Algorithmic Verification of Dynamical Systems *in JuliaReach*

Marcelo Forets
Universidad de la República, Uruguay
Universidad Tecnológica, Uruguay

Academic Visitor by the Australian National University, 2019

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

UTEC Universidad Tecnológica

Australian National University

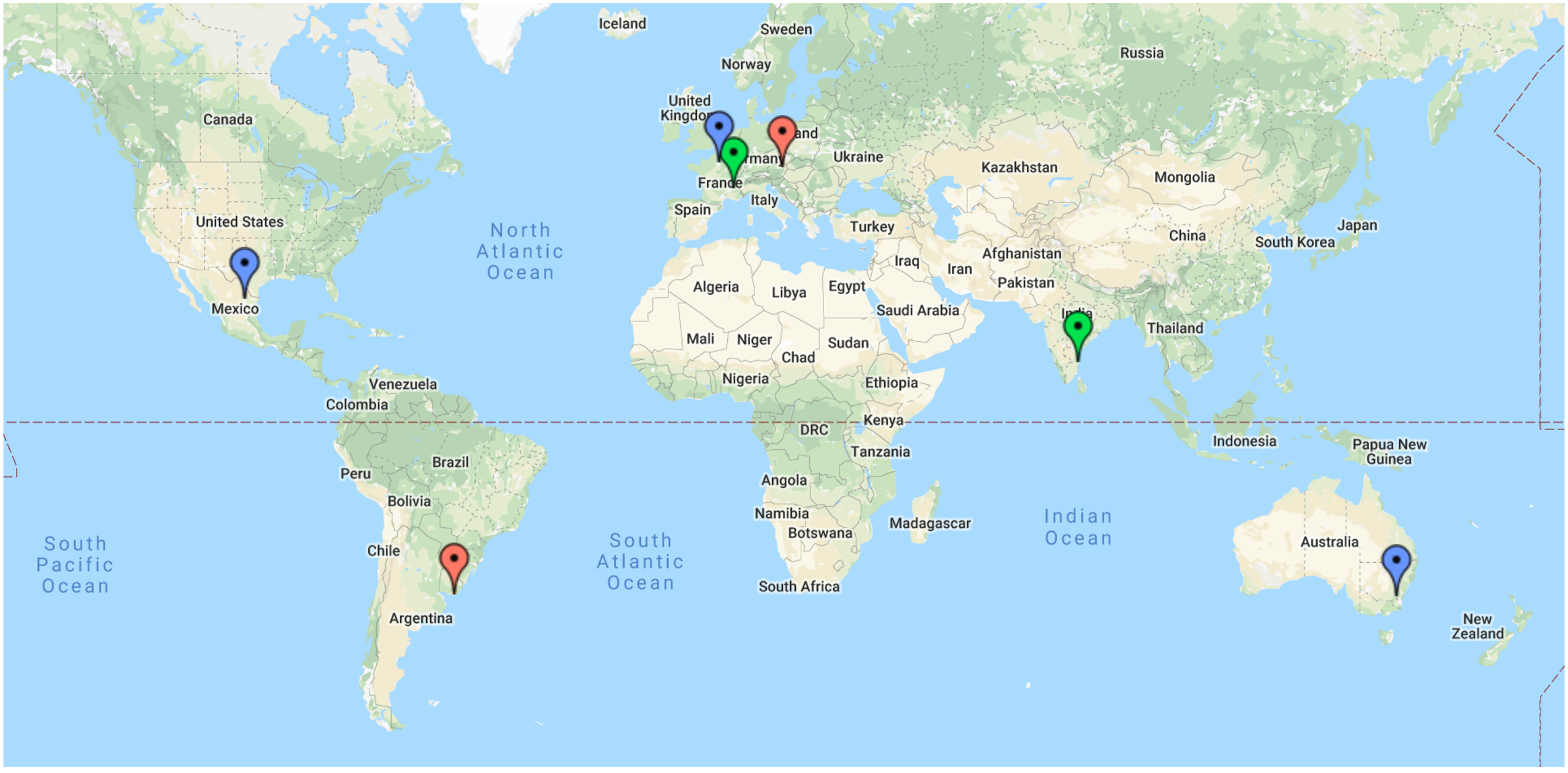
The *JuliaReach* team

JuliaReach

Reachability Computations for Dynamical Systems in Julia

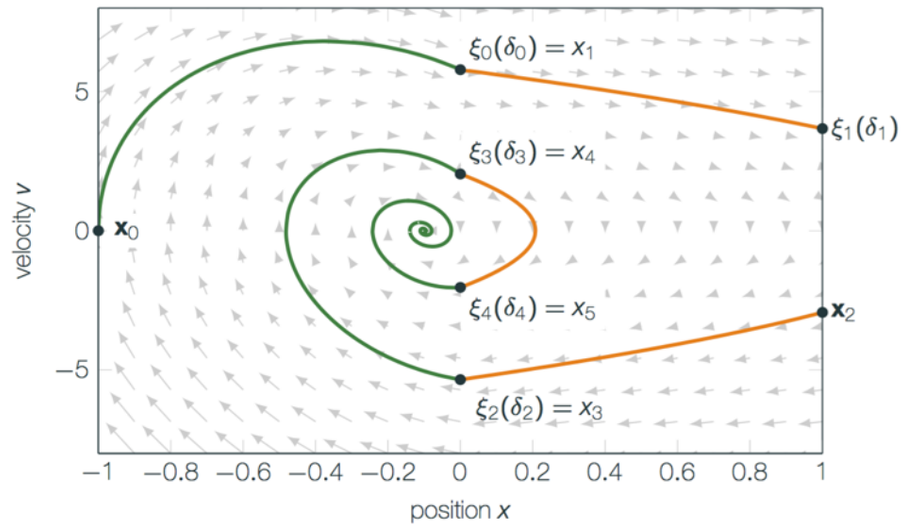
http://www.juliareach.org

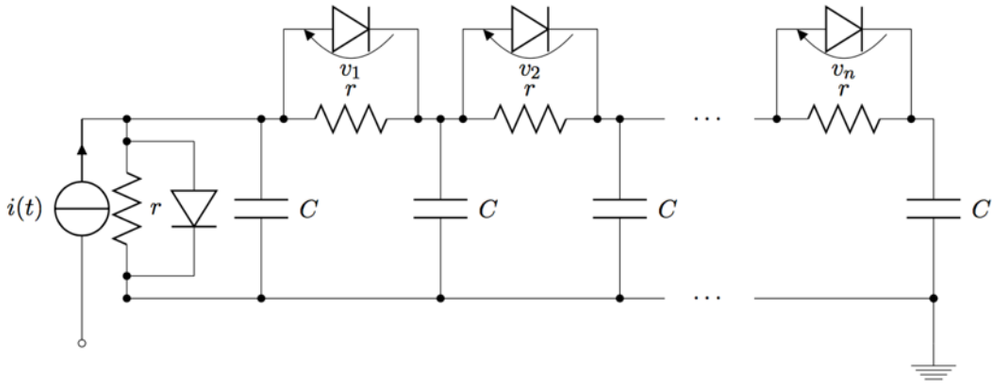
Developing Theoretical and Computational Methods for Formal Verification of Dynamical Systems



What are *dynamical systems?*

- Just about anything that evolves with time!
  - either discrete or continuous
  - or *both* continuous dynamics and discrete jumps





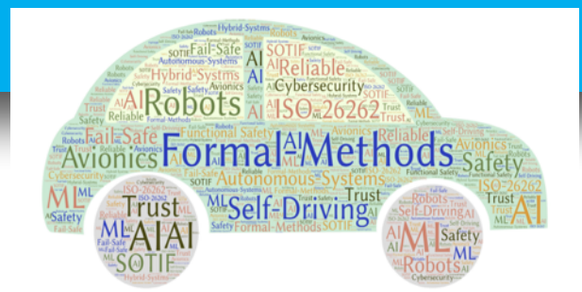
- Several mathematical formalisms are available:

ODEs | PDEs | DAEs | Hybrid Automata

The field of Reachability Analysis is concerned with understanding the **set of all possible behaviours** of such systems

UTEC
Universidad Tecnológica

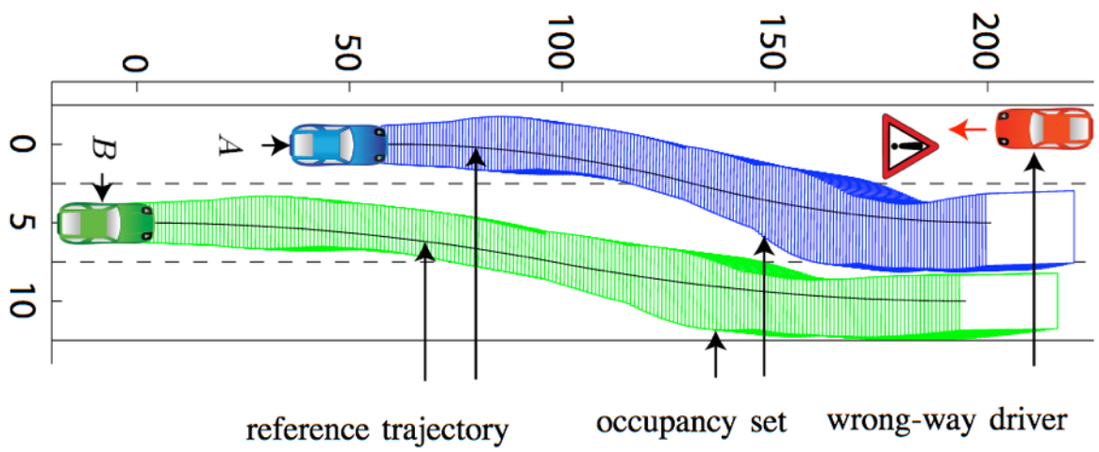
. . . and why do we care?

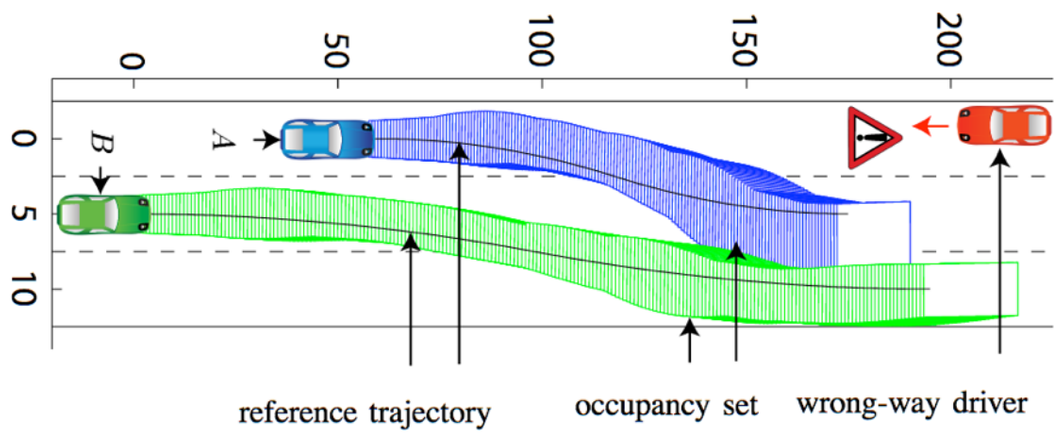


- From FT4DAS 2019 CfP:

Theme

Autonomous systems have been increasingly deployed in safety and mission critical application. For example, future autonomous cars are ready to hit the public roads in a few years. Due to a direct impact on human-lives, their functional safety, security and dependability are important for both general public and Original Equipment Manufacturers (OEMs). Formal Methods techniques have the potential to address some of the most important verification and dependability challenges associated with such autonomous systems. Indeed, industrial standards, such as ISO 26262, ISO 61508, IEC 62304, EN 50128 explicitly recommend the use of formal methods in the design and development of autonomous systems. The main purpose of this workshop is to bring together people from both industry and academia and serve as a forum to discuss practical applications of formal methods. Moreover, we believe this workshop will help to discuss the readiness of formal methods in industrial applications by discussing the needs of autonomous systems industry and challenges faced by formal methods researchers.

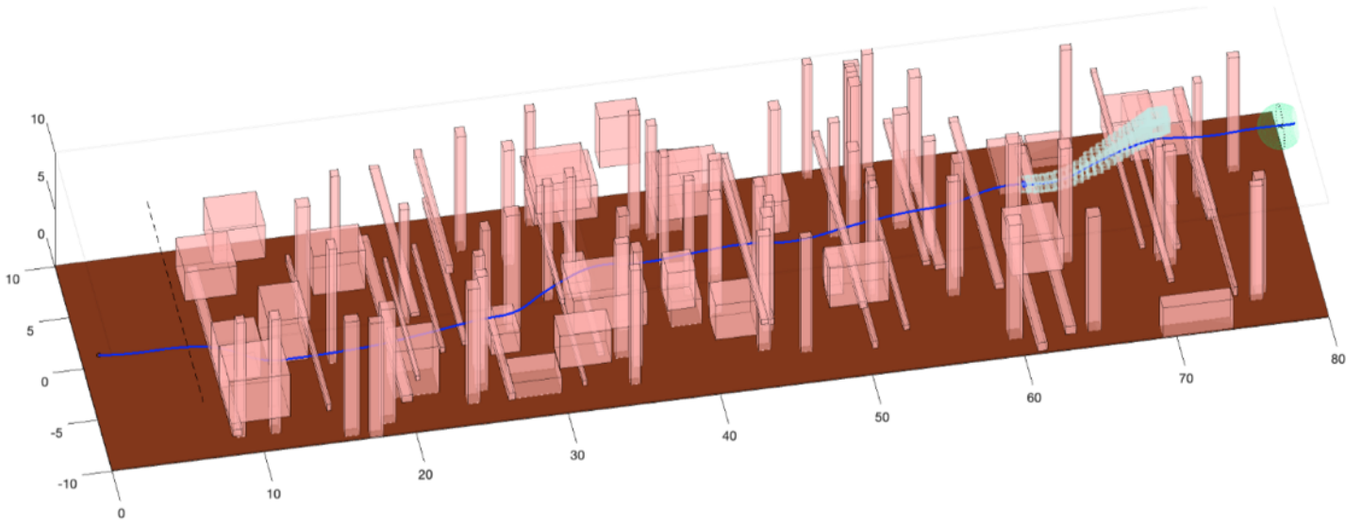




Formal Methods can provide **guarantees** on the behavior of dynamical systems subject to non-deterministic inputs, parameters or noise

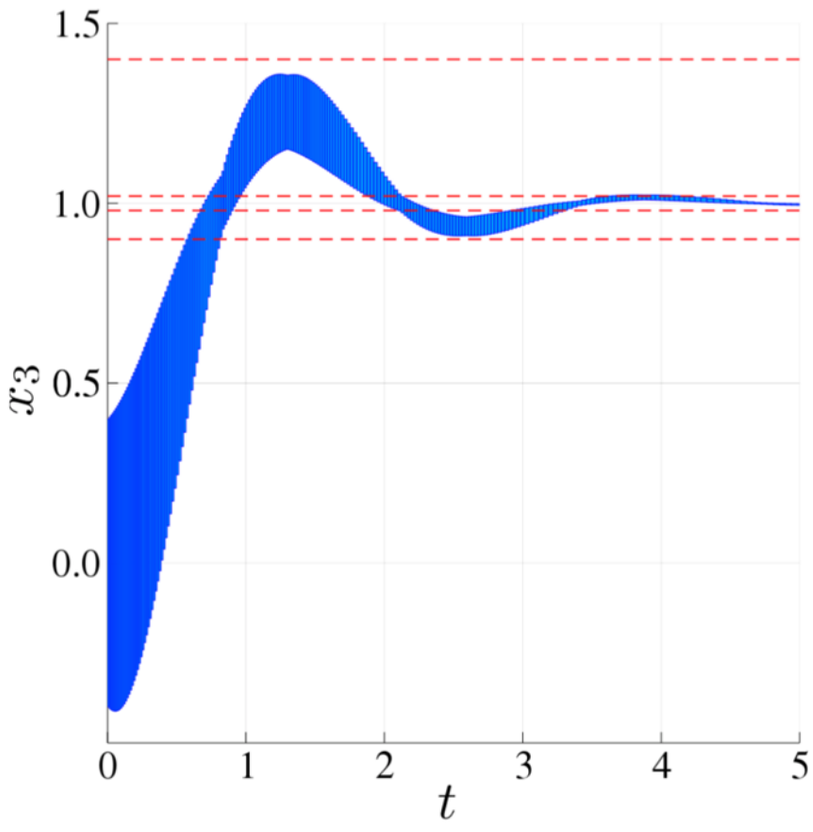
UTEC
Universidad Tecnológica

. . . and why do we care?

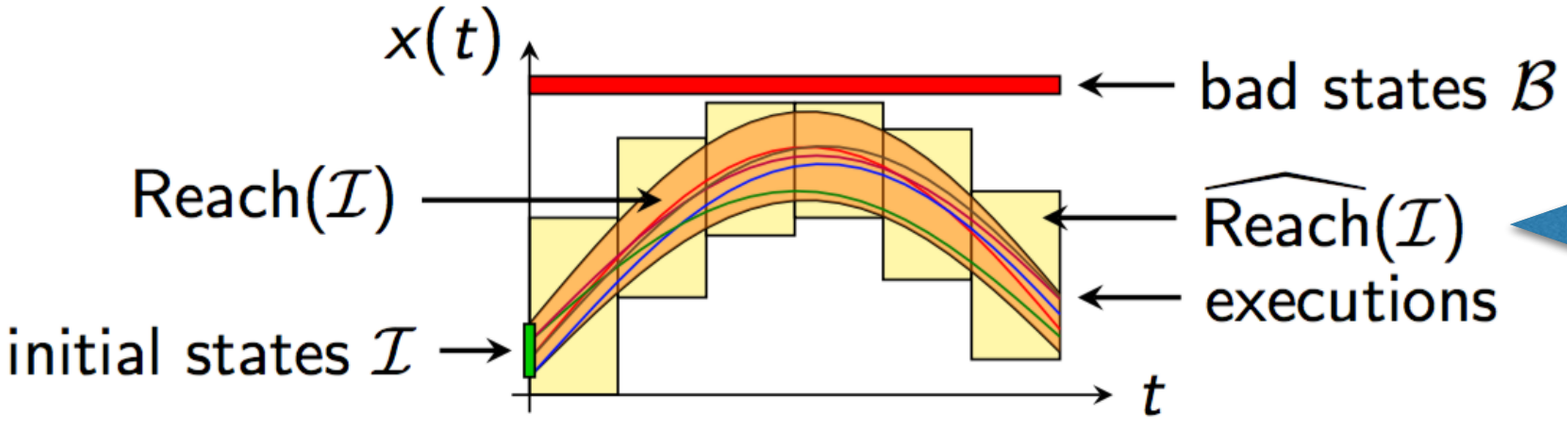


Safe, Aggressive Quadrotor Flight via Reachability-based Trajectory Design

Shreyas Kousik, Patrick Holmes, Ram Vasudevan*



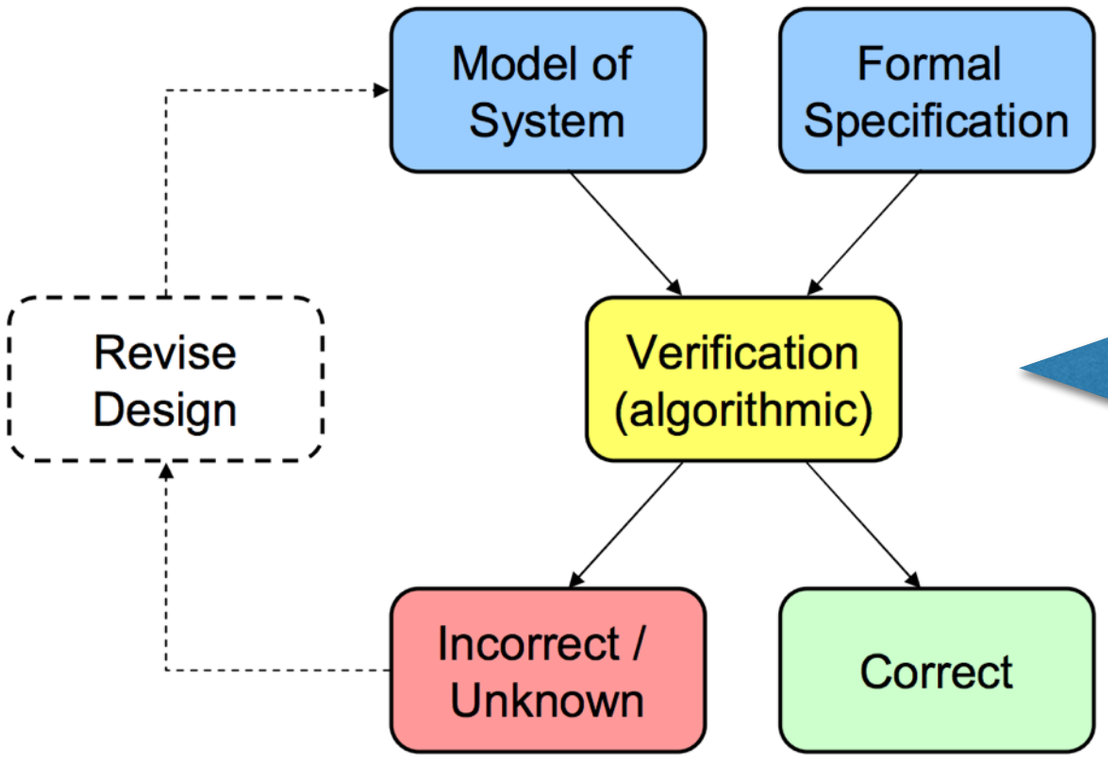
Reachable set overapproximations for the quadrotor model.



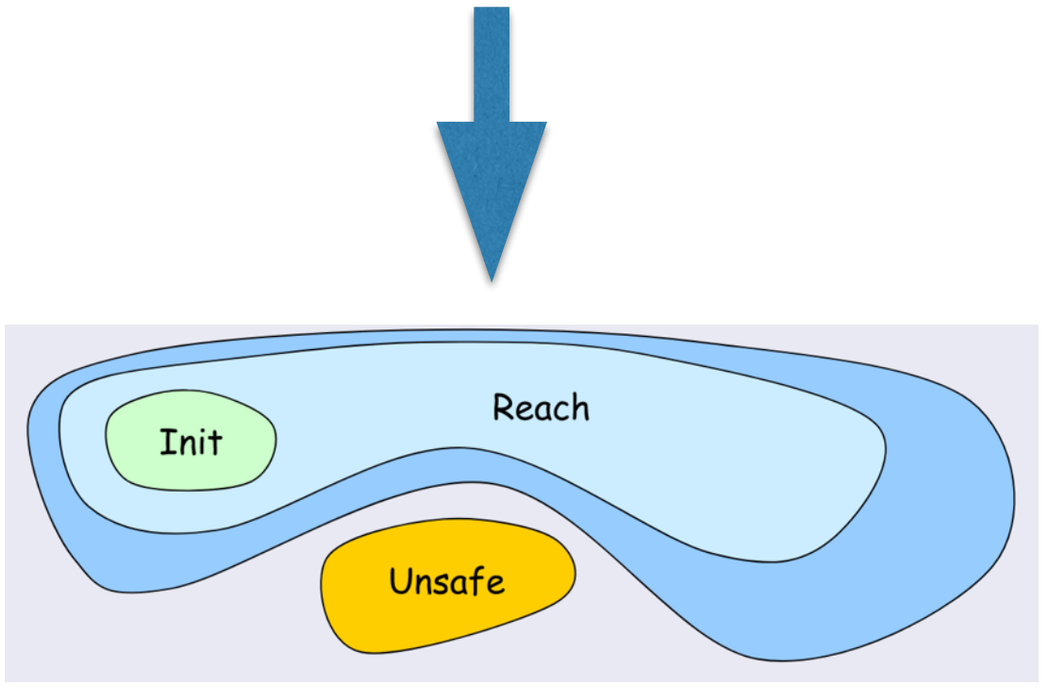
overapproximation

UTEC
Universidad Tecnológica

General idea

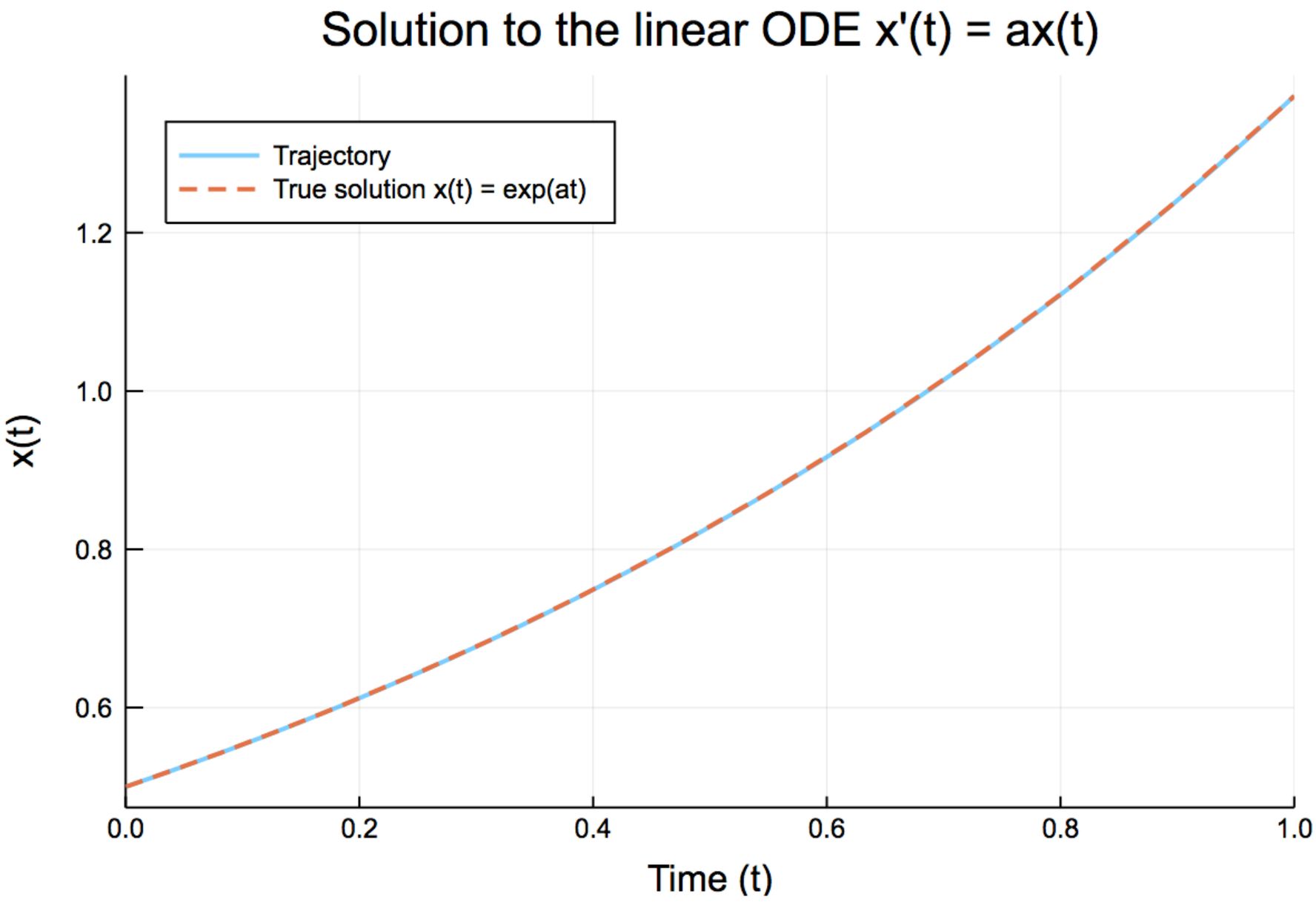


- mathematically rigorous
- exhaustive



UTEC
Universidad Tecnológica

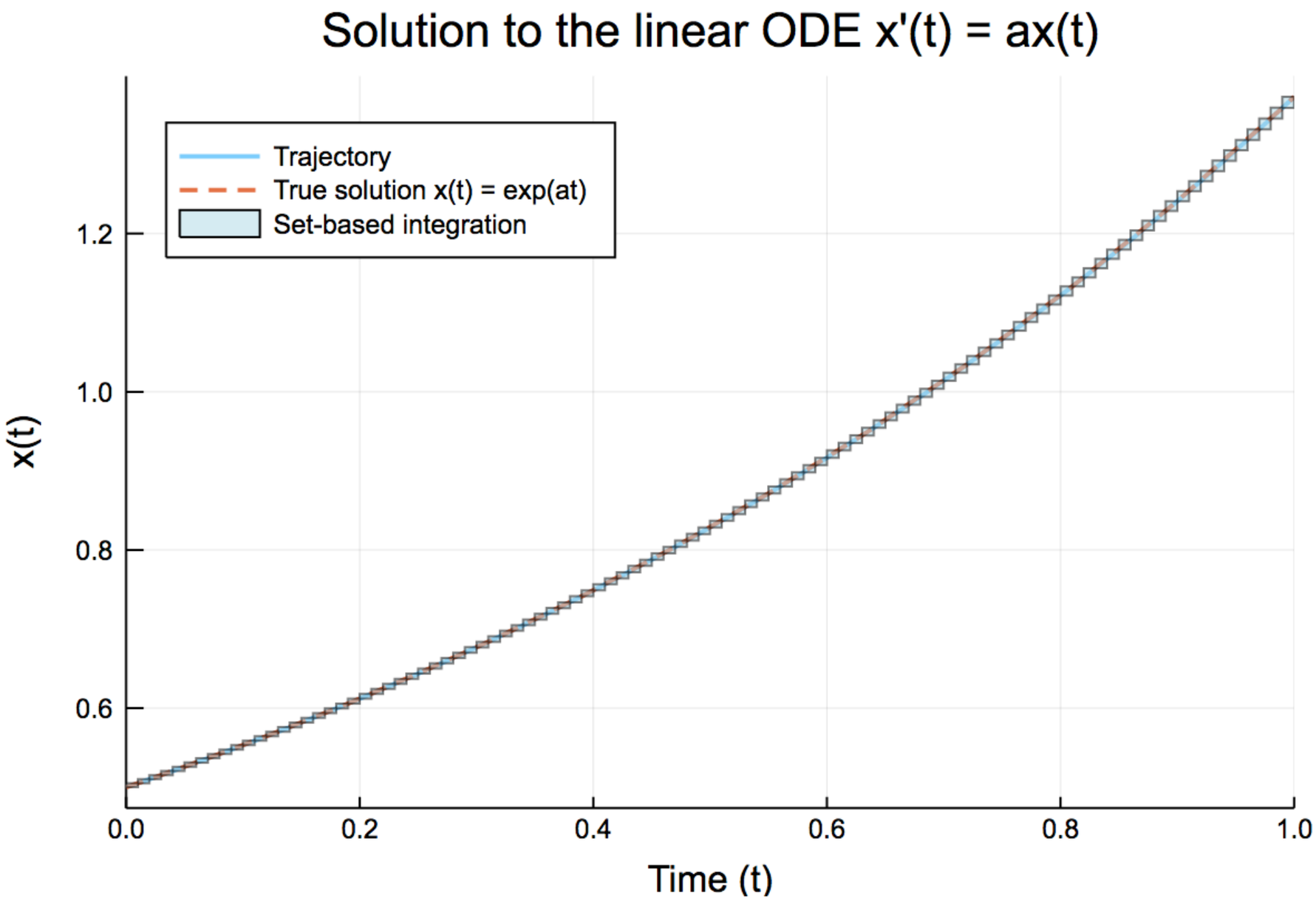
Example



time lapsed = 60ms

UTEC
Universidad Tecnológica

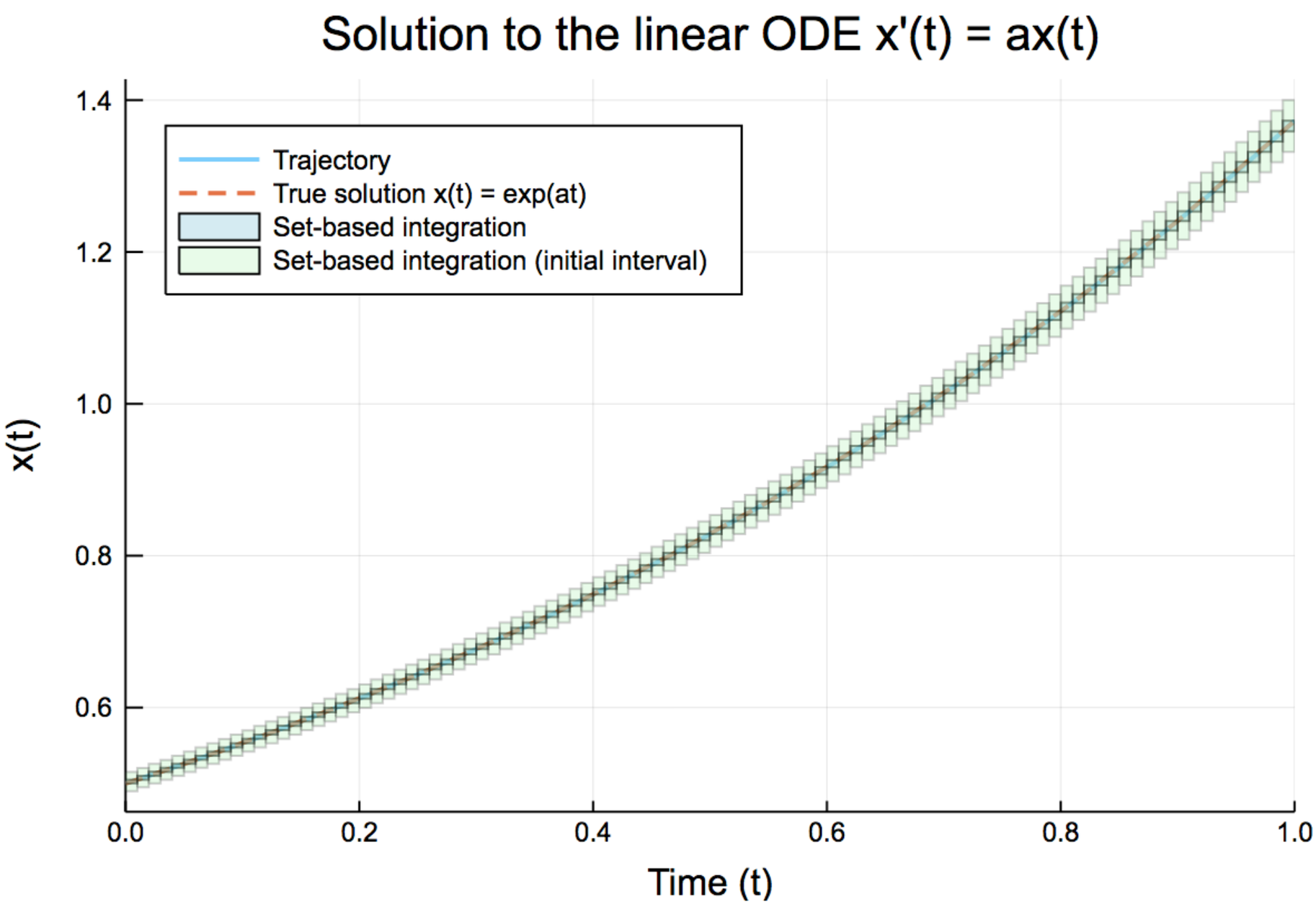
Example



time lapsed = 20ms

UTEC
Universidad Tecnológica

Example



time lapsed = 21ms

UTEC
Universidad Tecnológica

LTI Systems

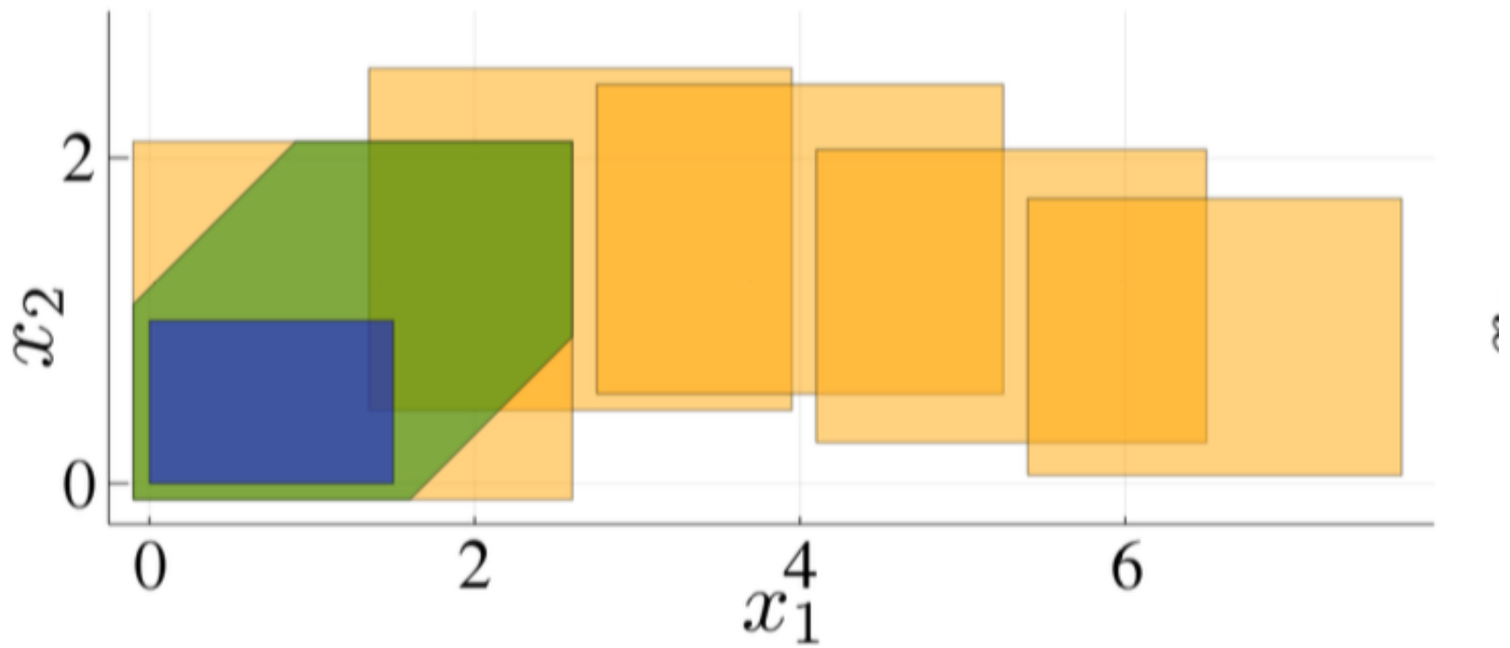
$$\dot{x}(t) = Ax(t) + Bu(t), \quad u(t) \in \mathcal{U}.$$

$$\xi_{x_0,u}(t) = e^{At}x_0 + \int_0^t e^{A(t-s)}Bu(s)\,ds.$$

$$Post_C((A,B,\mathcal{U}),\mathcal{X}_0) := \{\xi_{x_0,u}(t) \mid t \geq 0, x_0 \in \mathcal{X}_0, u(s) \in \mathcal{U} \text{ for all } s\}.$$

UTEC
Universidad Tecnológica

How do we actually compute flowpipes?



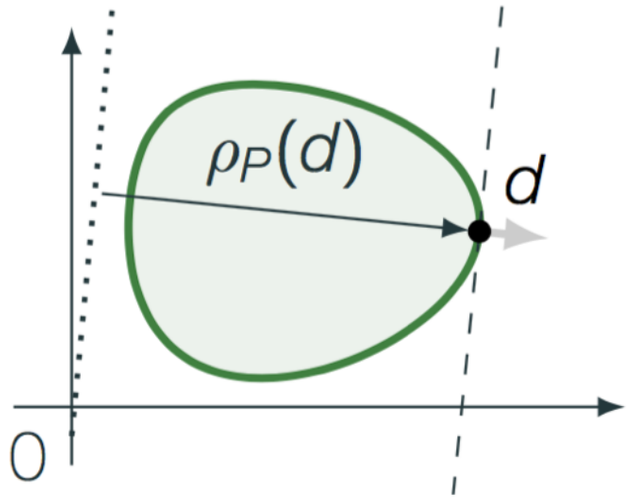
(a)

Fig. 1. (a) Starting from the set of initial states $\mathcal{X}_0$ (blue set), we first compute the set $\mathcal{X}(0)$ by time discretization (green set), then decompose the set into intervals and obtain $\widehat{\mathcal{X}}(0)$ (orange box around $\mathcal{X}(0)$), and finally compute the (decomposed) flowpipe $\widehat{\mathcal{X}}(1), \ldots, \widehat{\mathcal{X}}(4)$ by propagating each of the intervals (other orange sets). **(b)** The flowpipe from (a) together with a guard (red).

Operations on sets can be done efficiently using support functions. . .

- linear programming (LP): efficient for thousands of varaibles

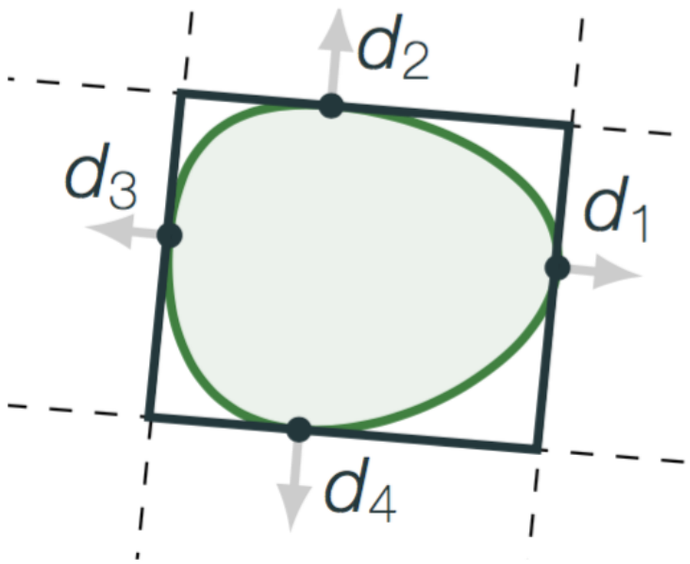
$$\rho_{\mathcal{P}}(\mathbf{d}) = \max\{\mathbf{d}^\top \mathbf{x} \mid \mathbf{x} \in \mathcal{P}\}$$



- (moreover, an analytical formula is available in many interesting cases!)

- we get a polyhedral overapproximation

$$\lceil \mathcal{P} \rceil_{\mathcal{D}} = \bigcap_{\mathbf{d} \in \mathcal{D}} \{\mathbf{d}^\top x \leq \rho_{\mathcal{P}}(\mathbf{d})\}$$



UTEC
Universidad Tecnológica

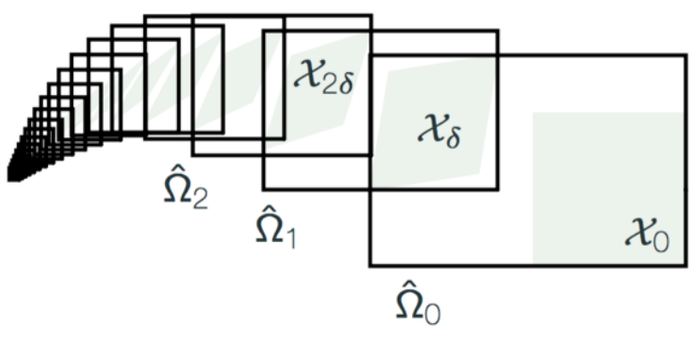
Support functions: computational cost

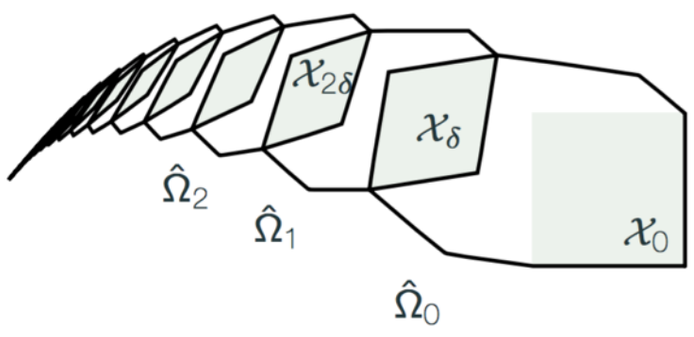
$$\rho_{M\mathcal{X}}(\ell) = \rho_{\mathcal{X}}(M^{\top}\ell),\ \mathcal{O}(mn)$$

$$\rho_{\mathcal{X}\oplus\mathcal{Y}}(\ell) = \rho_{\mathcal{X}}(\ell) + \rho_{\mathcal{Y}}(\ell),\ \mathcal{O}(1)$$

$$\rho_{\mathrm{chull}(\mathcal{P}\cup\mathcal{Q})}(\ell) = \max\{\rho_{\mathcal{P}}(\ell), \rho_{\mathcal{Q}}(\ell)\},\ \mathcal{O}(1)$$

#ops	polyhedra		ellipsoids	zonotopes	support f.
	m constr.	*k* gen.	$n \times n$ matrix	*k* generators	—
convex hull	exp	1	approx	n^2k approx	2#*ops*
Minkowski sum	exp	nk^2	approx	n	2#*ops*
linear map	n^2m / exp	n^2k	n^3	n^2k	n^2 + #*ops*
intersection	1	exp	approx	approx	opt. / approx





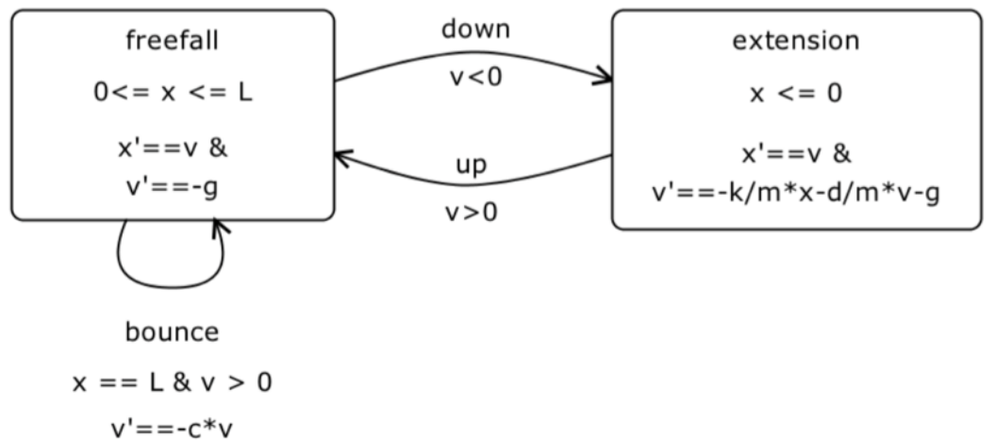
UTEC
Universidad Tecnológica

Going Hybrid: Linear Hybrid Systems

- modes & variables

$$\text{Loc} = \{\ell_1, \ldots, \ell_m\} \qquad X = \{x_1, \ldots, x_n\}$$

define the state space $\text{Loc} \times \mathbb{R}^X$



- transitions $\text{Edg} \subseteq \text{Loc} \times \text{Lab} \times \text{Loc}$

define switching modes with a synchronization label

- invariant $\text{Inv} \subseteq \text{Loc} \times \mathbb{R}^X$
  - flow (ODE) for each modes $\dot{\mathbf{x}} = f(\mathbf{x})$
  - jump relations for each transition $\text{Jump}(e) = \{(\mathbf{x}, \mathbf{x}') \mid \mathbf{x} \in \mathcal{G} \wedge \mathbf{x}' = r(\mathbf{x})\}$
- set of initial states $\text{Init} \subseteq \text{Inv}$

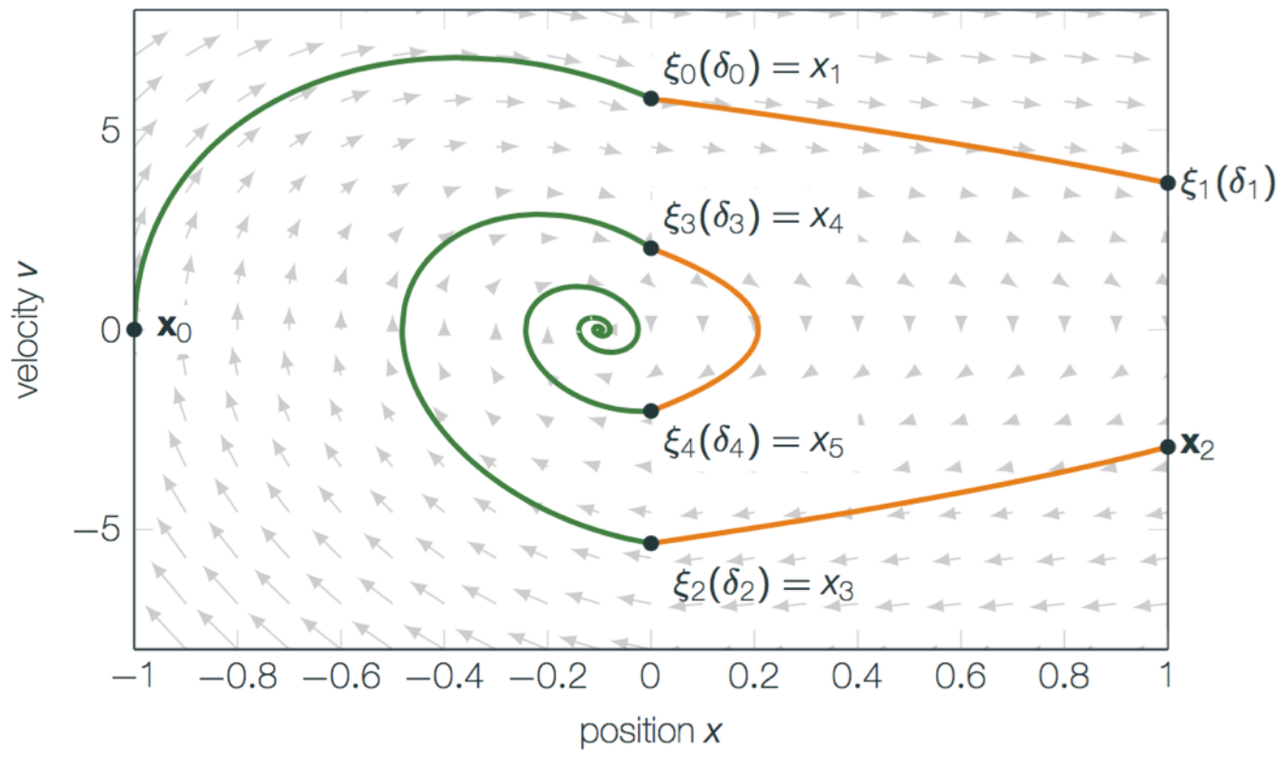
$$Post_D((\ell, \mathcal{X})) := \bigcup_{\ell' \in Loc} \{(\ell', Asgn((\ell, \ell')) \odot (\mathcal{X} \cap Inv(\ell) \cap Grd((\ell, \ell'))) \cap Inv(\ell'))\}$$

Discrete post-operator

$$Post_D((\ell, \mathcal{X})) := \bigcup_{\ell' \in Loc} \{(\ell', Asgn((\ell, \ell')) \odot (\mathcal{X} \cap Inv(\ell) \cap Grd((\ell, \ell'))) \cap Inv(\ell'))\}$$

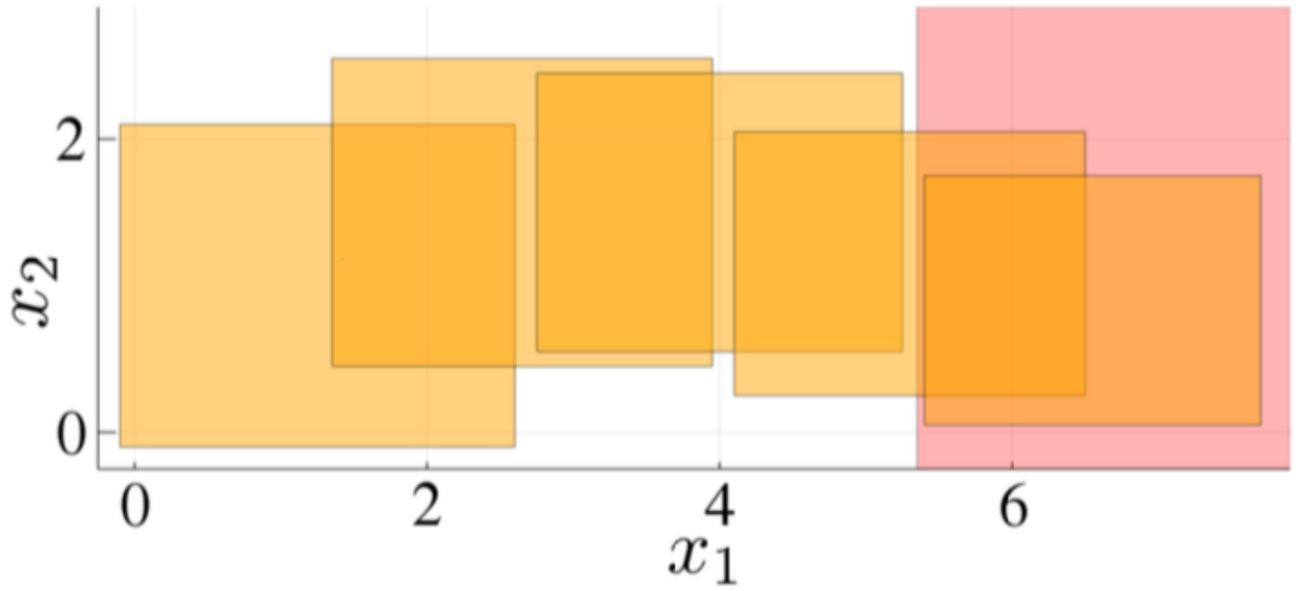
The *reach set* of $\mathcal{H}$ from a set of initial symbolic states $\mathcal{R}_0$ of $\mathcal{H}$ is the smallest set $\mathcal{R}$ of symbolic states such that

$$\mathcal{R}_0 \cup \bigcup_{(\ell,\mathcal{X}) \in \mathcal{R}} Post_D((\ell, Post_C(Flow(\ell), \mathcal{X}))) \subseteq \mathcal{R}. \quad (3)$$



$$(\ell_0, \mathbf{x}_0) \xrightarrow{\delta_0, \xi_0} (\ell_0, \xi_0(\delta_0)) \xrightarrow{\alpha_0} (\ell_1, \mathbf{x}_1) \xrightarrow{\delta_1, \xi_1} (\ell_1, \xi_1(\delta_1)) \ldots$$

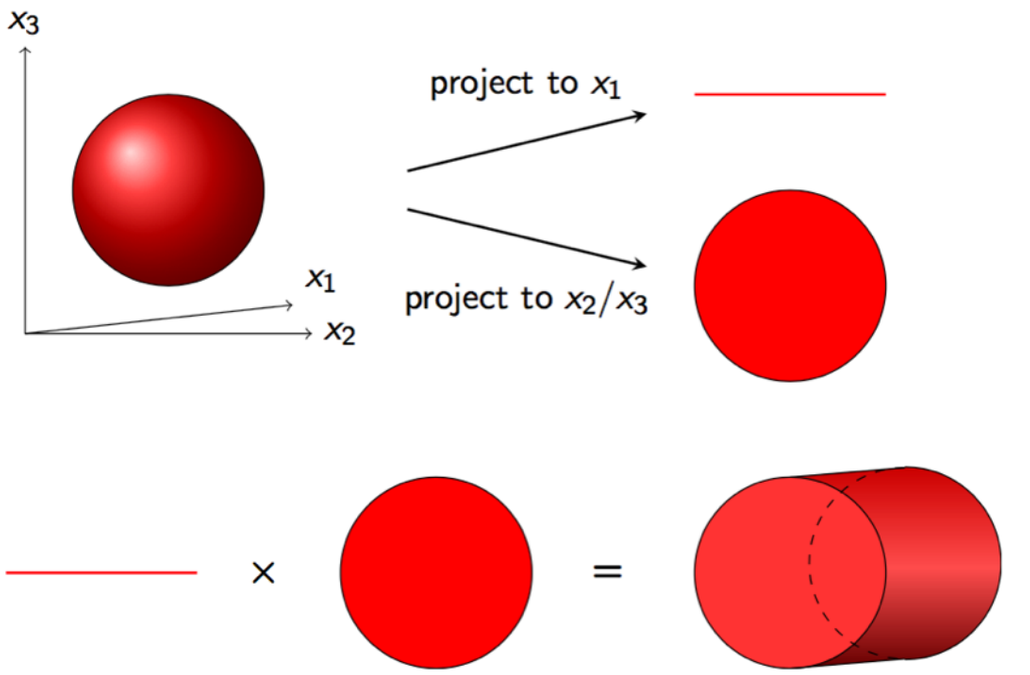
How do we actually compute flowpipes?

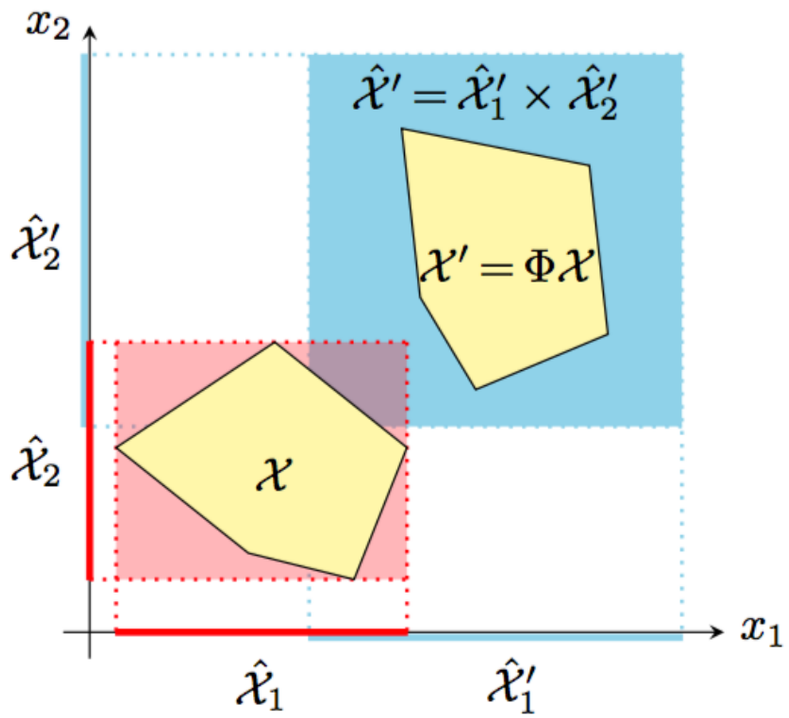


(b)

Fig. 1. (a) Starting from the set of initial states $\mathcal{X}_0$ (blue set), we first compute the set $\mathcal{X}(0)$ by time discretization (green set), then decompose the set into intervals and obtain $\widehat{\mathcal{X}}(0)$ (orange box around $\mathcal{X}(0)$), and finally compute the (decomposed) flowpipe $\widehat{\mathcal{X}}(1), \ldots, \widehat{\mathcal{X}}(4)$ by propagating each of the intervals (other orange sets). **(b)** The flowpipe from (a) together with a guard (red).

Decomposed reachability analysis





- HSCC'18

Reach Set Approximation through Decomposition with Low-dimensional Sets and High-dimensional Matrices

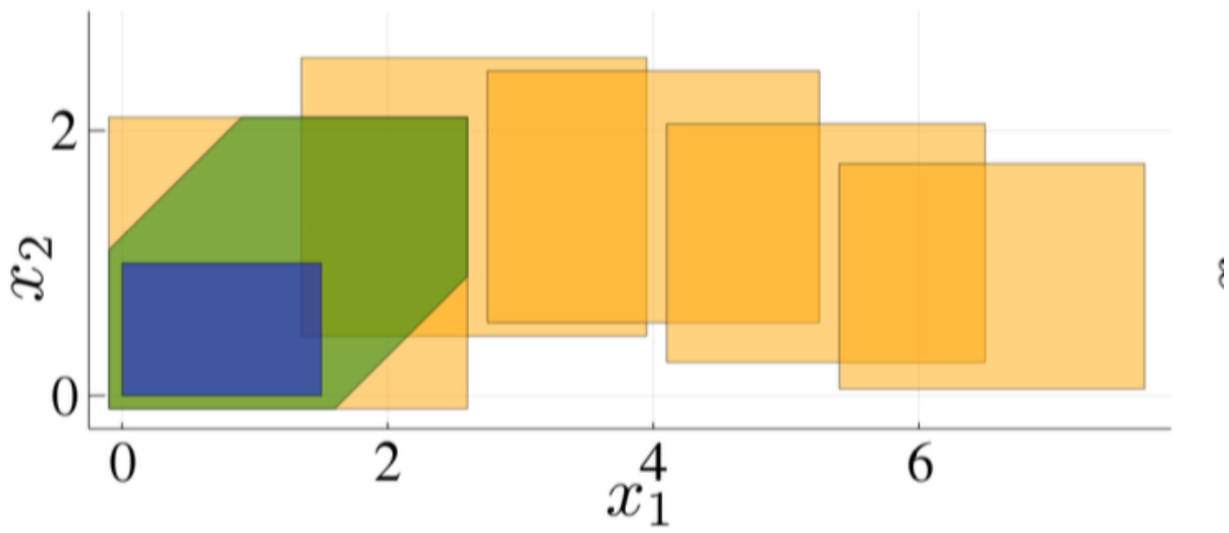
Sergiy Bogomolov
Australian National University
Canberra, Australia

Marcelo Forets
Goran Frehse
Frédéric Viry
Univ. Grenoble Alpes, VERIMAG
Grenoble, France

Andreas Podelski
Christian Schilling
University of Freiburg
Freiburg, Germany

UNIVERSITÉ Grenoble Alpes
Australian National University
Verimag
UNI FREIBURG
UTEC Universidad Tecnológica

Decomposed reachability analysis



(a)

$$\mathcal{X}(k) := \Phi\mathcal{X}(k-1) \oplus \mathcal{V} = \Phi^k\mathcal{X}(0) \oplus \bigoplus_{j=0}^{k-1} \Phi^j\mathcal{V}.$$

$$\mathcal{X}_i(k) := \bigoplus_{j=1}^{b} \Phi_{ij}^k\mathcal{X}_j(0) \oplus \bigoplus_{j=0}^{k-1} [\Phi_{i1}^j \cdots \Phi_{ib}^j]\mathcal{V} \qquad \text{where } \Phi^j = \begin{pmatrix} \Phi_{11}^j & \cdots & \Phi_{1b}^j \\ \vdots & \ddots & \vdots \\ \Phi_{b1}^j & \cdots & \Phi_{bb}^j \end{pmatrix}.$$

The above sequences $\mathcal{X}(k)$ resp. $\widehat{\mathcal{X}}(k)$ are called flowpipes.

UTEC
Universidad Tecnológica

Extension of decomposed reachability to Hybrid Systems

- **Results:**

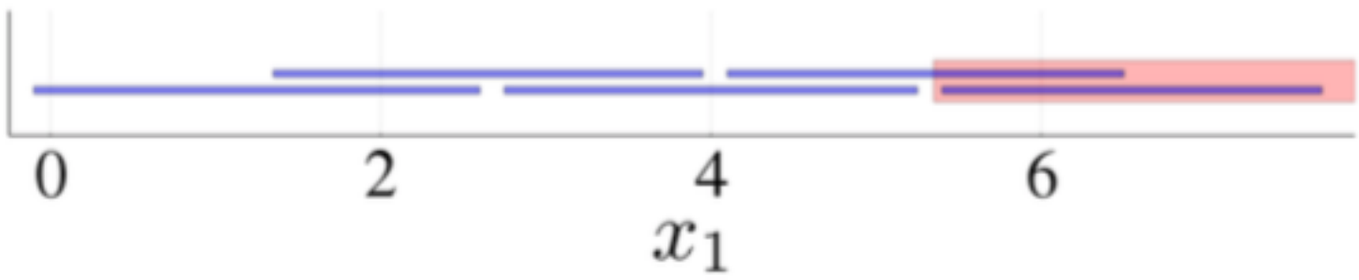
> We have presented an algorithm that integrates a decomposition-based reachability algorithm for LTI systems in the analysis loop for linear hybrid systems. The key insight is that intersections with polyhedral constraints can be efficiently detected and computed (approximately or often even exactly) in low dimensions. This enables the systematic focus on appropriate subspaces and the potential for bypassing large amounts of flowpipe computations.

UTEC
Universidad Tecnológica

Key idea 1) Exploit decomposed structure

Recall that $Post_C^{\square}$ computes flowpipes consisting of decomposed sets. The first improvement is to exploit the decomposed structure in order to perform all other operations (intersection, affine map, inclusion check, and convex hull) in low dimensions.

- Decomposed *intersections*



UTEC
Universidad Tecnológica

Key idea 1) Exploit decomposed structure

- Decomposed *intersections*

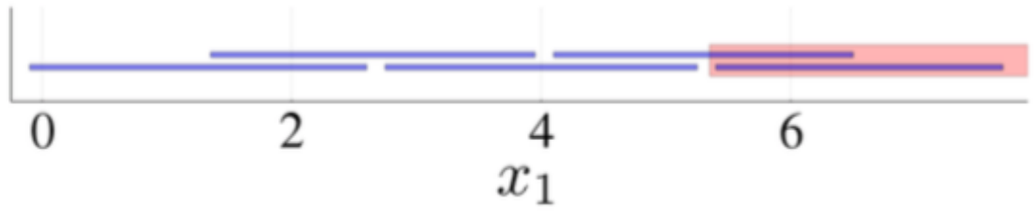


Fig. 3. The flowpipe from Figure 1(a) in dimension x_1 only consists of intervals (blue). The constraint $\mathcal{G}_1$ (red) is the guard $\mathcal{G}$ projected to x_1. For better visibility, we draw the sets thicker and add a slight offset to some of the intervals.

Example. Consider again Figure 3. We have already identified the intersection with the flowpipe for time steps 3 and 4. The resulting sets for $k = 3$ and $k = 4$ are $\widehat{\mathcal{X}}(k) \cap \mathcal{G} = \mathcal{X}_1(k) \cap \mathcal{G}_1 \times \mathcal{X}_2(k)$, where $\mathcal{G}_1$ was the projection of $\mathcal{G}$ to x_1. We emphasize that we compute the intersections in low dimensions, that we need not compute $\mathcal{X}_2(1)$ and $\mathcal{X}_2(2)$ at all, and that in this example all computations are exact (i.e., we obtain the same sets as in Figure 2(a)).

UTEC
Universidad Tecnológica

Key idea 2) Compute sparse flowpipes

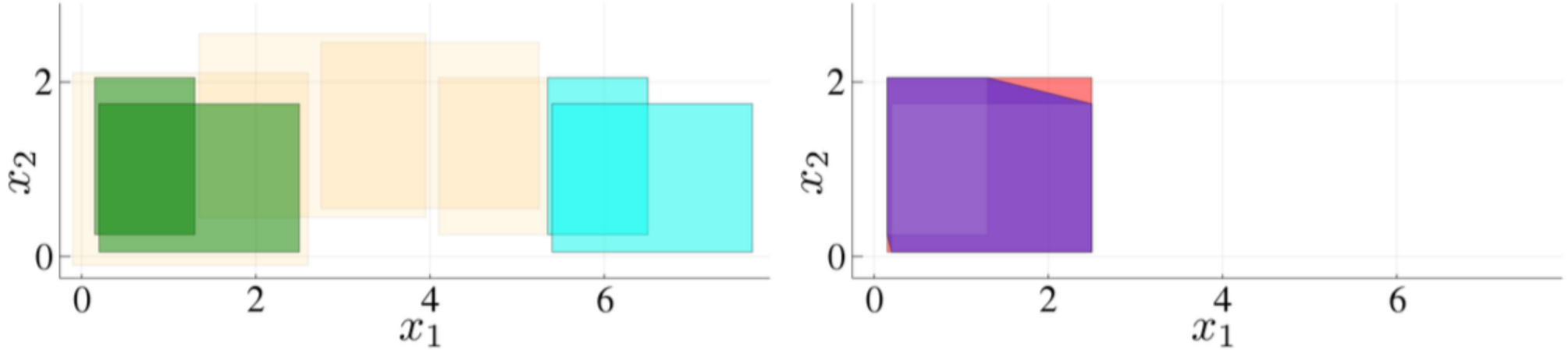
The second improvement is to compute flowpipes in a sparse way. Roughly speaking, we are only interested in those dimensions of a flowpipe that are relevant to determine intersection with a guard. Hence we only need to compute the other dimensions of the flowpipe after we detected such an intersection.

Example. Figure 2(b) shows the decomposed convex hull of the sets $\widehat{\mathcal{X}}(3) \cap \mathcal{G}$ and $\widehat{\mathcal{X}}(4) \cap \mathcal{G}$ after applying the translation. Since each block is one-dimensional in our example, we obtain the box approximation.

UTEC
Universidad Tecnológica

Key idea 2) Compute sparse flowpipes

The second improvement is to compute flowpipes in a sparse way. Roughly speaking, we are only interested in those dimensions of a flowpipe that are relevant to determine intersection with a guard. Hence we only need to compute the other dimensions of the flowpipe after we detected such an intersection.

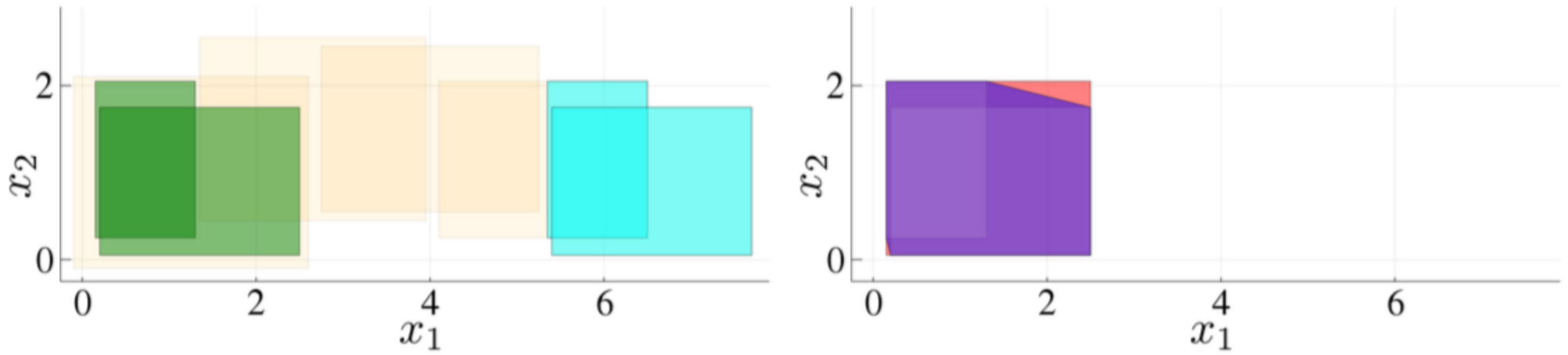


(a) **(b)**

Proposition 5. *Let* $\widehat{\mathcal{X}} = \bigtimes_j \mathcal{X}_j \in \mathcal{C}_n, \widehat{\mathcal{Y}} = \bigtimes_j \mathcal{Y}_j \in \mathcal{C}_n$ *be nonempty sets with identical block structure. Then* $\mathrm{CH}(\widehat{\mathcal{X}} \cup \widehat{\mathcal{Y}}) \subseteq \bigtimes_j \mathrm{CH}(\mathcal{X}_j \cup \mathcal{Y}_j)$.

UTEC
Universidad Tecnológica

Key idea 2) Compute sparse flowpipes



(a) **(b)**

Example. Figure 2(b) shows the decomposed convex hull of the sets $\widehat{\mathcal{X}}(3) \cap \mathcal{G}$ and $\widehat{\mathcal{X}}(4) \cap \mathcal{G}$ after applying the translation. Since each block is one-dimensional in our example, we obtain the box approximation.

Fig. 2. **(a)** The intersection of the flowpipe and the guard from Figure 1(b) (cyan) is shifted to the left by applying a translation (green). Both sets are contained in the first set of the flowpipe. **(b)** We approximate the union of the green sets from (a) using the convex hull (purple) and the decomposed convex hull (red).

UTEC
Universidad Tecnológica

Theoretical error bounds

Proposition 1. *Let $\mathcal{X} \in \mathcal{C}_n$ be nonempty, $p = \infty$, $r^p_{\mathcal{X}}$ be the radius of the box approximation of $\mathcal{X}$, and let π_j be appropriate projection matrices. Then $d^p_H(\mathcal{X}, \bigtimes_j \pi_j \mathcal{X}) \leq \|r^p_{\mathcal{X}}\|_p$.*

Proposition 2. *Let $\widehat{\mathcal{X}} = \bigtimes_j \mathcal{X}_j \in \mathcal{C}_n$, $\mathcal{Y} \in \mathcal{C}_n$, $\widehat{\mathcal{X}} \cap \mathcal{Y} \neq \emptyset$, $\widehat{\mathcal{Y}} := \bigtimes_j \pi_j \mathcal{Y}$ for appropriate projection matrices π_j corresponding to $\mathcal{X}_j$, and $p = \infty$. Then*

$$d^p_H(\widehat{\mathcal{X}} \cap \mathcal{Y}, \widehat{\mathcal{X}} \cap \widehat{\mathcal{Y}}) \leq \max_j \min(\|\Delta_p(\mathcal{X}_j)\|_p, \|\Delta_p(\pi_j \mathcal{Y})\|_p).$$

UTEC
Universidad Tecnológica

Theoretical error bounds

Proposition 3. *[11, Prop. 3] Let* $\mathcal{X} = \bigtimes_{j=1}^{b} \mathcal{X}_j \in \mathcal{C}_n$ *be nonempty,* $A \in \mathbb{R}^{n\times n}$, $q_j := \arg\max_i \|A_{ij}\|_p$ *(the index of the block with the largest matrix norm in the* j*-th block column) so that* $\alpha_j := \max_{i\neq q_j} \|A_{ij}\|_p$ *is the second largest matrix norm in the* j*-th block column. Let* $\alpha_{max} := \max_j \alpha_j$ *and* $\Delta_{sum} := \sum_j \Delta_\infty(\mathcal{X}_j)$. *Then*

$$d_H^p(A\mathcal{X}, \bigtimes_i \bigoplus_j A_{ij}\mathcal{X}_j) = \max_{\|d\|_p\leq 1} \sum_{i,j} \rho_{\mathcal{X}_j}(A_{ij}^T d_i) - \rho_{\mathcal{X}_j}\left(\sum_k A_{kj}^T d_k\right)$$

$$\leq (b-1)\sum_j \alpha_j \Delta_\infty(\mathcal{X}_j) \leq \frac{n}{2}\alpha_{max}\Delta_{sum}.$$

UTEC
Universidad Tecnológica

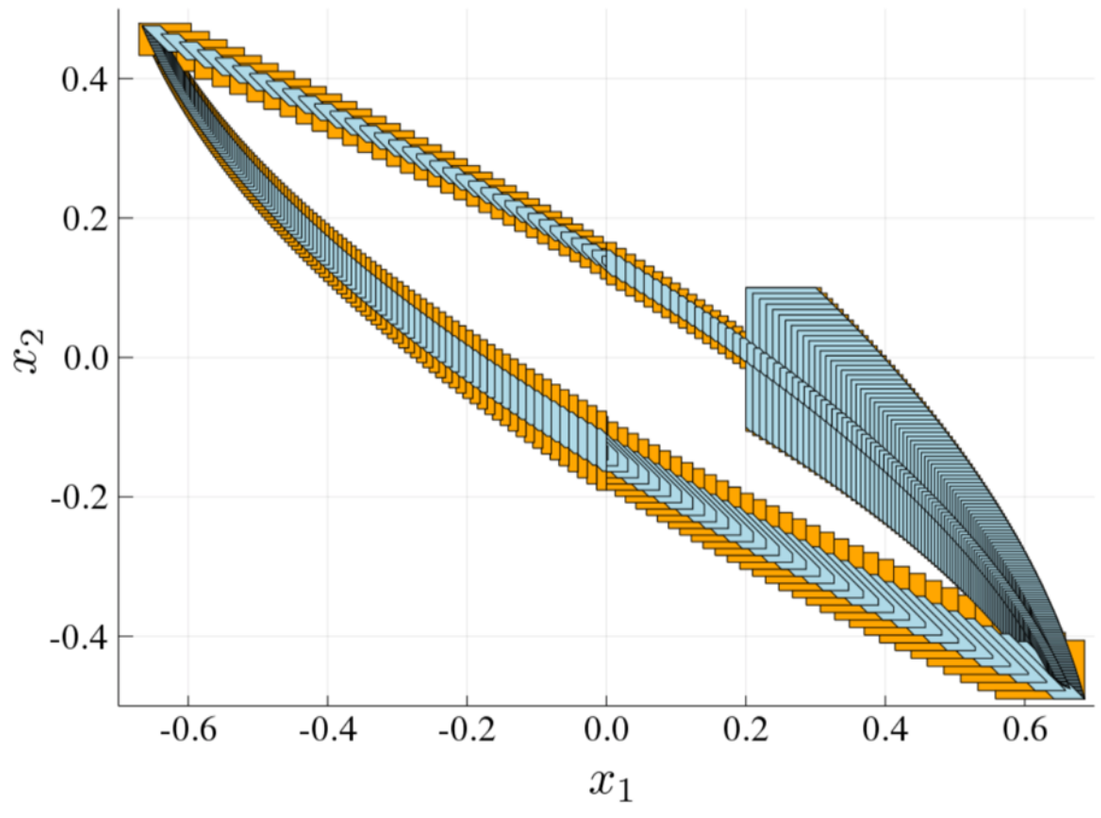
Our Recent Contribution

Reachability analysis of linear hybrid systems via block decomposition*

Sergiy Bogomolov[1], Marcelo Forets[2], Goran Frehse[3], Kostiantyn Potomkin[1], and Christian Schilling[4]

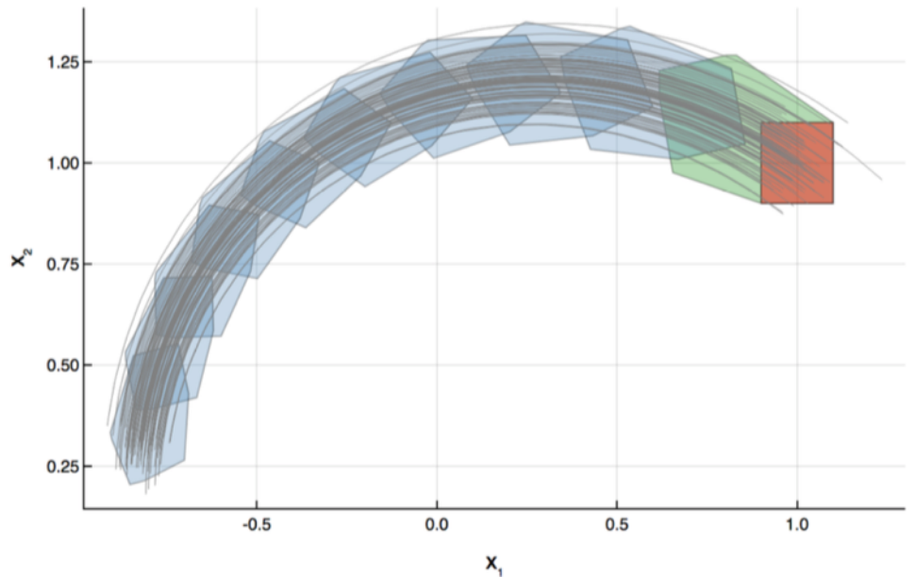
[1] Australian National University, Canberra, Australia
[2] Universidad de la República, CURE, Maldonado, Uruguay
[3] ENSTA ParisTech - U2IS, Palaiseau Cedex, France
[4] IST Austria, Klosterneuburg, Austria

Benchmark	Dim.	Jump	Block	Step	High-dim.	Low-dim.
spacecraft_noabort	5	1	1	0.04	1.4×10^1	7.6×10^0
spacecraft_120	5	2	1	0.04	4.3×10^0	5.0×10^0
linear_switching	5	4	1	0.001	1.2×10^0	9.0×10^{-1}
platoon_t20	10	4	1	0.001	5.3×10^1	1.1×10^1
platoon_tInf	10	52	1	0.001	8.5×10^2	1.4×10^2
filtered_osc256	256	5	1	0.01	1.6×10^2	3.1×10^1
filtered_osc256	256	5	2	0.01	1.2×10^2	1.8×10^1
filtered_osc256	256	5	2	0.0005	1.9×10^3	2.0×10^2
filtered_osc512	512	5	2	0.01	5.5×10^2	7.6×10^1
filtered_osc512	512	5	2	0.0005	TO	8.3×10^2
filtered_osc1024	1024	5	2	0.01	TO	5.0×10^2
filtered_osc1024	1024	5	2	0.0005	TO	3.4×10^3

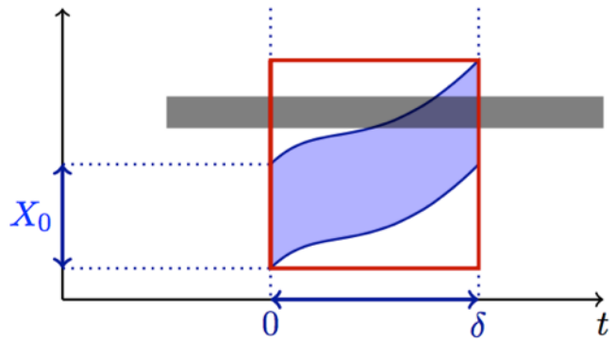


Perspectives

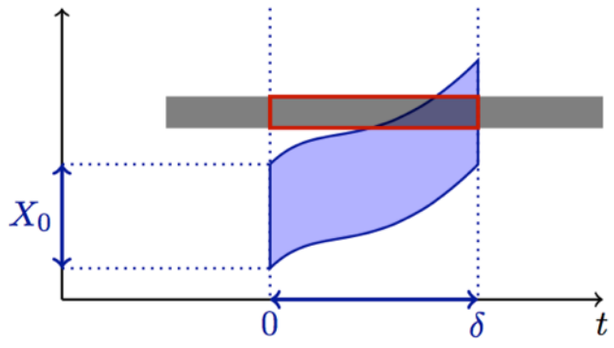
- Probabilistic reachability



- Improve flowpipe/guard intersection for Taylor-model based methods



(a) Over-approximate the flowpipe by a box



(b) Compute the intersection of the box and the guard

UTEC
Universidad Tecnológica

Perspectives

- Parallel Reachability Methods (eg. GPUs)

- Benchmarking and Application Domains

UTEC
Universidad Tecnológica

References

- Pictures in the introduction slides:

Safety Verification of Autonomous Vehicles for Coordinated Evasive Maneuvers

Matthias Althoff, Daniel Althoff, Dirk Wollherr and Martin Buss

Safe, Aggressive Quadrotor Flight via Reachability-based Trajectory Design

Shreyas Kousik, Patrick Holmes, Ram Vasudevan*

- Nonlinear ODEs:

ARCH-COMP19 Category Report:
Continuous and Hybrid Systems with Nonlinear Dynamics

Fabian Immler[1], Matthias Althoff[2], Luis Benet[3], Alexandre Chapoutot[4], Xin Chen[5], Marcelo Forets[6], Luca Geretti[7], Niklas Kochdumper[2], David P. Sanders[8], and Christian Schilling[9]

[1] Computer Science Department, Carnegie Mellon University, United States
fimmler@cs.cmu.edu
[2] Technische Universität München, Munich, Germany
althoff@in.tum.de,niklas.kochdumper@tum.de
[3] Instituto de Ciencias Físicas, Universidad Nacional Autónoma de México (UNAM), México
benet@icf.unam.mx
[4] ENSTA ParisTech, Palaiseau, France
alexandre.chapoutot@ensta-paristech.fr
[5] University of Dayton, Dayton, OH, United States
xchen4@udayton.edu
[6] Universidad de la República, Uruguay
mforets@gmail.com
[7] University of Verona, Verona, Italy
luca.geretti@univr.it
[8] Departamento de Física, Facultad de Ciencias Físicas, Universidad Nacional Autónoma de México (UNAM), México
dpsanders@ciencias.unam.mx
[9] IST Austria, Klosterneuburg, Austria
christian.schilling@ist.ac.at

UTEC
Universidad Tecnológica

UTEC
Universidad Tecnológica