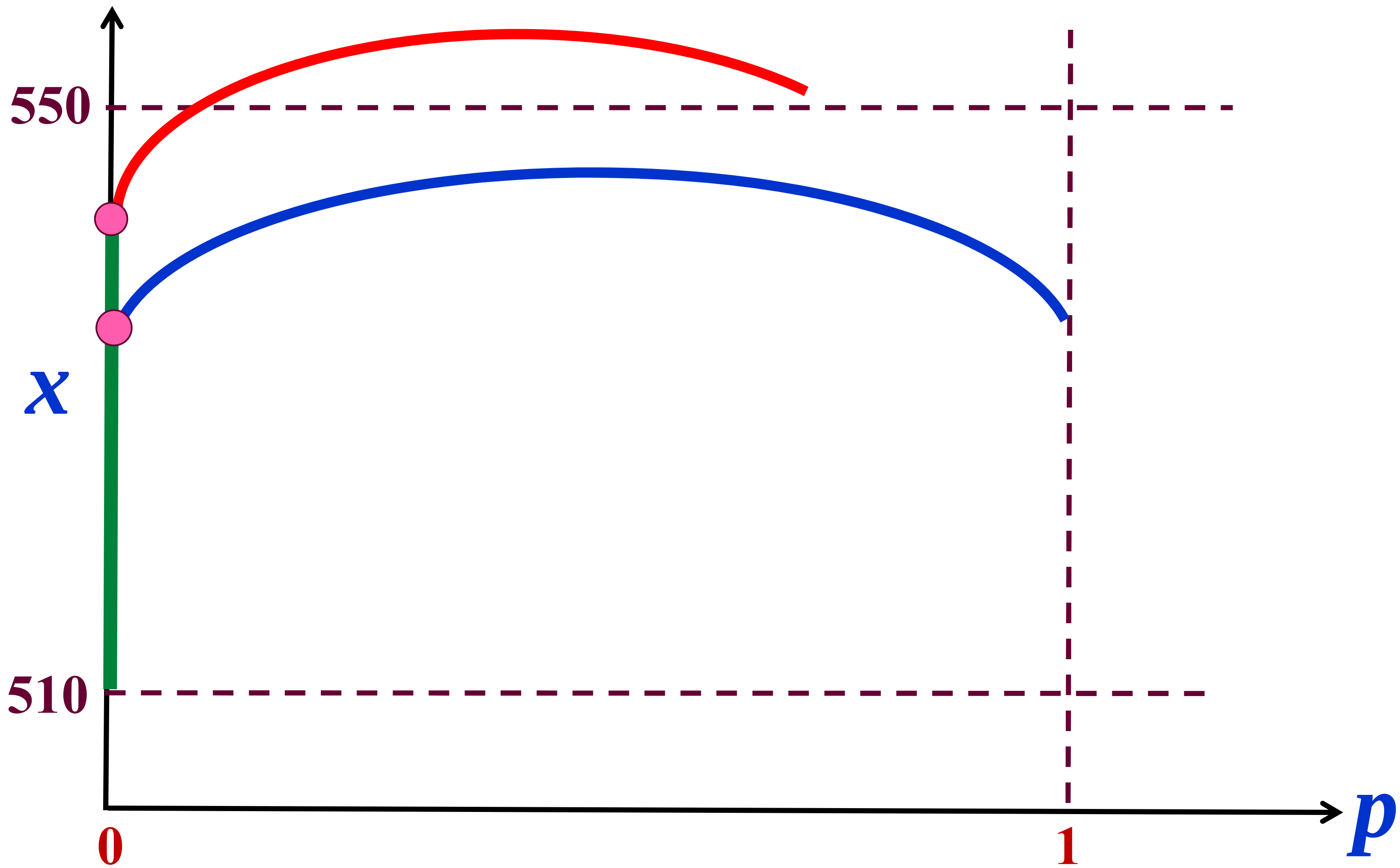
Hybrid Automata Model

- ***x***: **temperature of the reactor**
- ***p***: **fraction of the rod immersed into the reactor**

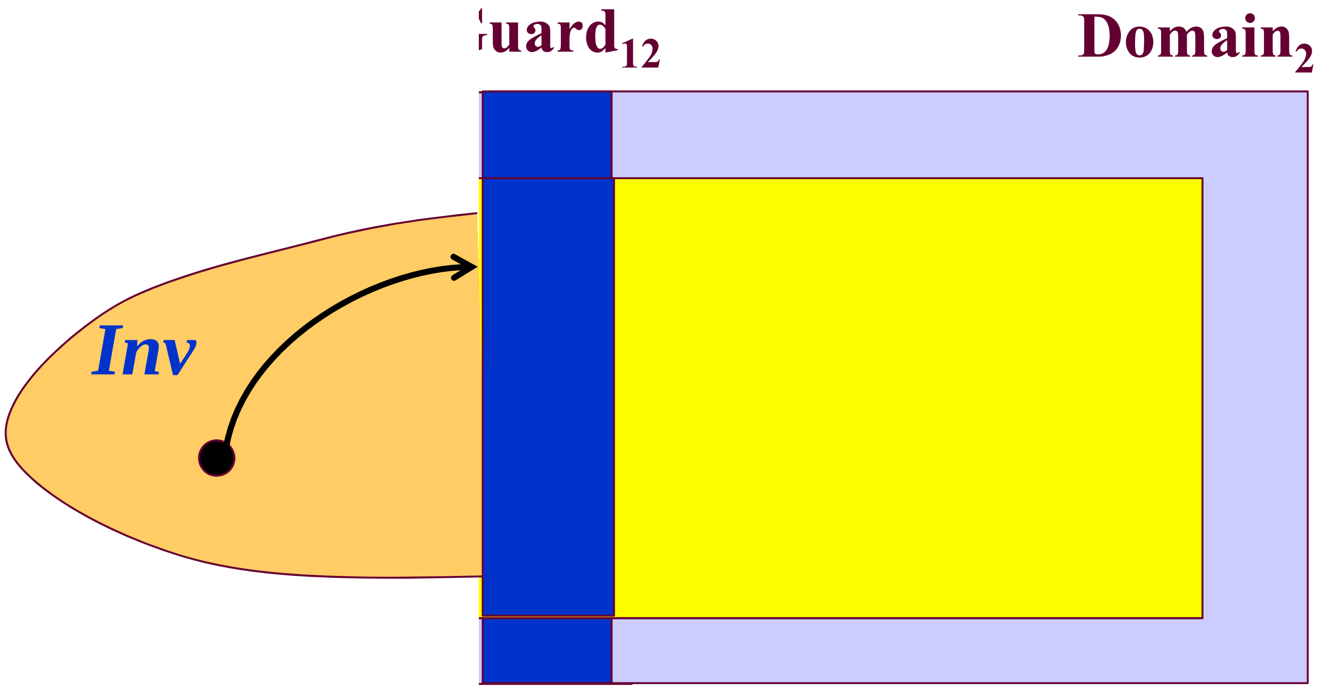


Violation of Safety

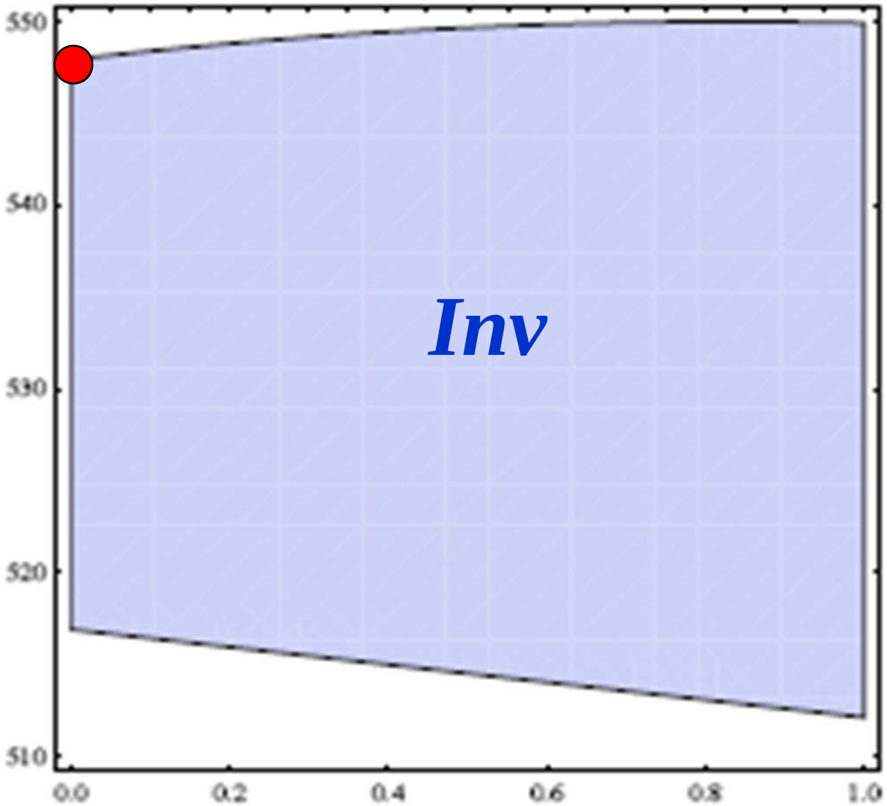
- 510≦x≦550



Invariant for Refinement



Result



$$x \le \frac{6575}{12} \approx 547.92$$

Optimization

- **Further refine the hybrid system according to certain optimization criteria**
- **polynomial objective function + semi-algebraic feasible region**
  - **Symbolic optimization**

$$c_3 = \inf_{\mathbf{u}_3} \sup_{\mathbf{u}_2} \min_{\mathbf{u}_1} g_3(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3) \quad \text{over } D_3(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$$

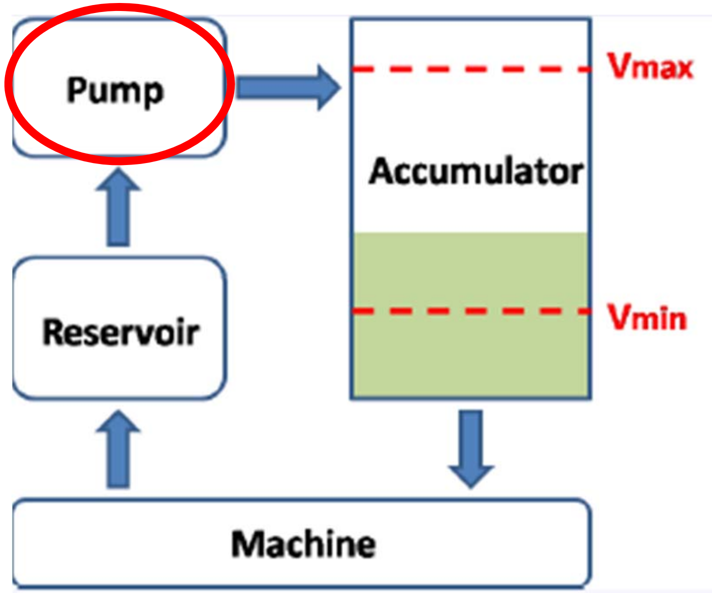
$$\exists \mathbf{u}_3.((\exists \mathbf{u}_1 \mathbf{u}_2 . D_3) \wedge \forall \mathbf{u}_2.(\exists \mathbf{u}_1 . D_3 \Rightarrow \exists \mathbf{u}_1.(D_3 \wedge g_3 \leq z))) \Leftrightarrow z \rhd c_3$$

Outline

- Background
- Invariant and Verification
- Invariant-Based Synthesis
- **Case Studies**
  - Oil pump
  - Lunar lander
- Conclusion

Oil Pump Switching

- First studied in [Cassez et al. HSCC09, 45% improvement]
- Provided by the German company HYDAC
- Determine the time points to switch the pump on/off s.t.

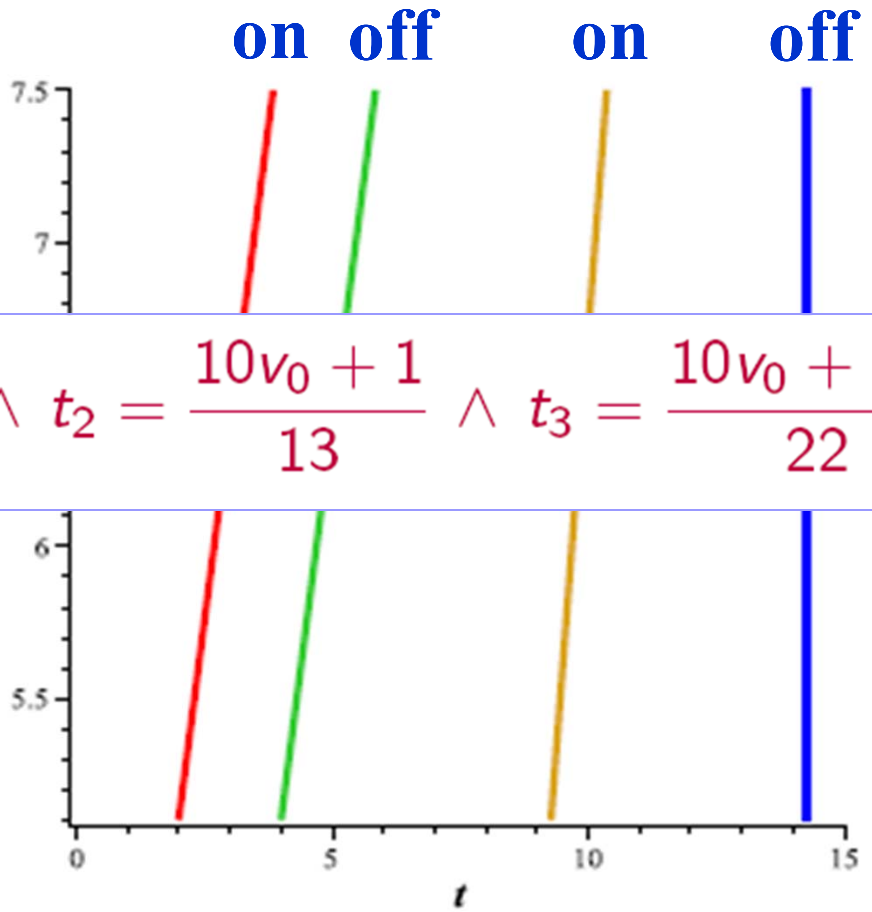


  - **Safety:** $v(t) \in [V_{\mathrm{min}}, V_{\mathrm{max}}], \quad \forall t \in [0, \infty)$
  - **Optimality:**

minimize $\lim_{T \to \infty} \frac{1}{T} \int_{t=0}^{T} v(t) \mathrm{d}t$

Synthesized Switching Controller

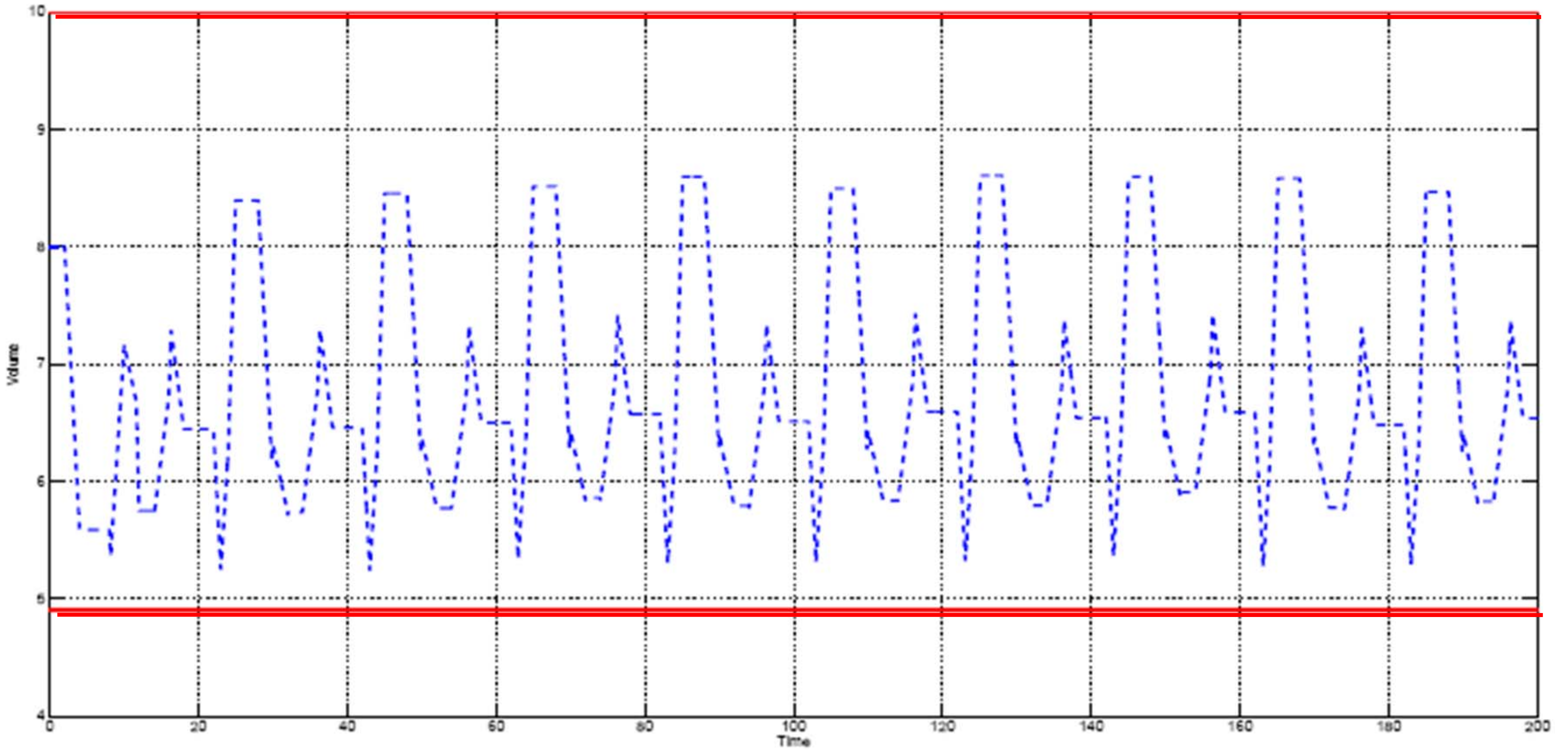
- ***v_0*** **is the initial volume of oil**



$$t_1 = \frac{10v_0 - 25}{13} \wedge t_2 = \frac{10v_0 + 1}{13} \wedge t_3 = \frac{10v_0 + 153}{22} \wedge t_4 = \frac{157}{11}$$

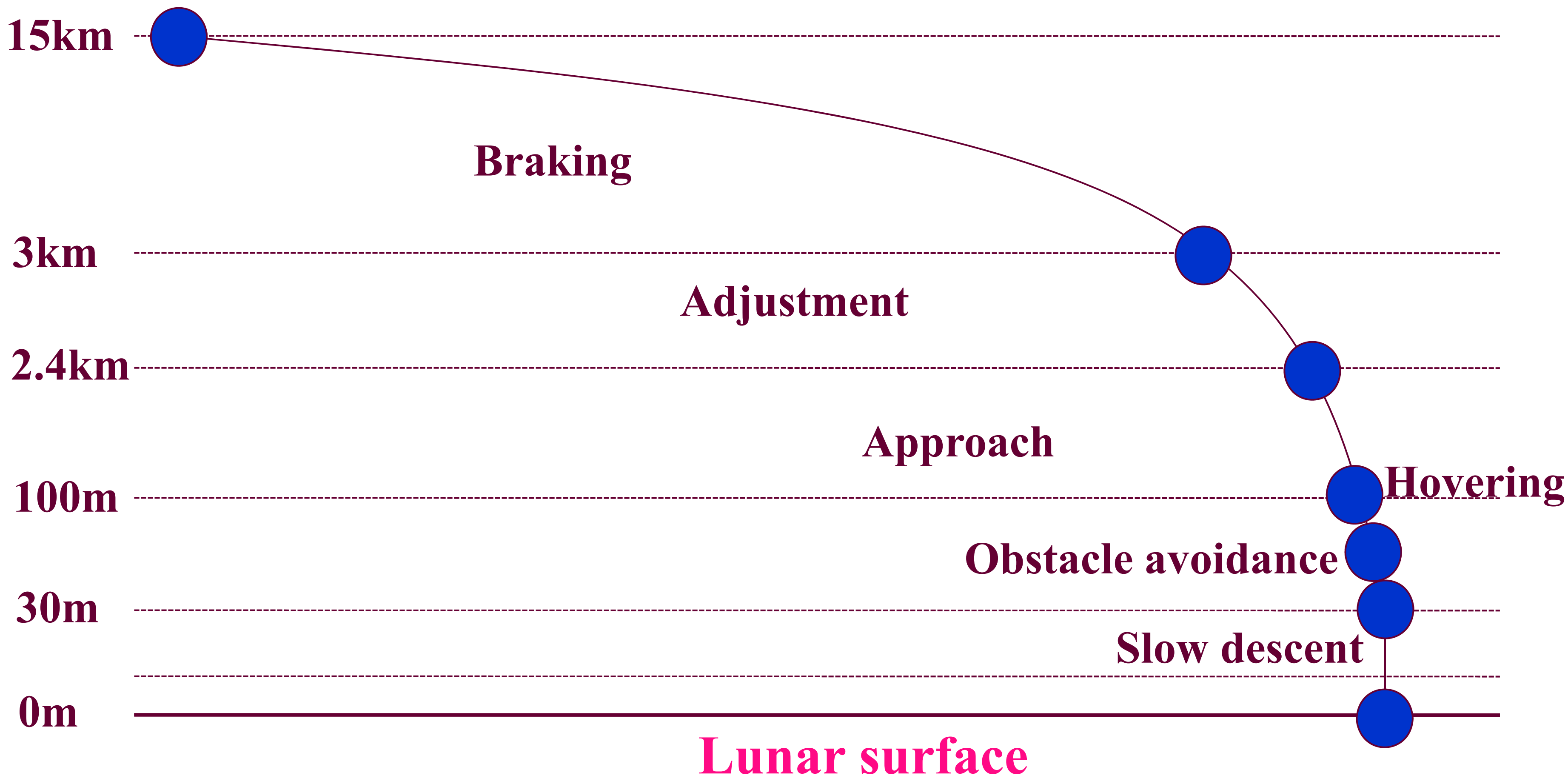
Performance

- **Safety**



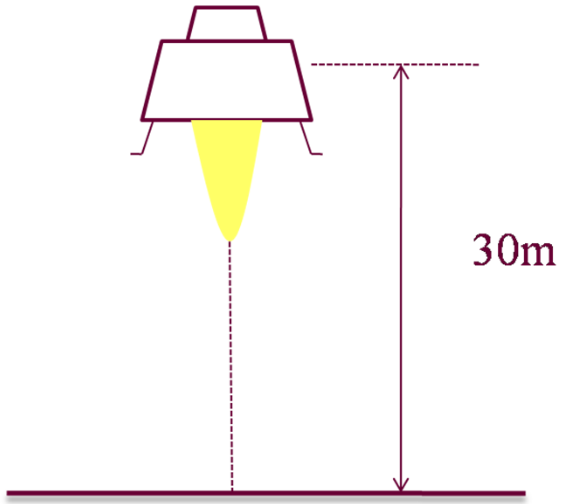
- **Improve the optimal value of** [HSCC09] **by 7.5%**
- **The synthesized controller is correct, also optimal**

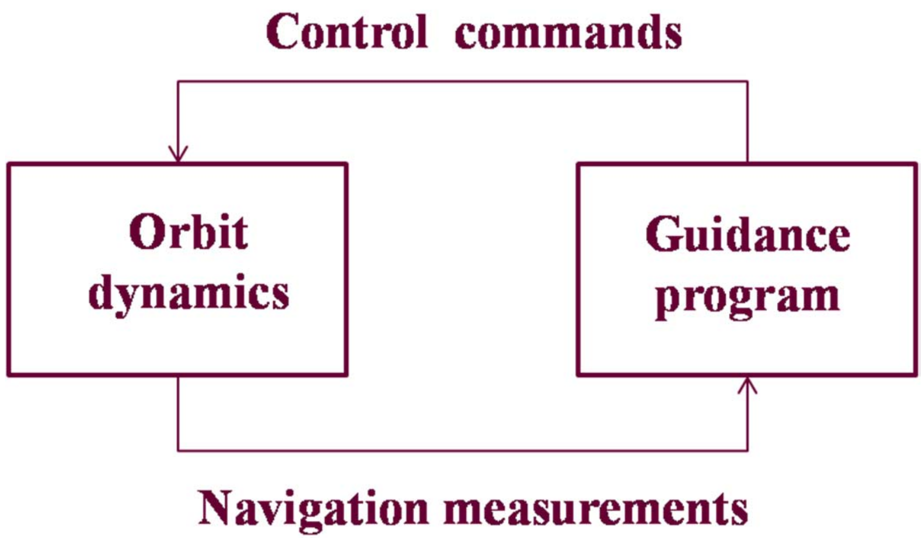
Soft Landing



Slow Descent Phase

- Trajectory control

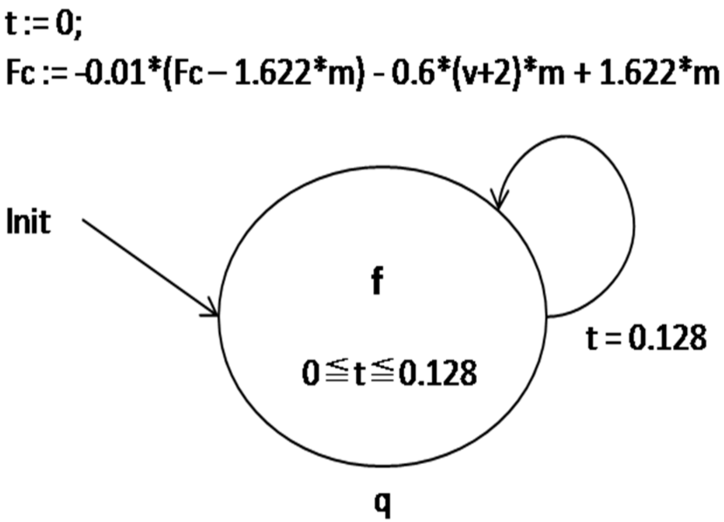




- Sampling period： **ΔT = 0.128s**
- Control objective: **v = -2m/s**

Hybrid Automata Model

- **Dynamics**



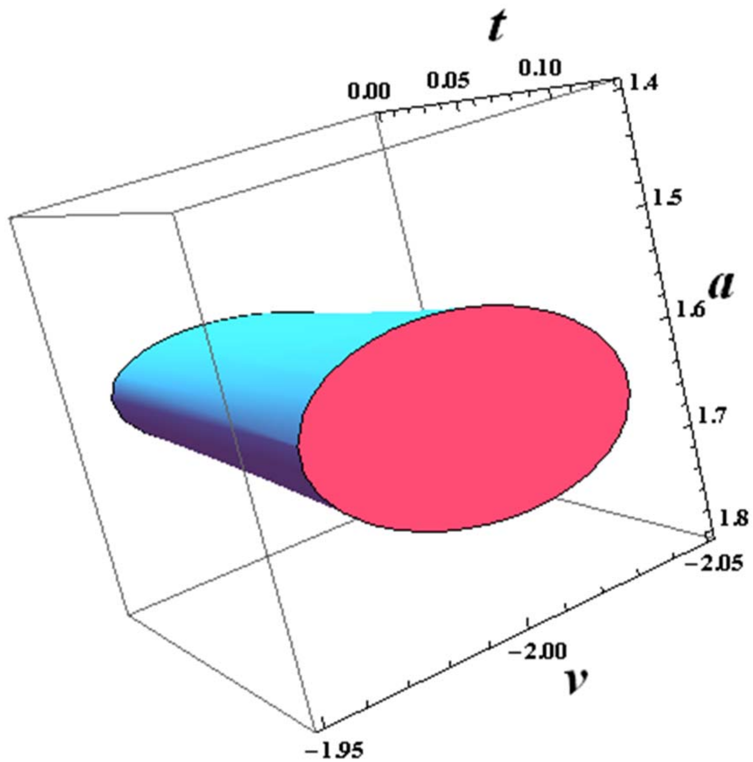
$$\mathrm{f} \widehat{=} \begin{cases} \dot{v} &= \dfrac{F_c}{m} - 1.622 \\ \dot{m} &= -\dfrac{F_c}{2500} \\ \dot{F}_c &= 0 \\ \dot{t} &= 1 \end{cases}$$

- **Replace the non-polynomial term by a new variable: *a = Fc/m***

Verification

- **Safety requirement: $|v - (-2)| \leqq 0.05$**

- **Generated Invariant:**



Kong, H., He, F., Song, X., Hung,W., Gu, M.: Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: CAV'13. pp. 242–257 (2013)

Conclusion

- **Hybrid systems attracts more and more interests with the development of safety critical embedded systems**
- **Invariant plays an important role in the study (formal verification, controller synthesis) of hybrid systems**
- **Semi-algebraic inductive invariant checking for polynomial continuous/hybrid systems is decidable**

Conclusion

- **Use parametric polynomials and symbolic computation to automatically discover invariants, and to perform optimization**
  - **rigorous**
  - **high complexity (may be combined with numeric computation)**
  - **Non-polynomial systems transformed to polynomials ones**
- **Case studies show good prospect of proposed methods**

Related references

- Hengjun Zhao, Mengfei Yang, Naijun Zhan, Bin Gu, Liang Zou and Yao Chen (2014): *Formal verification of a descent guidance control program of a lunar lander*, in Proc. of FM 2014, *Lecture Notes in Computer Science 8442*, pp.733-748.
- Hengjun Zhao, Naijun Zhan and Deepak Kapur (2013): *Synthesizing switching controllers for hybrid systems by generating invariants*, in Proc. of the Jifeng Festschrift, *Lecture Notes in Computer Science* 8051, pp.354-373.
- Hengjun Zhao, Naijun Zhan, Deepak Kapur, and Kim G. Larsen (2012): *A "hybrid" approach for synthesizing optimal controllers of hybrid systems: A Case study of the oil pump industrial example*, in Proc. of FM 2012, *Lecture Notes in Computer Science* 7436, pp.471-485, 2012.
- Jiang Liu, Naijun Zhan and Hengjun Zhao (2011):*Computing semi-algebraic invariants for polynomial dynamical systems*, in Proc. of EMSOFT 2011, pp.97-106, ACM Press.

Thanks!

Questions?