Timing contracts for embedded control systems

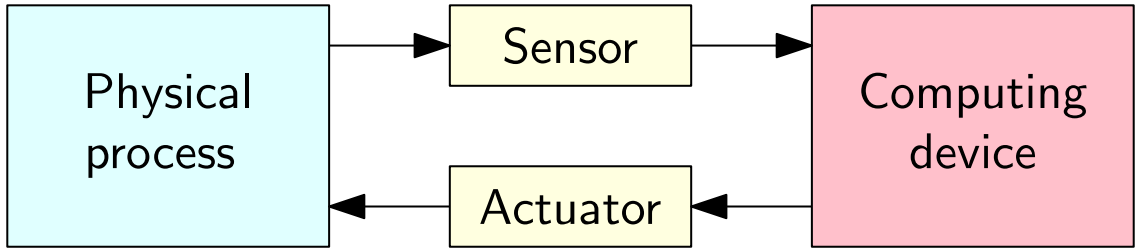
Antoine Girard

Joint work with Mohammad Al Khatib and Thao Dang

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

Co^4 *workshop, LAAS Toulouse*
October 26-28, 2016

Contract-based design of embedded control systems

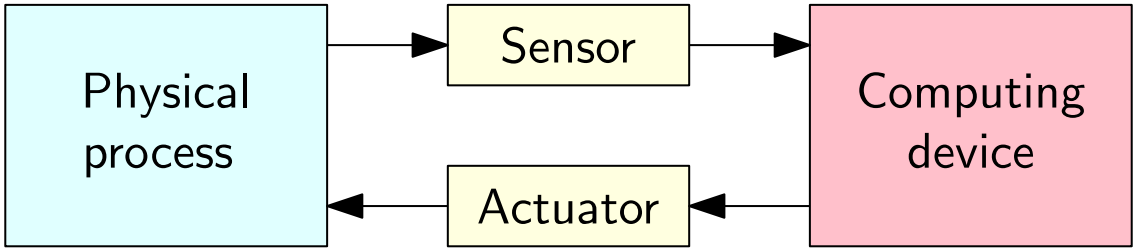


- A timing contract specifies constraints on instants at which certain operations must be performed (sampling, actuation, computation, etc.);

  [Derler et al., Cyber-physical system design contracts, ICCPS'13]

- Separation of concerns between control and computation:
  - Control engineers design a control law that is robust to all possible timing variations allowed by the contract;
  - Software engineers provide an implementation that conforms the contract.

System model



Embedded control systems of the form:

$$\begin{array}{rcll} \dot{z}(t) & = & Az(t) + Bu(t), & \\ u(t) & = & Kz(t_k^s), & \forall t \in [t_k^a, t_{k+1}^a) \end{array} \tag{1}$$

where $z(t) \in \mathbb{R}^p$, $u(t) \in \mathbb{R}^m$ and $(t_k^s)_{k\in\mathbb{N}}$, $(t_k^a)_{k\in\mathbb{N}}$ are the sequences of sampling and actuation instants.

We denote:

- $\tau_k = t_k^a - t_k^s$ the sampling-to-actuation delay.
- $h_k = t_{k+1}^s - t_k^s$ the sampling period.

Timing contracts

The sequences $(t_k^s)_{k\in\mathbb{N}}$ and $(t_k^a)_{k\in\mathbb{N}}$ satisfy a timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$:

$$\begin{array}{ll} 0 \leq t_0^s, & \\ t_k^s \leq t_k^a \leq t_{k+1}^s, & \forall k \in \mathbb{N} \\ \tau_k = t_k^a - t_k^s \in [\underline{\tau}, \overline{\tau}], & \forall k \in \mathbb{N} \\ h_k = t_{k+1}^s - t_k^s \in [\underline{h}, \overline{h}], & \forall k \in \mathbb{N}. \end{array}$$

where contract parameters $(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ belong to the following set:

$$\mathcal{C} = \left\{ (\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h}) \in \mathbb{R}_0^+ \times \mathbb{R}_0^+ \times \mathbb{R}^+ \times \mathbb{R}^+ : \underline{\tau} \leq \overline{\tau} \leq \overline{h}, \underline{h} \leq \overline{h} \right\}.$$

- $\underline{\tau}$, $\overline{\tau}$ provide bounds on the sampling-to-actuation delay.
- $\underline{h}$, $\overline{h}$ provide bounds on the sampling period.

Control engineering viewpoint – stability verification

Definition

System $\mathcal{S} = (A, B, K)$ is globally uniformly exponentially stable (GUES) under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if there exist $C \in \mathbb{R}^+$ and $\lambda \in \mathbb{R}^+$, such that for all $(t_k^s)_{k\in\mathbb{N}}$ and $(t_k^a)_{k\in\mathbb{N}}$ satisfying $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$, the solutions of (1) satisfy:

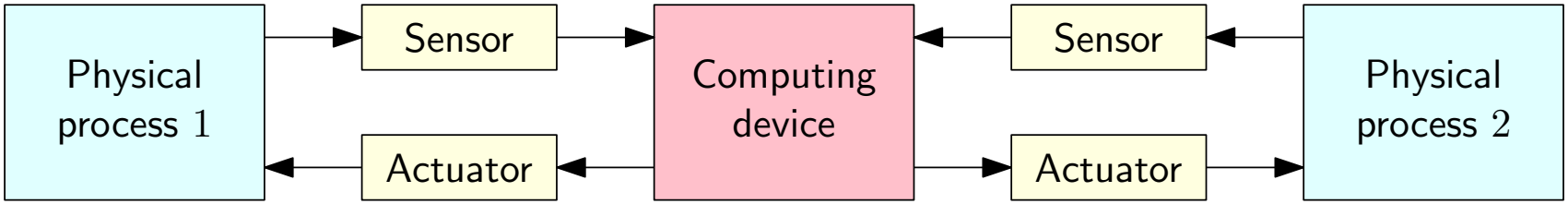
$$\|z(t)\| \leq Ce^{-\lambda(t-t_0^a)}\|z(t_0^a)\|, \ \forall t \geq t_0^a.$$

Problem (Stability verification)

Given: *System* $\mathcal{S} = (A, B, K)$;
Timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$;

Goal: *Verify that* $\mathcal{S}$ *is GUES under timing contract* $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$.

Computation model



Consider a set of systems $\{\mathcal{S}_i\}_{i=1,\dots,N}$, where:

- Each system $\mathcal{S}_i$ is subject to a timing contract $\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)$;
- All systems share a common computational resource.

Computation model:

- A control task is $\mathcal{T}_i = [\underline{c}_i, \overline{c}_i]$ where $\underline{c}_i$, $\overline{c}_i \in \mathbb{R}^+$ denote the best and worst case execution times for computing the input of $\mathcal{S}_i$.
- Computation of the input of $\mathcal{S}_i$ starts at instants $(t_k^{b_i})_{k\in\mathbb{N}}$ and ends at instants $(t_k^{e_i})_{k\in\mathbb{N}}$.

Computation model

- Under timing contract $\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)$, the sequences $(t_k^{s_i})_{k\in\mathbb{N}}$, $(t_k^{a_i})_{k\in\mathbb{N}}$, $(t_k^{b_i})_{k\in\mathbb{N}}$, $(t_k^{e_i})_{k\in\mathbb{N}}$ must satisfy:

$$\begin{array}{ll} 0 \leq t_0^{s_i} & \\ t_k^{s_i} \leq t_k^{b_i} \leq t_k^{e_i} \leq t_k^{a_i} \leq t_{k+1}^{s_i}, & \forall k \in \mathbb{N} \\ c_k^i = t_k^{e_i} - t_k^{b_i} \in [\underline{c}_i, \overline{c}_i], & \forall k \in \mathbb{N} \\ \tau_k^i = t_k^{a_i} - t_k^{s_i} \in [\underline{\tau}_i, \overline{\tau}_i], & \forall k \in \mathbb{N} \\ h_k^i = t_{k+1}^{s_i} - t_k^{s_i} \in [\underline{h}_i, \overline{h}_i], & \forall k \in \mathbb{N} \end{array} \tag{2}$$

- In addition, the shared computational resource can be used by at most one system at any time:

$$\forall i_1, i_2 \in \{1, \ldots, N\},\ i_1 \neq i_2, \implies \mathrm{Comp}_{i_1} \cap \mathrm{Comp}_{i_2} = \emptyset, \tag{3}$$

where $\mathrm{Comp}_i = \bigcup_{k\in\mathbb{N}} [t_k^{b_i}, t_k^{e_i})$.

Software engineering viewpoint – schedulability verification

Definition

Control tasks $\{\mathcal{T}_i = [\underline{c}_i, \overline{c}_i]\}_{i=1\ldots,N}$ are schedulable under timing contracts $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1\ldots,N}$ if for all $(c_k^i)_{k\in\mathbb{N}}$ with $c_k^i \in [\underline{c}_i, \overline{c}_i]$, for all $k \in \mathbb{N}$, $i = 1, \ldots, N$, there exist $(t_k^{s_i})_{k\in\mathbb{N}}$, $(t_k^{b_i})_{k\in\mathbb{N}}$, $(t_k^{e_i})_{k\in\mathbb{N}}$, and $(t_k^{a_i})_{k\in\mathbb{N}}$ satisfying (2-3), for all $i = 1, \ldots, N$.

Problem (Schedulability verification)

Given: *Control tasks* $\{\mathcal{T}_i = [\underline{c}_i, \overline{c}_i]\}_{i=1\ldots,N}$;
Timing contracts $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1\ldots,N}$;

Goal: *Verify that* $\{\mathcal{T}_i\}_{i=1\ldots,N}$ *is schedulable under timing contracts* $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1\ldots,N}$.

Requirement engineering viewpoint – contract synthesis

In practice, one has to come with timing contracts that can be met by both control and software engineers.

Problem (Contract synthesis)

Given: *Systems* $\{\mathcal{S}_i = (A_i, B_i, K_i)\}_{i=1\ldots,N}$;
Control tasks $\{\mathcal{T}_i = [\underline{c}_i, \overline{c}_i]\}_{i=1\ldots,N}$;

Goal: *Synthesize a parameter set* $\mathcal{P}^* \subseteq \mathcal{C}^N$ *such that for all* $(\underline{\tau}_1, \overline{\tau}_1, \underline{h}_1, \overline{h}_1, \ldots, \underline{\tau}_N, \overline{\tau}_N, \underline{h}_N, \overline{h}_N) \in \mathcal{P}^*$:

1. $\mathcal{S}_i$ *is GUES under timing contract* $\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)$, *for all* $i = 1, \ldots, N$;
2. $\{\mathcal{T}_i\}_{i=1\ldots,N}$ *is schedulable under timing contracts* $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1\ldots,N}$.

Stability Verification

Existing approaches

Several existing approaches for stability analysis of system $\mathcal{S} = (A, B, K)$ for instances of timing contracts $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$:

Modeling	Computation	References
Difference inclusions	LMI	[Cloosterman et al. 2010]
		[Donkers et al. 2011, Hetel et al. 2013]
	SOS	[Briat 2013, Seuret & Peet 2013]
	Set invariance	[Fiacchini & Morarescu 2016]
Time delay systems	LMI	[Fridman 2010, Liu et al. 2010]
Hybrid systems	LMI	[Naghshtabrizi et al. 2008]
	SOS	[Bauer et al. 2012]

Our approach:

- Reformulation as difference inclusions;
- Stability analysis using reachability analysis.

Reformulation as impulsive linear system

We rewrite the system under the form of an impulsive linear system:

$$\begin{array}{rcll} \dot{x}(t) & = & A_c x(t), & \forall t \in \mathbb{R}^+ \setminus \{t_k^s, t_k^a\}_{k\in\mathbb{N}} \\ x(t_k^s) & = & A_s x(t_k^{s-}), & \\ x(t_k^a) & = & A_a x(t_k^{a-}), & \end{array} \tag{4}$$

where $x(t) = (z(t), Kz(t_k^s), u(t)) \in \mathbb{R}^n$ for all $t \in [t_k^s, t_{k+1}^s)$ and

$$A_c = \begin{pmatrix} A & 0 & B \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; A_s = \begin{pmatrix} I_p & 0 & 0 \\ K & 0 & 0 \\ 0 & 0 & I_m \end{pmatrix}, A_a = \begin{pmatrix} I_p & 0 & 0 \\ 0 & I_m & 0 \\ 0 & I_m & 0 \end{pmatrix}.$$

Reformulation as impulsive linear system

Definition

System $\mathcal{S}' = (A_c, A_s, A_a)$ is globally uniformly exponentially stable (GUES) under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if there exist $C \in \mathbb{R}^+$ and $\lambda \in \mathbb{R}^+$, such that for all $(t_k^s)_{k\in\mathbb{N}}$ and $(t_k^a)_{k\in\mathbb{N}}$ satisfying $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$, the solutions of (4) satisfy:

$$\|x(t)\| \leq Ce^{-\lambda(t-t_0^a)}\|x(t_0^a)\|, \ \forall t \geq t_0^a.$$

Proposition

The following statements are equivalent:

(a) $\mathcal{S} = (A, B, K)$ *is GUES under timing contract* $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$;

(b) $\mathcal{S}' = (A_c, A_s, A_a)$ *is GUES under timing contract* $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$.

Necessary and sufficient stability conditions

Let us consider the set-valued map given fo $\Omega \subseteq \mathbb{R}^n$ by

$$\Phi(\Omega) = \text{Conv}\left(\bigcup_{\tau\in[\underline{\tau},\overline{\tau}]}\left(\bigcup_{w\in[\max(0,\underline{h}-\tau),\overline{h}-\tau]} e^{wA_c}A_a e^{\tau A_c}A_s\Omega\right)\right)$$

If Ω is the set of reachable states at time t_k^s then $\Phi(\Omega)$ is the convex hull of the set of reachable states at time t_{k+1}^s.

Theorem (Al Khatib, Girard & Dang, 2016)

Let $\Omega \subseteq \mathbb{R}^n$ compact with $0 \in Int(\Omega)$, the following are equivalent:

(a) *$\mathcal{S} = (A, B, K)$ is GUES under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$;*

(b) *$\exists \rho \in (0,1)$, $i, j \in \mathbb{N}$, $i < j$, such that $\Phi^j(\Omega) \subseteq \rho\Phi^i(\Omega)$;*

(c) *$\exists \rho \in (0,1)$, $j \in \mathbb{N}^+$, such that $\Phi^j(\Omega) \subseteq \rho Conv\left(\bigcup_{i=0}^{j-1}\Phi^i(\Omega)\right)$.*

Computational issues

- $\Phi(\Omega)$ cannot be computed exactly but needs to be approximated.
- Reachability analysis allows us to compute an accurate inclusion function $\hat{\Phi}$ for Φ satisfying:

$$\forall \Omega \subseteq \mathbb{R}^n, \Phi(\Omega) \subseteq \hat{\Phi}(\Omega).$$

  Moreover, the over-approximation error can be made arbitrarily small.
- Numerous available techniques:

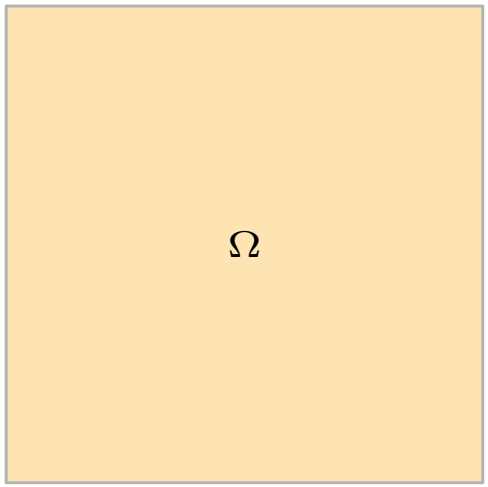
Set representation	References
Polytopes	[Dang et al. 2000, Chutinan & Krogh 1999]
Ellipsoids	[Kurzhanski & Varaiya 2000] [Botchkarev & Tripakis 2000]
Zonotopes	[Girard 2005, Le Guernic et al. 2006] [Althoff et al. 2010]
Support functions	[Le Guernic & Girard 2009, Frehse et al. 2011]

Sufficient stability conditions

Theorem (Al Khatib, Girard & Dang, 2016)

Let $\hat{\Phi}$ an inclusion function for Φ, let $\Omega \subseteq \mathbb{R}^n$ compact with $0 \in Int(\Omega)$, $\mathcal{S} = (A, B, K)$ is GUES under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if

$$\exists \rho \in (0,1),\ i,j \in \mathbb{N},\ i < j,\ \text{such that } \hat{\Phi}^j(\Omega) \subseteq \rho \hat{\Phi}^i(\Omega).$$

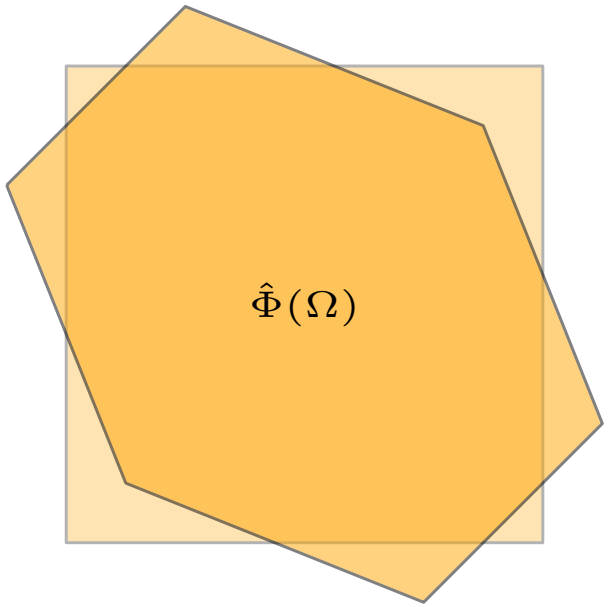


Sufficient stability conditions

Theorem (Al Khatib, Girard & Dang, 2016)

Let $\hat{\Phi}$ an inclusion function for Φ, let $\Omega \subseteq \mathbb{R}^n$ compact with $0 \in Int(\Omega)$, $\mathcal{S} = (A, B, K)$ is GUES under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if

$$\exists \rho \in (0,1),\ i,j \in \mathbb{N},\ i < j,\ \text{such that } \hat{\Phi}^j(\Omega) \subseteq \rho \hat{\Phi}^i(\Omega).$$

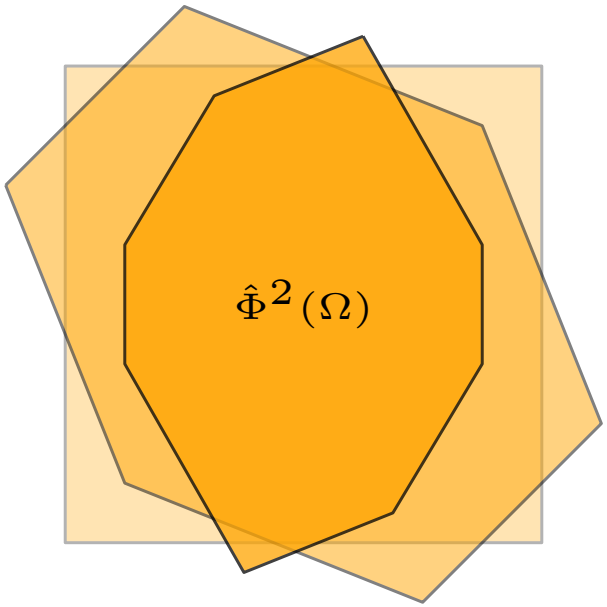


Sufficient stability conditions

Theorem (Al Khatib, Girard & Dang, 2016)

Let $\hat{\Phi}$ an inclusion function for Φ, let $\Omega \subseteq \mathbb{R}^n$ compact with $0 \in Int(\Omega)$, $\mathcal{S} = (A, B, K)$ is GUES under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if

$$\exists \rho \in (0,1),\ i,j \in \mathbb{N},\ i < j,\ \text{such that } \hat{\Phi}^j(\Omega) \subseteq \rho \hat{\Phi}^i(\Omega).$$

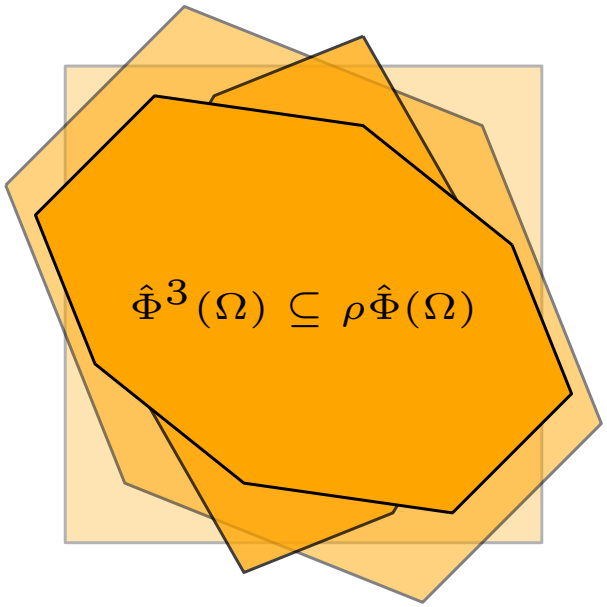


Sufficient stability conditions

Theorem (Al Khatib, Girard & Dang, 2016)

Let $\hat{\Phi}$ an inclusion function for Φ, let $\Omega \subseteq \mathbb{R}^n$ compact with $0 \in Int(\Omega)$, $\mathcal{S} = (A, B, K)$ is GUES under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$ if

$$\exists \rho \in (0,1),\ i,j \in \mathbb{N},\ i < j,\ \text{such that } \hat{\Phi}^j(\Omega) \subseteq \rho \hat{\Phi}^i(\Omega).$$



Numerical experiments

- We consider the systems $\mathcal{S}_1$ and $\mathcal{S}_2$ given by the matrices:

$$A_1 = \begin{pmatrix} 0 & 1 \\ 0 & -0.1 \end{pmatrix}, \; B_1 = \begin{pmatrix} 0 \\ 0.1 \end{pmatrix}, \; K_1 = \begin{pmatrix} -3.75 & -11.5 \end{pmatrix}.$$

$$A_2 = \begin{pmatrix} 0 & 1 \\ -2 & 0.1 \end{pmatrix}, \; B_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; K_2 = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

- Comparison with results obtained by the NCS toolbox (LMI based approaches).

  N. W. Bauer et al., **Networked control systems toolbox: Robust stability analysis made easy**. *IFAC NECSYS*, 2012.

Numerical experiments

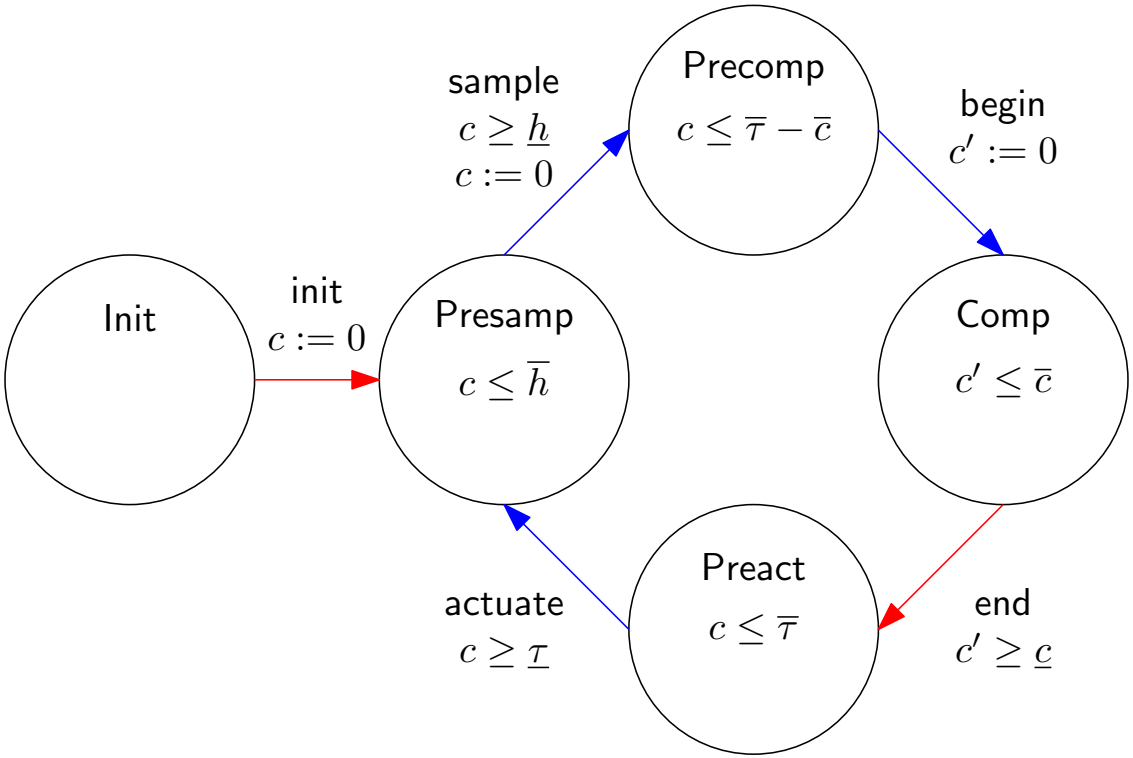
- Our method has been implemented in Matlab using the Multi-Parametric Toolbox.
- Experiments realized on a desktop with i5 4690 processor of frequency 3.5 GHz and a 7.8 GB RAM.

		$\underline{\tau}=0, \underline{h}=\overline{h}=h$			$\underline{\tau}=\overline{\tau}=0$			General contract				
		$\overline{\tau}$	h	T_{CPU}	$\underline{h}$	$\overline{h}$	T_{CPU}	$\underline{\tau}$	$\overline{\tau}$	$\underline{h}$	$\overline{h}$	T_{CPU}
$\mathcal{S}_1$	NCS	0.63	1	3.42	10^{-3}	1.7291	3.30	0	0.4	0.2	1.13	9.17
	Reach (exp1)	0.63	1	0.18	10^{-3}	1.7291	0.20	0	0.4	0.2	1.13	4.49
	Reach (exp2)	0.67	1	1.16	10^{-3}	1.7294	0.20	0	0.4	0.2	1.23	9.95
$\mathcal{S}_2$	NCS	0.78	1	2.07	0.4	0.45	1.91	0	0.1	0.4	0.44	3.62
	Reach (exp1)	0.78	1	0.41	0.4	0.45	0.21	0	0.1	0.4	0.44	1.13
	Reach (exp2)	1	1	2.97	0.4	1.88	1.22	0	0.1	0.4	1.71	5.15

Schedulability Verification

Reformulation as timed game automata

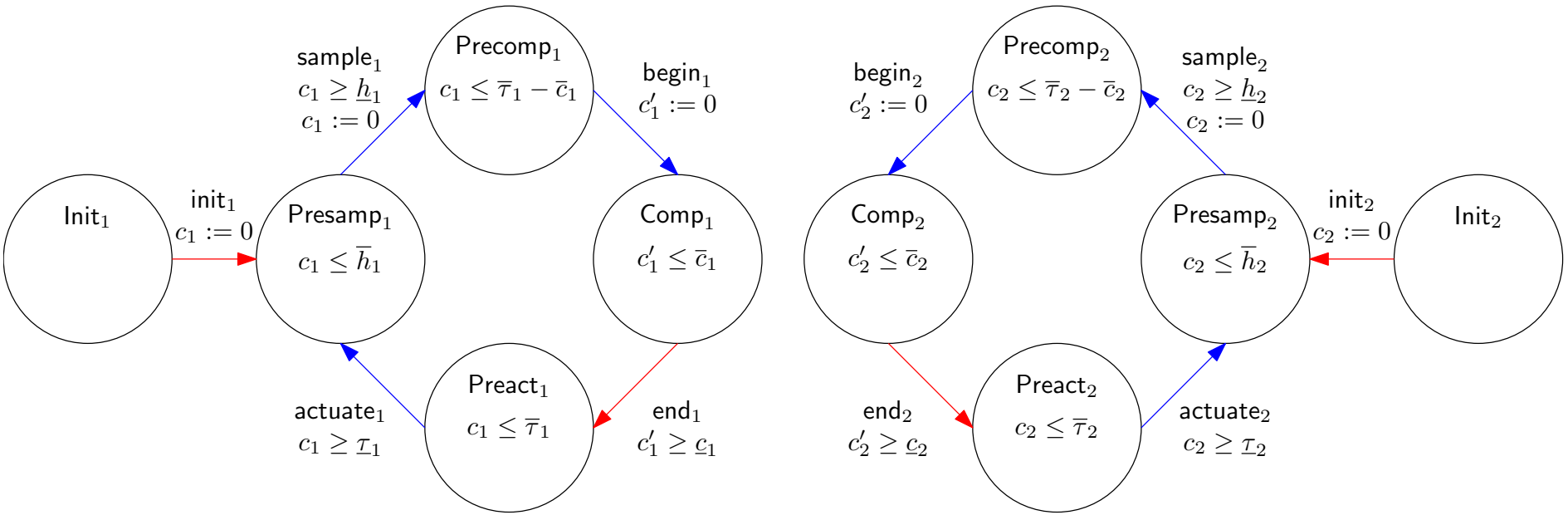
- Timed game automata are timed automata with controllable (by the scheduler) and uncontrollable actions.
- Model of the control task $\mathcal{T} = [\underline{c}, \overline{c}]$ under timing contract $\theta(\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$:



Reformulation as timed game automata

- Concurrent execution of control tasks $\{\mathcal{T}_i\}_{i=1,\dots,N}$ modeled by the network of timed game automata $\mathcal{N}_{TGA}$.
- Conflicting access to the shared computational resource given by the set of locations:

$$L_u = \{(l_1, \dots, l_N) : (l_i = \text{Comp}_i) \wedge (l_{i'} = \text{Comp}_{i'}) \wedge (i \neq i')\}.$$



Scheduling with timed games

Safety game $(\mathcal{N}_{TGA}, L_u)$:

- Synthesize a strategy for triggering controllable actions such that the set of unsafe locations L_u is avoided by all controlled executions of the network of timed game automata $\mathcal{N}_{TGA}$.
- Timed games can be solved using the tool UPPAAL-TIGA:

  G. Behrmann et al., **UPPAAL-TIGA: Time for playing games!** *CAV*, 2007.

Theorem (Al Khatib, Girard & Dang, 2016)

$\{\mathcal{T}_i\}_{i=1...,N}$ is schedulable under timing contracts $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1...,N}$ if there exists a winning strategy for the safety game $(\mathcal{N}_{TGA}, L_u)$.

Numerical experiments

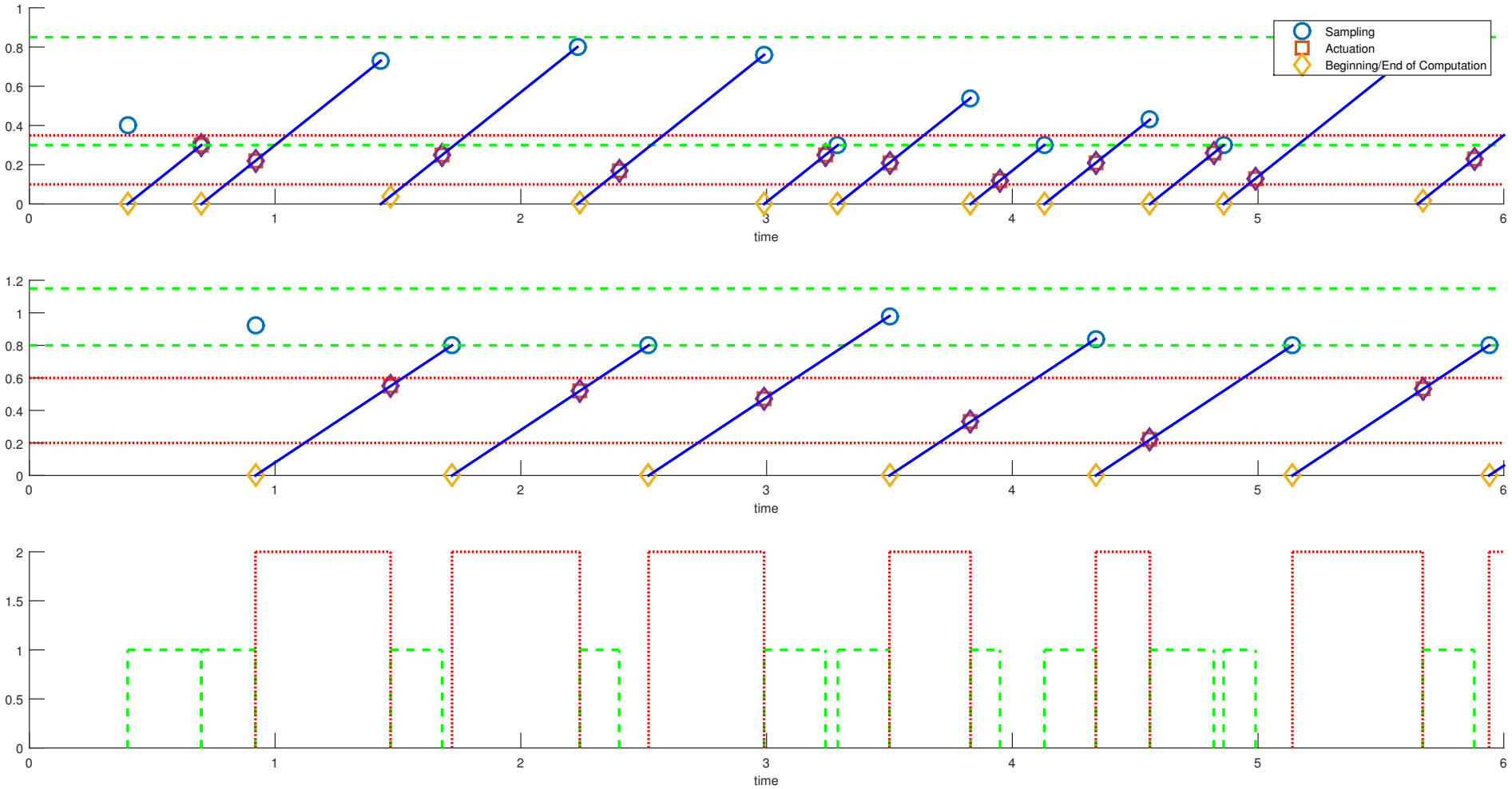
- We consider the systems $\mathcal{S}_1$ and $\mathcal{S}_2$ introduced previously with timing contracts $\{\theta(\underline{\tau}_i, \overline{\tau}_i, \underline{h}_i, \overline{h}_i)\}_{i=1,2}$ where:

$$\begin{array}{llll} \underline{\tau}_1 = 0.1, & \overline{\tau}_1 = 0.35, & \underline{h}_1 = 0.3, & \overline{h}_1 = 0.85 \\ \underline{\tau}_2 = 0.2, & \overline{\tau}_2 = 0.6, & \underline{h}_2 = 0.8, & \overline{h}_2 = 1.15 \end{array}$$

  Both systems are proved to be stable (CPU time: 1.96s, 1.5s).

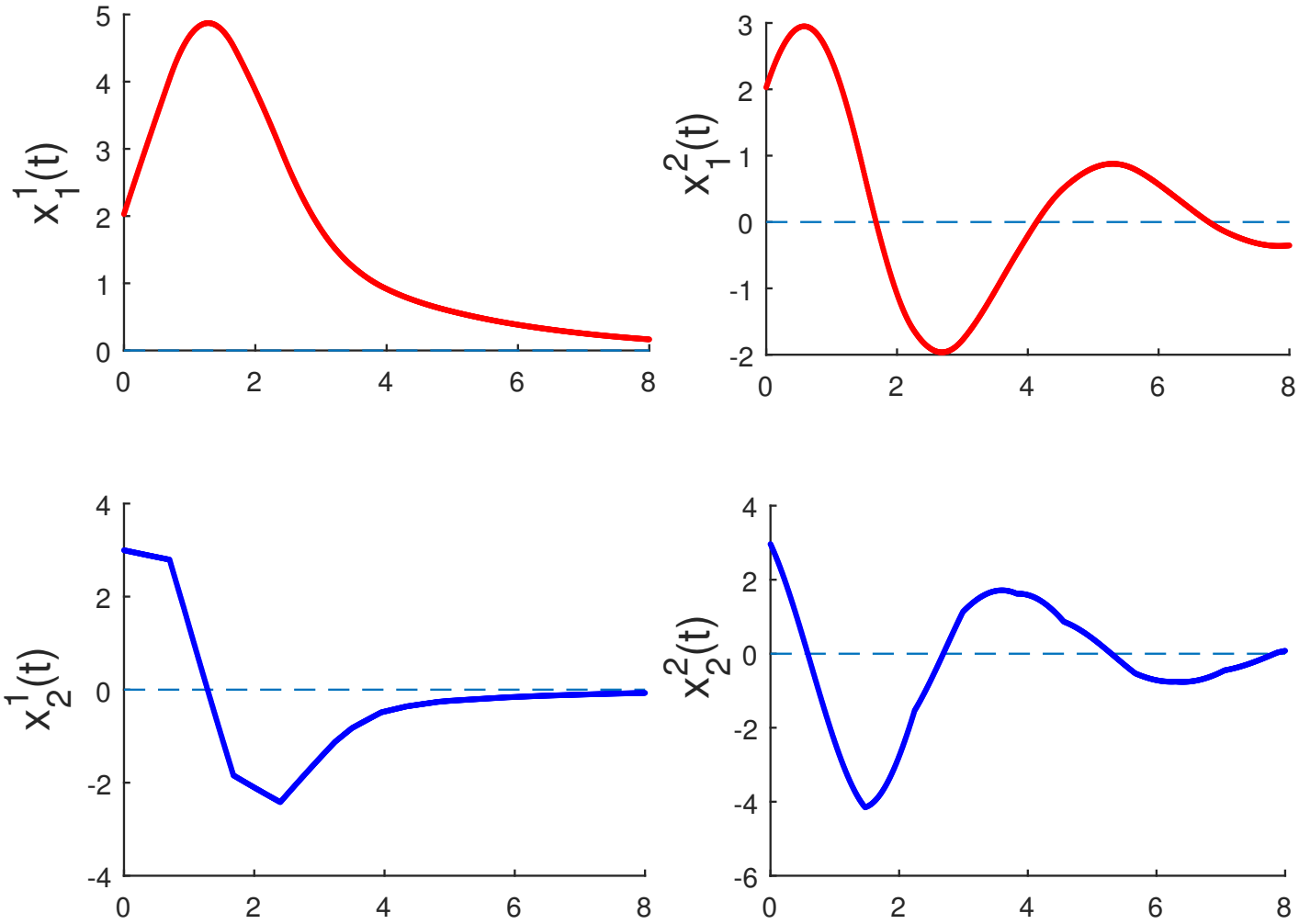
- Associated control tasks $\mathcal{T}_1 = [0.1, 0.3]$, $\mathcal{T}_2 = [0.2, 0.55]$ are proved to be schedulable (CPU time: 1.37s).

Numerical experiments



Timing of events and resource utilization.

Numerical experiments



Associated trajectories of $\mathcal{S}_1$ and $\mathcal{S}_2$.

Contract Synthesis

Partial orders for timing contract parameters

- We define a partial order over the set of contract parameters:

$$\mathcal{C} = \left\{ (\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h}) \in \mathbb{R}_0^+ \times \mathbb{R}_0^+ \times \mathbb{R}^+ \times \mathbb{R}^+ : \underline{\tau} \leq \overline{\tau} \leq \overline{h}, \underline{h} \leq \overline{h} \right\}.$$

- Let $\pi, \pi' \in \mathcal{C}$, with $\pi = (\underline{\tau}, \overline{\tau}, \underline{h}, \overline{h})$, $\pi' = (\underline{\tau}', \overline{\tau}', \underline{h}', \overline{h}')$, then

$$\pi \preceq \pi' \iff \begin{cases} [\underline{\tau}, \overline{\tau}] & \subseteq & [\underline{\tau}', \overline{\tau}'], \\ [\underline{h}, \overline{h}] & \subseteq & [\underline{h}', \overline{h}']. \end{cases}$$

  Intuitively, if $\pi \preceq \pi'$, then timing contract $\theta(\pi')$ is more permissive than $\theta(\pi)$.

- Let $\Pi, \Pi' \in \mathcal{C}^N$, with $\Pi = (\pi_1, \ldots, \pi_N)$, $\Pi' = (\pi'_1, \ldots, \pi'_N)$ then

$$\Pi \preceq \Pi' \iff \left(\forall i = 1, \ldots, N, \ \pi_i \leq \pi'_i \right).$$

Monotonicity of stability and schedulability

Let systems $\{\mathcal{S}_i = (A_i, B_i, K_i)\}_{i=1,\dots,N}$, control tasks $\{\mathcal{T}_i = [\underline{c}_i, \overline{c}_i]\}_{i=1\dots,N}$ and contract parameters $\Pi \in \mathcal{C}^N$, with $\Pi = (\pi_1, \dots, \pi_N)$, we define:

$$\mathrm{Stab}(\mathcal{S}_i, \pi_i)$$
$$\Updownarrow$$
$$[\mathcal{S}_i \text{ is GUES under timing contract } \theta(\pi_i)]\,.$$

$$\mathrm{Sched}(\{\mathcal{T}_i\}_{i=1\dots,N}, \Pi)$$
$$\Updownarrow$$
$$[\{\mathcal{T}_i\}_{i=1\dots,N} \text{ is schedulable under timing contract } \{\theta(\pi_i)\}_{i=1\dots,N}]\,.$$

Monotonicity of stability and schedulability

Proposition (Al Khatib, Girard & Dang, 2016)

Let $\Pi, \Pi' \in \mathcal{C}^N$, *with* $\Pi = (\pi_1, \ldots, \pi_N)$, $\Pi' = (\pi'_1, \ldots, \pi'_N)$, *then the following implications hold:*

- $(\pi_i \preceq \pi'_i) \wedge Stab(\mathcal{S}_i, \pi'_i) \implies Stab(\mathcal{S}_i, \pi_i)$;
- $(\pi_i \preceq \pi'_i) \wedge \neg Stab(\mathcal{S}_i, \pi_i) \implies \neg Stab(\mathcal{S}_i, \pi'_i)$;
- $(\Pi \preceq \Pi') \wedge Sched(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi) \implies Sched(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi')$;
- $(\Pi \preceq \Pi') \wedge \neg Sched(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi') \implies \neg Sched(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi)$.

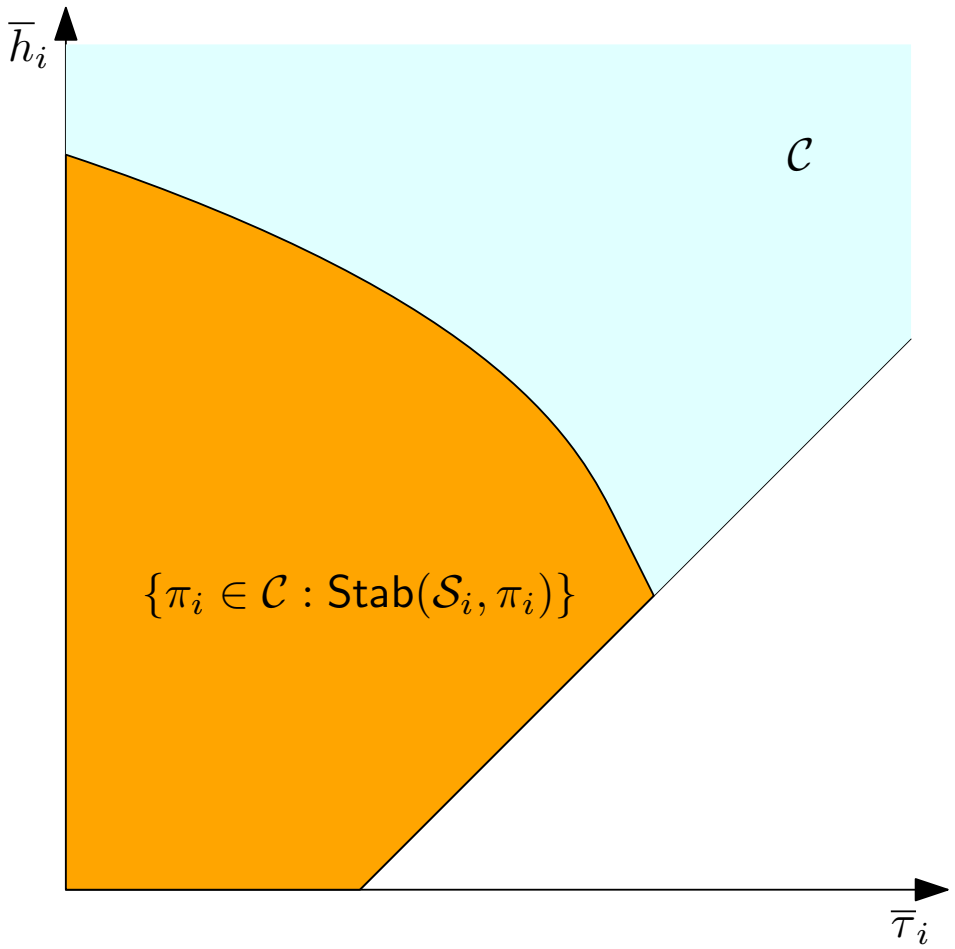
Contract synthesis using sampling-based approximation of monotone sets:

J. Legriel et al., **Approximating the Pareto front of multi-criteria optimization problems**. *TACAS*, 2010.

Contract synthesis – stability

For system $\mathcal{S}_i$, synthesize

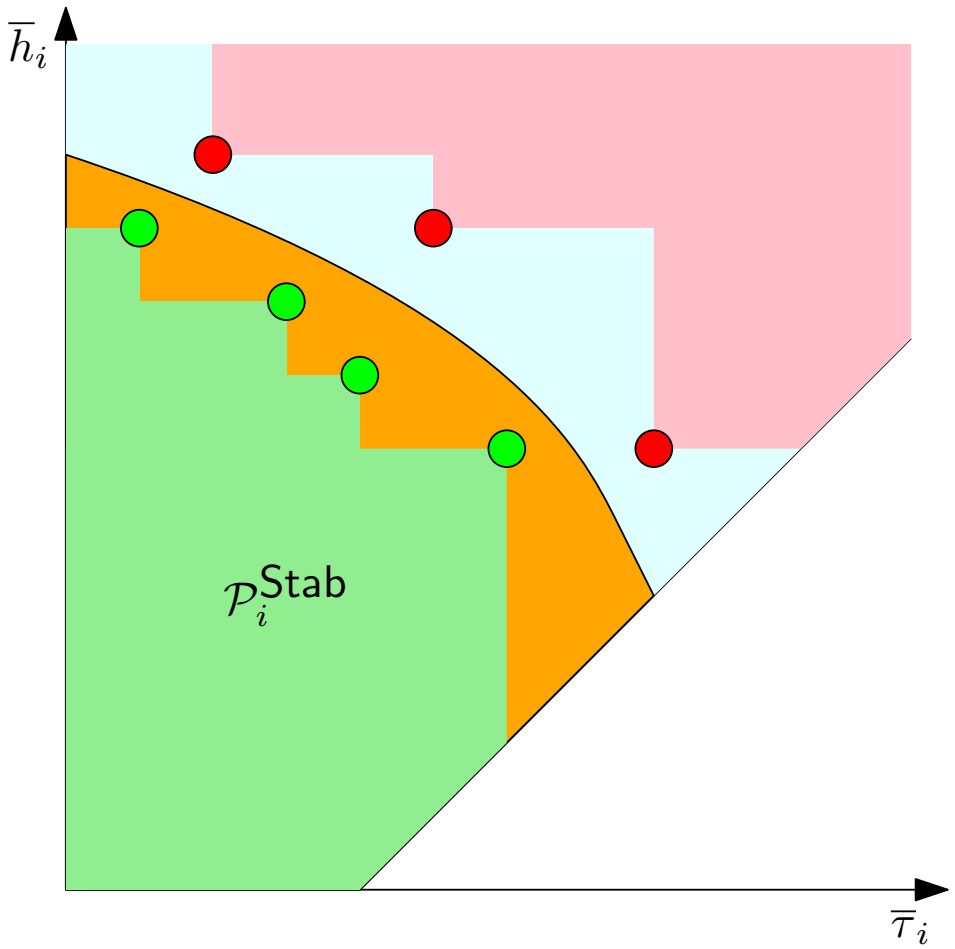
$$\mathcal{P}_i^{\text{stab}} \subseteq \{\pi_i \in \mathcal{C} : \text{Stab}(\mathcal{S}_i, \pi_i)\}$$



Contract synthesis – stability

For system $\mathcal{S}_i$, synthesize

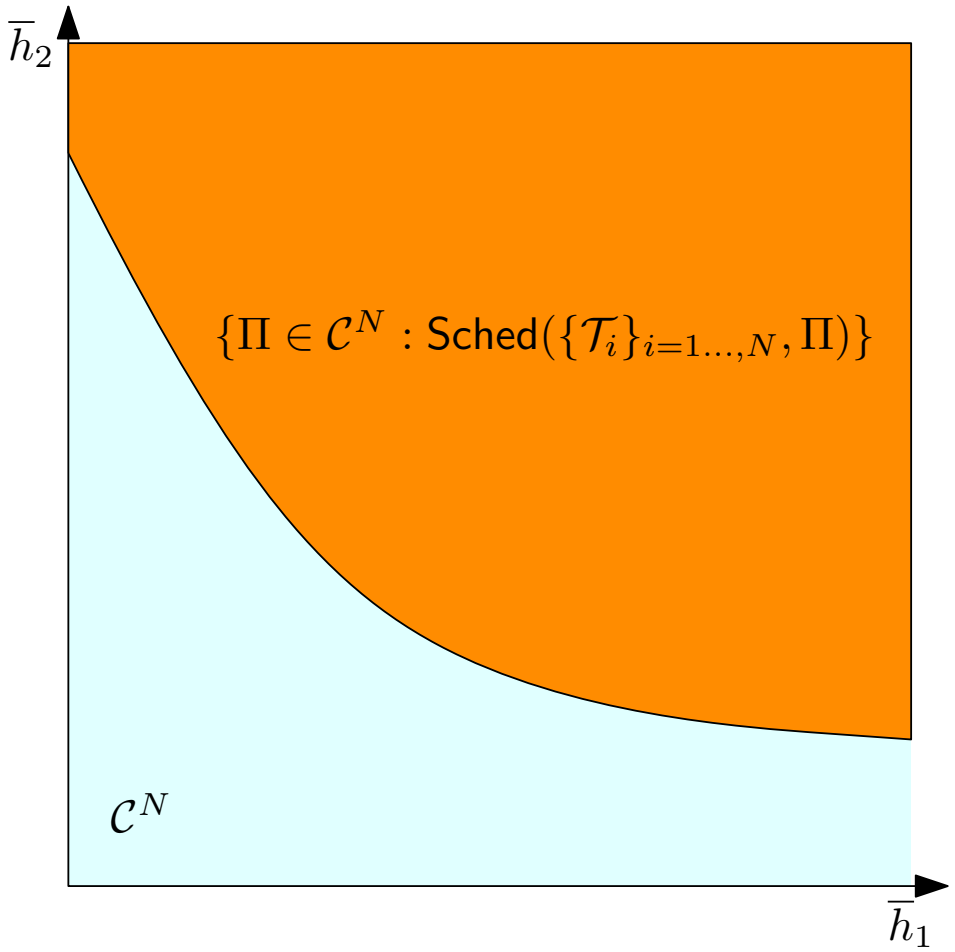
$$\mathcal{P}_i^{\mathsf{stab}} \subseteq \{\pi_i \in \mathcal{C} : \mathsf{Stab}(\mathcal{S}_i, \pi_i)\}$$



Contract synthesis – schedulability

For control tasks $\{\mathcal{T}_i\}_{i=1\ldots,N}$, synthesize

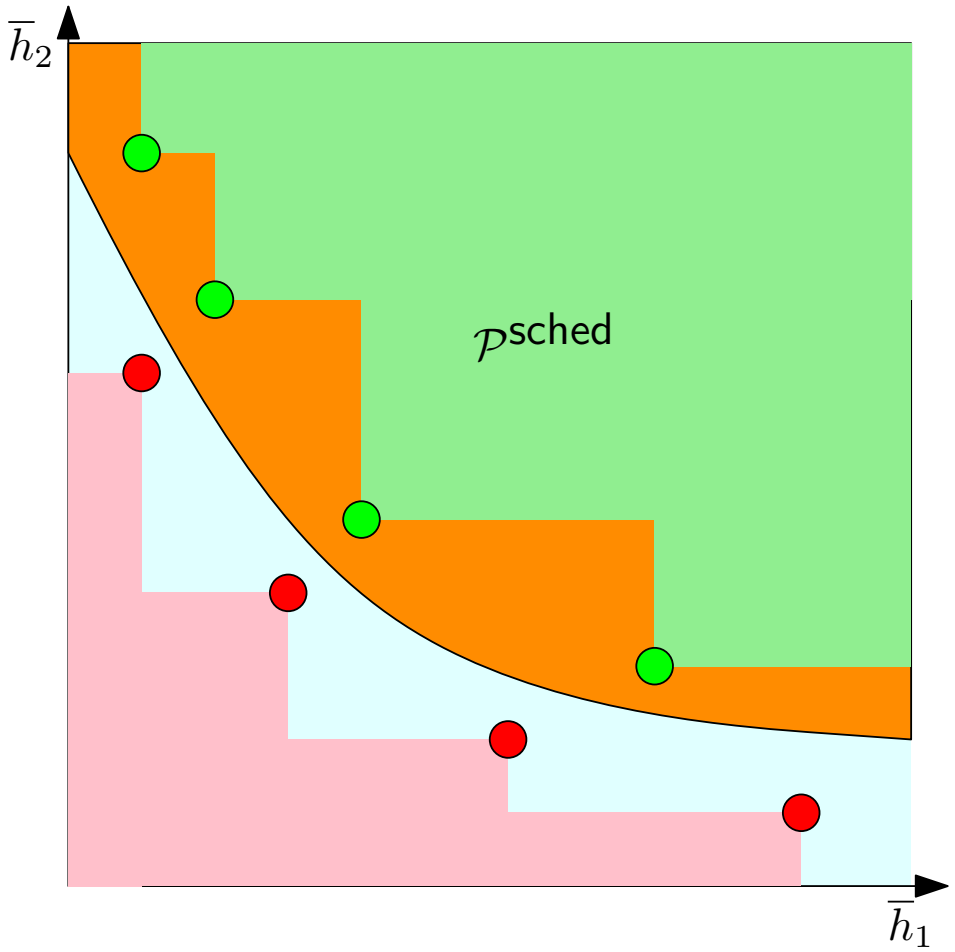
$$\mathcal{P}^{\text{sched}} \subseteq \{\Pi \in \mathcal{C}^N : \text{Sched}(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi)\}.$$



Contract synthesis – schedulability

For control tasks $\{\mathcal{T}_i\}_{i=1\ldots,N}$, synthesize

$$\mathcal{P}^{\text{sched}} \subseteq \{\Pi \in \mathcal{C}^N : \text{Sched}(\{\mathcal{T}_i\}_{i=1\ldots,N}, \Pi)\}.$$



Contract synthesis

Theorem (Al Khatib, Girard & Dang, 2016)

Let us define the set of contract parameters $\mathcal{P}^* \subseteq \mathcal{C}^N$ given by:

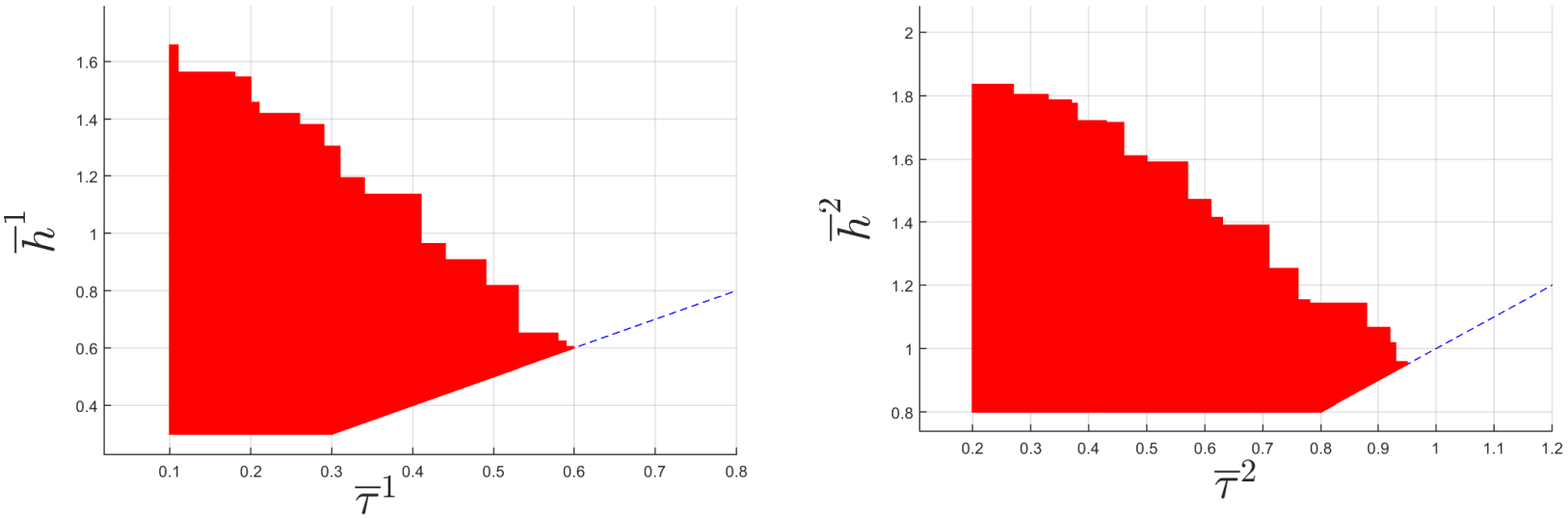
$$\mathcal{P}^* = (\mathcal{P}_1^{stab} \times \cdots \times \mathcal{P}_N^{stab}) \cap \mathcal{P}^{sched}.$$

Then, for all $\Pi = (\pi_1, \ldots, \pi_N) \in \mathcal{P}^*$:

1. *$\mathcal{S}_i$ is GUES under timing contract $\theta(\pi_i)$, for all $i = 1, \ldots, N$;*
2. *$\{\mathcal{T}_i\}_{i=1\ldots,N}$ is schedulable under timing contracts $\{\theta(\pi_i)\}_{i=1\ldots,N}$.*

Numerical experiments – stability

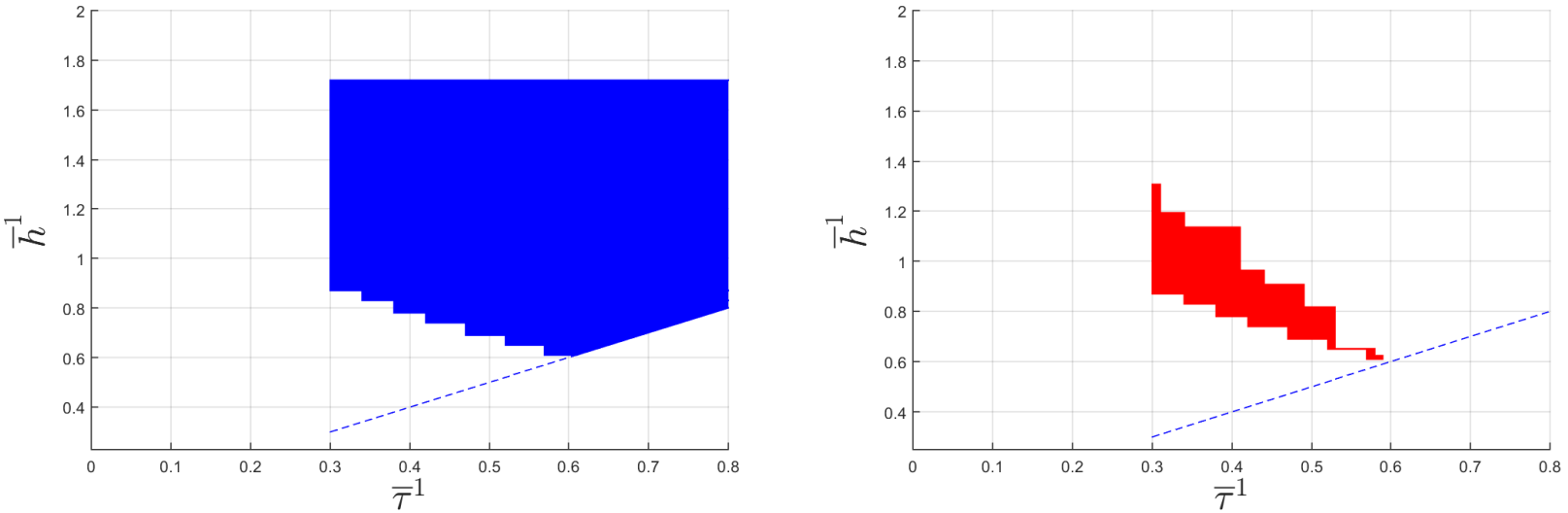
We consider the systems $\mathcal{S}_1$ and $\mathcal{S}_2$ introduced previously and the associated control tasks $\mathcal{T}_1 = [0.1, 0.3]$ and $\mathcal{T}_2 = [0.2, 0.55]$.



Projected stability sets $\mathcal{P}_1^{\text{stab}}$, $\mathcal{P}_2^{\text{stab}}$

Numerical experiments – schedulability

We fix parameters $\underline{\tau}^1 = 0.1$, $\underline{h}^1 = 0.3$, $\underline{\tau}^2 = 0.2$, $\underline{h}^2 = 0.8$.



Schedulability set $\mathcal{P}^{\text{sched}}$ and set $\mathcal{P}^* = (\mathcal{P}_1^{\text{stab}} \times \mathcal{P}_2^{\text{stab}}) \cap \mathcal{P}^{\text{sched}}$

(sections at $\overline{\tau}^2 = 0.6$, $\overline{h}^2 = 1.15$)

Conclusion

- Contract-based design of embedded control systems from multiple viewpoints:
  - Control engineering: stability verification;
  - Software engineering: schedulability verification;
  - Requirement engineering: contract synthesis.
- Algorithmic solution for each problem:
  - Reachability analysis (stability);
  - Timed game automata (scheduling);
  - Sampling-based approximation of monotone sets (contract synthesis).
- Possible extensions:
  - Co-design controller/scheduler/timing contracts (LMI techniques);
  - Scheduling on multicore architectures;
  - More general timing contracts (e.g. missed deadlines).

Postdoctoral Positions

We have openings for two postdoctoral researchers with the project CODECSYS – Contract based design of cyber-physical systems:

- Embedded control under mixed stochastic/deterministic timing uncertainty: a switched system approach
- Parametric contracts for hybrid systems design

Details at `https://sites.google.com/site/antoinesgirard/`