1st French Singaporean Workshop on Formal Methods and Applications

Control of Sampled Switched Systems using Invariance Analysis

Laurent FRIBOURG
LSV - ENS Cachan & CNRS

Plan

Sampled Switched Systems

Sampled Switched Systems

A switched system $\dot{x} = f_\sigma(x)$ is a family of continuous-time dynamical systems witth a rule that determines at each time which one is active

- state $x \in \mathbb{R}^n$
- mode : $p \in \mathcal{P}$ with $\{\dot{x} = f_p(x),\ p \in \mathcal{P}\}$
- switching signal $\sigma : [0, \infty) \to \mathcal{P}$

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

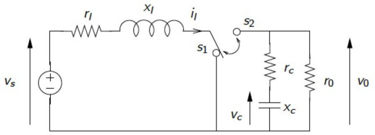
Control Problem

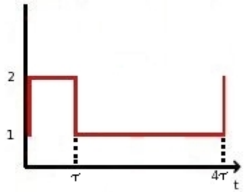
We consider the state-dependent control problem :

Find σ, i.e., the appropriate switched mode p every τ according to the current value of x, in order to achieve some goals (stability, safety,...)

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

Example : DC-DC Converter

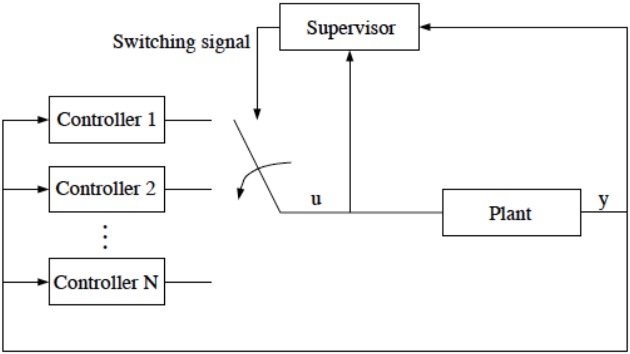




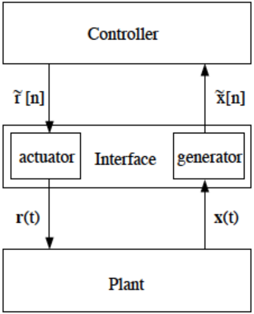
- Modes : $p = 1, 2$; sampling period τ
- A pattern π is a finite sequence of modes (e.g. $(2 \cdot 1 \cdot 1 \cdot 1)$)
- A state dependent control consists to select at each τ a mode (or a pattern) according to the current value of the state.

NB : widespread in portable electronic devices (phones, laptops) supplied with batteries, which contain sub-circuits, each with its own voltage level requirement $\neq$ from that supplied by the battery

Controlled Switched Systems : Schematic View



Digital Control/Plant As a Sampled Switched Syst



- If the digital control signal takes its values on a finite domain (quantization), then control/plant is a sampled switched system !
- Classical stabilisation become impossible (Brockett 1983) $\rightsquigarrow$ objective of practical stability

Safety and Stability Properties for the DC-DC Converter

- Example of safety property to be checked : no saturation

$$\forall t \geq 0 : \qquad i_l(t) \leq M$$

- Example of stability property to be checked : voltage regulation

$$v_{output}(t) - v_{reference} \leq \varepsilon \text{ as } t \to \infty$$

Affine Sampled Switched Systems

- Instead of considering all the continuous evolution, one observes the system only at periodic switching instants at times : τ, 2τ, ...
- An affine sampled switched system is of the form $\{\dot{x} = A_p x + b_p\}_{p \in P}$ with $A_p \in \mathbb{R}^{n \times n}$ and $b_p \in \mathbb{R}$
- Between two sampling times $i\tau$ and $(i+1)\tau$, the system is governed by a differential affine equation of the form $\dot{x}(t) = A_p x(t) + b_p$.

Affine Sampled Switched Systems (cont'd)

- We use $\mathbf{x}(t, x, p)$ to denote the point reached at time t under mode p from initial condition x. This defines a transition relation $\rightarrow_\tau^p$:

$$x \rightarrow_\tau^p x' \text{ iff } \mathbf{x}(\tau, x, p) = x'$$

- A sampled switched system can thus be viewed as a piecewise affine discrete-time system, since :

$$\mathbf{x}(\tau, x, p) = C_p x + d_p$$

with $C_p = e^{A_p \tau}$

Post Set Operators

- $Post_p(X) = \{x' \mid x \rightarrow^p_\tau x' \text{ for some } x \in X\}$
- $Post_\pi(X) = \{x' \mid x \rightarrow^{p_1}_\tau \cdots \rightarrow^{p_m}_\tau x' \text{ for some } x \in X\}$
  if π is a pattern of the form $(p_1 \cdots p_m)$
- The unfolding of $Post_\pi(X)$ is the union of X, $Post_\pi(X)$ and the intermediate sets :

$$X \cup Post_{p_1}(X) \cup Post_{p_1 \cdot p_2}(X) \cup \cdots \cup Post_{p_1 \cdots p_{m-1}}(X) \cup Post_\pi(X)$$

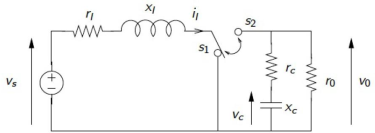
Dynamics of the DC-DC Converter

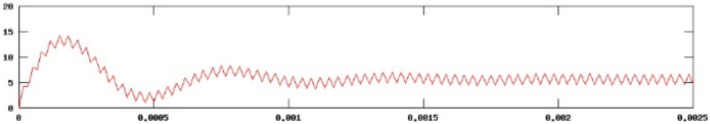
- The state x is (i_l, v_c).
- The dynamics associated with mode p $(p = 1, 2)$ is of the form $\dot{x}(t) = A_p x(t) + b_p$ with

$$A_1 = \begin{pmatrix} -\frac{r_l}{x_l} & 0 \\ 0 & -\frac{1}{x_c}\frac{1}{r_0+r_c} \end{pmatrix} \quad b_1 = \begin{pmatrix} \frac{v_s}{x_l} \\ 0 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} -\frac{1}{x_l}(r_l + \frac{r_0.r_c}{r_0+r_c}) & -\frac{1}{x_l}\frac{r_0}{r_0+r_c} \\ \frac{1}{x_c}\frac{r_0}{r_0+r_c} & -\frac{1}{x_c}\frac{1}{r_0+r_c} \end{pmatrix} \quad b_2 = \begin{pmatrix} \frac{v_s}{x_l} \\ 0 \end{pmatrix}$$

Control Objectives (DC-DC Converter Example)





- 1st objective (stability) : output voltage regulation of a constant desired reference
- 2nd objective (safety) : while maintaining some constraints of current limitation and/or maximal current and voltage ripple

Visualization of Safety Controlled Trajectories

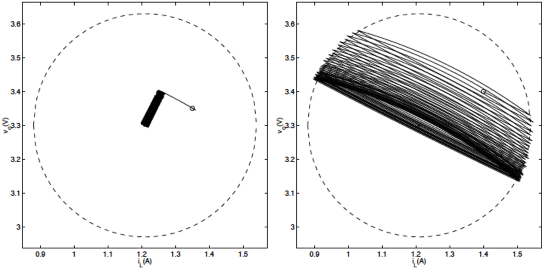
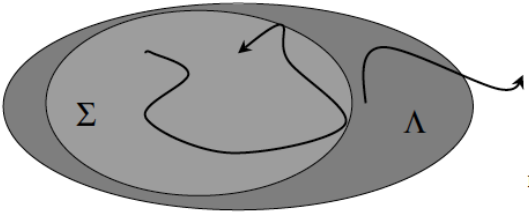


FIGURE: State trajectories of the DC-DC converter using a minimum ripple controller (left) and the minimum switching controller (right). The dashed line represents the boundary of the safe set

Safety Controllers via Invariant Synthesis



<u>Problem</u> : Given a set Λ, find a controlled invariant subset $\Sigma \subseteq \Lambda$ $(x(0) \in \Sigma \;\Rightarrow\; x(t) \in \Sigma$ for all $t \geq 0$ for some control rule)

If Λ represents the safe set, then every controlled trajectory starting in Σ is guaranteed to remain in the safety set ($\rightsquigarrow$ safety control).

Computation of the Maximal Invariant Subset

- Ramadge-Wonham's Algorithm :

  initialization : $W^0 = \emptyset, W^1 = \Lambda, i = 1$
  while $W^i \neq W^{i-1}$ do
  $\quad W^{i+1} = W^i \cap Pre(W^i)$
  $\quad i = i + 1$
  end while

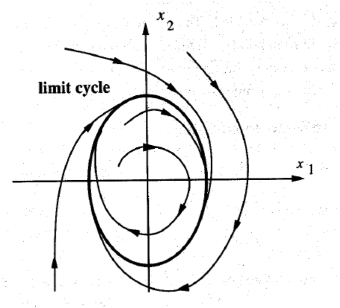
  where $Pre(W)$ is set of predecessors : $\{q \mid \exists q' \in W : \ q \ \rightarrow q'\}$

- When process terminates, $W^i = W^{i+1} =$ max. inv. subset of Λ
- Always terminates when the transition system is finite

Problem : How to exploit the algorithm for switched systems ?

Stability Controllers

- In switched systems, there is generally no equilibrium point. Stability can be ensured only in the neighborhood of a reference point (practical stability).
- Actually, there are often phenomena of convergence to limit cycles.



Problem : characterize position of limit cycle, basin of attraction.

Average Model

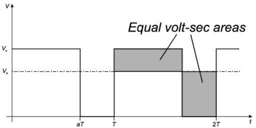
DC-DC Converter : Average Model

- $p = 1$: inductor stores energy
- $p = 2$: impedance higher, current $\searrow$, capacitor charge $\nearrow$
- if switching fast enough, inductor current always > 0, energy accumulated in inductor transferred to capacitor

Let D duty cycle (% time mode $p = 1$ is active)

- When $p = 1$, $\Delta I_1 = \frac{1}{L}\int_0^{DT} V_i dt = \frac{DT}{L} V_i$
- when $p = 2$, $\Delta I_2 = \int_{DT}^{T} \frac{(V_i - V_o)dt}{L} = \frac{(V_i - V_0)(1-D)T}{L}$
- $\Delta I_1 + \Delta I_2 = 0 \Rightarrow$

$$D = 1 - \frac{V_i}{V_o}$$



Rough and Partial Information

- Ignores the order and number of individual switchings during a cycle period, but takes only into account the average time one mode p is active.
- Considers only the permanent regime
- Gives a fictitious "average" equilibrium point

Still gives some basic information to the engineer on how to adjust the duty cycle

Approximate Bisimulation Method

Lyapunov Stabilities for Classical Systems

The system $\dot{x} = f(x)$ (with $f(O) = O$) is

- Lyapunov stable (LS) if
  $\forall \varepsilon > 0\ \exists \delta > 0\ |x(0)| < \delta \ \Rightarrow\ |x(t)| < \varepsilon$.
- asymptotically stable (AS) if it is LS and
  $\exists \delta > 0\ |x(0)| < \delta \ \Rightarrow\ \lim_{t\to\infty} |x(t)| = 0$.
- globally asymptotically stable (GAS) if it is LS and
  $x(0) \in \mathbb{R}^n \ \Rightarrow\ \lim_{t\to\infty} |x(t)| = 0$.
- incrementally globally asymptotically stable (δ-GAS) if
  $|\mathbf{x}(t, x_0) - \mathbf{x}(t, y_0)| \leq \beta(|x_0 - y_0|, t)$ for some $\mathcal{KL}$ function β

LS means that trajs starting close enough to O remain close enough.
AS means that trajs starting close enough eventually converge to O.
GAS means that every traj converges to O as $t \to \infty$.
δ-GAS means that all the traj. converge to the same reference traj. independently of their initial conditions.

Lyapunov Theorems for Classical Systems

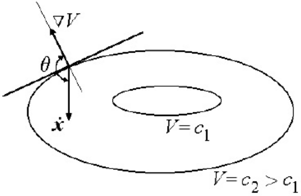
V is a Lyapunov candidate fn if it is *(locally) positive-definite*, i.e. : $V(x) > 0$ for all x (in some neighborhood of O) and $V(O) = 0$.

Theorem : Given a L. candidate fn V, the system is

- LS if $\dot{V}$ is locally negative *semi*-definite ($\dot{V}(x) \leq 0$).
- AS if $\dot{V}$ is *locally* negative definite ($\dot{V}(x) < 0$).
- GAS if $\dot{V}$ is *globally* negative definite ($\dot{V}(x) < 0$ if $x \neq O$), and V radially unbounded ($V(x) \to \infty$ as $|x| \to \infty$).
- δ-GAS if $\exists$ V s.t. $\dot{V}(x, x') \leq -\alpha V(x, x')$ if $x \neq x'$, and V radially unbounded.

Geometric Interpretation

$$\dot{V}(x) = \frac{\partial V}{\partial x}\dot{x} = |\frac{\partial V}{\partial x}|\ |f(x)|\ cos\theta < 0$$

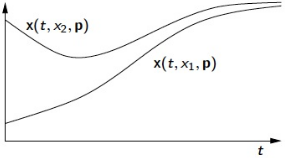


The trajectory is moving in the direction of decreasing V

NB : The set $\{x \in \mathbb{R}^n \,|V(x) \leq c\}$ is an invariant set, for each $c > 0$

δ-GUAS Stability for Switched Systems

The system $\dot{x} = f_\sigma(x)$ is incr. glob. unif. as. stable (δ-GUAS) if $\exists \beta \in \mathcal{KL}$ s.t. for all x_1, x_2, σ, t :
$|\mathbf{x}(t, x_1, \sigma) - \mathbf{x}(t, x_2, \sigma)| \leq \beta(|x_1 - x_2|, t) \rightarrow_{t\rightarrow\infty} 0$



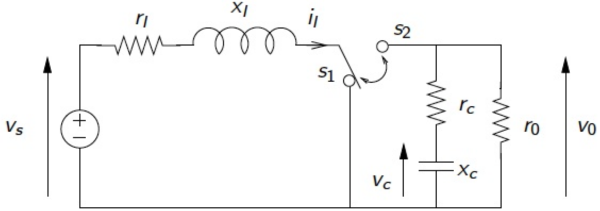
All traj. of Σ_p conv. to the same ref. traj. independently init. cond.

Theorem : $\dot{x} = f_\sigma(x)$ is δ-GUAS if $\exists\ V : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ s.t. :

- $\underline{\alpha}(|x_1 - x_2|) \leq V(x_1, x_2) \leq \overline{\alpha}(|x_1 - x_2|)$
- $\forall p, \frac{\partial V}{\partial x_1}(x_1, x_2) f_p(x_1) + \frac{\partial V}{\partial x_2}(x_1, x_2) f_p(x_2) \leq -\kappa V(x_1, x_2)$

Ex : Incremental Stability of DC-DC Converter

- Power converter with switching control:



- State variable: $x(t) = [i_l(t), v_c(t)]^T$.
- System dynamics: $\dot{x}(t) = A_p x(t) + b, \; p \in \{1, 2\}$.
- Common δ-GUAS Lyapunov function of the form:

$$V(x, y) = \sqrt{(x - y)^T M(x - y)}.$$

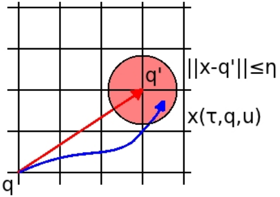
where M is positive definite symmetric ($\Rightarrow$ incremental stability)

Abstraction Σ_η of Σ [Girard-Pola-Tabuada]

The dense state space $\mathbb{R}^n$ is approximated by the lattice

$$[\mathbb{R}^n]_\eta = \{q \in \mathbb{R}^n \mid q_i = k_i \frac{2\eta}{\sqrt{n}},\ k_i \in \mathbb{Z},\ i = 1, \ldots, n\}$$

where $\eta > 0$ is a state space discretization parameter



$$\forall x \in \mathbb{R}^n\ \exists q' \in [\mathbb{R}^n]_\eta \quad |\mathbf{x}(\tau, q, u) - q'| \leq \eta$$

Definition of $\rightarrow_{\Sigma_\eta}$:

$$q \rightarrow_{\Sigma_\eta} q' \quad \text{iff} \quad \|\mathbf{x}(\tau, q, u) - q'\| \leq \eta$$

ε-Bisimilarity of Σ and Σ_η

Σ and Σ_η are ε-bisimilar if :

1. $|q_1 - x_1| \leq \varepsilon \wedge x_1 \rightarrow_\Sigma x_2 \Rightarrow \exists q_2 \; q_1 \rightarrow_{\Sigma_\eta} q_2 \wedge |q_2 - x_2| \leq \varepsilon$
2. $|q_1 - x_1| \leq \varepsilon \wedge q_1 \rightarrow_{\Sigma_\eta} q_2 \Rightarrow \exists x_2 \; x_1 \rightarrow_\Sigma x_2 \wedge |q_2 - x_2| \leq \varepsilon$

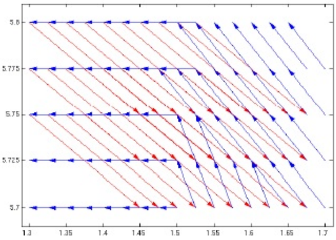
Theorem : If Σ is δ-GUAS (incrementally stable), then, for all ε there exists η such that Σ and Σ_η are ε-bisimular.

Hint : Accumulation of successive "rounding errors" is contained by the incremental stability property.

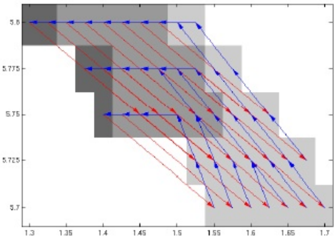
Application : In order to find a safety controller of Σ, find a safety controller of the finite transition system Σ_η (Ramadge-Wonham), then infer a safety controller of Σ (up to ε).

Safety Control via ε-bisimulation

1st model : $\tau = 0.5, \eta = \frac{1}{40\sqrt{2}}, \varepsilon = 2.6$



Symbolic model

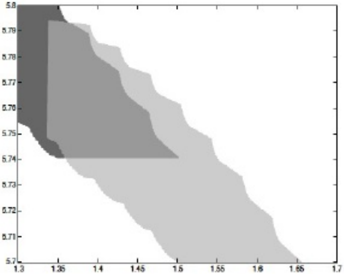


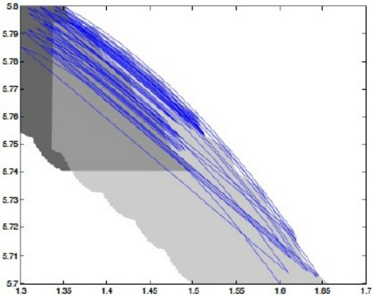
Supervisory controller

Each symbolic state corresponds to an aggregate of real states

Control of symbolic model

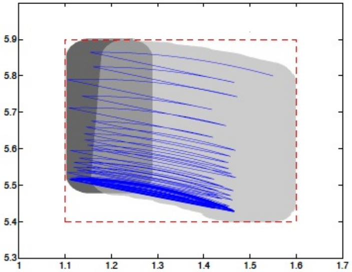
Second model : $\tau = 0.5, \eta = \frac{1}{4000\sqrt{2}}, \varepsilon = 0.026$ (642001 states !)



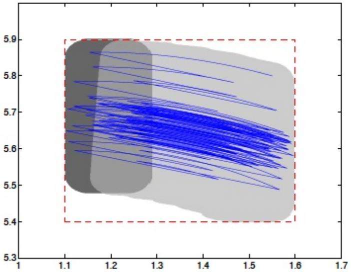


Safety Control of the DC-DC Converter

Using two possible implementations:



Lazy control



Stochastic control

Both implementations satisfy the safety specification.

NB : Limit cycle apparent !

ε-Abstraction of Sampled Switched Systems

- Simple to compute (based on a gridding of space).
- Any precision ε can be achieved by choosing appropriately the state sampling parameter η

but

1. For a good precision ε, huge number of points
2. Regions of uniform control are known *a posteriori*
3. No explanation of limit cycles

State Decomposition Method :

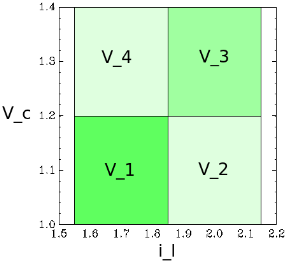
- alternative approach in order to identify *a priori* regions of uniform control as large as possible.
- $\rightsquigarrow$ simple explanation of limit cycles as minimal invariant subsets

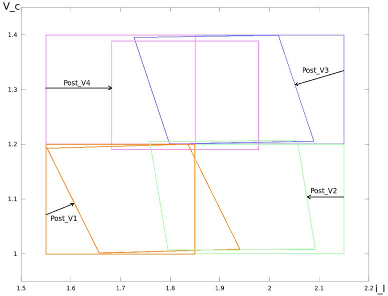
State Decomposition Method

State Decomposition Method

Problem (Decomposition) : Given a set R, find a decomposition Δ, i.e., a set of couples $\{(V_i, \pi_i)\}_{i\in I}$ such that :

1. $\bigcup_{i\in I} V_i = R$
2. $\forall i \in I \; Post_{\pi_i}(V_i) \subseteq R$.

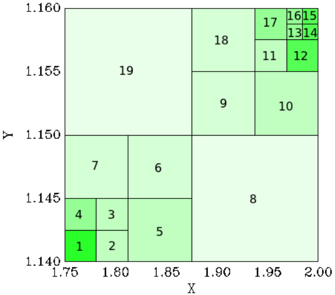




Let $Post_\Delta(X) =_{def} \bigcup_{i\in I} Post_{\pi_i}(X \cap V_i)$. Then : $Post_\Delta(R) \subseteq R$.

Application : Boost DC-DC Converter

For $R = [1.75, 2] \times [1.14, 1.18]$, a decomposition Δ with 16 boxes



Patterns $\pi_1 = (11222121222)$, $\pi_2 = \pi_3 = (122)$, $\pi_4 = (11222)$, ...

Application : Boost DC-DC Converter (cont'd)

State-dependent control : if the state is in V_i, apply π_i, and so on

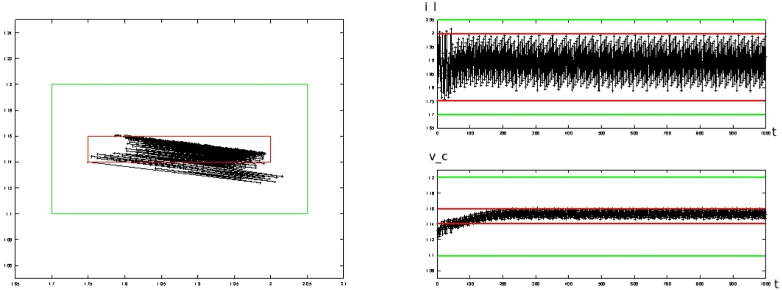


FIGURE: Simulation of the boost converter starting from $x_0 = (1, 75, 1.14)$ in plane (i_L, v_C) ; R in red

Green box $S = [1.7, 2.05] \times [1.1., 1.2]$ contains the unfolding of $Post_\Delta(R)$: we are ensured that the trajectories always stay within S

Remarks

- The unfolding is the counterpart of the ε-neighborhood of R in the approximate bi-similarity method
- The decomposition method uses forward computation (*Post*) rather than backward computation (*Pre*) as in Ramadage-Wonham based methods
- Can avoid problems of numerical instabilities in case of of contractive systems

Application to Multilevel Converter

The general function of a MC is to synthesize a desired AC voltage from several levels of DC voltages.

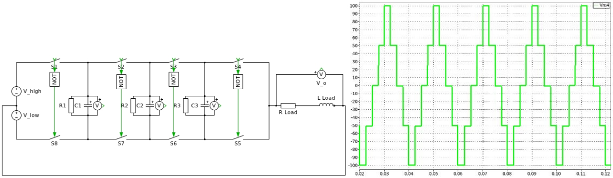


FIGURE: Electric scheme and ideal output for 5-level converter

- Stabilization objective : Find appropriate switching strategy in order to regulate the amplitude of the desired sinusoidal-like output voltage
- Safety objective : while minimizing capacitor voltage fluctuation (capacitor voltage balance)

Capacitor Voltages of Multilevel Converter

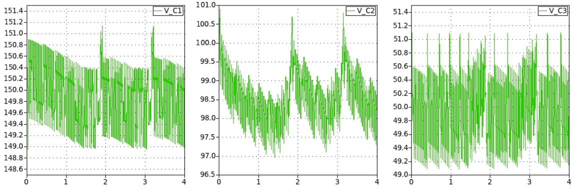


FIGURE: $v_{C1} = f(t)$, $v_{C1} = f(t)$, $v_{C1} = f(t)$

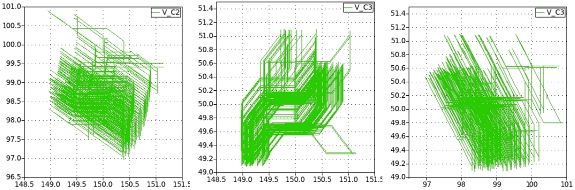


FIGURE: Planes $v_{C1} = v_{C2}$, $v_{C1} = v_{C3}$, $v_{C2} = v_{C3}$

Experimental confirmation : correct-by-design cntrl

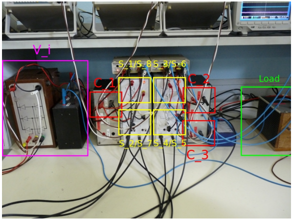


FIGURE: Prototype built by Electrical Engineering Lab SATIE

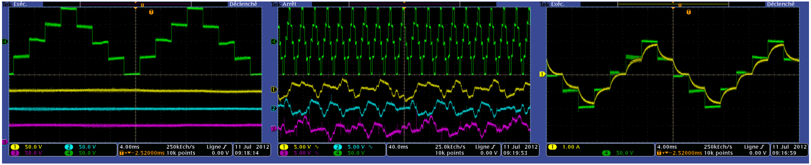
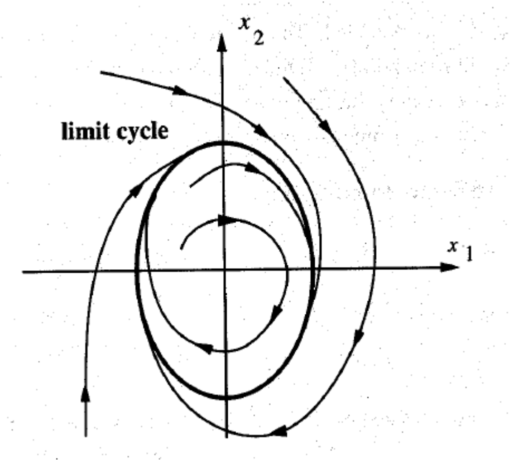


FIGURE: Output voltage and capacitor voltages

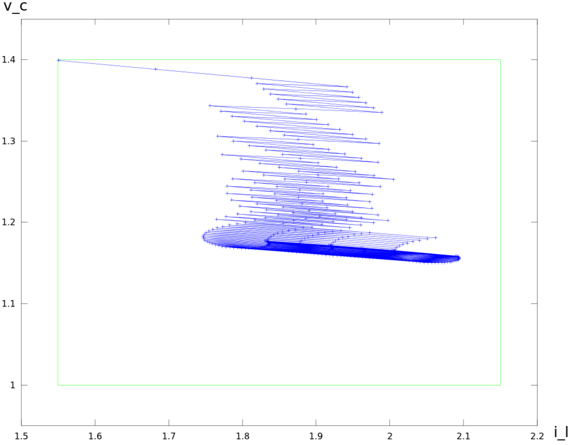
Stable Limit Cycle

Stable Limit Cycle



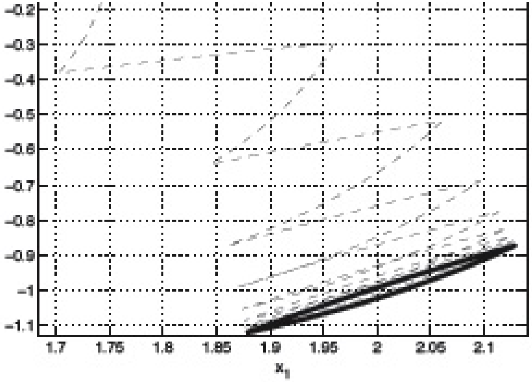
Convergence to a limit cycle

Example : Simulation for Boost of the control induced by the decomposition



Limit Cycle

Limit Cycle



Limit Cycle

Another Example : Two-Tank Problem

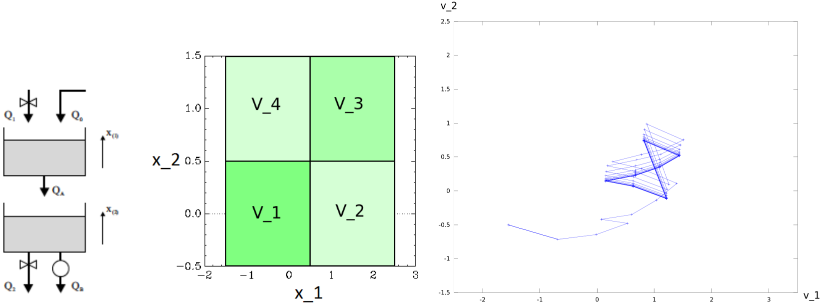


FIGURE: Decomposition and Limit Cycle of a Controlled Trajectory

Tanks filled with fluids controlled by control valves. tank 1 to 2.

Objective : Regulate fluid levels around predetermined values.

Symbolic Visual Explanation : Set Contraction

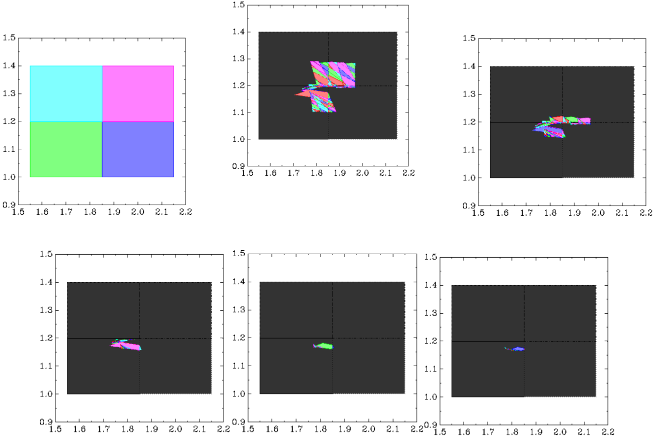


FIGURE: $Post_{\Delta}^{n}(R)$ for $n = 0, 20, 40, 60, 80, 100$

Limit Cycles of Balls

Since $Post_\Delta(R) \subseteq R$, $\{Post^i_\Delta\}_{i\geq 0}$ is a $\searrow$ sequences of nested compacts. Its limit $R^* = \bigcap_{i\geq 0} Post^i_\Delta(R)_{i\geq 0}$ exists and is nonempty.

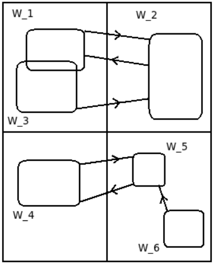
Suppose now that we have the separation property :

$$\exists N \; Post^N_\Delta(R) \cap \partial\Delta = \emptyset$$

Then :

- $Post^N_\Delta(R)$ is a $\bigcup$ of polyhedra ("balls") of the form $W_1, W_2, \ldots$.
- Furthermore, it forms oriented graph with a single outgoing edge ($W_i \rightarrow W_j$ if $Post_\Delta(W_i) \subseteq W_j$)
- $\exists M \geq N$: $Post^M_\Delta(R)$ is a (union of) cycles of balls.

Limit Cycle of Points



- Let $\mathcal{C}$ be a cycle of balls in R^*. Any B of $\mathcal{C}$ contains a fixed point b (by Brouwer since $Post_{\mathcal{C}}(B) = B$)
- Suppose now that we have the contraction property on B :

$$d(Post_{\mathcal{C}}(x), b) < d(x, b) \qquad \text{for all } x \in B, x \neq b$$

- Then $B \to \{a\}$ as $i \to \infty$, and R^* is union of cyclic points

Boost Example

$Post^N_\Delta(R) \cap \partial\Delta = \emptyset$ for $N = 93$ ($Post^N_\Delta(R)$: $\bigcup$ 4 polyhedra)

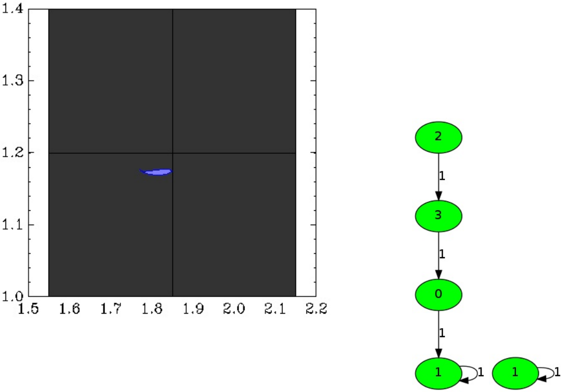


FIGURE: $Post^N_\Delta(R)$ and associated graph and limit cycle

Two-Tank Example

$Post^N_\Delta(R) \cap \partial\Delta = \emptyset$ for $N = 8$ ($Post^N_\Delta(R) : \bigcup$ 29 polyhedra)

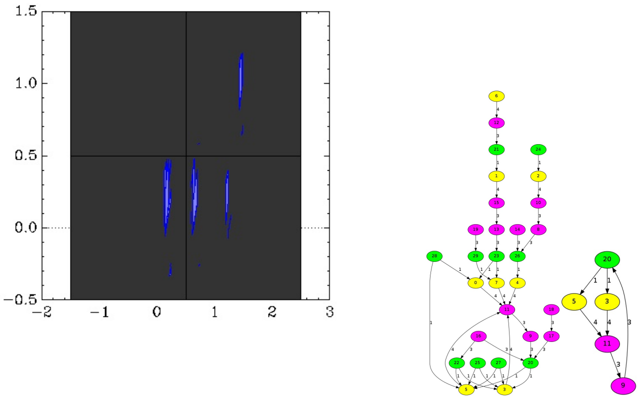


FIGURE: $Post^N_\Delta(R)$ and associated graph and limit cycle

Theorem

Suppose there exists Δ such that :

1. Decomposition :
$$Post_{\Delta}(R) \subseteq R$$
2. Separation :
$$\exists N \; Post_{\Delta}^{N}(R) \cap \partial\Delta = \emptyset$$
3. Contraction :
$$\forall x \in B \setminus \{b\} \quad d(Post_{\mathcal{C}}(x), b) < d(x, b)$$

Then $R^* = \bigcap_{i \geq 0} Post_{\Delta}^{i}(R)$ is a (union of) limit cycle(s) to which every trajectory starting in R converges.

NB : R^* is the minimal invariant subset of R for $Post_{\Delta}$

Recapitulation

Recapitulation

The control synthesis of sampled switched systems is an important and difficult problem. We have presented two approaches :

1. The approximate bisimulation method :
   - Assumption of incremental stability (δ-GUAS Lyapunov fn)
   - Computes the maximal invariant subset of a given safe set R
   - Uses Pre operator
   - Reduces the problem to a problem on a finite equivalent graph
2. The decomposition method :
   - Assumptions of decomposition, separation and contraction
   - Computes the minimal invariant subset of a given safe set R
   - Uses Post operator
   - Proof of convergence of the controlled trajectories to limit cycles

Perspectives

- Correct-By-Design Control of Power Converters
- Important for sustainable development and environmental issues (smart house, control of grids with renewable energy sources)
- Extension to non-affine dynamical systems (cf Romain's talk)
- Need for scaling up (today, limit $n = 7$)

Perspectives

- Correct-By-Design Control of Power Converters
- Important for sustainable development and environmental issues (smart house, control of grids with renewable energy sources)
- Extension to non-affine dynamical systems (cf Romain's talk)
- Need for scaling up (today, limit $n = 7$)

NB : Open PhD position at LSV on the topic !

References

- MS Branicky, Stability of switched and hybrid systems, Decision and Control, 1994.
- M. Senesky, G. Eirea, T Koo
  Hybrid modelling and control of power electronics
  Hybrid Systems : Computation and Control, Springer, 2003
- A. Girard, G. Pola, P. Tabuada
  Approximately bisimilar symbolic models for incrementally stable switched systems
  IEEE Transactions on Automatic Control 55 (1), 2010
- L. Fribourg, R. Soulat
  Stability controllers for sampled switched systems
  Proc. 7th International workshop on Reachability Problems (RP'2013), LNCS, Springer,2013.

Thanks !