Symbolic Control of Incrementally Stable Systems

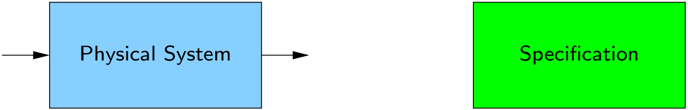
Antoine Girard

Laboratoire Jean Kuntzmann, Université Joseph Fourier
Grenoble, France

Workshop on Formal Verification of Embedded Control Systems
LCCC, Lund, April 17-19 2013

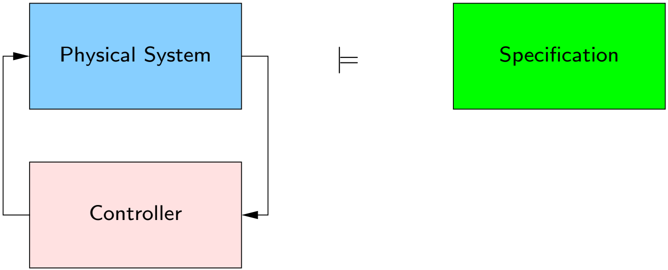
Motivation

Algorithmic synthesis of controllers from high level specifications:



Motivation

Algorithmic synthesis of controllers from high level specifications:



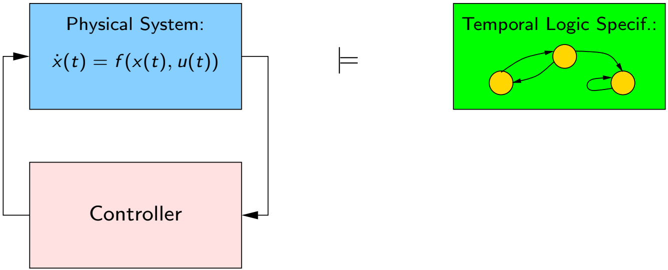
Motivation

- Specifications can be expressed using temporal logic (e.g. LTL):

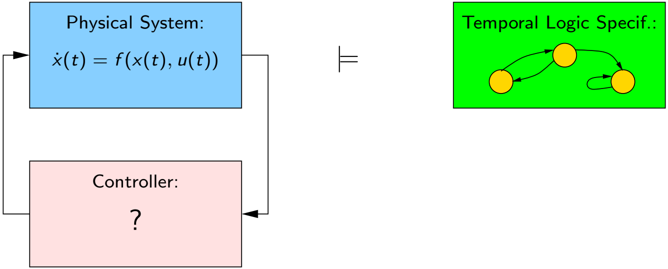
Safety	$\Box S$	(*Always S*)
Reachability	$\Diamond T$	(*Eventually T*)
Stability	$\Diamond(\Box T)$	
Recurrence	$\Box(\Diamond T)$	
Sequencing	$\Diamond(T_1 \wedge \Diamond T_2)$	
Coverage	$\Diamond T_1 \wedge \Diamond T_2$	
Fault recovery	$\Box(F \implies \Diamond R)$	

- LTL formula admits an equivalent (Büchi) automaton.

Algorithmic synthesis of controllers from high level specifications:



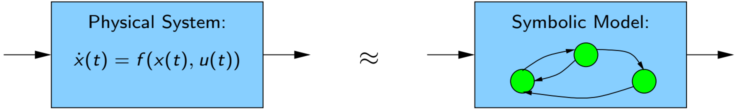
Algorithmic synthesis of controllers from high level specifications:



The problem is hard because the model and the specification are heterogeneous.

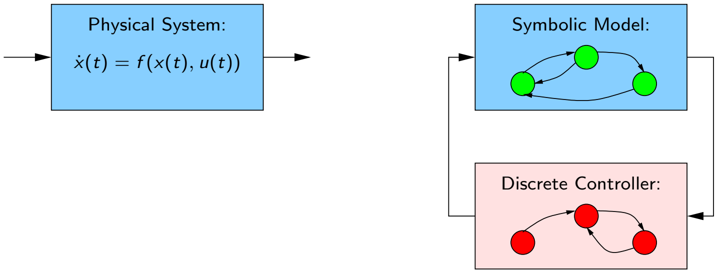
Symbolic Approach to Control Synthesis

Approximate symbolic (*discrete*) model that is "formally related" to the (*continuous*) dynamics of the physical system:



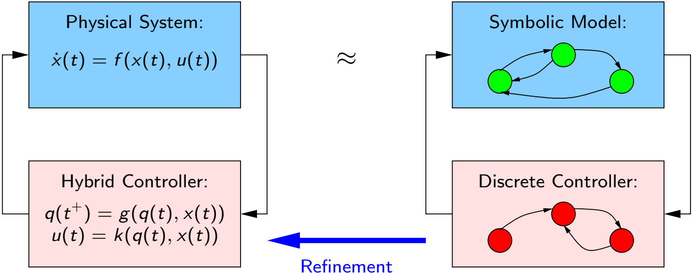
Symbolic Approach to Control Synthesis

Approximate symbolic (*discrete*) model that is "formally related" to the (*continuous*) dynamics of the physical system:



Symbolic Approach to Control Synthesis

Approximate symbolic (*discrete*) model that is "formally related" to the (*continuous*) dynamics of the physical system:



Outline of the Talk

1. Behavioral metrics for discrete and continuous systems
    - Language metric
    - Approximate bisimulation and bisimulation metric
2. Symbolic abstractions of incrementally stable systems
    - Incrementally stable switched systems
    - State-space approaches: from uniform to multi-scale abstractions
    - Input-space approach

Transition Systems

Unified modeling framework of discrete and (sampled) continuous systems.

Definition

A transition system is a tuple $T = (X, U, \delta, Y, H, X^0)$ where

- X is a (discrete or continuous) set of states;
- U is a (discrete or continuous) set of inputs;
- $\delta : X \times U \to 2^X$ is a transition relation;
- Y is a (discrete or continuous) set of outputs;
- $H : X \to Y$ is an ouput map;
- $X^0 \subseteq X$ is a set of initial states.

The transition system is said to be *discrete* or *symbolic* if X and U are countable or finite.

Transition Systems

- A *trajectory* of the transition system T is a finite or infinite sequence:

$$s = (x_0, u_0), (x_1, u_1), (x_2, u_2) \dots$$

where $x_0 \in X^0$ and $x_{k+1} \in \delta(x_k, u_k), \ \forall k$.

- The associated *observed trajectory* is

$$o = (y_0, u_0), (y_1, u_1), (y_2, u_2) \dots \text{ where } y_k = H(x_k), \ \forall k.$$

- The set $L(T)$ of observed trajectories of T is the *language* of transition system T.

Language Metric

- Traditional behavioral relationships for transition systems are based on language inclusion or equivalence.
- For systems observed over metric spaces, the distance between observed trajectories is more natural.
- Let $T_i = (X_i, U, \delta_i, Y, H_i, X_i^0)$, $i \in \{1,2\}$, be transition systems with a common set of inputs U and outputs Y equipped with a metric d. For $o^1 \in L(T_1), o^2 \in L(T_2)$,

$$d(o^1, o^2) = \begin{cases} \sup_k d(y_k^1, y_k^2) & \text{if } u_k^1 = u_k^2,\ \forall k \\ +\infty & \text{otherwise} \end{cases}$$

Language Metric

Definition

The language metric between T_1 and T_2 is given by

$$d_L(T_1, T_2) = \max \left\{ \sup_{o^1 \in L(T_1)} \inf_{o^2 \in L(T_2)} d(o^1, o^2), \sup_{o^2 \in L(T_2)} \inf_{o^1 \in L(T_1)} d(o^1, o^2) \right\}$$

- The language metric is generally hard to compute:
  - The choice of trajectory o^2 approximating o^1 may require knowledge of the whole trajectory o^1.
- Easier if the approximating trajectory can be selected transition after transition:
  - Bisimulation equivalence in the traditional setting.
  - Natural extension given by the bisimulation metric.

Approximate Bisimulation

Definition

Let $\varepsilon \in \mathbb{R}_0^+$, a relation $R \subseteq X_1 \times X_2$ is an *ε-approximate bisimulation relation* if for all $(x_1, x_2) \in R$:

1. $d(H_1(x_1), H_2(x_2)) \leq \varepsilon$;
2. $\forall u \in U$, $\forall x_1' \in \delta_1(x_1, u)$, $\exists x_2' \in \delta_2(x_2, u)$, such that $(x_1', x_2') \in R$;
3. $\forall u \in U$, $\forall x_2' \in \delta_2(x_2, u)$, $\exists x_1' \in \delta_1(x_1, u)$, such that $(x_1', x_2') \in R$.

Definition

T_1 and T_2 are *ε-approximately bisimilar* ($T_1 \sim_\varepsilon T_2$) if :

1. For all $x_1 \in X_1^0$, there exists $x_2 \in X_2^0$, such that $(x_1, x_2) \in R$;
2. For all $x_2 \in X_2^0$, there exists $x_1 \in X_1^0$, such that $(x_1, x_2) \in R$.

Bisimulation Metric

Definition

The bisimulation metric between T_1 and T_2 is given by

$$d_B(T_1, T_2) = \inf \left\{ \varepsilon \in \mathbb{R}_0^+ \mid T_1 \sim_\varepsilon T_2 \right\}$$

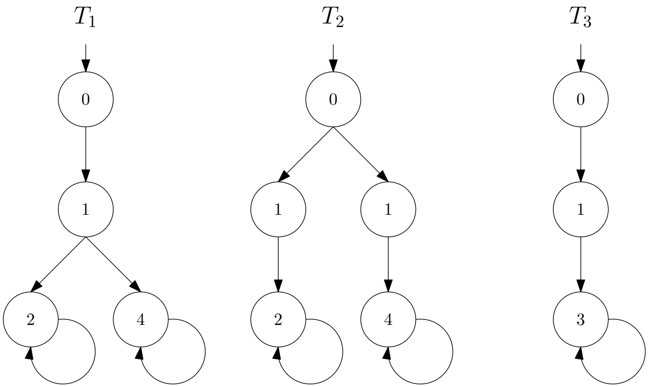
- Fixed-point computation of the bisimulation metric for symbolic systems.
- For other systems, computation of upper-bounds using the notion of *bisimulation functions*.

Theorem

The following inequality holds

$$d_L(T_1, T_2) \leq d_B(T_1, T_2).$$

A Simple Example



$$d_L(T_1, T_2) = 0,\ d_B(T_1, T_2) = 2.$$

$$d_L(T_1, T_3) = 1,\ d_B(T_1, T_3) = 1.$$

Outline of the Talk

1. Behavioral metrics for discrete and continuous systems
   - Language metric
   - Approximate bisimulation and bisimulation metric
2. Symbolic abstractions of incrementally stable systems
   - Incrementally stable switched systems
   - State-space approaches: from uniform to multi-scale abstractions
   - Input-space approach

Switched Systems

Continuous control systems with finite set of inputs:

Definition

A switched system is a tuple $\Sigma = (\mathbb{R}^n, P, \mathcal{F})$ where:

- $\mathbb{R}^n$ is the state space;
- $P = \{1, \dots, m\}$ is the finite set of modes;
- $F = \{f_p : \mathbb{R}^n \to \mathbb{R}^n |\ p \in P\}$ is the collection of vector fields.

For a switching signal $\mathbf{p} : \mathbb{R}^+ \to P$, initial state $x \in \mathbb{R}^n$, $\mathbf{x}(t, x, \mathbf{p})$ denotes the trajectory of Σ given by:

$$\dot{\mathbf{x}}(t) = f_{\mathbf{p}(t)}(\mathbf{x}(t)),\ \mathbf{x}(0) = x.$$

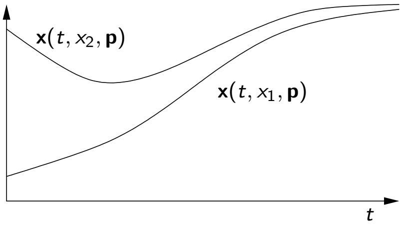
Incremental Stability

Asymptotic forgetfulness of past history:

Definition

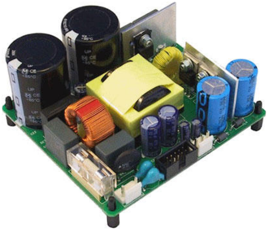
The switched system Σ is *incrementally globally uniformly asymptotically stable* (δ-GUAS) if there exists a $\mathcal{KL}$ function β such that for all initial conditions $x_1, x_2 \in \mathbb{R}^n$, for all switching signals $\mathbf{p} : \mathbb{R}^+ \to P$, for all $t \in \mathbb{R}^+$:

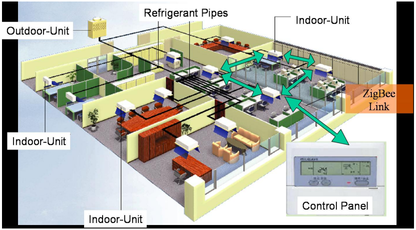
$$\|\mathbf{x}(t, x_1, \mathbf{p}) - \mathbf{x}(t, x_2, \mathbf{p})\| \leq \beta(\|x_1 - x_2\|, t) \to_{t \to +\infty} 0.$$



Examples of incrementally stable systems

- Power converters.
- Thermal dynamics in buildings.
- Road traffic.





Lyapunov Characterization

Definition

$V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ is a *common δ-GUAS Lyapunov function* for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x_1, x_2 \in \mathbb{R}^n$:

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|),$$

$$\forall p \in P,\ \frac{\partial V}{\partial x_1}(x_1, x_2) f_p(x_1) + \frac{\partial V}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V(x_1, x_2).$$

Theorem

If there exists a common δ-GUAS Lyapunov function, then Σ is δ-GUAS.

Lyapunov Characterization

Definition

$V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ is a *common δ-GUAS Lyapunov function* for Σ if there exist $\mathcal{K}_\infty$ functions $\underline{\alpha}$, $\overline{\alpha}$ and $\kappa \in \mathbb{R}^+$ such that for all $x_1, x_2 \in \mathbb{R}^n$:

$$\underline{\alpha}(\|x_1 - x_2\|) \leq V(x_1, x_2) \leq \overline{\alpha}(\|x_1 - x_2\|),$$

$$\forall p \in P,\ \frac{\partial V}{\partial x_1}(x_1, x_2) f_p(x_1) + \frac{\partial V}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V(x_1, x_2).$$

Theorem

If there exists a common δ-GUAS Lyapunov function, then Σ is δ-GUAS.

Supplementary assumption (true if working on a compact subset of $\mathbb{R}^n$):
There exists a $\mathcal{K}_\infty$ function γ such that

$$\forall x_1, x_2, x_3 \in \mathbb{R}^n,\ |V(x_1, x_2) - V(x_1, x_3)| \leq \gamma(\|x_2 - x_3\|).$$

Switched Systems as Transition Systems

- Consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{F})$ and a time sampling parameter $\tau > 0$.
- Let $T_\tau(\Sigma)$ be the transition system where:
  - the set of states is $X = \mathbb{R}^n$;
  - the set of inputs is $U = P$;
  - the transition relation is given by

$$x' \in \delta(x, p) \iff x' = \mathbf{x}(\tau, x, p);$$

  - the set of outputs is $Y = \mathbb{R}^n$;
  - the output map H is the identity map over $\mathbb{R}^n$;
  - the set of initial states is $X^0 = \mathbb{R}^n$.

Computation of the Symbolic Abstraction

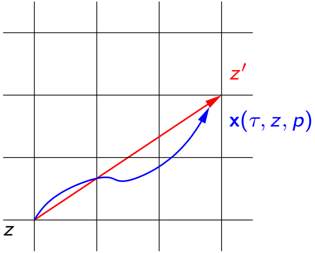
- We start by approximating the set of states $\mathbb{R}^n$ by:

$$[\mathbb{R}^n]_\eta = \left\{ z \in \mathbb{R}^n \;\middle|\; z_i = k_i \frac{2\eta}{\sqrt{n}},\ k_i \in \mathbb{Z},\ i = 1, ..., n \right\},$$

where $\eta > 0$ is a state sampling parameter:

$$\forall x \in \mathbb{R}^n,\ \exists z \in [\mathbb{R}^n]_\eta,\ \|x - z\| \leq \eta.$$

- Approximation of the transition relation = "rounding":



Approximation Theorem

Theorem

Let us assume that there exists $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ *which is a common* δ*-GUAS Lyapunov function for* Σ*. Consider sampling parameters* $\tau, \eta \in \mathbb{R}^+$ *and a desired precision* $\varepsilon \in \mathbb{R}^+$*. If*

$$\eta \leq \min\left\{\gamma^{-1}\left((1 - e^{-\kappa\tau})\underline{\alpha}(\varepsilon)\right), \overline{\alpha}^{-1}\left(\underline{\alpha}(\varepsilon)\right)\right\}$$

then, the relation $R \subseteq \mathbb{R}^n \times [\mathbb{R}^n]_\eta$ *given by*

$$R = \{(x, z) \in \mathbb{R}^n \times [\mathbb{R}^n]_\eta | \; V(x, z) \leq \underline{\alpha}(\varepsilon)\}$$

is an ε*-approximate bisimulation relation and* $T_\tau(\Sigma) \sim_\varepsilon T_{\tau,\eta}(\Sigma)$*.*

Main idea of the proof: show that accumulation of successive "rounding errors" is contained by incremental stability.

Comments on the Approximation Theorem

- Based on sampling (gridding) of time and space: simple to compute.
- For a given time sampling parameter τ, any precision ε can be achieved by choosing appropriately the state sampling parameter η (the smaller τ or ε, the smaller η).
- Uniform time and space discretization: excessive computation time and memory consumption.
- Overcome this problem with multi-scale symbolic abstractions: on-the-fly refinement where fast switching needed, guided by controller synthesis.

Switched Systems in a Multi-Scale Setting

- Consider a switched system $\Sigma = (\mathbb{R}^n, P, \mathcal{F})$, time and scale sampling parameters $\tau > 0$ and $N \in \mathbb{N}$.
- We change the control paradigm: the (aperiodic) controller chooses a mode and a duration during which it will be applied.
- Let $T_\tau^N(\Sigma)$ be the transition system where:
  - the set of states is $X = \mathbb{R}^n$;
  - the set of inputs is $U = P \times \Theta_\tau^N$ where $\Theta_\tau^N = \{2^{-s}\tau \mid s = 0, \dots, N\}$;
  - the transition relation is given by

$$x' \in \delta(x, (p, 2^{-s}\tau)) \iff x' = \mathbf{x}(2^{-s}\tau, x, p);$$

  - the set of outputs is $Y = \mathbb{R}^n$;
  - the output map H is the identity map over $\mathbb{R}^n$;
  - the set of initial states is $X^0 = \mathbb{R}^n$.

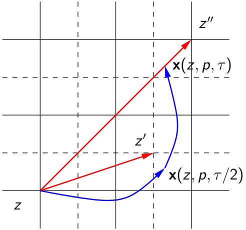
Multi-Scale Symbolic Abstraction

- The set of states $\mathbb{R}^n$ is approximated by a sequence of embedded lattices $Q^0 \subseteq Q^1 \subseteq ... \subseteq Q^N \subseteq \mathbb{R}^n$ with:

$$Q^s = [\mathbb{R}^n]_{2^{-s}\eta} = \left\{ z \in \mathbb{R}^n \;\middle|\; z_i = k_i \frac{2^{-s+1}\eta}{\sqrt{n}},\ k_i \in \mathbb{Z},\ i = 1, ..., n \right\}$$

  where $\eta > 0$ is a state sampling parameter:

- Approximation of the transition relation:



Fine scales reached only by transitions of shorter duration.

Approximation Theorem

Theorem

Let us assume that there exists $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ *which is a common* δ*-GUAS Lyapunov function for* Σ*. Consider sampling and scale parameters* $\tau, \eta \in \mathbb{R}^+$ *,* $N \in \mathbb{N}$ *and a desired precision* $\varepsilon \in \mathbb{R}^+$*. If*

$$\eta \leq \min\left\{\min_{s=0\ldots N}\left[2^s\gamma^{-1}\left((1-e^{-\kappa 2^{-s}\tau})\underline{\alpha}(\varepsilon)\right)\right], \overline{\alpha}^{-1}\left(\underline{\alpha}(\varepsilon)\right)\right\}$$

then, the relation $R \subseteq \mathbb{R}^n \times Q^N$ *given by*

$$R = \left\{(x,z) \in \mathbb{R}^n \times Q^N |\ V(x,z) \leq \underline{\alpha}(\varepsilon)\right\}$$

is an ε*-approximate bisimulation relation and* $T_\tau(\Sigma) \sim_\varepsilon T_{\tau,\eta}(\Sigma)$*.*

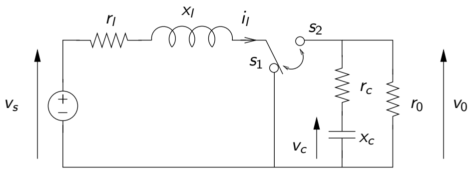
Controller Synthesis using Multi-Scale Abstractions

- Multi-scale abstractions are computed on the fly during controller synthesis using depth first search algorithm:
  - Start from initial states:
    $\rightarrow$ elements of the coarsest lattice.
  - Explore transitions of longer duration first and transitions of shorter duration only if specification cannot be met by transitions of longer durations:
    $\rightarrow$ fine lattices are explored only when necessary.
- For safety specifications: notion of maximal lazy safety controller.
- Tool CoSyMA: Controller Synthesis using Multi-Scale abstractions.
  `multiscale-dcs.gforge.inria.fr`

Example: DC-DC Converter

Power converter with switching control:

- Incrementally stable.
- Safety specification: $[1.15, 1.55] \times [5.45, 5.85]$.

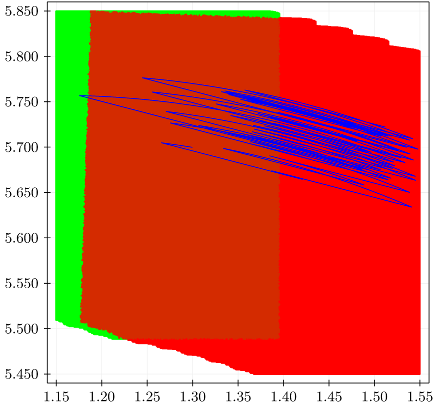


	Uniform abstraction $T_{\tau,\eta}(\Sigma)$ $\tau = 0.5,\ \eta = 0.0003,\ \varepsilon = 0.05$
Time	9.2s
Size (10^3)	936
Cont. ratio	93%

	Multi-scale abstraction $T^N_{\tau,\eta}(\Sigma)$ $N = 6, \tau = 32,\ \eta = 0.018,\ \varepsilon = 0.05$
Time	0.6s
Size (10^3)	6
Durations	4 (33%), 2 (9%), 1 (50%), 0.5 (8%)
Cont. Ratio	92%

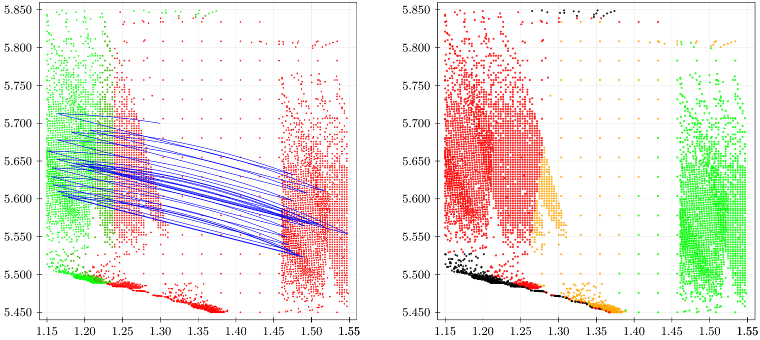
Example: Boost DC-DC Converter

Uniform abstraction $T_{\tau,\eta}(\Sigma)$:



Example: Boost DC-DC Converter

Multiscale abstraction $T^N_{\tau,\eta}(\Sigma)$:

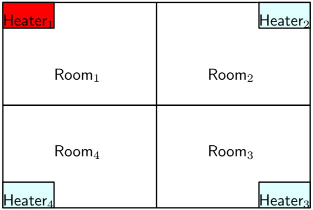


Modes Durations

Example: 4 Room Building

4 dimensional thermal model:

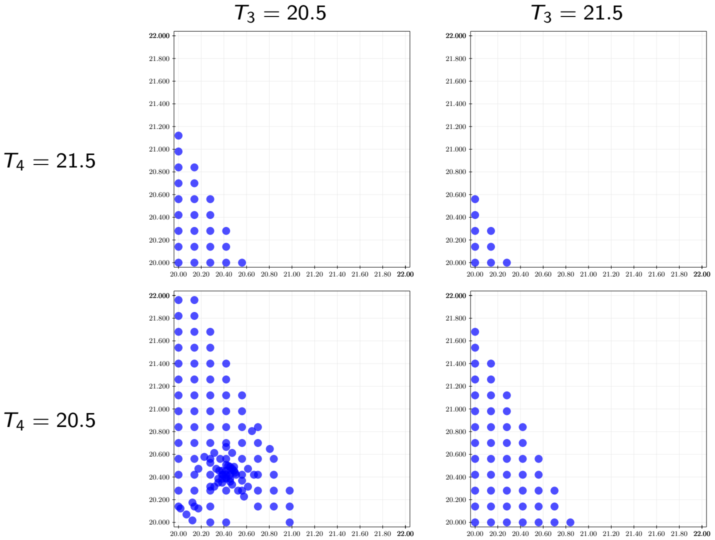
- Incrementally stable.
- At most one heater on at every instant.
- Safety specification: $[20, 22]^4$.



	Multi-scale abstractions $T^N_{\tau,\eta}(\Sigma)$ $N = 4, \tau = 80,\ \eta = 0.14,\ \varepsilon = 0.2$
Time	39s
Size (10^3)	232
Durations	20 (2%), 10 (91%), 5 (7%)
Cont. Ratio	99%

Example: 4 Room Building

Control maps (mode 1):



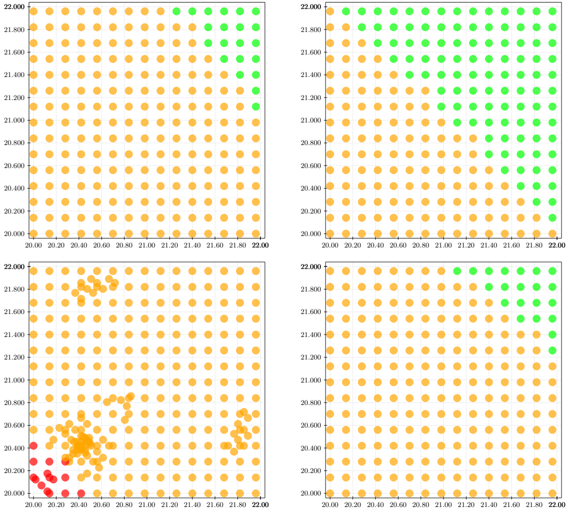
Example: 4 Room Building

Control maps (durations):

$T_3 = 20.5$ | $T_3 = 21.5$

$T_4 = 21.5$

$T_4 = 20.5$



Mode Sequences as Symbolic States

- State-space approaches suffer from the curse of dimensionality.
- Alternative: input-space approach
  - Incremental stability = asymptotic forgetfulness of past history,
  - Use mode sequences of given length N, representing the latest applied modes, as symbolic states of symbolic model $T_{\tau,N}(\Sigma)$,
  - The transition relation is given for $w = p_1 p_2 \ldots p_n$ and $p \in P$ by

$$w' \in \delta(w,p) \iff w' = p_2 \ldots p_n p.$$

  - The output map is defined for $w = p_1 p_2 \ldots p_n$ as

$$H(w) = \mathbf{x}(N\tau, x_s, \mathbf{p}_w) \text{ where } \mathbf{p}_w(t) = p_i,\ \forall t \in [(i-1)\tau, i\tau).$$

  where $x_s \in \mathbb{R}^n$ is a source state.

Approximation Theorem

Theorem

Let us assume that there exists $V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^+$ *which is a common* δ*-GUAS Lyapunov function for* Σ*. Consider time sampling parameter* $\tau \in \mathbb{R}^+$*, sequence length* $N \in \mathbb{N}$ *and a desired precision* $\varepsilon \in \mathbb{R}^+$*. Let*

$$\varepsilon \geq \underline{\alpha}^{-1}\left(\frac{\gamma\left(e^{-N\kappa\tau}\theta(x_s)\right)}{1-e^{-\kappa\tau}}\right)$$

where $\theta(x_s) = \max_{p\in P} V(\mathbf{x}(\tau, x_s, p), x_s)$*. Then, the relation* $R \subseteq \mathbb{R}^n \times P^N$ *given by*

$$R = \left\{(x,w) \in \mathbb{R}^n \times P^N |\ V(x, H(w)) \leq \underline{\alpha}(\varepsilon)\right\}$$

is an ε*-approximate bisimulation relation between* $T_\tau(\Sigma)$ *and* $T_{\tau,\eta}(\Sigma)$*.*

Comments on the Approximation Theorem

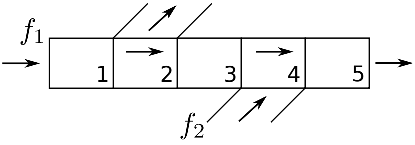
- The source state can be chosen so as to minimize $\theta(x_s)$.
- For a given time sampling parameter τ, any precision ε can be achieved by choosing appropriately the sequence length N.
- Number of symbolic states grows exponentially with the sequence length N.
- Asymptotic estimates show that for a given precision ε, the input-space approach leads to a smaller number of symbolic states than the (uniform) state-space approach as soon as

$$\ln(|P|) \leq \kappa \tau n.$$

Example: Road Traffic

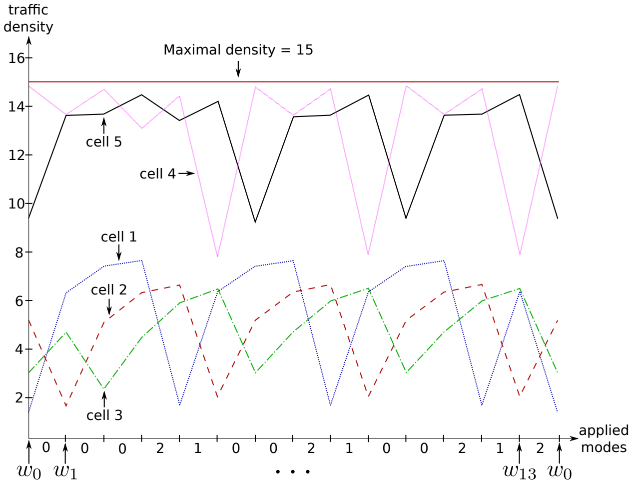
5 dimensional model:

- Incrementally stable.
- At least one green light.
- Safety specification: $[0, 15]^5$.
- Fairness constraint: red light no longer than 3 time units.



Sequence length N	10	12	14
Size (10^3)	59	531	4783
Precision ε	0.1	0.01	0.001

Periodic schedule for light coordination:



Conclusions

- Approximately bisimilar symbolic abstractions:
  - A rigorous tool for controller synthesis:
    Synthesized controllers are "correct by design".
  - Allow us to leverage efficient algorithmic techniques from discrete systems to continuous and hybrid systems.
  - Computable for interesting classes of systems: switched systems, continuous control systems...
  - Several approaches can help to reduce the computation burden.
- Ongoing and future work:
  - Tool CoSyMA: Controller Synthesis using Multi-scale Abstractions.
  - Multi-scale input-space approaches.
  - Symbolic models for infinite dimensional systems.

References

- Behavioral metrics for discrete and continuous systems:
  - G. and Pappas, Approximation metrics for discrete and continuous systems. IEEE TAC, 2007.
- Symbolic abstractions of incrementally stable systems:
  - Pola, G. and Tabuada, Approximately bisimilar symbolic models for nonlinear control systems. Automatica, 2008.
  - G., Pola and Tabuada, Approximately bisimilar symbolic models for incrementally stable switched systems. IEEE TAC, 2010.
  - Camara, G. and Goessler, Safety controller synthesis for switched systems using multi-scale symbolic models. CDC, 2011.
  - Mouelhi, G. and Goessler, CoSyMA: a tool for controller synthesis using multi-scale abstractions. HSCC, 2013.
  - Le Corronc, G. and Goessler, Mode sequences as symbolic states in abstractions of incrementally stable switched systems. Submitted.