

MTL ROBUST TESTING AND VERIFICATION FOR LPV SYSTEMS

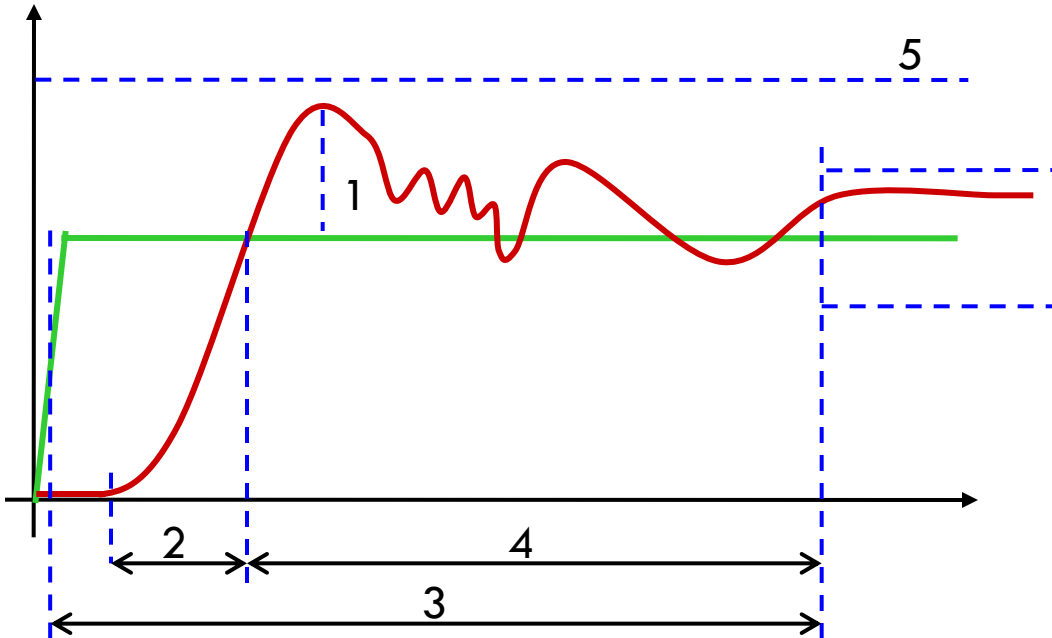
Georgios Fainekos, NEC Labs[♣]

George Pappas, University of Pennsylvania

[♣] Work performed at
the University of
Pennsylvania

ACC 2009, St. Louis, Missouri, 2009.06.11

Motivation – A study of transient dynamics

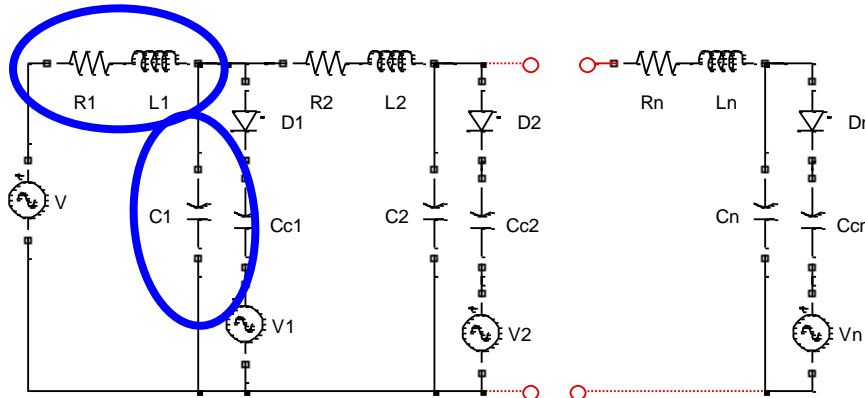


Desired Performance Characteristics

1. Overshoot
2. Rise time
3. Delay time
4. Settling time
5. Constraints on input/states
6. Response sensitivity

Use Linear or Metric
Temporal Logic

Example : Verifying a transmission line



System:

$$\dot{x}(t) = A_i x(t) + b_i U_{in}(t)$$

$$U_{out}(t) = Cx(t)$$

Step input ($t > 0$):

$$U_{in}(t) = 1$$

Steady state at $t = 0$:

$$x(0) = -A^{-1} b U_{in}(0)$$

Property:

$$\Phi = G \pi_1 \wedge F_{[0,0.85]} G \pi_2$$

$$O(\pi_1) = [-1.5, 1.5]$$

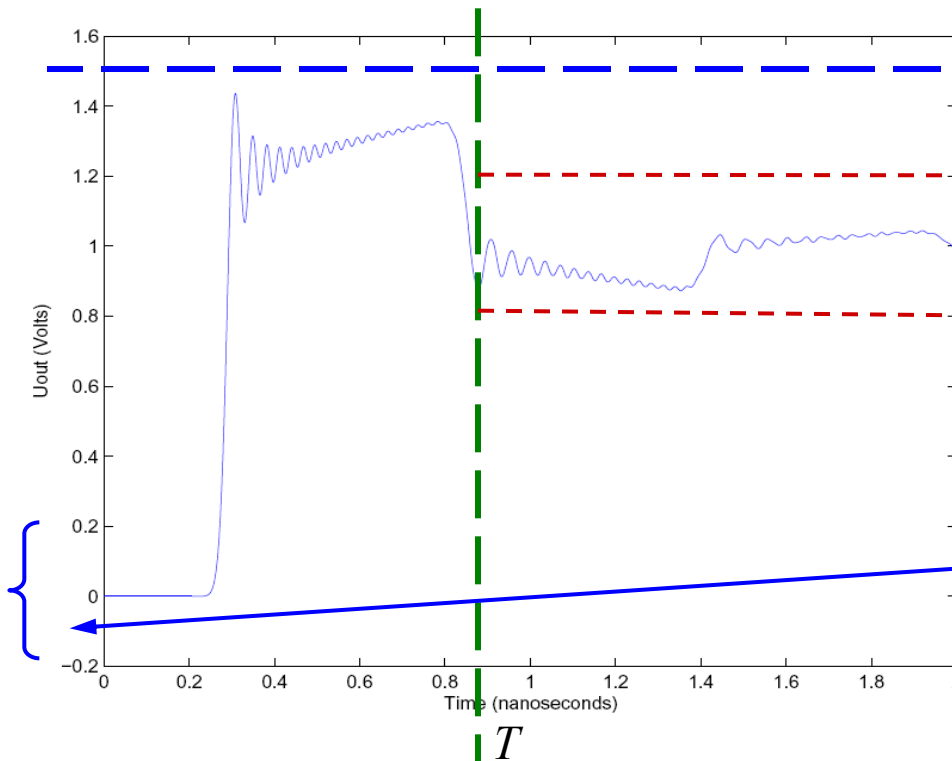
$$O(\pi_2) = [0.8, 1.2]$$

Initial conditions:

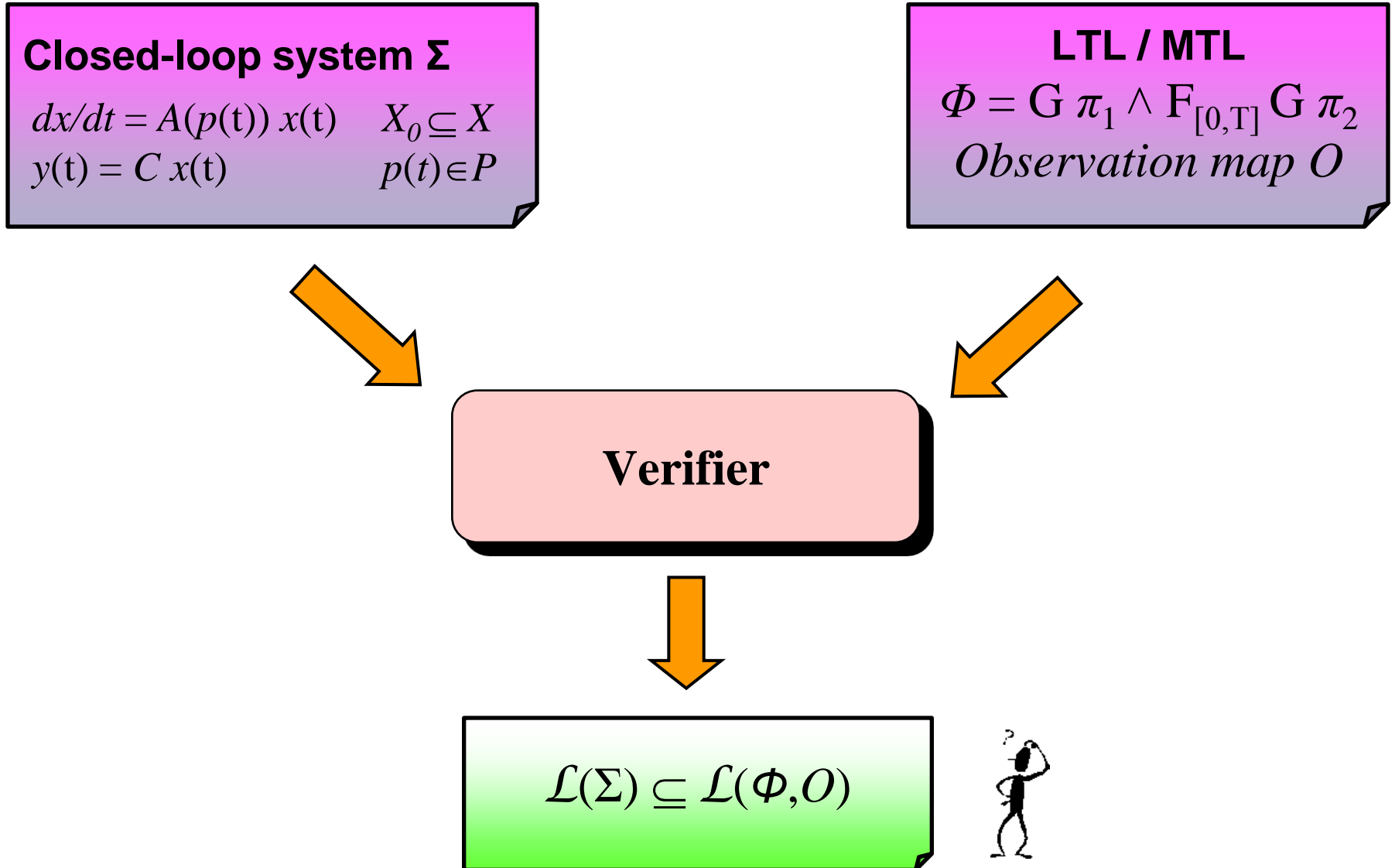
$$U_{in}(0) \in [-0.2, 0.2]$$

Uncertain parameters

$$e.g. C \in [a_1, a_2]$$



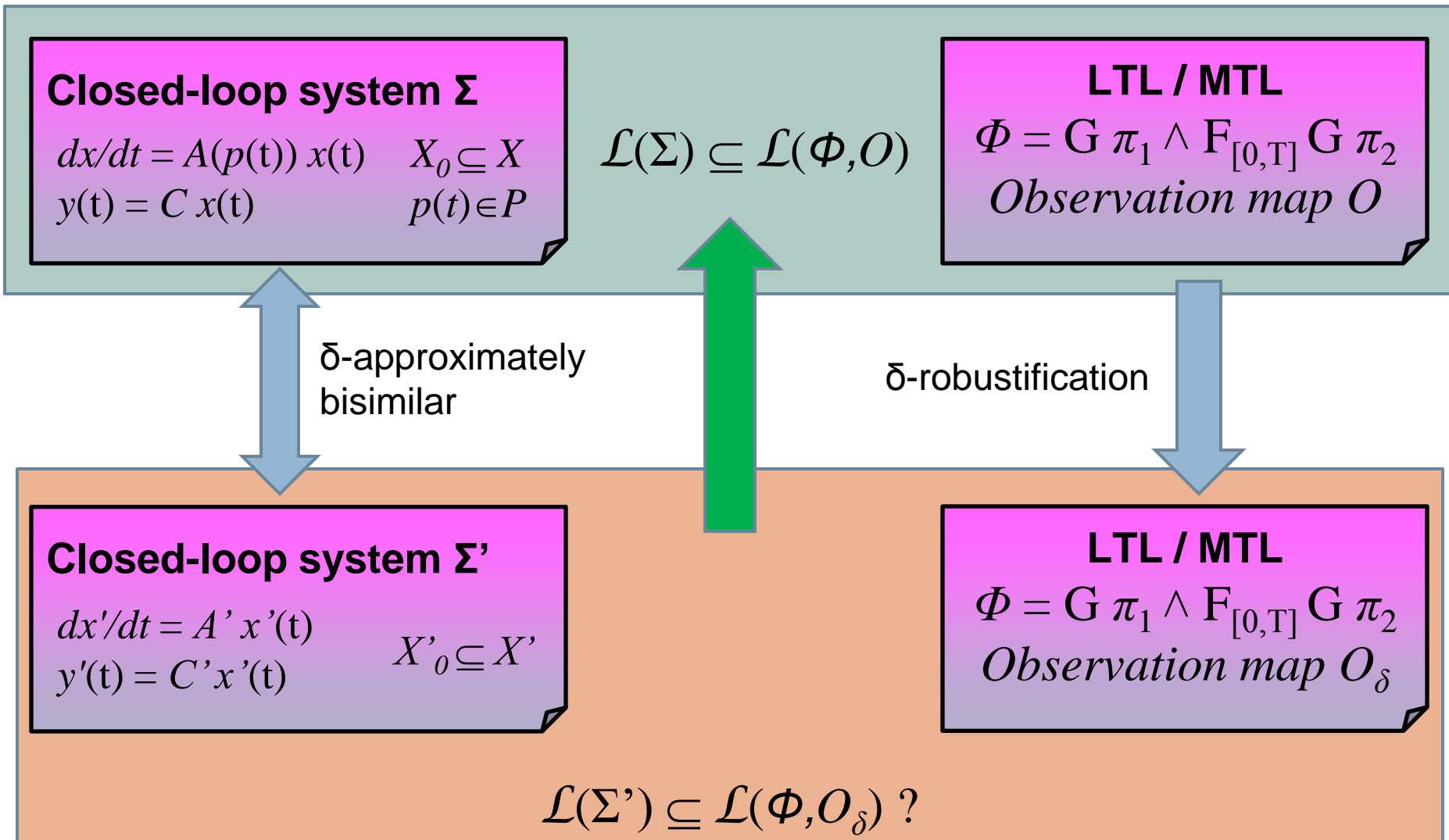
Problem Formulation



5

Overview of Solution

Solution Overview



7



Metric Temporal Logic

Definitions & System Robustness

Metric Temporal Logic (MTL)

Syntax:

$$\Phi ::= \top / \perp / \pi / \neg \pi / \Phi_1 \vee \Phi_2 / \Phi_1 \wedge \Phi_2 / \Phi_1 \mathcal{U}_I \Phi_2 / \Phi_1 \mathcal{R}_I \Phi_2$$

until  *release* 

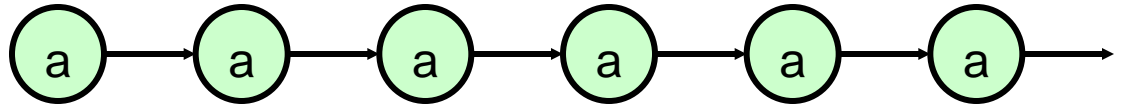
I can be of any bounded or unbounded interval of \mathbb{R}^+ , but $I \neq \emptyset$
i.e. $I = [0, +\infty)$, $I = [2.5, 9.8]$

Derived operators:

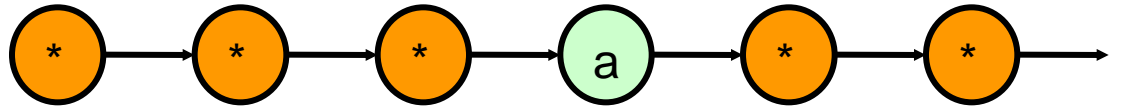
$$\begin{array}{ll} \text{Eventually (in the future)} & F_I \Phi := \top \mathcal{U}_I \Phi \\ \text{Always (globally)} & G_I \Phi := \perp \mathcal{R}_I \Phi \end{array}$$

LTL intuition

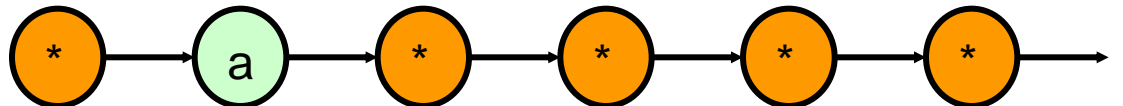
$G a$ - always a



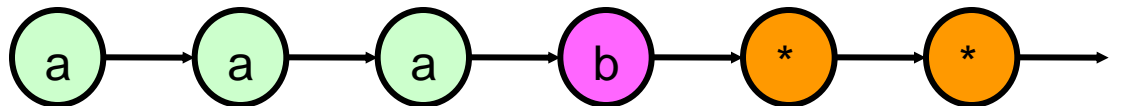
$F a$ - eventually a



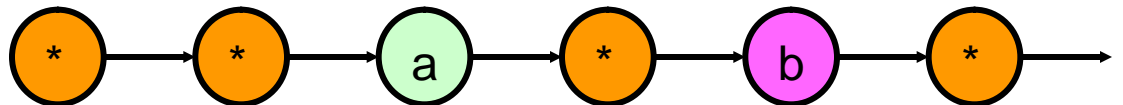
$X a$ - next state a



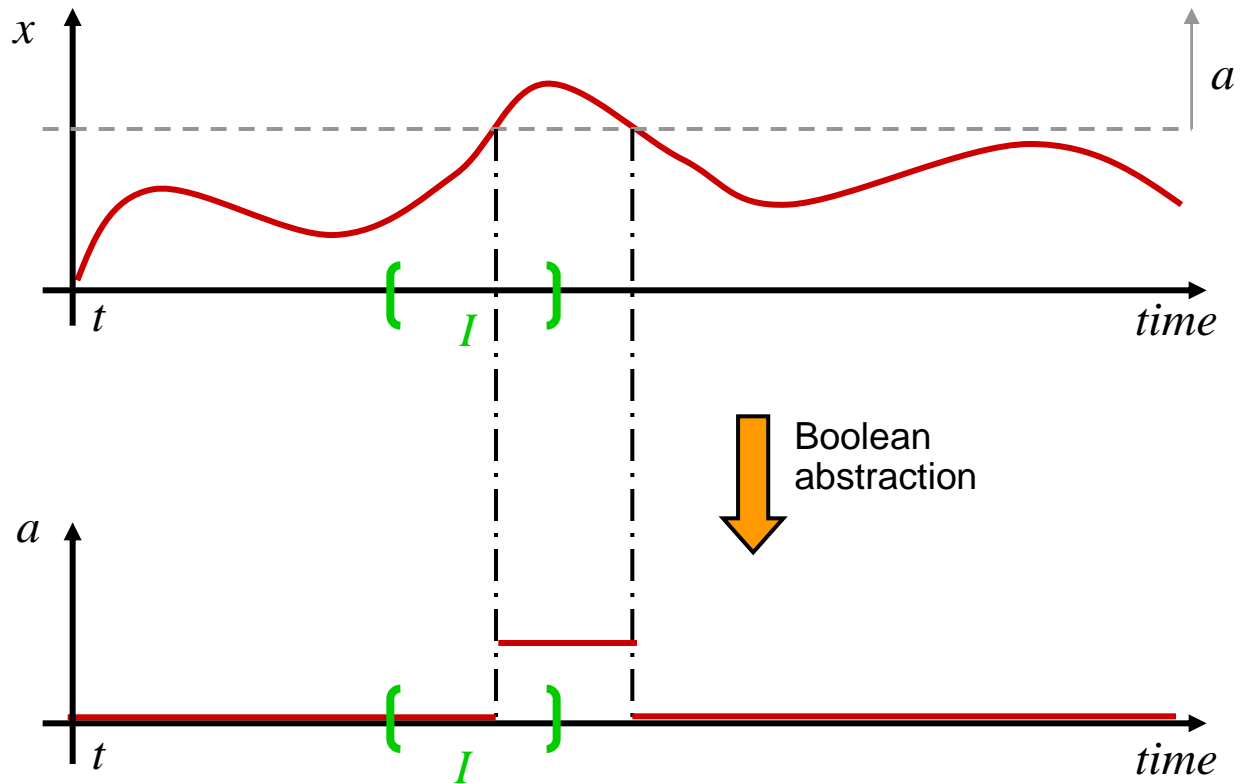
$a \mathcal{U} b$ - a until b



$a \mathcal{B} b$ - a before b



MTL : An example for signals

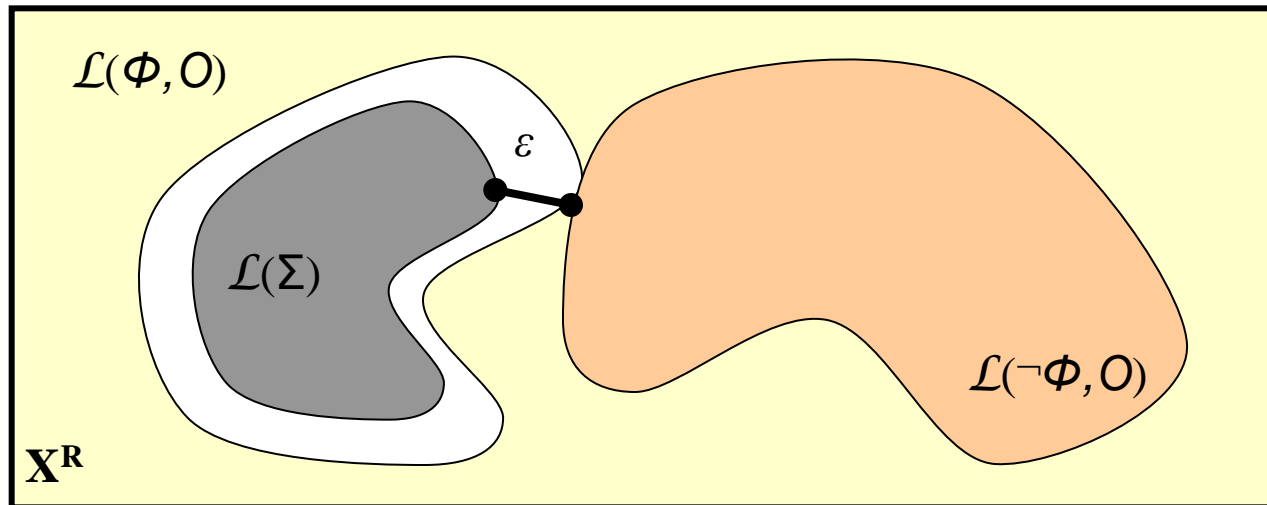
 $F_I a$

MTL System Robustness

Given a system Σ , we can define the *robustness degree* as

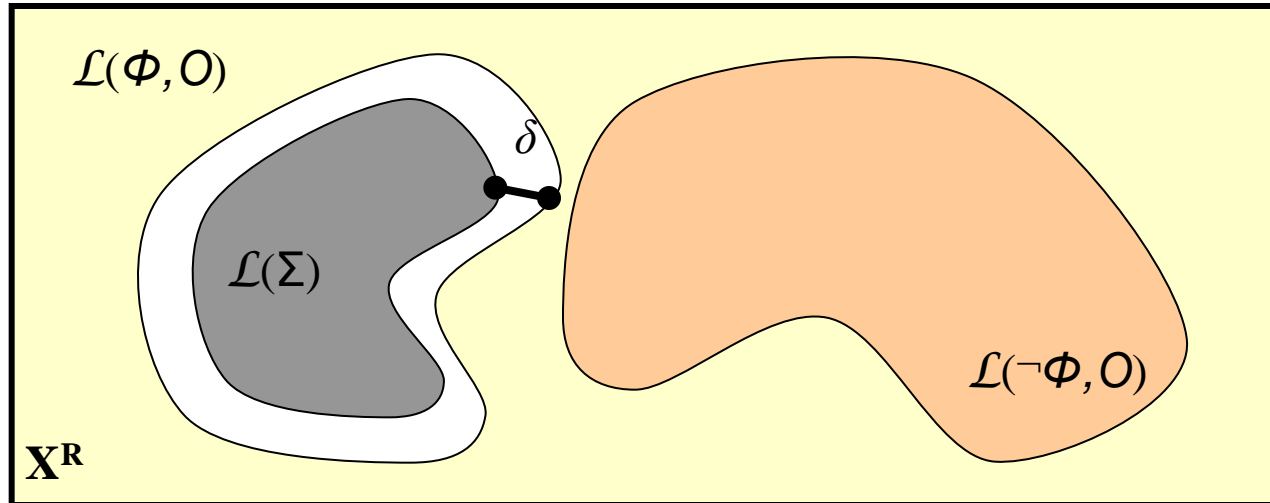
$$\varepsilon := \mathbf{dist}_\rho(\mathcal{L}(\Sigma), \mathcal{L}(\neg\Phi, O)) = \inf \{ \rho(s, s') \mid s \in \mathcal{L}(\Sigma), s' \in \mathcal{L}(\neg\Phi, O) \}$$

$$\rho(s, s') = \sup \{ d(s(t), s'(t)) \mid t \in R \}$$

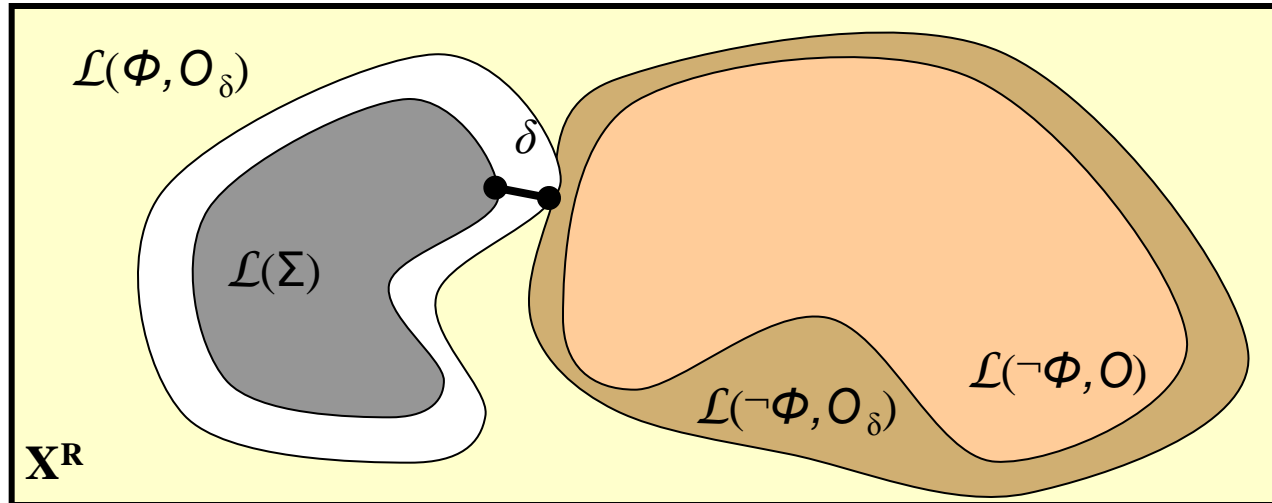


MTL System Robustness

However, in this case, we are given δ ...



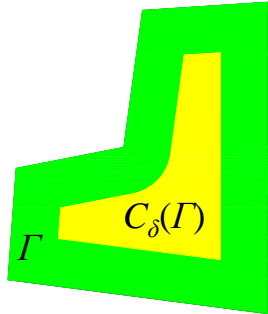
MTL System Robustness



$$O_\delta(\pi) = C_\delta(O(\pi))$$

$$O_\delta(\neg\pi) = C_\delta(X \setminus O(\pi))$$

$$C_\delta(\Gamma) = \{ a \in A \mid B_\delta(a) \subseteq \Gamma \}$$



Proposition:

Consider an MTL formula φ , a map $O : \Pi \rightarrow P(X)$ and a number $\delta > 0$, then $\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi, O_\delta)$ implies $B_\delta(\mathcal{L}(\Sigma)) \subseteq \mathcal{L}(\Phi, O)$ for any dynamical system Σ .

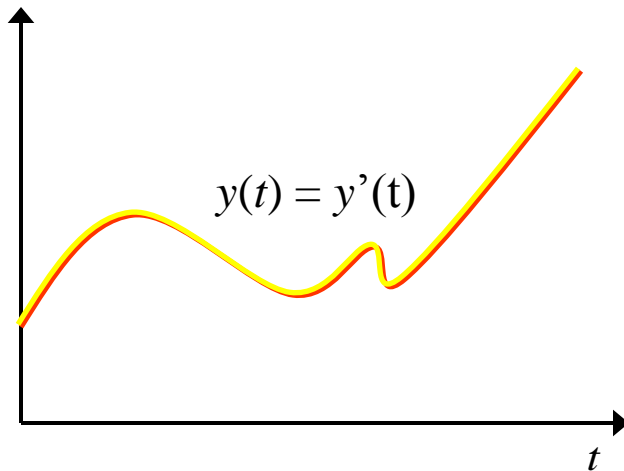
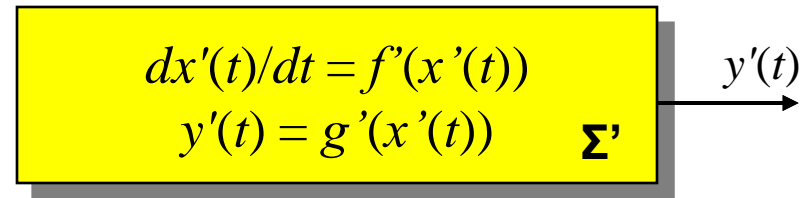
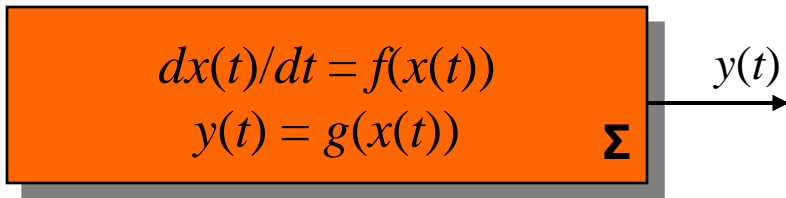
Proof (sketch) : We have to prove that for any observable trajectory y of Σ any signal y' in the tube $B_\delta(y)$ satisfies Φ . This is done by induction on the structure of the formula Φ .

15

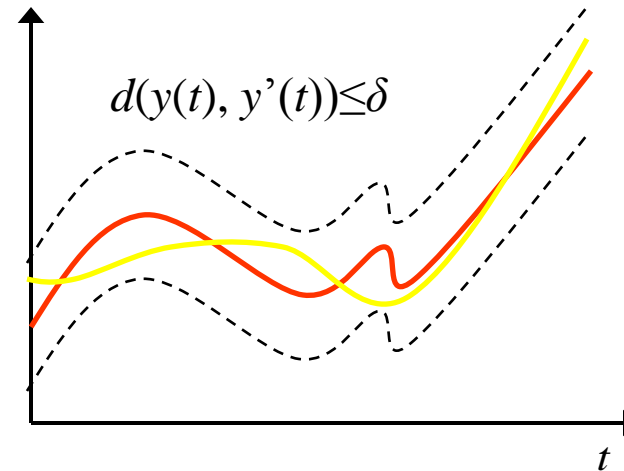
System Approximations

Approximate Bisimulation Relations

Approximate Simulation Relation: Review

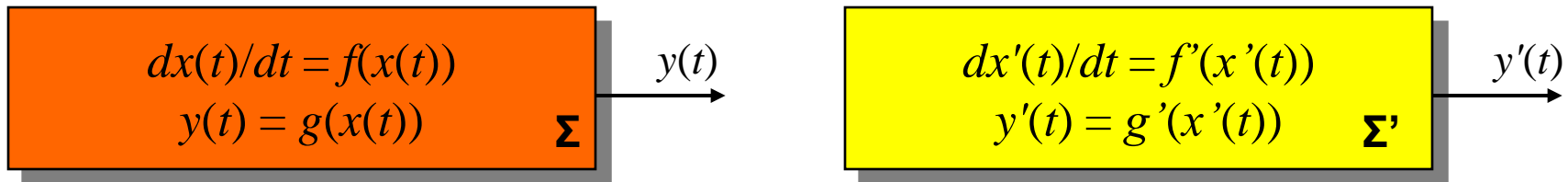


Exact simulation



Approximate simulation

Approximate Bisimulation Relation: Review



- A relation $R \subseteq X \times X'$ is a δ -approximate simulation if for all $(x_0, x'_0) \in R$,
 1. $d(g(x_0), g'(x'_0)) \leq \delta$
 2. for all $T \geq 0$, for all trajectories $x(t)$ of Σ such that $x(0)=x_0$, there exists a trajectory $x'(t)$ of Σ' such that $x'(0)=x'_0$ satisfying:

$$\forall t \in [0, T] . (x(t), x'(t)) \in R$$

3. for all $T \geq 0$, for all trajectories $x'(t)$ of Σ' such that $x'(0)=x'_0$, there exists a trajectory $x(t)$ of Σ such that $x(0)=x_0$ satisfying:

$$\forall t \in [0, T] . (x(t), x'(t)) \in R$$

If the initial set of states of Σ and Σ' are in R (i.e. $(x_0, x'_0) \in R$), then

any observed trajectory of Σ has an observed trajectory of Σ' in its δ -neighborhood and vice versa.

Bisimulation functions & Games: Review

Definition: A function $F : X \times X' \rightarrow \mathbb{R}^+$ is a *bisimulation function* between Σ and Σ' if for all $\delta \geq 0$, $R = \{ (x, x') \mid F(x, x') \leq \delta \}$ is δ -approximate bisimulation relation.

Theorem: Let F be a bisimulation function between Σ and Σ' and

$$\delta \geq \max \left(\sup_{x \in X} \inf_{x' \in X'} F(x, x'), \sup_{x' \in X'} \inf_{x \in X} F(x, x') \right)$$

If δ has a finite value, then Σ and Σ' are δ -approximate bisimilar.

Approximations between LPV Systems

Theorem: Let Σ and Σ' be two LPV systems and V be continuously differentiable such that for any $(x, x') \in X \times X'$

$$V(x, x') \geq \|Cx - C'x'\|^2$$

$$\forall p \in P. \forall p' \in P'. \nabla V(x, x') \begin{bmatrix} A(p)x \\ A'(p')x' \end{bmatrix} \leq 0$$

Then, $F(x, x') = \sqrt{V(x, x')}$ is a bisimulation function between Σ and Σ' .

Approximations between LPV Systems

Theorem: Let Σ and Σ' be two LPV systems. If there exists a positive semidefinite matrix M such that

$$M \geq \begin{bmatrix} C^T C & -C^T C' \\ -C'^T C & C'^T C' \end{bmatrix}$$

$$\forall p \in EP(P). \forall p' \in EP(P'). \begin{bmatrix} A^T(p) & 0 \\ 0 & A'^T(p') \end{bmatrix} M + M \begin{bmatrix} A(p) & 0 \\ 0 & A'(p') \end{bmatrix} \leq 0$$

Then $F(x, x') = \sqrt{\begin{bmatrix} x^T & x'^T \end{bmatrix} M \begin{bmatrix} x^T & x'^T \end{bmatrix}^T}$ is a bisimulation function between Σ and Σ' .

Proof (sketch) : The 2nd matrix inequality is derived similar to Horisberger and Belanger, Regulators for linear, time invariant plants with uncertain parameters, IEEE TAC, 21(5):705–708, 1976.

Approximating an LPV with an LTI System

Corollary: Let Σ be an LPV system and $p' \in P$. If there exists a positive semidefinite matrix M such that

$$M \geq \begin{bmatrix} C^T C & -C^T C \\ -C^T C & C^T C \end{bmatrix}$$

$$\forall p \in EP(P). \begin{bmatrix} A^T(p) & 0 \\ 0 & A^T(p') \end{bmatrix} M + M \begin{bmatrix} A(p) & 0 \\ 0 & A(p') \end{bmatrix} \leq 0$$

Then $F(x_0, x'_0) = \sqrt{[x_0^T \ x'_0{}^T] M [x_0^T \ x'_0{}^T]^T}$ is a bisimulation function between Σ and Σ' .

Approximating an LPV with an LTI System

Proposition: Let Σ be an LPV system, $p' \in P$ and let

$$F(x, x') = \sqrt{V(x, x')} = \sqrt{\begin{bmatrix} x^T & x'^T \end{bmatrix} M \begin{bmatrix} x^T & x'^T \end{bmatrix}^T}$$

be a bisimulation function between Σ and $\Sigma(p')$. Then, the solution of the static games

$$\max \left(\sup_{x \in EP(X_0)} \inf_{x' \in X_0} F(x, x'), \sup_{x' \in EP(X_0)} \inf_{x \in X_0} F(x, x') \right)$$

computes the optimal points \underline{x} and \underline{x}' which provide an upper bound $\underline{\delta} = F(\underline{x}, \underline{x}')$ for the approximate bisimulation relation.

23

System Approximation & MTL

Putting Everything together

Proposition:

Consider an MTL formula φ and a map $O : \Pi \rightarrow P(X)$. If systems Σ and Σ' are δ -approximately bisimilar and $B_\delta(\mathcal{L}(\Sigma')) \subseteq \mathcal{L}(\Phi, O)$, then $\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi, O)$.

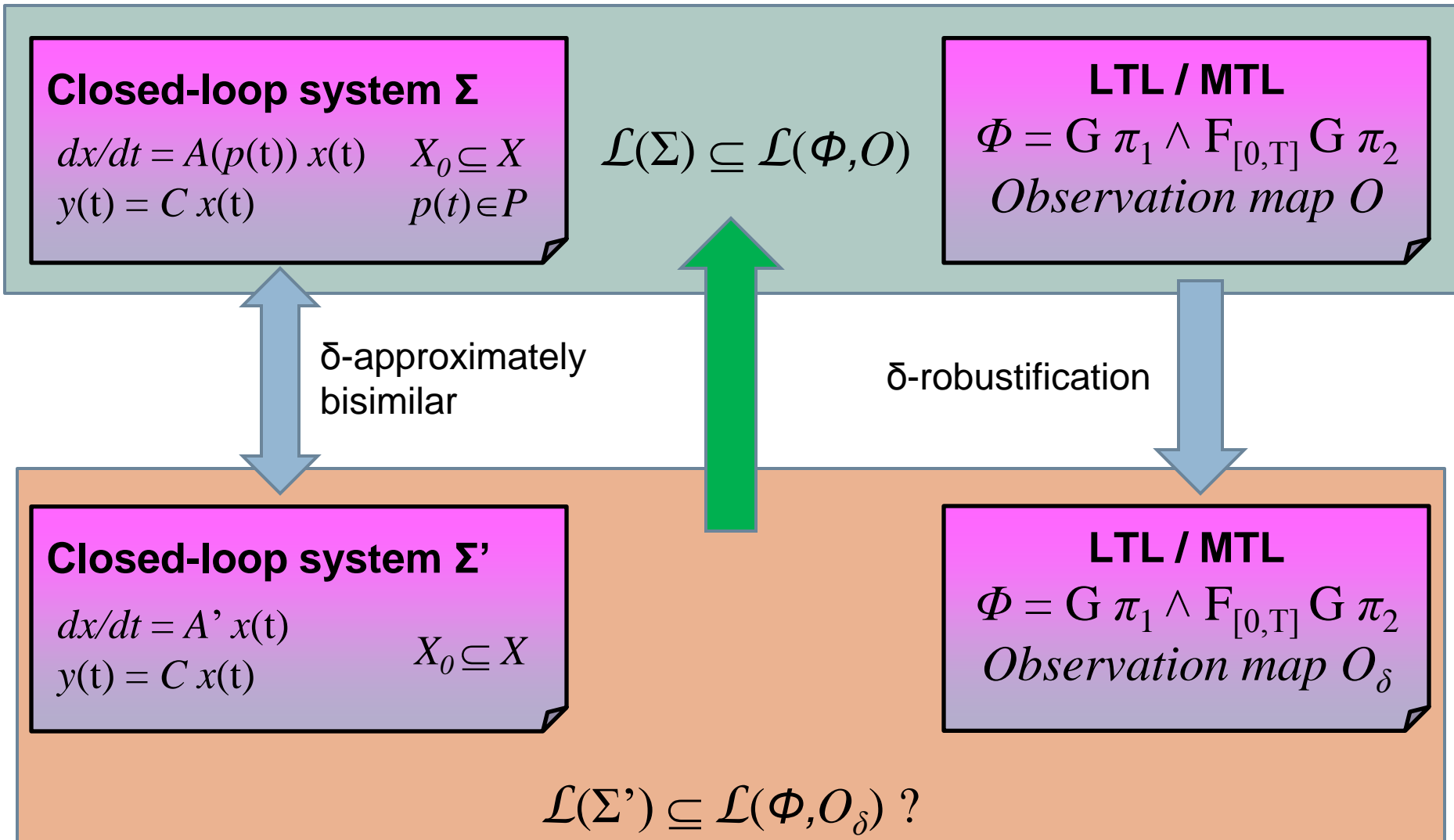
Corollary:

Consider an MTL formula φ and a map $O : \Pi \rightarrow P(X)$. If systems Σ and Σ' are δ -approximately bisimilar and $\mathcal{L}(\Sigma') \subseteq \mathcal{L}(\Phi, O_\delta)$, then $\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi, O)$.

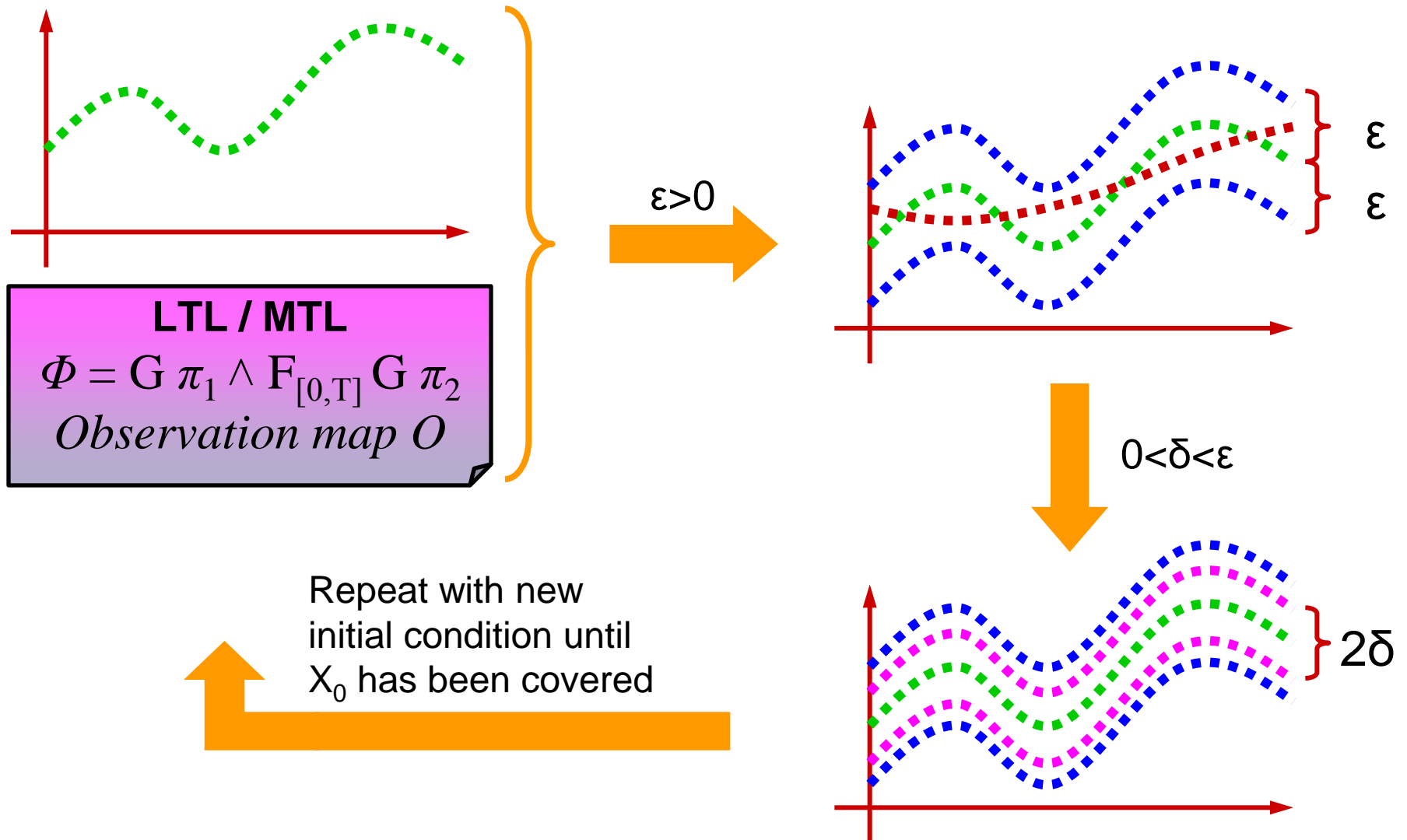
Solution Overview

25

UPenn



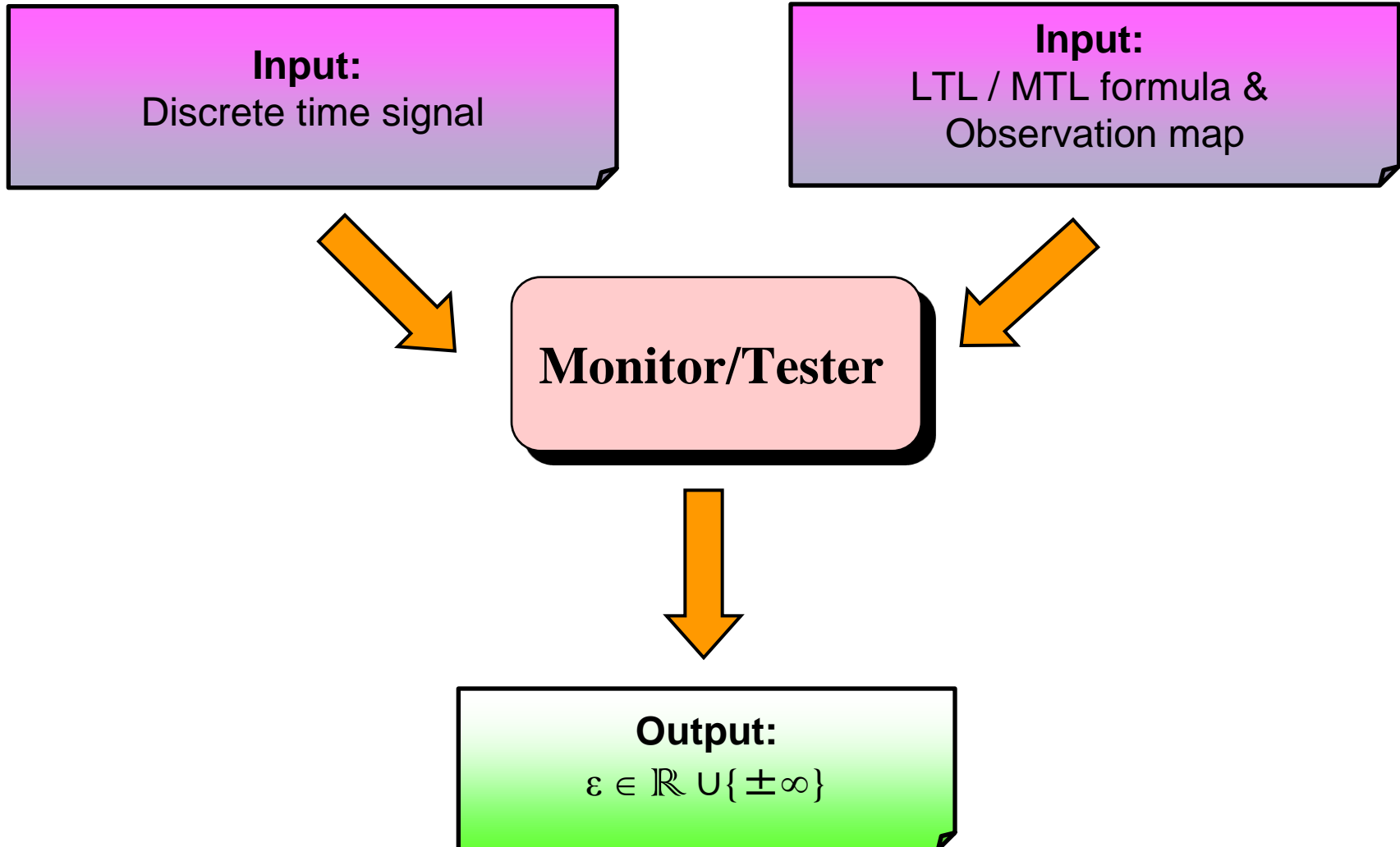
MTL Robust Testing



Software toolbox : TaLiRo

27

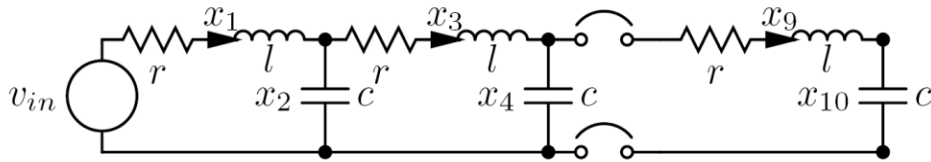
UPenn



28

Numerical Examples

Example : Transmission line



$$x(0) \in X_0 = \prod_{i=1}^5 (\{0\} \times [-\alpha, \alpha])$$

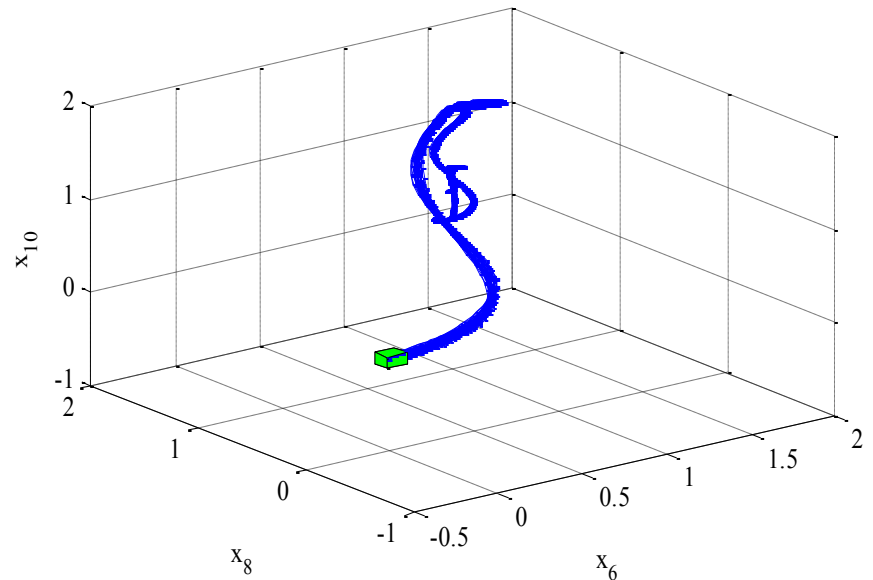
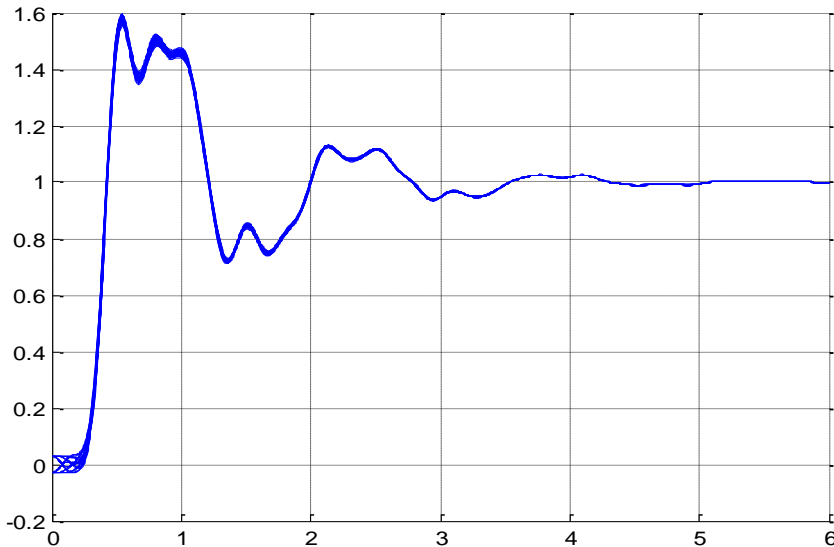
$$c(t) \in [c_0 - \beta, c_0 + \beta]$$

Instance	1	2	3	4
α	0.01	0.03	0.06	0.1
δ	0.1124	0.1150	0.1198	0.1281
safe	✓	✓	✓	✓
# of sim.	1	1	33	1057

$$\psi_1 = \square \pi_1 \wedge \diamond_{\leq 3} \square \pi_2$$

$$\mathcal{O}(\pi_1) = \{\hat{y} \in \mathbb{R}^5 \mid \bigwedge_{i=1}^5 |\hat{y}_i| \leq 2\}$$

$$\mathcal{O}(\pi_2) = \{\hat{y} \in \mathbb{R}^5 \mid 0.8 \leq \hat{y}_5 \leq 1.2\}$$



Example : Nonlinear systems

30

UPenn

$$\dot{x}_1(t) = 0.05 \sin^2(x_2(t))x_1(t) - 2.5x_2(t)$$

$$\dot{x}_2(t) = 0.5x_1(t) - x_2(t)$$

$$X_0 = [0.4, 0.8] \times [-0.3, -0.1]$$

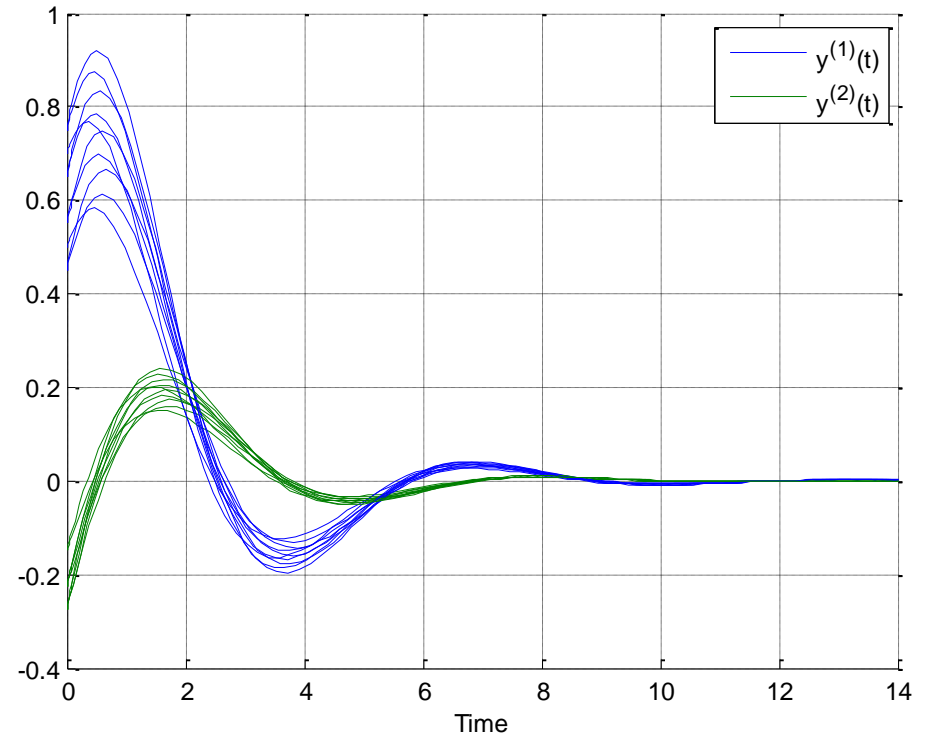
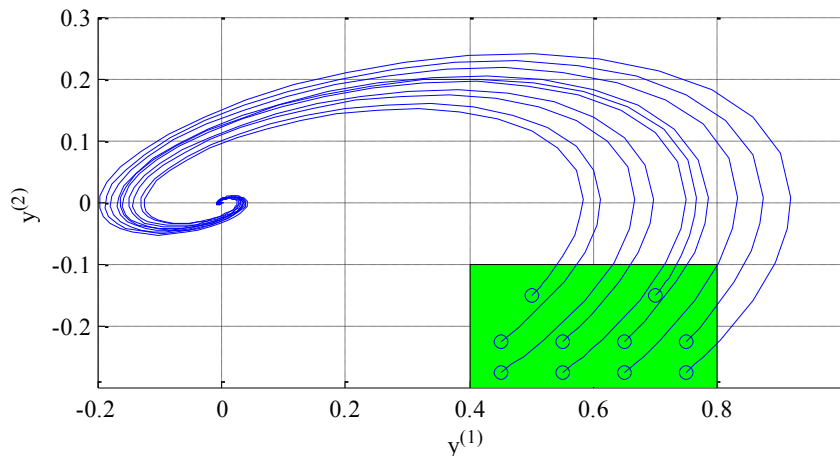
$$\psi_2 = \square \pi_3 \wedge \square_{\geq 8} \pi_4$$

$$\mathcal{O}(\pi_3) = \mathbb{R} \times [-0.6, 0.6]$$

$$\mathcal{O}(\pi_4) = [-0.4, 0.4] \times [-0.4, 0.4]$$

$$\dot{x}(t) = \begin{bmatrix} 0.05p(t) & -2.5 \\ 0.5 & -1 \end{bmatrix} x(t)$$

$$p(t) \in P = [0, 1]$$



Prior work & Related research

- Mine & collaborators work:
 - Fainekos and Pappas, *Robustness of temporal logic specifications*, FATES/RV 2006
 - Fainekos, Girard and Pappas, *Temporal logic verification using simulation*, FORMATS 2006
 - Girard & Pappas, *Approximation Metrics for Discrete and Continuous Systems*, IEEE TAC, 52(5):782-798, May 2007
 - Julius, Fainekos, Anand, Lee, Pappas, *Robust Test Generation and Coverage for Hybrid Systems*, HSCC 2007
 - Fainekos and Pappas, *Robust Sampling for MITL specifications*, FORMATS 2007
- Related research:
 - Althoff, Stursberg and Buss, *Reachability analysis of linear systems with uncertain parameters and inputs*, CDC'07
 - Donze and Maler, *Systematic simulation using sensitivity analysis*, HSCC'07
 - Ramdani, Meslem, and Candau, *Reachability of uncertain nonlinear systems using a nonlinear hybridization*, HSCC'08
 - Lerda, Kapinski, Clarke, and Krogh. *Verification of supervisory control software using state proximity and merging*, HSCC'08
 - Batt, Belta, and Weiss, *Temporal logic analysis of gene networks under parameter uncertainty*, IEEE TAC, 53(Special Issue):215–229, Jan. 2008.
 - Dang, Donze, Maler, and Shalev. *Sensitive state-space exploration*. CDC'08

Conclusions / Future Work

- ✓ Model Checking and Exhaustive Verification are the holy grail, but **expensive** for Continuous and Hybrid Systems
 - ✓ **Light-weight verification** can help practitioners
- ✓ **Solution: A new approach** to system testing using simulations
 - ✓ **Main theme:** A system that is robust with respect to an MTL property is easier to verify!
 - ✓ If completeness is not achieved, we get coverage guarantees

➤ Future work

- Relaxing timing constraints (Robustness wrt time)
 - [Huang et al '06], [Henzinger et al '06], [Bouyer et al '05], ...
- Hybrid Systems
 - Julius, Fainekos, Anand, Lee, Pappas, Robust Test Generation and Coverage for Hybrid Systems, HSCC 2007
- Non-deterministic systems
 - [Girard and Pappas '06]

