Analyse d'Atteignabilité des Systèmes Dynamiques Hybrides

Antoine Girard

Laboratoire des Signaux et Systèmes, CNRS
Gif-sur-Yvette, France

LMCS 2015, Rennes

24 novembre, 2015

Hybrid systems

Dynamical systems with continuous and discrete behaviors.

- In the physical sciences :
  - Models are traditionally continuous (ODE, PDE...) ;
  - Numerous sources of hybrid behaviors : mechanical impacts, electrical diodes, biological switches...
- In computer science :
  - Models of reactive systems are discrete (Automata, DEDS...) ;
  - Models become hybrid when reactive systems are subject to timing constraints (Timed Automata) or are interacting with the physical world (Hybrid Automata).

Theory of hybrid systems has rapidly grown since the 90s at the interface of computer science and control theory.

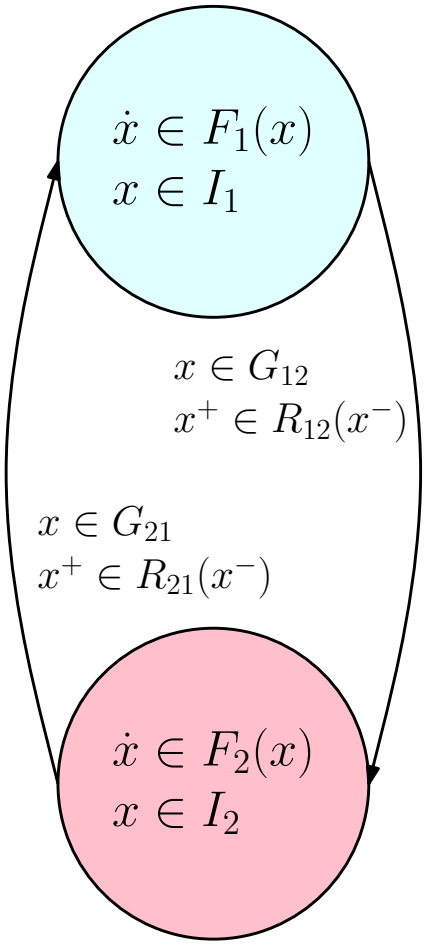
Outline of the talk

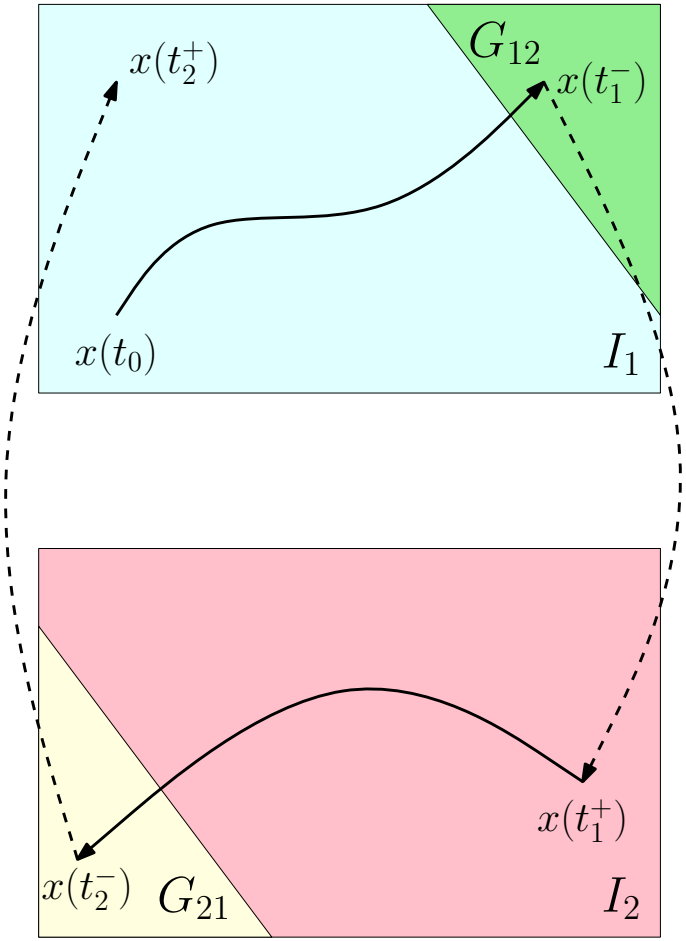
- Reachability analysis of hybrid systems
  - Fundamentals of reachability analysis
  - Approximation of the reachable set of linear systems
  - Applications

Joint work with C. Le Guernic, O. Maler, G. Frehse, M. Al Khatib and T. Dang.

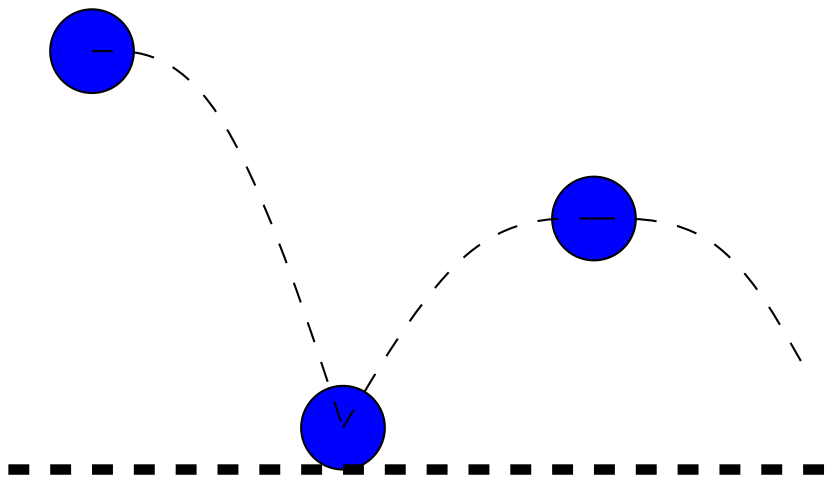
Hybrid automaton

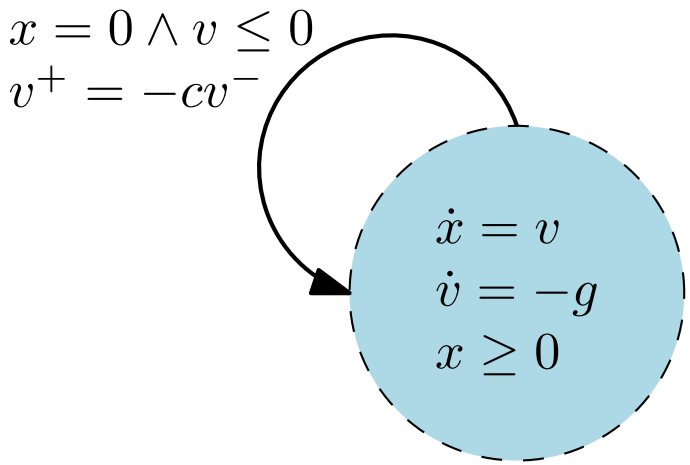
Popular mathematical description of hybrid systems.



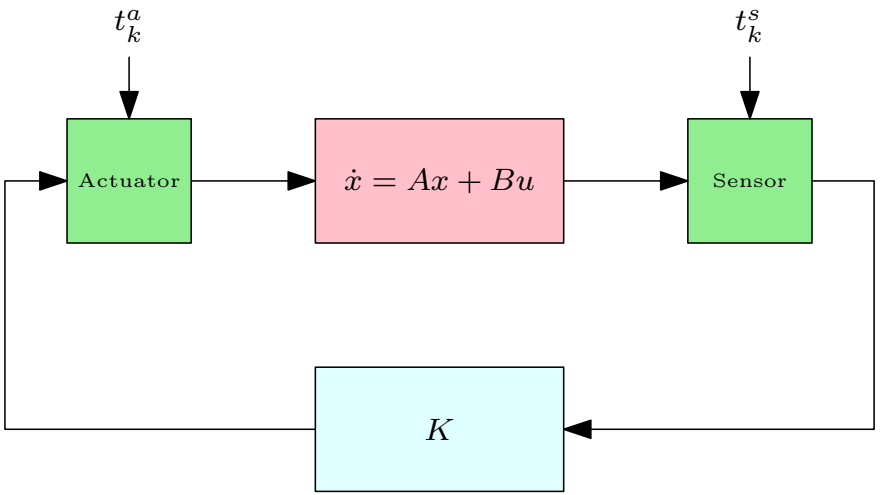


Example : bouncing ball



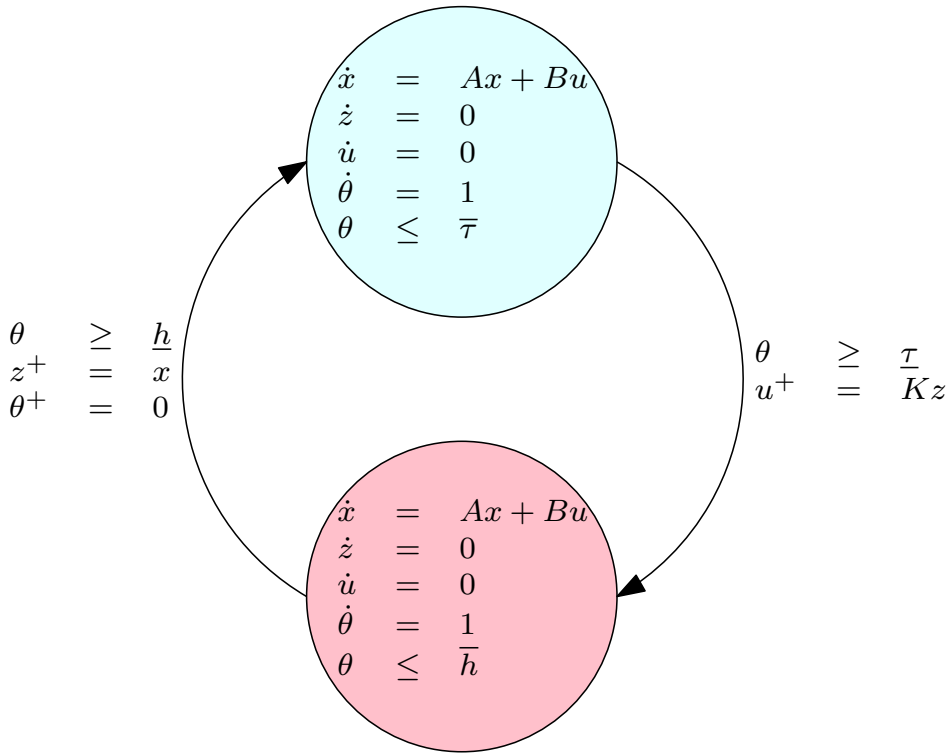


Example : embedded control system



Timing contract:

$$\begin{cases} t_k^a - t_k^s \in [\underline{\tau}, \overline{\tau}] \\ t_{k+1}^s \geq t_k^a \\ t_{k+1}^s - t_k^s \in [\underline{h}, \overline{h}] \end{cases}$$

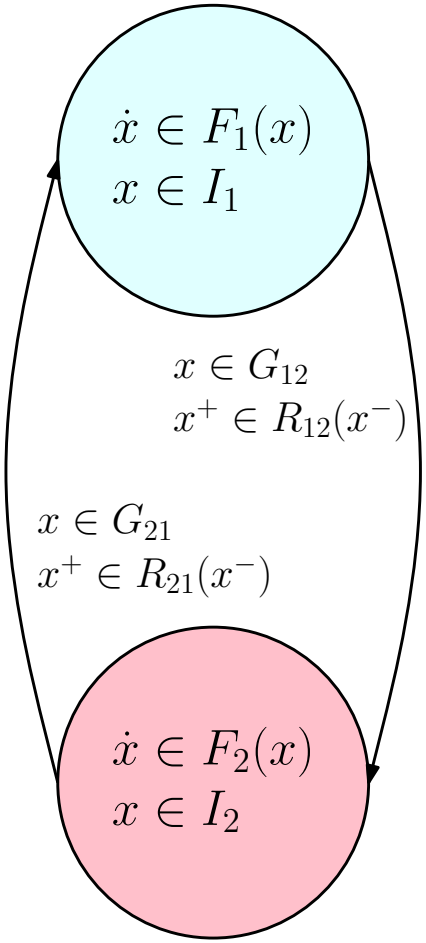


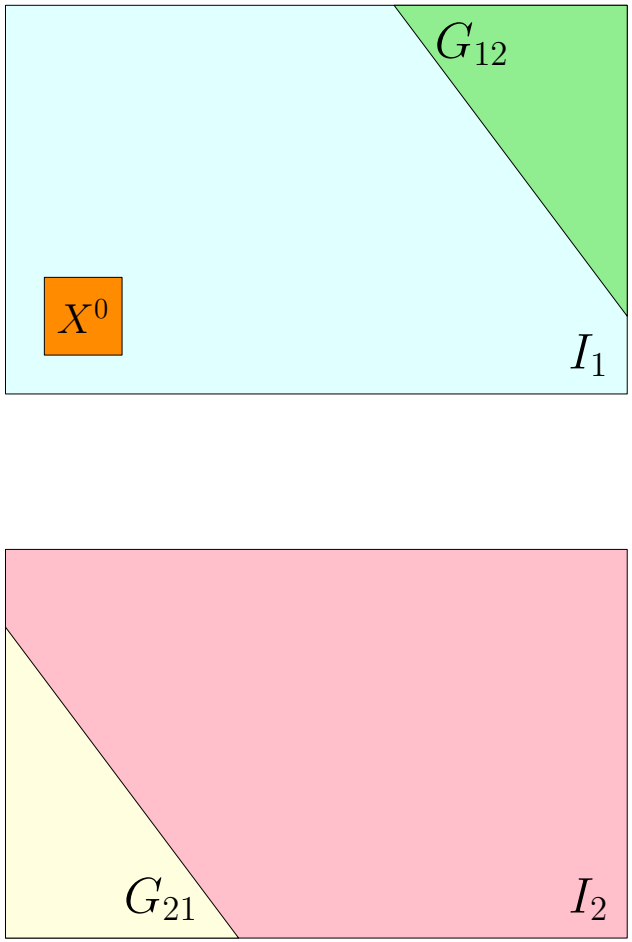
Hybrid automaton

- Several sources of non-determinism :
  - Differential inclusions, enabling guards, set-valued resets...
  - Result of disturbance modeling, system abstraction, partial specification...
- No continuity w.r.t. initial conditions, parameters...
- Simulation not always suitable for exploring effectively the behaviors of a hybrid automaton.
- Reachability analysis :
  - Compute the set of all trajectories for all initial conditions and parameters under all manifestations of non-determinism...
  - Interesting by itself ; useful for verification, controller synthesis, computation of symbolic models...

Reachability analysis

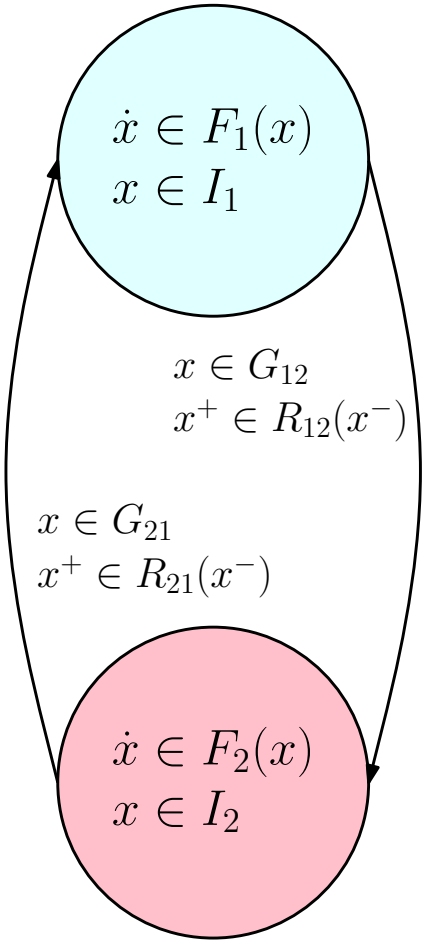
Reachability algorithm, informally :

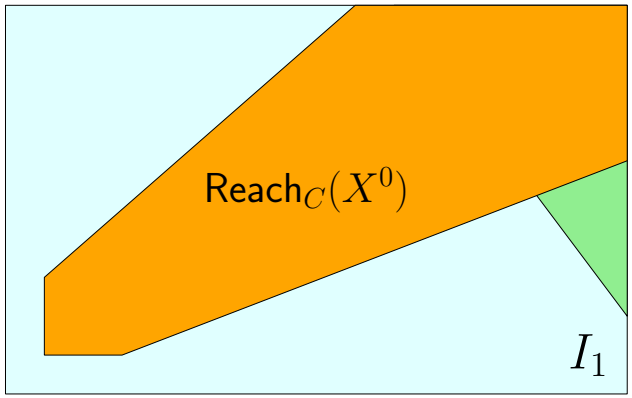


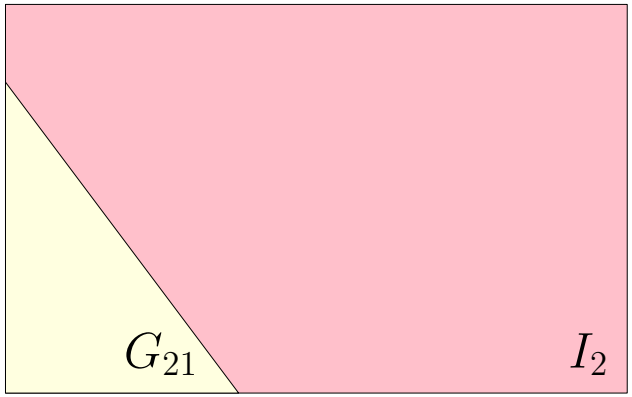


Reachability analysis

Reachability algorithm, informally :

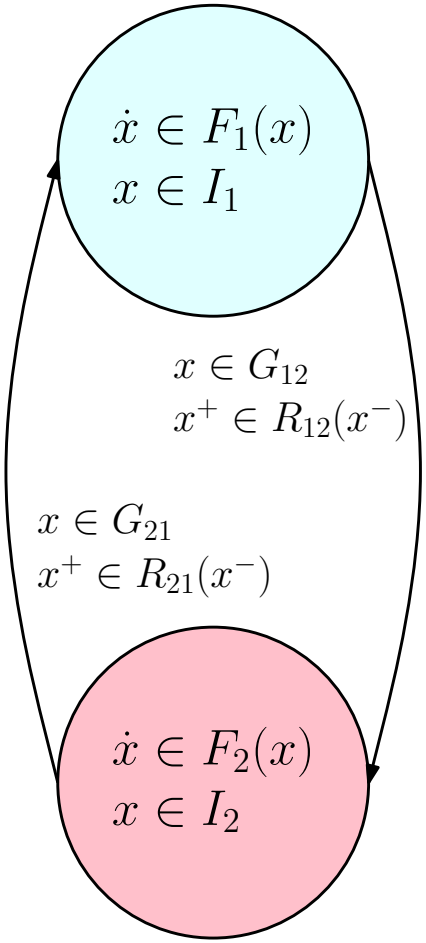


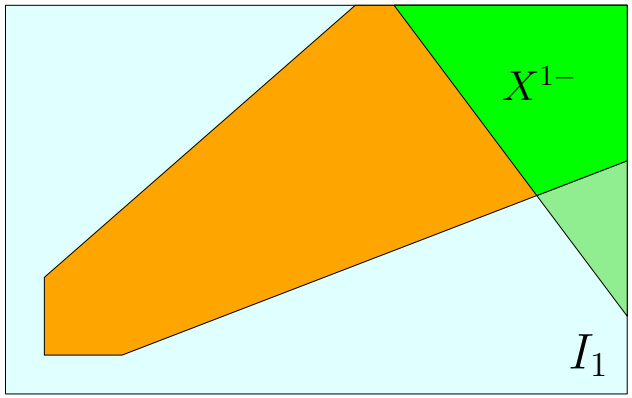


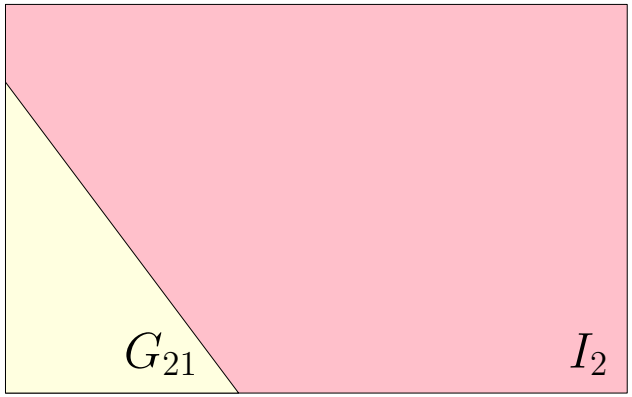


Reachability analysis

Reachability algorithm, informally :

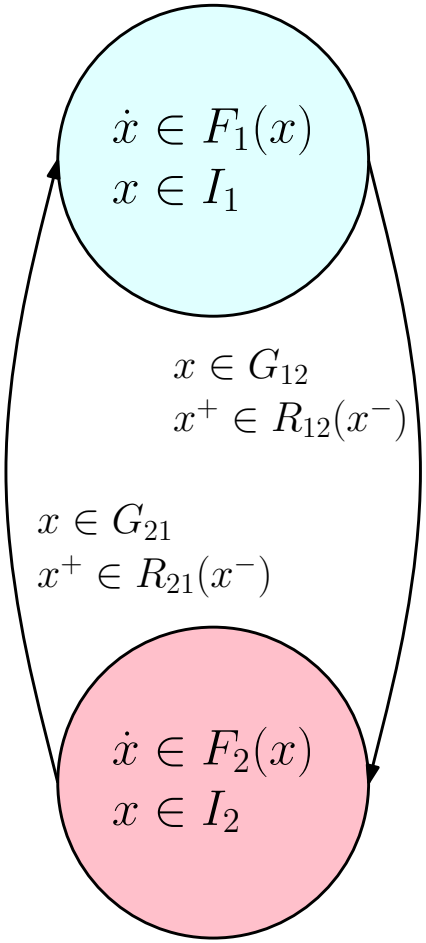


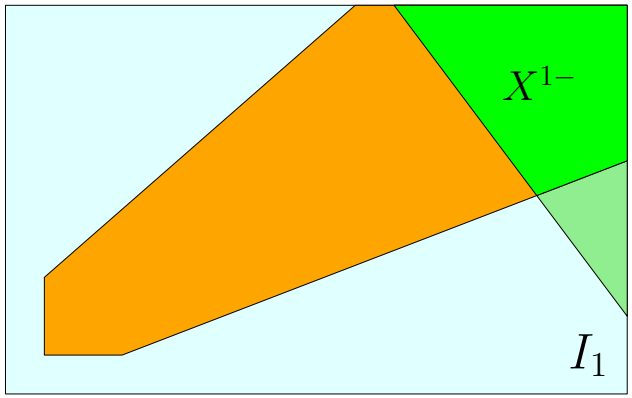


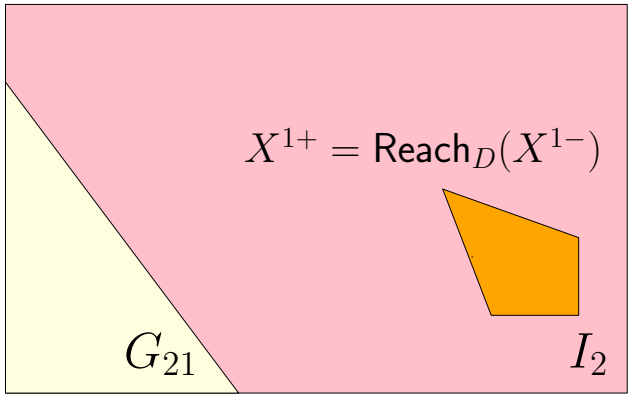


Reachability analysis

Reachability algorithm, informally :

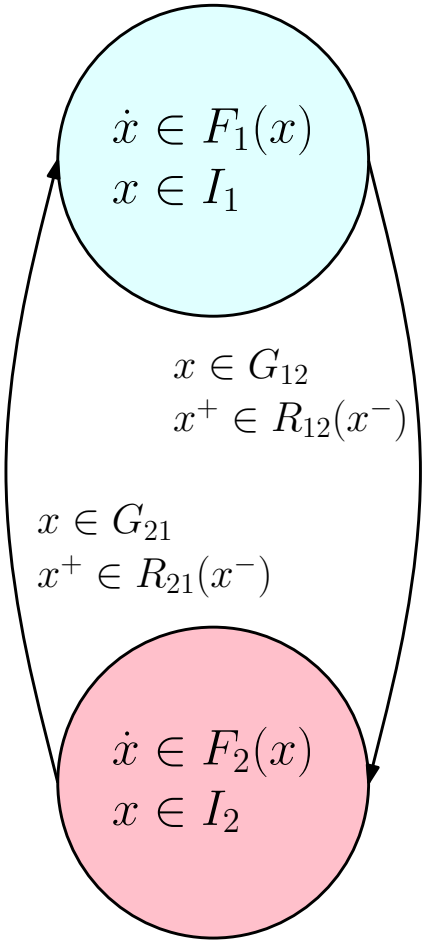


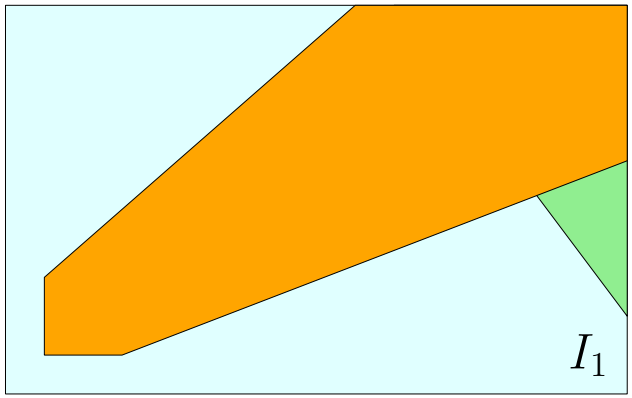


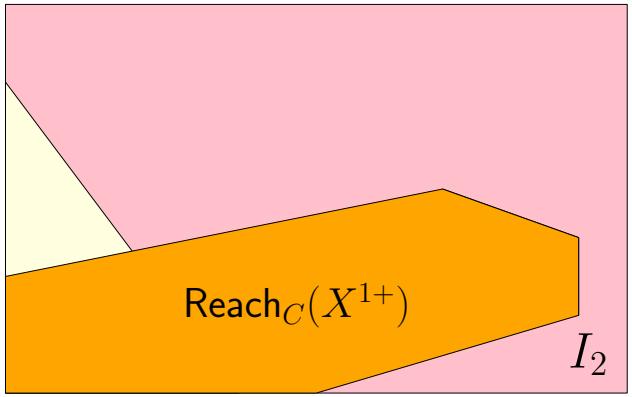


Reachability analysis

Reachability algorithm, informally :







Reachability analysis of linear systems

- Consider a linear system of the form :

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + \mathbf{v}(t),\ \mathbf{x}(0) \in X^0\ \mathbf{v}(t) \in V,$$

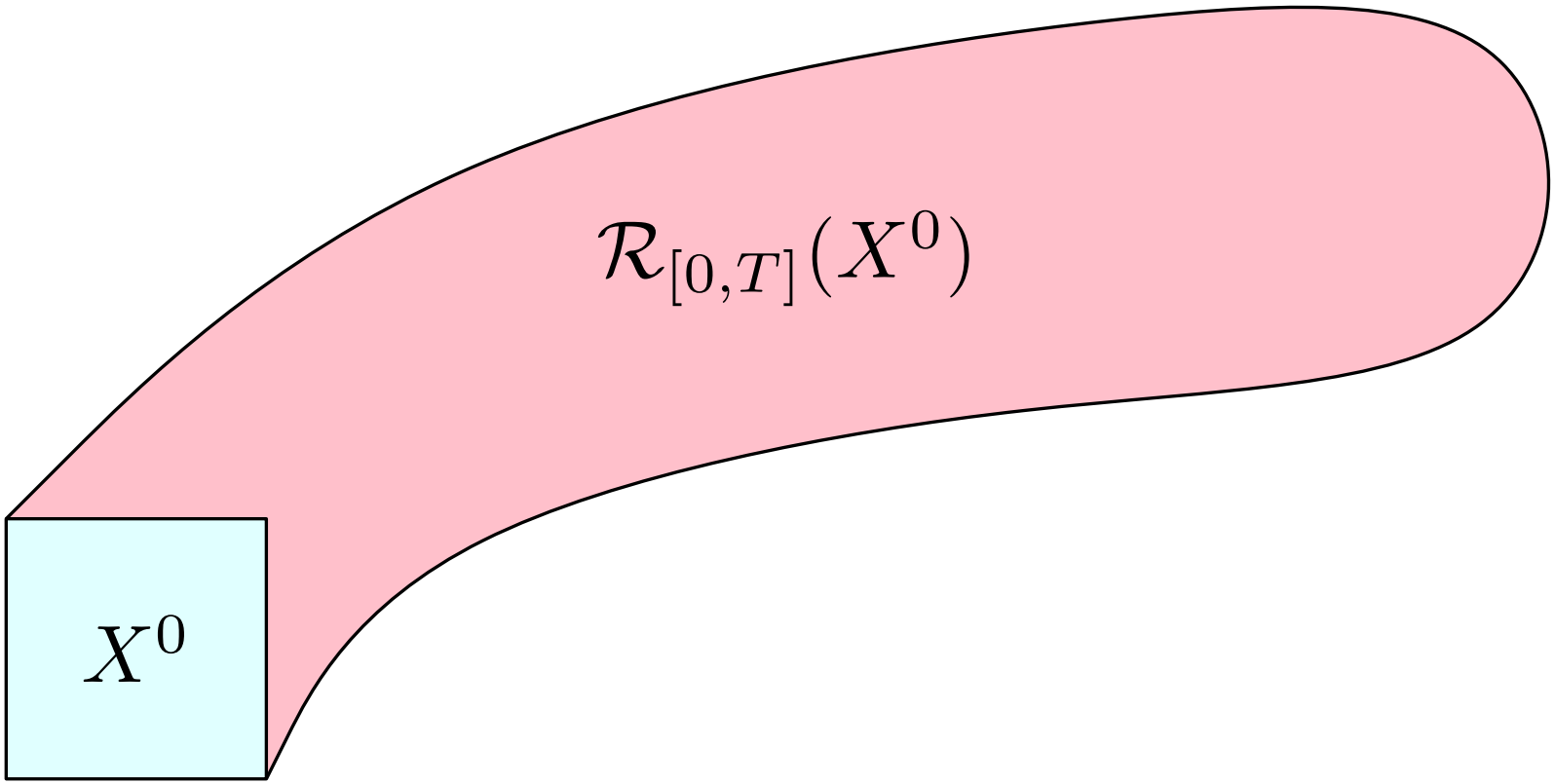
  where X^0 and V are compact convex subsets of $\mathbb{R}^n$.

- Over-approximation of the reachable set $\mathcal{R}_{[0,T]}(X^0)$:
  - Let $\tau = T/N$, we have

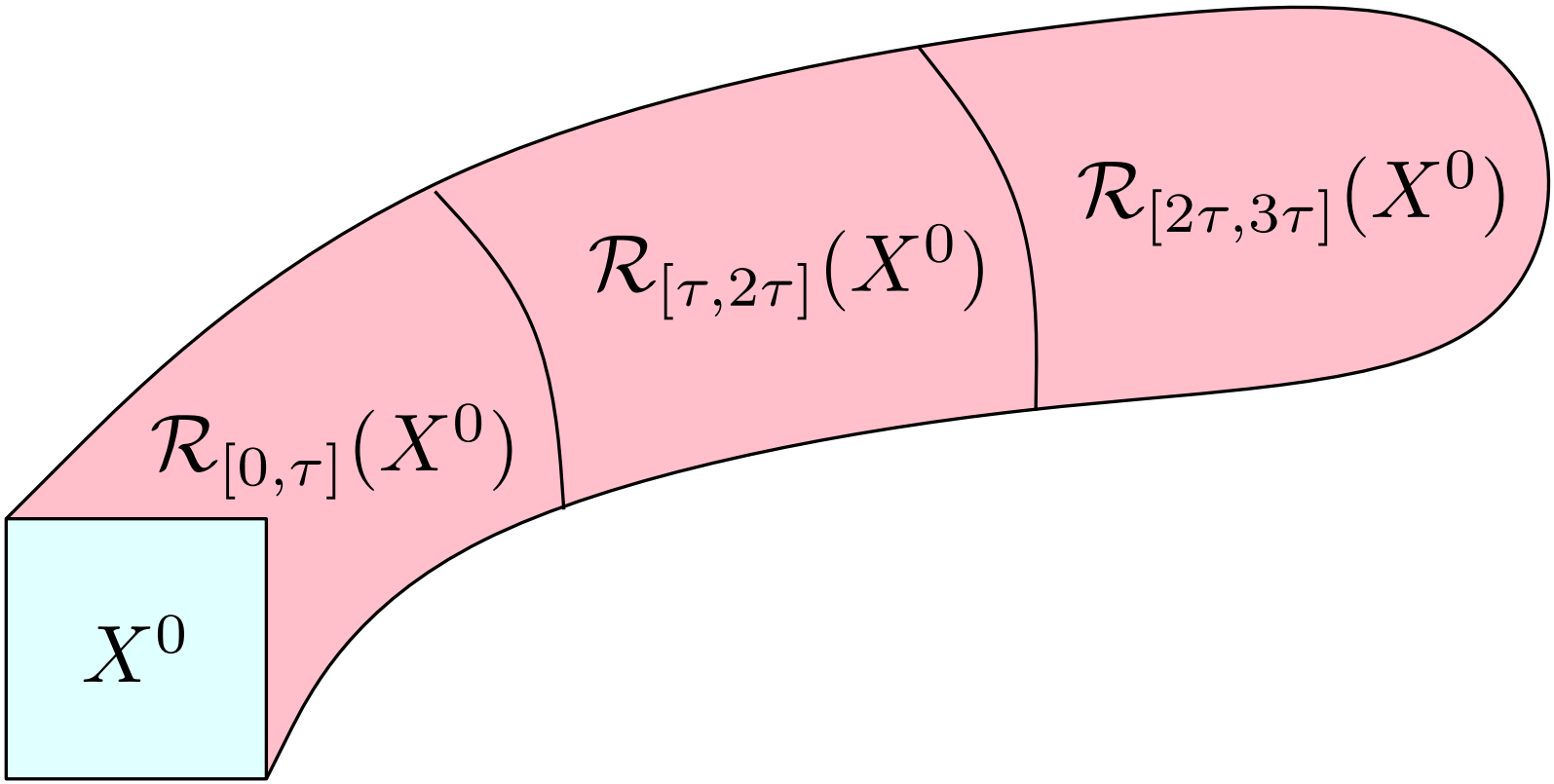
$$\mathcal{R}_{[0,T]}(X^0) = \bigcup_{i=0}^{N-1} \mathcal{R}_{[i\tau,(i+1)\tau]}(X^0).$$

  - Each $\mathcal{R}_{[i\tau,(i+1)\tau]}(X^0)$ over-approximated by a compact convex set Ω_i.

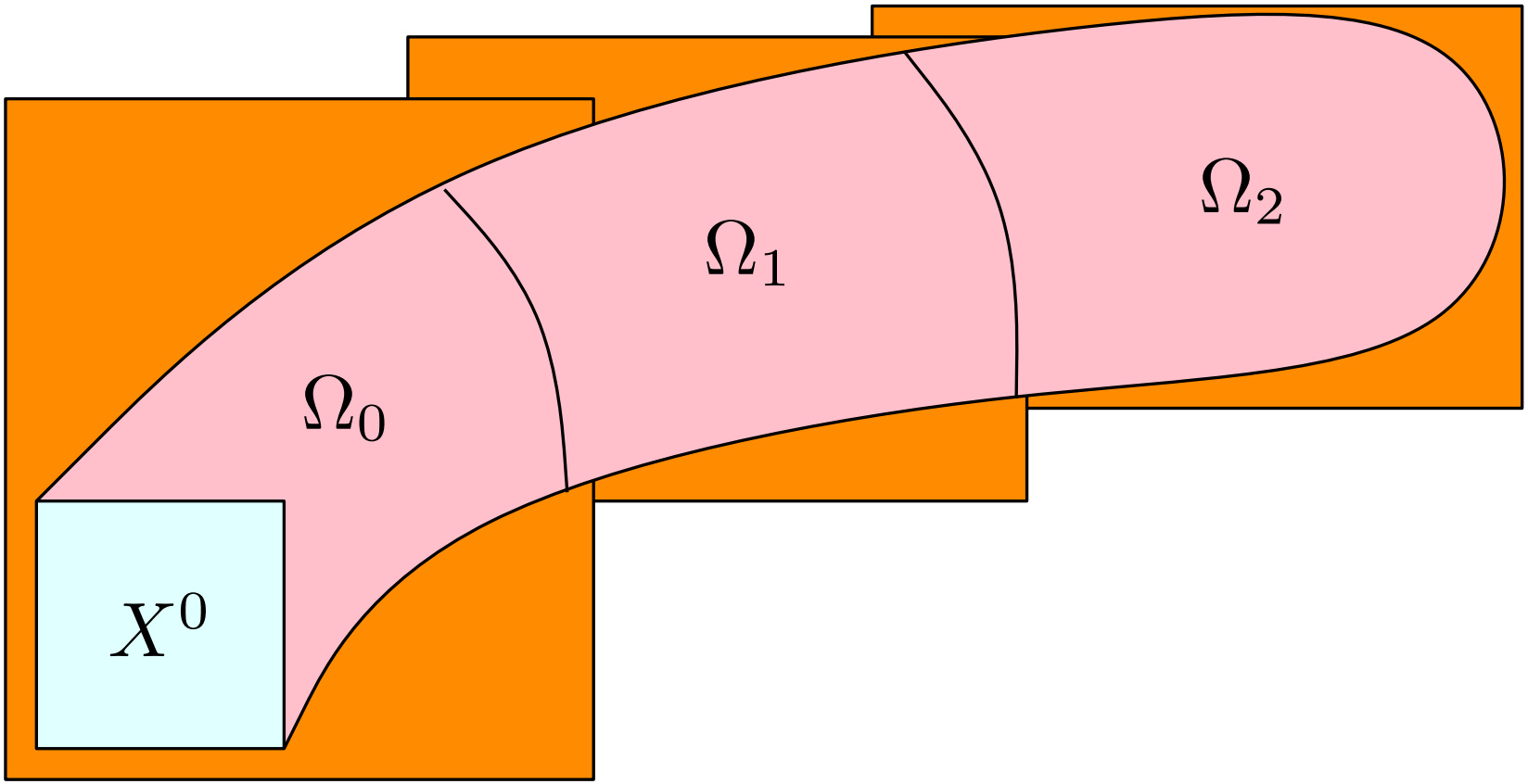
Reachability analysis of linear systems



Reachability analysis of linear systems



Reachability analysis of linear systems



Approximation scheme

- Initialization of the sequence :

$$\begin{aligned} \mathcal{R}_\tau(X^0) &\approx e^{\tau A}X^0 \oplus \tau V \\ \mathcal{R}_{[0,\tau]}(X^0) &\approx \text{Conv}(X^0, e^{\tau A}X^0 \oplus \tau V) \\ \mathcal{R}_{[0,\tau]}(X^0) &\subseteq \text{Conv}(X^0, e^{\tau A}X^0 \oplus \tau V \oplus \alpha_\tau \mathcal{B}) =: \Omega_0 \end{aligned}$$

  where $\alpha_\tau = O(\tau^2)$ depends on τ, A, X_0, V (explicit relation).

- Recurrence relation :

$$\begin{aligned} \mathcal{R}_{[(i+1)\tau,(i+2)\tau]}(X^0) &= \mathcal{R}_\tau(\mathcal{R}_{[i\tau,(i+1)\tau]}(X^0)) \\ &\approx e^{\tau A}\left(\mathcal{R}_{[i\tau,(i+1)\tau]}(X^0)\right) \oplus \tau V \\ &\subseteq e^{\tau A}\left(\mathcal{R}_{[i\tau,(i+1)\tau]}(X^0)\right) \oplus \tau V \oplus \beta_\tau \mathcal{B} \\ &\subseteq e^{\tau A}\Omega_i \oplus \tau V \oplus \beta_\tau \mathcal{B} =: \Omega_{i+1} \end{aligned}$$

  where $\beta_\tau = O(\tau^2)$ depends on τ, A, V (explicit relation).

Approximation scheme

Theorem

For all $i = 0, \ldots, N-1$, $\mathcal{R}_{[i\tau,(i+1)\tau]}(X^0) \subseteq \Omega_i$ *and*

$$d_H(\Omega_i, \mathcal{R}_{[i\tau,(i+1)\tau]}(X^0)) \leq \tau e^{T\|A\|} \left(\frac{\|A\|}{4} D_{X^0} + \tau \|A\|^2 R_{X0} + e^{\tau\|A\|} R_V \right)$$

where d_H *is the Hausdorff distance.*

In practice, for computing an over-approximation of the reachable set, we need to :

1. Choose a data structure to represent a class of compact convex sets ;
2. Compute (efficiently) for this class of compact convex sets, linear transformations, Minkowski sum and convex hull.

Set representation : polytopes

- Polytopes form a fairly large (dense) class of compact convex sets.
- Canonical representations :
  - $\mathcal{H}$-polytope :

$$P = \{x \in \mathbb{R}^n | \ c_k \cdot x \leq d_k, \ k = 1, \ldots, m\}.$$

  - $\mathcal{V}$-polytope :

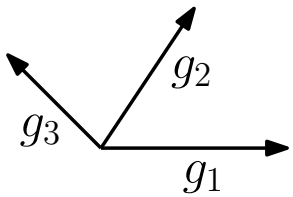
$$P = \text{Conv}(x_1, \ldots, x_p).$$

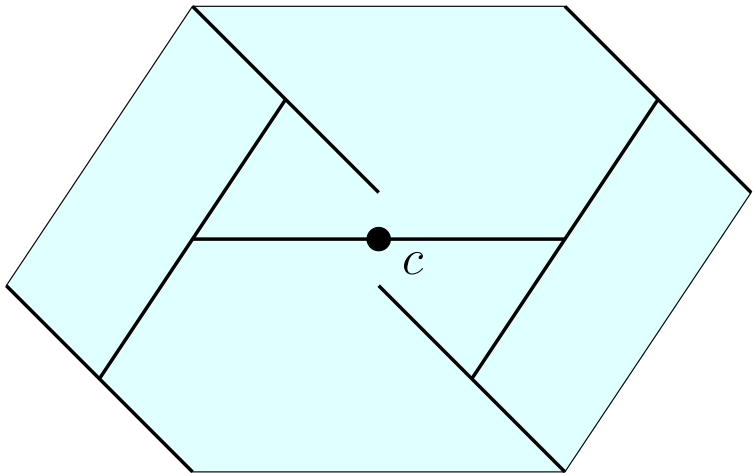
- Polytopes are closed under linear transformations, Minkowski sum and convex hull.
- In high dimension, lack of efficient algorithms to compute Minkowski sum and combinatorial increase of the size of representations.

Set representation : zonotopes

- Smallest class of polytopes containing intervals and closed under linear transformations and Minkowski sum.
- Canonical representation :

$$\begin{aligned} Z &= \left\{ x \in \mathbb{R}^n \middle| \; x = c + \sum_{i=1}^{i=p} x_i g_i, \; -1 \leq x_i \leq 1 \right\} \\ &= (c, \langle g_1, \ldots, g_p \rangle). \end{aligned}$$





Reachability analysis using zonotopes

- Efficient computation of linear transformations and Minkowski sum :

$$\begin{aligned} AZ &= (Ac, \langle Ag_1, \ldots, Ag_p \rangle) \\ Z \oplus Z' &= (c + c', \langle g_1, \ldots, g_p, g'_1, \ldots, g'_{p'} \rangle). \end{aligned}$$

- Easy implementation of

$$\Omega_{i+1} := e^{\tau A} \Omega_i \oplus \tau V \oplus \beta_\tau \mathcal{B}.$$

- Zonotopes not closed under convex hull : compute a zonotope Ω_0 such that

$$\mathrm{Conv}(X^0, e^{\tau A} X^0 \oplus \tau V) \oplus \alpha_\tau \mathcal{B} \subseteq \Omega_0.$$

- Efficient implementation of reachability analysis with time/space complexity in $O(N)$.

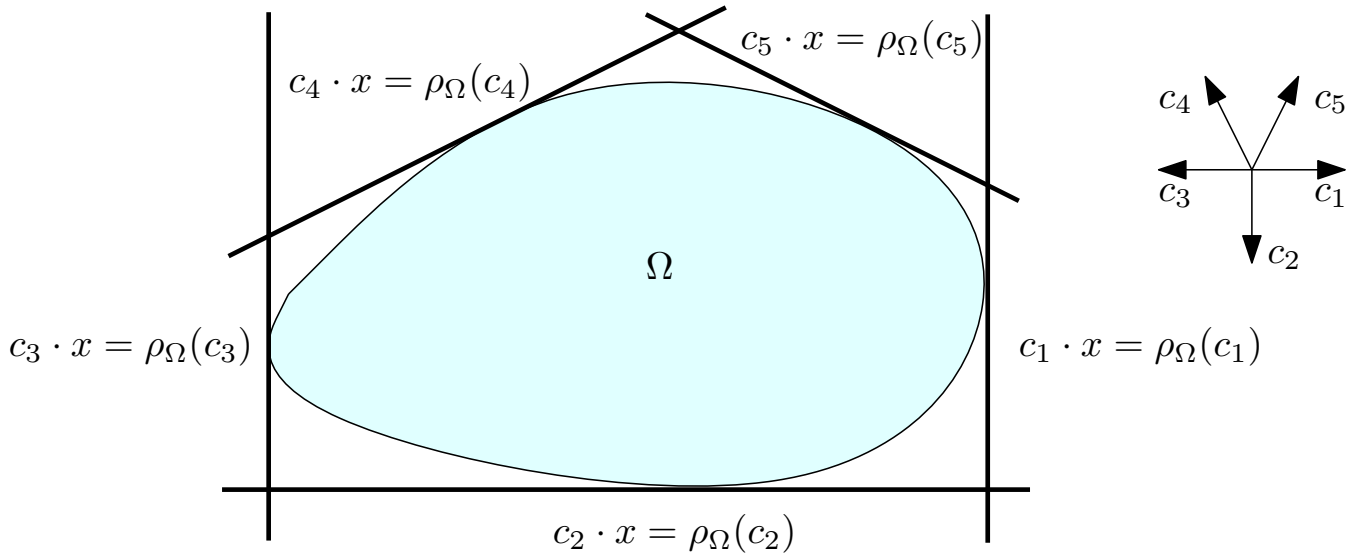
Set representation : support functions

- Functional representation of a compact convex set $\Omega \subseteq \mathbb{R}^n$:

$$\rho_\Omega(c) = \max_{x \in \Omega} c \cdot x.$$

- Polytopic over-approximation of Ω :

$$\Omega \subseteq \bigcap_{i=1}^{r} \{x \in \mathbb{R}^n | \; c_i \cdot x \leq \rho_\Omega(c_i)\}.$$



Reachability analysis using support functions

- Efficient computation of linear transformations, Minkowski sum and convex hull :

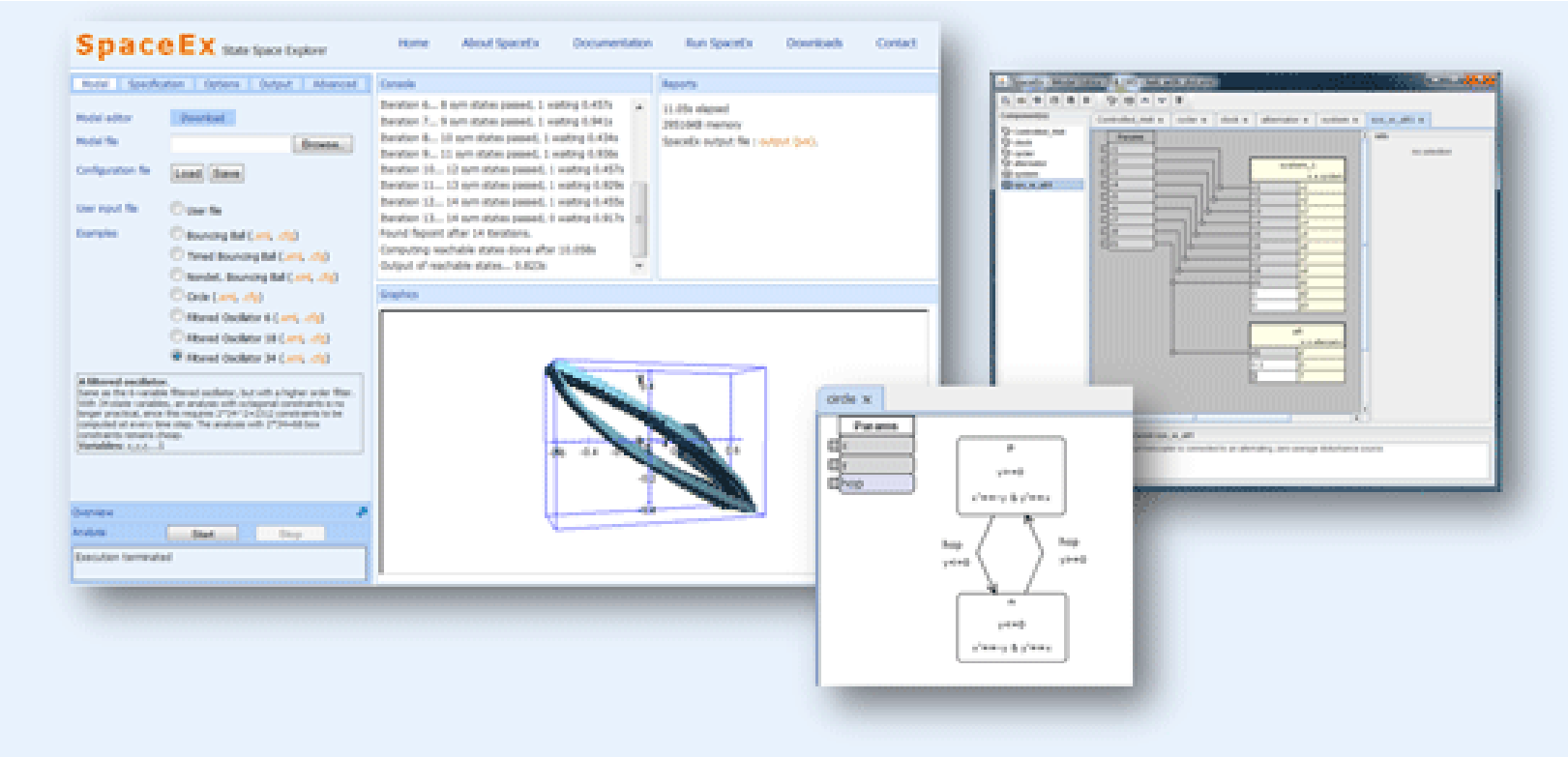
$$\begin{aligned}
\rho_{\lambda\Omega}(c) &= \lambda\rho_{\Omega}(c) \\
\rho_{A\Omega}(c) &= \rho_{\Omega}(A^T c) \\
\rho_{\Omega_1\oplus\Omega_2}(c) &= \rho_{\Omega_1}(c) + \rho_{\Omega_2}(c) \\
\rho_{\mathrm{Conv}(\Omega_1,\Omega_2)}(c) &= \max(\rho_{\Omega_1}(c), \rho_{\Omega_2}(c)).
\end{aligned}$$

- Efficient computation of support functions for :
  - Ellipsoids (explicit formula).
  - Zonotopes (explicit formula).
  - Polytopes (solution of a linear program).
  - Convex sets (solution of a convex optimization problem).
- Efficient implementation of reachability analysis with time/space complexity in $O(N)$.

Applications

Verification platform SpaceEx :

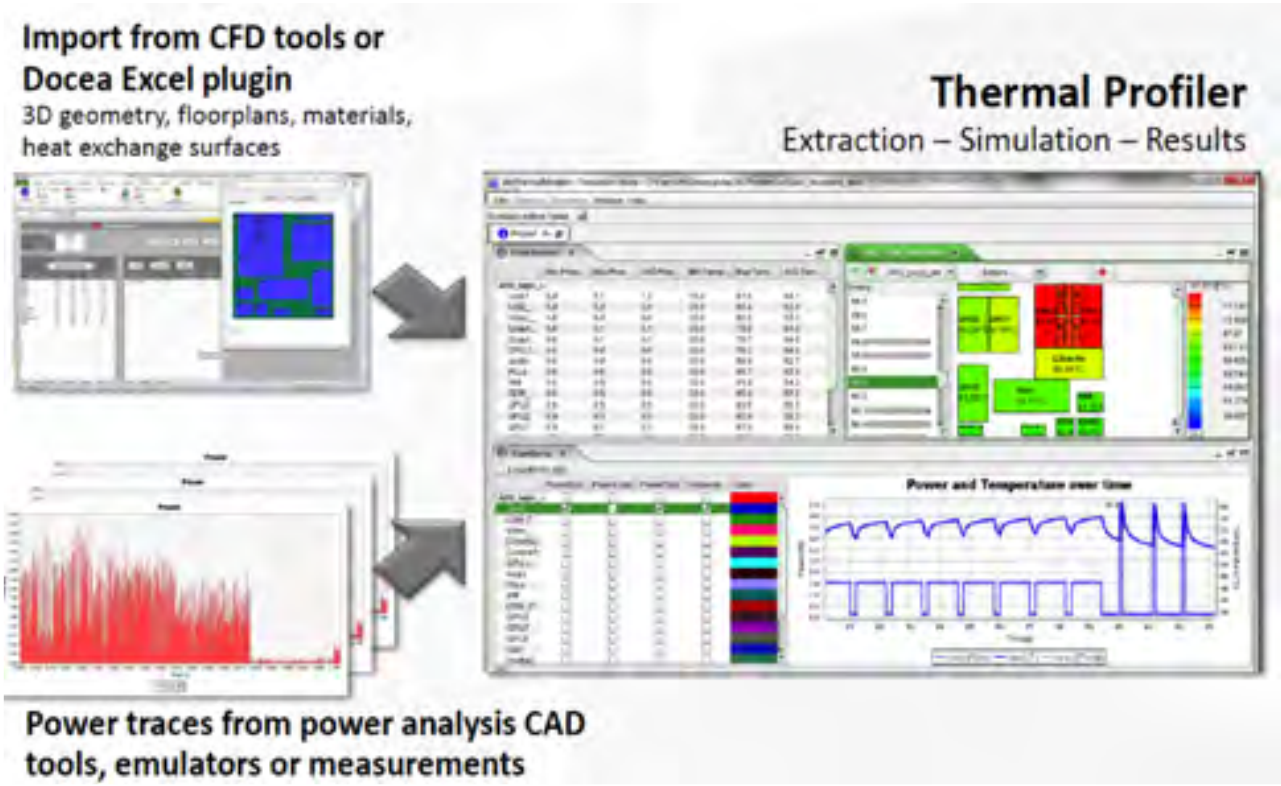
- Reachability analysis of hybrid systems using support functions.
- Developped at Verimag (PI : Goran Frehse).



Applications

Thermal Profiler (DOCEA Power) :

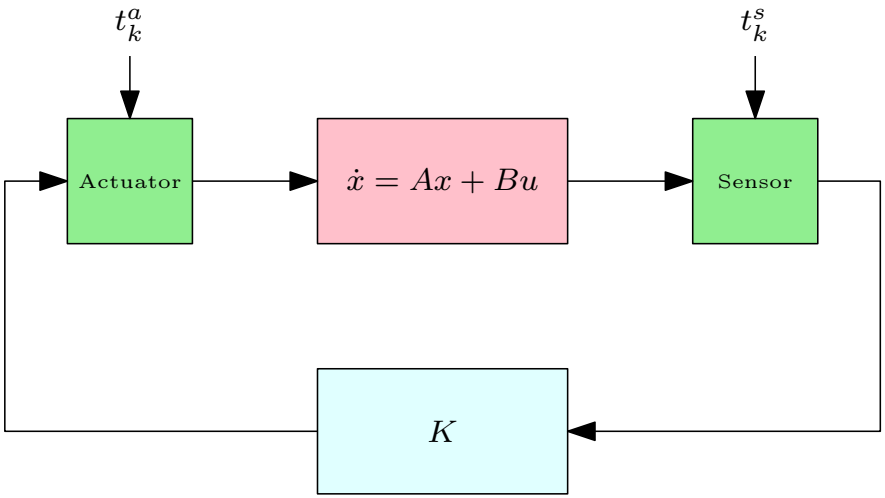
- Verification of qualitative and quantitative properties of reduced-order thermal models using reachability analysis.



Applications

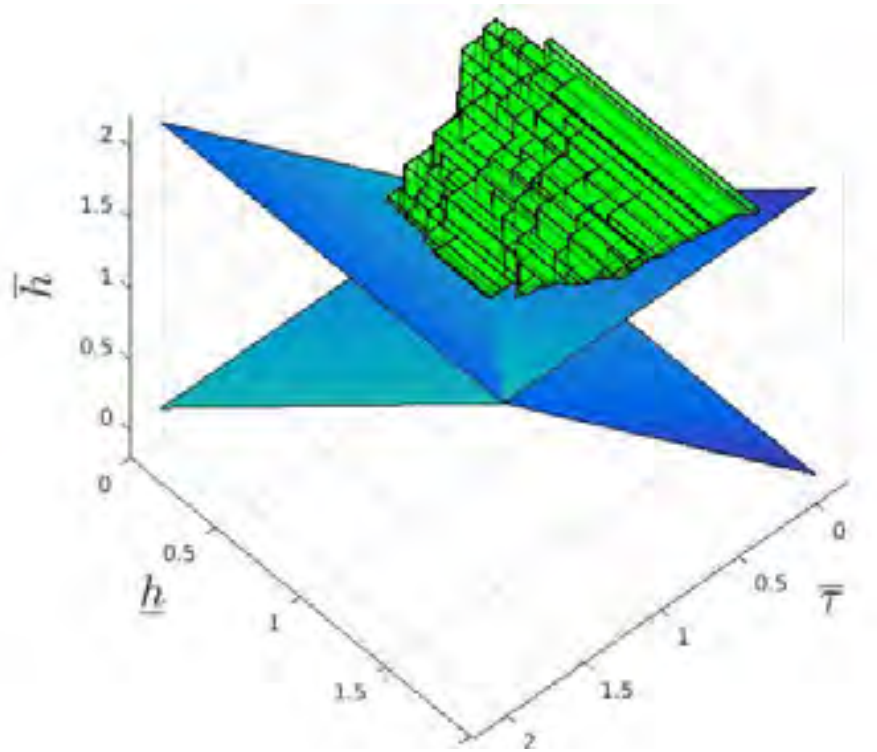
Contract-based design of embedded control systems :

- Stability verification and timing contract synthesis using reachability analysis.



Timing contract:

$$\begin{cases} t_k^a - t_k^s \in [\underline{\tau}, \overline{\tau}] \\ t_{k+1}^s \geq t_k^a \\ t_{k+1}^s - t_k^s \in [\underline{h}, \overline{h}] \end{cases}$$



Main references

- A. Girard, **Reachability of uncertain linear systems using zonotopes**. *Hybrid Systems : Computation and Control*, 2005.
- A. Girard, C. Le Guernic and O. Maler, **Efficient computation of reachable sets of linear time-invariant systems with inputs**. *Hybrid Systems : Computation and Control*, 2006.
- C. Le Guernic and A. Girard, **Reachability analysis of linear systems using support functions**. *Nonlinear Analysis : Hybrid Systems*, 2010.
- G. Frehse et al., **SpaceEx : scalable verification of hybrid systems**. *Computer Aided Verification*, 2011.
- A. Girard et al., **Assessing the quality of reduced order models of heat transfer in electronic devices**. *European Conference on Mathematics for Industry*, 2014.
- M. Al Khatib, A. Girard and T. Dang, **Verification and synthesis of timing contracts for embedded controllers**. *Submitted*, 2015.

Conclusion

- Reachability analysis of hybrid systems :
  - Twenty years of research :
    R. Alur et al., **The algorithmic analysis of hybrid systems**. *Theoretical computer science*, 1995.
  - Quite mature for linear hybrid systems, nonlinear hybrid systems remain a challenge.
  - Current efforts to transition from theory to practice :
    Workshop on Applied Verification for Continuous and Hybrid Systems (`http://cps-vo.org/group/ARCH`)
  - Dedicated algorithms for specific classes of systems.