Reachability through Abstraction

Hybrid Systems: Reachability

Goran Frehse

February 22, 2017

Ph.D. Course: Hybrid Systems
Ph.D. in Information Technology
Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB)
Politecnico di Milano

Overview

- Reachability Based on Abstractions
  - Simulation Relations
  - Hybridization
  - Approximate Simulation
- Reachability through Numerical Simulation

Simulation Relations[1]

State-Transition System $T = (S, \rightarrow, s^0)$,

- set of states S,
- transition relation $s \rightarrow s'$,
- initial state $s^0 \in S$.

Simulation Relation $\preceq \subseteq S_1 \times S_2$ **:**

$$s_1 \preceq s_2 \quad \text{if} \quad s_1 \rightarrow_1 s_1' \Rightarrow s_2 \rightarrow_2 s_2' \text{ with } s_1' \preceq s_2'.$$

T_2 **simulates** T_1 if $s_1^0 \preceq s_2^0$.

---

[1] R. Milner, "An algebraic definition of simulation between programs," in *Proc. of the 2nd Int. Joint Conference on Artificial Intelligence. London, UK, September 1971*, D. C. Cooper, Ed., William Kaufmann, British Computer Society, 1971, pp. 481–489.

Simulation Relations

Simulation relations **preserve safety** properties:

Given $s_1^0 \preceq s_2^0$, **bad** states B_1, let the **abstraction** of B_1

$$\alpha_{\preceq}(B_1) = \{s_2 \in S_2 \mid \exists b_1 \in B_1 : b_1 \preceq s_2\},$$

If $\alpha_{\preceq}(B_1)$ is unreachable in T_2, then B_1 is unreachable in T_1.

Simulation Relations for Hybrid Automata

State-transition **semantics** $[\![H]\!] = (S, \to, s^0)$,

- set of states $S = \text{Loc} \times \mathbb{R}^X$,
- transition relation $s \to s'$:
  - $s \xrightarrow{\delta} s'$: s' reachable through elapse of δ time
  - $s \xrightarrow{\alpha} s'$: s' reachable through transition α
- initial state $s^0 \in S$.

H_2 **simulates** H_1: $[\![H_2]\!]$ simulates $[\![H_1]\!]$

Overview

- Reachability Based on Abstractions
  - Simulation Relations
  - Hybridization
  - Approximate Simulation
- Reachability through Numerical Simulation

Phase-Portait Approximation & Hybridization[2]

H_1 and H_2 identical except in each location the flow

$$H_1: \quad \dot{\mathbf{x}} \in f_1(\mathbf{x}) \qquad\qquad H_2: \quad \dot{\mathbf{x}} \in f_2(\mathbf{x})$$

satisfies $f_1(\mathbf{x}) \subseteq f_2(\mathbf{x})$. Then H_2 simulates H_1 with

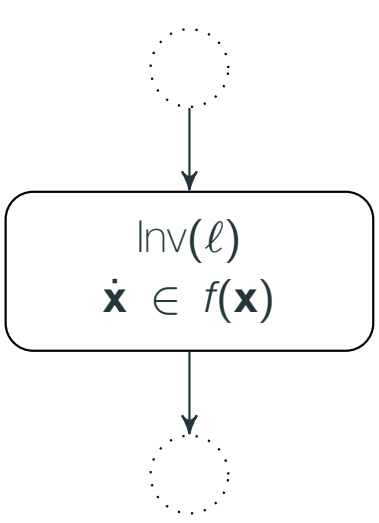
$$s_1 \preceq s_2 \quad \equiv \quad s_1 = s_2$$

$$\Rightarrow \alpha_{\preceq}(B_1) = B_1.$$

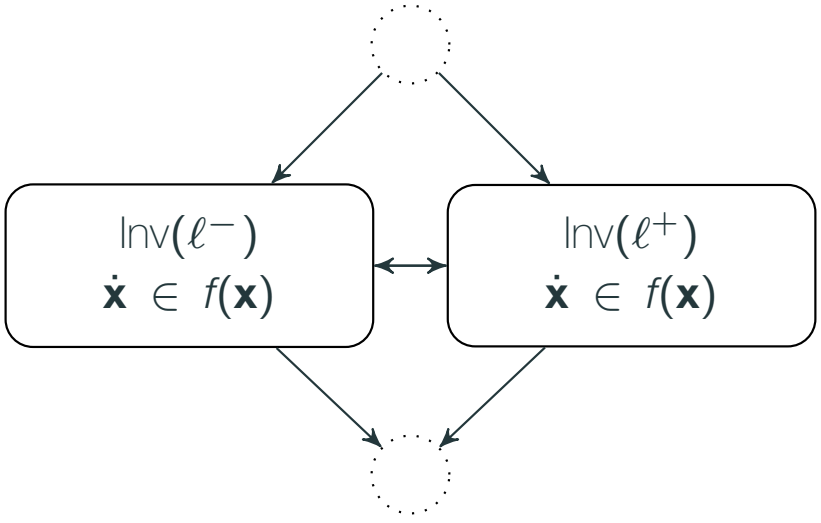
---

[2] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi, "Algorithmic analysis of nonlinear hybrid systems," *IEEE Transactions on Automatic Control*, vol. 43, pp. 540–554, 1998.

Phase-Portait Approximation & Hybridization



(a) H_1



(b) H_2

H_2 simulates H_1 if jumps unobservable and

$$\text{Inv}(\ell) \subseteq \text{Inv}(\ell^-) \cup \text{Inv}(\ell^+)$$

$$\Rightarrow \alpha_{\preceq}(B_1) = B_1|_{\ell \to \ell^-} \cup B_1|_{\ell \to \ell^+}.$$

Approximating Nonlinear Dynamics

approximate nonlinear dynamics

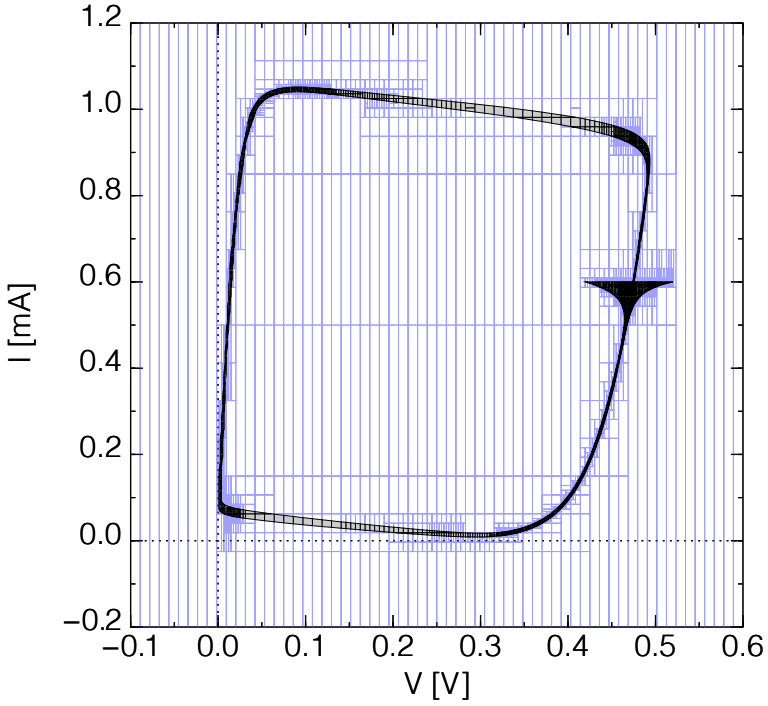
$$\dot{\mathbf{x}} \in f(\mathbf{x})$$

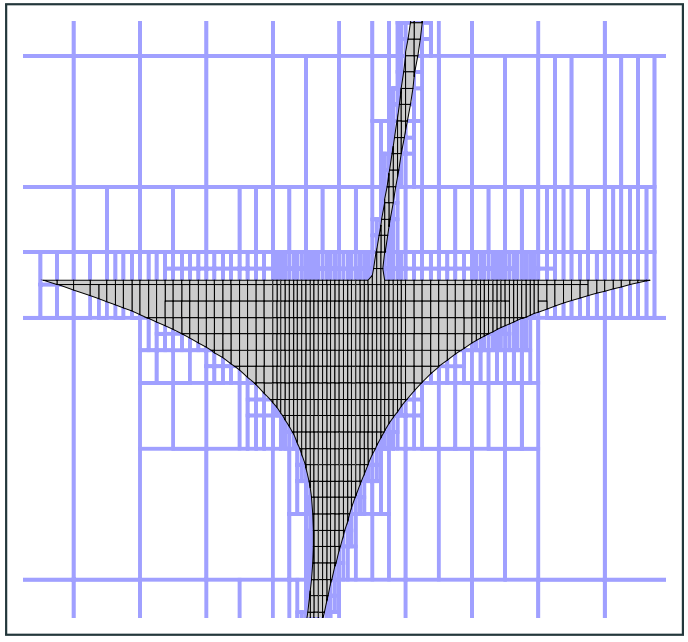
with piecewise constant dynamics $\dot{\mathbf{x}} \in \mathcal{Q}$

$$\mathcal{Q} = \{ f(\mathbf{x}) \mid \mathbf{x} \in \mathrm{Inv}(\ell) \}$$

splitting invariant reduces approximation error

Example: 2-dim. Tunnel Diode Oscillator[3]





tiny invariants for high precision, not scalable

[3] G. Frehse, B. H. Krogh, R. A. Rutenbar, and O. Maler, "Time domain verification of oscillator circuit properties," in *FAC'05*, ser. ENTCS, vol. 153, 2006, pp. 9–22.

Approximating Nonlinear Dynamics

approximate nonlinear dynamics

$$\dot{\mathbf{x}} \in f(\mathbf{x})$$

with piecewise affine dynamics $\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{b} + \mathbf{u}, \mathbf{u} \in \mathcal{U}$

linearization:

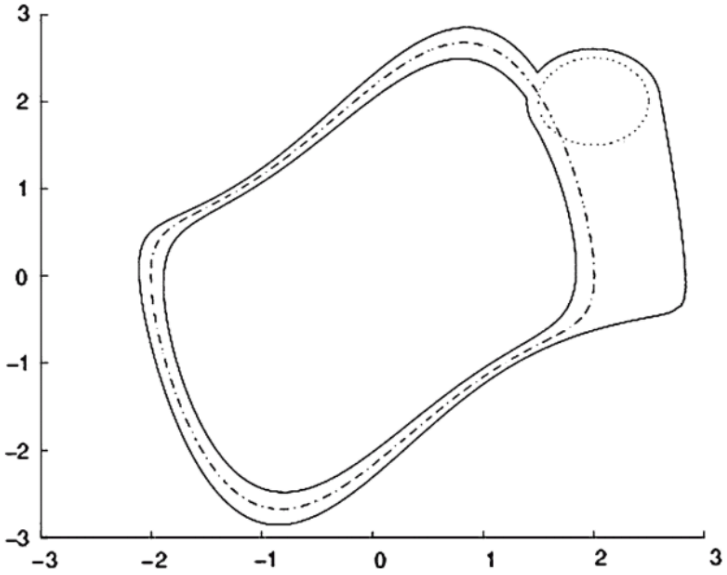
$$a_{ij} = \frac{\partial f_i}{\partial x_j}(\mathbf{x}_0), \quad \mathbf{b} = f(\mathbf{x}_0) - A\mathbf{x}_0.$$

approximation error:

$$\mathcal{U} = \{\, f(\mathbf{x}) - (A\mathbf{x} + \mathbf{b}) \mid \mathbf{x} \in \mathrm{Inv}(\ell) \,\}.$$

Example: Van der Pol Oscillator[4]

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= y(1 - x^2) - x \end{aligned}$$



hybridization with partition of size 0.05

partitioning doesn't scale well $\Rightarrow$ use sliding window

[4] E. Asarin, T. Dang, and A. Girard, "Hybridization methods for the analysis of nonlinear systems," *Acta Inf.*, vol. 43, no. 7, pp. 451–476, 2007.

Overview

- Reachability Based on Abstractions
  - Simulation Relations
  - Hybridization
  - Approximate Simulation
- Reachability through Numerical Simulation

Simulation Relations

matching identical traces:

$$s_1 \preceq s_2 \text{ only if } p(s_1) = p(s_2)$$

$\Rightarrow$ T_2 may be much simpler than T_1

bisimilar if $s_1 \preceq s_2$ and $s_2 \preceq^{\mathsf{T}} s_1$ are simulation relations.

identifying bisimilar states in a system
$\Rightarrow$ accelerate analysis through on-the-fly minimization

Simulation Relations for Continuous Systems

observed trace of $x(t)$:

$$p(x(t)) = p(x_0) + \frac{\partial p(x_0)}{\partial x}\frac{\dot{x}(0)}{1!}t + \frac{\partial^2 p(x_0)}{\partial x^2}\frac{\dot{x}(0)^2}{2!}t^2 + \frac{\partial p(x_0)}{\partial x}\frac{\ddot{x}(0)}{2!}t^2 + \cdots$$

contains state information, since

$$x(t) = x(0) + \frac{\dot{x}(0)}{1!}t + \frac{\ddot{x}(0)}{2!}t^2 + \cdots$$

identical traces $\rightsquigarrow$ equivalent dynamics

except in particular cases.[5]

---

[5] A. van der Schaft, "Equivalence of dynamical systems by bisimulation," *IEEE transactions on automatic control*, vol. 49, no. 12, pp. 2160–2172, 2004.

Approximate Simulation (Girard, Julius, Pappas '08)[6]

matching ε-close observable behavior:

$$\mathbf{x}_1 \preceq_\varepsilon \mathbf{x}_2 \text{ only if } \|p(\mathbf{x}_1) - p(\mathbf{x}_2)\| \leq \varepsilon$$

$\Rightarrow$ traces from $\mathbf{x}_1$ and $\mathbf{x}_2$ never more than ε apart (also in the future)

How close do traces need to be initially?

Approximate Simulation

possible choice:

$$\mathbf{x}_1 \preceq_\varepsilon \mathbf{x}_2 \equiv \|p(\mathbf{x}_1) - p(\mathbf{x}_2)\| \leq \varepsilon$$

applicable if contractive:

$$\tfrac{d}{dt}\|p(\mathbf{x}_1) - p(\mathbf{x}_2)\| \leq 0.$$

better: find upper bound $V(\mathbf{x}_1, \mathbf{x}_2)$ that is contractive

Simulation Functions

a simulation function $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^{\geq 0}$ satisfies

$$V(\mathbf{x}_1, \mathbf{x}_2) \geq \|p(\mathbf{x}_1) - p(\mathbf{x}_2)\|$$

$$\frac{d}{dt} V(\mathbf{x}_1, \mathbf{x}_2) \leq 0$$

simulation relation: $\mathbf{x}_1 \preceq_\varepsilon \mathbf{x}_2 \equiv V(\mathbf{x}_1, \mathbf{x}_2) \leq \varepsilon$

Simulation Functions

with dynamics $\dot{\mathbf{x}}_1 = f_1(\mathbf{x}_1)$, $\dot{\mathbf{x}}_2 = f_2(\mathbf{x}_2)$,

$$\frac{d}{dt}V(\mathbf{x}_1, \mathbf{x}_2) = \frac{\partial V}{\partial \mathbf{x}_1} f_1(\mathbf{x}_1) + \frac{\partial V}{\partial \mathbf{x}_2} f_2(\mathbf{x}_2)$$

computing $V(\mathbf{x}_1, \mathbf{x}_2)$ for

- linear dynamics: linear matrix inequalities,
- polynomial dynamics: sums of squares program

Approximate Simulation for Hybrid Automata[6]

Consider hybrid automata H_1 and H_2 with

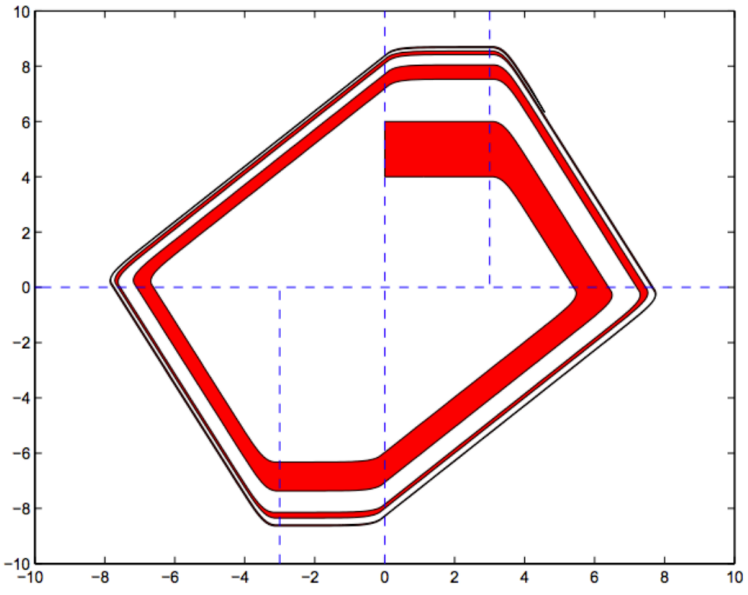
- identical locations and transitions,
- $V(\mathbf{x}_1, \mathbf{x}_2)$ a simulation function in all locations,
- only identity jumps (for simplicity).

Then H_2 ε-simulates H_1 if

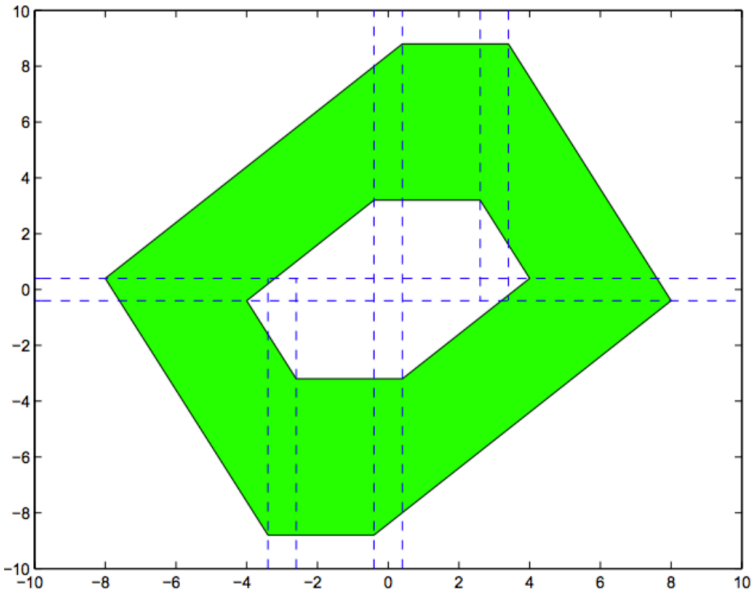
- $\varepsilon \geq \max_{\mathbf{x}_1 \in \mathrm{Init}_1(\ell)} \min_{\mathbf{x}_2 \in \mathrm{Init}_2(\ell)} V(\mathbf{x}_1, \mathbf{x}_2)$,
- $\mathrm{Inv}_2(\ell) \supseteq \alpha_{\preceq_\varepsilon}(\mathrm{Inv}_1(\ell))$,
- $\mathcal{G}_2 \supseteq \alpha_{\preceq_\varepsilon}(\mathcal{G}_1)$.

General case: $V_\ell(\mathbf{x}_1, \mathbf{x}_2)$ location dependent

Example: Patrolling Robot[6]



(a) H_1: piecewise affine dynamics, 6 variables



(b) H_2: pw. constant dynamics, 2 variables, $H_1 \preceq_{0.4} H_2$

reachable states much easier to compute for H_2

Approximate Simulation

Extensions:[6]

- bisimilar time- and state discretization,
- bounded- and unbounded safety verification,
- controller synthesis

[6] A. Girard and G. J. Pappas, "Approximate bisimulation: A bridge between computer science and control theory," *European Journal of Control*, vol. 17, no. 5, pp. 568–578, 2011.

Overview

Reachability Based on Abstractions

Reachability through Numerical Simulation

- Signal Temporal Logic
- Principle
- Variations

Signal Temporal Logic (STL) (Maler, Nickovic, '04)[8]

Signal: $x_i : \mathbb{R}^{\geq 0} \to \mathbb{R} \cup \{\top, \bot\}$

Trace: $w = \{x_1, \ldots, x_N\}$

STL Syntax: variable x_i, time interval I, property φ,

$$\varphi := \text{true} \mid x_i \geq 0 \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \; \mathrm{U}_I \; \varphi,$$

can express boolean and temporal operators (*eventually*, *globally*, etc.) with bounded and unbounded time.

Signal Temporal Logic (STL)

Syntax: $\varphi := \mathrm{true} \mid x_i \geq 0 \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathrm{U}_I \varphi.$

Boolean Semantics:

$$
\begin{aligned}
& w, t \models \mathrm{true} \\
& w, t \models x_i \geq 0 \quad \text{iff} \quad x_i(t) \geq 0 \\
& w, t \models \neg\varphi \quad \text{iff} \quad w, t \not\models \varphi \\
& w, t \models \varphi \wedge \psi \quad \text{iff} \quad w, t \models \varphi \text{ and } w, t \models \psi \\
& w, t \models \varphi \ \mathrm{U}_I \ \psi \quad \text{iff} \quad \exists t' \in t + I : w, t' \models \psi \wedge \\
& \qquad\qquad\qquad\qquad\qquad\qquad \forall t'' \in [t, t'] : w, t'' \models \varphi
\end{aligned}
$$

STL – Quantitative Semantics[7]

Syntax: $\varphi := \text{true} \mid x_i \geq 0 \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \mathrm{U}_I \varphi.$

Quantitative Semantics: robustness estimation

$$
\begin{aligned}
\rho(\text{true}, w, t) &= \top \\
\rho(x_i \geq 0, w, t) &= x_i(t) \\
\rho(\neg\varphi, w, t) &= -\rho(\varphi, w, t) \\
\rho(\varphi \wedge \psi, w, t) &= \min\{\rho(\varphi, w, t), \rho(\psi, w, t)\} \\
\rho(\varphi \ \mathrm{U}_I \ \psi, w, t) &= \sup_{t' \in t+I} \min\Big\{\rho(\psi, w, t'), \\
&\qquad \inf_{t'' \in [t,t']} \rho(\phi, w, t'')\Big\}
\end{aligned}
$$

[7] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theor. Comp. Science*, vol. 410, no. 42, pp. 4262–4291, 2009.

STL – Quantitative Semantics

sign of $\rho(\varphi, w, t)$ determines satisfaction status of φ

magnitude of $\rho(\varphi, w, t)$ determines robustness :

any trace w' satisfies ϕ if

$$\|w - w'\|_\infty < \rho(\varphi, w, t).$$

STL – Quantitative Semantics

for piecewise linear w, $\rho(\varphi, w, t)$ computable in time[8]

$$\mathcal{O}\left(|\varphi| \cdot d^{h(\varphi)} \cdot |w|\right),$$

- $|\varphi|$: number of nodes in AST
- $h(\varphi)$: depth of AST
- d : constant
- $|w|$: number of breakpoints

[8] A. Donzé, T. Ferrere, and O. Maler, "Efficient robust monitoring for stl," in *Computer Aided Verification*, Springer, 2013, pp. 264–279.

Overview

Reachability Based on Abstractions

Reachability through Numerical Simulation

- Signal Temporal Logic
- Principle
- Variations

Reachability through Numerical Simulation

Asumptions:

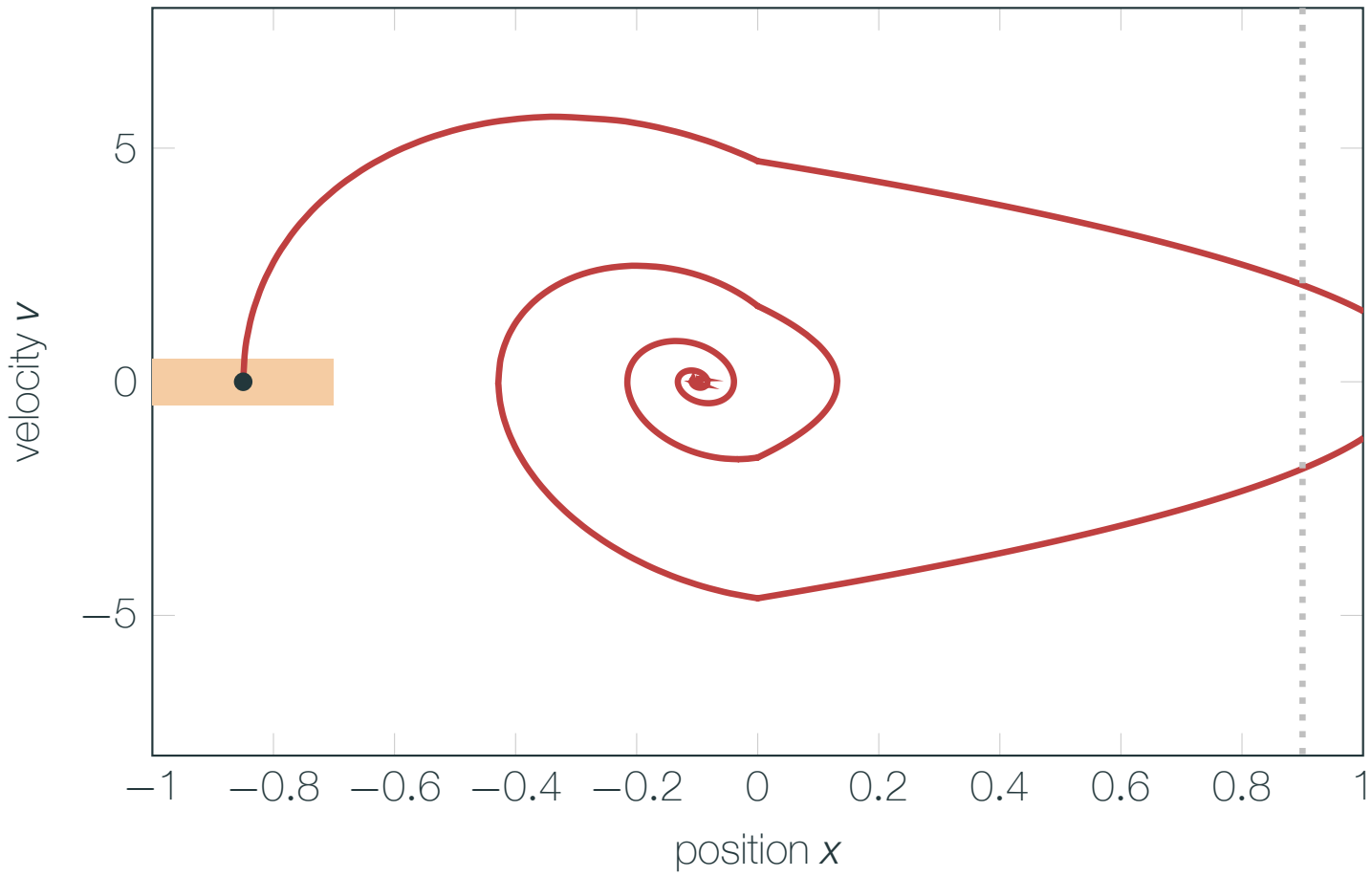
- assume computed traces sufficiently accurate
- equivalent neighborhood of initial state identifiable

Principle:

- sample initial states
- decide property on traces
- extend result to equivalent sets of initial states

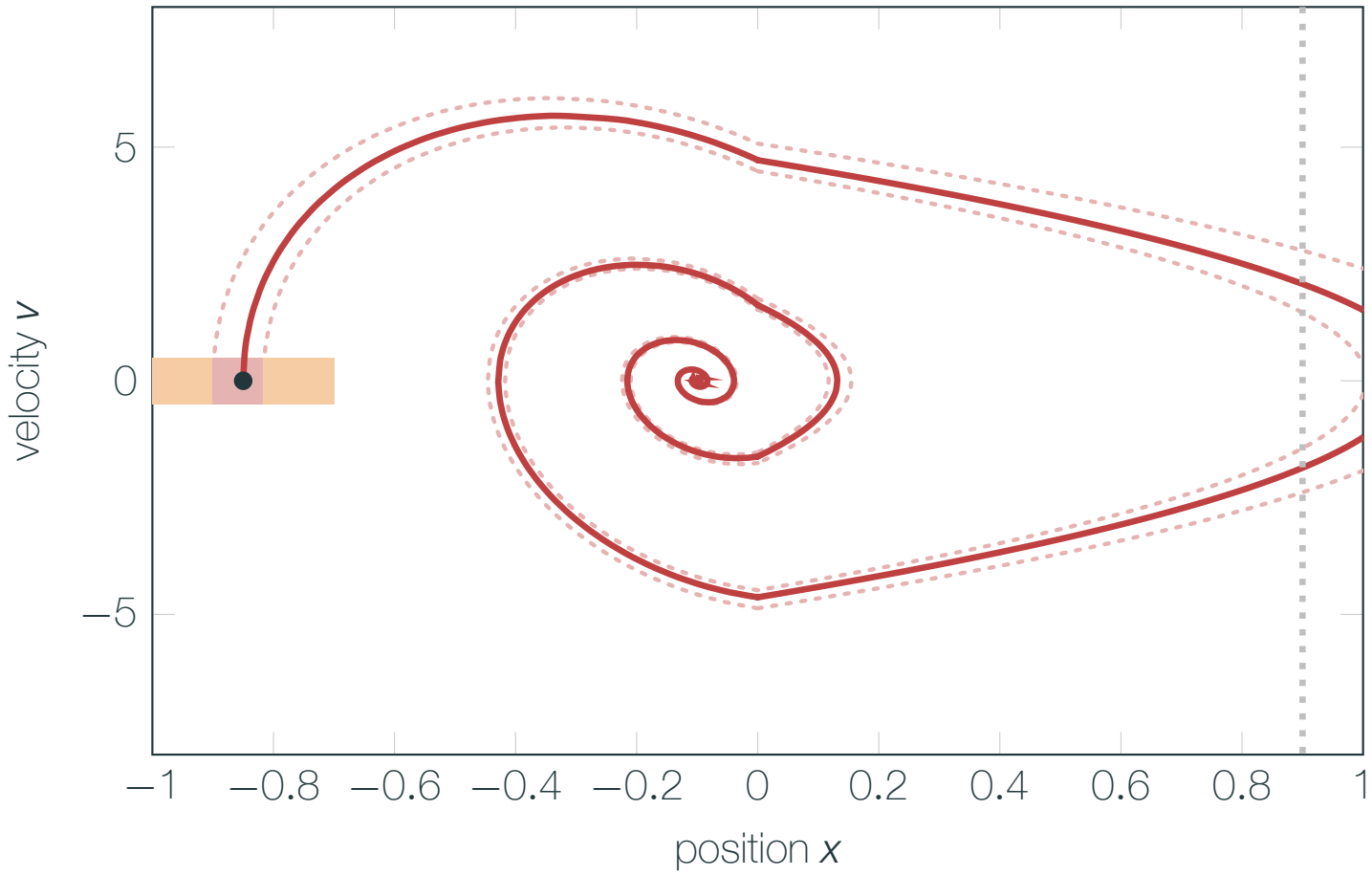
sampling of initial states limited to low dimensional sets

Reachability through Numerical Simulation



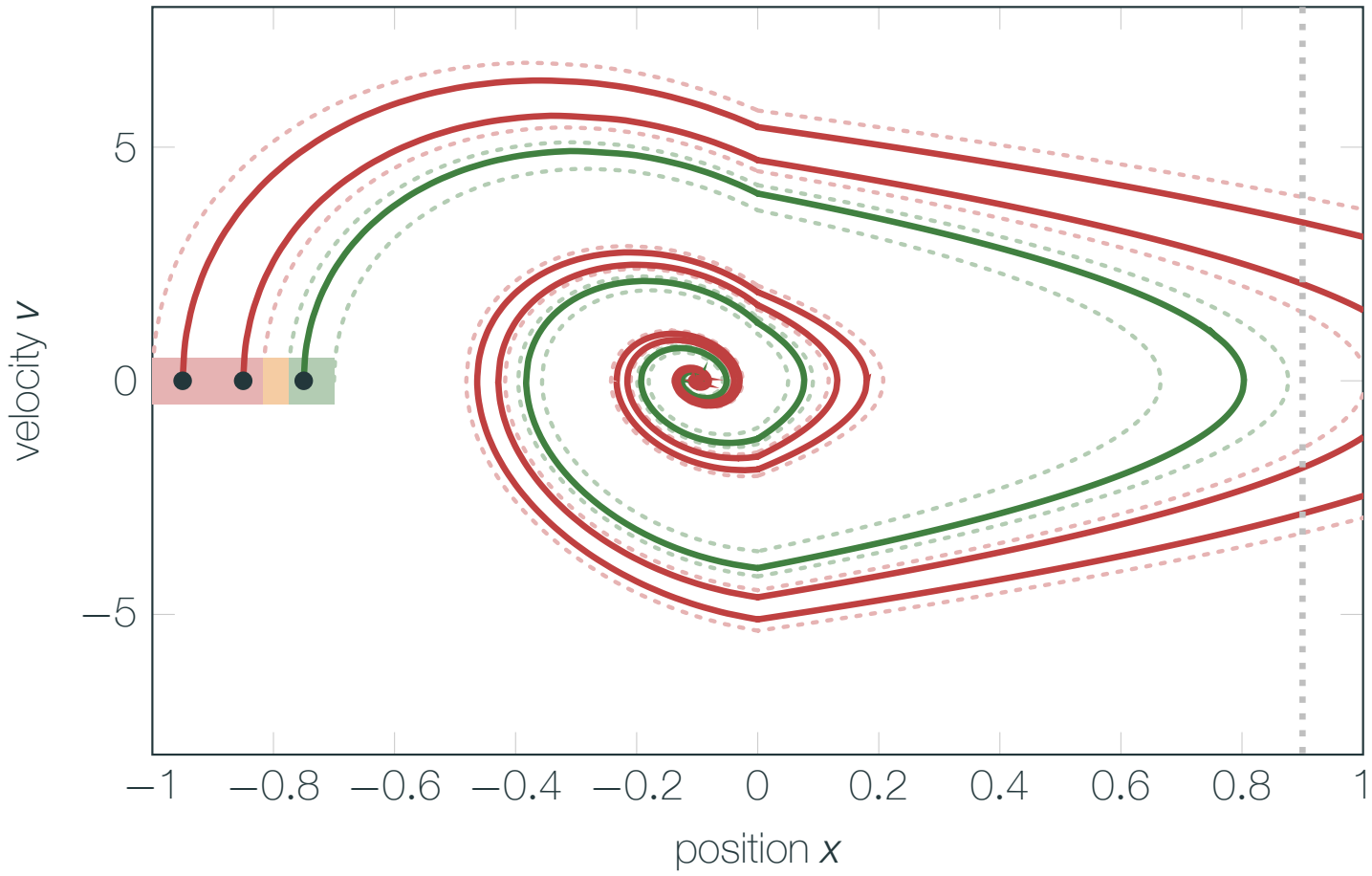
trace violates property $x \leq 0.9$ with robustness 0.1

Reachability through Numerical Simulation



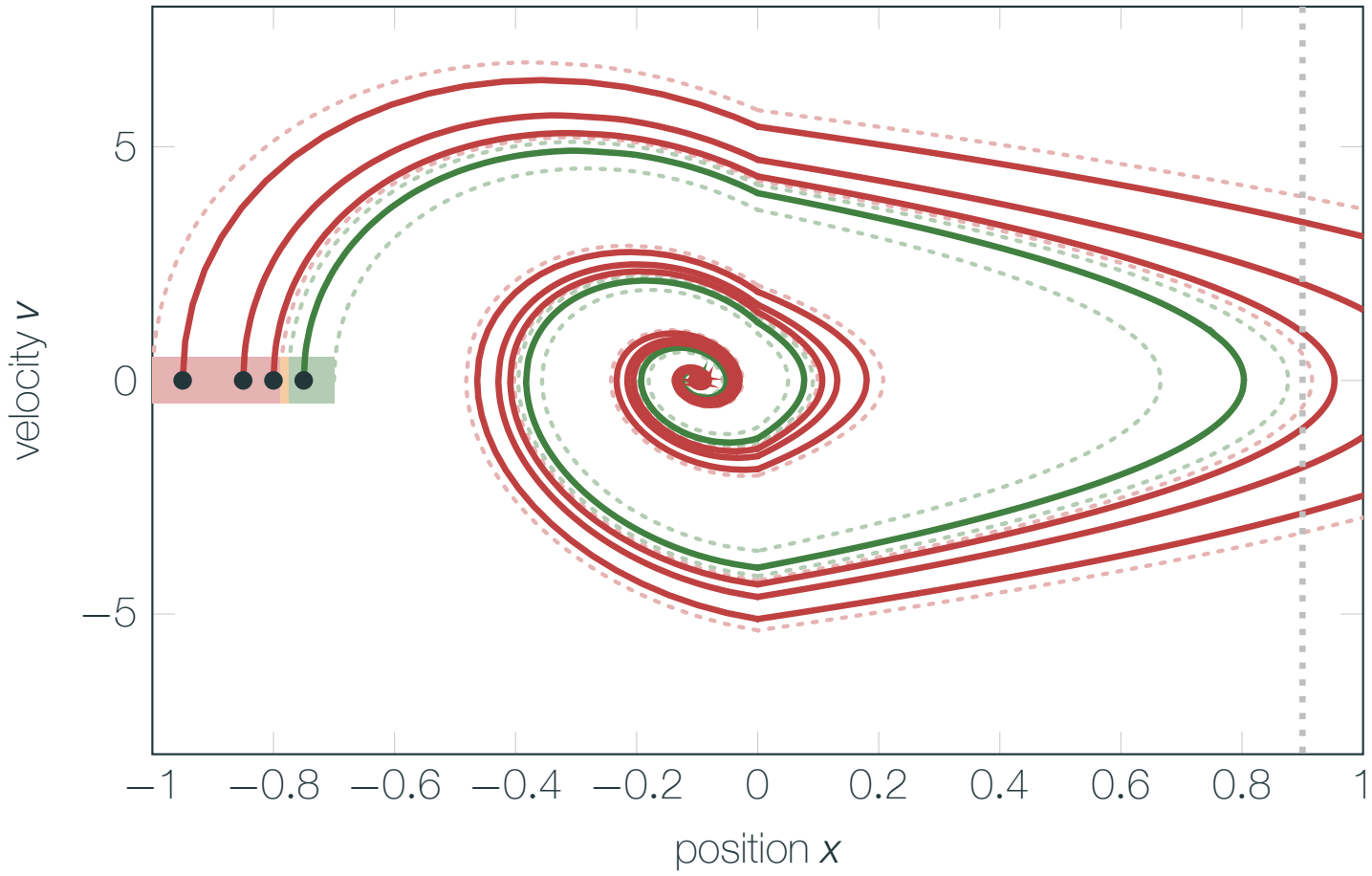
identify equivalent initial states and mark as decided

Reachability through Numerical Simulation



repeat: compute traces, identify equivalent initial states

Reachability through Numerical Simulation



stop when desired coverage achieved

Overview

Reachability Based on Abstractions

Reachability through Numerical Simulation

- Signal Temporal Logic
- Principle
- Variations

Finding Equivalent Initial States

using bisimulation:

$$\mathbf{x}_1 \preceq_\varepsilon \mathbf{x}_2 \quad \Rightarrow \quad \|w_{\mathbf{x}_1} - w_{\mathbf{x}_2}\| \leq \varepsilon$$

given robustness of $w_{\mathbf{x}_1}$, obtain neighborhood from $V(\mathbf{x}_1, \mathbf{x}_2)$

tool with related approach (discrepancy): C2E2 (S. Mitra)[9]

[9] P. S. Duggirala, S. Mitra, M. Viswanathan, and M. Potok, "C2e2: A verification tool for stateflow models," in *TACAS'15*, Springer.

Finding Equivalent Initial States

using sensitivity:[10]

- with sensitivity information from ODE solver:
  influence of variations of the initial state on variation of robustness
- black-box capable
- extends to parameter synthesis

tool: Breach (A. Donzé)

[10] A. Donzé and O. Maler, "Robust satisfaction of temporal logic over real-valued signals," in *FORMATS'10*, Springer, 2010.

Falsification[11]

search counter-example that falsifies the property

- use statistics or optimization to pick next initial state
- black-box capable
- no claim for confirming property
- suitable for path-planning

tool: S-TaLiRo (G. Fainekos)

[11] S. Sankaranarayanan and G. Fainekos, "Falsification of temporal properties of hybrid systems using the cross-entropy method," in *HSCC'12*.

References

[6] A. Girard, A. A. Julius, and G. J. Pappas, "Approximate simulation relations for hybrid systems," *Discrete Event Dynamic Systems*, vol. 18, no. 2, pp. 163–179, 2008.

[8] O. Maler and D. Nickovic, "Monitoring temporal properties of continuous signals," in *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, Springer, 2004, pp. 152–166.