Guaranteed control synthesis for continuous systems in Uppaal-Tiga

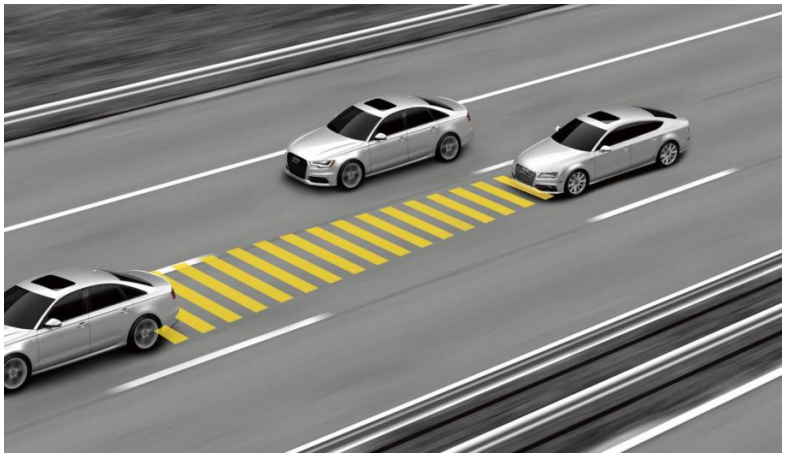
CyPhy 2018

Kim G. Larsen, Adrien Le Coënt,
Jakob H. Taankvist, Marius Mikučionis

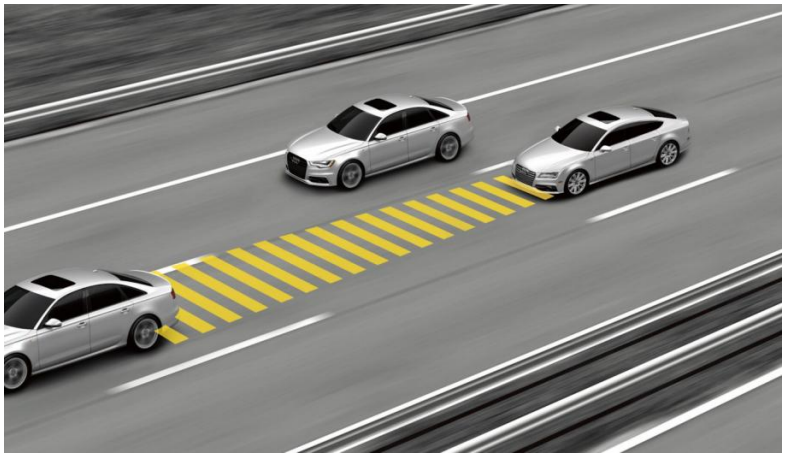
AALBORG UNIVERSITET

DEIS

Context: control systems



Context: control systems



Issues: guaranteed control synthesis for safety/stability/reachability of safety critical systems

Outline

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

- state $x \in \mathbb{R}^n$

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

- state $x \in \mathbb{R}^n$
- bounded perturbation $d(\cdot) : \mathbb{R}^+ \longrightarrow D \subset \mathbb{R}^m$

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

- state $x \in \mathbb{R}^n$
- bounded perturbation $d(\cdot) : \mathbb{R}^+ \longrightarrow D \subset \mathbb{R}^m$
- switching signal $\sigma(\cdot) : \mathbb{R}^+ \longrightarrow U$ (piecewise constant)

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

- state $x \in \mathbb{R}^n$
- bounded perturbation $d(\cdot) : \mathbb{R}^+ \longrightarrow D \subset \mathbb{R}^m$
- switching signal $\sigma(\cdot) : \mathbb{R}^+ \longrightarrow U$ (piecewise constant)
- $U = \{1, \ldots, N\}$ finite set of modes, associated with the dynamics

$$\dot{x}(t) = f_u(x(t), d(t)), \ u \in U$$

Switched Systems

A continuous-time switched system

$$\dot{x}(t) = f_{\sigma(t)}(x(t), d(t)) \tag{1}$$

is a family of continuous-time dynamical systems with a rule σ that determines at each time which one is active

- state $x \in \mathbb{R}^n$
- bounded perturbation $d(\cdot) : \mathbb{R}^+ \longrightarrow D \subset \mathbb{R}^m$
- switching signal $\sigma(\cdot) : \mathbb{R}^+ \longrightarrow U$ (piecewise constant)
- $U = \{1, \ldots, N\}$ finite set of modes, associated with the dynamics

$$\dot{x}(t) = f_u(x(t), d(t)), \ u \in U$$

We focus on sampled switched systems: switching instants occur periodically every τ, i.e. σ is constant on $[i\tau, (i+1)\tau)$

Examples of switched systems

Control of switched systems: possible approaches

- Optimal control [Trélat, Rubio, Fattorini,...]
  - Minimization under constraints of a cost function

Control of switched systems: possible approaches

- Optimal control [Trélat, Rubio, Fattorini,...]
  - Minimization under constraints of a cost function
- Lyapunov approaches [Krstic, Teel, Coron, Sigalotti, Liberzon...]
  - Stability analysis and stabilization using Lyapunov functions

Control of switched systems: possible approaches

- Optimal control [Trélat, Rubio, Fattorini,...]
  - Minimization under constraints of a cost function
- Lyapunov approaches [Krstic, Teel, Coron, Sigalotti, Liberzon...]
  - Stability analysis and stabilization using Lyapunov functions
- Symbolic methods

Control of switched systems: possible approaches

- Optimal control [Trélat, Rubio, Fattorini,...]
  - Minimization under constraints of a cost function
- Lyapunov approaches [Krstic, Teel, Coron, Sigalotti, Liberzon...]
  - Stability analysis and stabilization using Lyapunov functions
- Symbolic methods
  - Finite state abstraction methods:
    - Approximate bisimulation (PESSOA/CoSyMA) [Tabuada,Girard...]
    - Feedback refinement relations (SCOTS) [Zamani, Rungger, Reissig...]

Control of switched systems: possible approaches

- Optimal control [Trélat, Rubio, Fattorini,...]
  - Minimization under constraints of a cost function
- Lyapunov approaches [Krstic, Teel, Coron, Sigalotti, Liberzon...]
  - Stability analysis and stabilization using Lyapunov functions
- Symbolic methods
  - Finite state abstraction methods:
    - Approximate bisimulation (PESSOA/CoSyMA) [Tabuada,Girard...]
    - Feedback refinement relations (SCOTS) [Zamani, Rungger, Reissig...]
  - Tiling methods:
    - Uniform tiling [Girard, Witrant, Arcak...]
    - Adaptive state-space bisection (MINIMATOR) [Soulat, Fribourg]

Control Synthesis Problem

We consider the state-dependent control problem of synthesizing σ:

Control Synthesis Problem

We consider the state-dependent control problem of synthesizing σ:

At each sampling time $k\tau$, find the appropriate switched mode $u \in U$ according to the current value of x, in order to achieve some objectives:

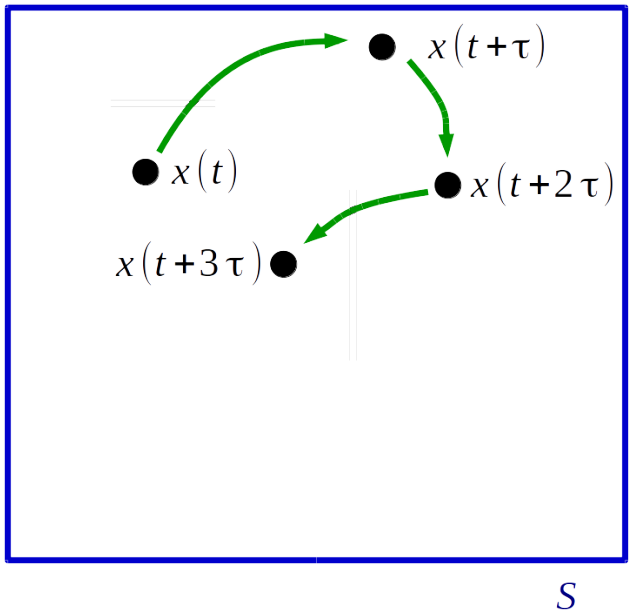
Control Synthesis Problem

We consider the state-dependent control problem of synthesizing σ:

At each sampling time $k\tau$, find the appropriate switched mode $u \in U$ according to the current value of x, in order to achieve some objectives:

Given a set S:

- Safety in S: $x(t)$ stays in S forever



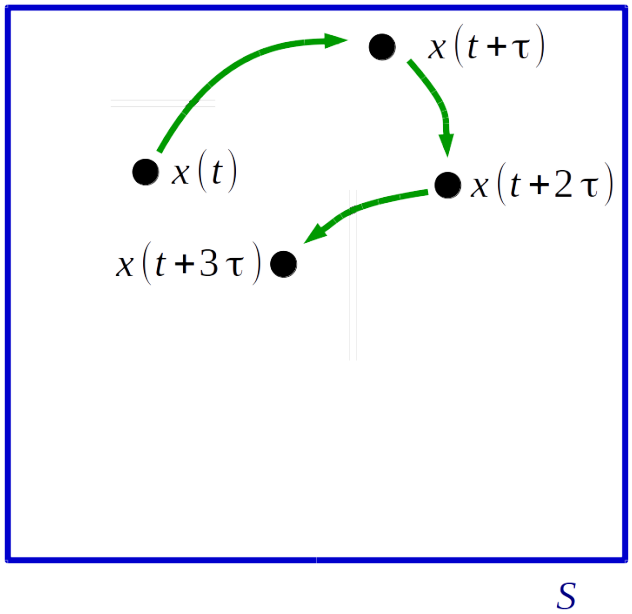
Control Synthesis Problem

We consider the state-dependent control problem of synthesizing σ:

At each sampling time $k\tau$, find the appropriate switched mode $u \in U$ according to the current value of x, in order to achieve some objectives:

Given a set S:

- Safety in S: $x(t)$ stays in S forever



NB: classic stabilization impossible here (no common equilibrium pt)
$\rightsquigarrow$ practical stability

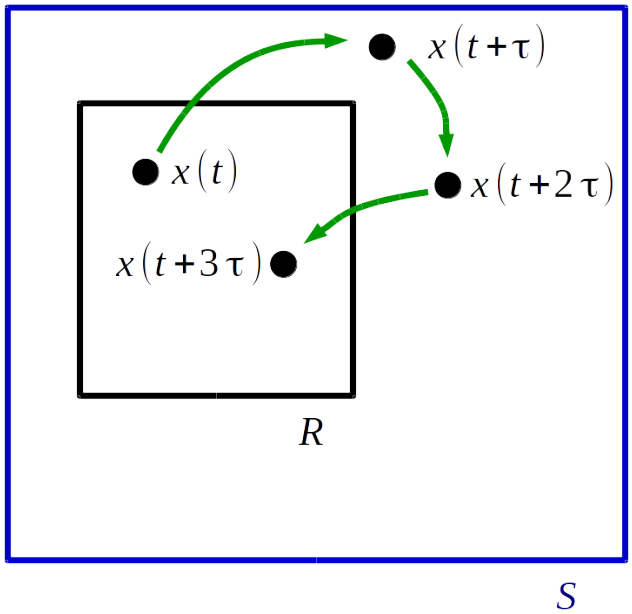
Control Synthesis Problem

We consider the state-dependent control problem of synthesizing σ:

At each sampling time $k\tau$, find the appropriate switched mode $u \in U$ according to the current value of x, in order to achieve some objectives:

Given two sets R, S:

- (R, S)-stability: $x(t)$ returns in R infinitely often, at some multiples of sampling period τ, and always stays in S

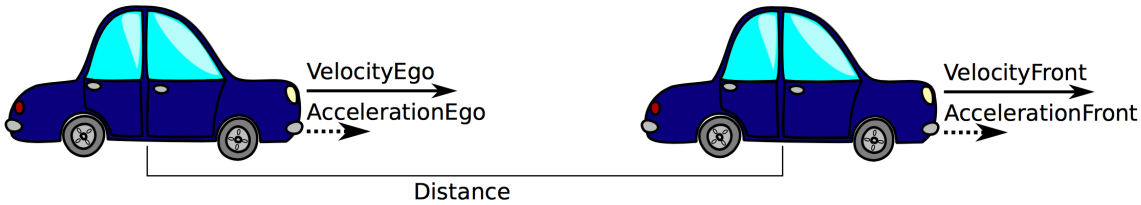


NB: classic stabilization impossible here (no common equilibrium pt)
$\rightsquigarrow$ practical stability

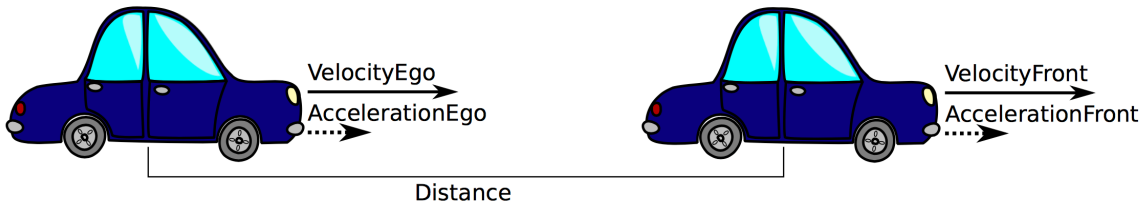
Outline

Outline

A cruise control application



A cruise control application



$$\dot{v}_f = a_f \tag{2}$$

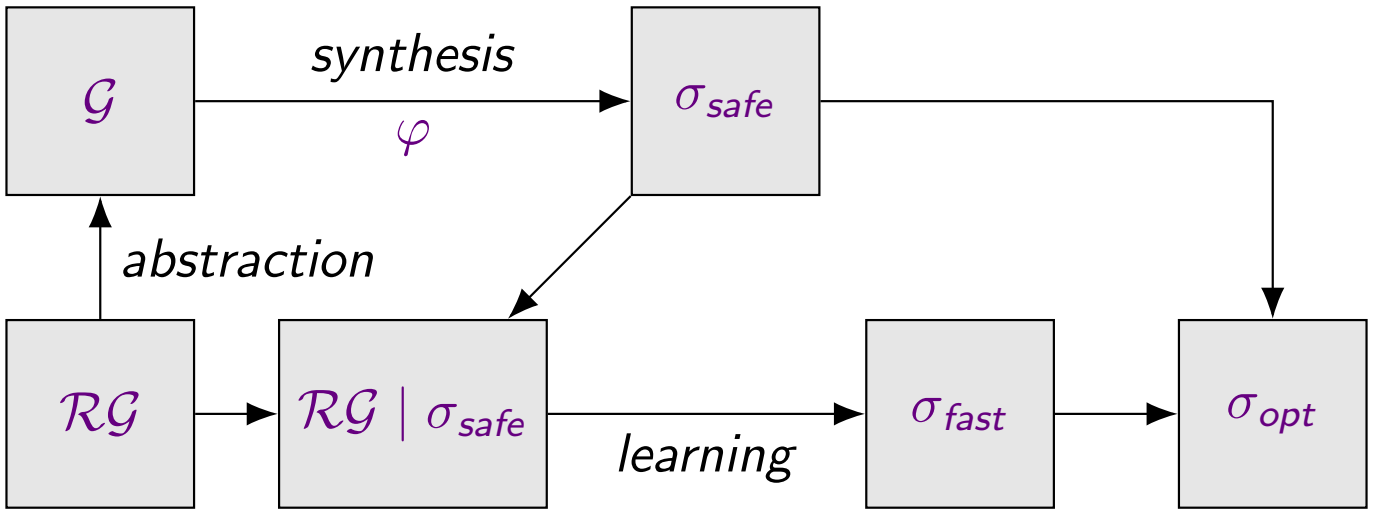
$$\dot{v}_e = a_e \tag{3}$$

$$\dot{d} = v_f - v_f \tag{4}$$

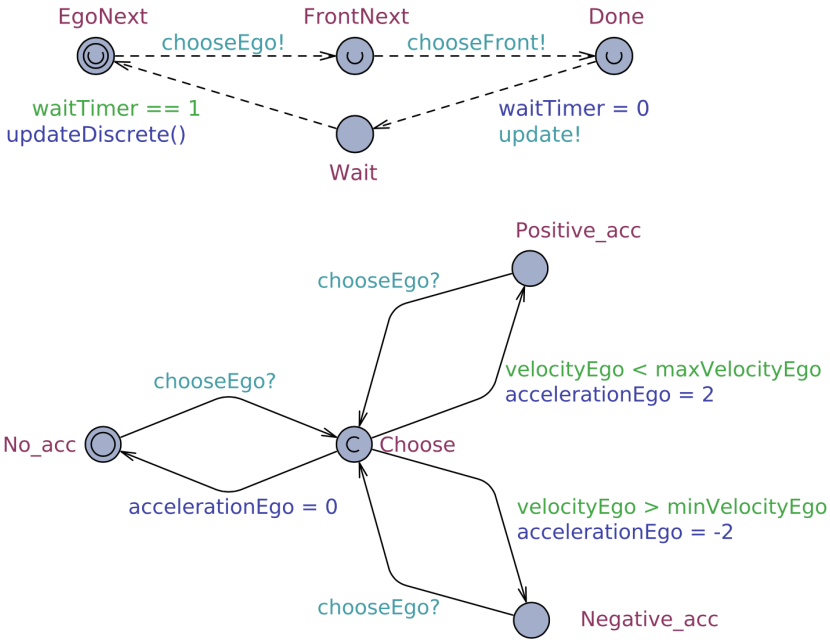
a_f and a_e can take the values -2, 0, and 2, resulting in an 8-mode switched system

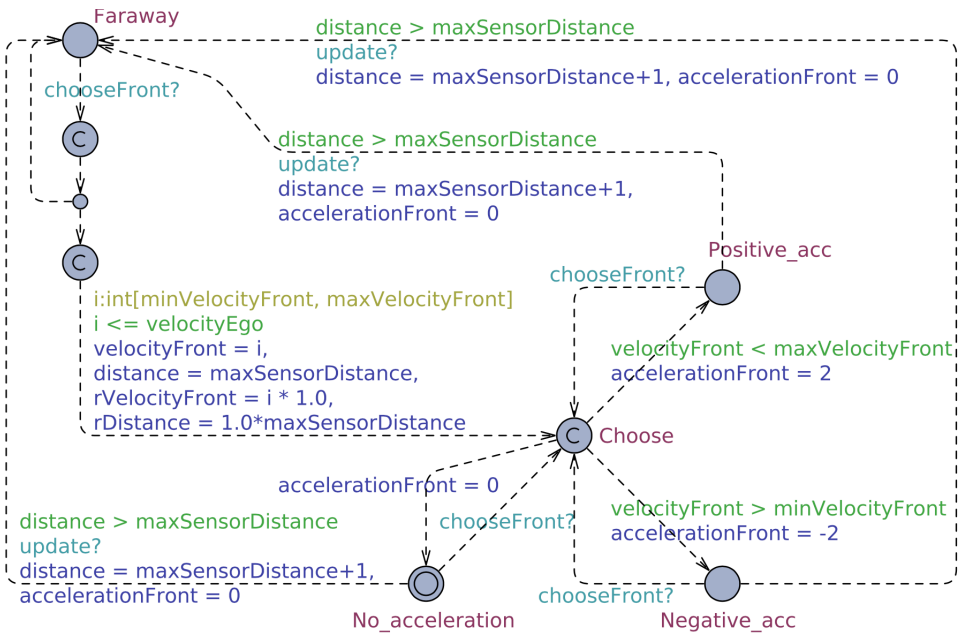
Safety set: $S = [-10, 20] \times [-10, 20] \times [5, 200]$.

Uppaal Stratego original workflow



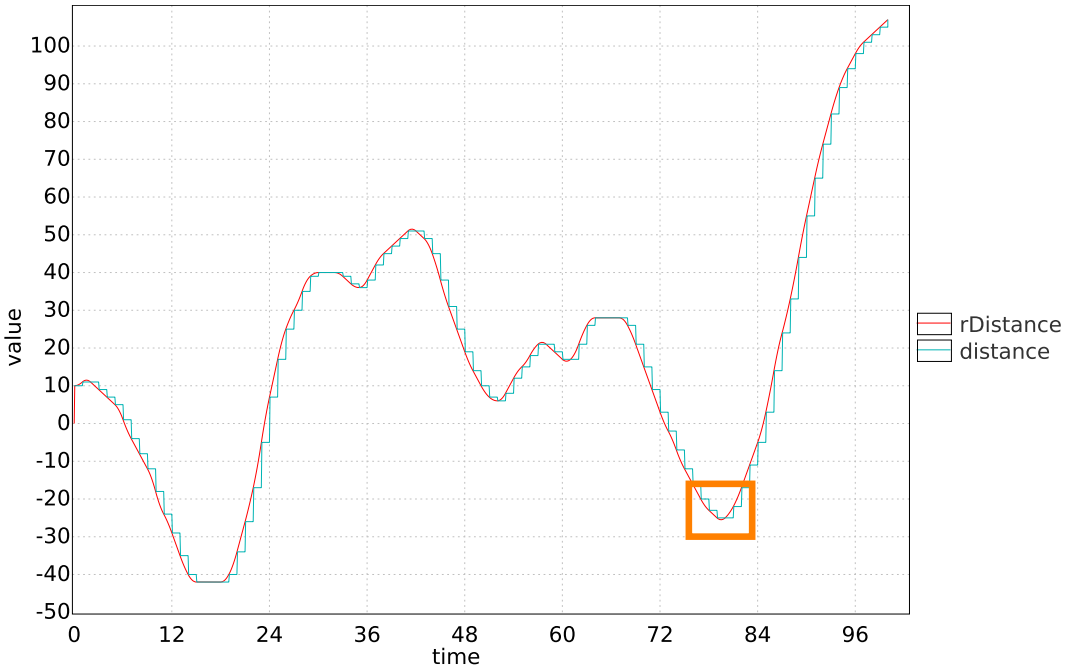
Timed game model of the cruise control

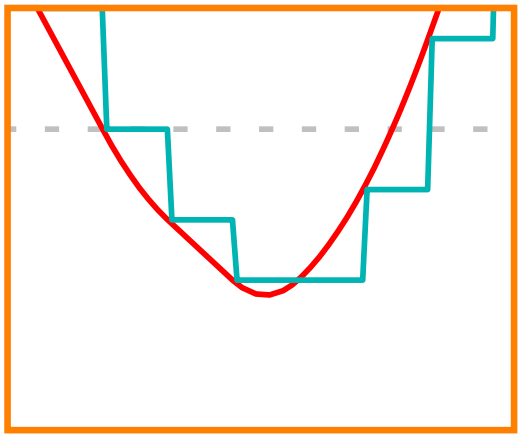




Standard discretization of the dynamics

Kim G. Larsen, Marius Mikučionis, Jakob H. Taankvist. *Safe and optimal adaptive cruise control*. 2015.





Guaranteed Euler scheme

$(H0)$ (Lipschitz): for all $j \in U$, there exists a constant $L_j > 0$ such that:

$$\|f_j(y) - f_j(x)\| \leq L_j \|y - x\| \quad \forall x, y \in S.$$

$(H1)$ (One-sided Lipschitz/Strong monotony): for all $j \in U$, there exists a constant $\lambda_j \in \mathbb{R}$ such that

$$\langle f_j(y) - f_j(x), y - x \rangle \leq \lambda_j \|y - x\|^2 \quad \forall x, y \in T,$$

NB: constants computed by constrained optimization.

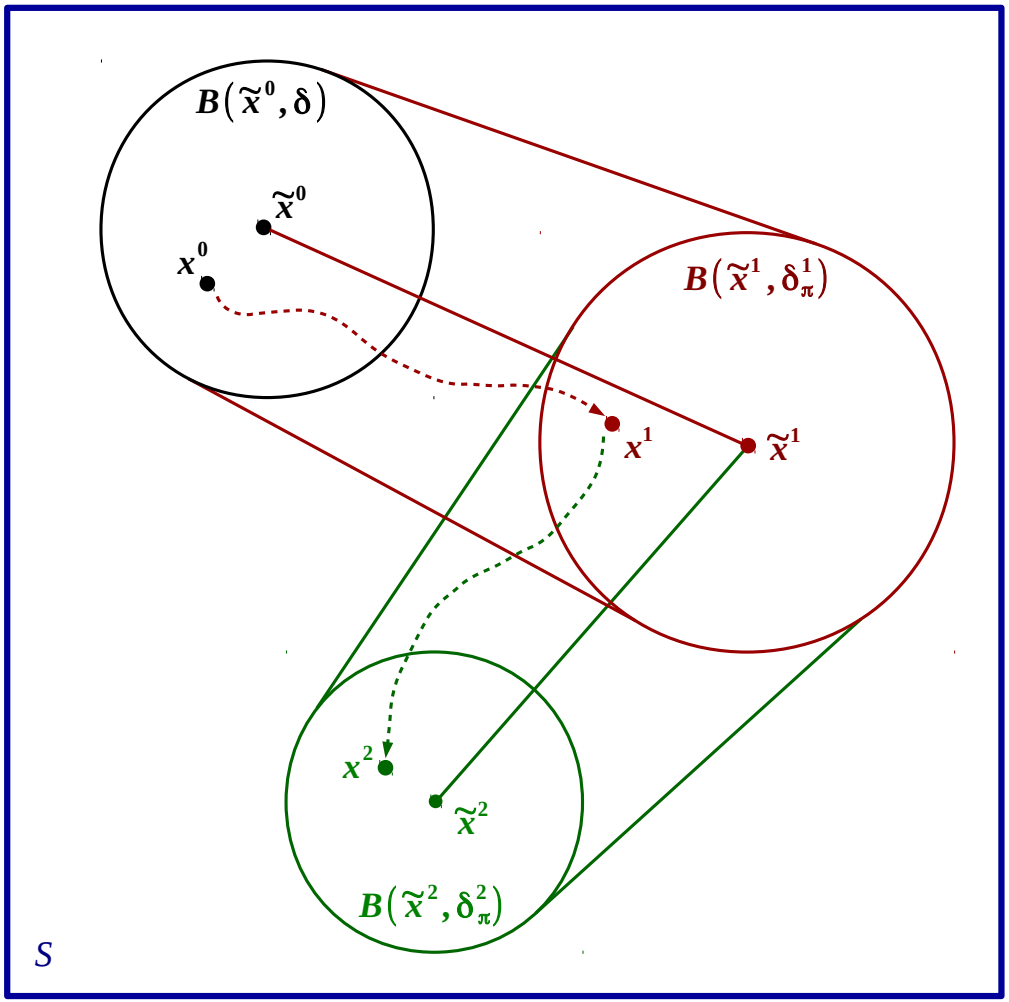
Guaranteed Euler scheme

Theorem

Given a sampled switched system satisfying (H0-H1), consider a point $\tilde{x}^0$ *and a positive real* δ*. We have, for all* $x^0 \in B(\tilde{x}^0, \delta)$, $t \in [0, \tau]$ *and* $j \in U$*:* $\phi_j(t; x^0) \in B(\tilde{\phi}_j(t; \tilde{x}^0), \delta_j(t))$.
with

- *if* $\lambda_j < 0$: $\delta_j(t) = \left(\delta^2 e^{\lambda_j t} + \frac{C_j^2}{\lambda_j^2}\left(t^2 + \frac{2t}{\lambda_j} + \frac{2}{\lambda_j^2}\left(1 - e^{\lambda_j t}\right)\right)\right)^{\frac{1}{2}}$
- *if* $\lambda_j = 0$: $\delta_j(t) = \left(\delta^2 e^t + C_j^2(-t^2 - 2t + 2(e^t - 1))\right)^{\frac{1}{2}}$
- *if* $\lambda_j > 0$: $\delta_j(t) = \left(\delta^2 e^{3\lambda_j t} + \frac{C_j^2}{3\lambda_j^2}\left(-t^2 - \frac{2t}{3\lambda_j} + \frac{2}{9\lambda_j^2}\left(e^{3\lambda_j t} - 1\right)\right)\right)^{\frac{1}{2}}$

Application to guaranteed integration



The guaranteed Euler scheme in UPPAAL TIGA

Theorem

Consider system (1) *satisfying (H0) and (H1), and an initial condition* $x_0 \in S$ *at time* 0.

- *If* x_0 *is an integer, let* $x'_0 = x_0$
- *Otherwise, let* $x'_0 = \frac{\lfloor x_0 \rfloor + \lceil x_0 \rceil}{2}$

Let $h = \tau / k$ *be the step size of the Euler method. Given a controller* C*, let us compute iteratively two sequences of integer states as follows:*

$$y_0^{min} = \lfloor x'_0 \rfloor \quad at\ t = 0$$

$$y_0^{max} = \lceil x'_0 \rceil \quad at\ t = 0$$

and

$$y_{i+1}^{min} = h^k_{C(i\tau)}\left(\frac{y_i^{max} + y_i^{min}}{2}, \left\| \frac{y_i^{max} - y_i^{min}}{2} \right\|\right) \quad at\ t = (i+1)\tau$$

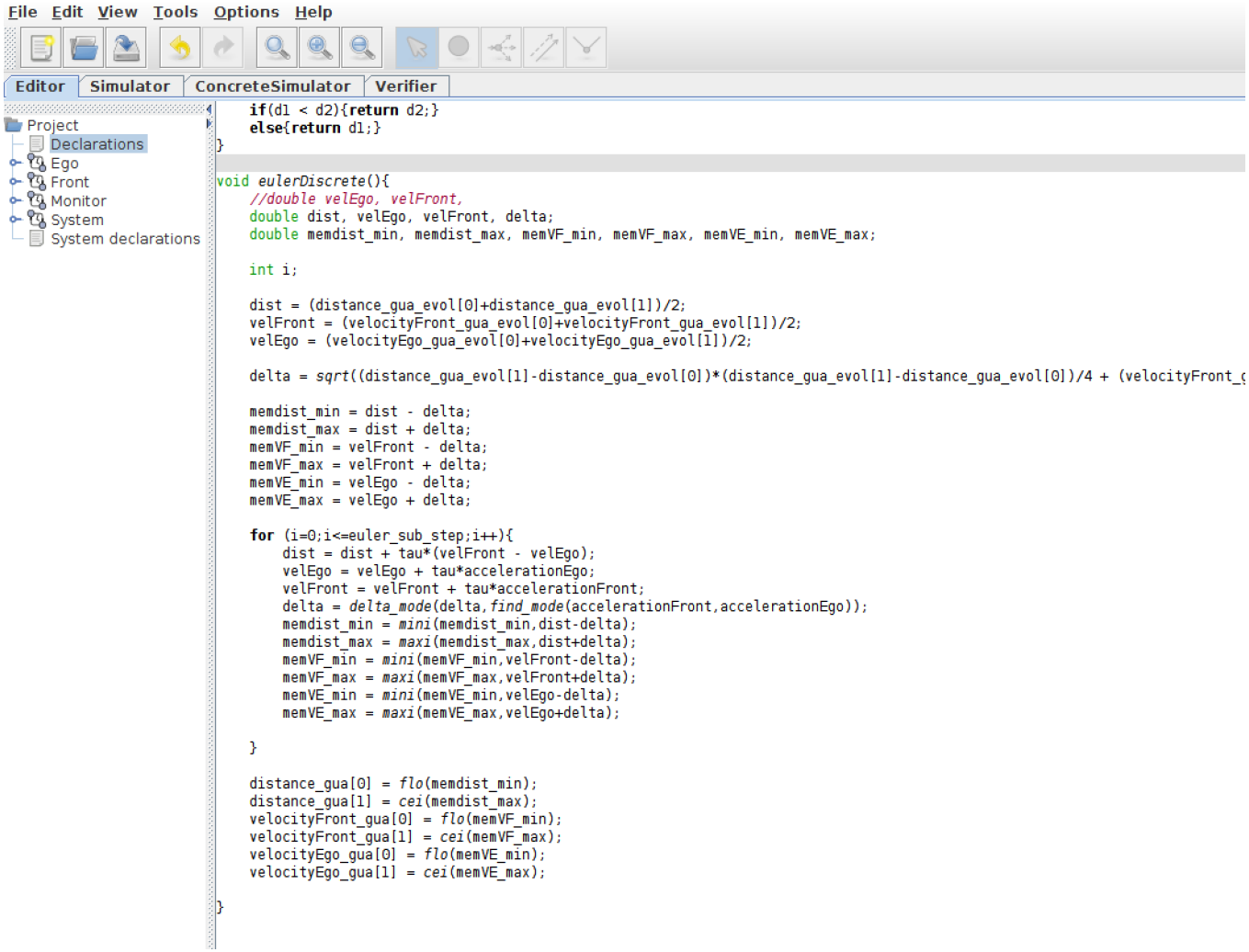
$$y_{i+1}^{max} = g^k_{C(i\tau)}\left(\frac{y_i^{max} + y_i^{min}}{2}, \left\| \frac{y_i^{max} - y_i^{min}}{2} \right\|\right) \quad at\ t = (i+1)\tau$$

If controller C *verifies, for all* $t = i\tau$ *with* $i \in \mathbb{N}$*:*

$$H^k_{C(t)}\left(\frac{y_i^{max} + y_i^{min}}{2}, \left\| \frac{y_i^{max} - y_i^{min}}{2} \right\|\right) \in S \wedge G^k_{C(t)}\left(\frac{y_i^{max} + y_i^{min}}{2}, \left\| \frac{y_i^{max} - y_i^{min}}{2} \right\|\right) \in S, \tag{5}$$

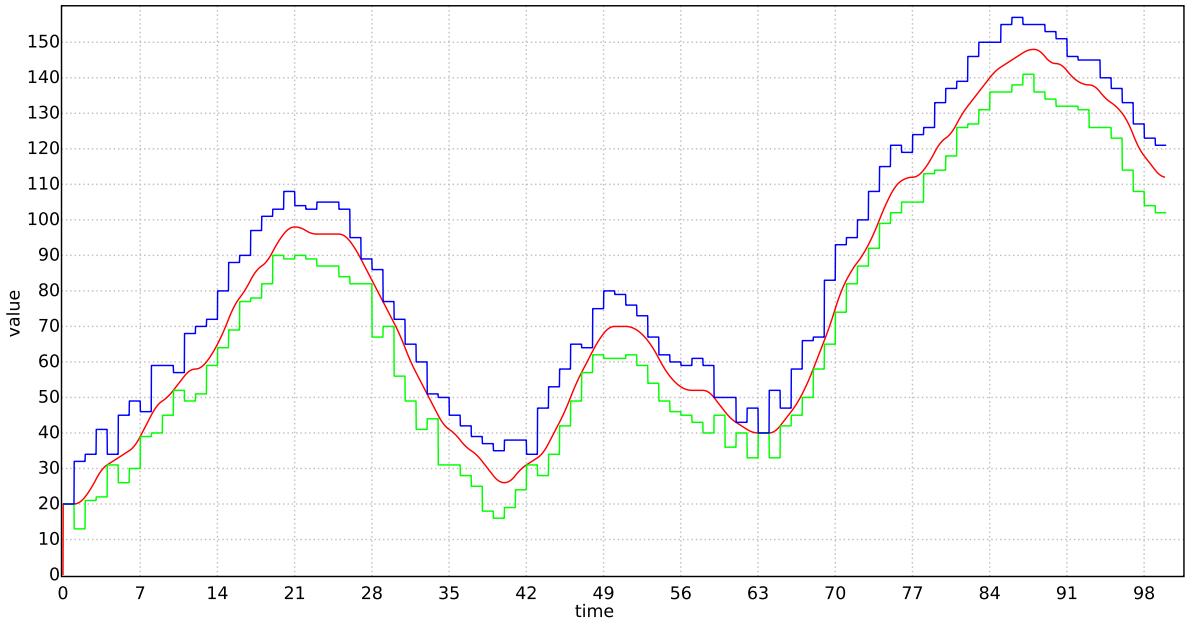
then system (1) *is safe with respect to* S*.*

Example of UPPAAL implementaiton



Integer approximation of the continuous dynamics

Integer bounding of the real distance within time:



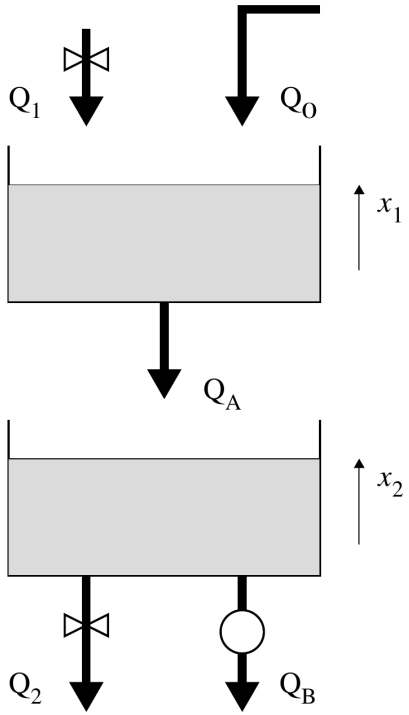
Requirement: all functions must use integers as inputs and return integers

Two tank case study

- Dynamics:

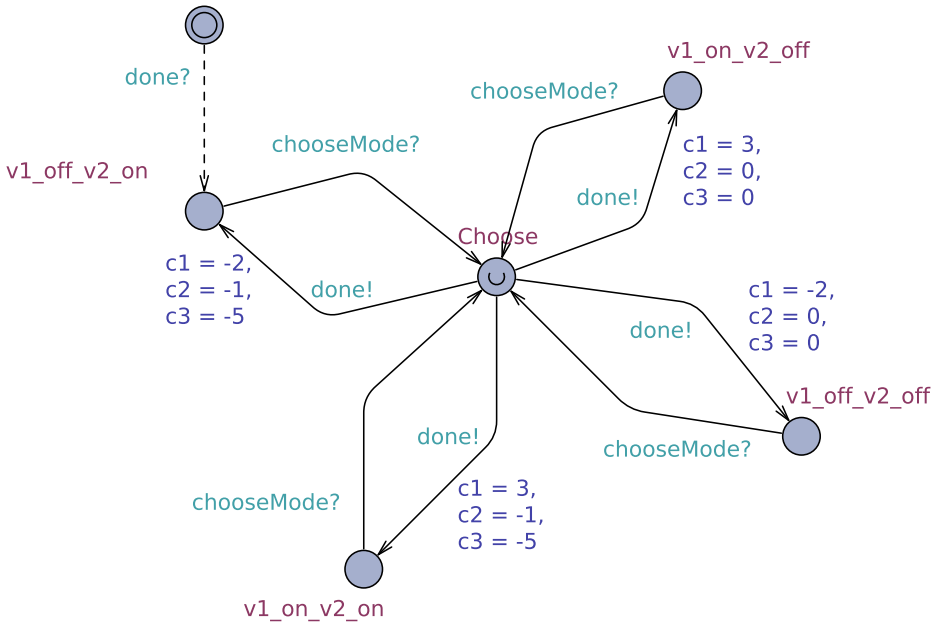
$$\dot{x}_1 = -x_1 + c_1$$
$$\dot{x}_2 = x_1 + c_2 x_2 + c_3$$

with $c_1 \in \{-2, 3\}$, $c_2 \in \{0, -1\}$, $c_3 \in \{0, -5\}$.



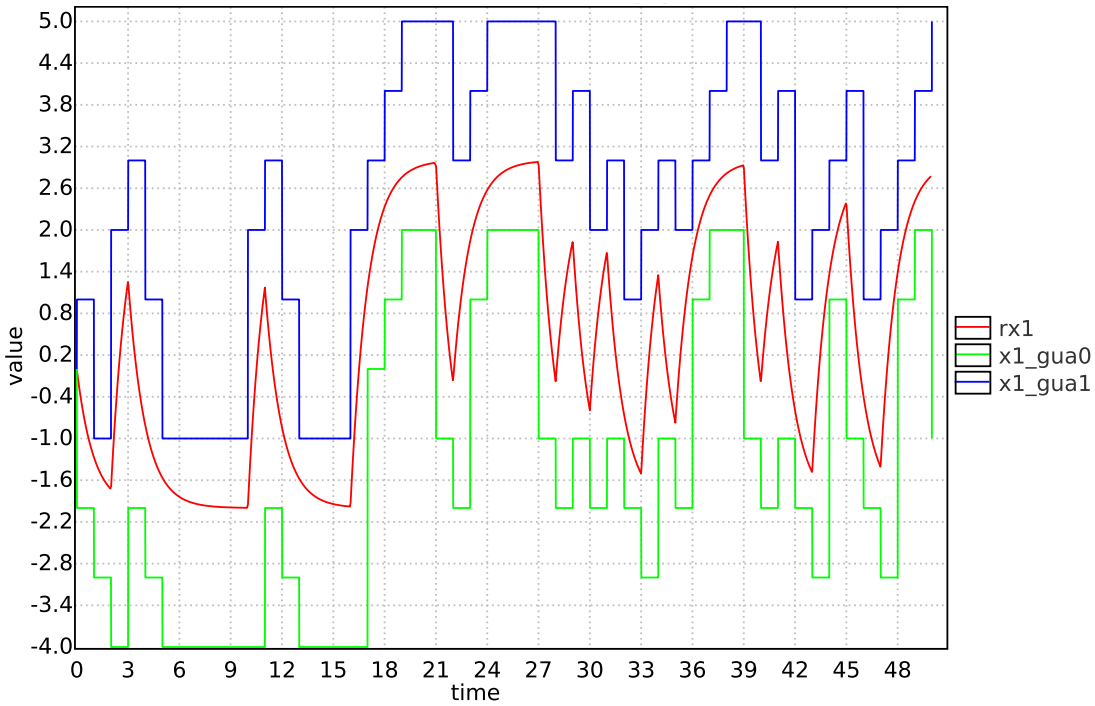
Two tank case study

Timed game model:



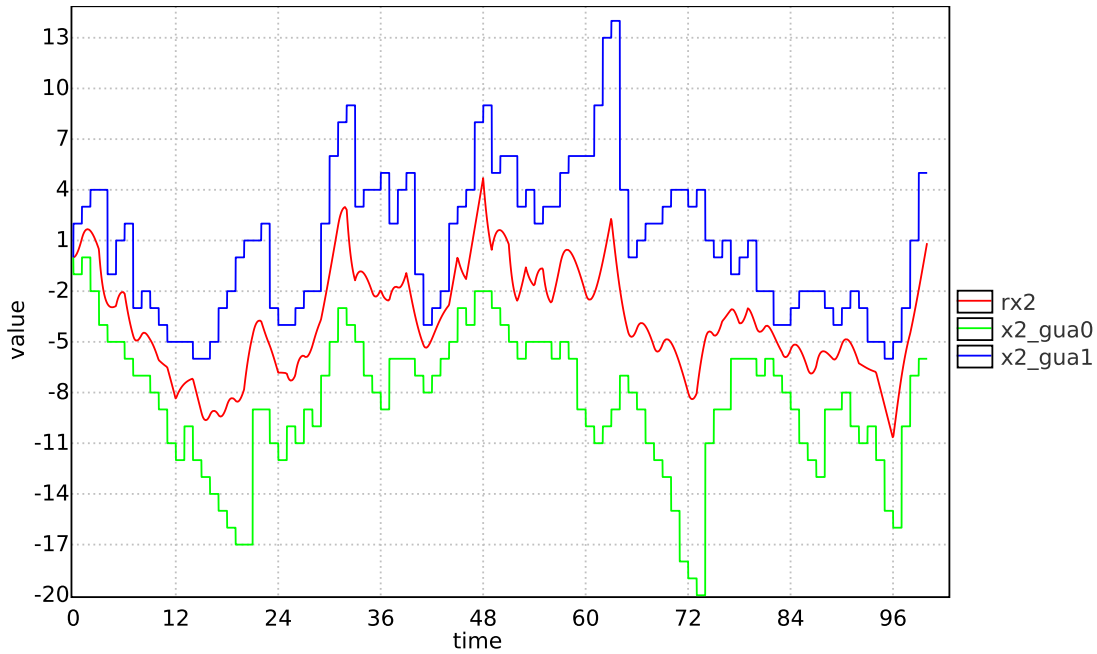
Two tank case study

Guaranteed simulations:



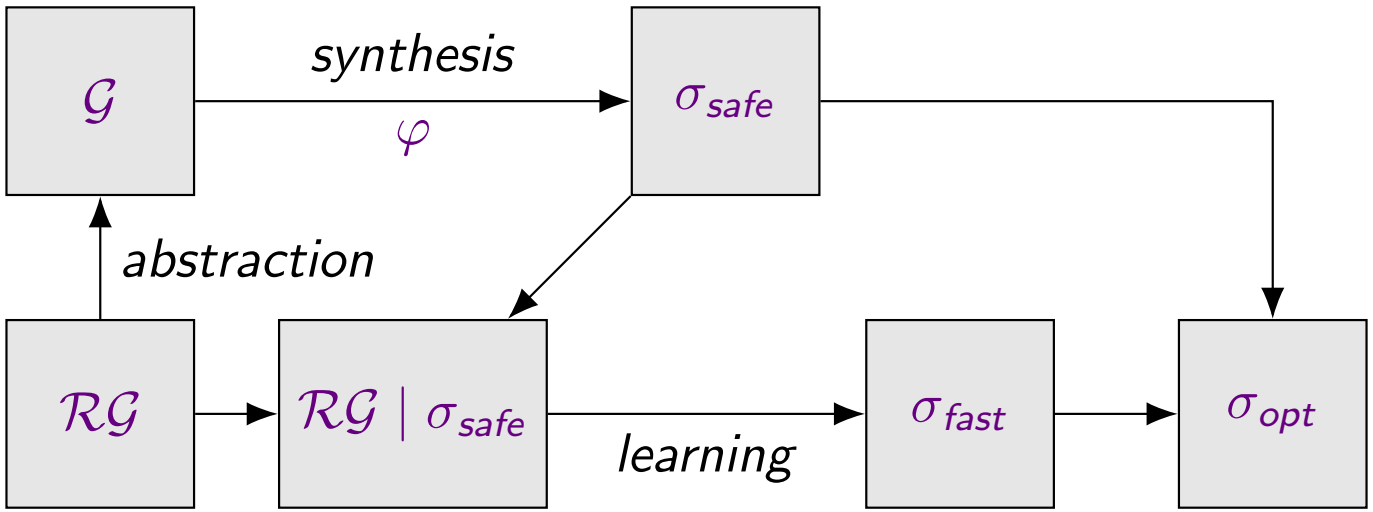
Two tank case study

Guaranteed simulations:



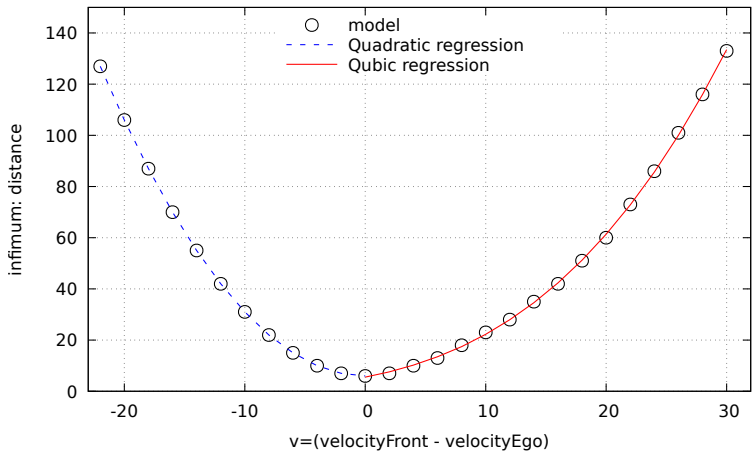
Outline

Uppaal Stratego original workflow

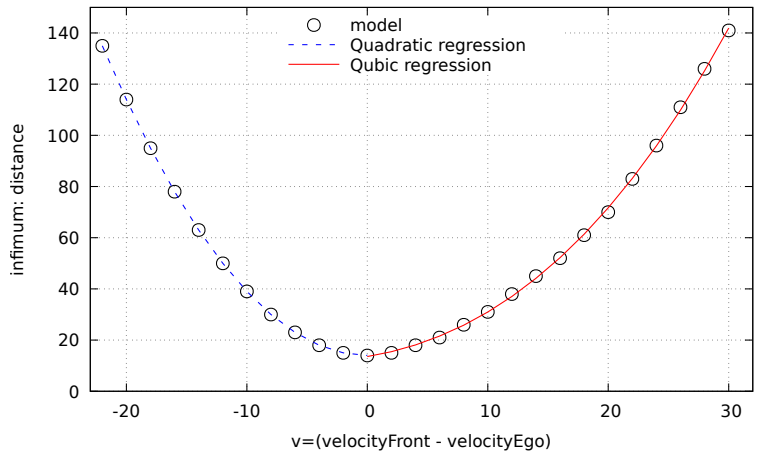


Optimization of the safe strategy

Smallest achievable distance under the (guaranteed) safe strategy as a function of the relative velocity of the two cars:



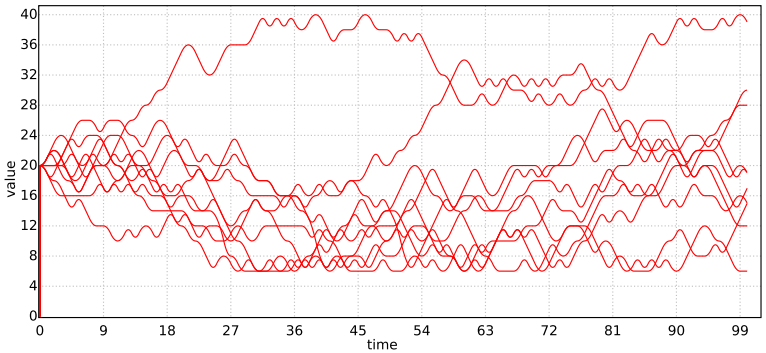
(a) Strategy previously computed.



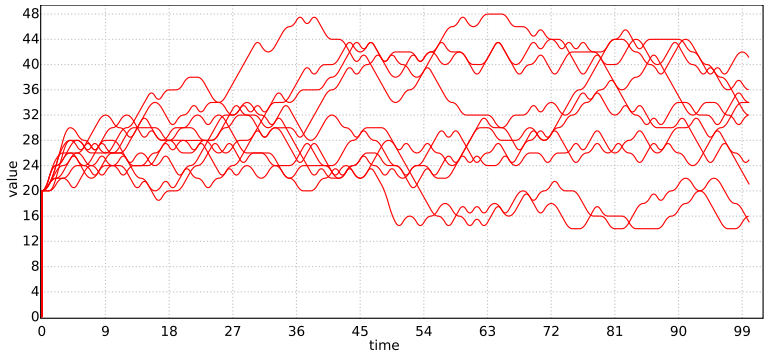
(b) Safe and guaranteed strategy.

Optimization of the safe strategy

Distance over time for 10 simulations under the two different optimised strategies:



(a) Optimised strategy computed previously.



(b) Optimised safe and guaranteed strategy.

Conclusions

Our approach:

- Abstraction from SHG (Switched System) to TG
- Use of UPPAAL TIGA for synthesizing strategies for TG
- Any kind further optimization/model checking is possible

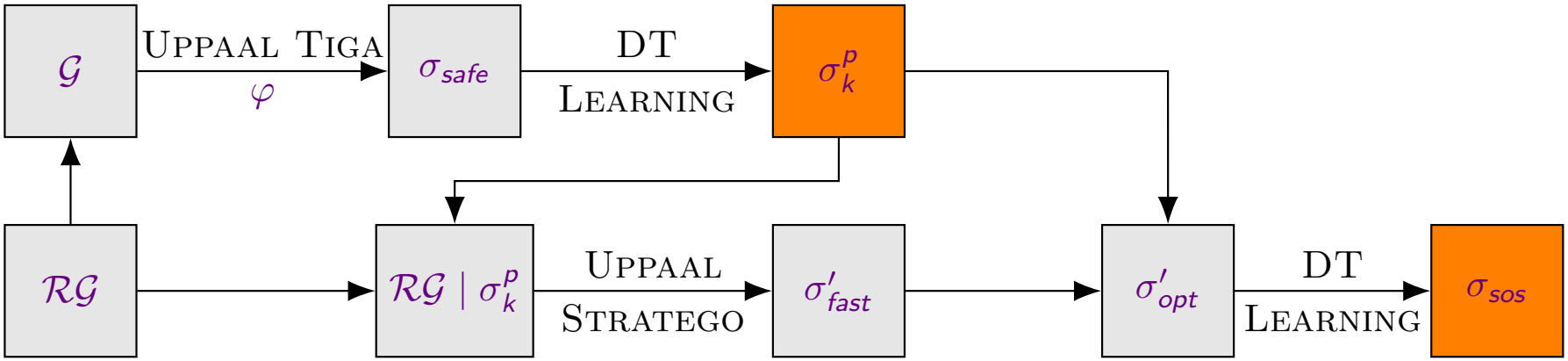
Pros:

- Implemented entirely in UPPAAL (no need of external libraries)
- Possibility of handling time-dependent objectives

Cons:

- Twice as many variables as the original switched system

Future work


$\mathcal{G}$
Uppaal Tiga
φ
σ_{safe}
DT
Learning
σ^p_k
$\mathcal{RG}$
$\mathcal{RG} \mid \sigma^p_k$
Uppaal
Stratego
σ'_{fast}
σ'_{opt}
DT
Learning
σ_{sos}

New framework

Definition (Stochastic Hybrid Game)

A *stochastic hybrid game* G is a tuple (C, U, X, F, δ) where:

1. C is a controller with a finite set of (controllable) modes $C = \{c_1, \ldots, c_k\}$,
2. U is the environment with a finite set of (uncontrollable) modes $U = \{u_1, \ldots, u_l\}$,
3. $X = \{x_1, \ldots, x_n\}$ is a finite set of continuous (real-valued) variables,
4. for each $c \in C$ and $u \in U$, $F_{c,u} : \mathbb{R}_{>0} \times \mathbb{R}^X \to \mathbb{R}^X$ is the flow-function that describes the evolution of the continuous variables over time in the combined mode (c, u), and
5. δ is a family of probability functions $\delta_\gamma : U \to [0, 1]$. More precisely, $\delta_\gamma(u')$ is the probability that u in the global configuration $\gamma = (c, u, v)$ will change to the uncontrollable mode u'.