ARIADNE: dominance checking of nonlinear hybrid automata using reachability analysis

Luca Benvenuti[1] Davide Bresolin[2] Pieter Collins[3]
Alberto Ferrari[4] Luca Geretti[2] Tiziano Villa[2]

[1] Università di Roma "La Sapienza", Roma, Italy

[2] Università di Verona, Verona, Italy

[3] Maastricht University, Maastricht, The Netherlands

[4] ALES S.r.l., Roma, Italy

RP'12
17-19 September 2012
Bordeaux, France

Hybrid system model

- A set of discrete locations;
- A continuous $\mathbb{R}^n$ space for each location;
- First-order differential system of nonlinear equations for each location;
- Transitions between locations according to nonlinear guards and reset functions.

Enclosures

In general we can't represent a set $S \subset \mathbb{R}^n$ exactly, or doing so requires a lot of accuracy.

$\rightarrow$ We use an overapproximating *enclosure* represented by a polynomial $f : [-1, 1]^m \mapsto \mathbb{R}^n$.

Evolution steps

- Continuous: integration of dynamics from an *initial* set, to obtain a *final* set and a *reached* set;
- Discrete: if the set satisfies a guard, the corresponding reset function is applied to the set.

Fundamentals

Enclosures and evolution in ARIADNE

Enclosures

In general we can't represent a set $S \subset \mathbb{R}^n$ exactly, or doing so requires a lot of accuracy.
$\rightarrow$ We use an overapproximating *enclosure* represented by a polynomial $f : [-1, 1]^m \mapsto \mathbb{R}^n$.

Evolution steps

- Continuous: integration of dynamics from an *initial* set, to obtain a *final* set and a *reached* set;
- Discrete: if the set satisfies a guard, the corresponding reset function is applied to the set.

Reachability sets

Outer and ε-lower reachability sets

We are able to compute two kinds of approximations of Re:

- Outer reachability set O: an uncontrolled over-approximation of Re, such that $Re \subset O$;
- ε-lower reachability set L_ε: a controlled over-approximation of a subset of Re, such that $\forall x \in L_\varepsilon,\ \exists x' \in Re \ \ s.t.\ ||x - x'|| \leq \varepsilon$,

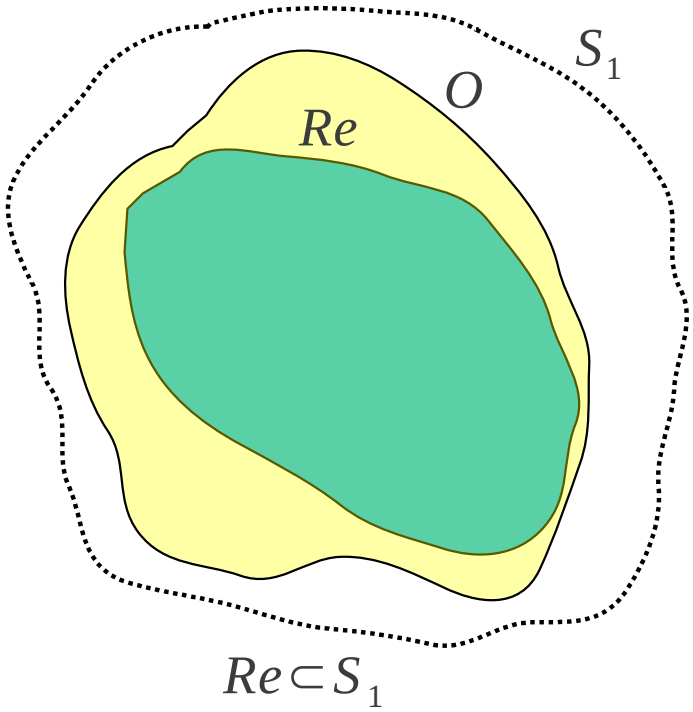
where both depend on some accuracy settings.
Computationally, a reachability set is the union of (overlapping) sets obtained from the evolution of the system.

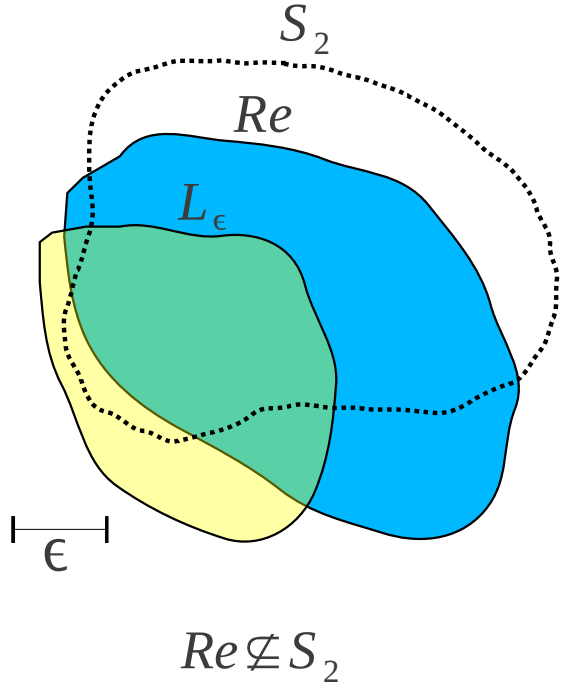
Reachability sets

The purpose of analysing such sets

Given a generic set S,

- O can be analysed to verify whether $Re \subset S$ is true;
- L_ε can be analysed to verify whether $Re \not\subseteq S$ is true.





Computation of O and L_ε

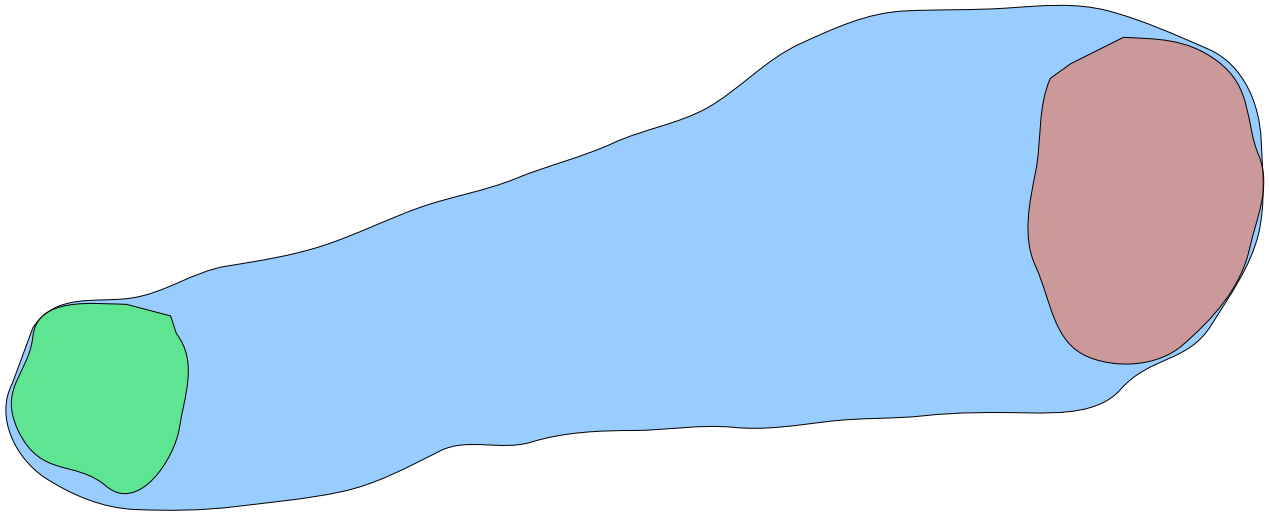
Basic definitions

The reachability calculation is iterative, with step $k \geq 0$.

- $\tilde{F}_k$: final set of enclosures from an initial set $\tilde{I}_k$;
- $\tilde{Re}_k$: reached set of enclosures from I_k, with $\tilde{F}_k \subseteq \tilde{Re}_k$;

Given a set Q, we can obtain a *discretised* set $\overline{Q}$ in respect to a grid, whose granularity depends on the accuracy.

- $\overline{F}_k$, $\overline{Re}_k$: discretisations of $\tilde{F}_k$, $\tilde{Re}_k$;



Computation of O and L_ε

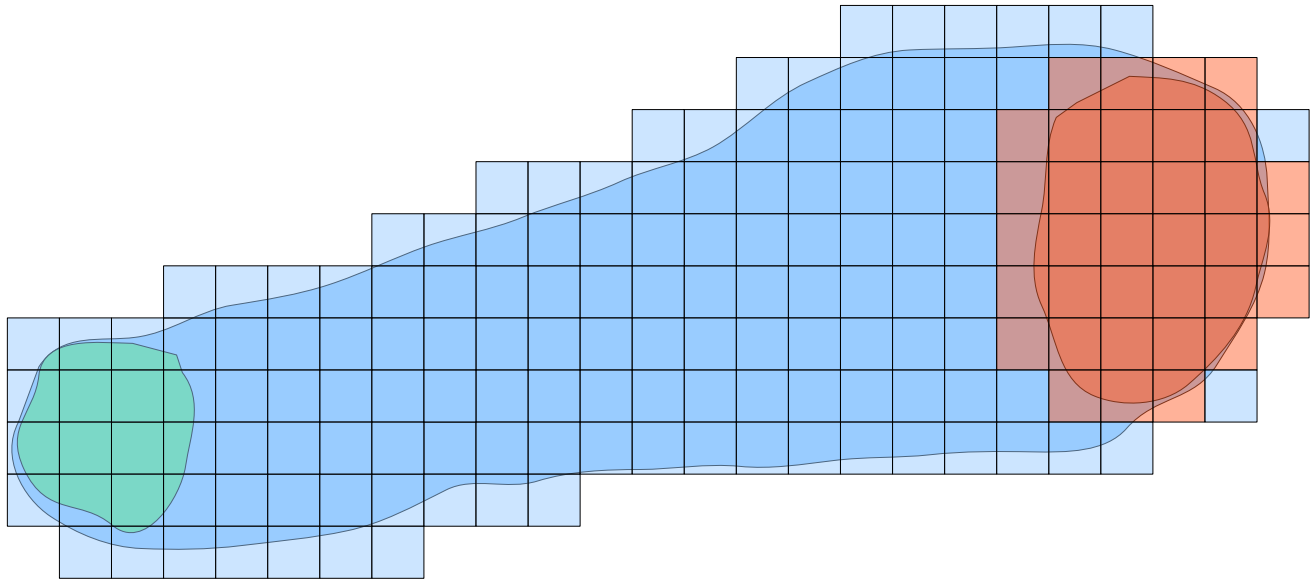
Basic definitions

The reachability calculation is iterative, with step $k \geq 0$.

- $\tilde{F}_k$: final set of enclosures from an initial set $\tilde{I}_k$;
- $\tilde{Re}_k$: reached set of enclosures from I_k, with $\tilde{F}_k \subseteq \tilde{Re}_k$;

Given a set Q, we can obtain a *discretised* set $\overline{Q}$ in respect to a grid, whose granularity depends on the accuracy.

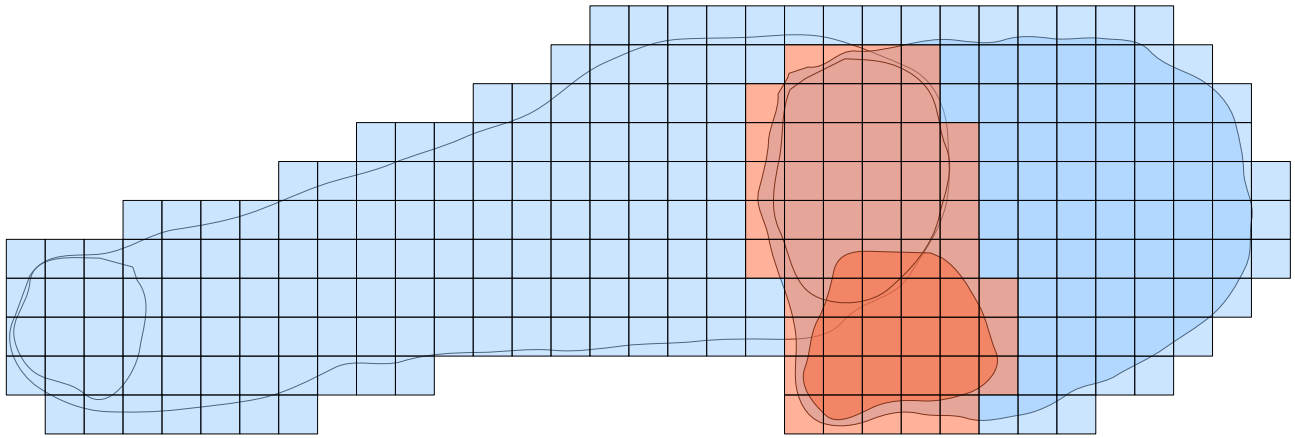
- $\overline{F}_k$, $\overline{Re}_k$: discretisations of $\tilde{F}_k$, $\tilde{Re}_k$;



Computation of O and L_ε

Supporting definitions

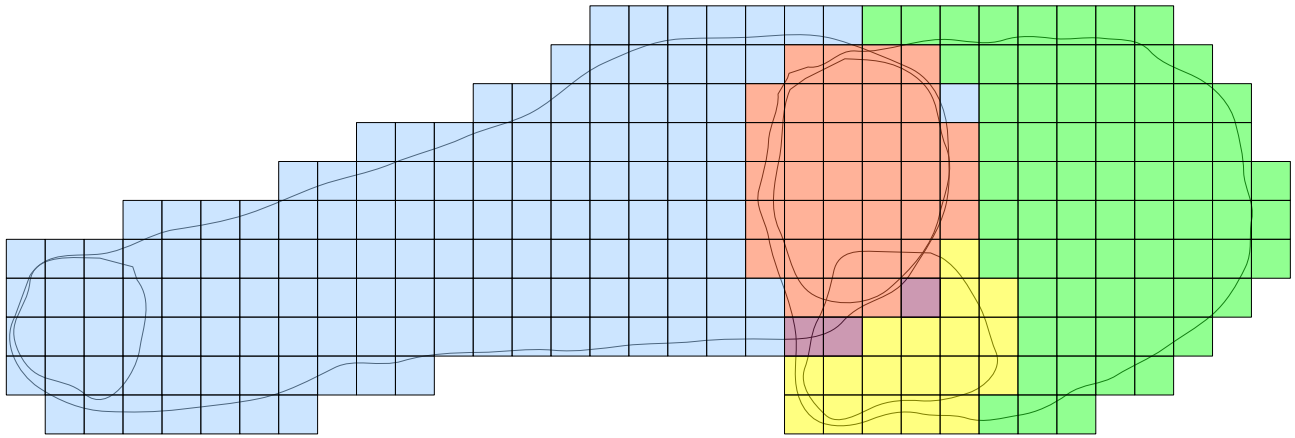
- $\overline{F}^a_k$: accumulated discretised final set, up to step k;
- $\overline{Re}^a_k$: accumulated discretised reached set, up to k;
- $\overline{F}^r_k$: residual discretised final set, i.e. $\overline{F}_k \setminus \overline{F}^a_{k-1}$;
- $\overline{Re}^r_k$: residual discretised reached set, i.e. $\overline{Re}_k \setminus \overline{Re}^a_{k-1}$;
- $\tilde{J}_k$: jump set, obtained by applying transitions to $\overline{Re}^r_k$;



Computation of O and L_ε

Supporting definitions

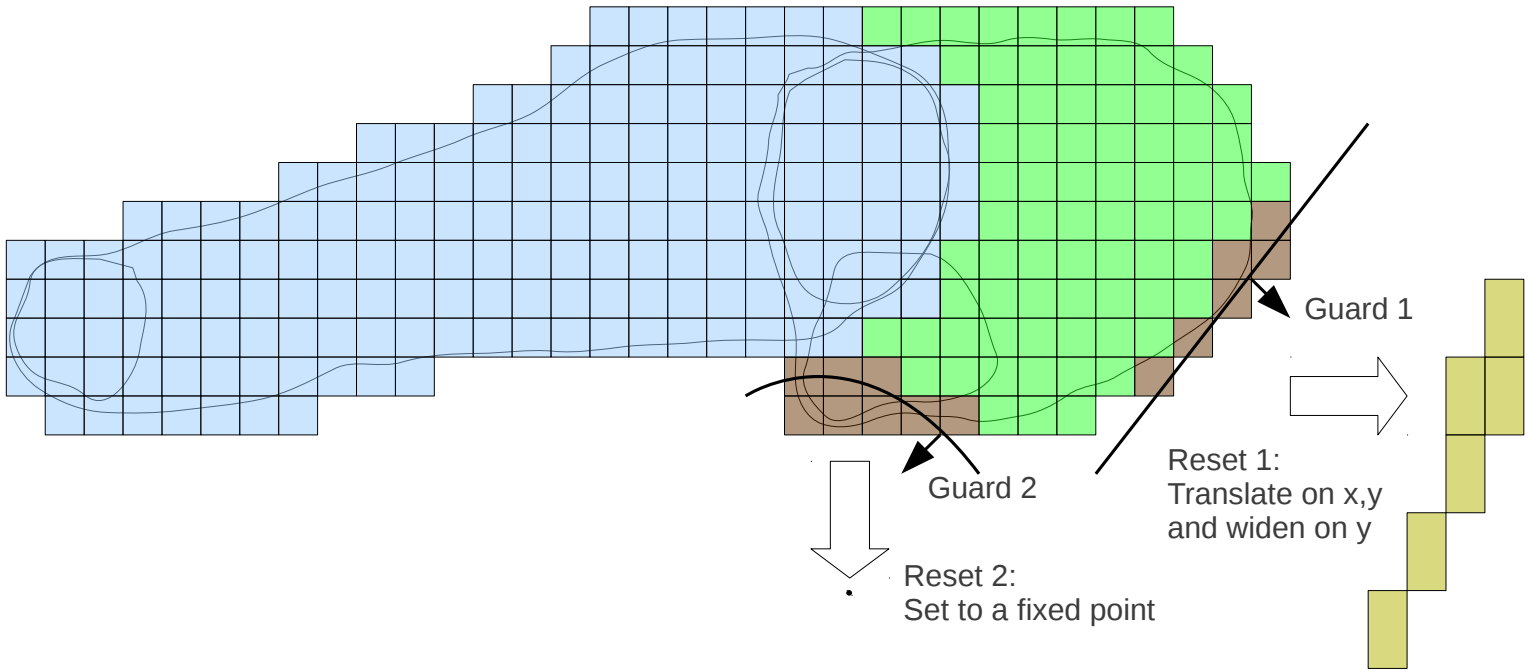
- $\overline{F}^a_k$: accumulated discretised final set, up to step k;
- $\overline{Re}^a_k$: accumulated discretised reached set, up to k;
- $\overline{F}^r_k$: residual discretised final set, i.e. $\overline{F}_k \setminus \overline{F}^a_{k-1}$;
- $\overline{Re}^r_k$: residual discretised reached set, i.e. $\overline{Re}_k \setminus \overline{Re}^a_{k-1}$;
- $\tilde{J}_k$: jump set, obtained by applying transitions to $\overline{Re}^r_k$;



Computation of O and L_ε

Supporting definitions

- $\overline{F}^a_k$: accumulated discretised final set, up to step k;
- $\overline{Re}^a_k$: accumulated discretised reached set, up to k;
- $\overline{F}^r_k$: residual discretised final set, i.e. $\overline{F}_k \setminus \overline{F}^a_{k-1}$;
- $\overline{Re}^r_k$: residual discretised reached set, i.e. $\overline{Re}_k \setminus \overline{Re}^a_{k-1}$;
- $\tilde{J}_k$: jump set, obtained by applying transitions to $\overline{Re}^r_k$;



Computation of O and L_ε

Accuracy settings

User settings

- B: bounding domain for the continuous variables on each location

Automated settings

- Depth: how many times the domain must be split along each continuous variable;

Dependent settings

- $\vec{\gamma}$: grid lengths;
- $t^e_{\max}$: maximum evolution time for an iteration;
- $d_{\max}$: maximum radius of an enclosure.

Computation of O and L_ε

Accuracy settings

User settings

- B: bounding domain for the continuous variables on each location

Automated settings

- Depth: how many times the domain must be split along each continuous variable;

Dependent settings

- $\vec{\gamma}$: grid lengths;
- $t^e_{\max}$: maximum evolution time for an iteration;
- $d_{\max}$: maximum radius of an enclosure.

Computation of O and L_ε

Accuracy settings

User settings

- B: bounding domain for the continuous variables on each location

Automated settings

- Depth: how many times the domain must be split along each continuous variable;

Dependent settings

- $\vec{\gamma}$: grid lengths;
- $t^e_{\max}$: maximum evolution time for an iteration;
- $d_{\max}$: maximum radius of an enclosure.

Computation of O and L_ε

Outer reachability flow

Starting from the initial set $I_0 = I$, for the k-th iteration,

1. Get $\tilde{Re}_k$ and $\tilde{F}_k$ under continuous evolution only, stopping if $t^e_{\max}$ or $d_{\max}$ are hit;
2. Set $I_{k+1} = \overline{F}^r_k \cup \tilde{J}_k$;
3. If $\overline{Re}^r_k \not\subseteq B$, terminate with failure;
4. If $I_{k+1} = \emptyset$, terminate with success, yielding $O = \overline{Re}^a_k$.

Comments

- Failure means that we cannot guarantee an over-approximation of Re for the chosen accuracy settings.

Computation of O and L_ε

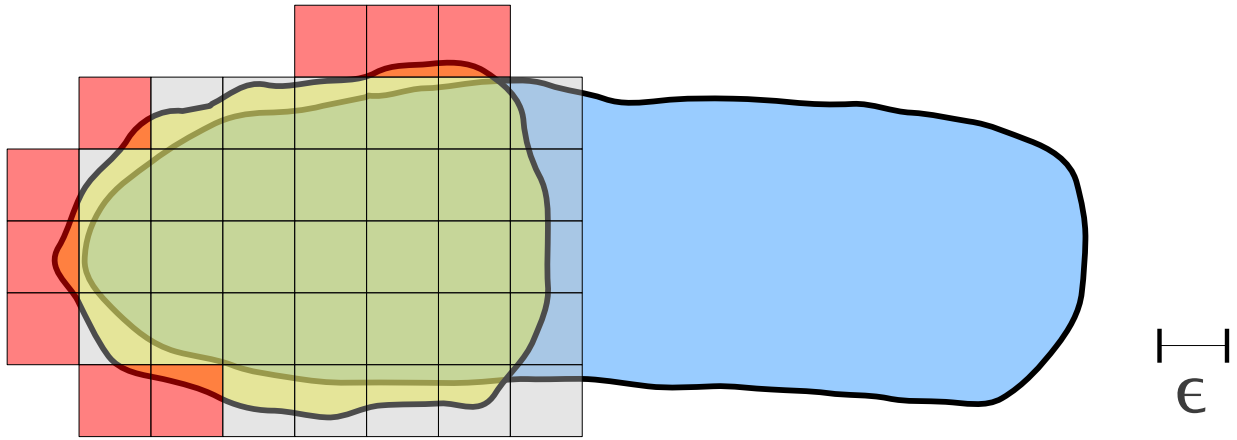
ε-lower reachability in general

Any evolution set must contain at least one point of Re

Given $\tilde{Re}_k$, we can then check $||\tilde{Re}_k - Re|| < \varepsilon$ by checking the diameter of $\tilde{Re}_k$, with no actual knowledge of Re.

We can't use discretised sets for evolution

Since discretisation does not guarantee the condition above.



Computation of O and L_ε

ε-lower reachability flow

Starting from the initial set $I_0 = I$, for the k-th iteration,

1. Get $\tilde{Re}_k$ and $\tilde{F}_k$ until a transition is performed, stopping if $t^e_{\max}$ or $d_{\max}$ are hit;
2. Set $I_{k+1} = \tilde{F}_k$;
3. If $\tilde{Re}_k \cap B = \emptyset$, terminate with failure;
4. If $||\tilde{Re}_k - Re|| \geq \varepsilon$, terminate with success, yielding $L_\varepsilon = \overline{Re}^a_{k-1}$;
5. If $\overline{Re}^r_k = \emptyset$, terminate with success, yielding $L_\varepsilon = \overline{Re}^a_k$;

Comments

- Failure means that the domain is ill-chosen;
- The conditions in 4 and 5 do not allow to obtain an infinite-time reachability.

Dominance checking

What does that mean?

- Given two automata $\mathcal{H}_1$ and $\mathcal{H}_2$, identify a common "assumptions" space G (i.e., initial conditions, parameters, etc.) and a common "guarantees" space V (i.e., a subset of the reachable space);
- Check whether for weaker assumptions on $\mathcal{H}_2$, stronger promises for $\mathcal{H}_2$ are obtained in respect to $\mathcal{H}_1$.

In practice?

Choose $I_{\mathcal{H}_2}|_G \supseteq I_{\mathcal{H}_1}|_G$ and check whether $Re_{\mathcal{H}_2}|_V \subset Re_{\mathcal{H}_1}|_V$.

Dominance checking

What does that mean?

- Given two automata $\mathcal{H}_1$ and $\mathcal{H}_2$, identify a common "assumptions" space G (i.e., initial conditions, parameters, etc.) and a common "guarantees" space V (i.e., a subset of the reachable space);
- Check whether for weaker assumptions on $\mathcal{H}_2$, stronger promises for $\mathcal{H}_2$ are obtained in respect to $\mathcal{H}_1$.

In practice?

Choose $I_{\mathcal{H}_2}|_G \supseteq I_{\mathcal{H}_1}|_G$ and check whether $Re_{\mathcal{H}_2}|_V \subset Re_{\mathcal{H}_1}|_V$.

The dominance checking flow

Iteratively with progressively higher accuracy (i.e., depth):

1. Compute an outer-approximation O_2 of $Re_{\mathcal{H}_2}$;
2. Compute an ε-lower approximation $L_{\varepsilon,1}$ of $Re_{\mathcal{H}_1}$;
3. If $O_2|_V \subset \varepsilon\text{-}int(L_{\varepsilon,1})|_V$, where $\varepsilon\text{-}int(L_{\varepsilon,1})$ is obtained by removing a border of size ε from $int(L_{\varepsilon,1})$, then $\mathcal{H}_2$ dominates $\mathcal{H}_1$. Exit with **true**;
4. Compute an outer-approximation O_1 of $Re_{\mathcal{H}_1}$;
5. Compute an ε-lower approximation $L_{\varepsilon,2}$ of $Re_{\mathcal{H}_2}$;
6. If $\varepsilon\text{-}int(L_{\varepsilon,2})|_V \not\subseteq O_1|_V$, where $\varepsilon\text{-}int(L_{\varepsilon,2})$ is obtained by removing a border of size ε from $int(L_{\varepsilon,2})$, then $\mathcal{H}_2$ does not dominate $\mathcal{H}_1$. Exit with **false**;
7. Otherwise, increase the depth and restart from 1.

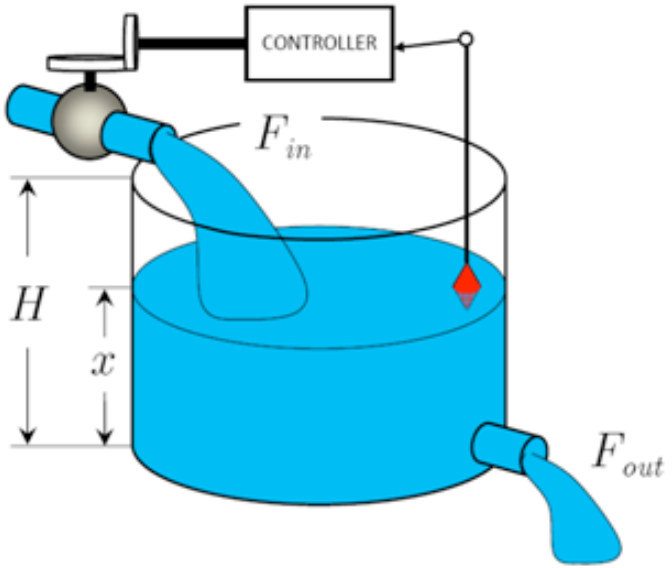
If a user-defined time budget is hit, exit with **indeterminate**.

The systems to compare

Two water-tank systems

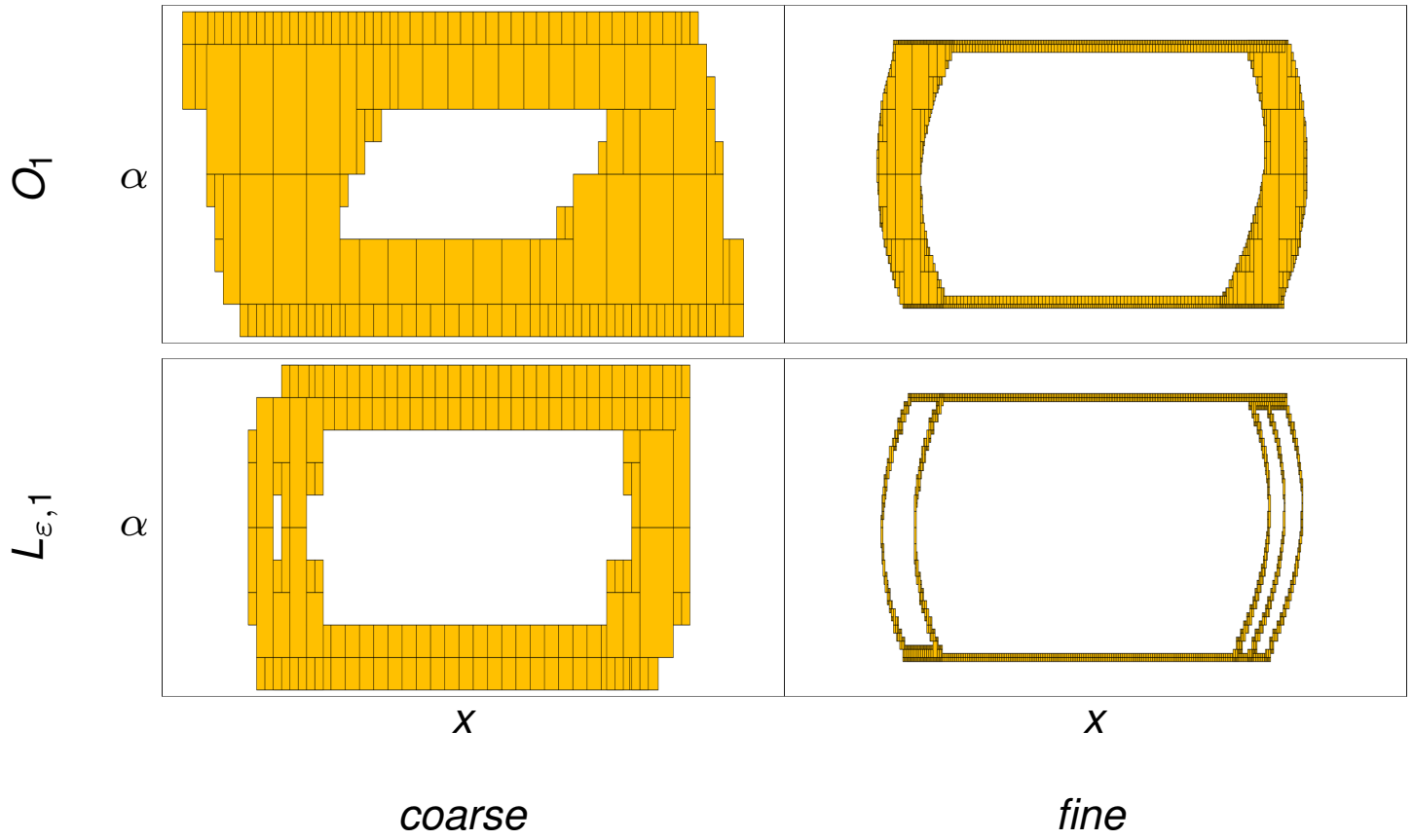
- $\mathcal{H}_1$ uses a hysteretic controller;
- $\mathcal{H}_2$ uses a proportional controller.

Output variables: valve aperture α and water level x.



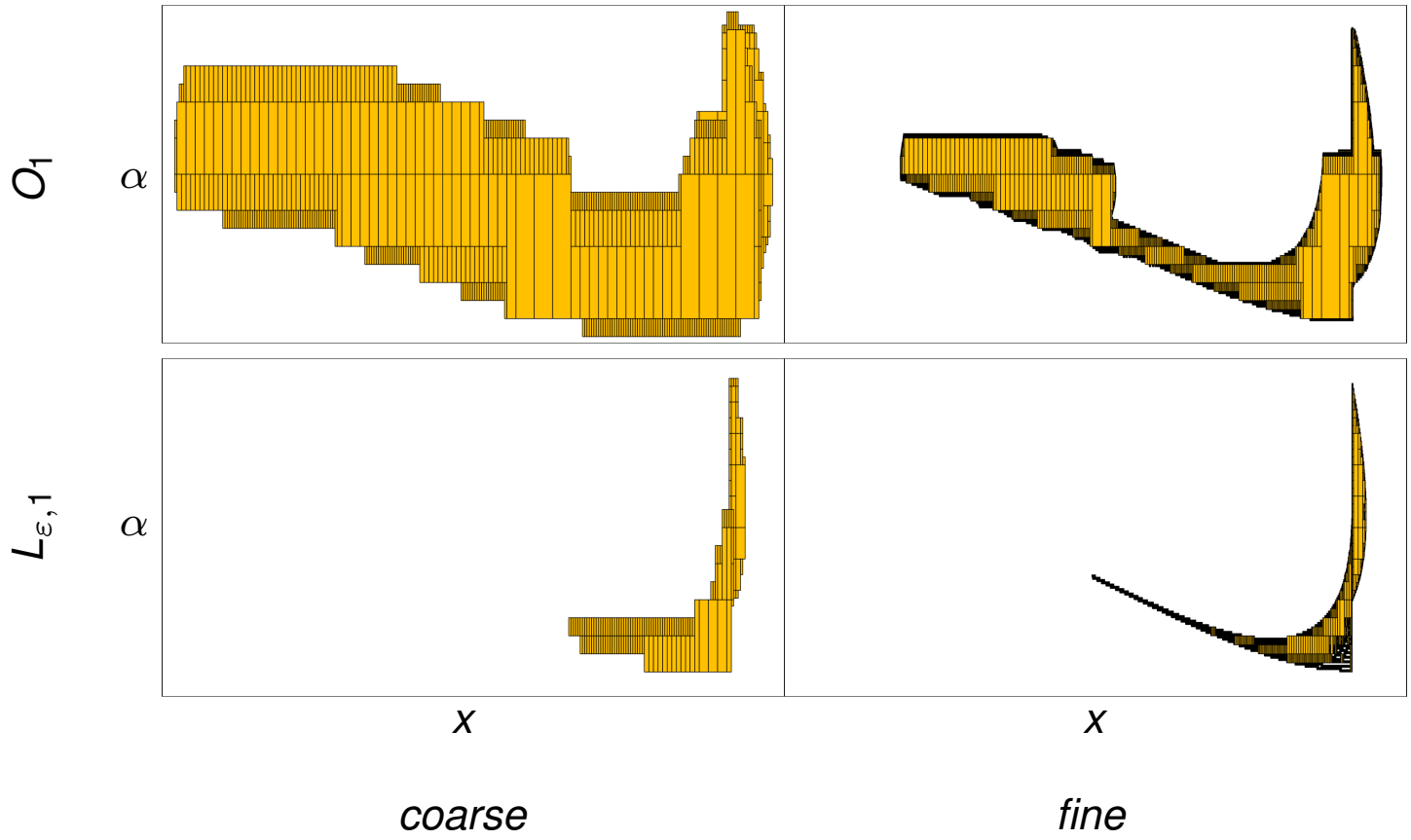
Reachability results

Hysteretic controller



Reachability results

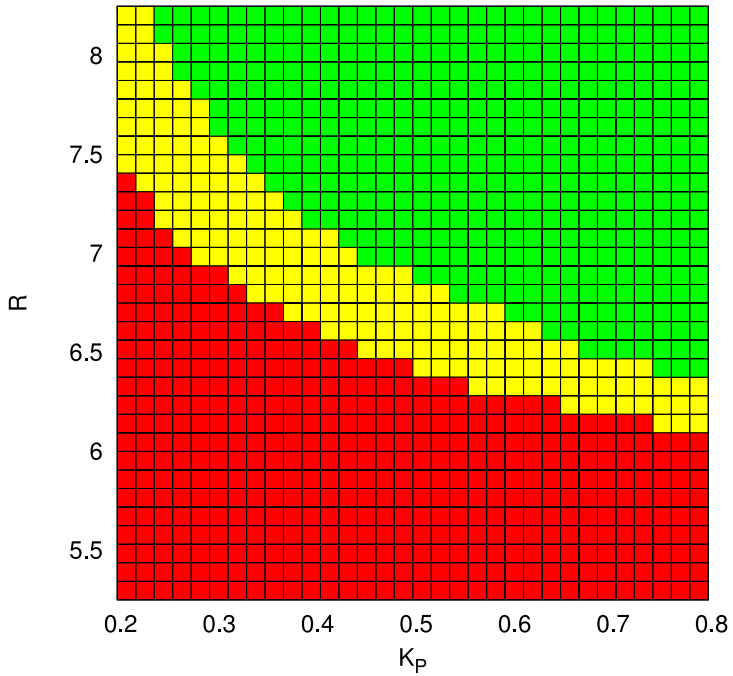
Proportional controller



Dominance results

Obtained for different values of two parameters: the gain K_P and the reference height R of the proportional controller.

- Green: proportional dominates hysteretic for all points;
- Red: proportional does not dominate hysteretic in at least one point;
- Yellow: insufficient accuracy to obtain a result.



Conclusions

Advantages of ARIADNE

- Designed for nonlinear hybrid systems analysis;
- ε-lower approximations allow to look for counterexamples;
- Complex verification strategies can be adopted.

Future work

- Move from the "grid" representation to a more efficient and scalable solution;
- Implement differential inclusions (currently able to model constant behavior within an interval);
- Implement backward reachability (already available for O, very tricky for L_ε).

Conclusions

Advantages of ARIADNE

- Designed for nonlinear hybrid systems analysis;
- ε-lower approximations allow to look for counterexamples;
- Complex verification strategies can be adopted.

Future work

- Move from the "grid" representation to a more efficient and scalable solution;
- Implement differential inclusions (currently able to model constant behavior within an interval);
- Implement backward reachability (already available for O, very tricky for L_ε).