Probabilistic Abstraction and Verification of Nonlinear Dynamical Systems

David JULIEN
david.julien@univ-nantes.fr

Nantes Université - LS2N (VELO)
B. DELAHAYE, G. CANTIN, G. ARDOUREL

22 Mai 2025

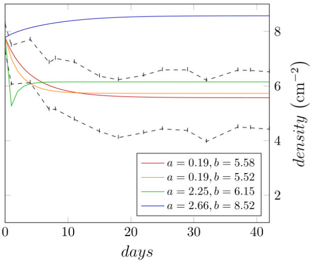
Background & Definitions

Definitions

- ODE: $\frac{\mathrm{d}}{\mathrm{d}t}z(t) = f(z(t))$;
- dynamical system: pair (Ω, f) where $\Omega \subseteq \mathbb{R}^n$ and f is $\mathbf{C}^1$;
- trajectory: solution $z :]a, b[\to \mathbb{R}^n$ to that ODE.

$$\frac{\mathrm{d}}{\mathrm{d}t}x(t) = ax(t)(1 - \frac{b}{x(t)})$$

$$\to f(\cdot) = a[\cdot](1 - \frac{b}{[\cdot]}), \quad a, b \in \mathbb{R}$$



Simulations for the density of *Aurelia aurita* polyps.

Background & Definitions

Definitions

- ODE: $\frac{\mathrm{d}}{\mathrm{d}t}z(t) = f(z(t))$;
- dynamica… ;
- trajector…

Parameterized ODEs

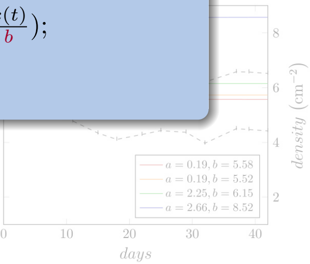
- $\frac{\mathrm{d}}{\mathrm{d}t}z(t) = f(z(t), \lambda)$;
- ex: $\frac{\mathrm{d}}{\mathrm{d}t}x(t) = ax(t)(1 - \frac{x(t)}{b})$;

  $\rightarrow$ change of dynamics?

  $\rightarrow$ change of position?

$$\frac{\mathrm{d}}{\mathrm{d}t}x(t) = \ldots$$

$$\rightarrow f(\cdot) = a[\cdot](1 - \frac{b}{[\cdot]}), \quad a, b \in \mathbb{R}$$



Simulations for the density of *Aurelia aurita* polyps.

Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parameter space Λ;

Two types of transition

- continuous transition (internal evolution) according to f and λ;
- discrete transition (external change of dynamics / position)

Hybrid automaton modeling a watch hand.

Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parameter space Λ;

Two types of transition

- continuous transition (internal evolution) according to f and λ;
- discrete transition (external change of dynamics / position)

Hybrid automaton modeling a watch hand.

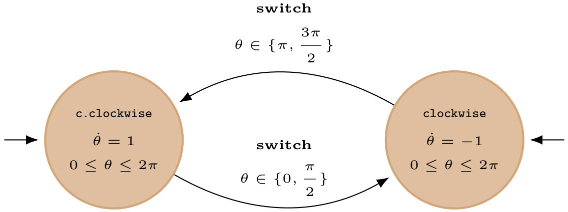
Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parameter space Λ;

Two types of transition

- continuous transition (internal evolution) according to f and λ;
- discrete transition (external change of dynamics / position)



Hybrid automaton modeling a watch hand.

Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parame

Two types of transition

- continuous transition (internal evolution) according to f and λ;
- n (external ics / position)

Limitations [1]

- too expressive;
- rectangular automata only;
- reachability is undecidable if variables are not reset;

  $\rightarrow$ abstract it?

Hybrid automaton modeling a watch hand.

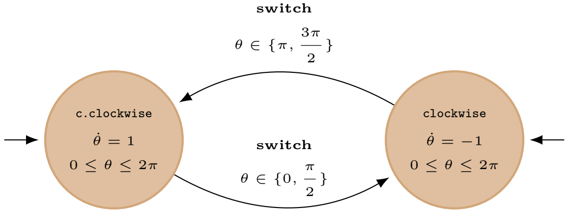
Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parameter space Λ;
- a discretization $\mathcal{T}$ of the timeline;

Two types of transition

- continuous transition (internal evolution) according to f and λ;
- discrete transition (external change of dynamics / position)



Hybrid automaton modeling a watch hand.

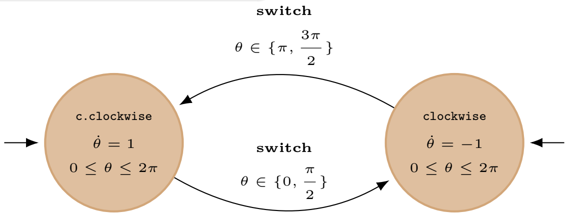
Introducing resets

Hybrid Dynamical Systems

- a function f defining an ODE;
- a phase space Ω;
- a parameter space Λ;
- a discretization $\mathcal{T}$ of the timeline;
- a finite set $\mathcal{D}$ of distributions over Ω or Λ.

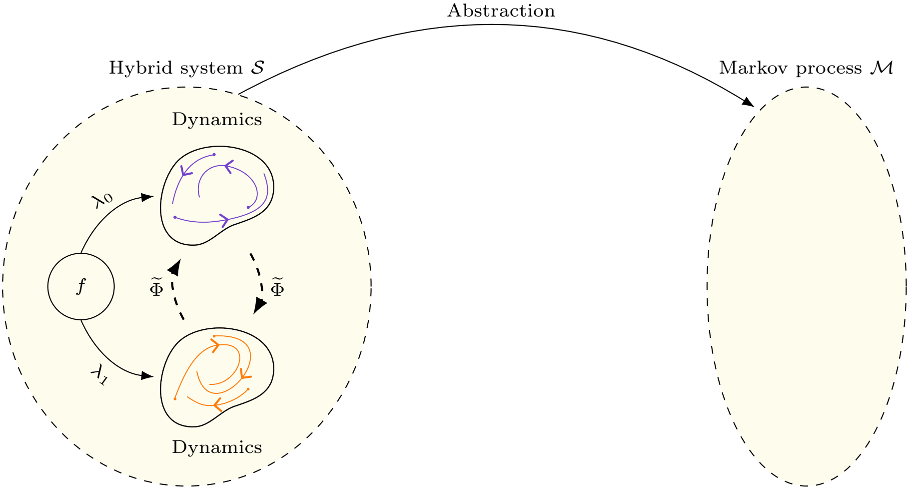
Two types of transition

- continuous transition (internal evolution) according to f and λ;
- discrete transition (external change of dynamics / position) through the realization of a probability distribution at timepoint $t_i \in \mathcal{T}$.

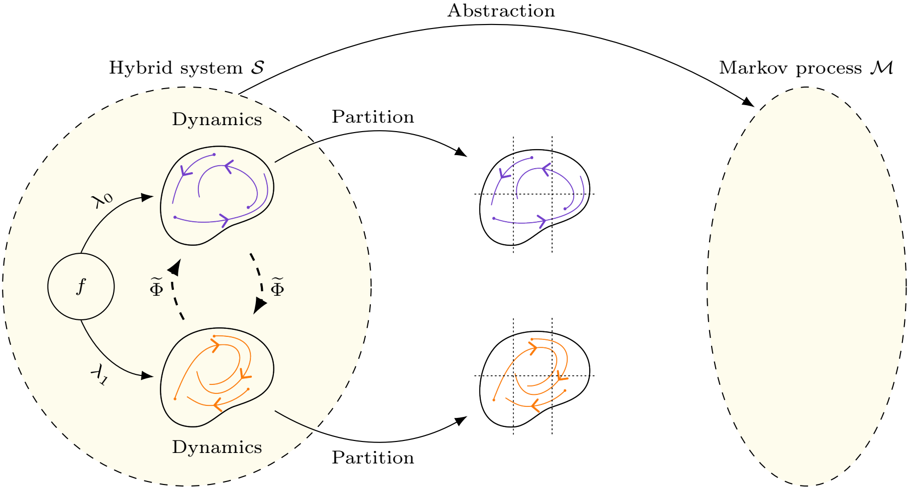


Hybrid automaton modeling a watch hand.

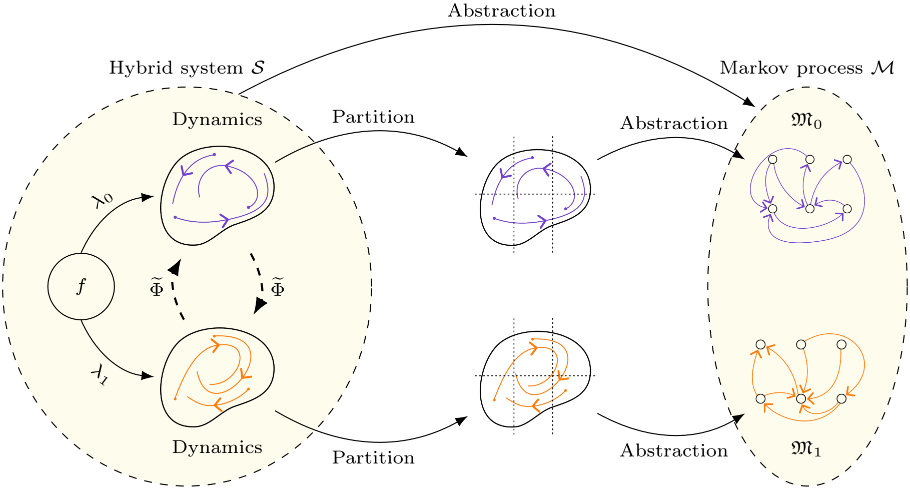
Intuition of the abstraction



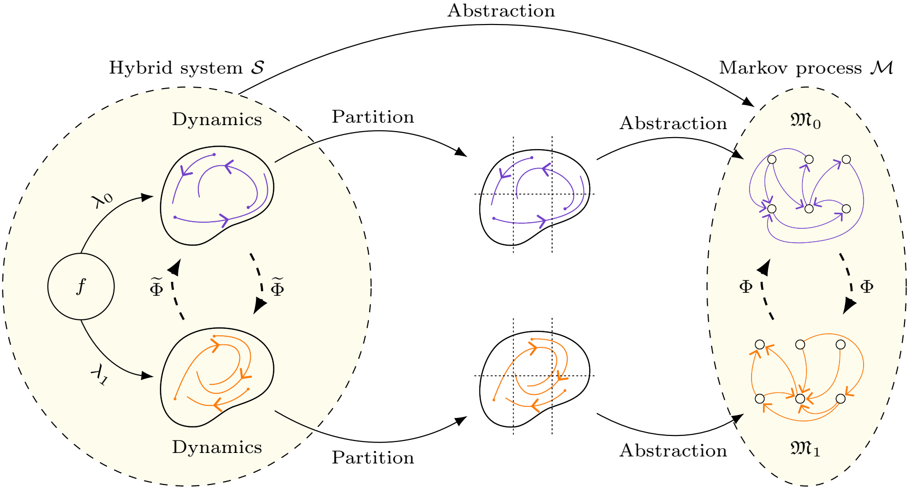
Intuition of the abstraction

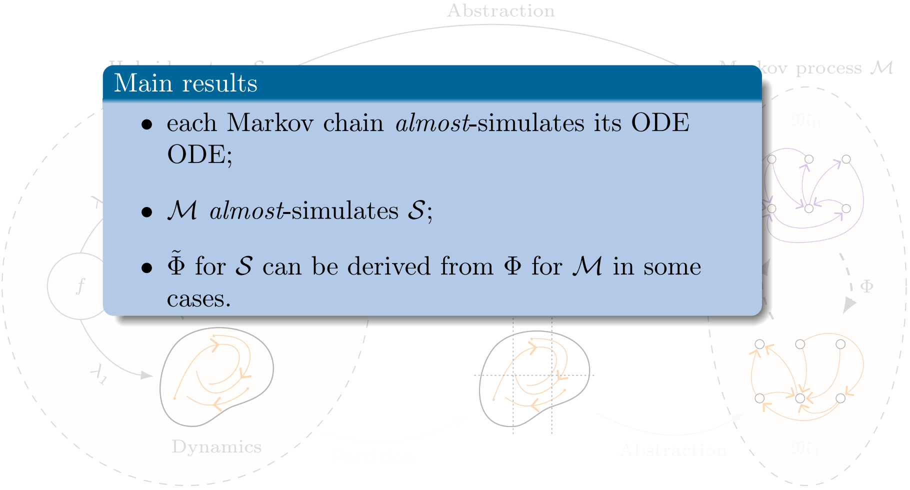


Intuition of the abstraction



Intuition of the abstraction





Main results

- each Markov chain *almost*-simulates its ODE ODE;
- $\mathcal{M}$ *almost*-simulates $\mathcal{S}$;
- $\tilde{\Phi}$ for $\mathcal{S}$ can be derived from Φ for $\mathcal{M}$ in some cases.

Outline

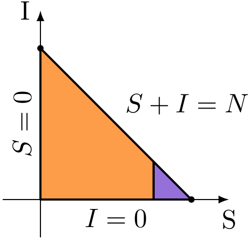
1. A Markov chain *almost* simulates an ODE
2. *Almost*-simulation?
3. A MDP *almost*-simulates a hybrid system

Case study: An epidemiological model [2]

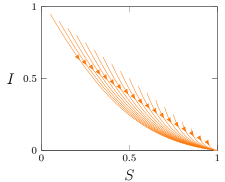
The SIR model

$$\frac{\mathrm{d}S}{\mathrm{d}t} = \alpha - \delta S - \beta \frac{IS}{N},$$
$$\frac{\mathrm{d}I}{\mathrm{d}t} = \beta \frac{IS}{N} - (\gamma + \delta) I, \quad (1)$$
$$\frac{\mathrm{d}R}{\mathrm{d}t} = \gamma I - \delta R,$$

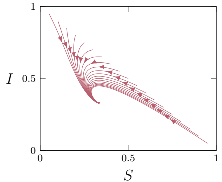
$N = S + I + R$ is constant.



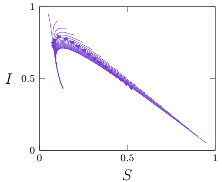
A partition of the phase space of the model.



(a) $\lambda_1 = (0.5, 0.5, 0.5, 0.5)$.



(b) $\lambda_2 = (0.5, 3, 0.5, 0.5)$.



(c) $\lambda_3 = (0.5, 7.5, 0.5, 0.5)$.

Respective representations of the dynamics of the system induced by Eq. (1) and different values for $(\alpha, \beta, \gamma, \delta)$.

Building Markov chains

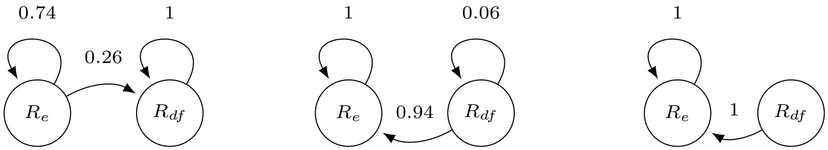
Densities as probabilities

- Fix a duration $\tau > 0$.
- $p_{i,j} = \frac{\mu(\{x_0 \in R_i | x(x_0,\tau) \in R_j\})}{\mu(R_i)}$
  $\Rightarrow x_0 \in R_i$ inducing a trajectory stopping in R_j.

Building a Markov chain

$(\mathfrak{Q}, \mathbb{P})$ with a set $\mathfrak{Q}$ of states and a transition probability distribution $\mathbb{P}$;

- $\mathfrak{Q}$ = regions of the phase space;
- $\mathbb{P}(R_i, R_j) = p_{i,j}$.



(a) $\lambda_1 = (0.5, 0.5, 0.5, 0.5)$. (b) $\lambda_2 = (0.5, 3, 0.5, 0.5)$. (c) $\lambda_3 = (0.5, 7.5, 0.5, 0.5)$.

Almost-simulation

Definition

$\mathcal{R} \subseteq States(\mathcal{S}) \times States(\mathcal{M})$ such that:

1. for any initial state x_i for $\mathcal{S}$, there exists an initial state R_i for $\mathcal{M}$ such that $(x_i, R_i) \in \mathcal{R}$;
2. for any pair $(x_{in}, R_{in}) \in \mathcal{R}$ and any successor x_{out} of x_{in}, there exists a successor R_{out} of R_{in} such that $(x_{out}, R_{out}) \in \mathcal{R}$.

$\Rightarrow (x, R) \in \mathcal{R} \Leftrightarrow x \in R$

Almost-simulation

Definition

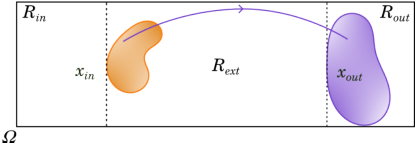
$\mathcal{R} \subseteq States(\mathcal{S}) \times States(\mathcal{M})$ such that:

1. for any initial state x_i for $\mathcal{S}$, there exists an initial state R_i for $\mathcal{M}$ such that $(x_i, R_i) \in \mathcal{R}$;
2. for any pair $(x_{in}, R_{in}) \in \mathcal{R}$ and any successor x_{out} of x_{in}, there exists a successor R_{out} of R_{in} such that $(x_{out}, R_{out}) \in \mathcal{R}$.

$\Rightarrow (x, R) \in \mathcal{R} \Leftrightarrow x \in R$

The border problem

$R_{in} \to R_{out}$ in $\mathcal{M}$ iff ball around x_{in} such that all trajectories stop in R_{out}.



Almost-simulation

Definition

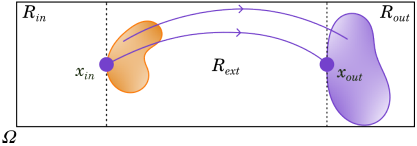
$\mathcal{R} \subseteq States(\mathcal{S}) \times States(\mathcal{M})$ such that:

1. for any initial state x_i for $\mathcal{S}$, there exists an initial state R_i for $\mathcal{M}$ such that $(x_i, R_i) \in \mathcal{R}$;
2. for any pair $(x_{in}, R_{in}) \in \mathcal{R}$ and any successor x_{out} of x_{in}, there exists a successor R_{out} of R_{in} such that $(x_{out}, R_{out}) \in \mathcal{R}$.

$\Rightarrow (x, R) \in \mathcal{R} \Leftrightarrow x \in R$

The border problem

$R_{in} \rightarrow R_{out}$ in $\mathcal{M}$ iff ball around x_{in} such that all trajectories stop in R_{out}.
$\Rightarrow$ not trivial if x_{in} on a border!



Almost-simulation

Definition

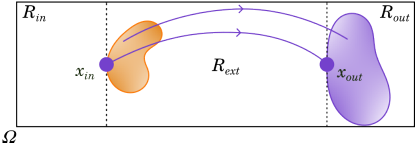
$\mathcal{R} \subseteq States(\mathcal{S}) \times States(\mathcal{M})$ such that:

1. for any initial state x_i for $\mathcal{S}$, there exists an initial state R_i for $\mathcal{M}$ such that $(x_i, R_i) \in \mathcal{R}$;
2. for any pair $(x_{in}, R_{in}) \in \mathcal{R}$ and any successor x_{out} of x_{in}, there exists a successor R_{out} of R_{in} such that $(x_{out}, R_{out}) \in \mathcal{R}$.
3. *almost*-simulation $\Leftrightarrow$ 2. holds almost everywhere.

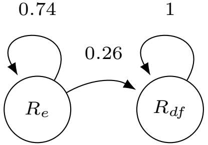
$\Rightarrow (x, R) \in \mathcal{R} \Leftrightarrow x \in R$

The border problem

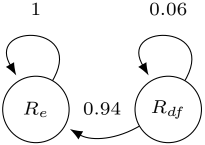
$R_{in} \rightarrow R_{out}$ in $\mathcal{M}$ iff ball around x_{in} such that all trajectories stop in R_{out}.
$\Rightarrow$ not trivial if x_{in} on a border!



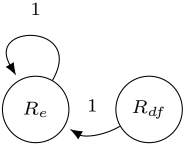
First result



(a) $\lambda_1 = (0.5, 0.5, 0.5, 0.5)$.

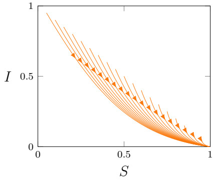


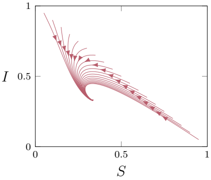
(b) $\lambda_2 = (0.5, 3, 0.5, 0.5)$.

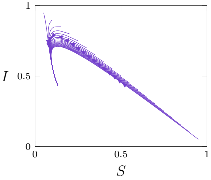


(c) $\lambda_3 = (0.5, 7.5, 0.5, 0.5)$.

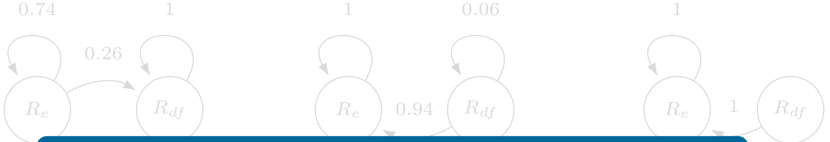
$\Downarrow$







First result

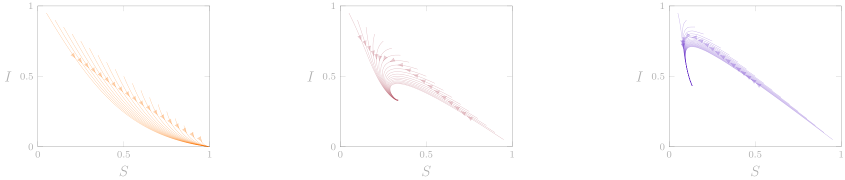


(a) λ … .5, 0.5, 0.5).

First result

The Markov chain $\mathfrak{M}$ *almost*-simulates the ODE $\mathfrak{S}_\lambda$.

$$\Rightarrow \mathbb{P}(\varphi(\mathfrak{M})) = 1 \Rightarrow \mathbb{P}(\varphi(\mathfrak{S}_\lambda)) = 1$$



Aggregating the chains

Building a Markov Decision Process

$(\mathcal{Q}, \mathcal{A}, \mathbb{P})$ with a set $\mathcal{Q}$ of states, a parameterizable transition probability distribution$\mathbb{P}(\cdot, \cdot, \cdot)$, a set $\mathcal{A}$ of actions.

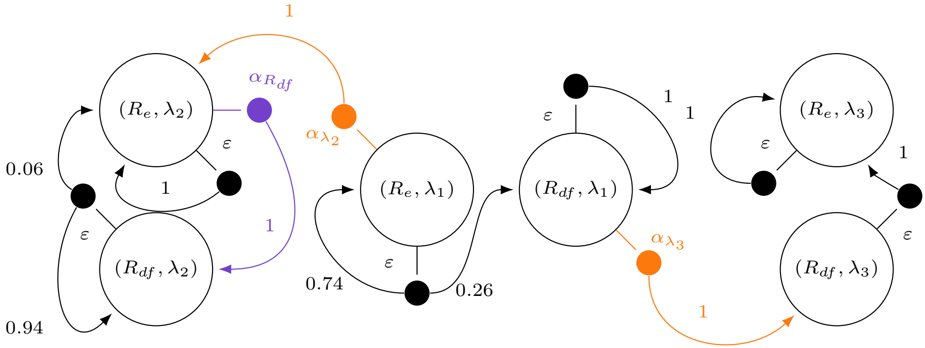
- $\mathcal{Q} = \{(R, \lambda) \in \mathfrak{Q} \times \Lambda\}$;
- actions a;
- for each a, a probability distribution $\mathbb{P}_a = \mathbb{P}(\cdot, a, \cdot)$ over the states of $\mathcal{Q}$;

Three types of action

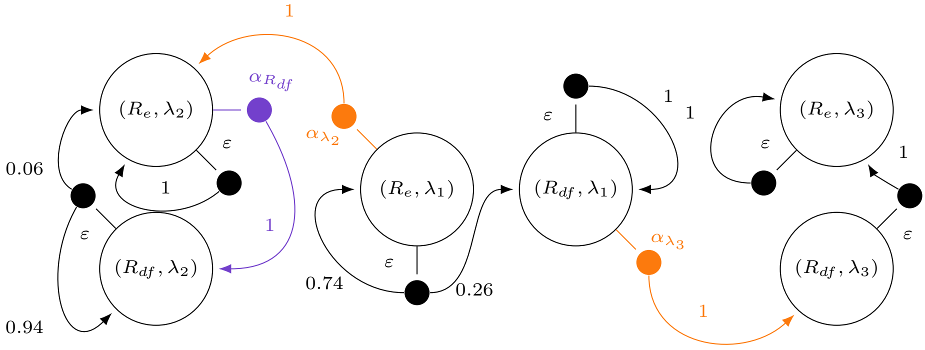
- ε: evolution according to current dynamics;
- $\alpha_{\mathbb{D}^{\mathfrak{Q}}}$: discrete reset of region according to $\mathbb{D}^{\mathfrak{Q}}$;
- $\alpha_{\mathbb{D}^{\Lambda}}$: discrete reset of dynamics according to $\mathbb{D}^{\Lambda}$.

an action $\alpha_{\mathbb{D}}$ corresponds to a distribution $\mathbb{D} \in \mathcal{D}$ for $\mathcal{S}$.

Building a MDP



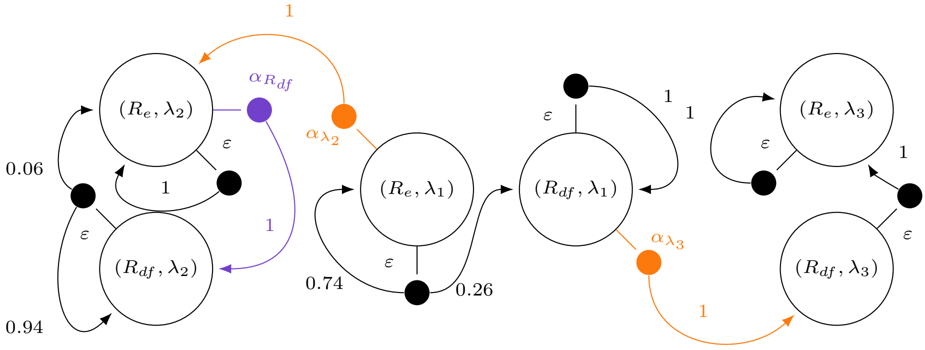
Building a MDP



Theorem

The produced MDP *almost*-simulates $\mathcal{S}$.

Building a MDP



Theorem

The produced MDP *almost*-simulates $\mathcal{S}$.
Given a property φ, $\mathbb{P}(\varphi(\mathcal{M})) = 1 \Rightarrow \mathbb{P}(\tilde{(}\varphi(\mathcal{S})) = 1$.

A strategy for $\mathcal{M}$ leads to a strategy for $\mathcal{S}$

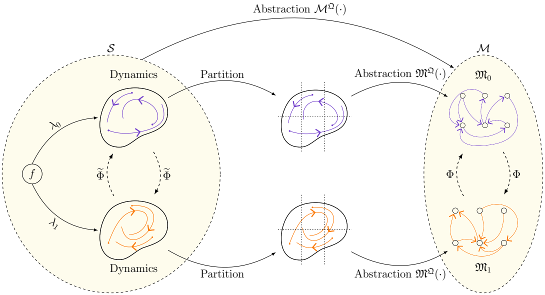
	λ_1	λ_2	λ_3	$\lambda_3^{\leq 6}$	$\lambda_3^{\leq 4}$
$R_{e,1}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$R_{e,2}$	ε	ε	$\alpha_{R_{e,3}}$	$\varnothing$	$\varnothing$
$R_{e,3}$	ε	α_{λ_1}	α_{λ_2}	α_{λ_2}	$\varnothing$
$R_{e,4}$	ε	α_{λ_1}	α_{λ_2}	α_{λ_2}	$\varnothing$
$R_{e,5}$	ε	α_{λ_1}	α_{λ_2}	$\alpha_{R_{df}}$	$\alpha_{R_{df}}$
R_{df}	ε	α_{λ_1}	α_{λ_1}	α_{λ_1}	α_{λ_1}

Table 1: An example of winning strategy Φ for the studied property, where costs are introduced, so that ε-action is free, and α_R-actions are more expensive than α_λ-actions.

	λ_1	λ_2	λ_3	$\lambda_3^{\leq 6}$	$\lambda_3^{\leq 4}$
$R_{e,1}$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$R_{e,2}$	τ	τ	$\mathbb{D}_{\widetilde{x}_3}$	$\varnothing$	$\varnothing$
$R_{e,3}$	τ	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_2}$	$\mathbb{D}_{\lambda_2}$	$\varnothing$
$R_{e,4}$	τ	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_2}$	$\mathbb{D}_{\lambda_2}$	$\varnothing$
$R_{e,5}$	τ	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_2}$	$\mathbb{D}_{\widetilde{x}_{df}}$	$\mathbb{D}_{\widetilde{x}_{df}}$
R_{df}	τ	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_1}$	$\mathbb{D}_{\lambda_1}$

Table 2: An example of winning strategy $\widetilde{\Phi}$ for $\mathcal{S}$ w.r.t. the studied property, where costs are introduced, so that τ-transition is free, and $\mathbb{D}_R$-transitions are more expensive than $\mathbb{D}_\lambda$-transitions.

Merci de votre attention



Bibliography

[1] Thomas A. Henzinger et al. "What's Decidable about Hybrid Automata?" In: *Journal of Computer and System Sciences* 57.1 (Aug. 1998), pp. 94–124. ISSN: 0022-0000. DOI: 10.1006/jcss.1998.1581.

[2] William O. Kermack and Anderson G. McKendrick. "Contributions to the mathematical theory of epidemics—II. The problem of endemicity". In: *Bulletin of Mathematical Biology* 53.1–2 (Mar. 1991), pp. 57–87. ISSN: 1522-9602. DOI: 10.1007/bf02464424.