Algorithmic Verification of Stability of Hybrid Systems

Pavithra Prabhakar
Kansas State University

Mysore Park Workshop

Joint work with Miriam Garcia Soto
(IMDEA Software Institute, Madrid)

Cyber-Physical Systems (CPS)

Systems in which software "cyber" interacts with the "physical" world

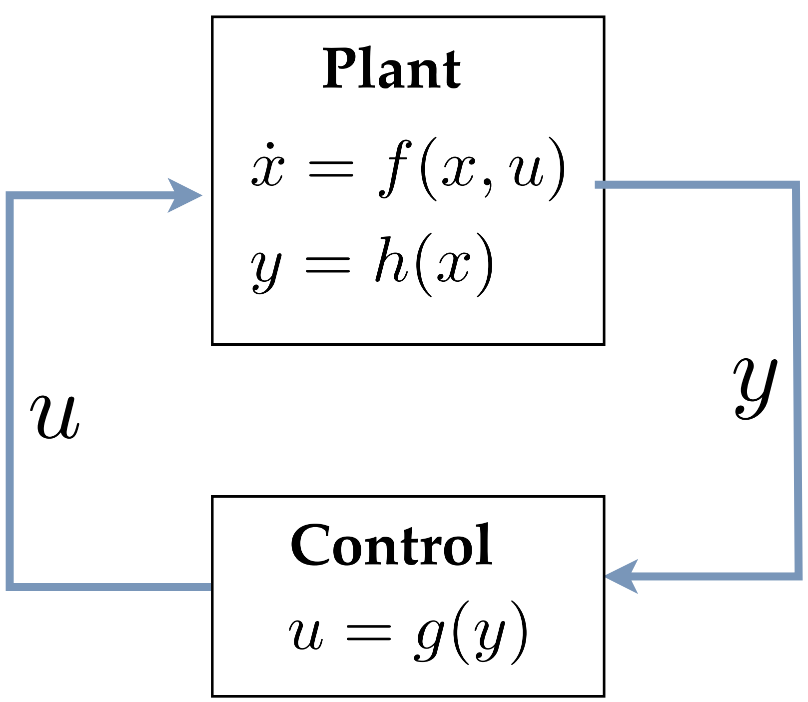
Medical Devices

Automotive

Robotics

Aeronautics

Process control

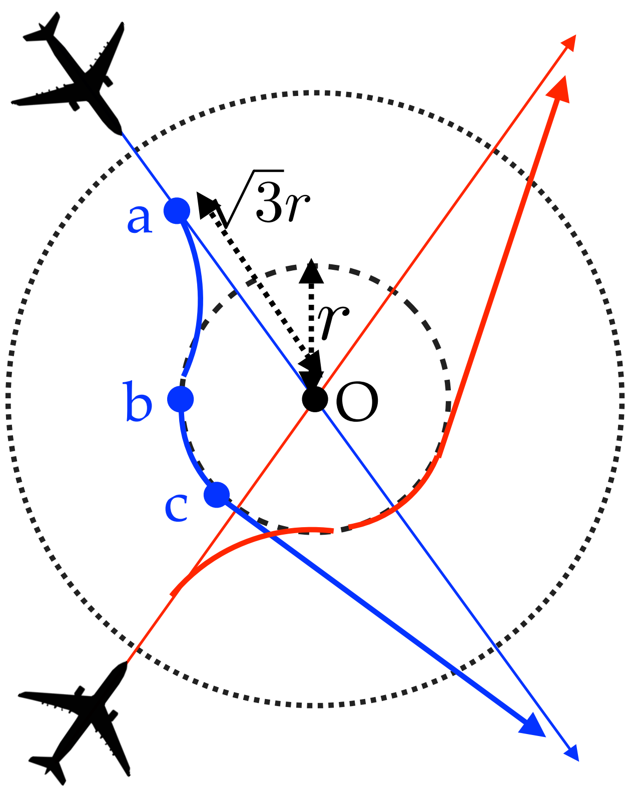


Hybrid Systems

Systems with mixed discrete-continuous behaviors

Hybrid Systems

Air traffic collision avoidance protocol



$\mathbf{x} = (x_1, x_2)$: position of the airplane
$\mathbf{d} = (d_1, d_2)$: velocity of the airplane

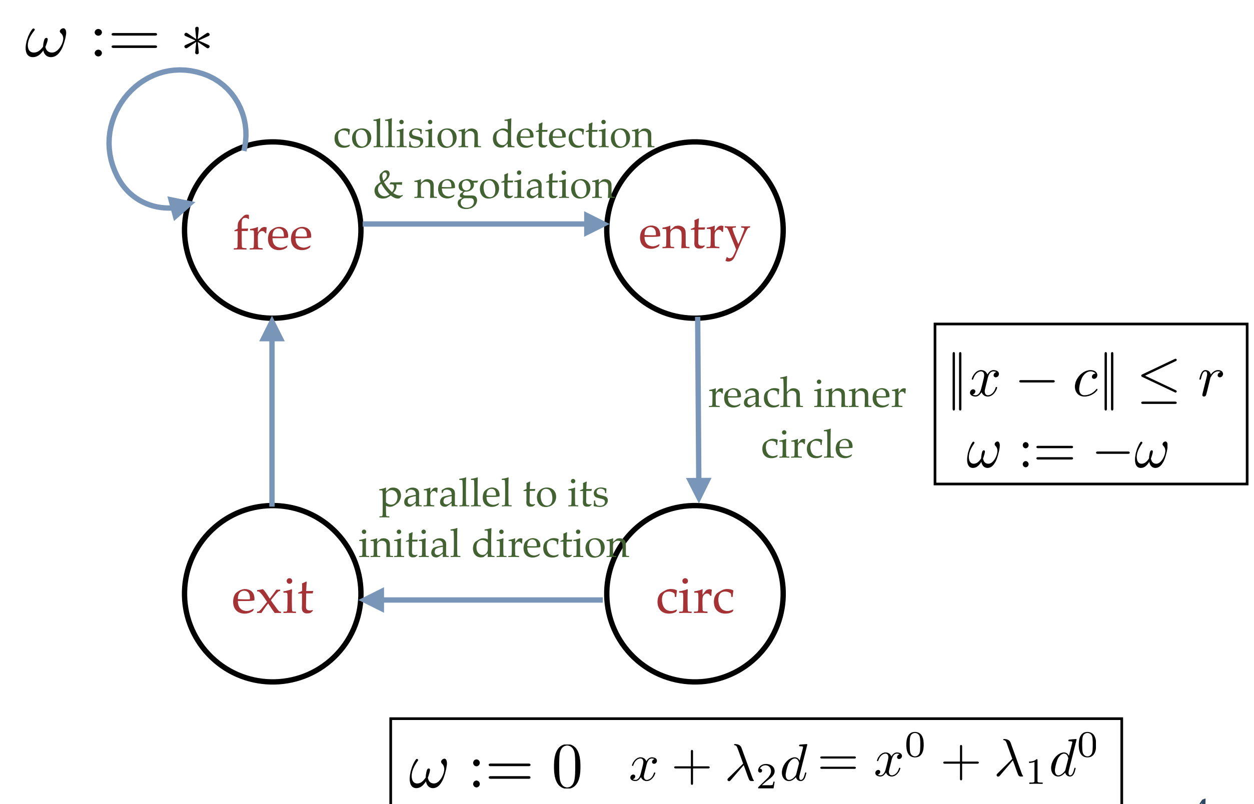
$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{d}_1 \\ \dot{d}_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -\omega \\ 0 & 0 & \omega & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ d_1 \\ d_2 \end{bmatrix}$$

ω: the angular velocity

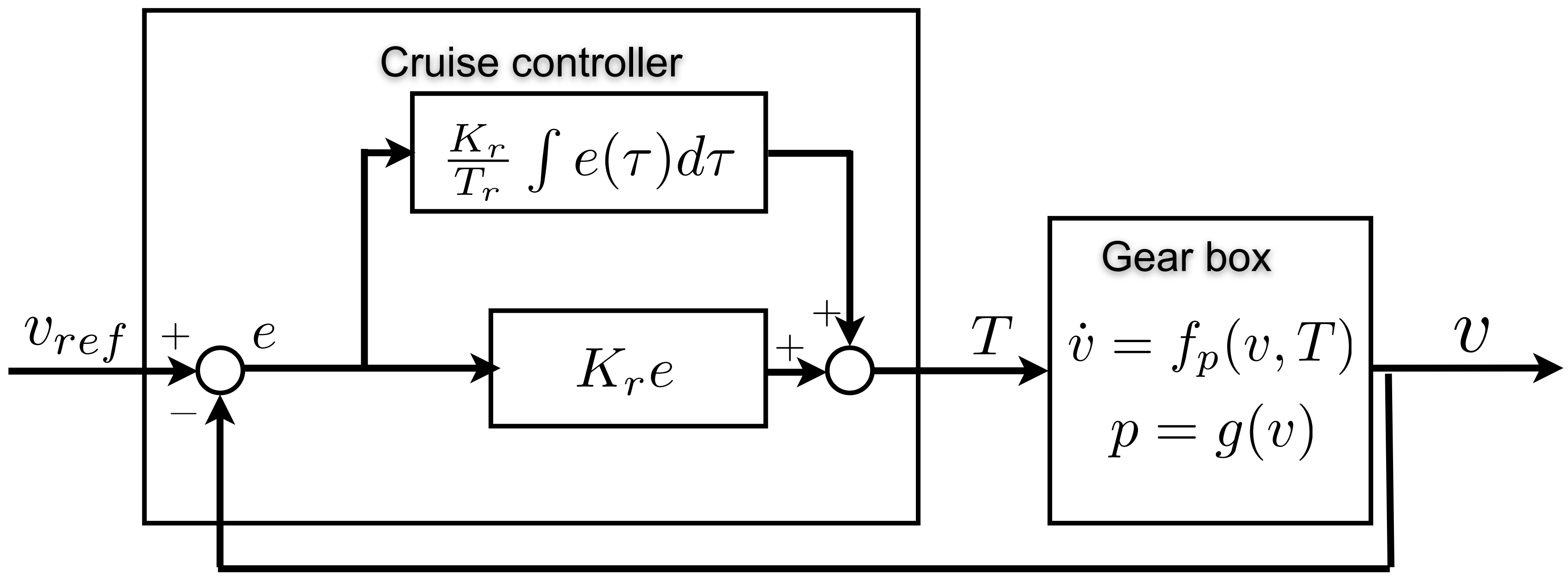
Minimum separation

The aircraft maintain a minimum distance between them always

$$\|x - y\| \leq p \qquad c = x + \lambda d = y + \lambda e$$
$$\|x - c\| = \sqrt{3}r \qquad (r\omega)^2 = \|d\|^2 \qquad x^0 := x,\ d^0 := d$$



Automatic Gear Box & Cruise Control



Velocity v reaches v_{ref}

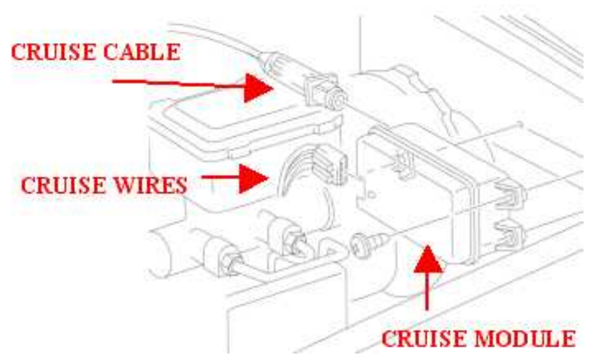
even in the presence of disturbances

Stability

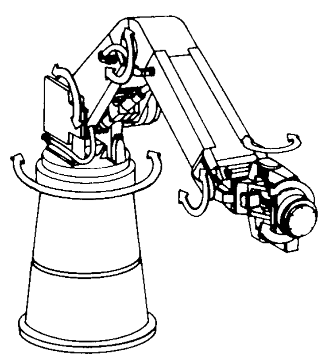
Stability

Stability is a fundamental property in control system design

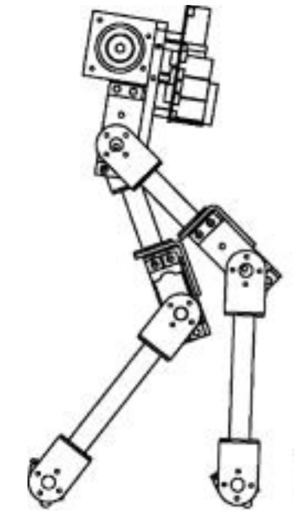
- It captures the notion that small perturbations in the initial state or input result in only small deviations from the nominal behavior



Cruise control



Robotic arm

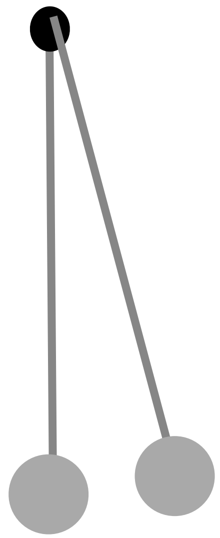


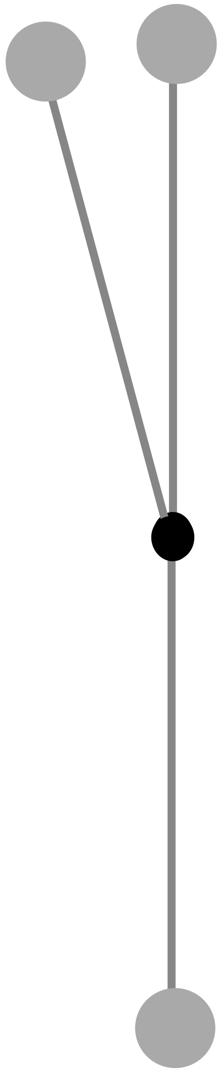
Bipedal robot walking

- Set-point stability
- Stability of the periodic orbit

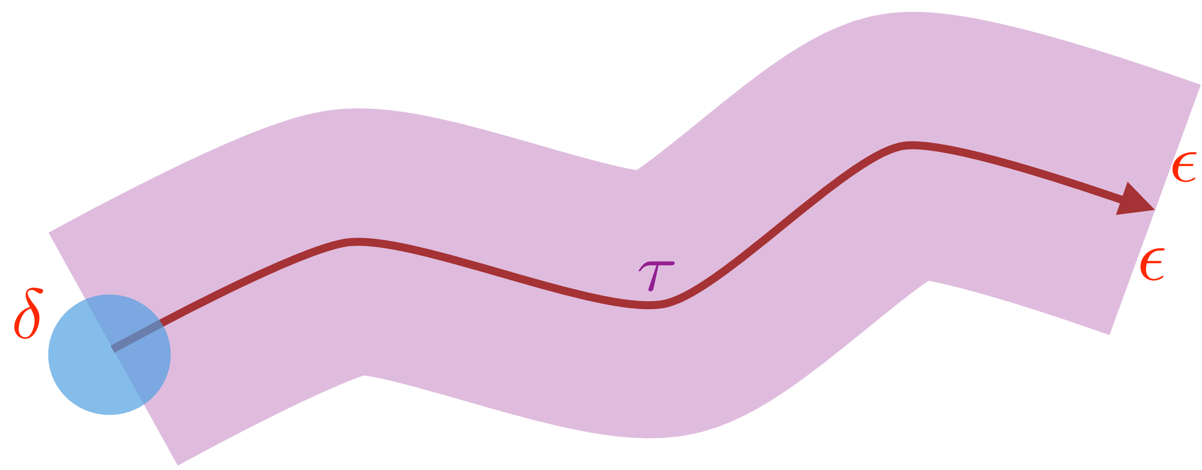
Stability

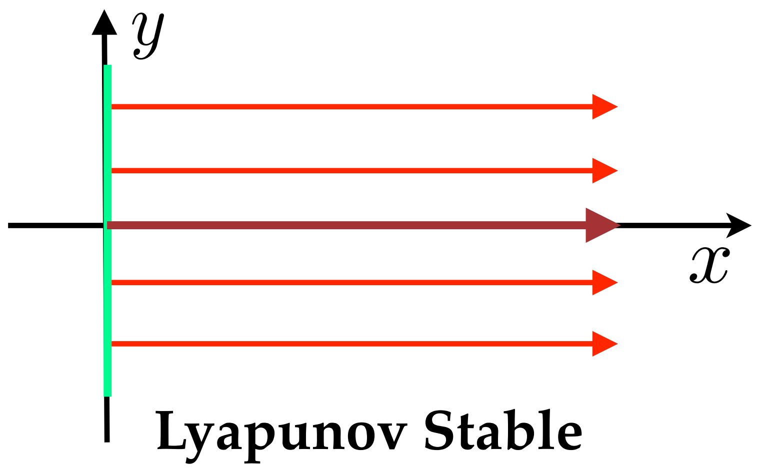
- Small perturbations in the initial state lead to small deviations in the system behavior

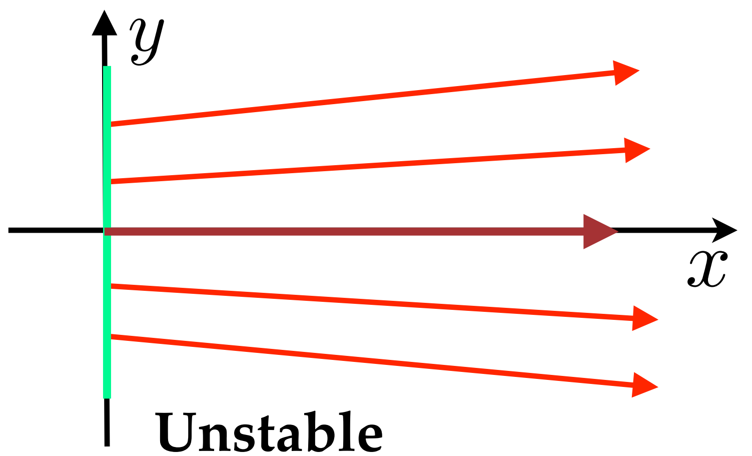


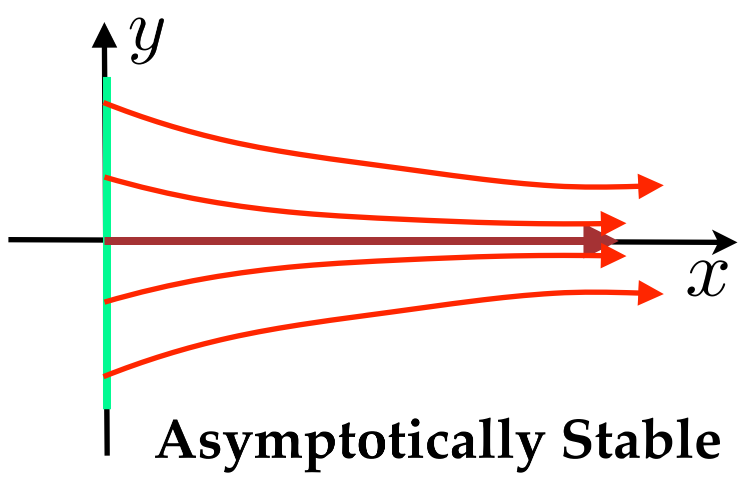


Lyapunov and asymptotic stability









Lyapunov Stability

A system is Lyapunov stable with respect to a trajectory τ if

$$\forall \epsilon > 0, \exists \delta > 0, \forall \tau'$$

$$|\tau(0) - \tau'(0)| < \delta \Rightarrow \forall t \geq 0 \ |\tau(t) - \tau'(t)| < \epsilon$$

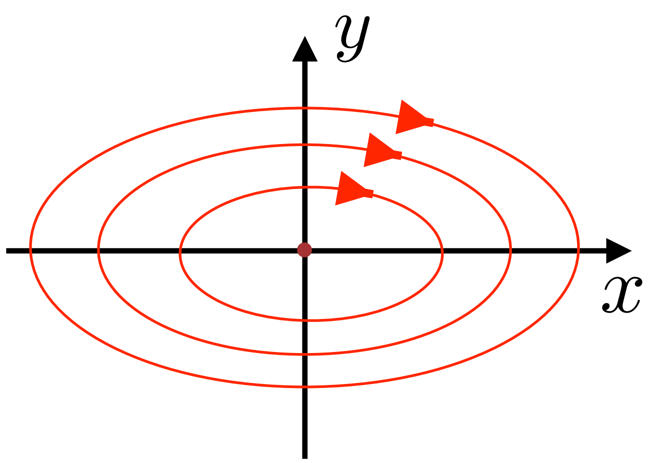
Asymptotic Stability

Asymptotic stability in addition requires convergence to the reference trajectory

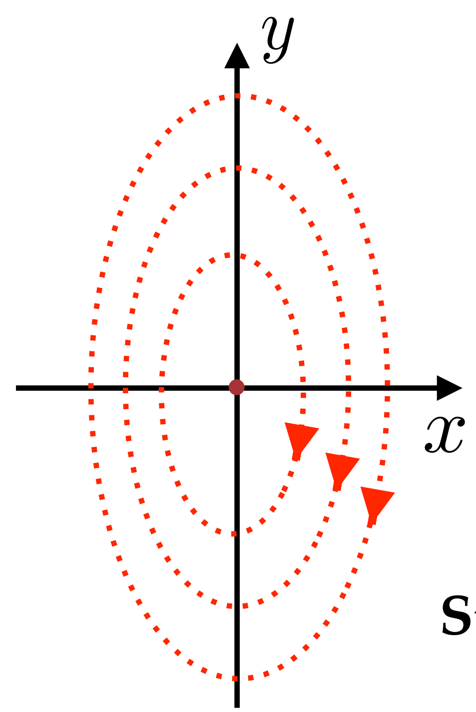
Challenges in Stability Verification for Hybrid Systems

Stability analysis

Linear dynamical systems



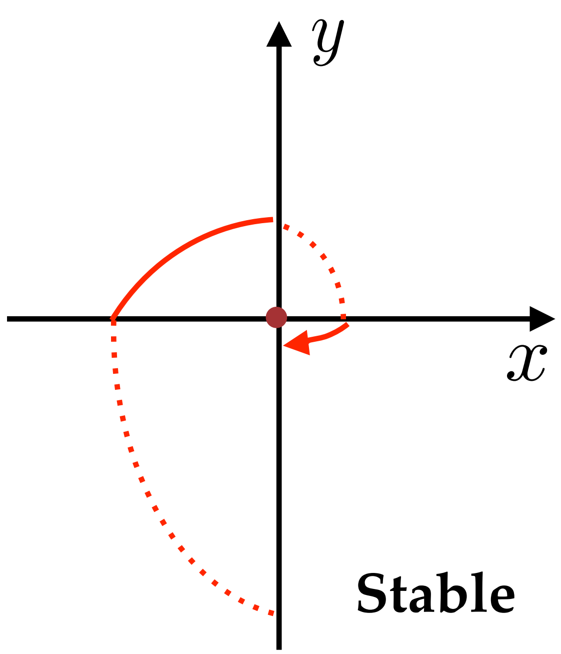
Stable



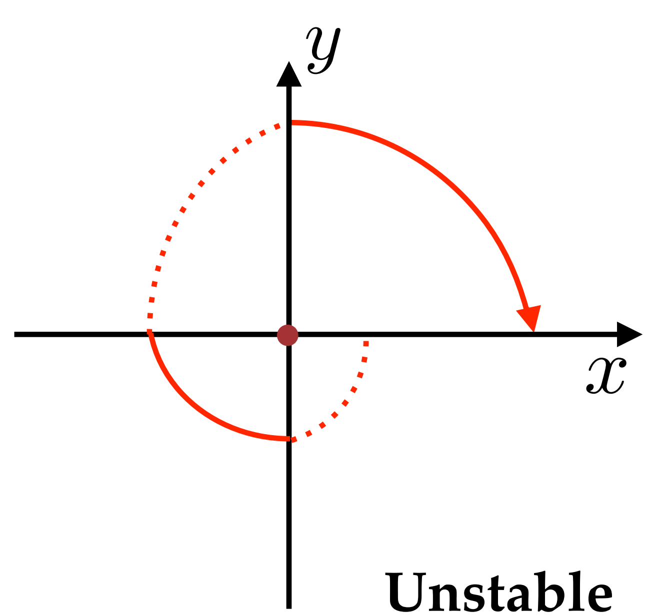
Stable

Stability can be determined by eigen values analysis

Linear hybrid systems



Stable



Unstable

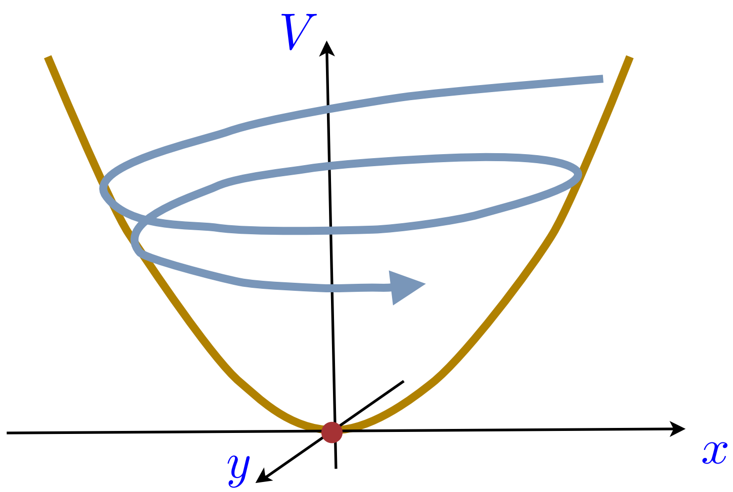
Eigen value analysis does not suffice for switched linear system

Current techniques for Stability Verification

Lyapunov's second method

Lyapunov function:

- Continuously differentiable
  $V : \mathbb{R}^n \to \mathbb{R}^+$
- Positive definite
  $V(x) \geq 0 \, \forall x$
- Decreases along any trajectory
  $\frac{\partial V(x)}{\partial x} F(x) \leq 0 \ \forall x$



Template based automated search

- Choose a template
- Polynomial with coefficients as parameters
- Encode (a relaxation) of the constraints as a sum-of-square programming problem
- Use existing tools for SOS

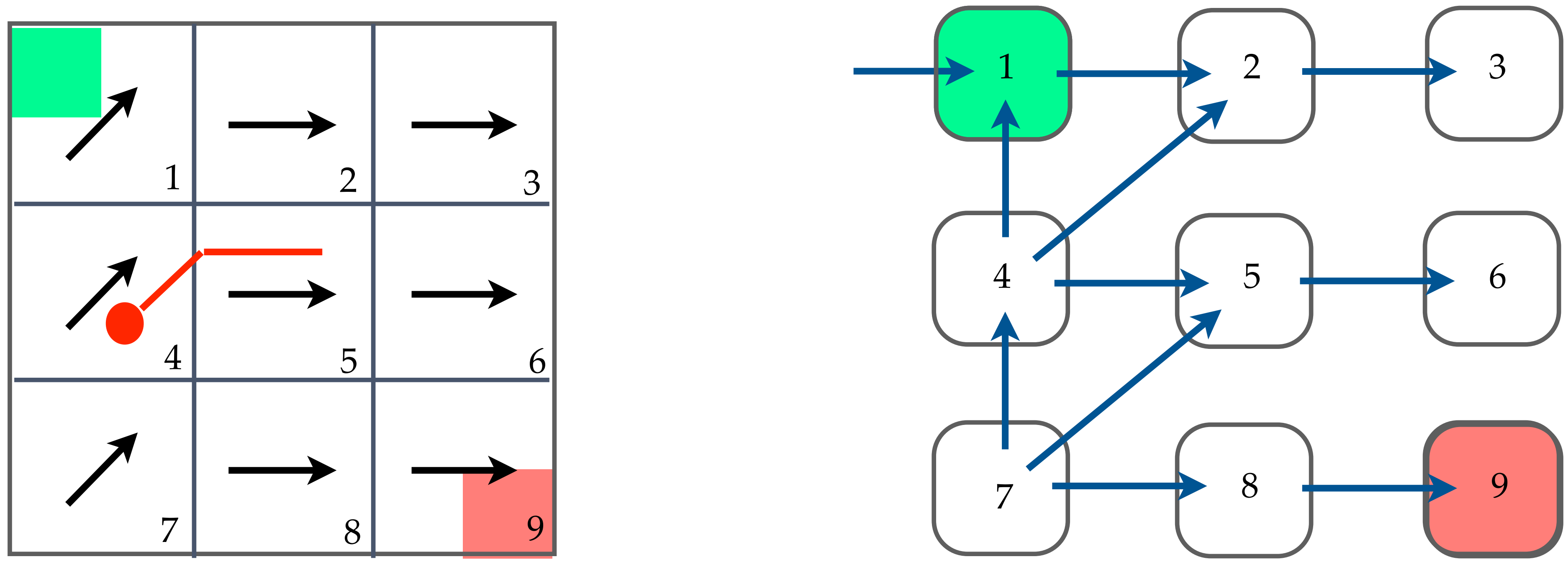
Shortcomings:

- Success depends crucially on the choice of the template
- The current methods provide no insight into the reason for the failure, when a template fails to prove stability
- No guidance regarding the choice of the next template

A CEGAR framework

Counter-example guided abstraction refinement

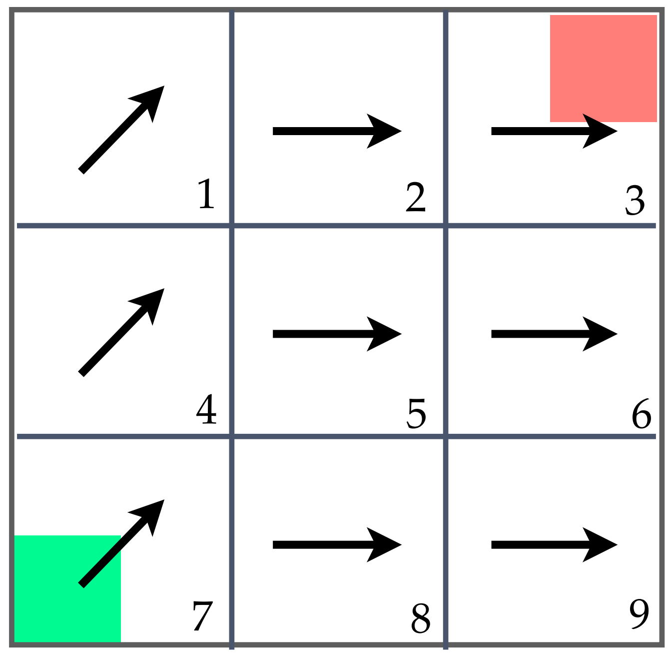
Abstraction

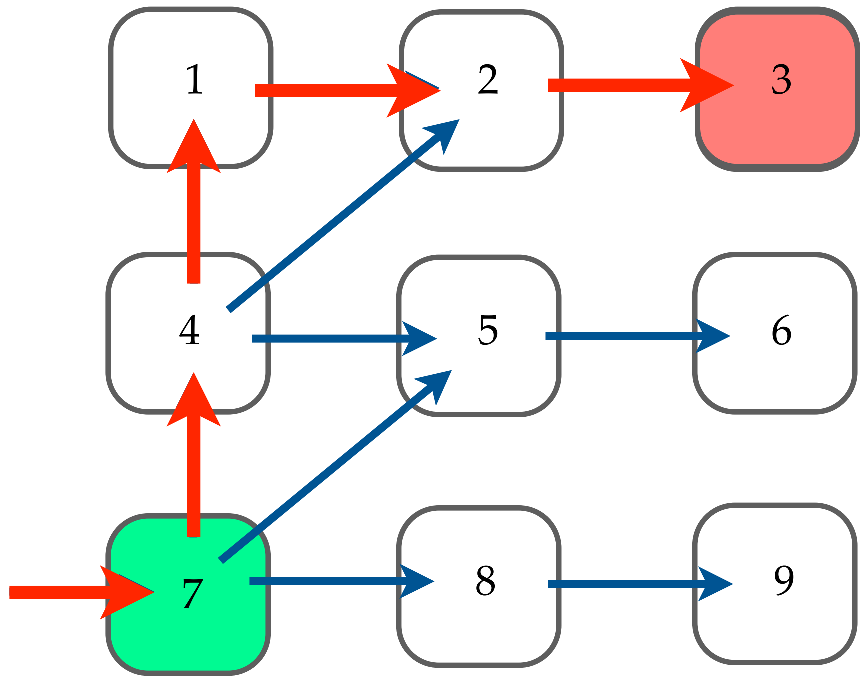


Safety Analysis

- Every trajectory corresponds to a path in the graph
- Absence of a path from green to red node implies safety

Abstraction



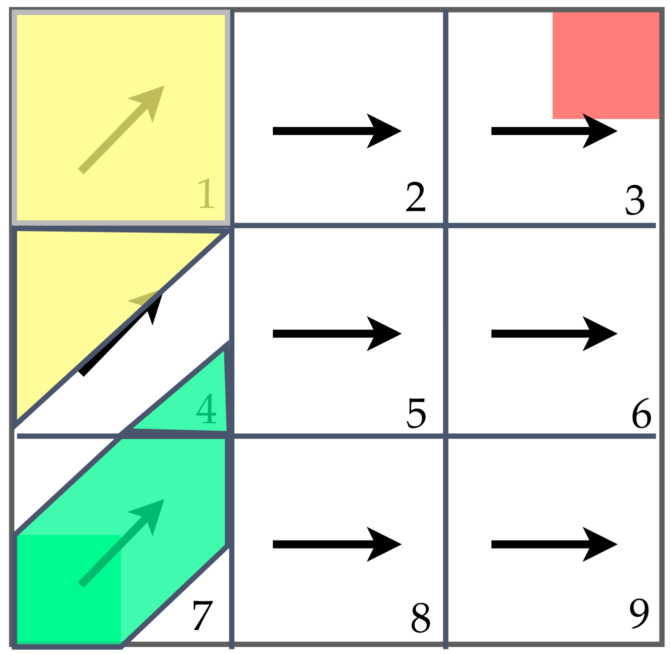


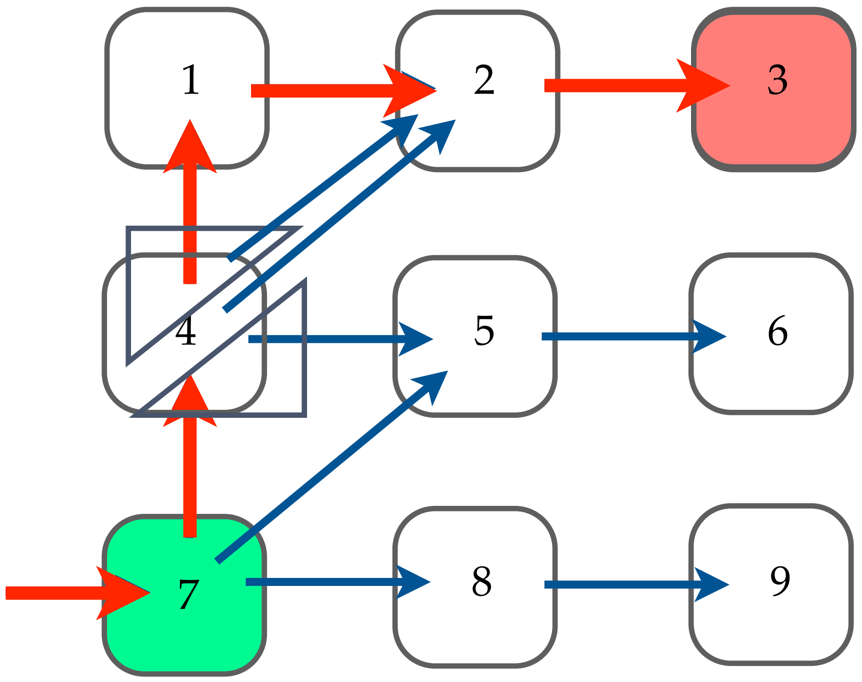
Safety Analysis

- Every trajectory corresponds to a path in the graph
- Absence of a path from green to red node implies safety

- The above system is safe
- The abstract graph has a counter-example
- Right abstractions are hard to find!

Refinement





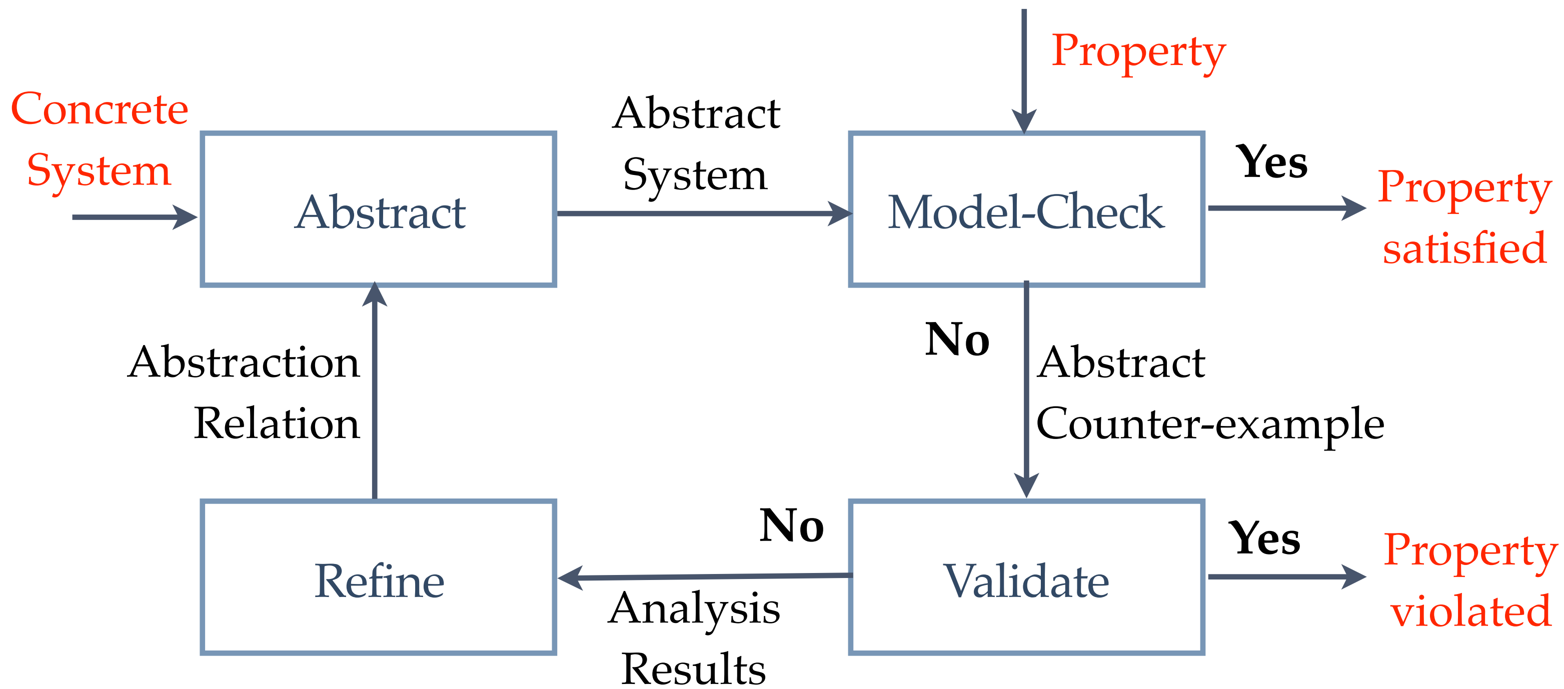
Safety Analysis

- Every trajectory corresponds to a path in the graph
- Absence of a path from green to red node implies safety

- The above system is safe
- The abstract graph has a counter-example
- Right abstractions are hard to find!

- Refine by analyzing the abstract counter-example

Counter-example guided abstraction refinement



- **CEGAR for discrete systems** [Kurshan et al. 93, Clarke et al. 00, Ball et al. 02]
- **CEGAR for hybrid systems safety verification** [Alur et al 03, Clarke et al 03, Prabhakar et al 13]

Template based search

- Success depends crucially on the choice of the template
- No insight into the reason for the failure, when a template fails to prove stability
- No guidance regarding the choice of the next template

CEGAR framework

- Systematically iterate over the abstract systems
- Returns a counter-example in the case that the abstraction fails
- The counter-example can be used to guide the choice of the next abstraction

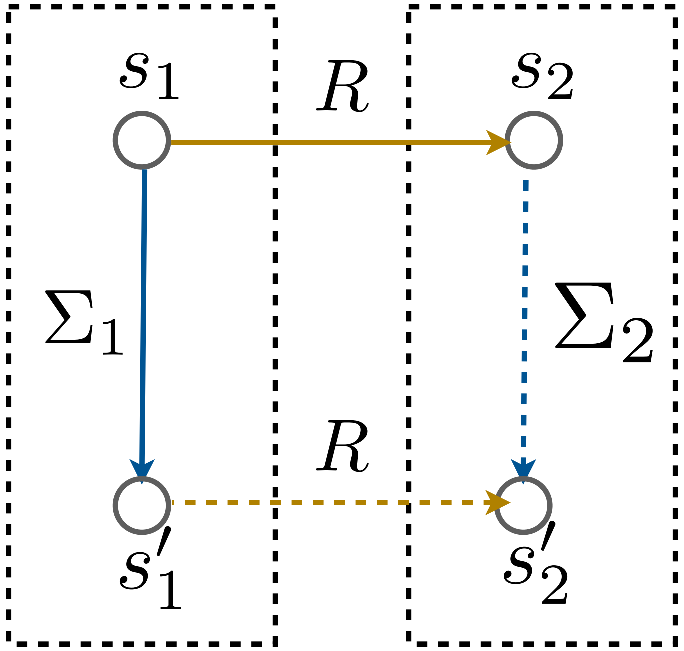
What are the ingredients for CEGAR?

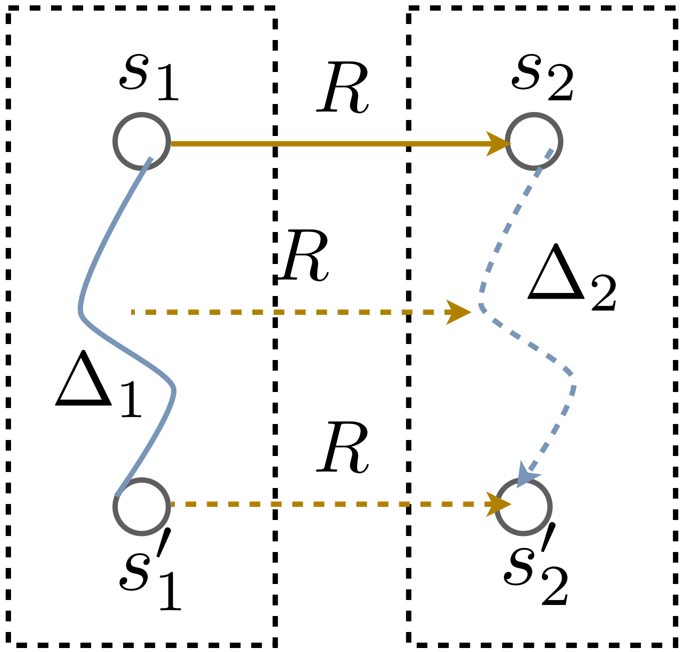
CEGAR questions

- What pre-orders preserve stability?
- How do we construct abstractions/ refinement?

Simulations and Bisimulations

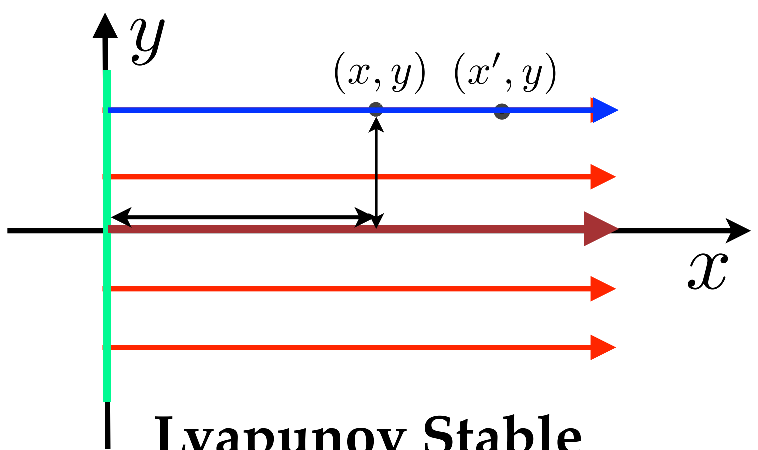
Simulation between $\mathcal{T}_1$ and $\mathcal{T}_2$ is a binary relation $R \subseteq \mathcal{S}_1 \times \mathcal{S}_2$



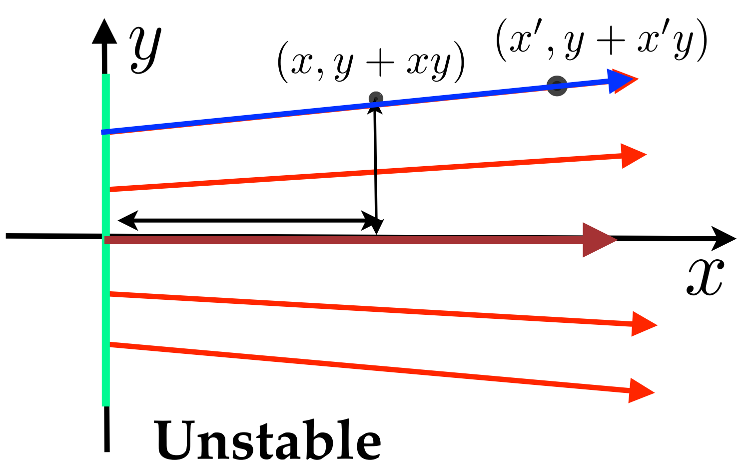


- Every path of the first system has a matching path in the second system
- Bisimulations preserve several discrete-time properties [Timed automata, Multi-rate automata, O-minimal automata]

Stability is not bisimulation invariant!



Lyapunov Stable



Unstable

$$(0, y), t \mapsto (t, y) \qquad\qquad (0, y), t \mapsto (t, y + yt)$$

Preorders for reasoning about stability of hybrid systems.Pavithra Prabhakar, Geir Dullerud and Mahesh Viswanathan.
15th ACM International Conference on Hybrid Systems: Computation and Control (HSCC), 2012. Honorable mention best paper award.

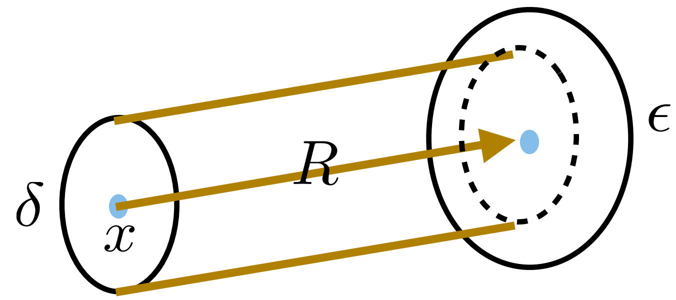
Uniformly continuous (bi)-simulations

R is a uniformly continuous simulation from $\mathcal{T}_1$ to $\mathcal{T}_2$ if

1. R is a simulation and
2. R is uniformly continuous.

$$\forall \epsilon > 0, \exists \delta > 0 \text{ such that } \forall x \in Dom(R),$$

$$R(B_\delta(x)) \subseteq B_\epsilon(R(x))$$



Theorem

Let R be a uniformly continuous simulation from $\mathcal{T}_1$ to $\mathcal{T}_2$, and be consistent with τ_1 and τ_2.

$\mathcal{T}_2$ is stable with respect to τ_2 implies $\mathcal{T}_1$ is stable with respect to τ_1

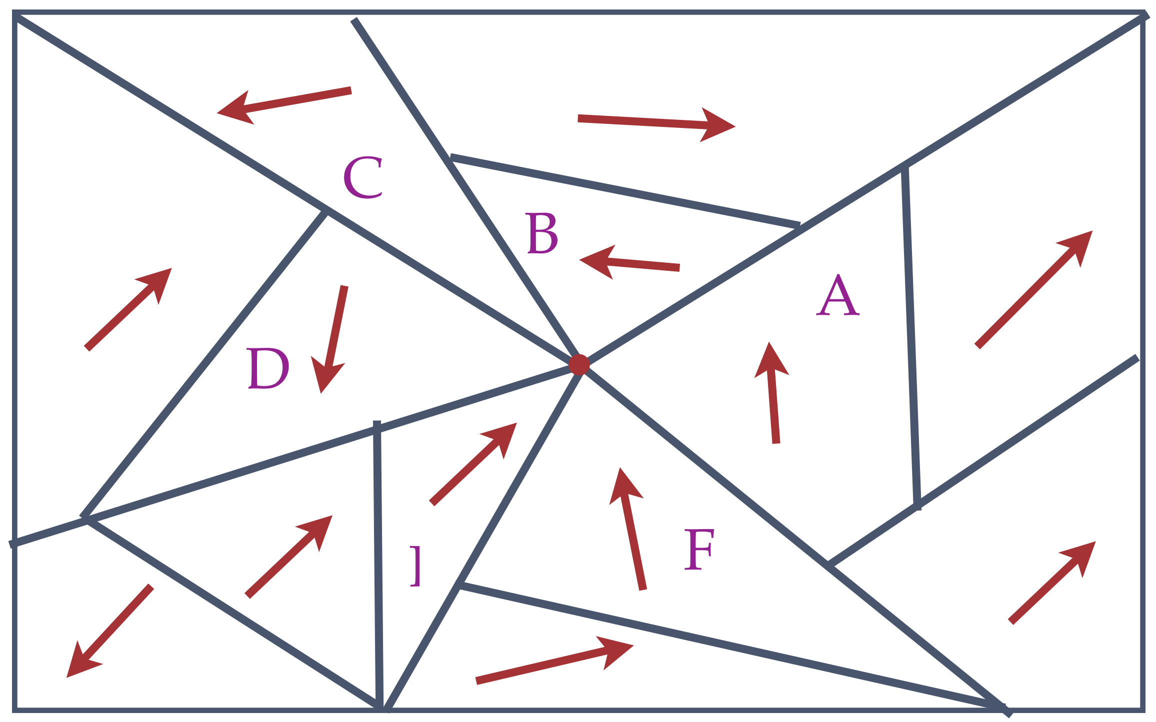
- Continuous simulations suffice for stability with respect to an equilibrium point
- Classical stability analysis techniques —- Lyapunov's second method and Linearization —- are instances of stability analysis based on uniformly continuous simulations

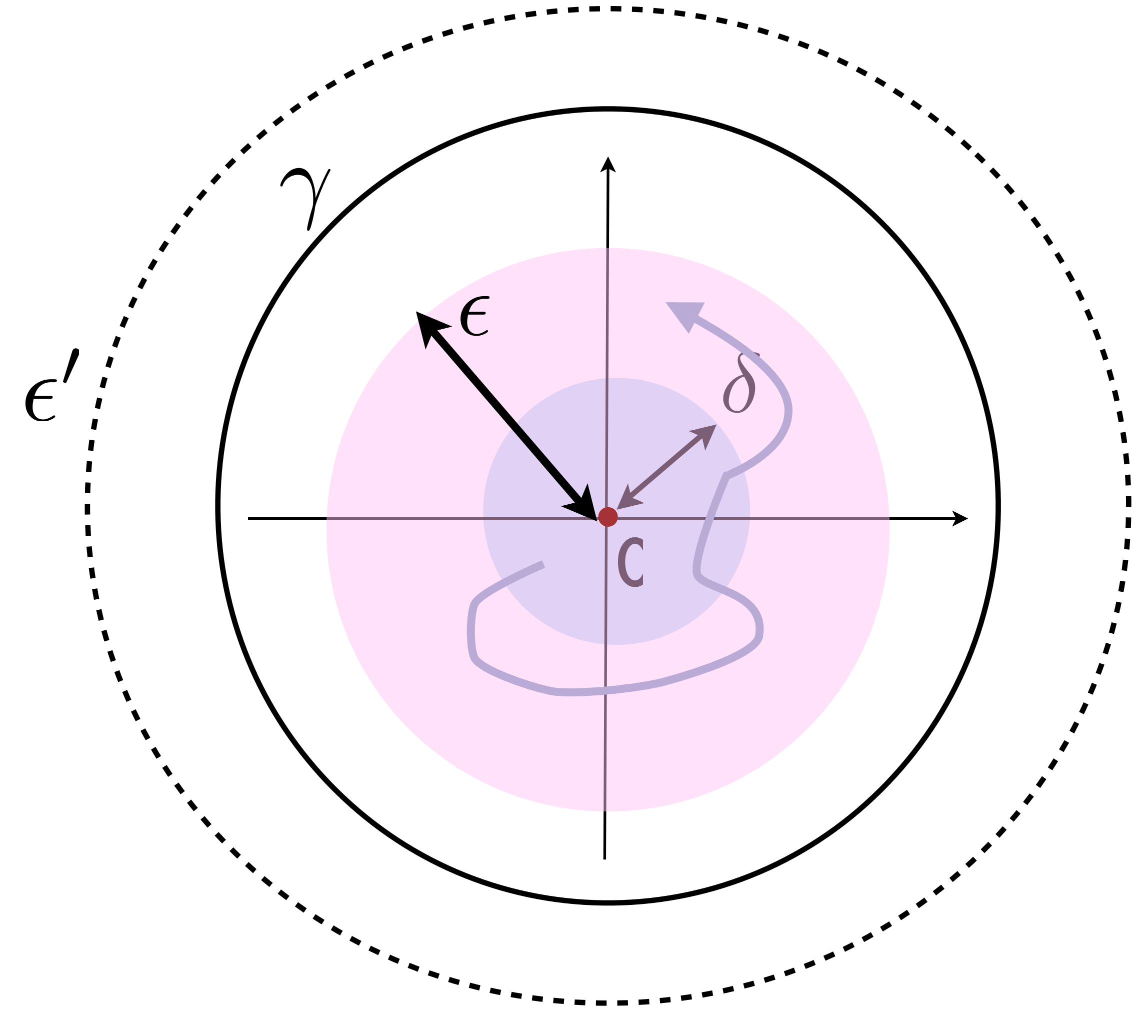
Preorders for reasoning about stability of hybrid systems with inputs. Pavithra Prabhakar, Jun Liu and Richard Murray. International conference on Embedded Software (EMSOFT), 2013. Invited paper at the 50th Allerton conference.

Abstraction based Analysis

- What pre-orders preserve stability?
- How do we construct abstractions?

Piecewise Constant Derivative System



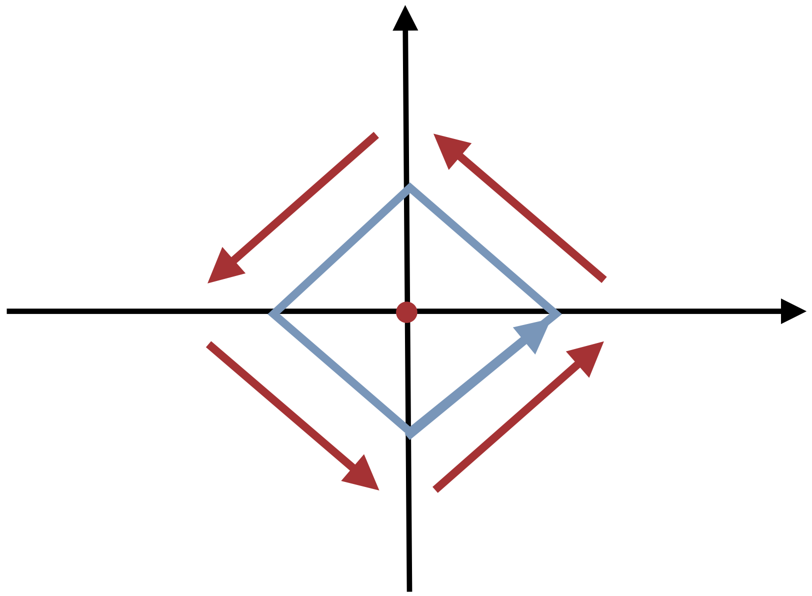


$$\exists\gamma > 0, \forall\epsilon \in (0, \gamma]$$

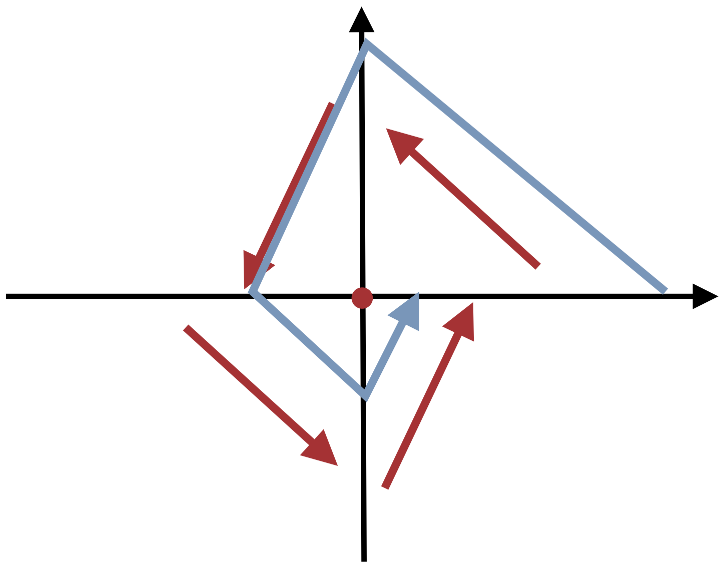
$$\cancel{\forall\epsilon > 0,}\ \exists\delta > 0, [(\tau(0) \in B_\delta(0)) \Rightarrow \forall t(\tau(t) \in B_\epsilon(0))]$$

- Special structure in a small neighborhood
- Homogenous linear constraints matter

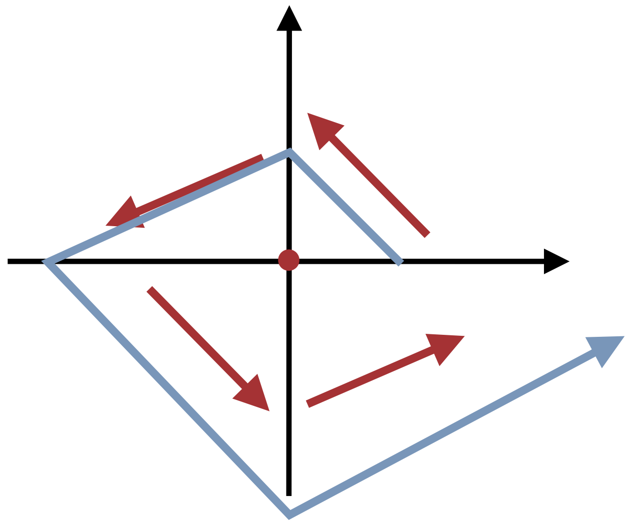
PCD examples



Lyapunov stable but
Not asymptotically stable



Both Lyapunov stable and
asymptotically stable

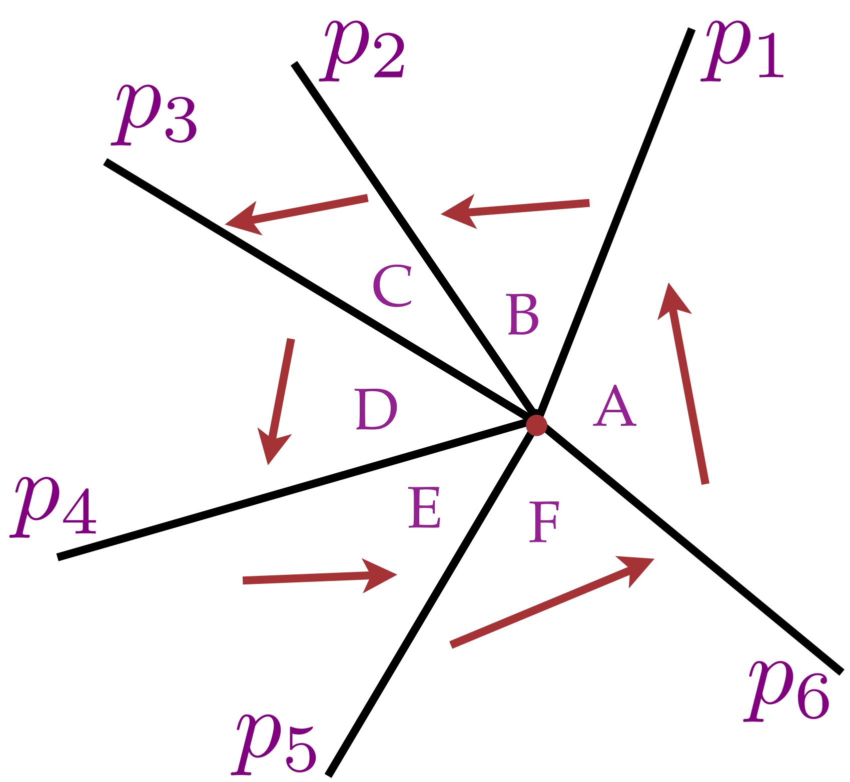


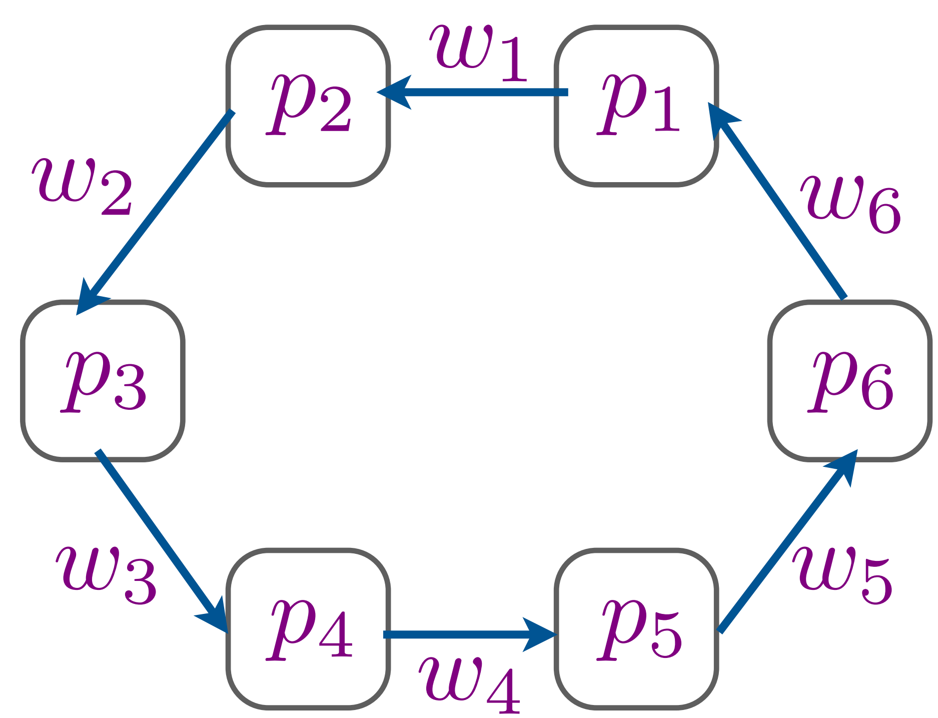
Unstable

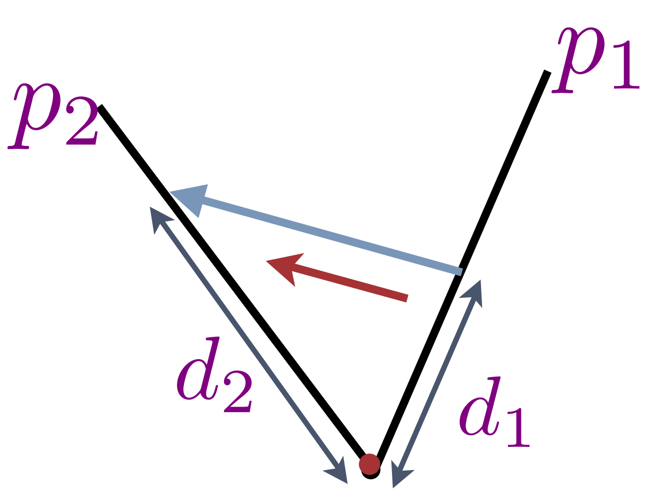
Theorem

Verifying Lyapunov/Asymptotic Stability is undecidable in 5 dimensions for PCDs, but is decidable in 2 dimension for a more general class of systems.

Predicate abstraction



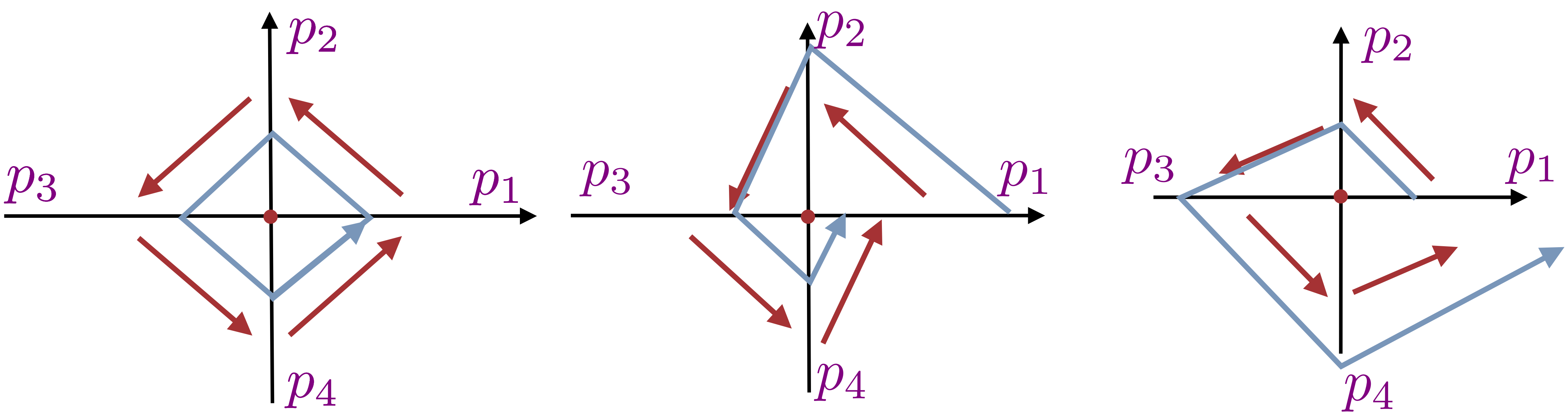


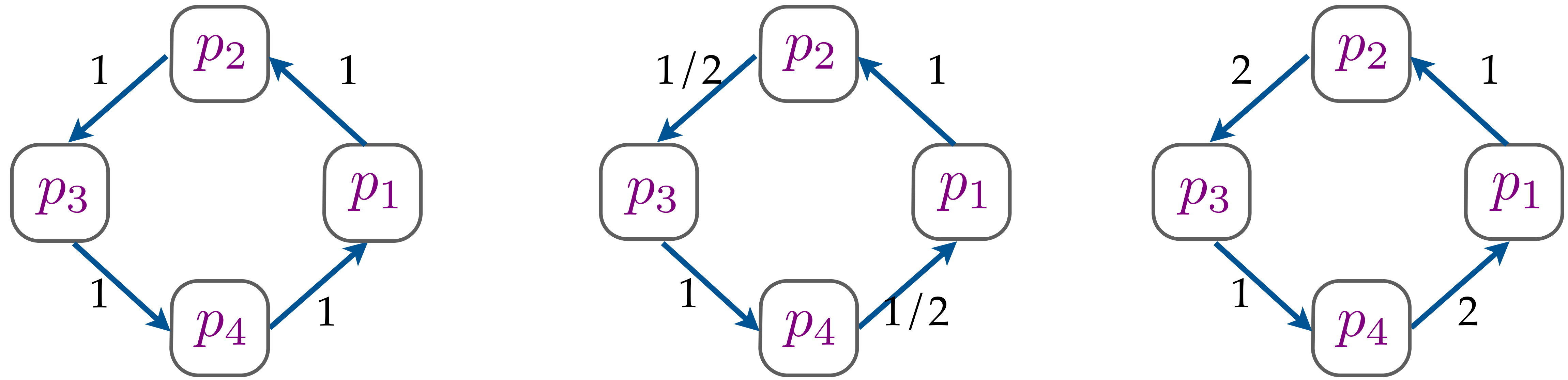


$$w(e) = \frac{|d_2|}{|d_1|}$$

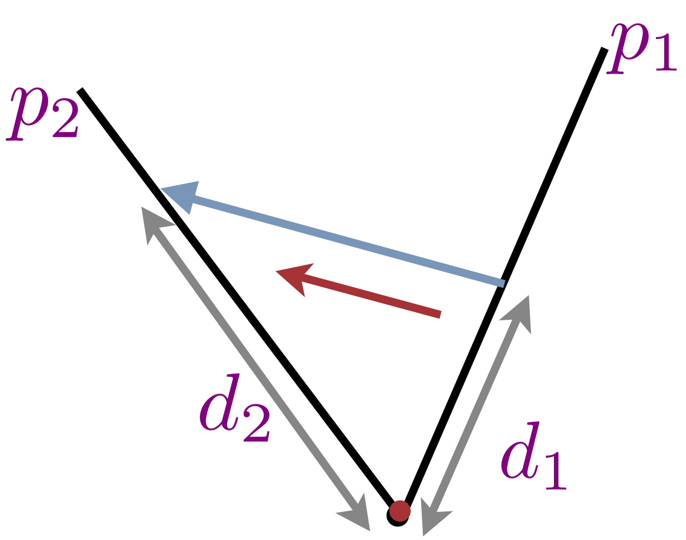
Weights capture information about distance to the origin along the executions

Weighted Graph Construction

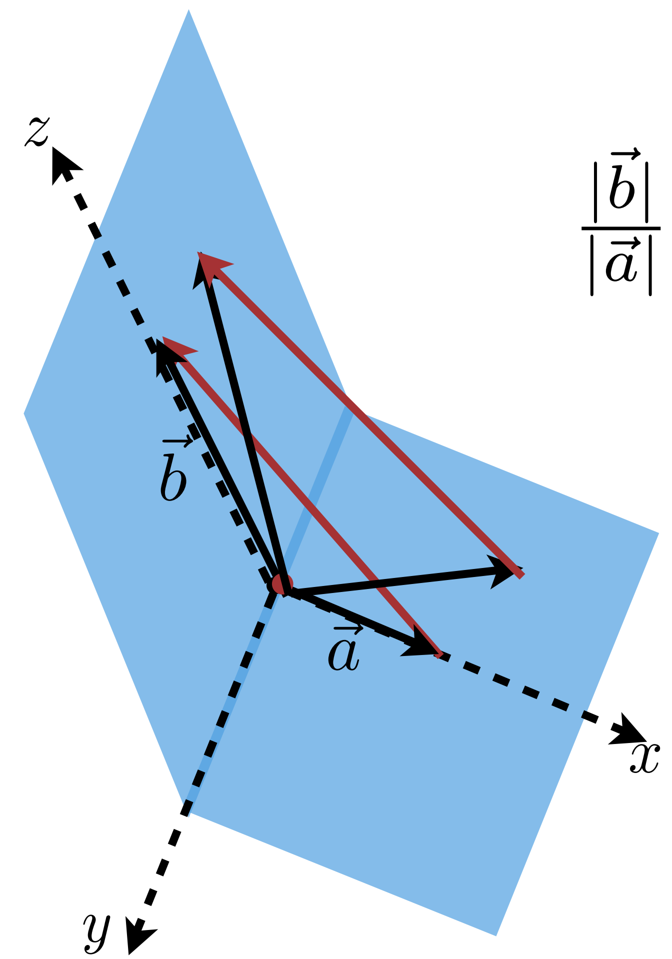




A remark on weight computation



$$w(e) = \frac{|d_2|}{|d_1|}$$



$$\frac{|\vec{b}|}{|\vec{a}|} \qquad \frac{|\vec{b}+\vec{c}|}{|\vec{a}+\vec{c}|}$$

$$\sup \frac{|v_2|}{|v_1|}$$

$$t \geq 0, v_1 \in f_1, v_2 \in f_2, v_2 = v_1 + \varphi t$$

$$\vec{a} \to \vec{b} \text{ implies } \alpha\vec{a} \to \alpha\vec{b}$$

Soundness of Abstraction

Theorem

The piecewise constant derivative system is Lyapunov stable if

- there are no edges with infinite weights and
- the weighted graph does not contain any cycles with product of weights on the edges greater than 1

Abstraction based model-checking of stability of hybrid systems. P. Prabhakar, M. G. Soto. CAV'13

Quantitative Predicate Abstraction

Let $\mathcal{H}$ be a hybrid system.

Let $\mathcal{P} = \{P_1, \ldots, P_k\}$ a finite partition of its state-space

Construct a weighted graph $\mathcal{G} = (V, E, W)$, where:

- $V = \mathcal{P}$
- $(P_1, P_2) \in E$ if there exists P such that $Reach(P_1, P, P_2) \neq \emptyset$
- $W(e) = \sup\{\frac{\|y\|}{\|x\|} \mid (x, y) \in Reach(P_1, P, P_2)\}$, where $e = (P_1, P_2)$

$$Reach(P_1, P, P_2) = \{(s_1, s_2) \mid s_1 \in P_1, s_2 \in P_2, s_1 \overset{P}{\rightsquigarrow} s_2\}$$

Soundness holds under certain finite variability conditions on the dynamics with respect to the partition

Foundations for Quantative predicate abstraction for stability analysis of hybrid systems. P. Prabhakar, M. G. Soto. VMCAI'15

Rectangular and polyhedral dynamics

$$Reach(P_1, P, P_2) = \{(s_1, s_2) \mid s_1 \in P_1, s_2 \in P_2, s_1 \overset{P}{\leadsto} s_2\}$$

Constant derivative $\dot{x} = \varphi$

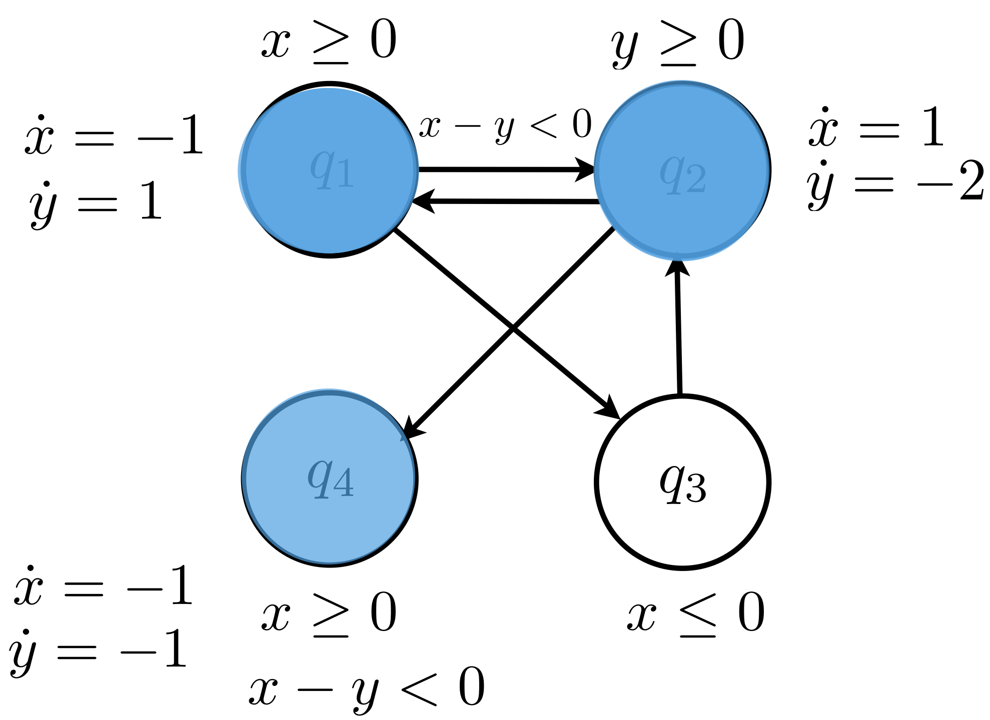
$$\sup \frac{|v_2|}{|v_1|}$$

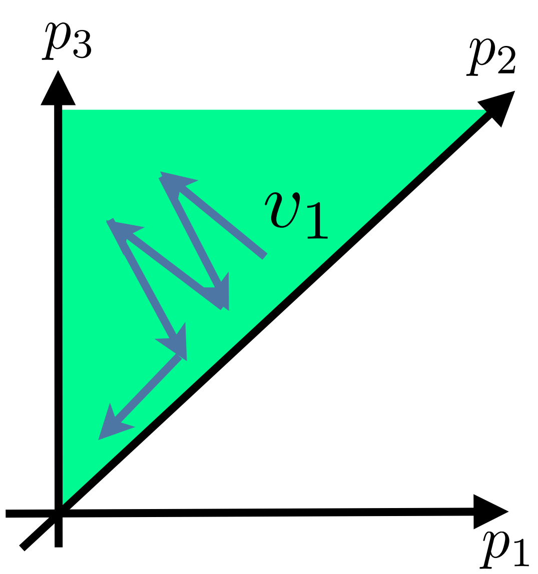
$$t \geq 0, v_1 \in f_1, v_2 \in f_2, v_2 = v_1 + \varphi t \quad \varphi \in P$$

Polyhedral dynamics $\dot{x} \in P$, P is a polyhedral set

Polyhedral switched systems

- Overlapping guards and invariants

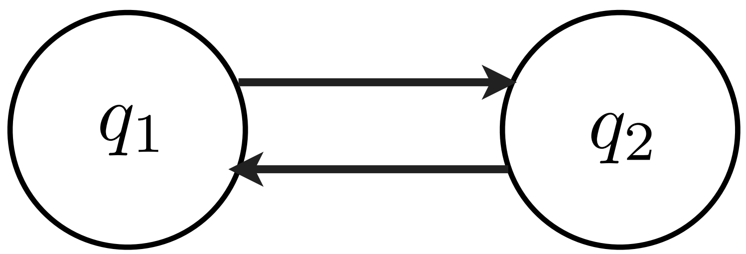


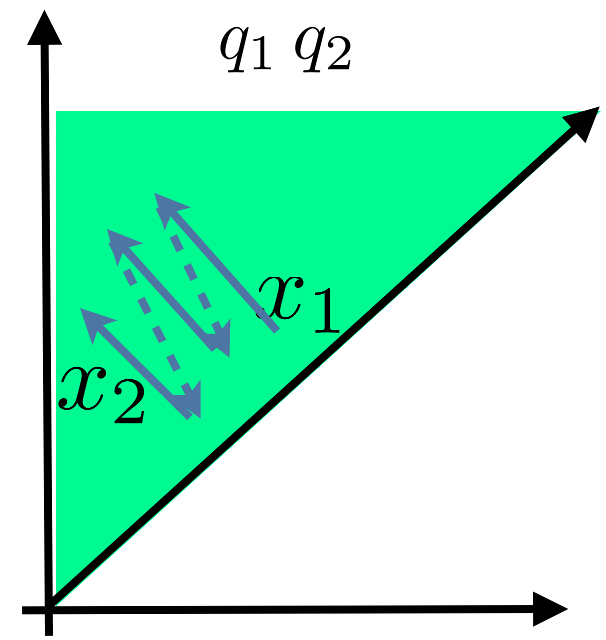


- The number of switchings is not bounded
- Compute the reachability relation for a strongly connected component

Polyhedral switched systems contd.

Strongly connected component





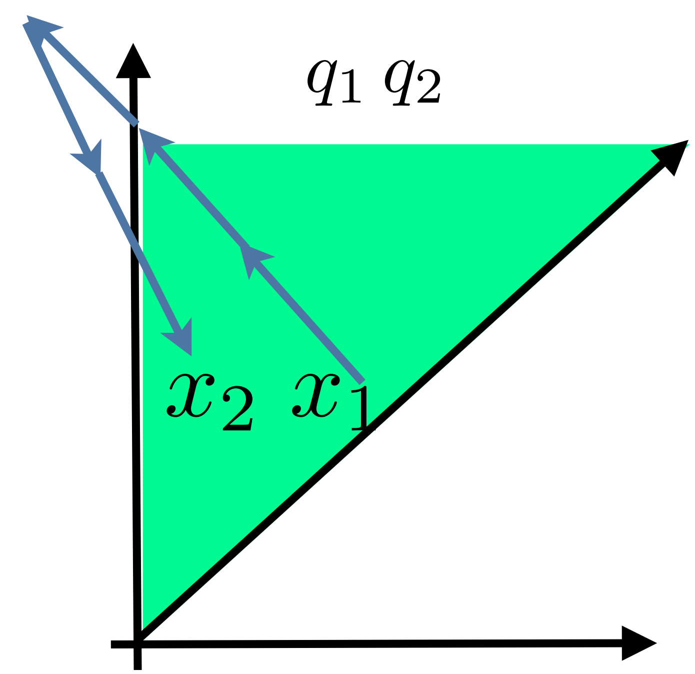
$$x_2 = x_1 + a_1 t_1 + a_2 t_2 + a_1 t_3 + a_2 t_4 + \ldots$$

$$x_1 \in R, x_1 + a_1 t_1 \in R, x_1 + a_1 t_1 + a_2 t_2 \in R, \ldots$$

$$\Downarrow$$

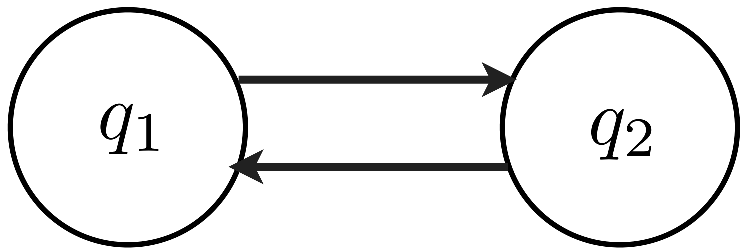
$$x_2 = x_1 + a_1 t_1' + a_2 t_2'$$

$$x_1 \in R, x_2 \in R$$



Polyhedral switched systems contd.

Strongly connected component



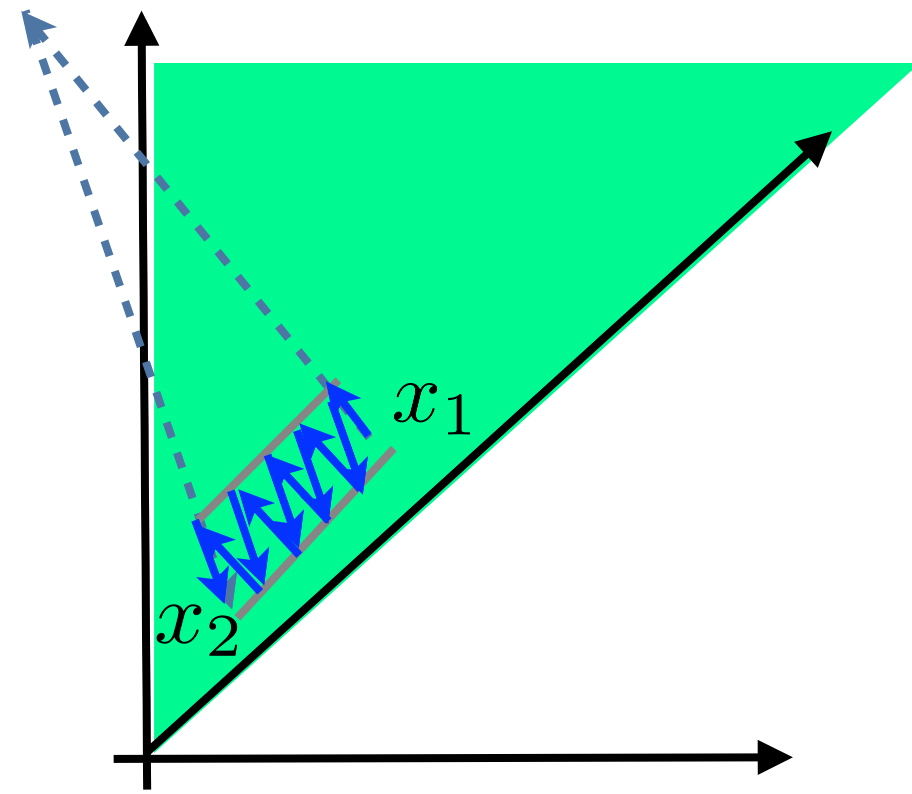
$$x_2 = x_1 + a_1t_1 + a_2t_2 + a_1t_3 + a_2t_4 + \ldots$$

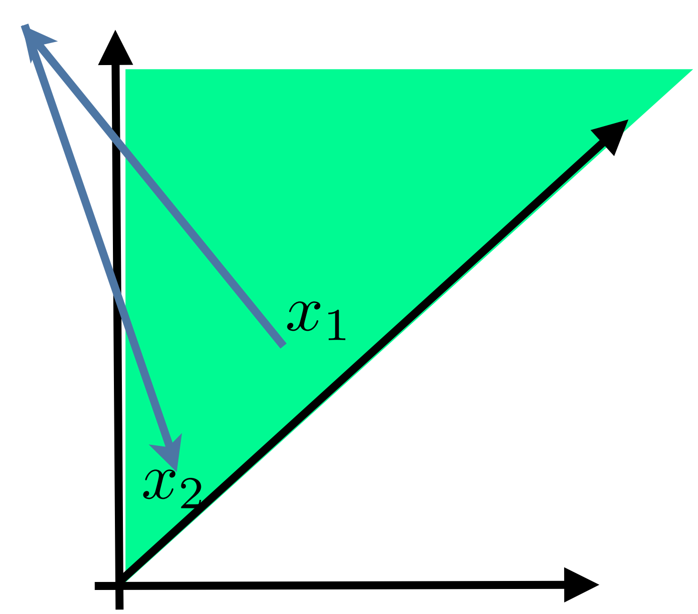
$$x_1 \in R, x_1 + a_1t_1 \in R, x_1 + a_1t_1 + a_2t_2 \in R, \ldots$$

$\Uparrow$

$$x_2 = x_1 + a_1t_1' + a_2t_2'$$

$$x_1 \in R, x_2 \in R$$





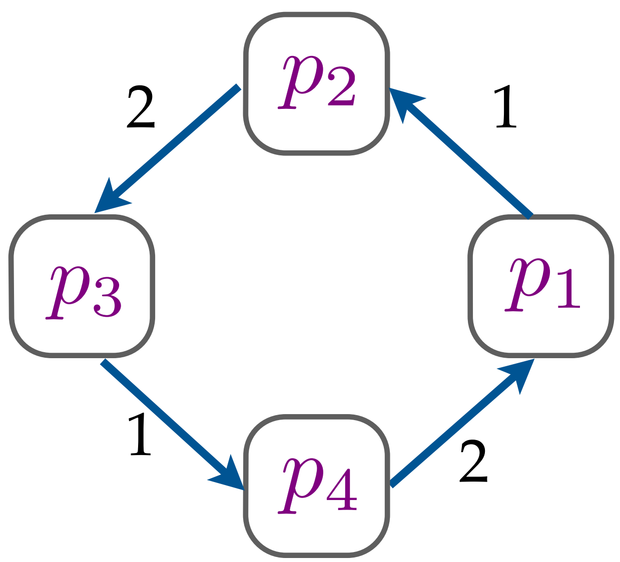
Summary

- Can compute abstractions for PCD and polyhedral hybrid systems
- Quantitative predicate abstraction is sound for a general class of hybrid systems
- What happens if the abstraction fails to deduce stability?
- It returns a counter-example!

Validation: Counter-example Analysis

Counter-example

- If the abstract system fails to prove stability, then it returns a counter-example.

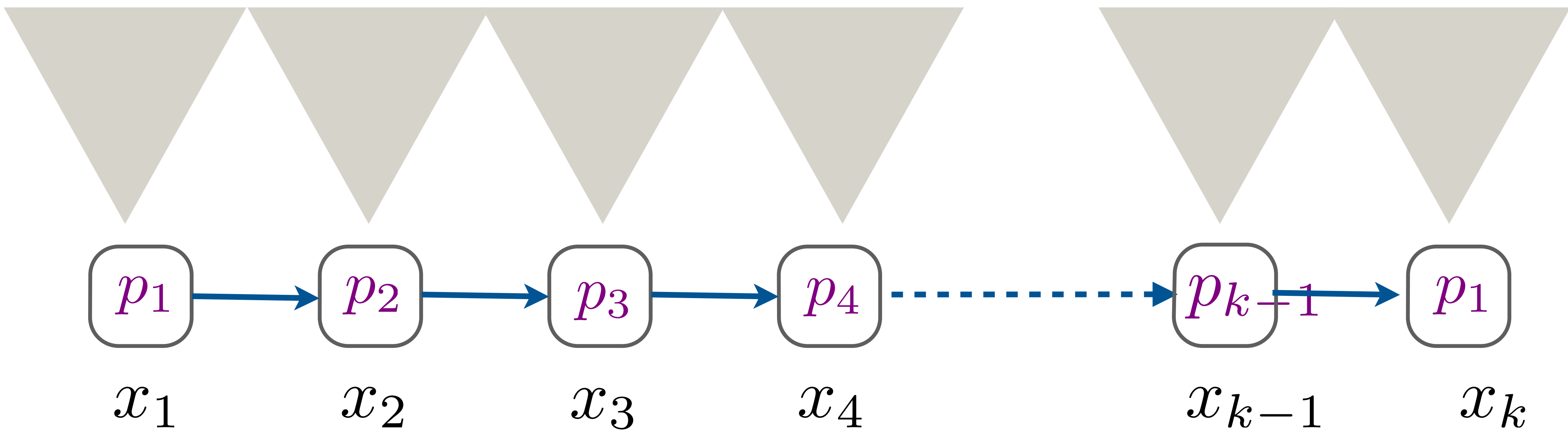


- A cycle with product of weight greater than 1

- Need to check if it is spurious — can the system follow the cycle to exhibit trajectories which diverge

- Validation — checking spuriousness — is not a bounded model-checking problem

Validation



Theorem

A counter example $p_1 \to p_2 \to p_3 \to \cdots \to p_1$ is valid

if and only if

$$\exists \alpha > 1 : x_1 \overset{P_1}{\rightsquigarrow} x_2 \overset{P_2}{\rightsquigarrow} x_3 \ldots \overset{P_k}{\rightsquigarrow} x_k \wedge x_k = \alpha x_1$$

Validation

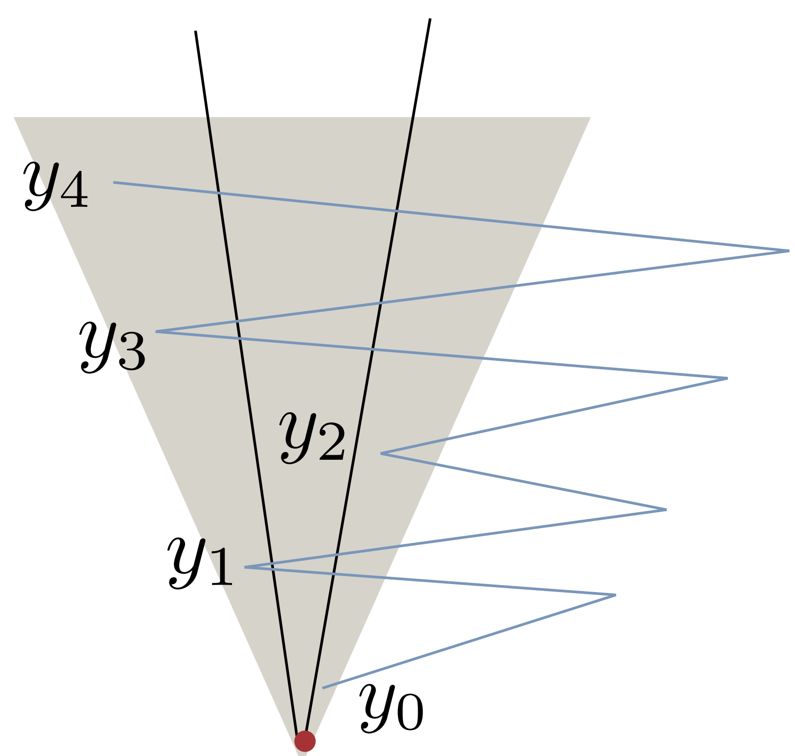
$$\exists \alpha > 1 : x_1 \overset{P_1}{\rightsquigarrow} x_2 \overset{P_2}{\rightsquigarrow} x_3 \ldots \overset{P_k}{\rightsquigarrow} x_k \wedge x_k = \alpha x_1$$

$$y_1 \mapsto \alpha y_1 \mapsto \alpha^2 y_1 \mapsto \alpha^3 y_1$$

Validation

$$y_1 \mapsto y_2 \quad \mapsto y_3 \quad \mapsto y_4$$

Need not have a pair $y_{i+1} = \alpha y_i$ for $\alpha > 1$



Validation

$$G : S \to 2^S$$

$$y \mapsto Y$$

S S

$$\alpha y^* \in G(y^*)$$

Has some similarity with fix point

$$y^* \mapsto y^*$$

Validation

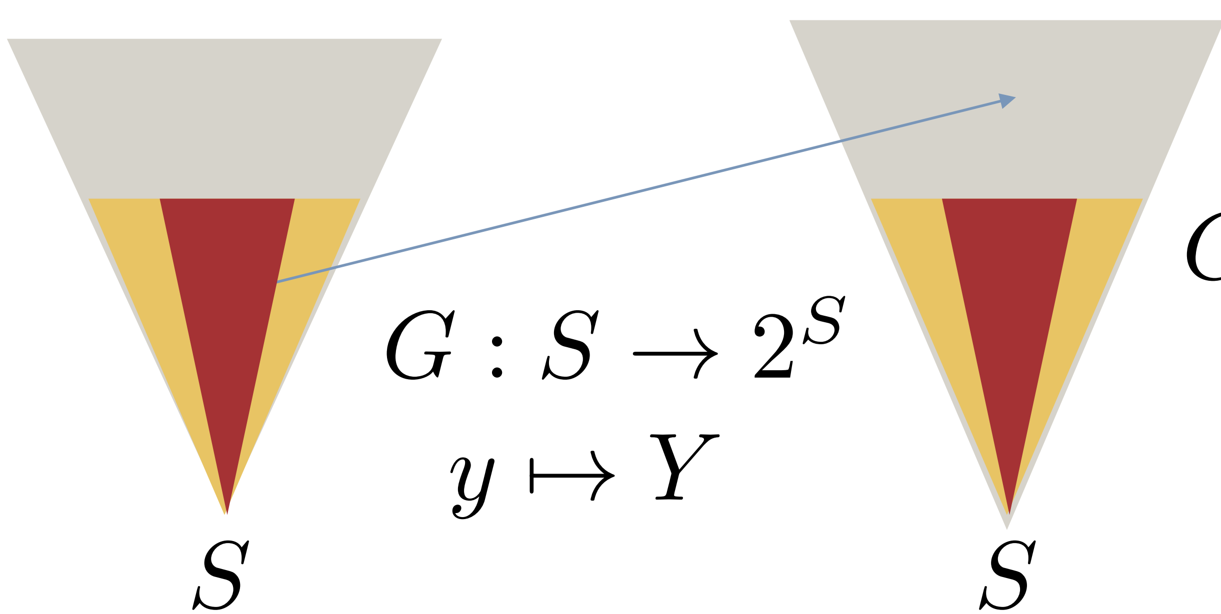
Kakutani's Theorem

Let **S** be a **non-empty, compact and convex** set.

Let **H** be a set-valued function **S** to **S** such that

- its graph is a closed set
- **H(s)** is non-empty and convex for all **s** in **S**

Then **H** has a fixpoint



$$G : S \to 2^S$$
$$y \mapsto Y$$

$$G' : S \to 2^S \text{ given by } s \mapsto \frac{G(s)}{w}$$

S' with states from which there are infinite executions following the cycle

Validation and Refinement Summary

- If the counter-example is spurious, perform a backward propagation along the weights on the edges to compute the point of refinement
- Refine as before by splitting the region at the point of refinement
- Some improvements:
  - If an infinite execution (not necessarily diverging) does not exist, then can try to “eliminate” the cycle.
  - If infinite executions exist, but no diverging executions, then reduce the weight on some edge of the cycle.

Linear Hybrid Systems

Linear dynamical systems

Linear dynamical systems

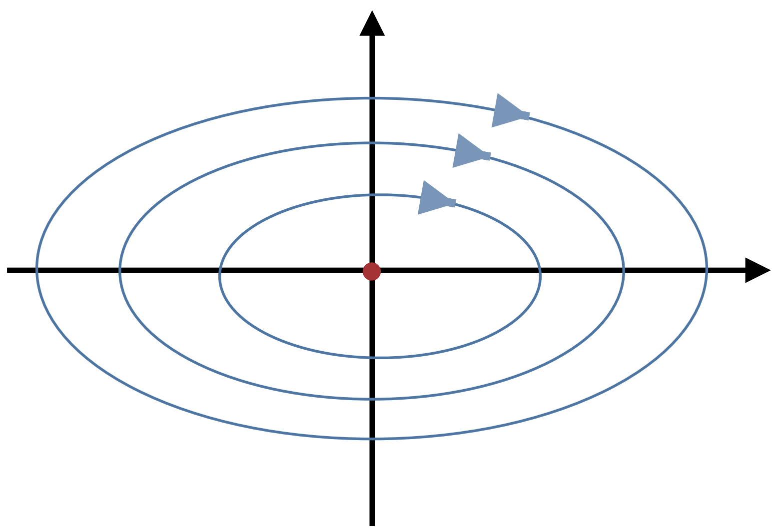
$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

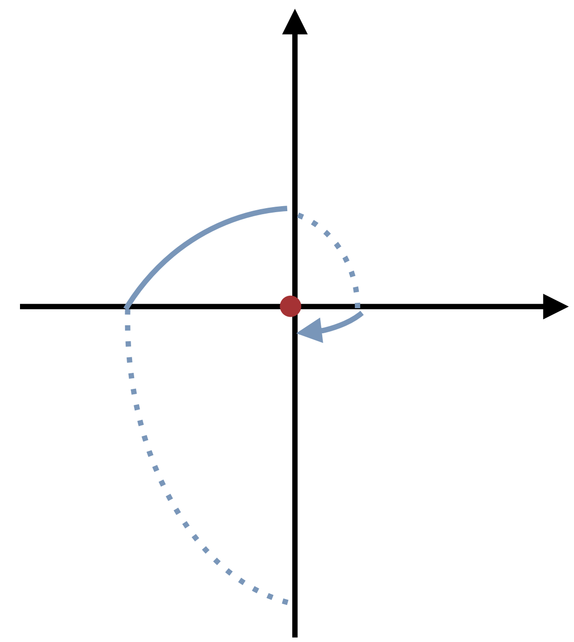
A very important class of control system

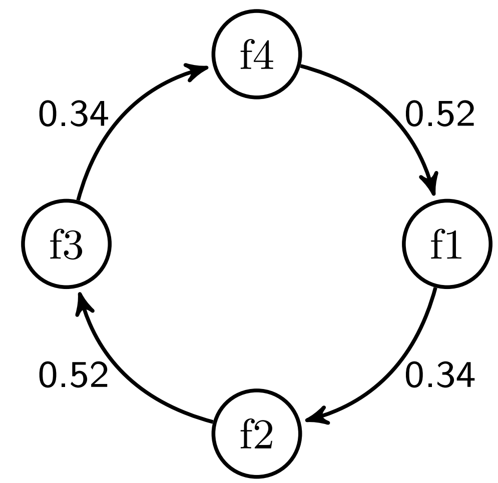
$$Reach(P_1, P, P_2) = \{(s_1, s_2) \mid s_1 \in P_1, s_2 \in P_2, s_1 \overset{P}{\rightsquigarrow} s_2\}$$

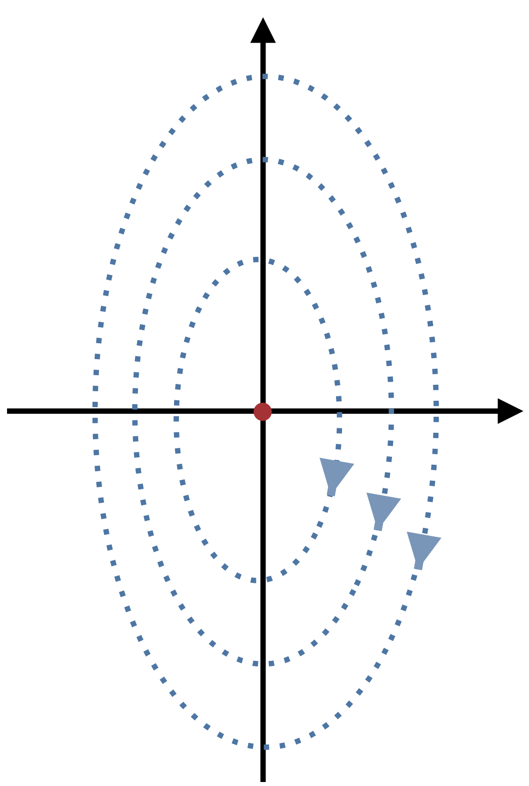
- Solution is an exponential function
- Need a representation on which optimization can be performed
- Approximation methods [Girard et al., Frehse et al., PP]

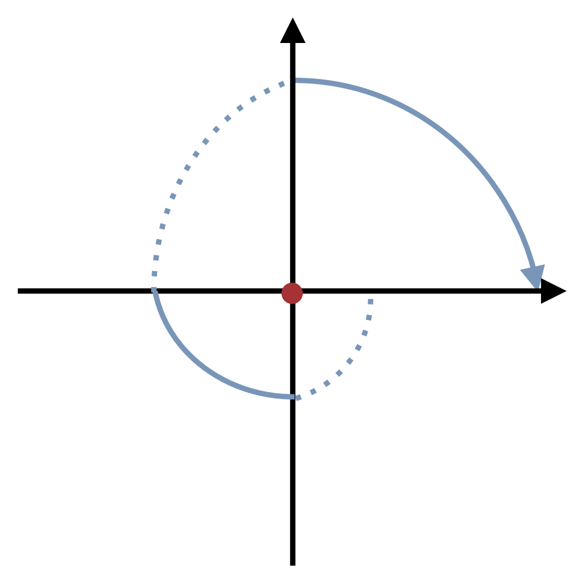
Switched Linear Systems

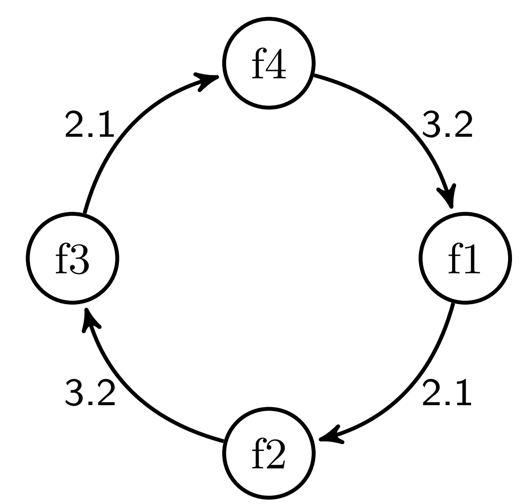




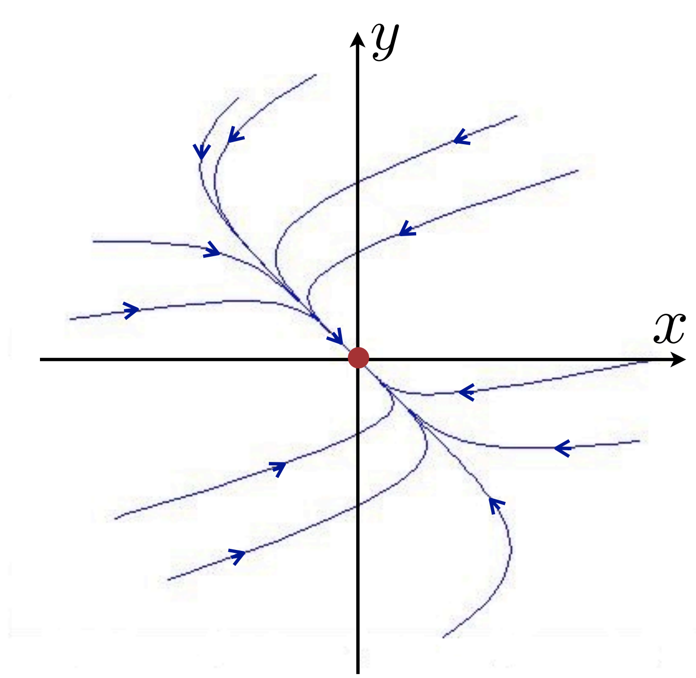


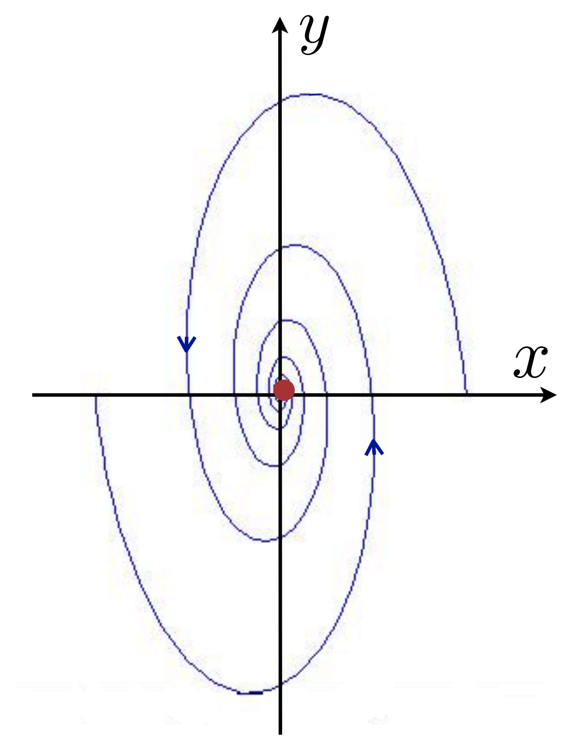


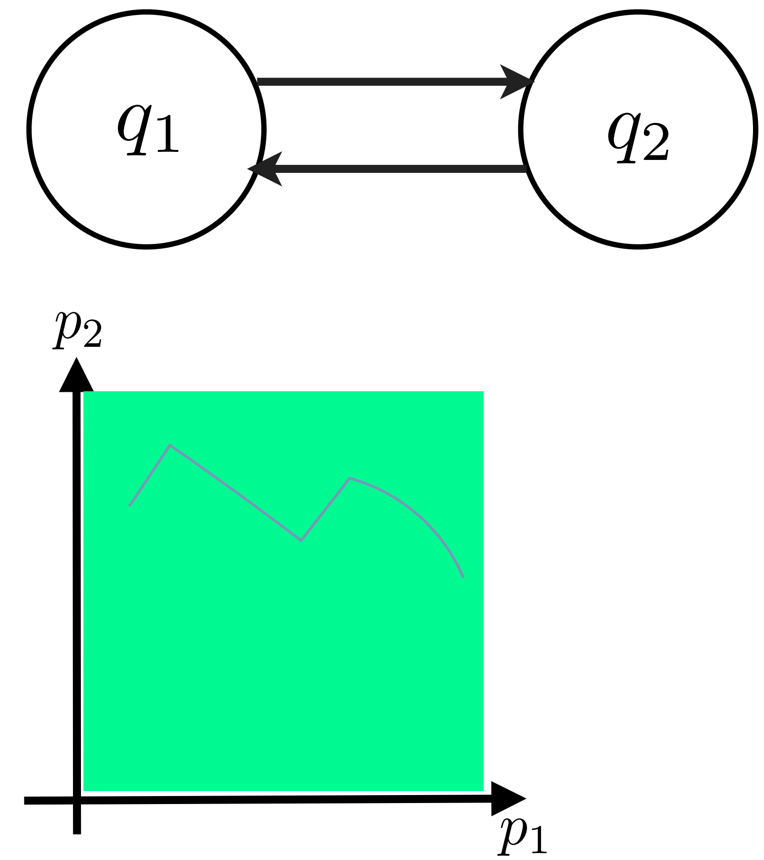




Arbitrary switching example

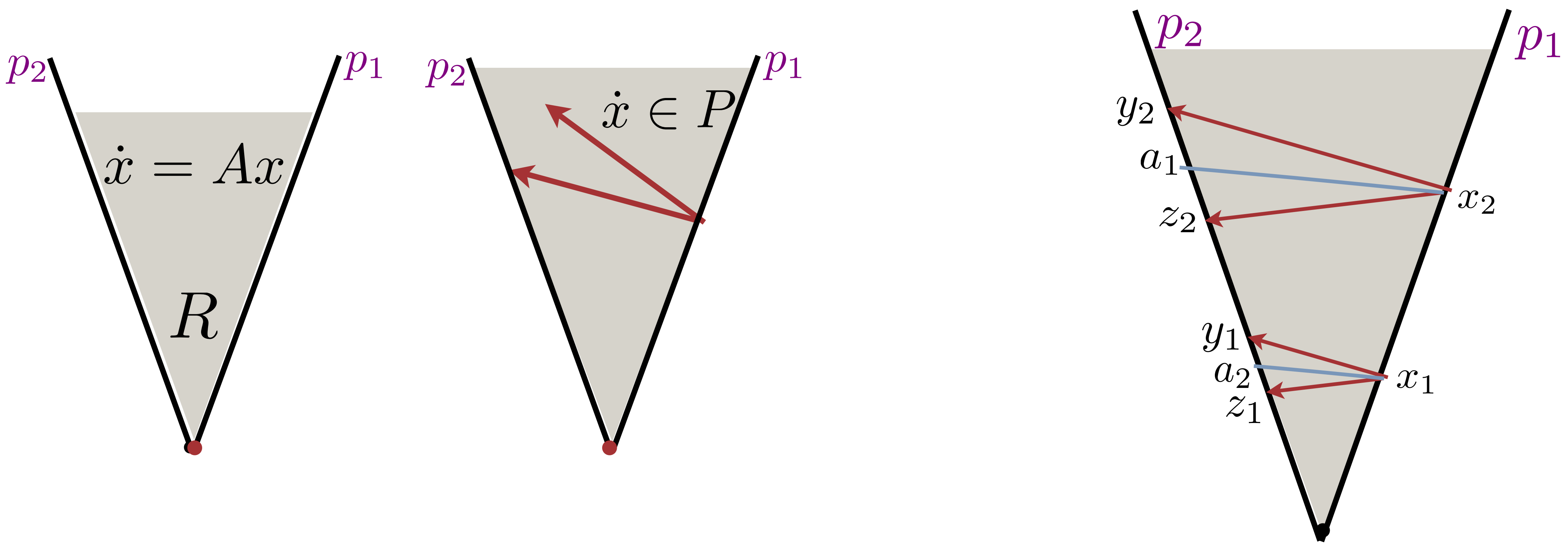






$$V(x) = 19.576{x_1}^6 + 11.627{x_1}^5 x_2 + 15.267{x_1}^4 x_2 + 3.0857{x_1}^3{x_2}^3 + 8.9471{x_1}^2{x_2}^4 - 1.3629 x_1{x_2}^5 + 1.0539{x_2}^6.$$

Hybridization for stability



$$P = \{Ax \,|\, x \in R\}$$

- Conical partitions do not ensure bounded error approximation of the reachability relation
- However, they ensure bounded error approximation of the scaling

Completeness for linear systems

Theorem

For every linear dynamical system that is asymptotically stable, there exists a polyhedral hybrid system abstraction that is asymptotically stable.

Proof Idea

$$\dot{x} \in f(x) \qquad \dot{x} \in g(x)$$

$$d(f(x), g(x)) < \epsilon \text{ implies } d(\sigma_f(x_0, t), \sigma_g(x_0, t)) \leq m(\epsilon, T) \text{ for a time bound } T$$

- Inspired from a classical result from differential inclusions theory, that states that if the Hausdorff distance between two differential inclusions is bounded by **g**, then the solutions within time **T** are bounded by some exponential function of **(g, T)**

Completeness for linear systems

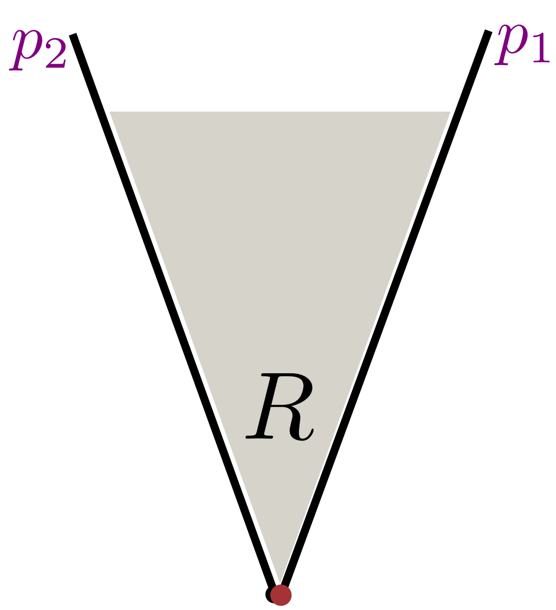
Theorem

For every linear dynamical system that is asymptotically stable, there exists a polyhedral hybrid system abstraction that is asymptotically stable.

Proof Idea

$$\dot{x} \in f(x) \qquad \dot{x} \in g(x)$$

$$d(f(x), g(x)) < \epsilon \text{ implies } d(\sigma_f(x_0, t), \sigma_g(x_0, t)) \leq m(\epsilon, T) \text{ for a time bound } T$$



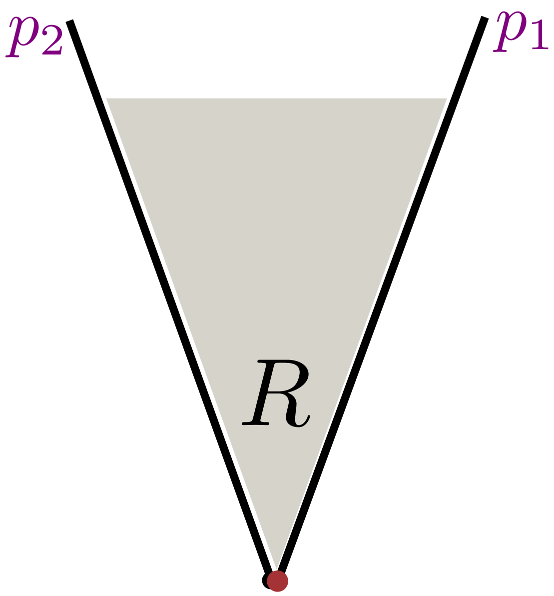
$$\dot{x} = Ax$$
$$\dot{x} \in P$$
$$P = \{Ax \mid x \in R\}$$

Polyhedral

$$\dot{x} = Ax$$
$$\dot{x} \in P\|x\|$$
$$d(f(x), g(x)) < \epsilon\|x\|$$

Polyhedral-like

Proof continued ….



$$\dot{x} = Ax$$
$$\dot{x} \in P$$
$$P = \{Ax \mid x \in R\}$$

Polyhedral

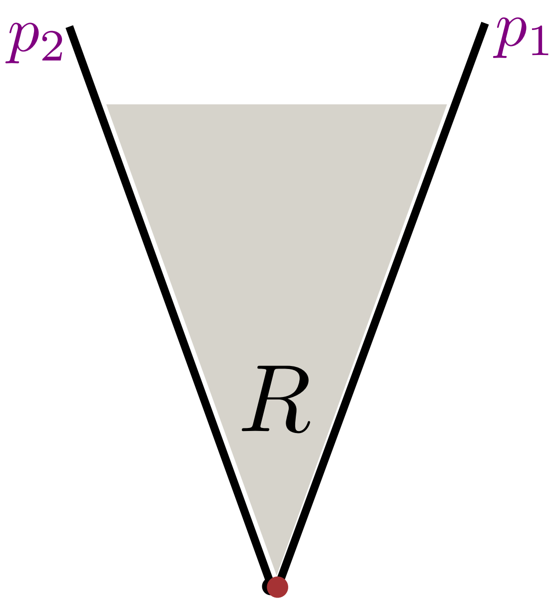
$$\dot{x} = Ax$$
$$\dot{x} \in P\|x\|$$
$$d(f(x), g(x)) < \epsilon\|x\|$$
$$d(\sigma_f(x_0, t), \sigma_g(x_0, t)) < m(\epsilon, T)$$

Polyhedral-like

Polyhedral system stable iff Polyhedral-like system stable

If the linear system is asymptotically stable, then there exists a polyhedral-like system that is stable

Proof continued ….



$$\dot{x} = Ax$$
$$\dot{x} \in P$$
$$P = \{Ax \mid x \in R\}$$

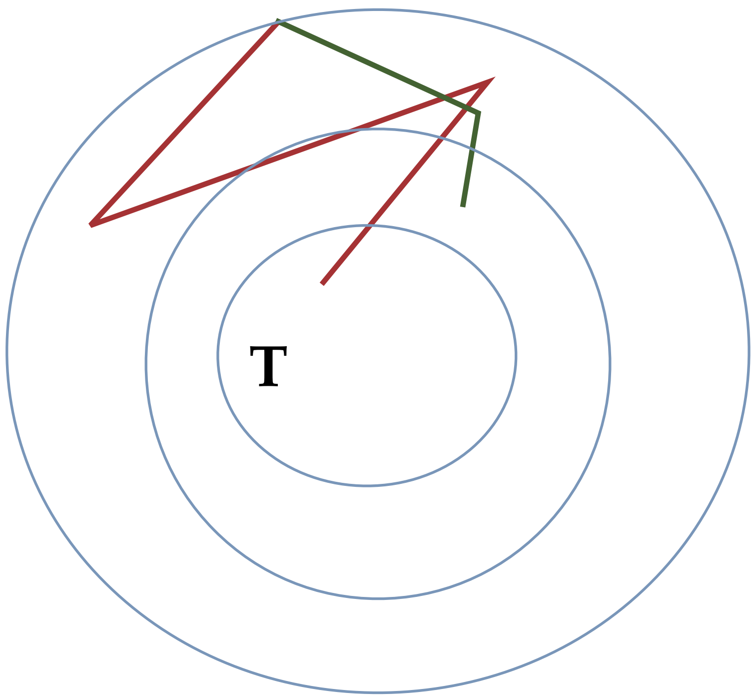
Polyhedral

$$\dot{x} = Ax$$
$$\dot{x} \in P\|x\|$$
$$d(f(x), g(x)) < \epsilon\|x\|$$
$$d(\sigma_f(x_0, t), \sigma_g(x_0, t)) < m(\epsilon, T)$$

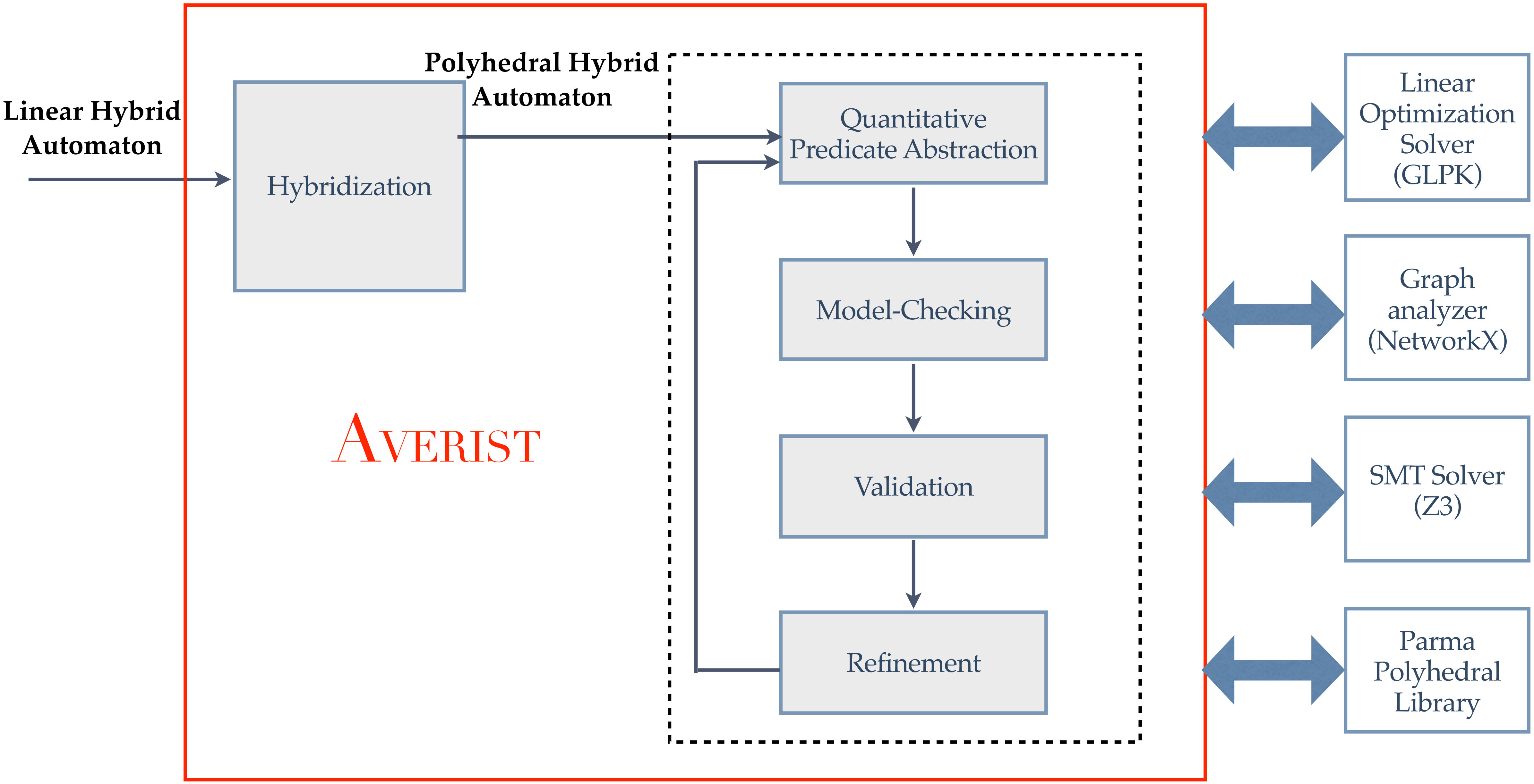
Polyhedral-like

If the linear system is asymptotically stable, then there exists a polyhedral-like system that is stable

Asymptotically stable linear systems are uniformly converging — choose the ϵ such that the error in the solutions between polyhedral-like and linear systems is bounded by 1/4 for the time **T** it takes for the trajectories of the linear system to be 1/2 the distance where they started



AVERIST : Algorithmic VERIfier for STability



Experiments

		AVERIST			STABHYLI		
Dimension / name		Regions	Runtime	Proved Stability	Degree	LF found	Runtime
2D	AS1	129	31	Yes	6	Yes	8
	SS4 1	9	<1	Yes	8	–	452
	SS8 1	17	<1	Yes	6	–	443
	SS16 1	33	1	Yes	4	–	177
3D	AS 4	147	194	Yes	6	–	410
	SS4 4	771	484	Yes	2	Yes	75
	SS8 4	771	470	Yes	2	Yes	15
	SS16 4	771	568	Yes	2	Yes	138
4D	AS 7	81	625	Yes	2	–	12
	SS4 7	81	119	Yes	2	–	101
	SS8 7	153	234	Yes	2	–	1071
	SS16 7	297	533	Yes	2	–	339
	AS 9	–	out	No	4	Yes	34
	SS4 9	81	125	Yes	4	–	105
	SS8 9	153	247	Yes	2	–	16

Lyapunov's method suffers from numerical instability

- 6th degree polynomial returned, but no 8th degree polynomial
- LF found for arbitrary switched system, but not for restricted switched system
- Common LF found, but no multiple LF

AVERIST

- Prove stability in many more cases than Stabhyli
- The verification time increases slower with respect to the number of regions as compared to the degree of the polynomial
- Abstraction computation is parallelizable
- Stabhyli can handle non-linear hybrid systems

Conclusion

- An algorithmic verification method for stability analysis based on abstraction-refinement and hybridization
- Works for polyhedral and linear hybrid systems
- Future Work: Non-linear systems and case studies

References

- *Pre-orders for reasoning about stability.*
  P. Prabhakar, G. E. Dullerud, M. Viswanathan. HSCC'12
- *Pre-orders for reasoning about stability properties with respect to inputs of hybrid systems.*
  P. Prabhakar, J. Liu, R. M. Murray. EMSOFT'13
- *On the decidability of stability of hybrid systems.*
  P. Prabhakar, M. Viswanathan. HSCC'13
- *Abstraction based model-checking of stability of hybrid systems.*
  P. Prabhakar, M. G. Soto. CAV'13
- *An algorithmic approach to stability verification of polyhedral switched systems.*
  P. Prabhakar, M. G. Soto. ACC'14
- *Foundations for Quantative predicate abstraction for stability analysis of hybrid systems.*
  P. Prabhakar, M. G. Soto. VMCAI'15
- *Hybridization for stability analysis of switched linear systems.*
  P. Prabhakar, M. G. Soto. HSCC'16