
SpaceEx: Scalable Verification of Hybrid Systems

Colas LE GUERNIC

April 29, 2011

joint work with:

Goran Frehse, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel,
Rodolfo Ripado, Antoine Girard, Thao Dang, and Oded Maler.

Introduction

SpaceEx

Hybrid Systems

Example

CMACS

Parameter

Estimation in

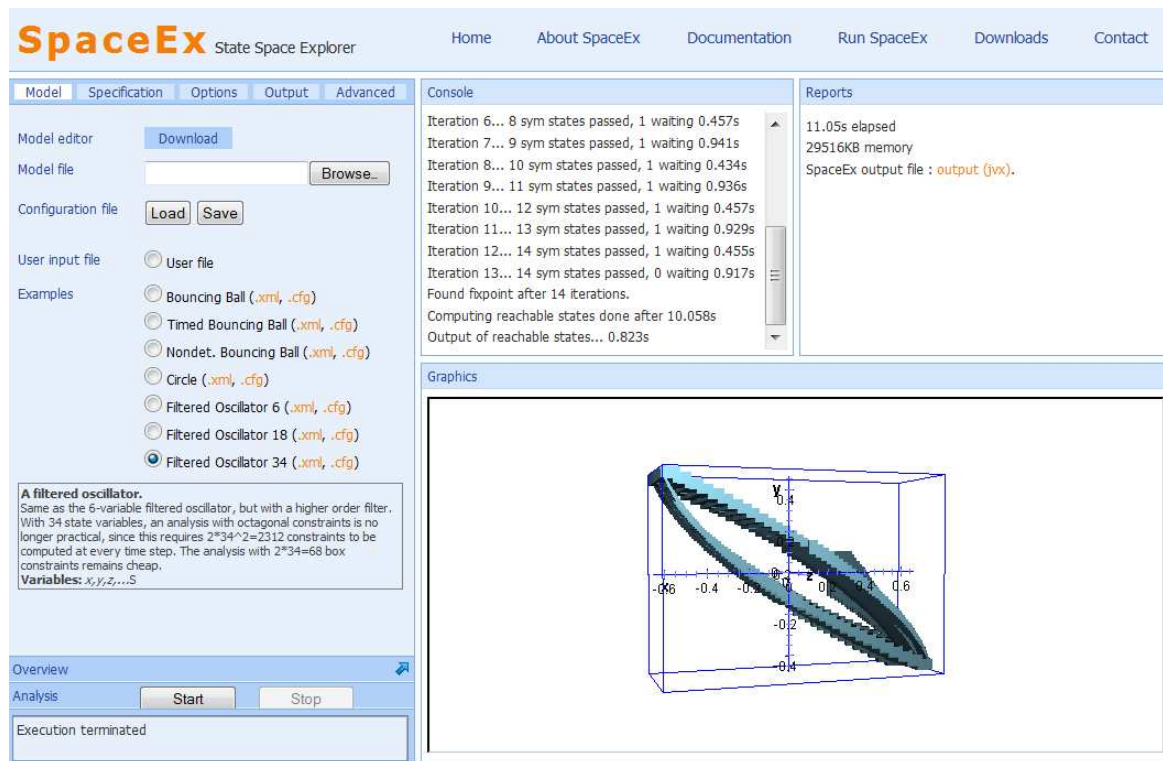
SpaceEx

Reachability Analysis

Support Function

SpaceEx

SpaceEx is a software platform for reachability and safety verification of hybrid systems developed at Verimag.



The screenshot shows the SpaceEx web interface. The top navigation bar includes links for Home, About SpaceEx, Documentation, Run SpaceEx, Downloads, and Contact. The main interface is divided into several sections:

- Model editor:** Includes a 'Download' button, a 'Model file' input field with a 'Browse...' button, and a 'Configuration file' section with 'Load' and 'Save' buttons.
- User input file:** A radio button for 'User file'.
- Examples:** A list of example models with radio buttons:
 - Bouncing Ball (.xml, .cfg)
 - Timed Bouncing Ball (.xml, .cfg)
 - Nondet. Bouncing Ball (.xml, .cfg)
 - Circle (.xml, .cfg)
 - Filtered Oscillator 6 (.xml, .cfg)
 - Filtered Oscillator 18 (.xml, .cfg)
 - Filtered Oscillator 34 (.xml, .cfg)** (selected)
- Console:** A log window showing the progress of an analysis:


```
Iteration 6... 8 sym states passed, 1 waiting 0.457s
Iteration 7... 9 sym states passed, 1 waiting 0.941s
Iteration 8... 10 sym states passed, 1 waiting 0.434s
Iteration 9... 11 sym states passed, 1 waiting 0.936s
Iteration 10... 12 sym states passed, 1 waiting 0.457s
Iteration 11... 13 sym states passed, 1 waiting 0.929s
Iteration 12... 14 sym states passed, 1 waiting 0.455s
Iteration 13... 14 sym states passed, 0 waiting 0.917s
Found fixpoint after 14 iterations.
Computing reachable states done after 10.058s.
Output of reachable states... 0.823s
```
- Reports:** A window showing summary information:


```
11.05s elapsed
29516KB memory
SpaceEx output file : output (jvx).
```
- Graphics:** A 3D plot showing a complex, curved surface representing the reachable set of a filtered oscillator. The axes are labeled X, Y, and Z, with values ranging from approximately -0.6 to 0.6.
- Overview:** A section with 'Start' and 'Stop' buttons, and a status message: 'Execution terminated'.

<http://spaceex.imag.fr/>

Introduction

SpaceEx

Hybrid Systems

Example

CMACS

Parameter

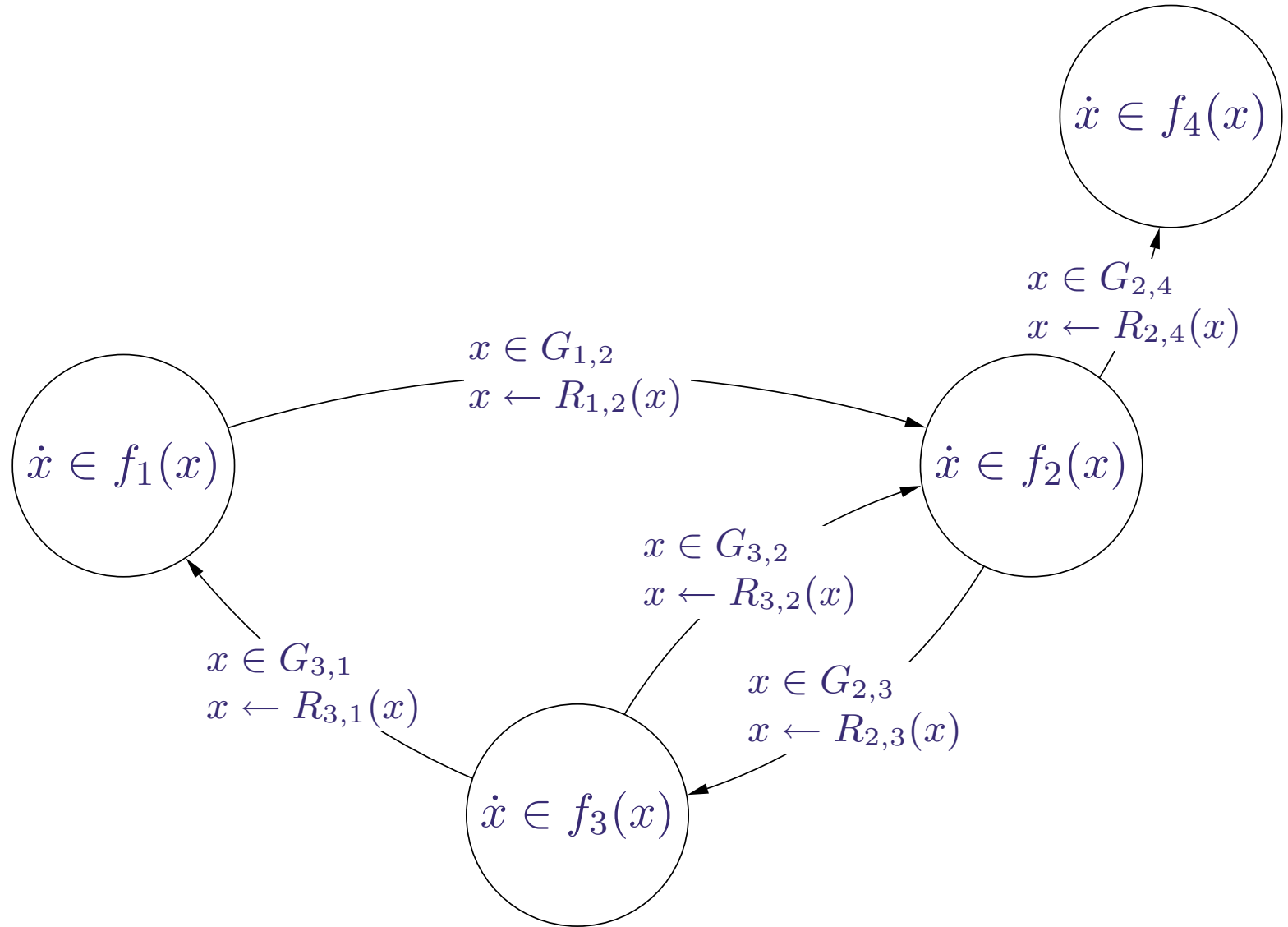
Estimation in

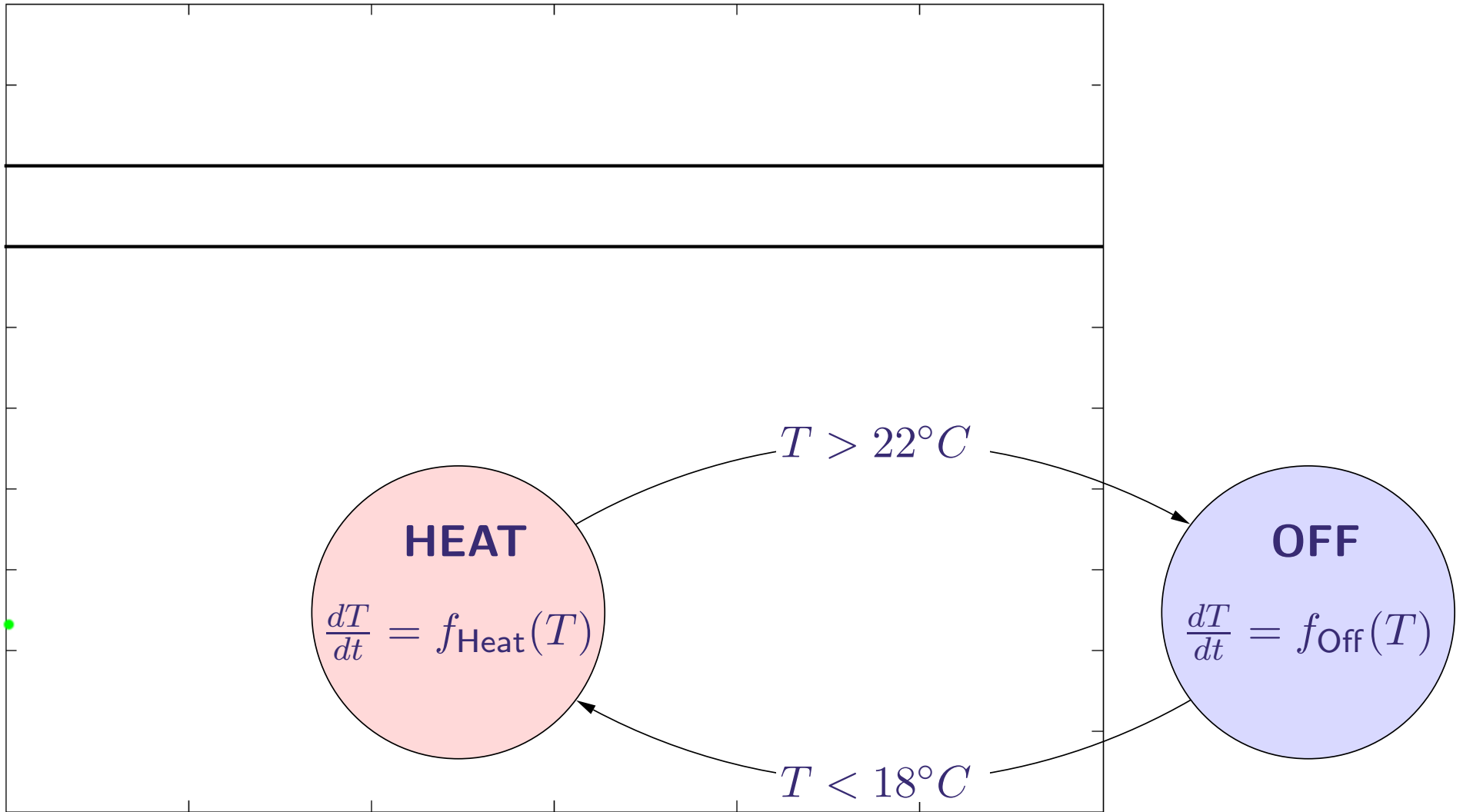
SpaceEx

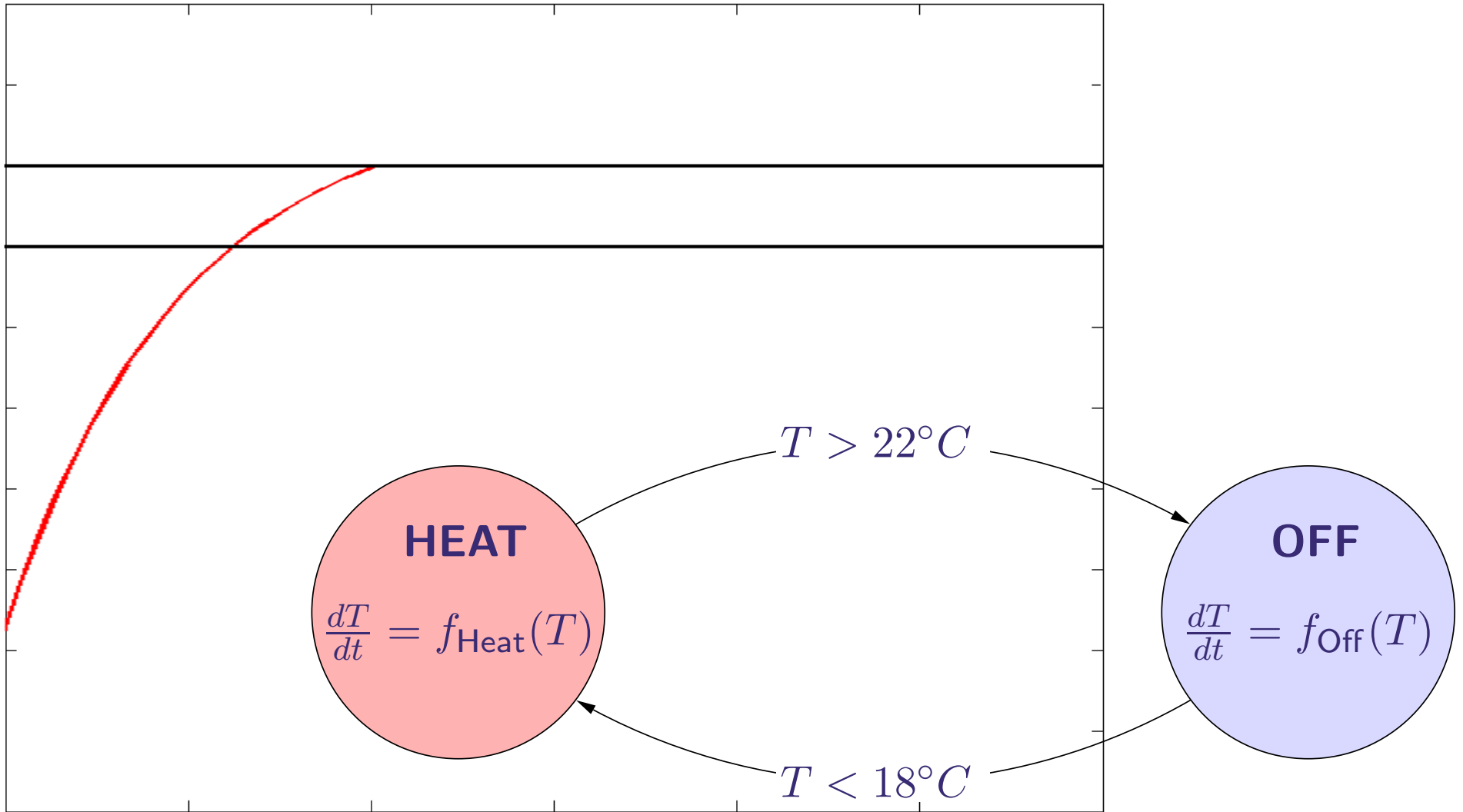
Reachability Analysis

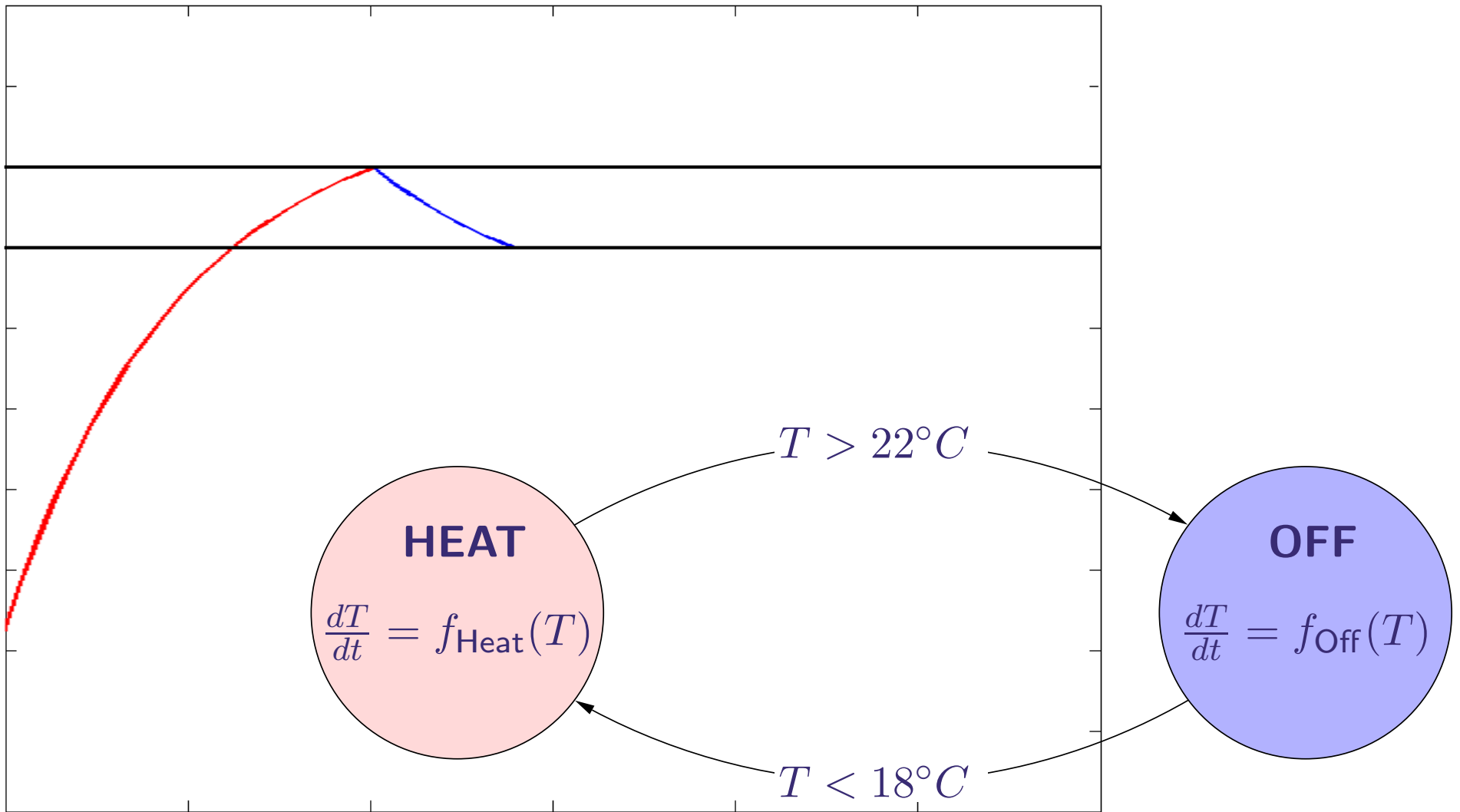
Support Function

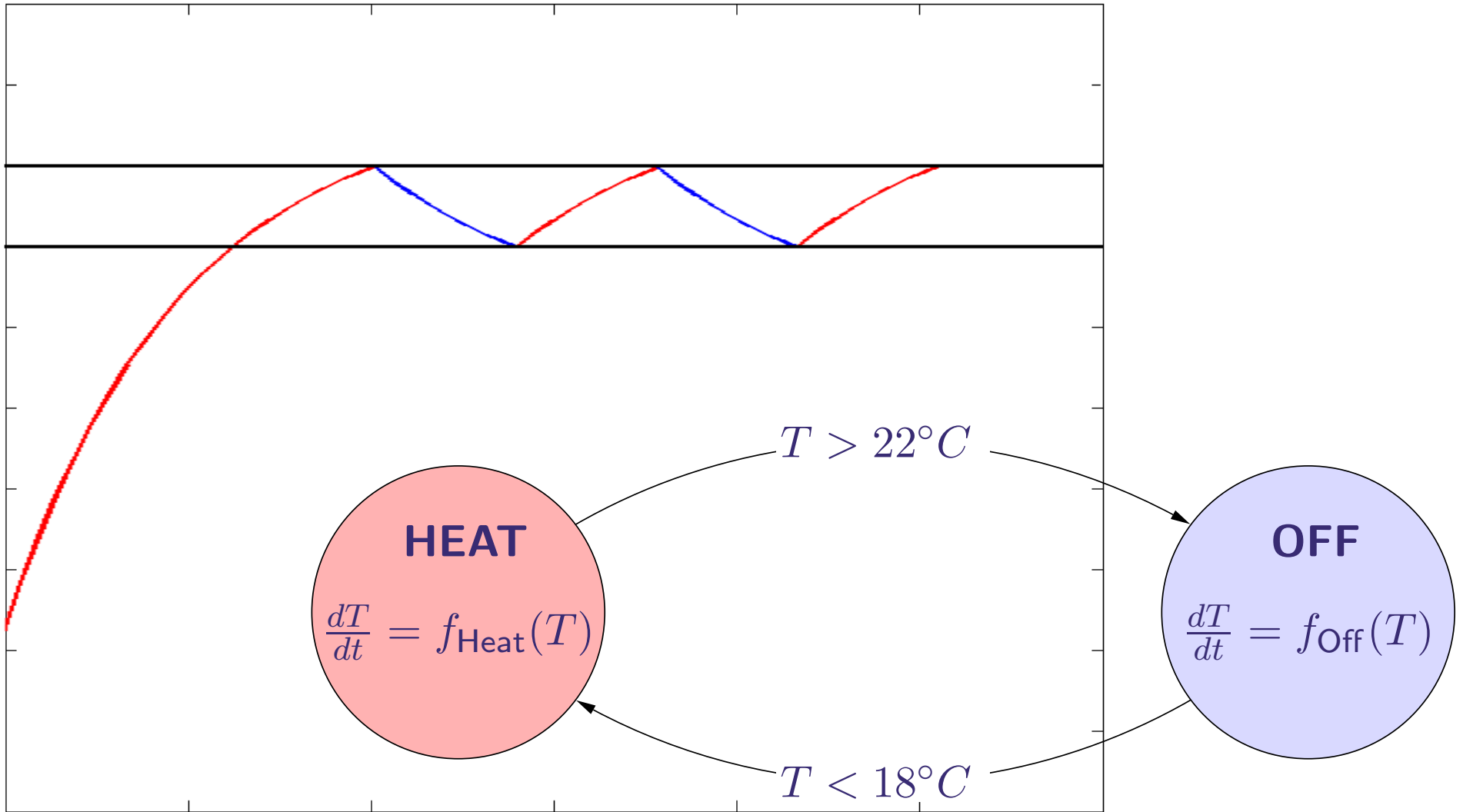
SpaceEx

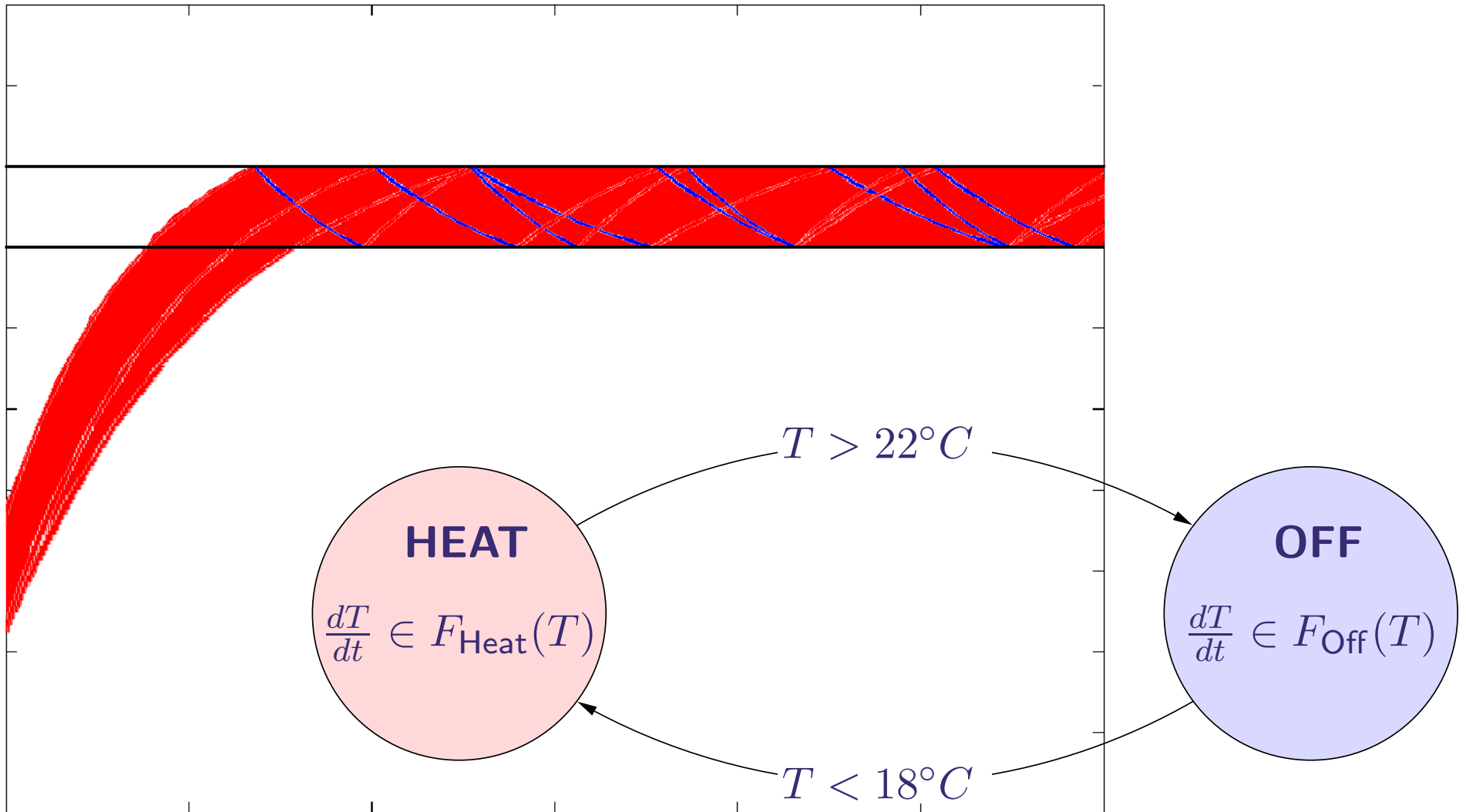












Introduction

SpaceX

Hybrid Systems

Example

CMACS

Parameter

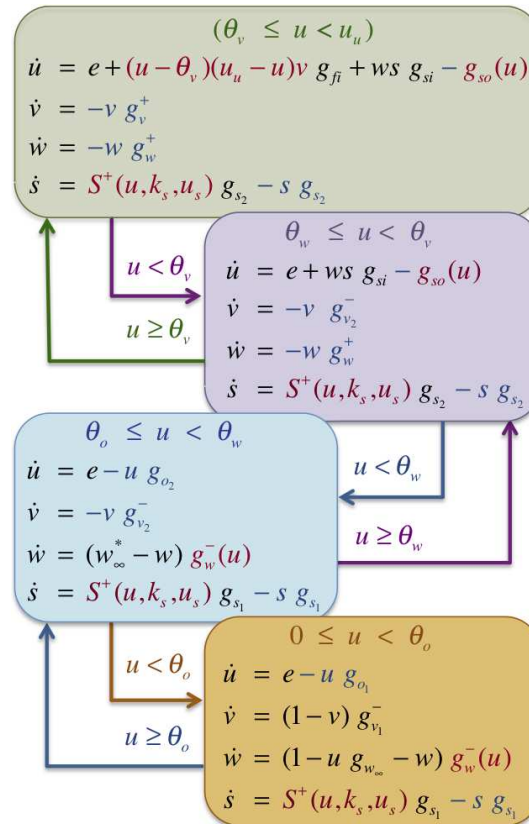
Estimation in

SpaceX

Reachability Analysis

Support Function

SpaceX



Introduction

SpaceX

Hybrid Systems

Example

CMACS

Parameter

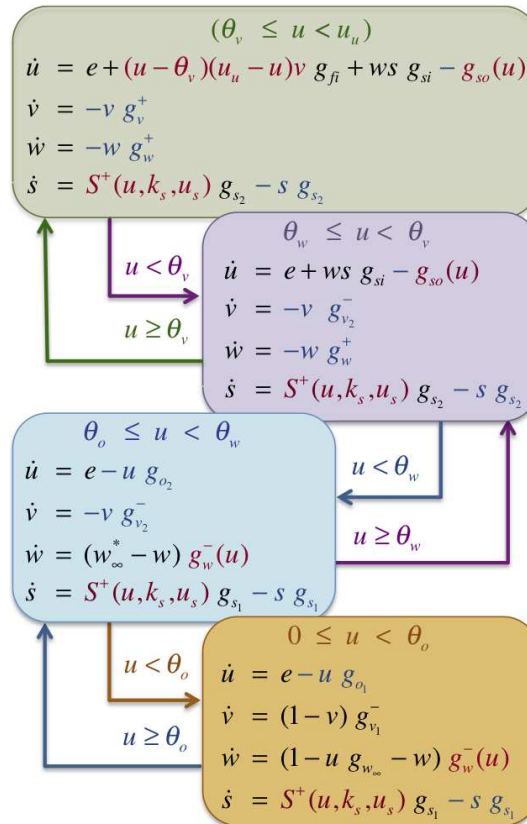
Estimation in

SpaceX

Reachability Analysis

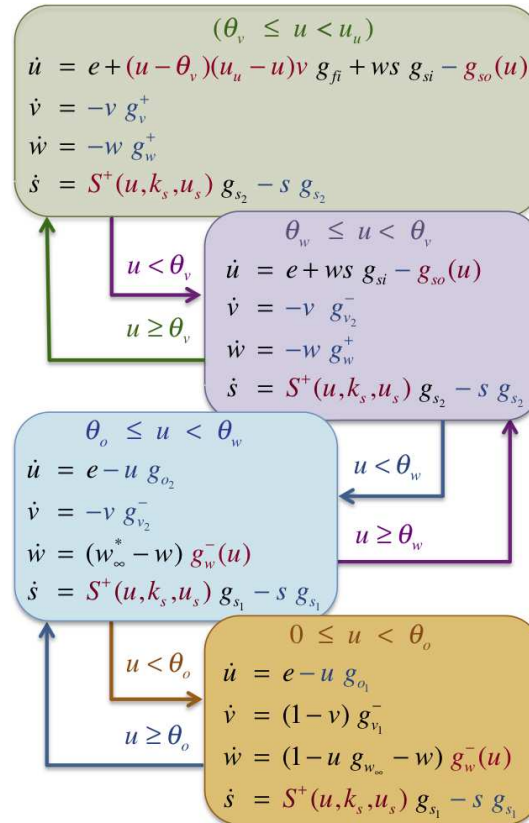
Support Function

SpaceX



Parameter Estimation with RoVerGeNe.

- Introduction
- SpaceEx
- Hybrid Systems
- Example
- CMACS**
- Parameter Estimation in SpaceEx
- Reachability Analysis
- Support Function
- SpaceEx



Parameter Estimation with RoVerGeNe.

Based on abstractions by discrete automata.

[Introduction](#)[SpaceEx](#)[Hybrid Systems](#)[Example](#)[CMACS](#)[Parameter Estimation in SpaceEx](#)[Reachability Analysis](#)[Support Function](#)[SpaceEx](#)

SpaceEx, Reachability for:

LHA

$$\dot{x} \in \mathcal{P}$$

HA with linear dynamics

$$\dot{x} \in \{Ax + u \mid u \in \mathcal{U}\}$$

No parameter estimation.

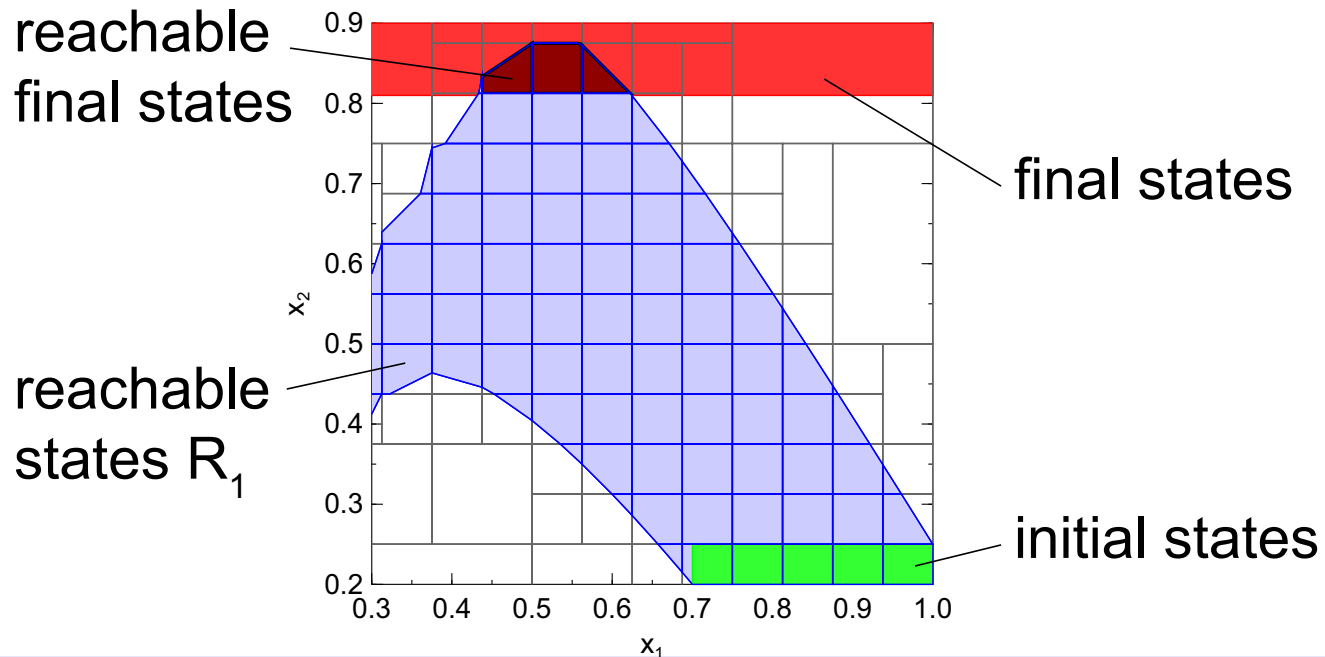
- [Introduction](#)
- [SpaceEx](#)
- [Hybrid Systems](#)
- [Example](#)
- [CMACS](#)
- [Parameter Estimation in SpaceEx](#)**
- [Reachability Analysis](#)
- [Support Function](#)
- [SpaceEx](#)

SpaceEx, Reachability for:

LHA
 $\dot{x} \in \mathcal{P}$

HA with linear dynamics
 $\dot{x} \in \{Ax + u \mid u \in \mathcal{U}\}$

Parameters as variables with 0 derivative.



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

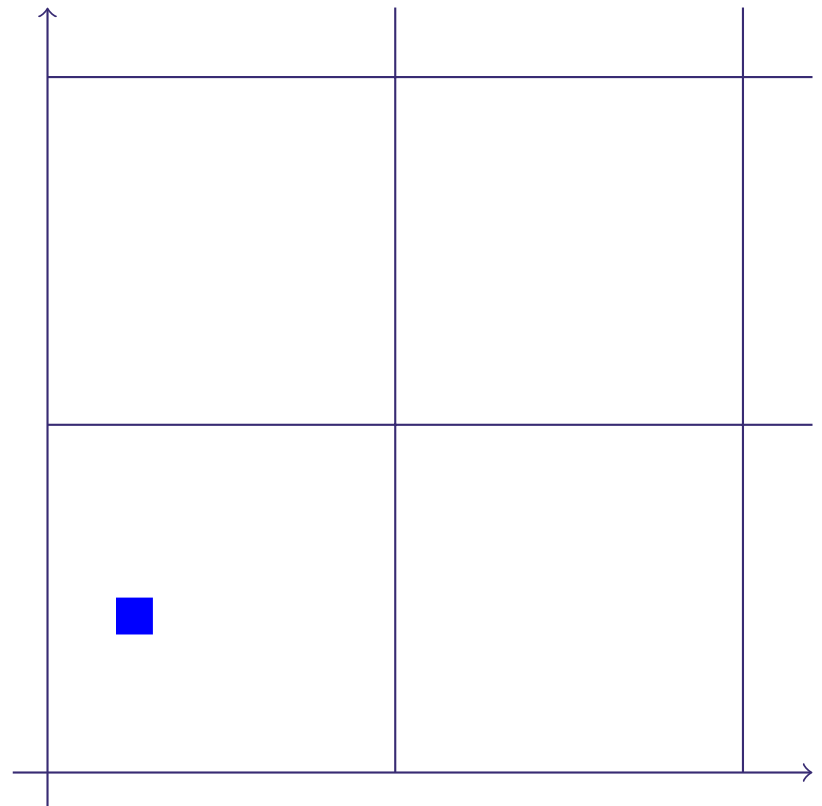
Representing Sets

Scalable

Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

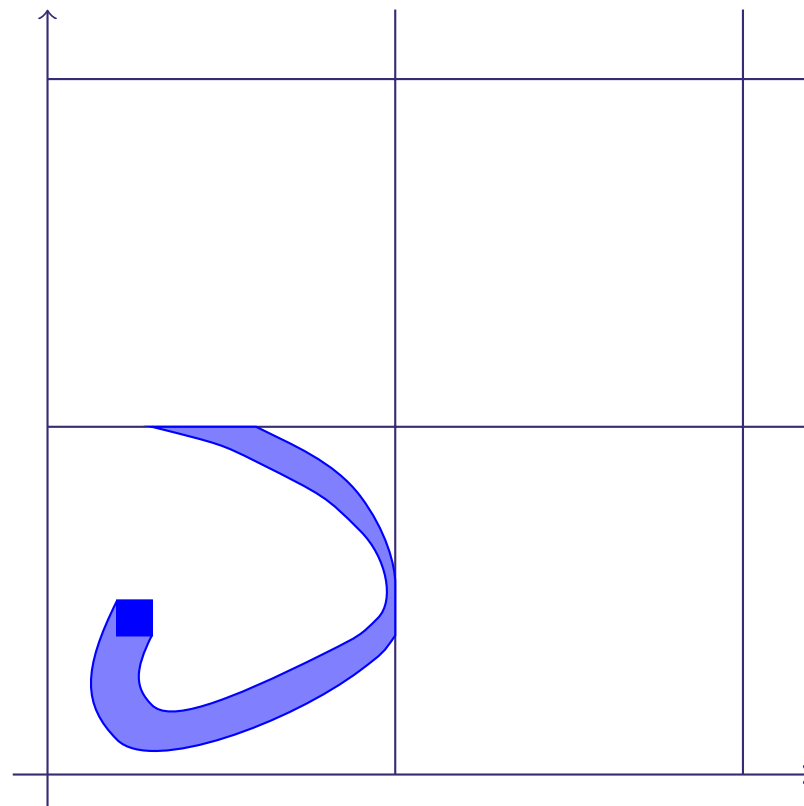
Scalable

Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps

$Post_c$: Continuous evolution



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

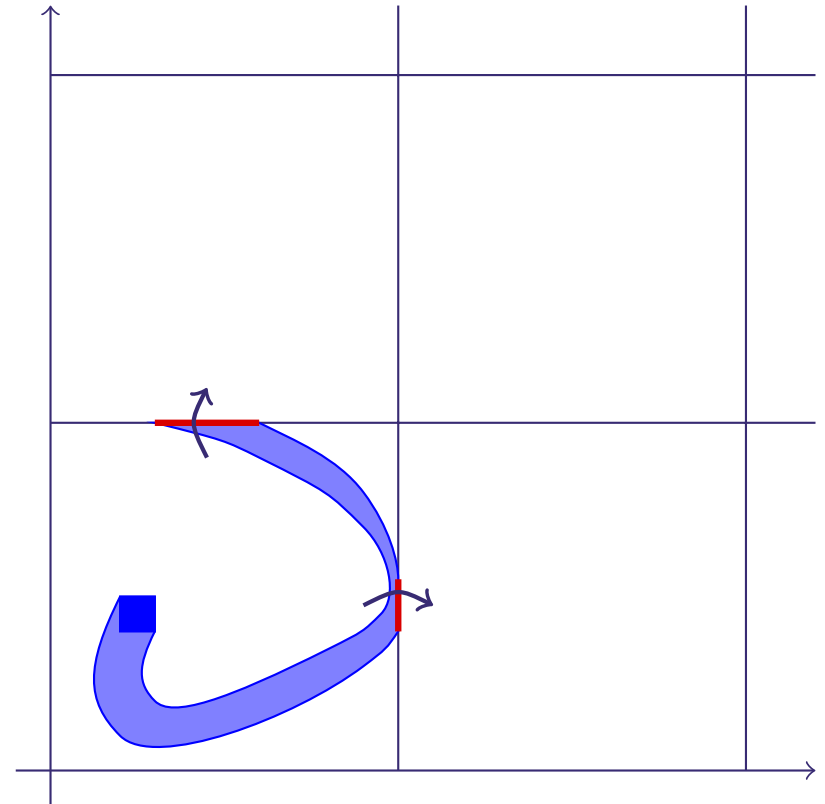
Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps

$Post_c$: Continuous evolution

$Post_d$: Discrete transition



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

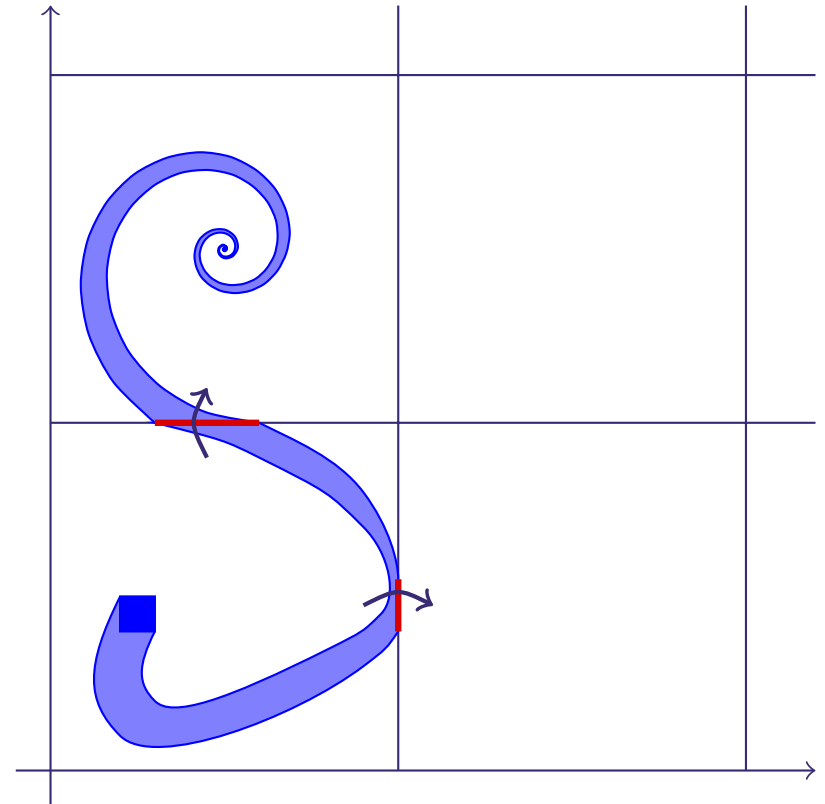
Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps

$Post_c$: Continuous evolution

$Post_d$: Discrete transition



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

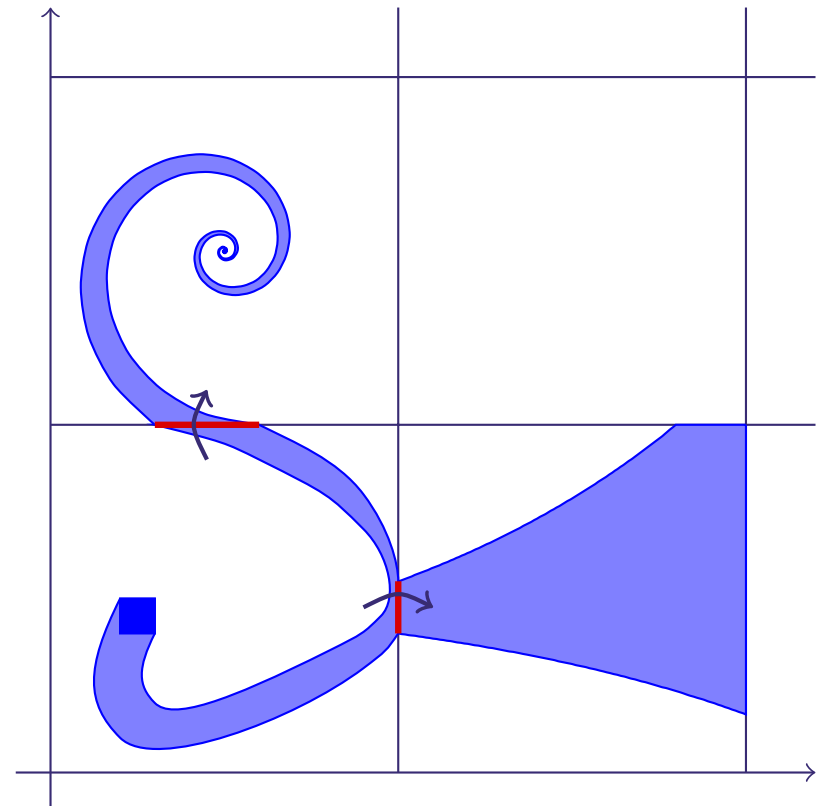
Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps

$Post_c$: Continuous evolution

$Post_d$: Discrete transition



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

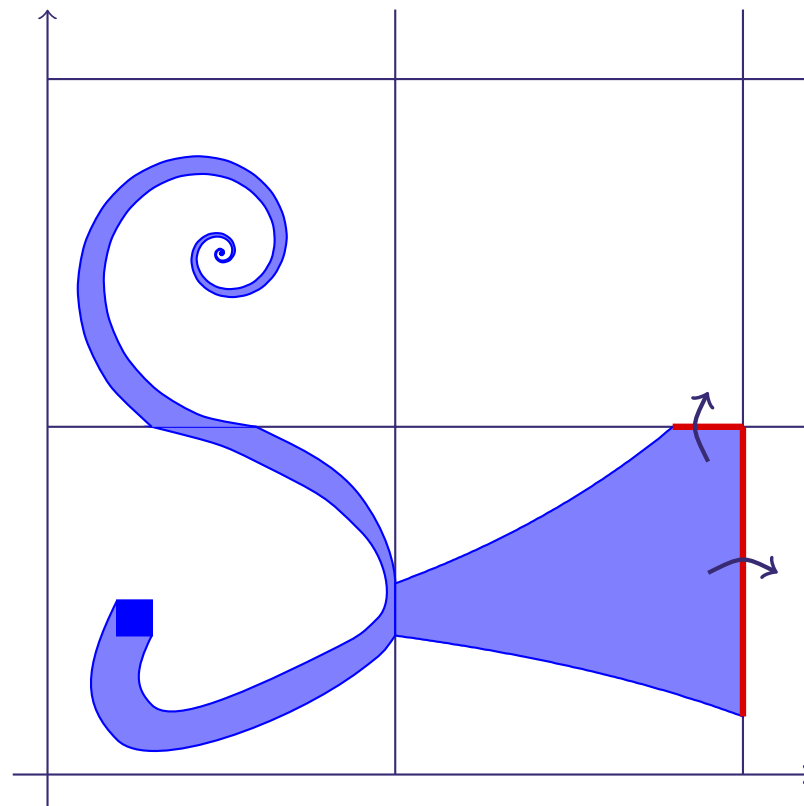
Support Function

SpaceEx

- Continuous Dynamics: $\dot{x} \in Ax \oplus \mathcal{U}$ and $x(t) \in \mathcal{I}$
- Hyperplanar guards
- Affine Reset Maps

$Post_c$: Continuous evolution

$Post_d$: Discrete transition



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

Support Function

SpaceEx

Describe all $x(t) \in \mathbb{R}^d$ for any t in $[0; T]$ such that :

$$\dot{x}(t) = Ax(t) + u(t) \quad \text{with } x(0) \in \mathcal{X}_0 \text{ and } u(t) \in \mathcal{U}$$

[Introduction](#)[Reachability Analysis](#)[Reachability Analysis](#)[LTI](#)[Guards](#)[Representing Sets](#)[Scalable](#)[Support Function](#)[SpaceEx](#)

Describe all $x(t) \in \mathbb{R}^d$ for any t in $[0; T]$ such that :

$$\dot{x}(t) = Ax(t) + u(t) \quad \text{with } x(0) \in \mathcal{X}_0 \text{ and } u(t) \in \mathcal{U}$$

Analytical solution for a given input function u :

$$x(t) = e^{tA}x(0) + \int_0^t e^{(t-s)A}u(s) ds$$

[Introduction](#)[Reachability Analysis](#)[Reachability Analysis](#)[LTI](#)[Guards](#)[Representing Sets](#)[Scalable](#)[Support Function](#)[SpaceEx](#)

Describe all $x(t) \in \mathbb{R}^d$ for any t in $[0; T]$ such that :

$$\dot{x}(t) = Ax(t) + u(t) \quad \text{with } x(0) \in \mathcal{X}_0 \text{ and } u(t) \in \mathcal{U}$$

Analytical solution for a given input function u :

$$x(t) = e^{tA}x(0) + \int_0^t e^{(t-s)A}u(s) ds$$

Temporal discretization:

$$\text{Reach}_{[t_k, t_k + \delta_k]}(\mathcal{X}_0) = e^{At_k} \text{Reach}_{[0, \delta_k]}(\mathcal{X}_0) \oplus \text{Reach}_{[t_k, t_k]}(\{0\})$$

- Introduction
- Reachability Analysis
- Reachability Analysis
- LTI**
- Guards
- Representing Sets
- Scalable
- Support Function
- SpaceEx

Describe all $x(t) \in \mathbb{R}^d$ for any t in $[0; T]$ such that :

$$\dot{x}(t) = Ax(t) + u(t) \quad \text{with } x(0) \in \mathcal{X}_0 \text{ and } u(t) \in \mathcal{U}$$

Analytical solution for a given input function u :

$$x(t) = e^{tA}x(0) + \int_0^t e^{(t-s)A}u(s) ds$$

Temporal discretization:

$$\begin{aligned} \Psi_{k+1} &= \Psi_k \oplus e^{At_k} \Psi_{\delta_k}(\mathcal{U}) \\ \Omega_k &= e^{At_k} \Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U}) \oplus \Psi_k \end{aligned}$$

[Introduction](#)

[Reachability Analysis](#)

[Reachability Analysis](#)

[LTI](#)

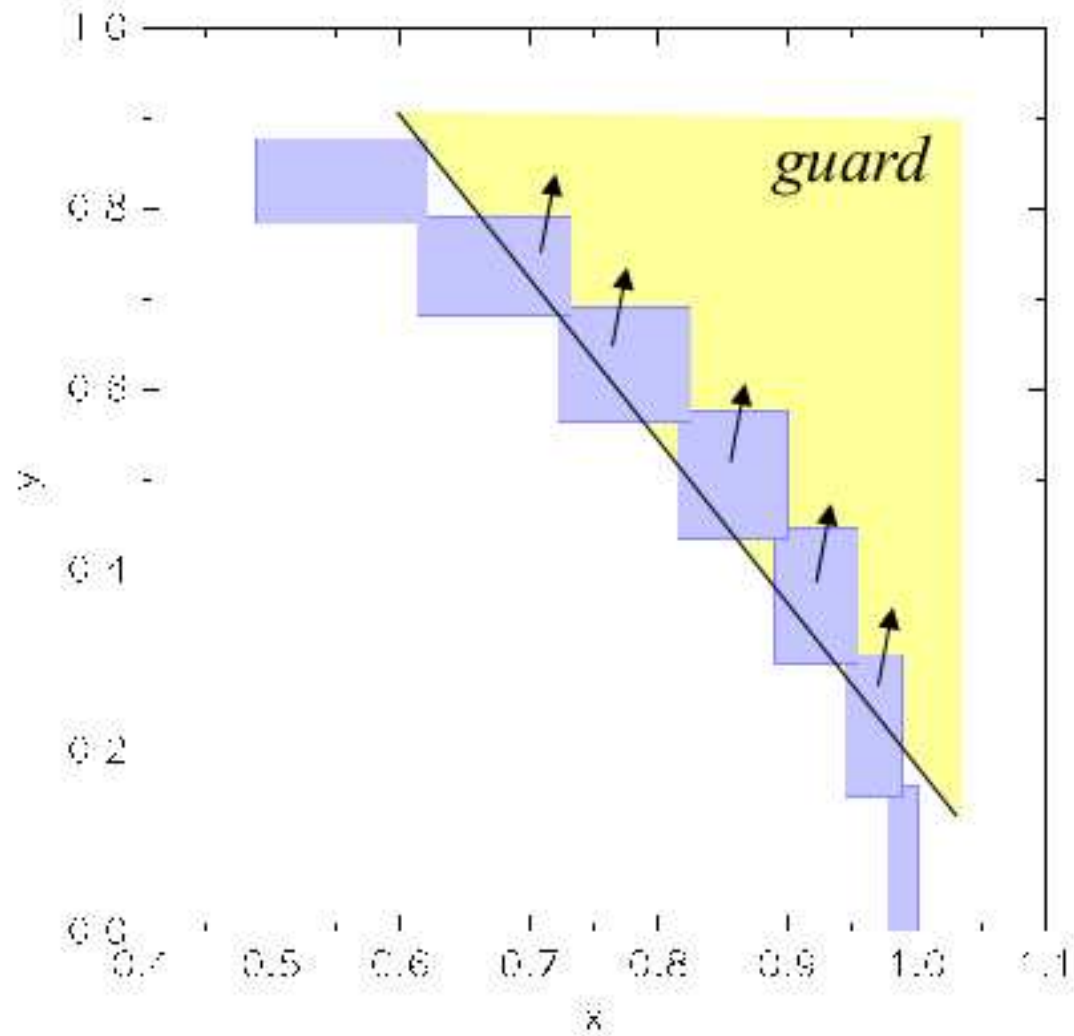
Guards

[Representing Sets](#)

[Scalable](#)

[Support Function](#)

[SpaceEx](#)



[Introduction](#)

[Reachability Analysis](#)

[Reachability Analysis](#)

[LTI](#)

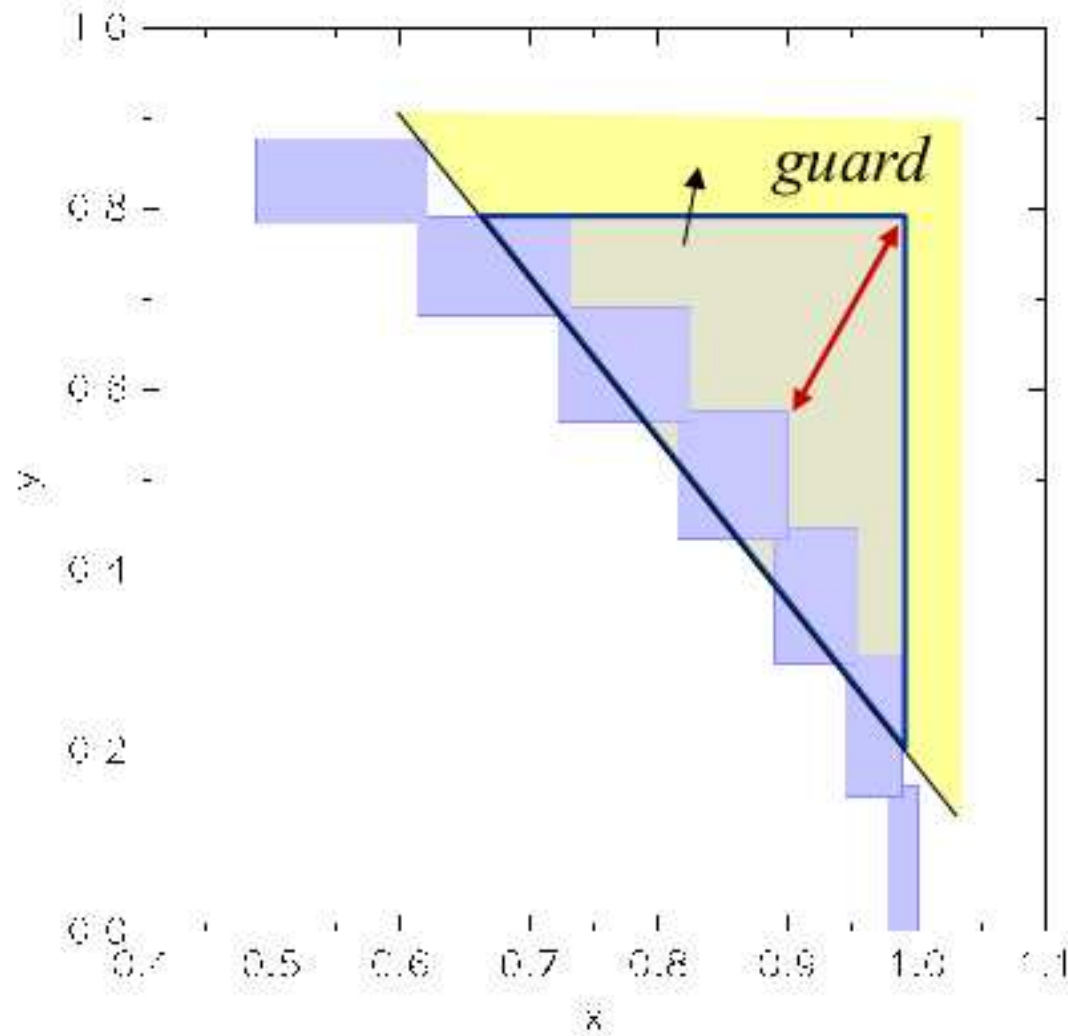
Guards

[Representing Sets](#)

[Scalable](#)

[Support Function](#)

[SpaceEx](#)



Introduction

Reachability Analysis

Reachability Analysis

LTI

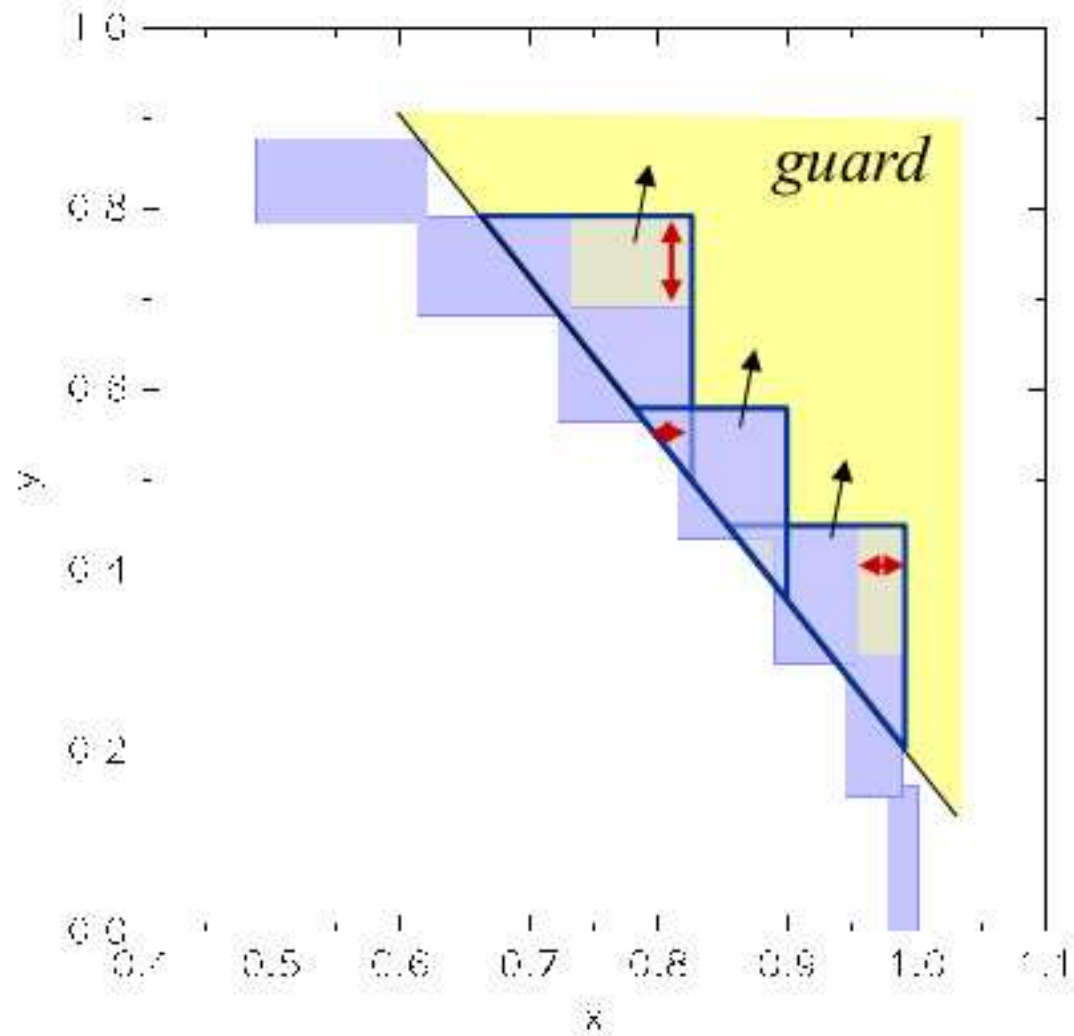
Guards

Representing Sets

Scalable

Support Function

SpaceEx



[Introduction](#)

[Reachability Analysis](#)

[Reachability Analysis](#)

[LTI](#)

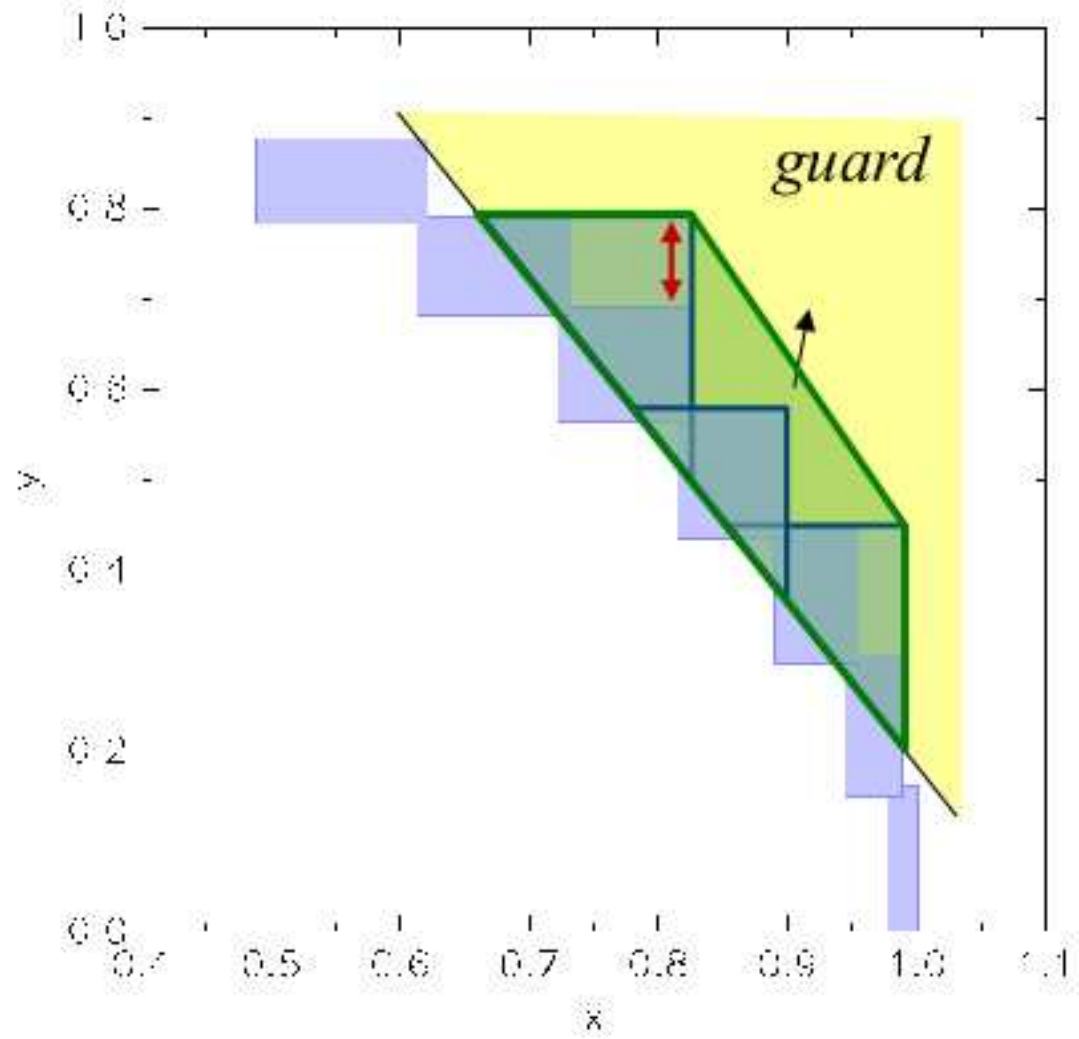
Guards

[Representing Sets](#)

[Scalable](#)

[Support Function](#)

[SpaceEx](#)



Introduction

Reachability Analysis

Reachability Analysis

LTI

Guards

Representing Sets

Scalable

Support Function

SpaceEx

Operators	Polyhedra		Zonotopes	Support Functions
	Constraints	Vertices		
Affine transform	-	++	++	++
Minkowski sum	--	-	++	++
Intersection	++	--	--	-
Containment	++	--	?	--
Convex hull	--	++	--	++

Introduction

Reachability Analysis

Reachability Analysis

LTI

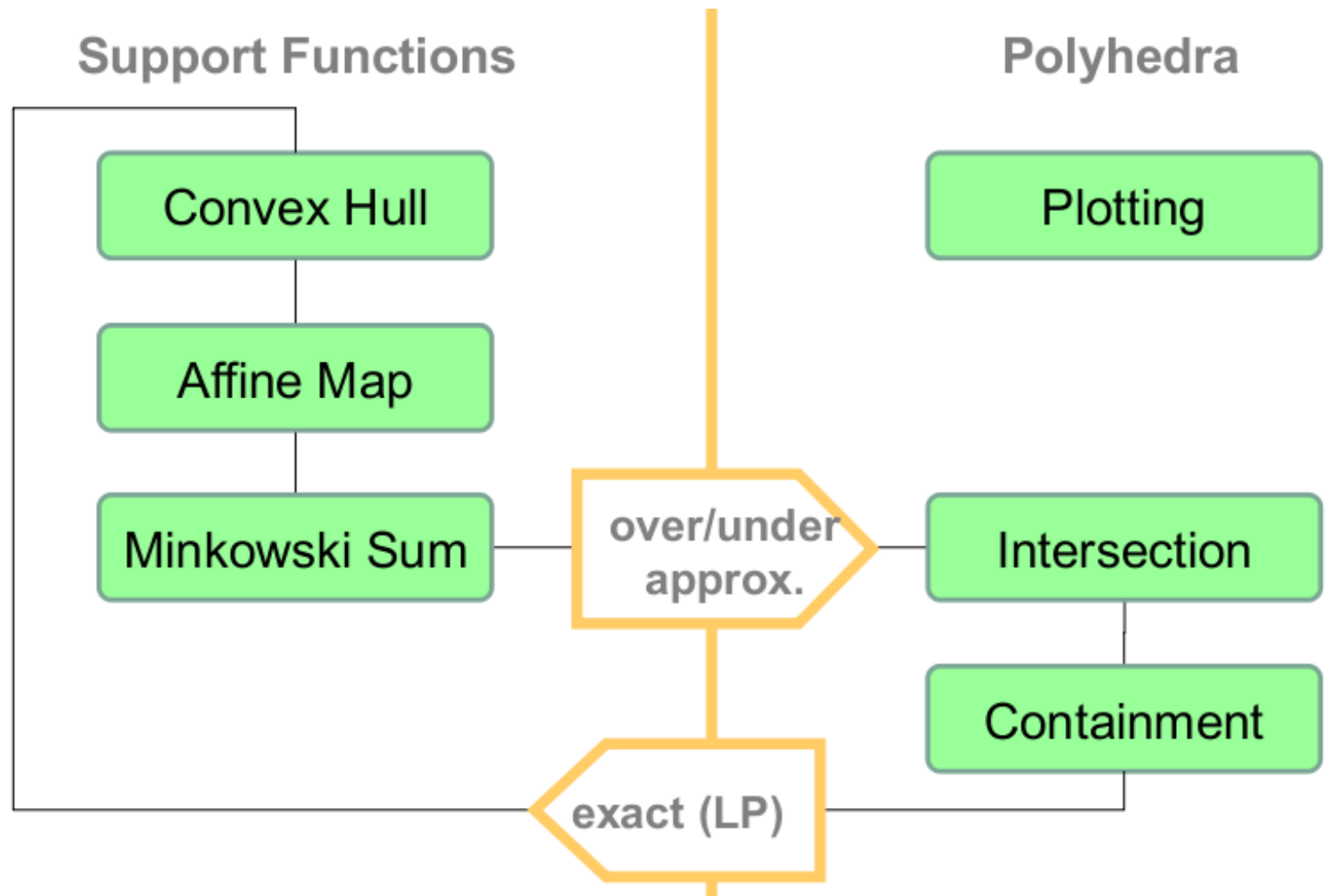
Guards

Representing Sets

Scalable

Support Function

SpaceEx



Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

Support Function

[Introduction](#)[Reachability Analysis](#)[Support Function](#)[Definition](#)[Examples](#)[Representing sets](#)[Properties](#) $\rho_{\Omega_k}(\ell)$ $\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$ $\rho_{\Omega_{[0, \delta_k]}}(\ell)$ [Time Step](#)[SpaceEx](#)

The support function of a compact convex set $\mathcal{S} \subseteq \mathbb{R}^d$, denoted $\rho_{\mathcal{S}}$, is defined as:

$$\begin{aligned} \rho_{\mathcal{S}} : \mathbb{R}^d &\rightarrow \mathbb{R} \\ \ell &\mapsto \max_{x \in \mathcal{S}} \ell \cdot x \end{aligned}$$

[Introduction](#)

[Reachability Analysis](#)

[Support Function](#)

Definition

[Examples](#)

[Representing sets](#)

[Properties](#)

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

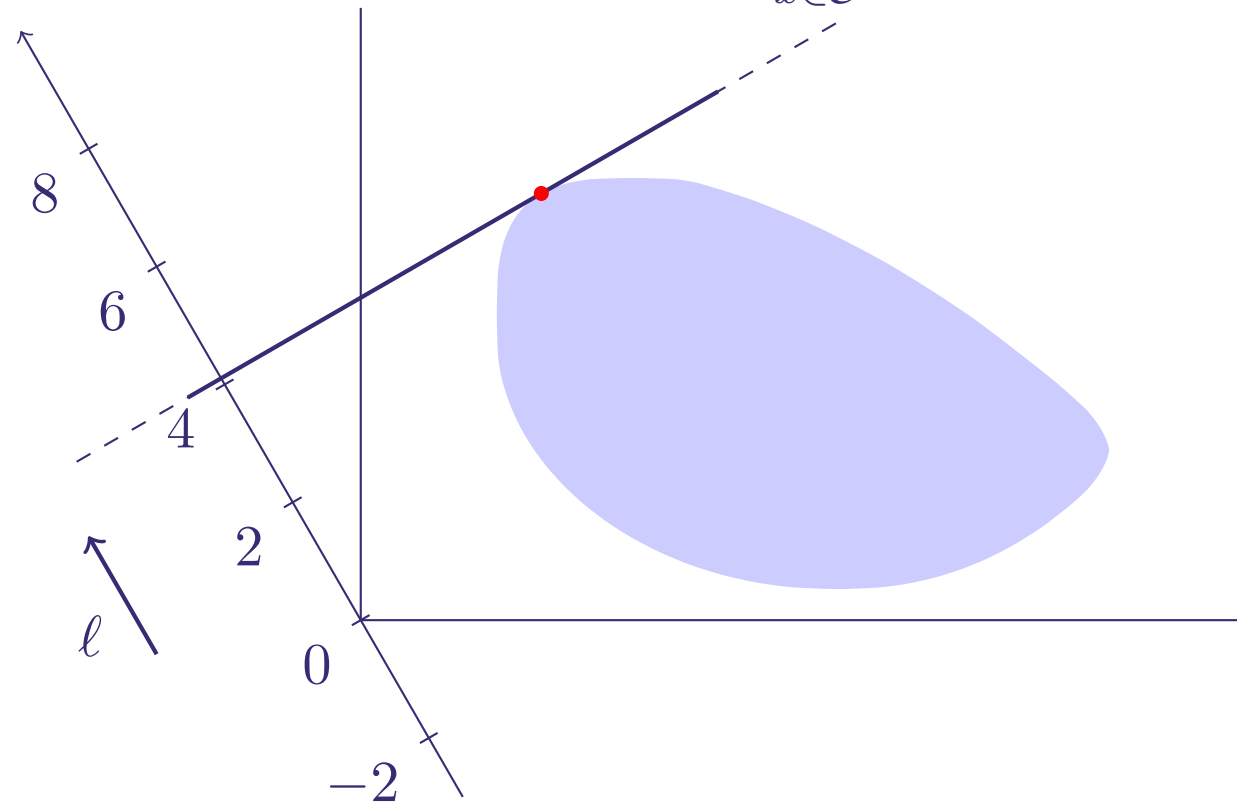
[Time Step](#)

[SpaceEx](#)

The support function of a compact convex set $\mathcal{S} \subseteq \mathbb{R}^d$, denoted $\rho_{\mathcal{S}}$, is defined as:

$$\rho_{\mathcal{S}} : \mathbb{R}^d \rightarrow \mathbb{R}$$

$$\ell \mapsto \max_{x \in \mathcal{S}} \ell \cdot x$$



Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

- support function of the unit cube \mathcal{B}_∞ :

$$\rho_{\mathcal{B}_\infty}(\ell) = \|\ell\|_1 = \sum_{i=0}^{d-1} |\ell_i|$$

- support function of a ball \mathcal{S} of center c and radius r :

$$\rho_{\mathcal{S}}(\ell) = c \cdot \ell + r \|\ell\|_2$$

- support function of a polytope $\mathcal{P} = \{x : Ax \leq b\}$: any LP algorithm solving:

$$\begin{cases} \max x \cdot \ell \\ Ax \leq b \end{cases}$$

Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

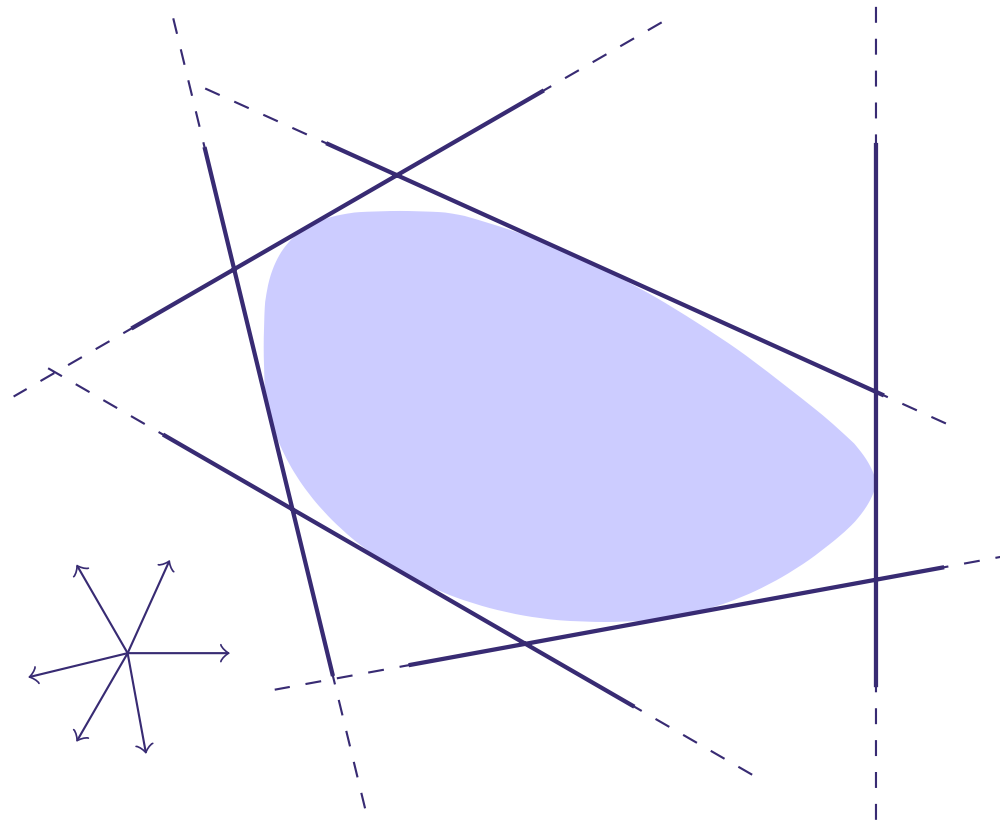
$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

If \mathcal{S} is convex, then:

$$\mathcal{S} = \bigcap_{\ell \in \mathbb{R}^d} \{x : x \cdot \ell \leq \rho_{\mathcal{S}}(\ell)\}$$



[Introduction](#)[Reachability Analysis](#)[Support Function](#)[Definition](#)[Examples](#)[Representing sets](#)[Properties](#)[ρ_{Ω_k}\(ℓ\)](#)[Ω_{\[0, δ_k\]}\(X₀, U\)](#)[ρ_{Ω_{\[0, δ_k\]}}\(ℓ\)](#)[Time Step](#)[SpaceEx](#)

- Linear transformation:

$$\rho_{AS}(\ell) = \rho_S(A^\top \ell)$$

- Minkowski sum:

$$\mathcal{X} \oplus \mathcal{Y} = \{x + y : x \in \mathcal{X} \text{ and } y \in \mathcal{Y}\}$$

$$\rho_{\mathcal{X} \oplus \mathcal{Y}}(\ell) = \rho_{\mathcal{X}}(\ell) + \rho_{\mathcal{Y}}(\ell)$$

- Convex union:

$$\rho_{CH(\mathcal{X} \cup \mathcal{Y})}(\ell) = \max(\rho_{\mathcal{X}}(\ell), \rho_{\mathcal{Y}}(\ell))$$

Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

$$\Psi_{k+1} = \Psi_k \oplus e^{At_k} \Psi_{\delta_k}(\mathcal{U})$$

$$\Omega_k = e^{At_k} \Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U}) \oplus \Psi_k$$

For any direction ℓ :

$$\psi_{k+1}(\ell) = \psi_k(\ell) + \rho_{\Psi_{\delta_k}}((e^{At_k})^\top \ell)$$

$$\rho_{\Omega_k}(\ell) = \rho_{\Omega_{[0, \delta_k]}}((e^{At_k})^\top \ell) \oplus \psi_k(\ell)$$

Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

Let $\lambda \in [0, 1]$, and $\Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)$ be the convex set defined by :

$$\begin{aligned} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta) = & (1 - \lambda)\mathcal{X}_0 \oplus \lambda e^{\delta A} \mathcal{X}_0 \oplus \lambda \delta \mathcal{U} \\ & \oplus (\lambda \mathcal{E}_\Omega^+(\mathcal{X}_0, \delta) \cap (1 - \lambda) \mathcal{E}_\Omega^-(\mathcal{X}_0, \delta)) \oplus \lambda^2 \mathcal{E}_\Psi(\mathcal{U}, \delta) \end{aligned}$$

where $\mathcal{E}_\Omega^+(\mathcal{X}_0, \delta) = \square(\Phi_2(|A|, \delta) \square(A^2 \mathcal{X}_0))$
 and $\mathcal{E}_\Omega^-(\mathcal{X}_0, \delta) = \square(\Phi_2(|A|, \delta) \square(A^2 e^{\delta A} \mathcal{X}_0))$
 and $\mathcal{E}_\Psi(\mathcal{U}, \delta) = \square(\Phi_2(|A|, \delta) \square(A\mathcal{U}))$.

Then $\text{Reach}_{\lambda\delta, \lambda\delta}(\mathcal{X}_0, \mathcal{U}) \subseteq \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)$. If we define $\Omega_{[0, \delta]}(\mathcal{X}_0, \mathcal{U})$ as:

$$\Omega_{[0, \delta]}(\mathcal{X}_0, \mathcal{U}) = \text{CH}\left(\bigcup_{\lambda \in [0, 1]} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)\right),$$

then $\text{Reach}_{0, \delta}(\mathcal{X}_0) \subseteq \Omega_{[0, \delta]}(\mathcal{X}_0, \mathcal{U})$.

Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

$$\begin{aligned} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta) &= (1 - \lambda)\mathcal{X}_0 \oplus \lambda e^{\delta A} \mathcal{X}_0 \oplus \lambda \delta \mathcal{U} \\ &\oplus (\lambda \mathcal{E}_\Omega^+(\mathcal{X}_0, \delta) \cap (1 - \lambda) \mathcal{E}_\Omega^-(\mathcal{X}_0, \delta)) \oplus \lambda^2 \mathcal{E}_\Psi(\mathcal{U}, \delta) \end{aligned}$$

$$\Omega_{[0, \delta]}(\mathcal{X}_0, \mathcal{U}) = \text{CH}\left(\bigcup_{\lambda \in [0, 1]} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)\right),$$

Introduction

Reachability Analysis

Support Function

Definition

Examples

Representing sets

Properties

$\rho_{\Omega_k}(\ell)$

$\Omega_{[0, \delta_k]}(\mathcal{X}_0, \mathcal{U})$

$\rho_{\Omega_{[0, \delta_k]}}(\ell)$

Time Step

SpaceEx

$$\begin{aligned} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta) &= (1 - \lambda)\mathcal{X}_0 \oplus \lambda e^{\delta A} \mathcal{X}_0 \oplus \lambda \delta \mathcal{U} \\ &\oplus (\lambda \mathcal{E}_\Omega^+(\mathcal{X}_0, \delta) \cap (1 - \lambda) \mathcal{E}_\Omega^-(\mathcal{X}_0, \delta)) \oplus \lambda^2 \mathcal{E}_\Psi(\mathcal{U}, \delta) \end{aligned}$$

$$\Omega_{[0, \delta]}(\mathcal{X}_0, \mathcal{U}) = \text{CH}\left(\bigcup_{\lambda \in [0, 1]} \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)\right),$$

$$\begin{aligned} \rho_{\Omega_{[0, \delta]}}(\ell) &= \max_{\lambda \in [0, 1]} \left((1 - \lambda) \rho_{\mathcal{X}_0}(\ell) + \lambda \rho_{\mathcal{X}_0}((e^{\delta A})^\top \ell) + \lambda \delta \rho_{\mathcal{U}}(\ell) \right. \\ &\quad \left. + \rho_{\lambda \mathcal{E}_\Omega^+ \cap (1 - \lambda) \mathcal{E}_\Omega^-}(\ell) + \lambda^2 \rho_{\mathcal{E}_\Psi}(\ell) \right) \end{aligned}$$

- [Introduction](#)
- [Reachability Analysis](#)
- [Support Function](#)
- [Definition](#)
- [Examples](#)
- [Representing sets](#)
- [Properties](#)
- [ρ_{Ω_k}\(ℓ\)](#)
- [Ω_{\[0, δ_k\]}\(X₀, U\)](#)
- [ρ_{Ω_{\[0, δ_k\]}}\(ℓ\)](#)
- [Time Step](#)**
- [SpaceEx](#)

- A user defined time step is arbitrary
- Time step guided by requested quality of approximation:

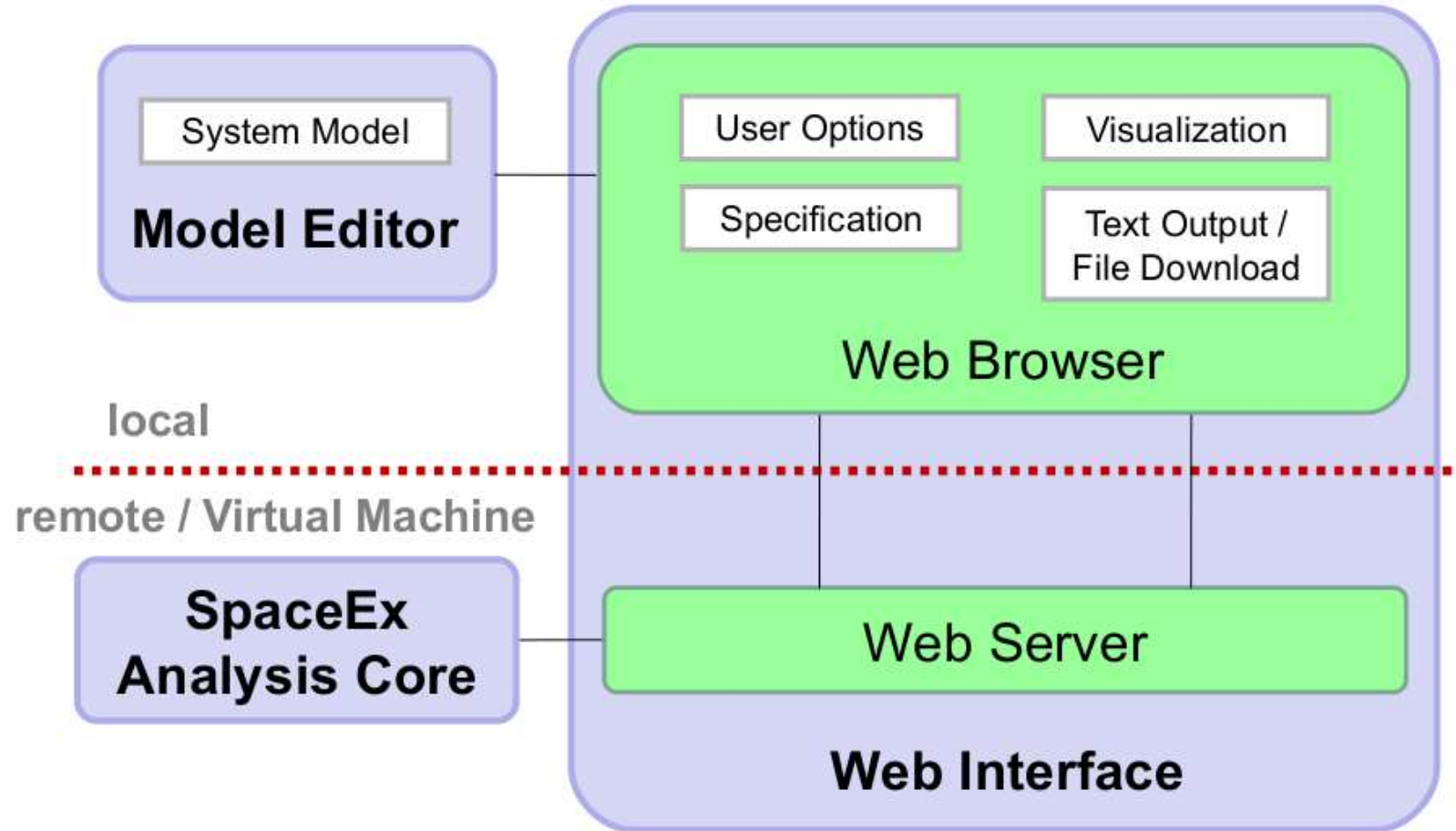
$$\epsilon_{\Omega_k}(\ell) = \rho(\ell, \Omega_k) - \rho(\ell, \text{Reach}_{t_k, t_{k+1}}(\mathcal{X}_0))$$

- linear accumulation of errors

$$\epsilon_{\Psi_k}(\ell) + \epsilon_{\Psi_{\delta_k^\Psi}}(\mathcal{U})(e^{At_k^\Psi} \ell) \leq \frac{t_k^\Psi + \delta_k^\Psi}{T} \hat{\epsilon}_\Psi$$

- computed independently for each direction

- [Introduction](#)
- [Reachability Analysis](#)
- [Support Function](#)
- [SpaceEx](#)
- [Architecture](#)



Introduction

Reachability Analysis

Support Function

SpaceEx

Thank you