

Robustness of Temporal Logic Specifications



Georgios E. Fainekos

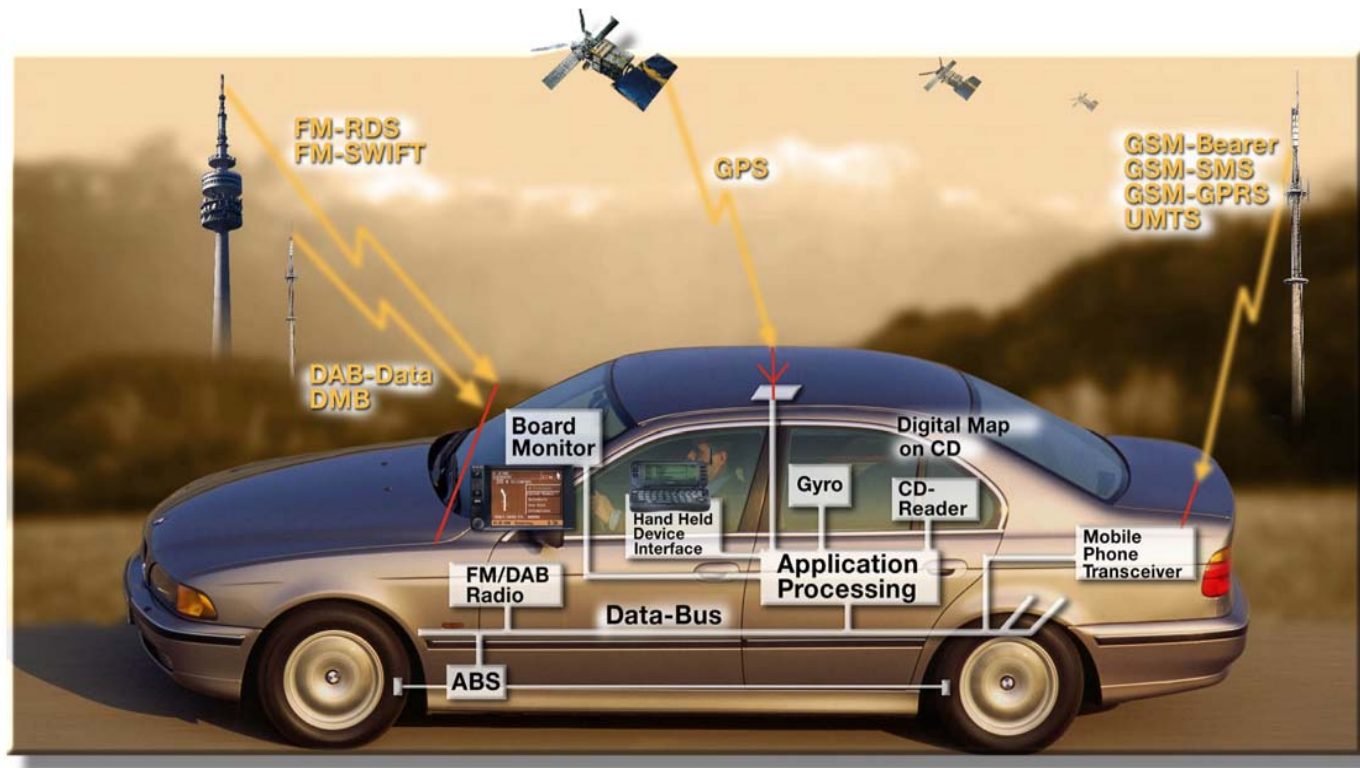
PhD Thesis Defense - June 23, 2008

Department of Computer and Information Science
University of Pennsylvania

✉ fainekos at seas upenn edu

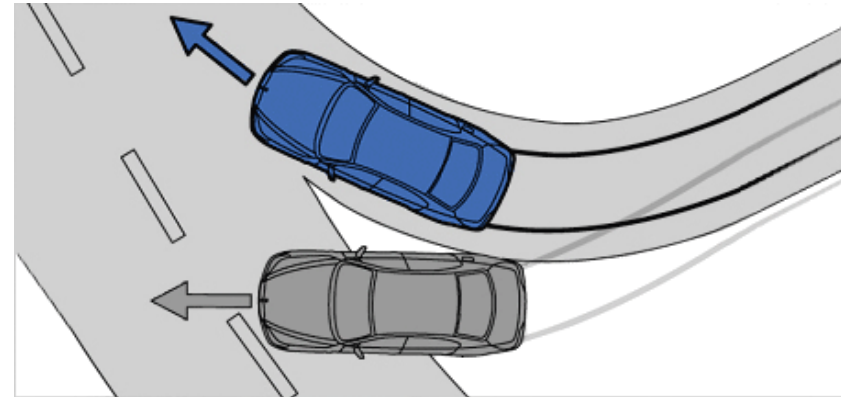
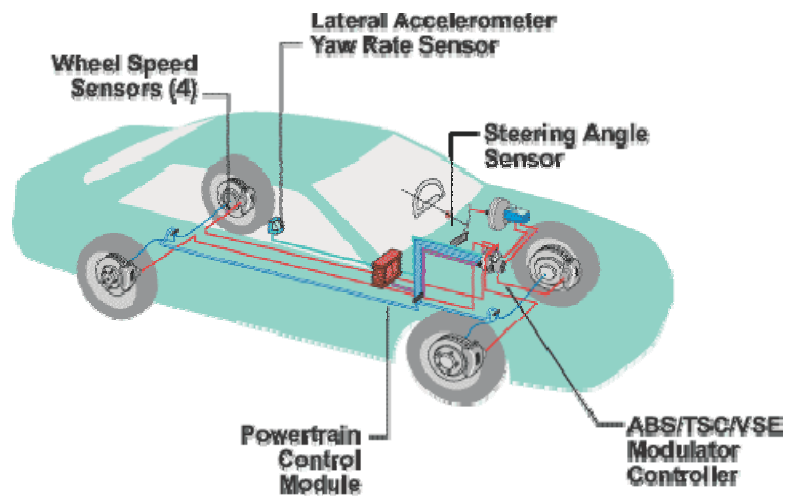
🌐 <http://www.seas.upenn.edu/~fainekos/>

Embedded in : Automotive Systems



Latest BMW : 72 networked microprocessors
90% of innovation on electronics

Embedded in : Automotive Systems



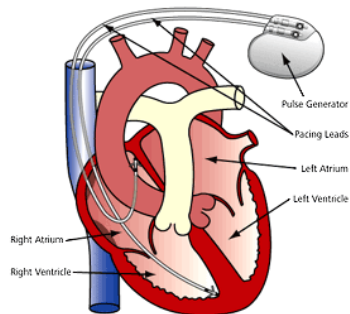
Embedded in : Avionics



Boeing 777 : 1280 networked microprocessors
50% of design cost (\$ and time)

Embedded in : Medical Devices

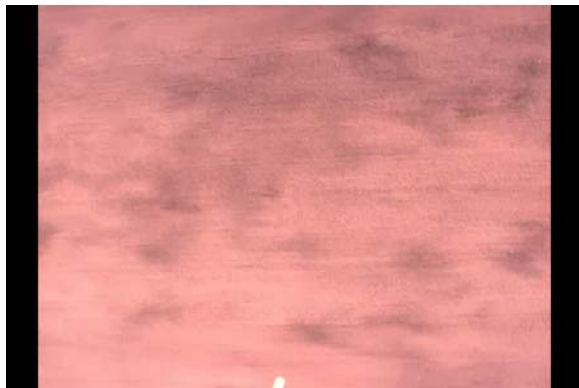
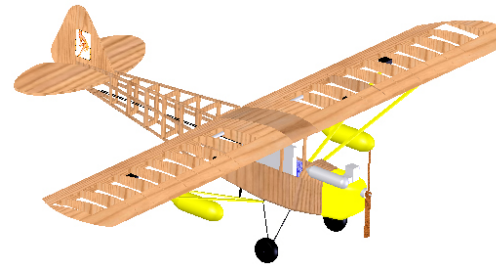
Vision : Doctor-on-a-chip
 Operating room of the future
 Remote monitoring of elderly
 Digital hospital



Embedded in : Robotics

UAV

UGV

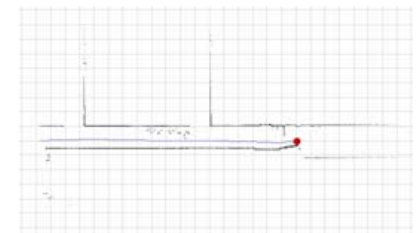


Deployable POD
(Robotic Agent, Sensor ,
Beacon, Landmark etc.)

Hi Res Camera & IMU
POD Controllable PAN
Motion

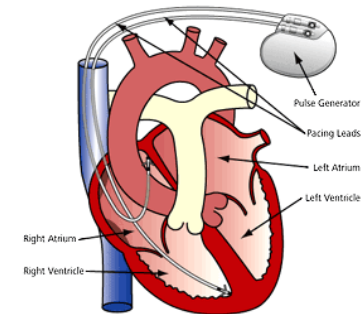


Bayraktar, Fainekos, Pappas, *Experimental Cooperative Control of Fixed-Wing Unmanned Aerial Vehicles*, CDC 07



Cyber-Physical Systems : Challenges

- Composition and Modularity
 - Important for heterogeneous systems
- Robustness, Safety, and Security
 - Security cannot always be guaranteed, is system robust?
- Control and Hybrid Systems
 - Closing the loops at all levels
- Computational Abstractions
 - New models and programming languages
- Reconfigurable / Networked Systems
 - Sensor networks embedded in critical infrastructure
- Model-based Development
 - From models to platform-dependend implementations
- Verification, Validation, and Certification
 - Safety-critical computing systems
 - Particularly important for government agencies
- Education and Training
 - No education in cyber-physical systems
 - Education in system architecture/integration?



Contributions of the thesis

✓ A **new** notion of **robustness** for temporal logics

Fainekos and Pappas, *Robustness of temporal logic specifications*, FATES/RV 2006

Fainekos and Pappas, *Robustness of TL specifications for continuous time signals*, TCS (Submitted)

✓ From discrete time to continuous time

Fainekos and Pappas, *Robust Sampling for MITL specifications*, FORMATS 2007

Fainekos and Pappas, *Robustness of TL specifications for continuous time signals*, TCS (Submitted)

✓ Bounded time TL verification of dynamical systems

Fainekos, Girard and Pappas, *Temporal logic verification using simulation*, FORMATS 2006

Fainekos and Pappas, *MTL Robust Testing for LPV Systems*, RTSS 2008 (Submitted)

✓ Hybrid automata synthesis from TL specifications

Fainekos et al, *Hierarchical Synthesis of Hybrid Controllers from TL Specifications*, HSCC 2007

Fainekos et al, *Temporal Logic Motion Planning for Dynamic Robots*, Automatica (Accepted)

Fainekos, Kress-Gazit and Pappas, *Temporal Logic Motion Planning for Mobile Robots*, ICRA 2005

Fainekos, Kress-Gazit and Pappas, *Hybrid Controllers for Path Planning*, CDC 2005

Talk Overview

Introduction

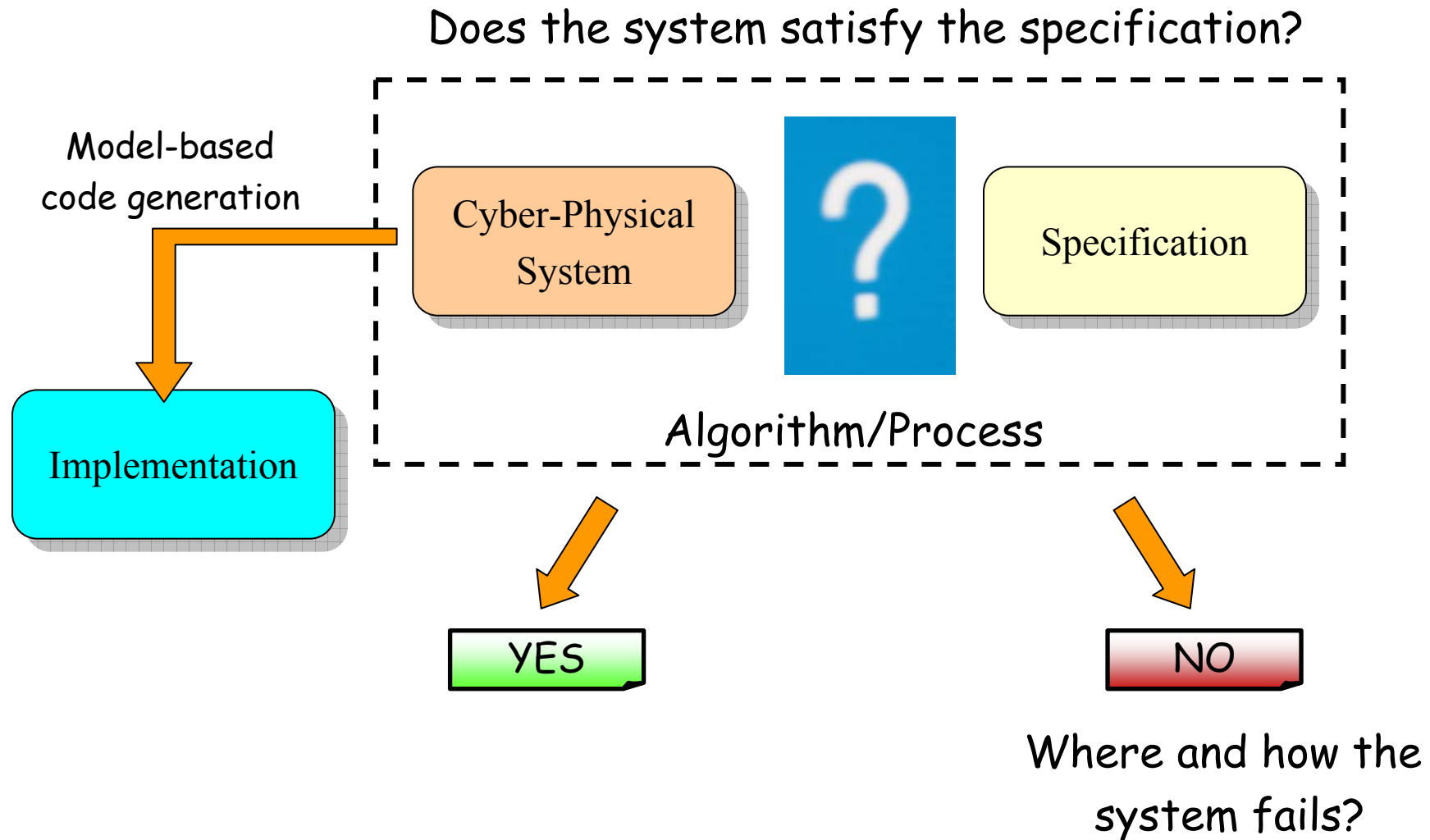
- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

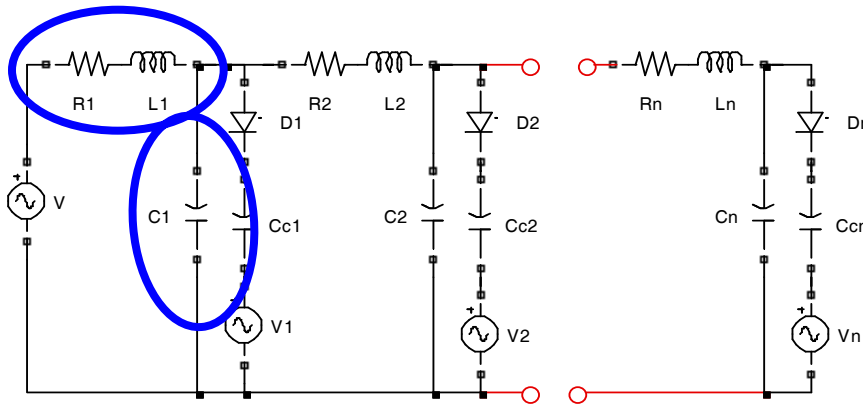
Final remarks - Future work

Certification / Verification



Example : Verifying a transmission line

11



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:

$$\Phi = G p_1 \wedge F_{[0,0.85]} G p_2$$

$$\mathcal{O}(p_1) = [-1.5, 1.5]$$

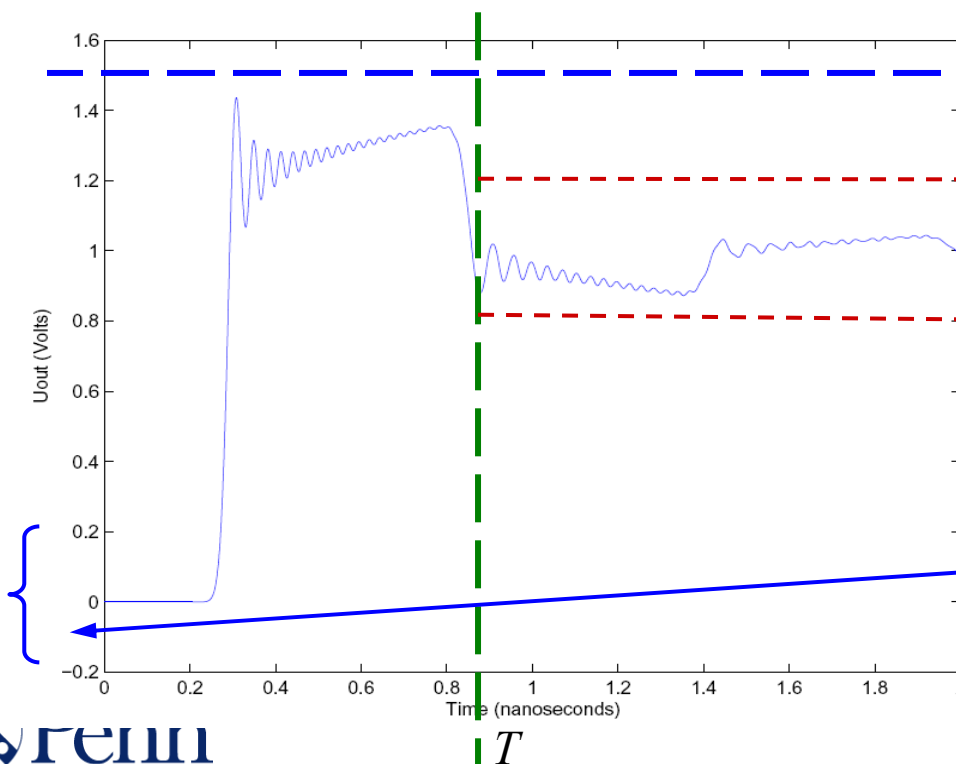
$$\mathcal{O}(p_2) = [0.8, 1.2]$$

Initial conditions:

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

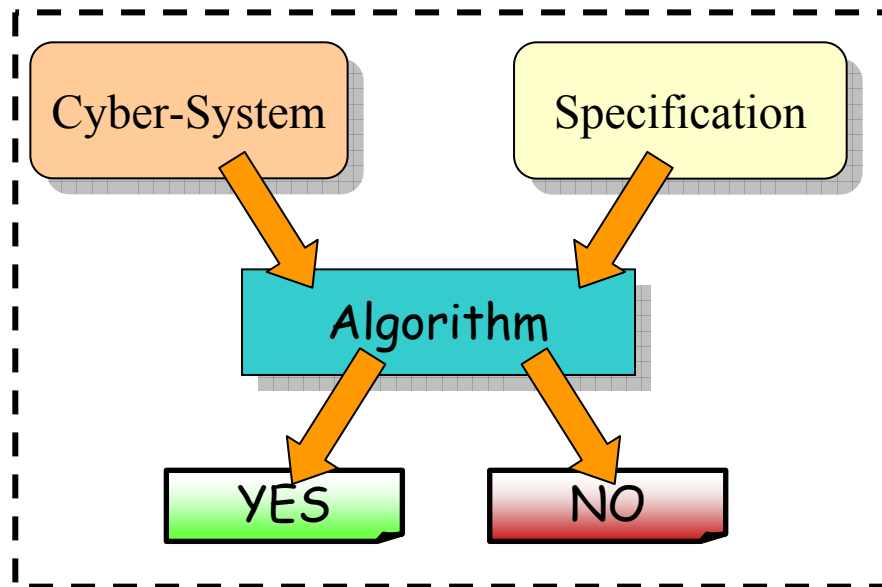
Uncertain parameters

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



What can we verify?

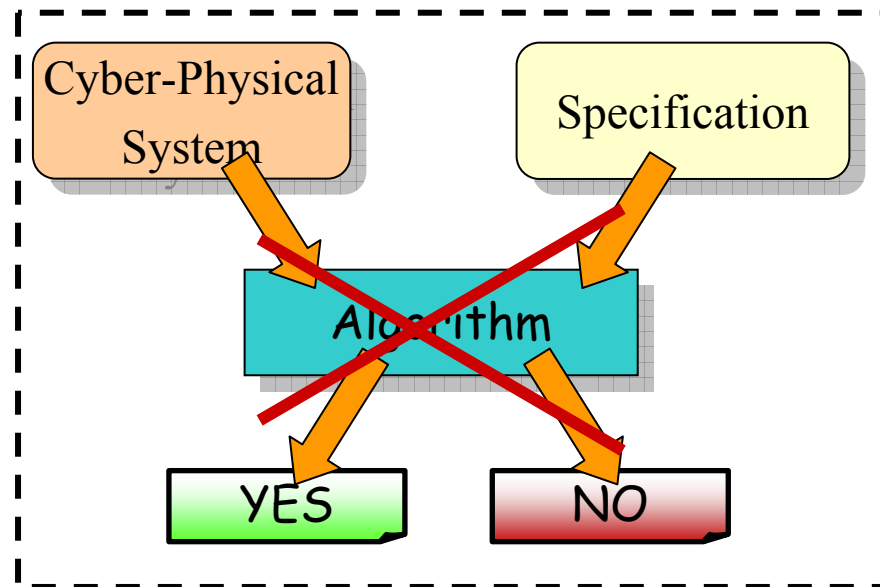
- Verifying **Cyber** systems is a **decidable** problem
 - The Turing award this year was given to the founders of model checking : E. Clark, A. Emerson and J. Sifakis



- Applications in verification of software, hardware, protocols etc.
- Many software toolboxes : SPIN, SMV etc

What about hybrid (embedded) systems?

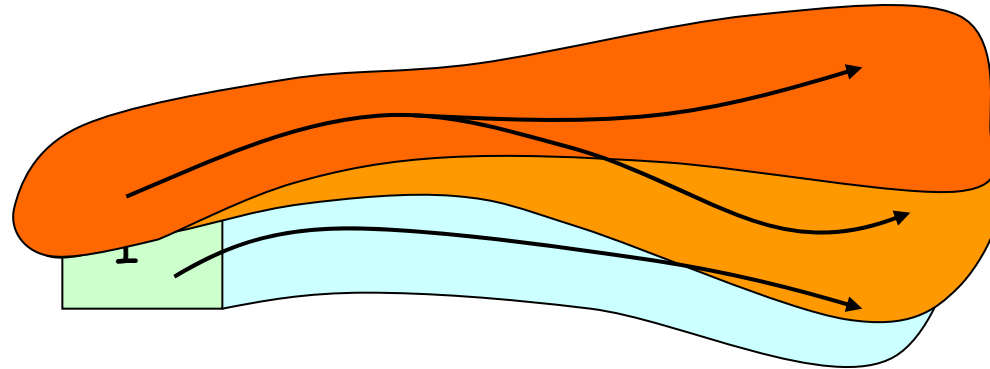
- In general, verifying a hybrid system is **undecidable**
 - R. Alur and C. Courcoubetis and N. Halbwachs and T. A. Henzinger and P.-H. Ho and X. Nicollin and A. Olivero and J. Sifakis and S. Yovine, The algorithmic analysis of hybrid systems, TCS
 - Henzinger, Kopke, Puri, Varaiya, What's decidable about hybrid automata? Proceedings of the twenty-seventh annual ACM symposium on Theory of computing.



What can be done?

- Previous approaches to the undecidability problem :
 - identifying decidable classes :
 - ◆ Alur, Henzinger, Pappas, Lafferriere, ...
 - semi-decidable algorithms :
 - ◆ Krogh, Alur, Henzinger, Dang, Ivančić, Girard, Mitchell, Tomlin, Maler, ...
 - barrier certificates :
 - ◆ Prajna, Jadbabaie, ...
 - systematic simulations / model based testing :
 - ◆ Krogh, Maler, Dang, Lee, Sokolsky, Kumar, Esposito, LaValle, Vardi, ...
- In Practice : **Simulations !**
 - ◆ Schuller, Brangs, Rothfuß, Lutz, Breit: *Development methodology for dynamic stability control systems*, International Journal of Vehicle Design 2002 - Vol. 28, No.1/2/3 pp. 37-56
 - ◆ Gielen, Rutenbar: *Computer-Aided Design of Analog and Mixed-Signal Integrated Circuits*, Proceedings of the IEEE, Vol. 88, No. 12, 2000

ROBUST SIMULATIONS



Advantages :

- ◆ A finite number of simulations
- ◆ Coverage guarantees
- ◆ Scales as well as simulation scales
- ◆ More complicated specifications than safety
- ◆ Almost no parameters to set besides the simulation parameters
- New tools : we need metrics

Talk Overview

Introduction

- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

Metric Temporal Logic (MTL)

Syntax: $\Phi ::= \top \mid \perp \mid p \mid \neg p \mid \Phi_1 \vee \Phi_2 \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \mathcal{U}_I \Phi_2 \mid \Phi_1 \mathcal{R}_I \Phi_2$

until *release*

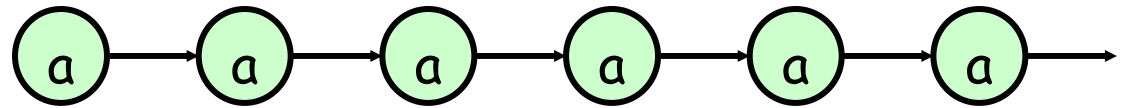
I can be of any bounded or unbounded interval of \mathbb{R}^+ , but $I \neq \emptyset$
 i.e. $I = [0, +\infty)$, $I = [2.5, 9.8]$

Derived operators:

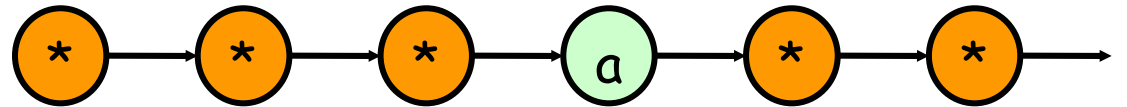
Eventually (in the future) $F_I \Phi := \top \mathcal{U}_I \Phi$
Always (globally) $G_I \Phi := \perp \mathcal{R}_I \Phi$

LTL intuition

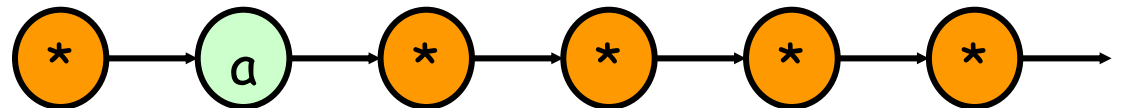
$G a$ - always a



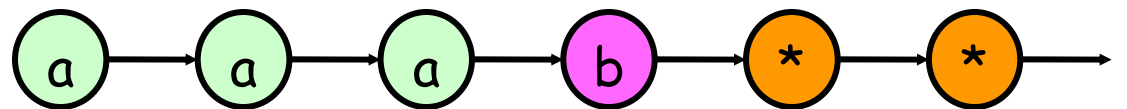
$F a$ - eventually a



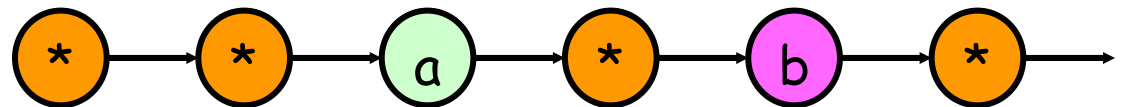
$X a$ - next state a



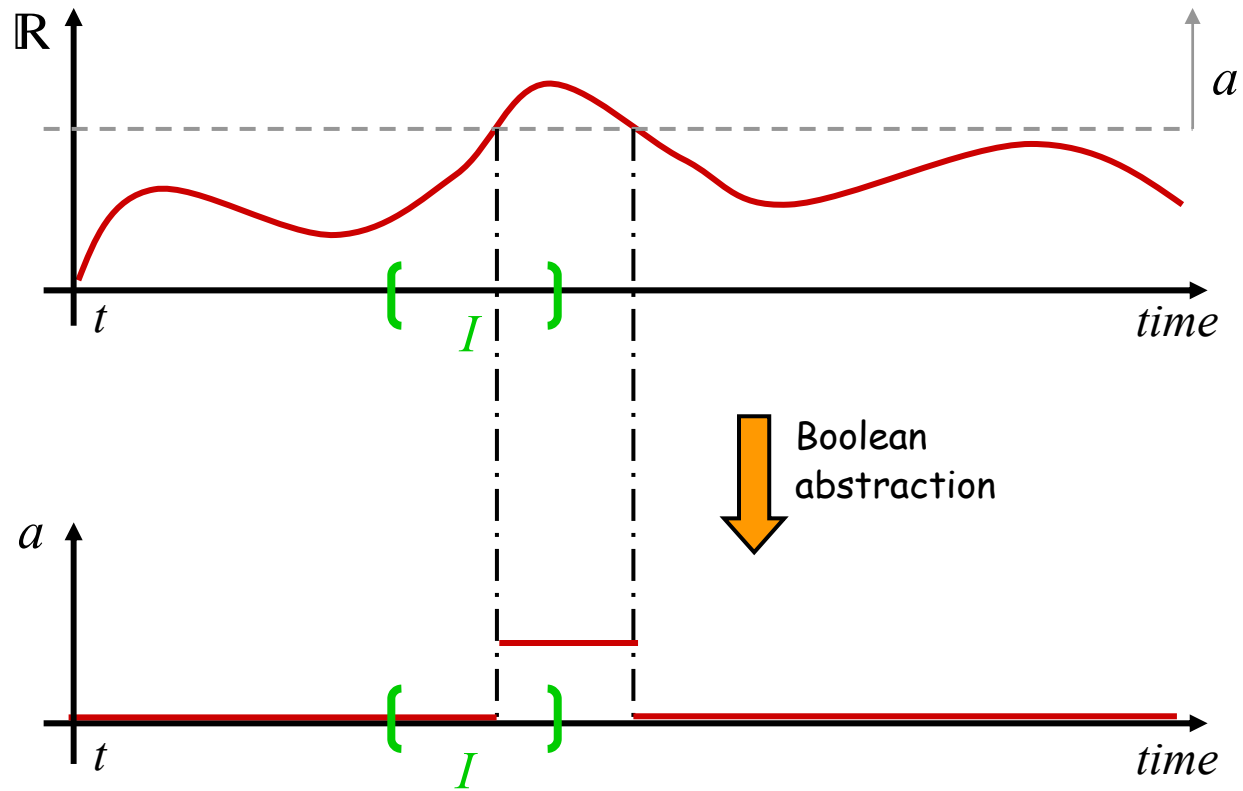
$a U b$ - a until b



$a B b$ - a before b

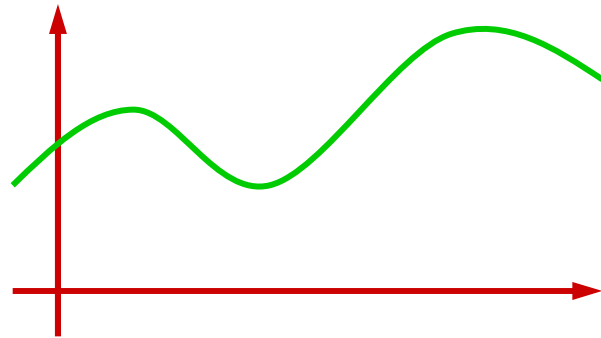


MTL : An example for signals

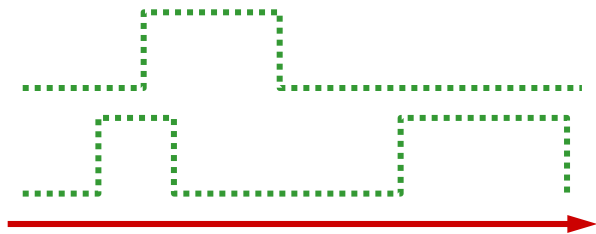


$F_I a$

Temporal Logic Testing



A/D
Boolean
abstraction



LTL / MTL
 $\Phi = G p_1 \wedge F_{[0,T]} G p_2$

Monitoring
Algorithm

Truth Value
 $\{\perp, T\}$

[Maler and Nickovic '04]
 [Thati and Rosu '04]
 [Rosu and Havelund '05]
 [Geilen '01]
 others ...

Talk Overview

Introduction

- Application areas
- Challenges
- Thesis Contributions

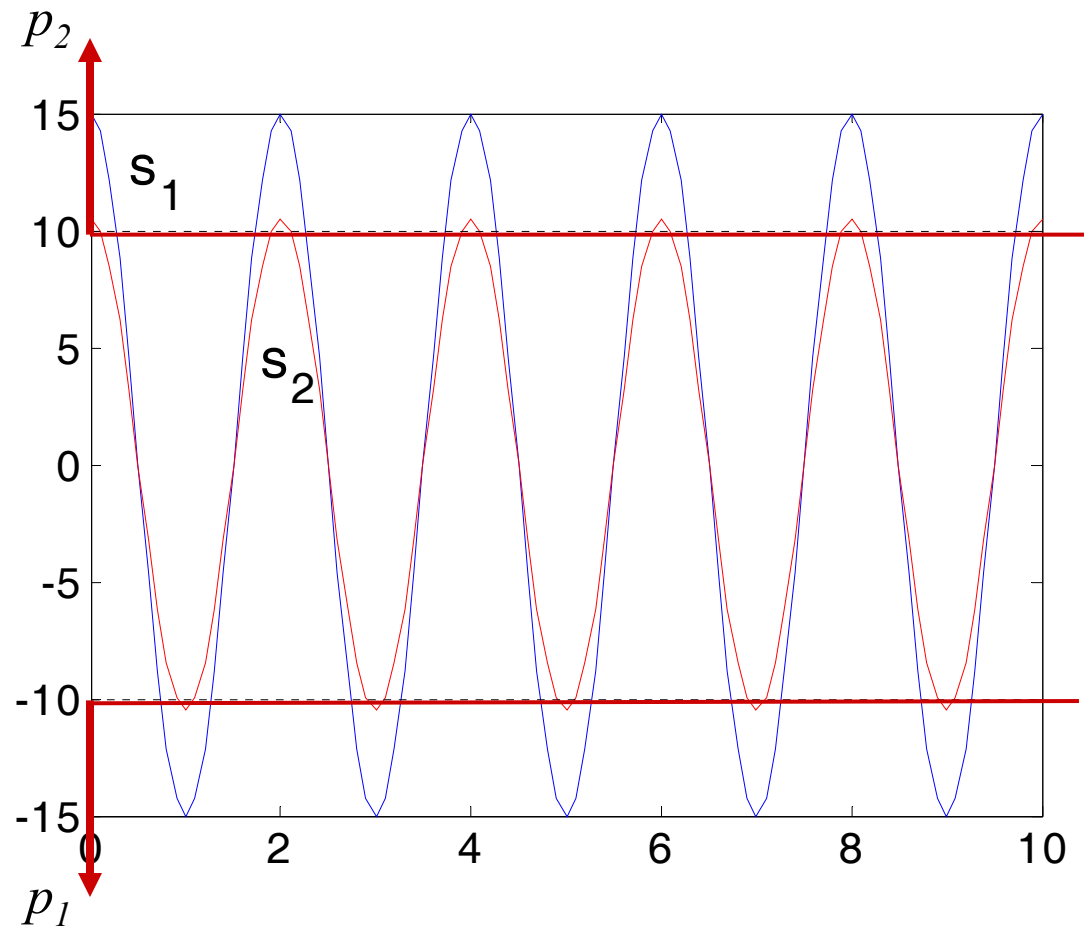
Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

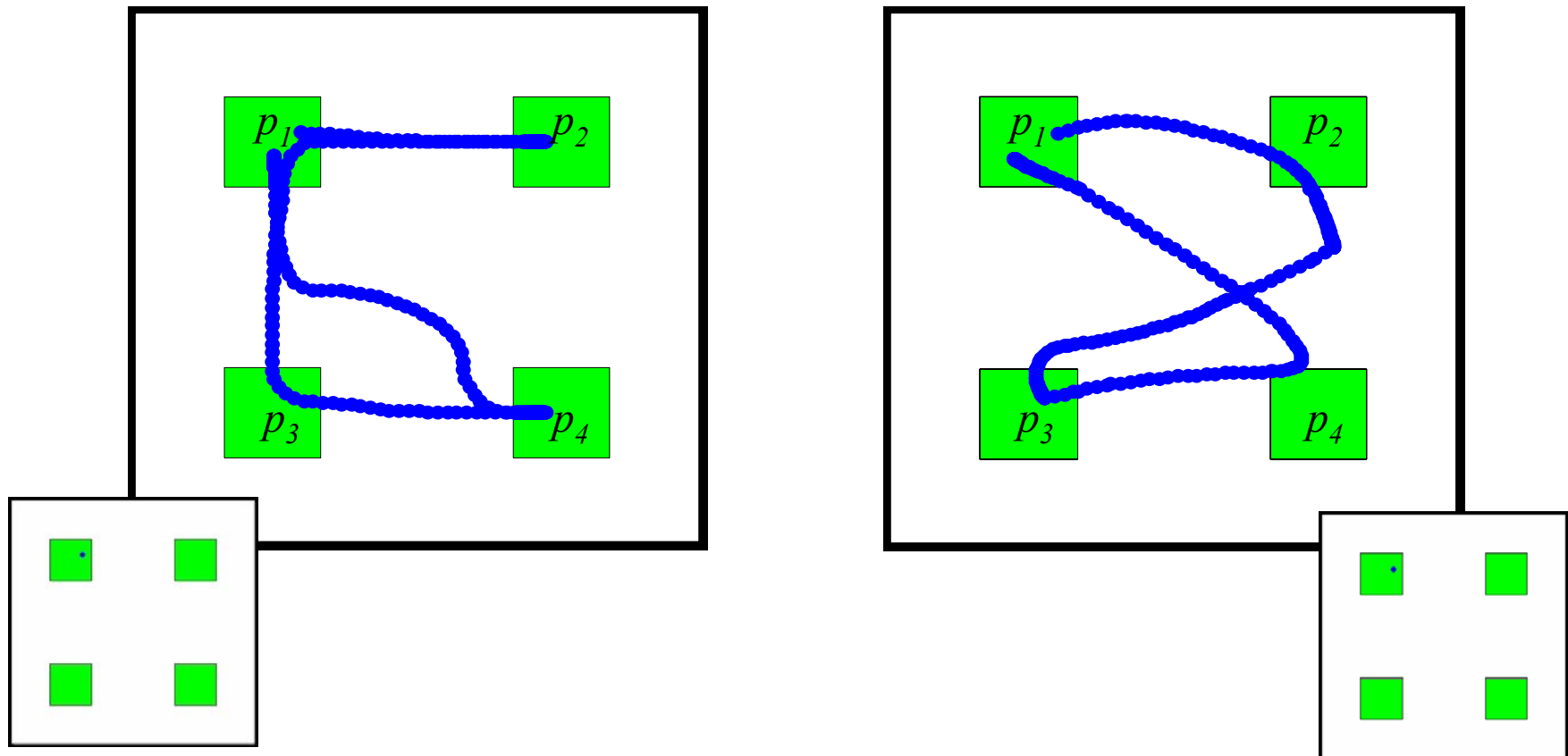
Two signals that satisfy the same spec, but ...

MTL Spec:
 $G(p_1 \rightarrow F_{\leq 2} p_2)$

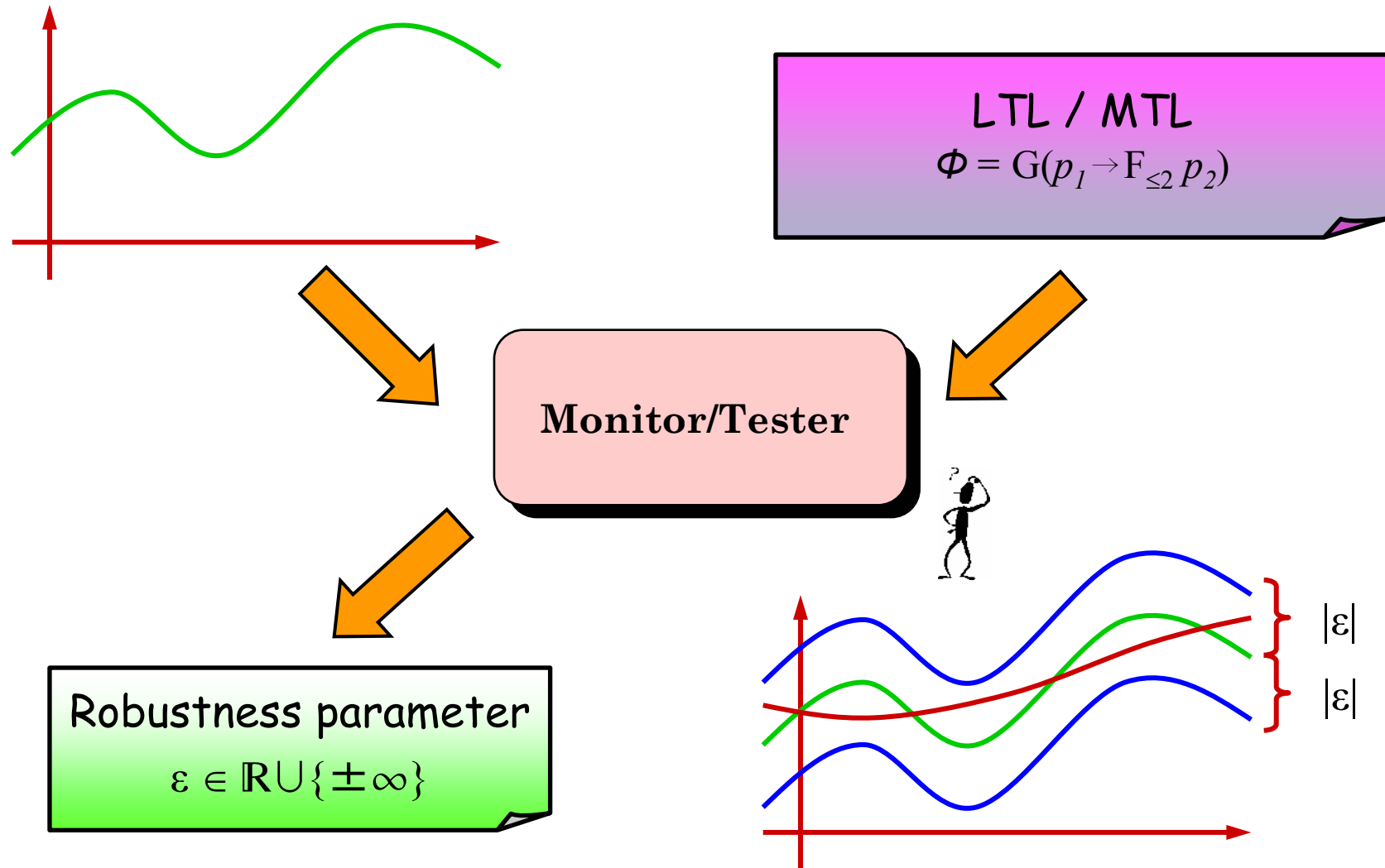


LTL to motion planning

$$F(p_2 \wedge F(p_3 \wedge F(p_4 \wedge \neg(p_2 \vee p_3) \mathcal{U} p_1)))$$



Robustness of Temporal Logics



Fainekos and Pappas, *Robustness of temporal logic specifications*, FATES/RV 2006

Fainekos and Pappas, *Robustness of temporal logic specifications for signals*, Submitted to TCS, 2007

Related Research

➤ Robustness in temporal logics

➤ WRT time :

- Huang, Voeten, Geilen '03, *Real-time property preservation in approximations of timed systems*
- Henzinger, Majumdar, Prabhu '05, *Quantifying similarities between timed systems*
- ...

➤ WRT state :

- de Alfaro, Faella, Stoelinga '04, *Linear and Branching Metrics for Quantitative Transition Systems*
- Lamine, Kabanza '00, *Using fuzzy TL for monitoring behavior-based mobile robots*
- de Alfaro, Faella, Henzinger, Majumdar, Stoelinga '04, *Model Checking Discounted Temporal Properties*
- Huth, Kwiatkowska '97, *Quantitative analysis and model checking*

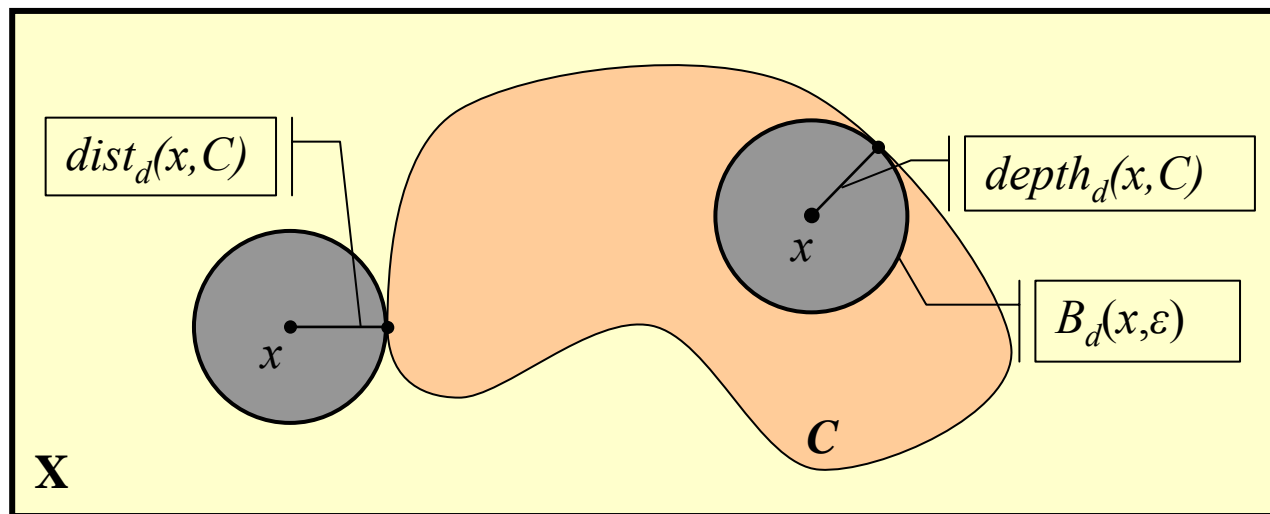
(Signed) Distance

Let $x \in X$ be a point, $C \subseteq X$ be a set and d be a metric. Then we define

$$\text{dist}_d(x, C) := \inf\{d(x, y) \mid y \in \text{cl}(C)\}$$

$$\text{depth}_d(x, C) := \text{dist}_d(x, X \setminus C)$$

$$\text{Dist}_d(x, C) := \begin{cases} -\text{dist}_d(x, C) & \text{if } x \notin C \\ \text{depth}_d(x, C) & \text{if } x \in C \end{cases}$$

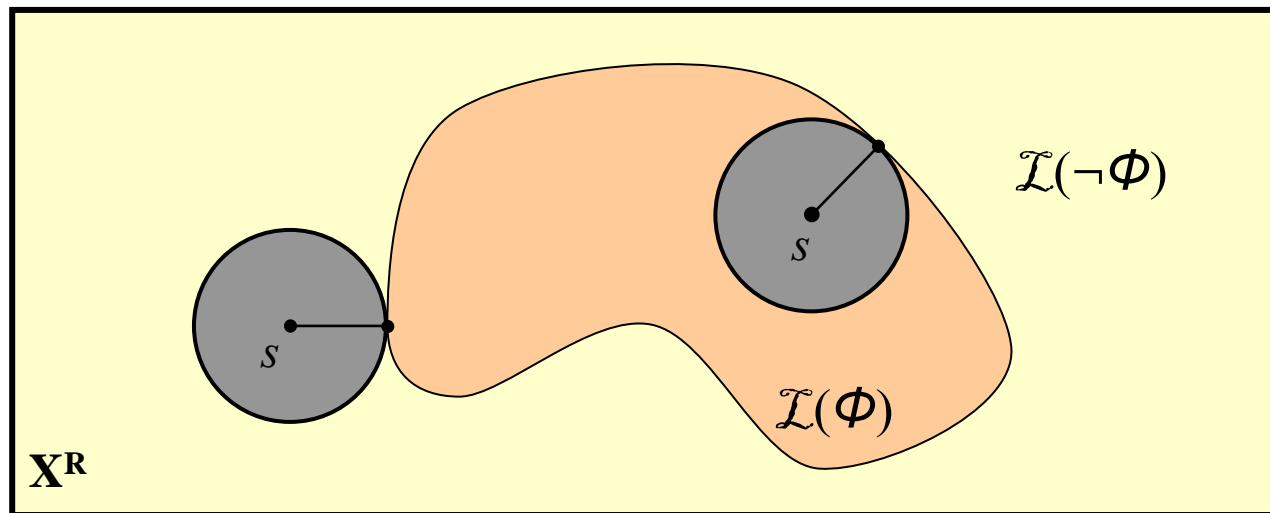


Definition of robustness for signals

Given a signal s , we can define the *robustness degree* as

$$\varepsilon := \mathbf{Dist}_\rho(s, \mathcal{L}(\Phi))$$

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



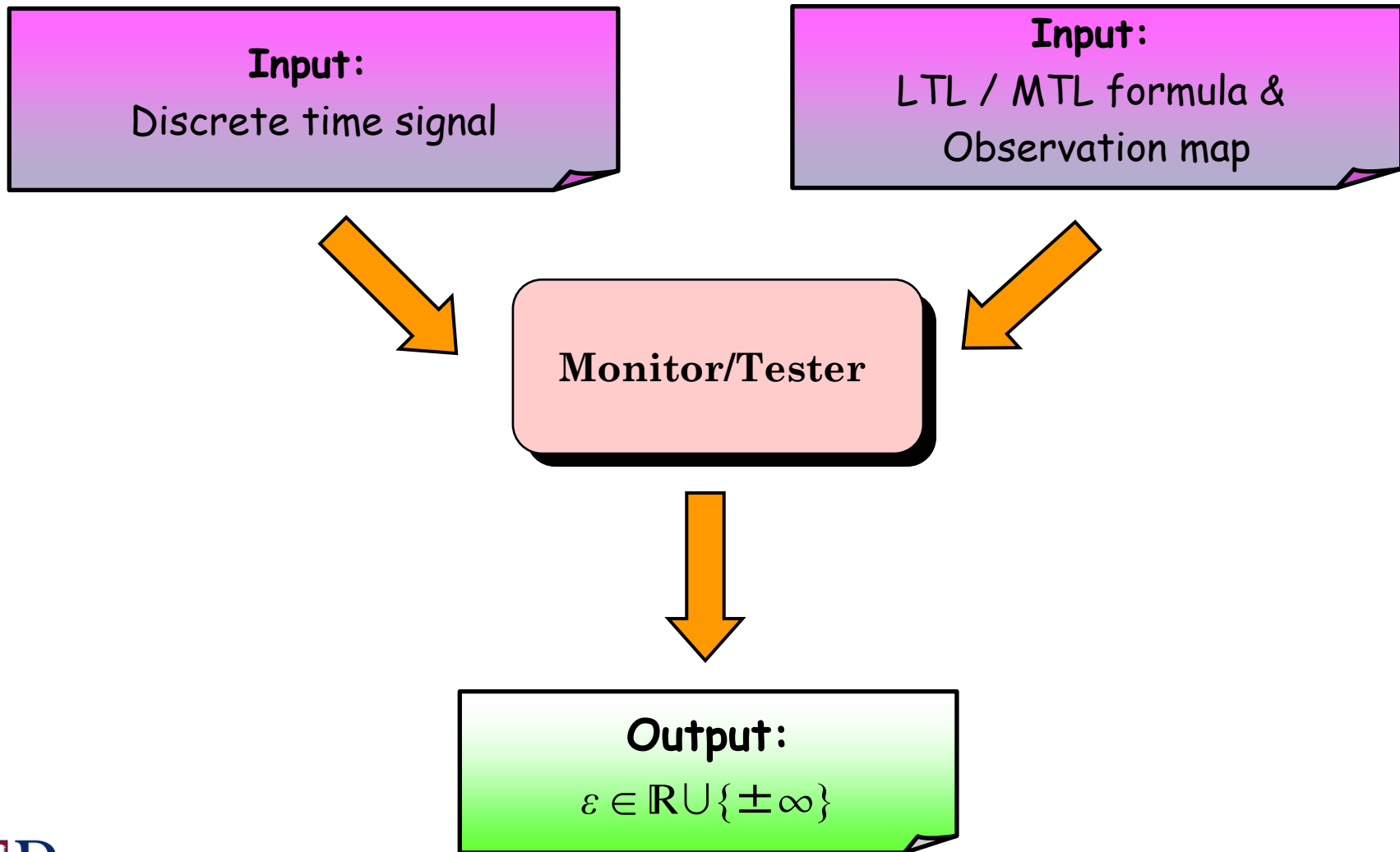
Main result

Theorem: Let Φ be an MTL formula, s be a (continuous or discrete time) signal and $|\varepsilon| > 0$ be the *robustness parameter* of Φ with respect to s , then for all s' in $B_\rho(s, \varepsilon)$ we have that $s \models \Phi$ iff $s' \models \Phi$

Fainekos and Pappas, Robustness of temporal logic specifications, FATES/RV 2006
Fainekos and Pappas, *Robustness of temporal logic specifications for signals*, Submitted to Theoretical Computer Science, 2007
Fainekos and Pappas, *Robustness of temporal logic specifications for finite timed state sequences in metric spaces*, Technical Report MS-CIS-04-32, 2004

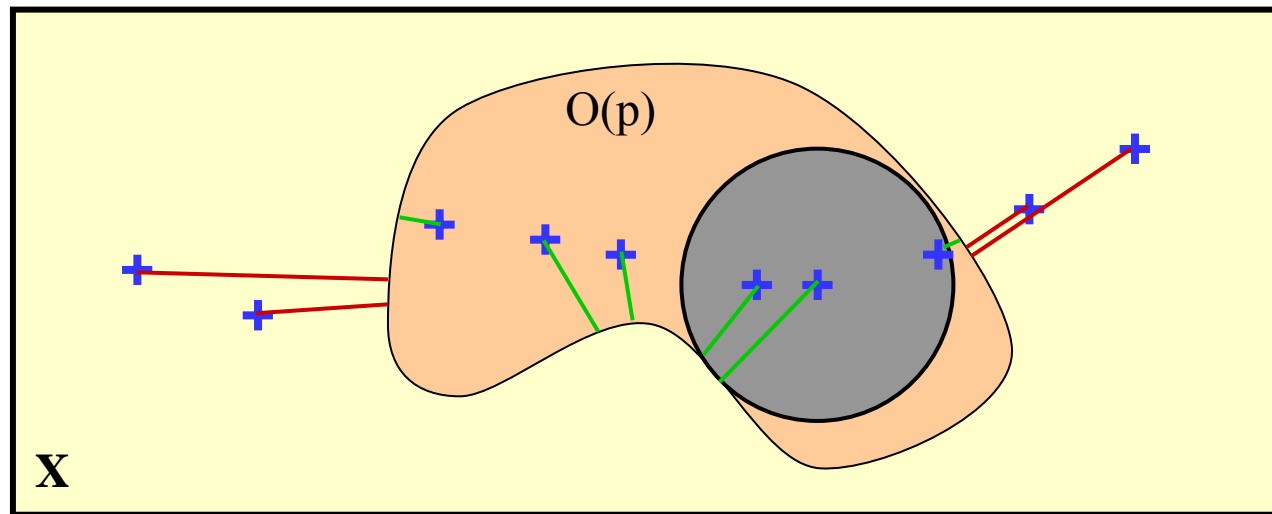
Software toolbox : TaLiRo

Available at : <http://www.seas.upenn.edu/~fainekos/robustness.html>



Intuition - Example

Specification : $Fp = T \mathcal{U} p$

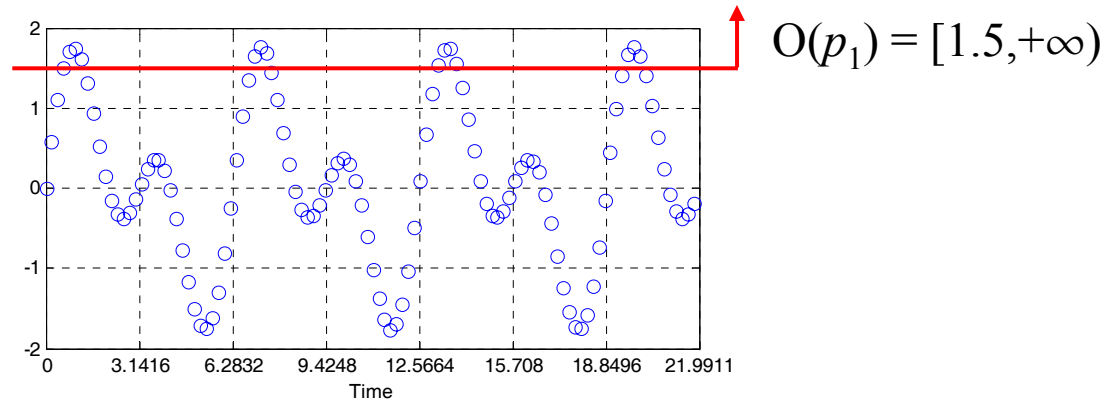


$$\llbracket \phi_1 \mathcal{U}_I \phi_2 \rrbracket_D(\mu, i) = \begin{cases} (K_\epsilon^\infty(0, \mathcal{I}) \cap \llbracket \phi_2 \rrbracket_D(\mu, i)) \sqcup \\ \sqcup \left(\llbracket \phi_1 \rrbracket_D(\mu, i) \cap \llbracket \phi_1 \mathcal{U}_{I-\delta\tau(i)} \phi_2 \rrbracket_D(\mu, i+1) \right) & \text{if } i < \max N \\ K_\epsilon^\infty(0, \mathcal{I}) \cap \llbracket \phi_2 \rrbracket_D(\mu, i) & \text{otherwise} \end{cases}$$

Running TaLiRo on a Dell PowerEdge 1650

33

$$s(i) = \sin \tau(i) + \sin 2\tau(i)$$
$$\tau(i) = 0.2i$$

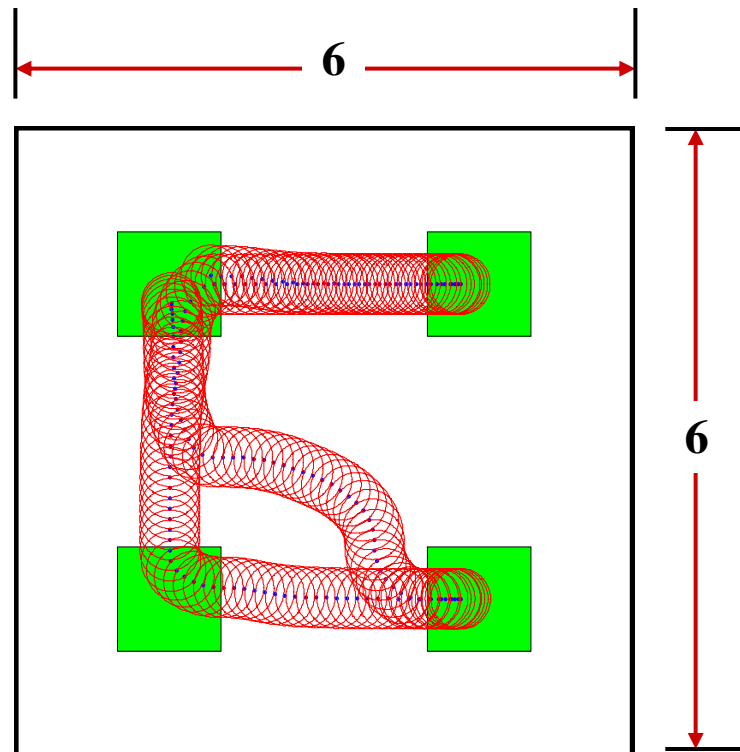


$$G(p_1 \rightarrow F_{(0.0,1.0)} \neg p_1)$$

signal's time domain	number of samples	computation time (sec)	robustness
[0, 21.99]	110	0.00	0.097603
[0, 188.49]	943	0.03	0.097603
[0, 6283.2]	31,416	1.05	0.092065
[0, 219911.48]	1,099,558	37.61	0.091793

Guaranteed correctness under noise and uncertainty

$$F_{I_2}(p_2 \wedge F_{I_3}(p_3 \wedge F_{I_4}(p_4 \wedge \neg(p_2 \vee p_3) \mathcal{U}_{II} p_1)))$$



Assume:
sensor accuracy ± 0.1

Robustness estimate

$$\varepsilon = 0.28872$$

Talk Overview

Introduction

- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

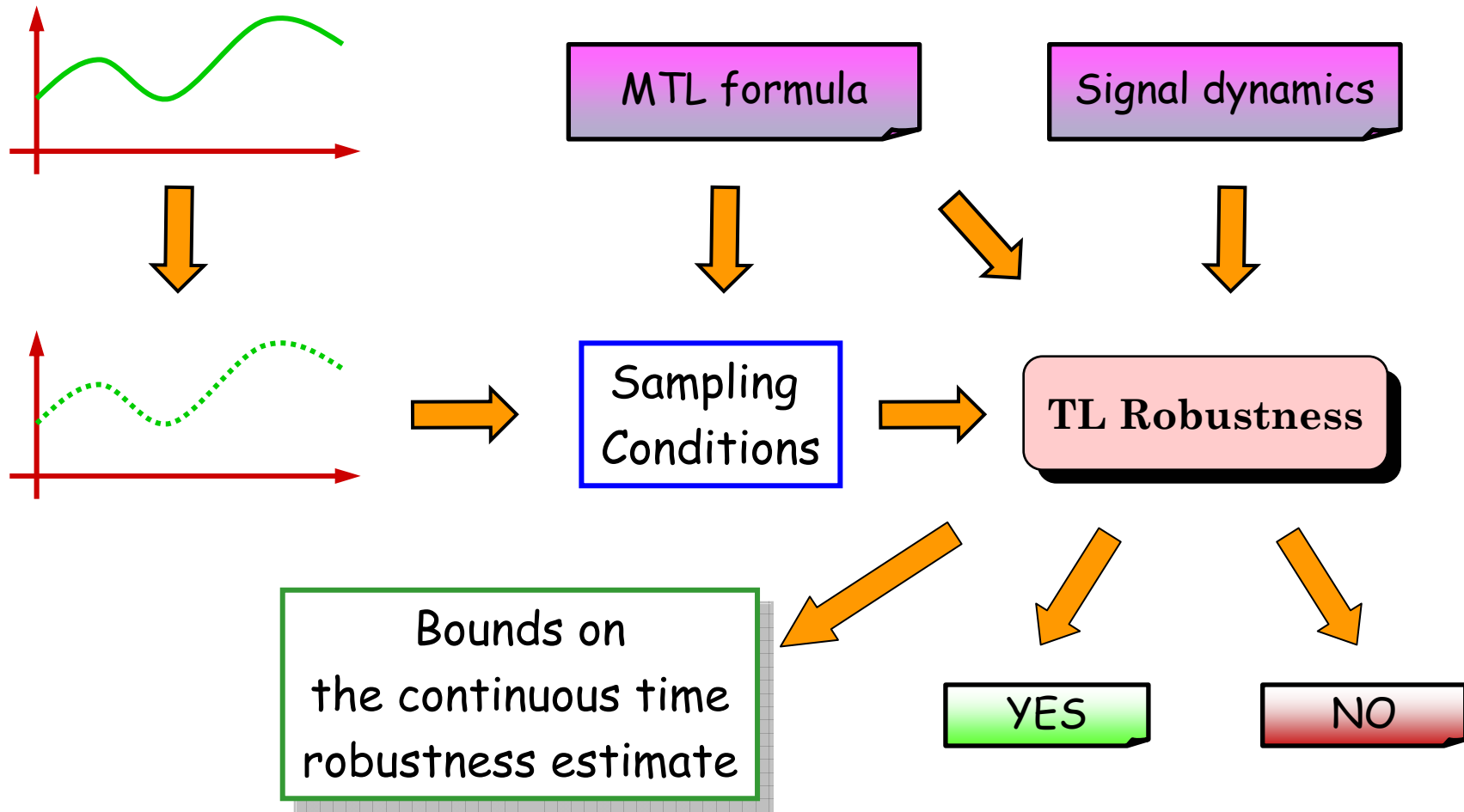
- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals

- ◆ From Discrete Time to Continuous Time
- ◆ From Signals to Systems

- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

From Discrete to Continuous Time

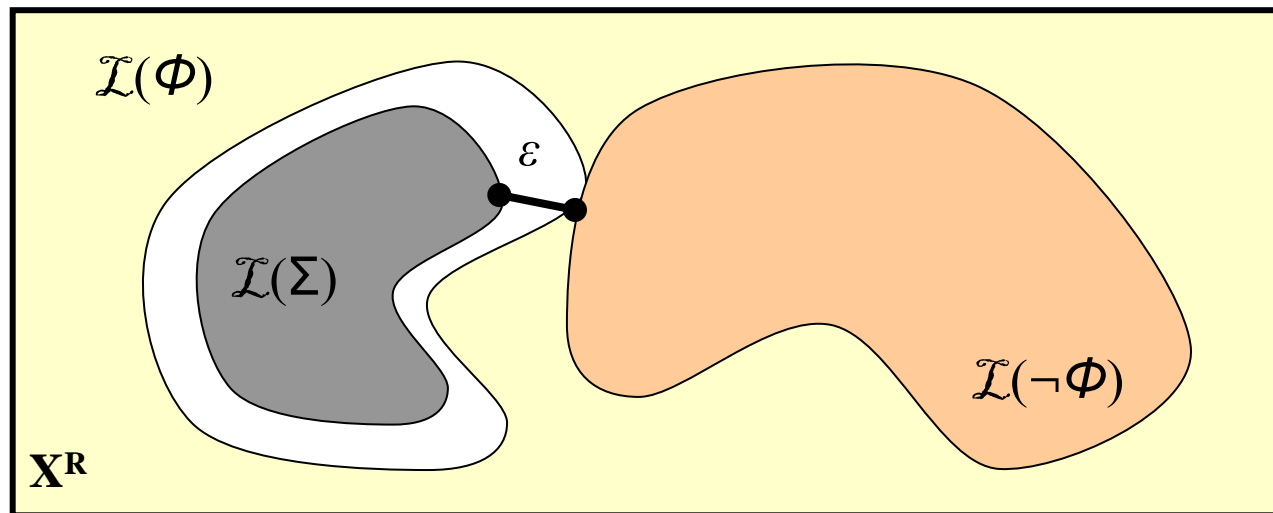


From Signals to Systems

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

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

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



Talk Overview

Introduction

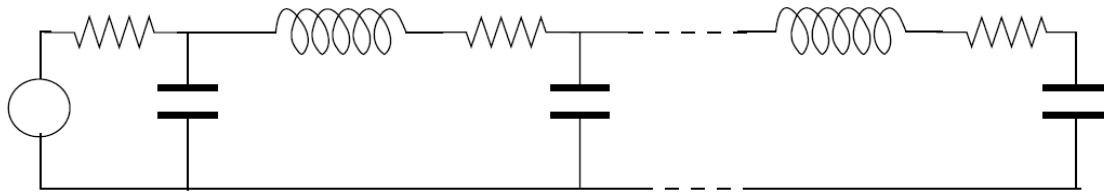
- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

Example : a study of transient dynamics



System (dim 81):

$$\dot{x}(t) = Ax(t) + bU_{in}(t)$$

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

Step input ($t > 0$):

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

Steady state at $t = 0^-$:

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

Property:

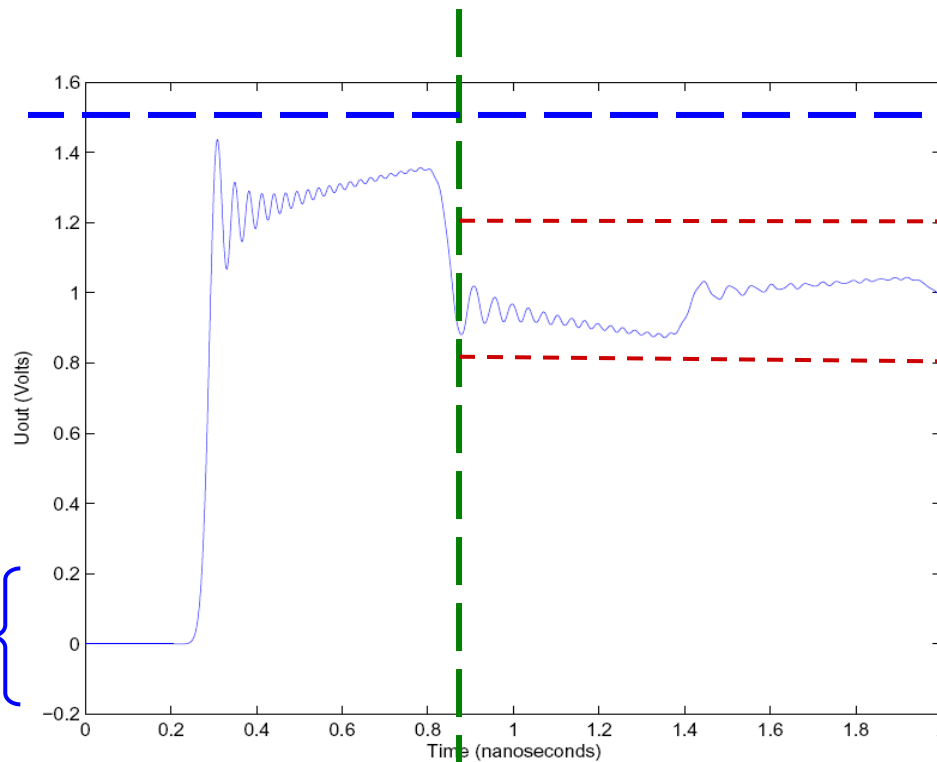
$$\Phi = G p_1 \wedge F_{[0,T]} G p_2$$

$$\mathcal{O}(p_1) = [-1.5, 1.5]$$

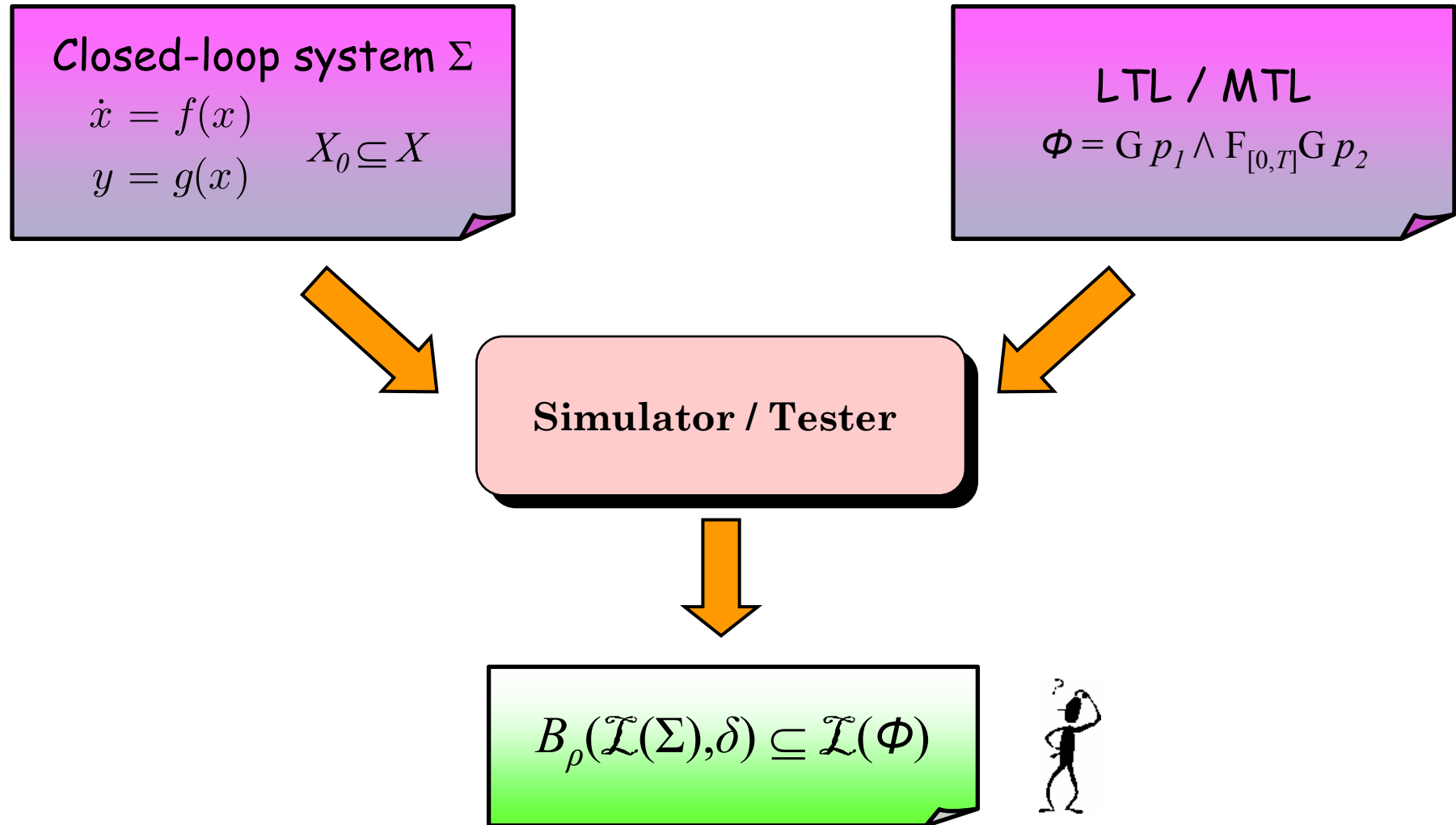
$$\mathcal{O}(p_2) = [0.8, 1.2]$$

Initial conditions:

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



Robust TL testing of analog systems



Fainekos, Girard and Pappas, *Temporal logic verification using simulation*, FORMATS 2006

Fainekos and Pappas, *MTL Robust Testing for LPV Systems*, RTSS 2008 (Submitted)



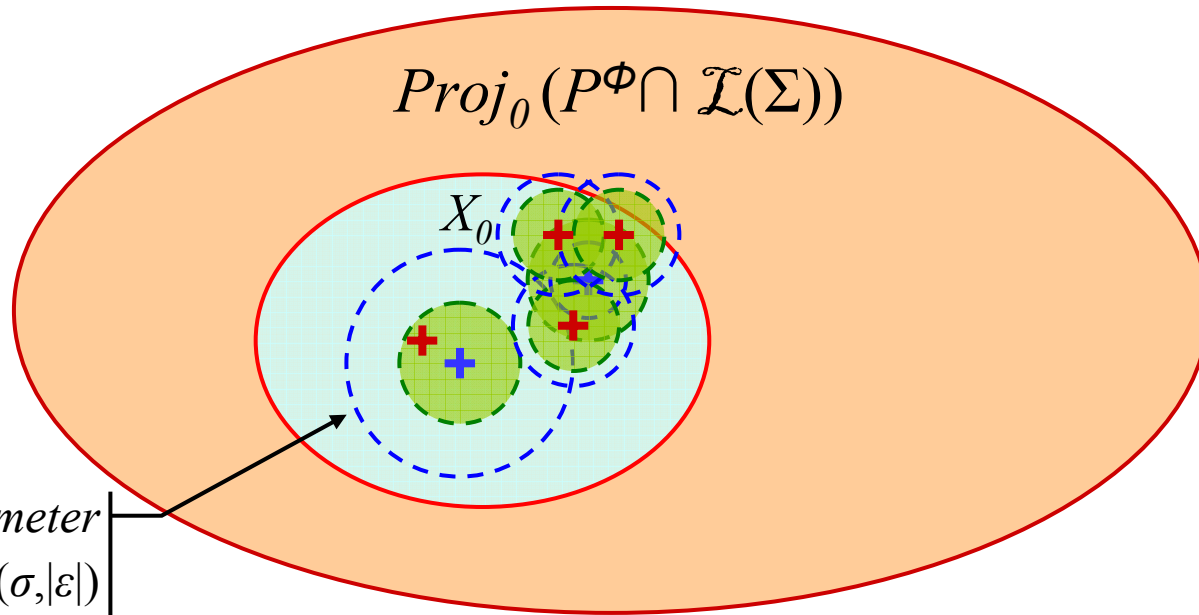
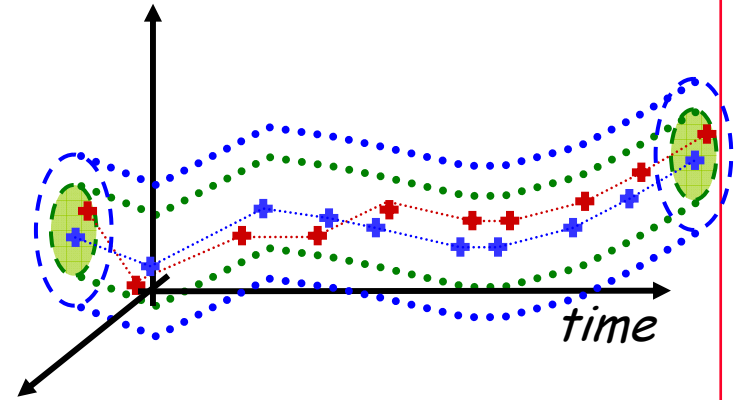
Related Research

- **Verification/Testing of Analog Systems (using TL)**
 - Hartong, Hedrich, Barke '02, *On Discrete Modeling and Model Checking for Nonlinear Analog Systems*
 - Ghosh, Vemuri '99, *Formal Verification of Synthesized Analog Designs*
 - Frehse, Krogh, Rutenbar, Maler '05, *Time Domain Verification of Oscillator Circuit Properties*
 - Gupta, Krogh, Rutenbar '04, *Towards Formal Verification of Analog Designs*
 - Donze, Maler '07, *Systematic Simulation using Sensitivity Analysis*

Main idea

Closed-loop system Σ :
 $\dot{x} = f(x)$
 $y = g(x)$
 $X_0 \subseteq X$
 Specification Φ

$$\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)$$



ϵ robustness parameter
 $B_\rho(\sigma, |\epsilon|)$

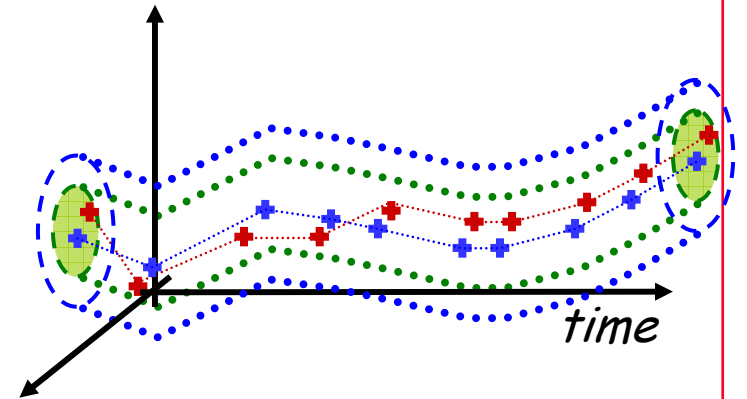
Achieving coverage I

Closed-loop system Σ :

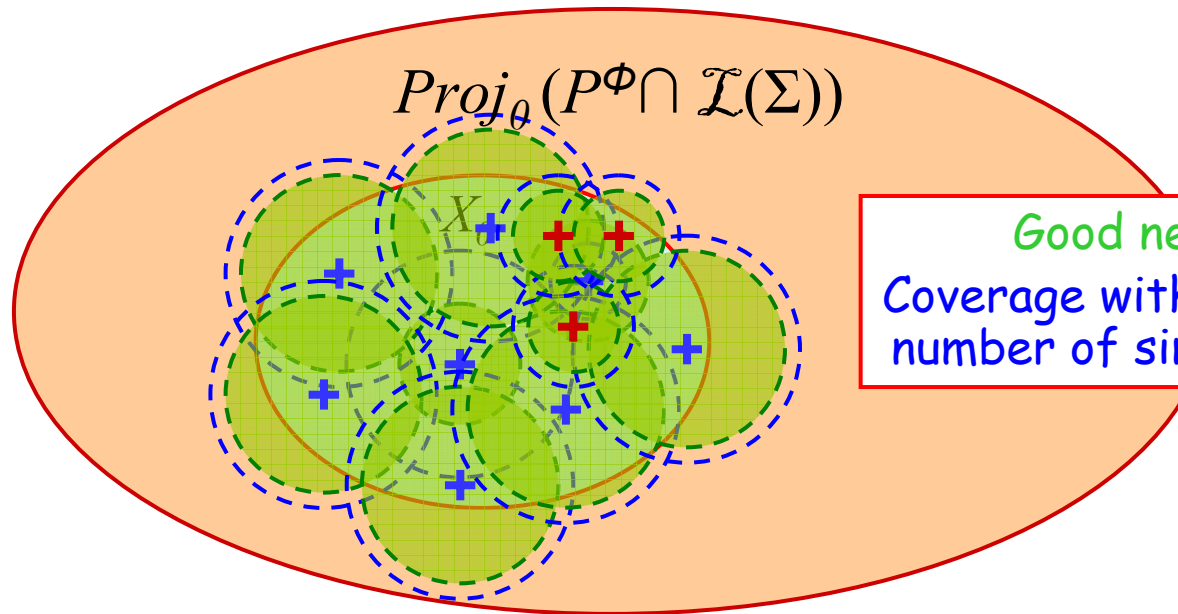
$$\begin{aligned} \dot{x} &= f(x) \\ y &= g(x) \end{aligned} \quad X_0 \subseteq X$$

Specification Φ

$$\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)$$



$$\text{Proj}_\theta (P^\Phi \cap \mathcal{L}(\Sigma))$$



Good news!
Coverage with a finite
number of simulations

Computing bisimulation functions

Quadratic Bisimulation Functions for Deterministic Linear Systems

$$\begin{array}{l} \dot{x} = Ax \\ y = Cx \end{array} \rightarrow y$$

$$V(x) = \sqrt{x^T M x}$$

is a bisimulation function if

$$M \geq C^T C$$

$$A^T M + M A \leq 0$$

Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

WeA16.4

Approximate Bisimulations for Constrained Linear Systems

Antoine Girard and George J. Pappas

Bisimulation Functions using Sum Of Squares Relaxation

$$\begin{array}{l} \dot{x} = f(x) \\ y = g(x) \end{array} \rightarrow y$$

$$V(x_1, x_2) = \sqrt{q(x_1, x_2)}$$

is a bisimulation function if

$$q(x_1, x_2) - \|g_1(x_1) - g_2(x_2)\|^2 \text{ is SOS}$$

$$-\frac{\partial q(x_1, x_2)}{\partial x_1} f_1(x_1) - \frac{\partial q(x_1, x_2)}{\partial x_2} f_2(x_2) \text{ is SOS}$$

Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

MoB01.3

Approximate Bisimulations for Nonlinear Dynamical Systems

Antoine Girard and George J. Pappas

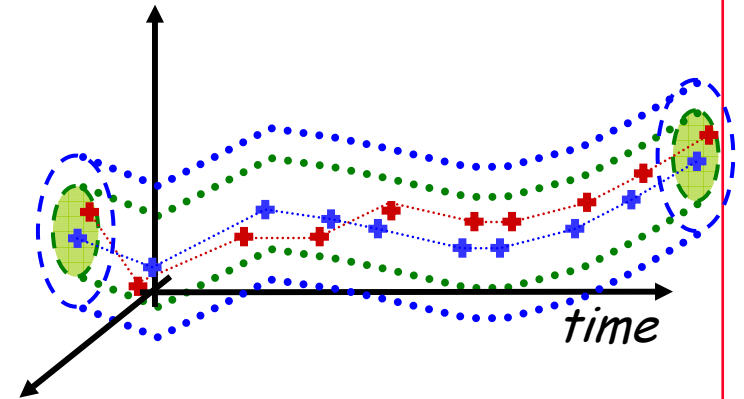
Achieving coverage II

Closed-loop system Σ :

$$\begin{aligned} \dot{x} &= f(x) \\ y &= g(x) \end{aligned} \quad X_0 \subseteq X$$

Specification Φ

$$\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)$$



$$\text{Proj}_0(P^\Phi \cap \mathcal{L}(\Sigma))$$

X_0



Even better news!
It is possible to verify
the system with
just one simulation

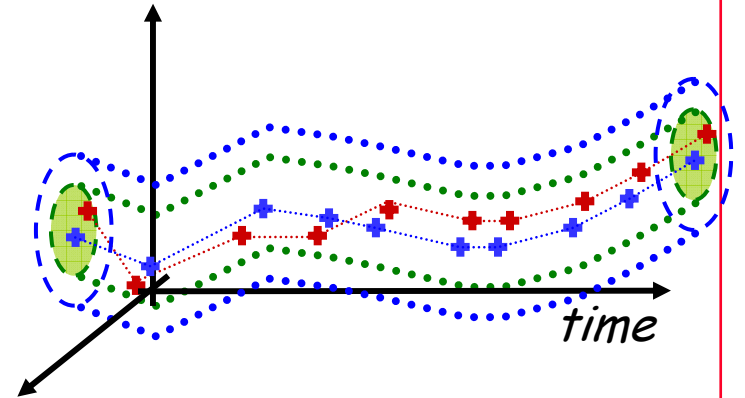
Quick falsification

Closed-loop system Σ :

$$\begin{aligned} \dot{x} &= f(x) \\ y &= g(x) \end{aligned} \quad X_0 \subseteq X$$

Specification Φ

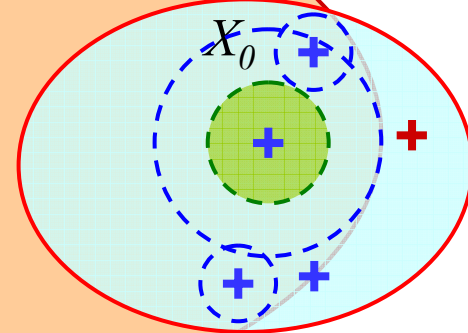
$$\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)$$



$$\text{Proj}_0(P^\Phi \cap \mathcal{L}(\Sigma))$$

Observation!

A robust system with respect to the property requires less simulations



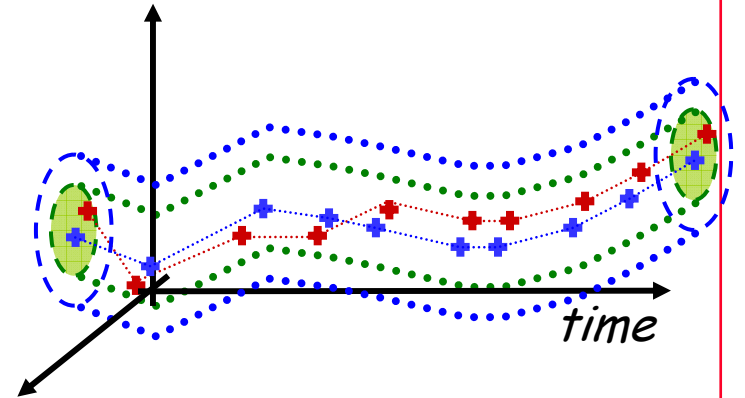
Coverage certificates

Closed-loop system Σ :

$$\begin{aligned} \dot{x} &= f(x) \\ y &= g(x) \end{aligned} \quad X_0 \subseteq X$$

Specification Φ

$$\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)$$



$$\text{Proj}_0(P^\Phi \cap \mathcal{L}(\Sigma))$$

 X_0

Good news!

We get coverage guarantees after K iterations.

Main results

48

Theorem: Let V be a bisimulation function, let (x_1, y_1) be a trajectory of Σ , ε be the robustness parameter of Φ wrt y_1 and $\delta > 0$, then for any other trajectory (x_2, y_2) such that $V(x_1(0), x_2(0)) < \varepsilon - \delta$ implies that the robustness parameter of Φ wrt y_1 is greater or equal to δ .

Proposition: Let V be a bisimulation function. For any compact set of initial conditions $X_0 \subseteq \mathbb{R}$, for all $\zeta > 0$, there exists a finite set of points $\{x_1, \dots, x_r\} \subseteq X_0$ such that
for all $x \in X_0$, there exists x_i , such that $V(x, x_i) \leq \zeta$



Main results

49

Theorem: Let $(x_1, y_1), \dots, (x_r, y_r)$ be trajectories of Σ such that $\mathbf{Disc}(X_0, \zeta) = \{x_1(0), \dots, x_r(0)\}$. Let ε_i be the robustness parameter of Φ wrt y_i . Then,

$$\forall i \in \{1, \dots, r\} . \varepsilon_i > \zeta + \delta \implies B_\rho(\mathcal{L}(\Sigma), \delta) \subseteq \mathcal{L}(\Phi)$$

Proposition: If Σ_1 is δ -approximately simulated by Σ_2 and

$$B_\rho(\mathcal{L}(\Sigma_2), \delta) \subseteq \mathcal{L}(\Phi)$$

then

$$\mathcal{L}(\Sigma_1) \subseteq \mathcal{L}(\Phi)$$

Fainekos, Girard and Pappas, *Temporal logic verification using simulation*, FORMATS 2006

Fainekos, *Robustness of Temporal Logic Specifications*, PhD Thesis 2008

Fainekos and Pappas, *MTL Robust Testing for LPV Systems*, RTSS 2008 (Submitted)



Verification example

Consider the linear system with dynamics

$$A = \begin{bmatrix} 0.025 & -2.5 \\ 0.5 & -1 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

with initial conditions

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

Verify that it satisfies the specification

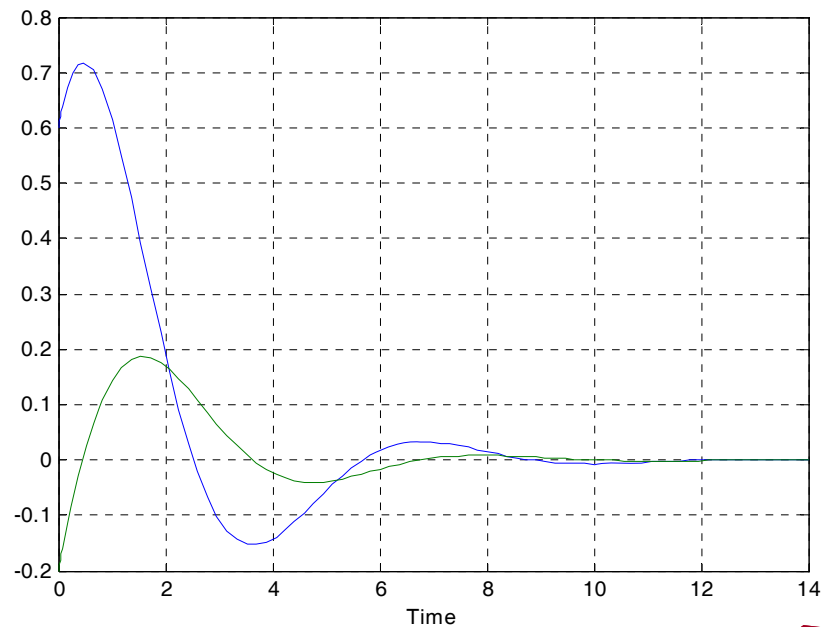
$$\Phi = G p_1 \wedge G_{[8, \infty]} p_2$$

where

$$O(p_1) = \mathbb{R} \times [-0.6, 0.6] \text{ and}$$

$$O(p_2) = [-0.4, 0.4] \times [-0.4, 0.4]$$

with robustness $\delta = 0.2125$ over the time domain $[0, 14]$.



Verification example - Initialization

Compute the bisimulation function $V(x) = \sqrt{x^T M x}$

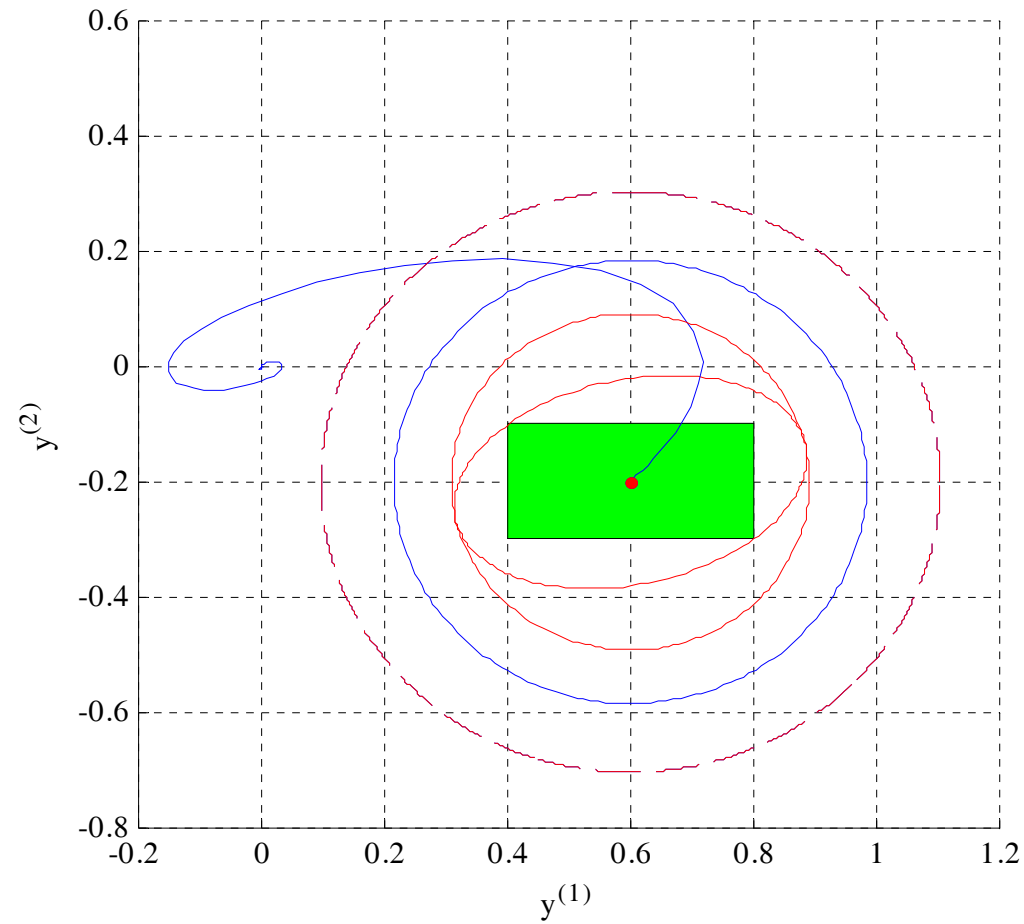
$$\left. \begin{array}{l} M \geq C^T C \\ A^T M + M A \leq 0 \end{array} \right\} \Rightarrow M = \begin{bmatrix} 1.0940 & -0.3895 \\ -0.3895 & 2.6142 \end{bmatrix}$$

Choose as first point the center x_c of the hyper-rectangle

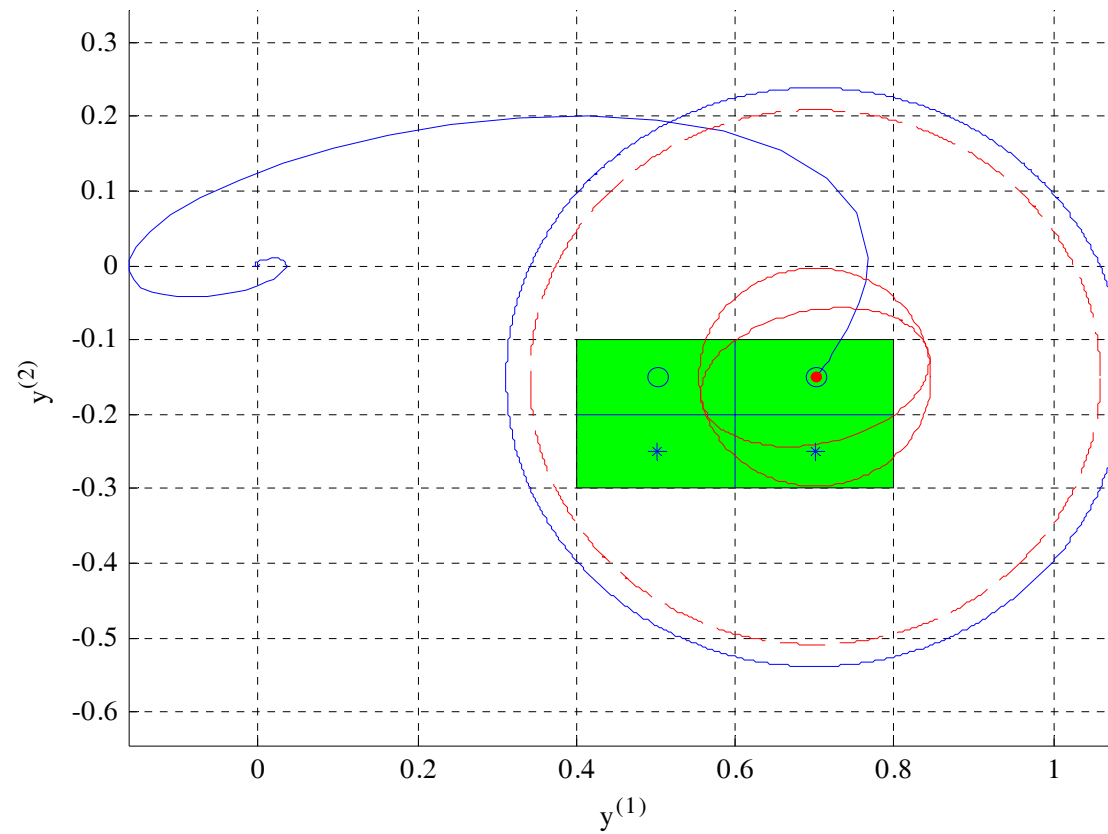
Compute the maximum value of the bisimulation function of all the points in the set X_0 relative to x_c

Verification example - First test

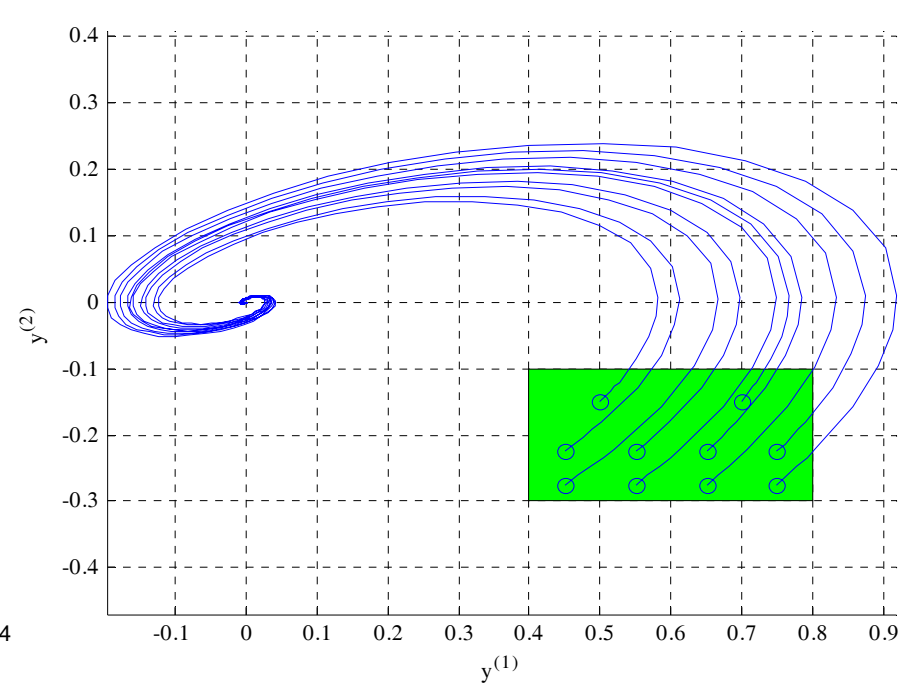
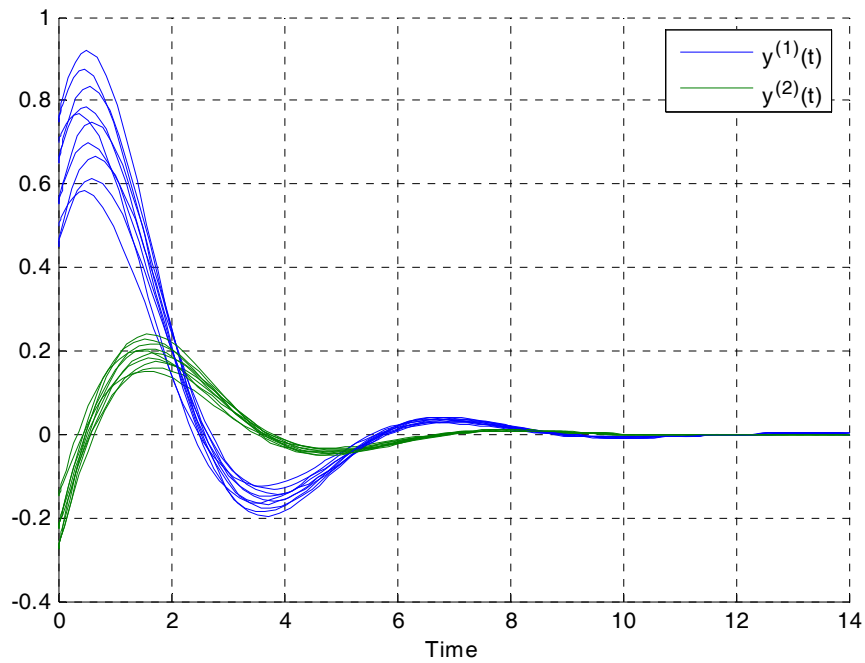
52



Verification example - 2nd iteration



Verification example - 3rd iteration



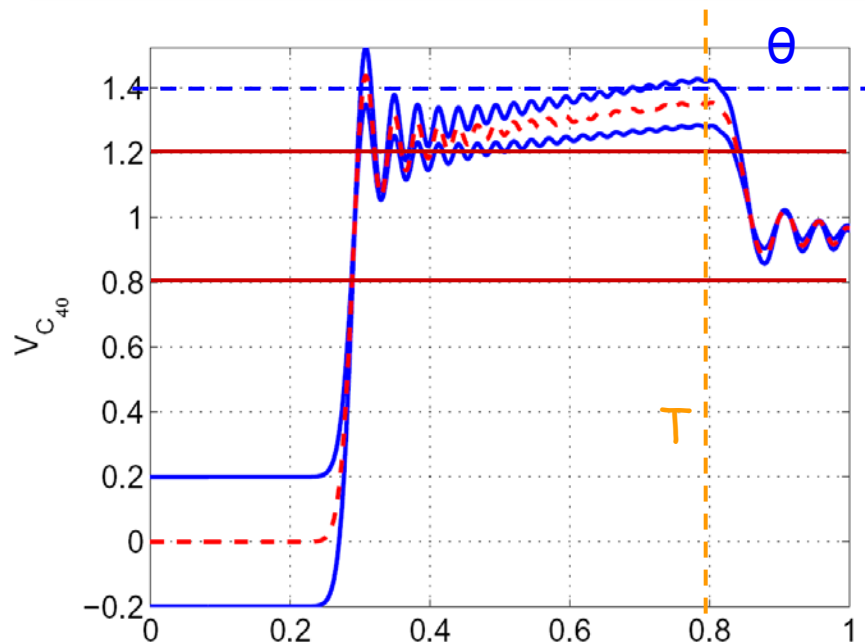
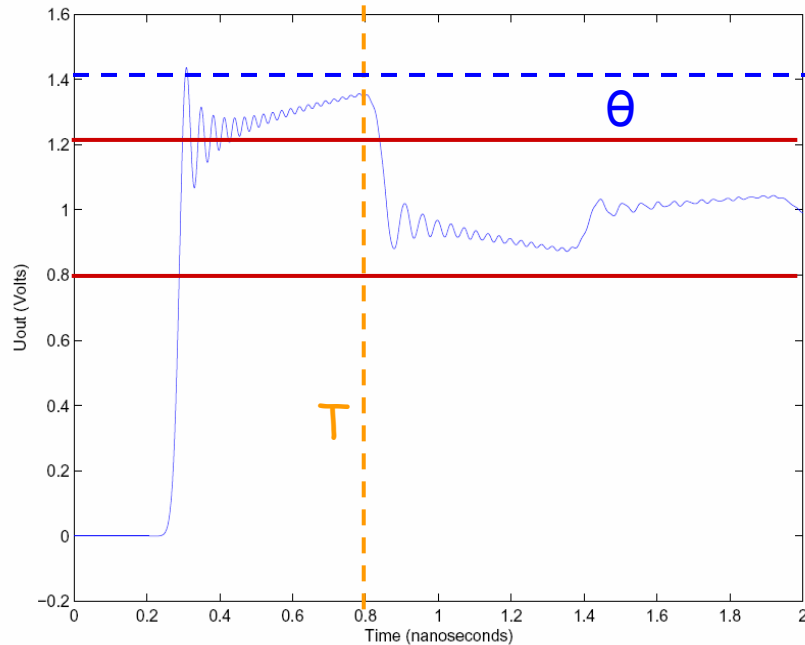
Experimental Results

(MATLAB toolbox)

Property:

$$\Phi = G p_1 \wedge F_{[0,T]} G p_2$$

$$\mathcal{O}(p_1) = [-\theta, \theta], \quad \mathcal{O}(p_2) = [0.8, 1.2]$$



from Zhi Han's PhD Thesis 2005

	T=0.8	T=1.2	T=1.6
$\theta=1.4$	False 1	False 1	False 1
$\theta=1.5$	False 1	False 15	False 13
$\theta=1.6$	False 1	True 17	True 7

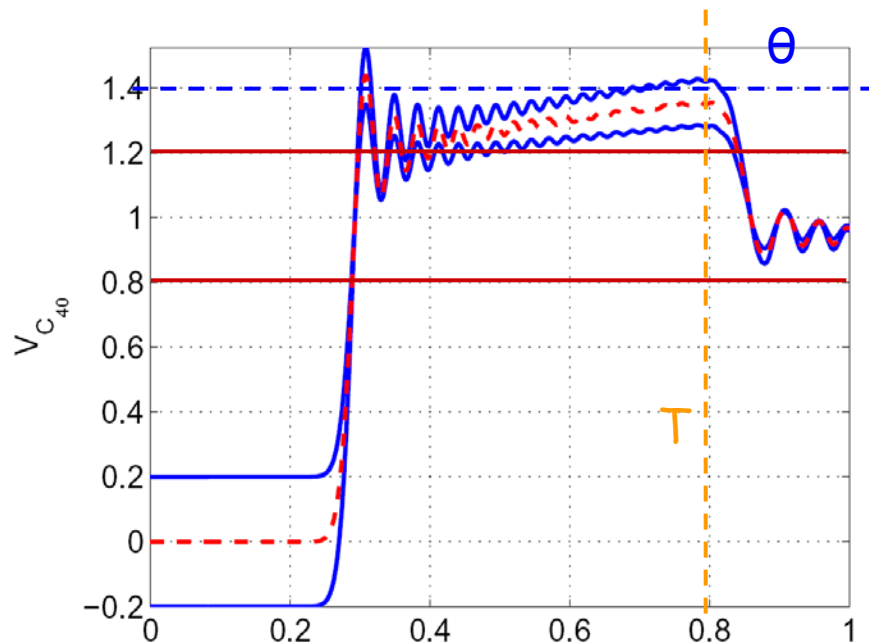
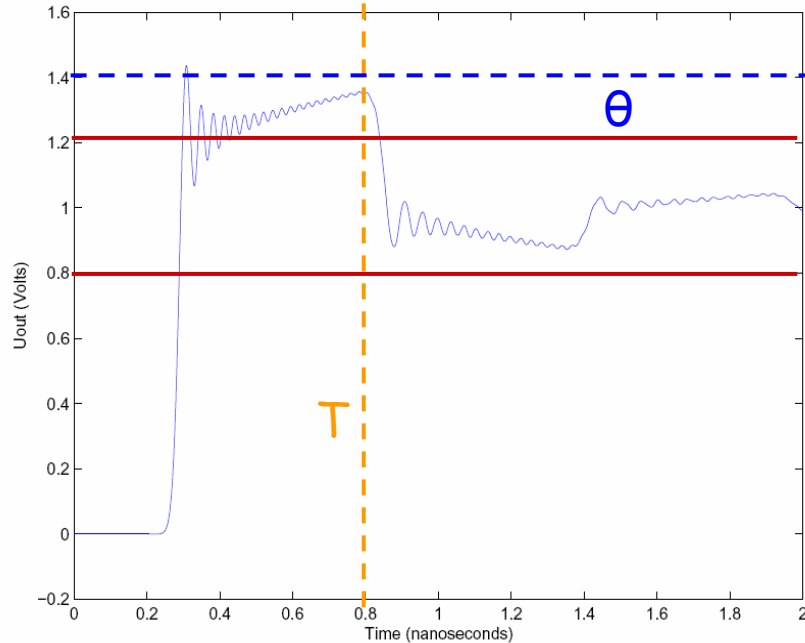
Experimental Results

(MATLAB toolbox)

Property:

$$\Phi = G p_1 \wedge F_{[0,T]} G p_2$$

$$\mathcal{O}(p_1) = [-\theta, \theta], \quad \mathcal{O}(p_2) = [0.8, 1.2]$$



from Zhi Han's PhD Thesis 2005

	T=0.8	T=1.2	T=1.6
$\theta=1.4$	False 1	False 1	False 1
$\theta=1.5$	False 1	False 15	False 13
$\theta=1.6$	False 1	True 17	True 7

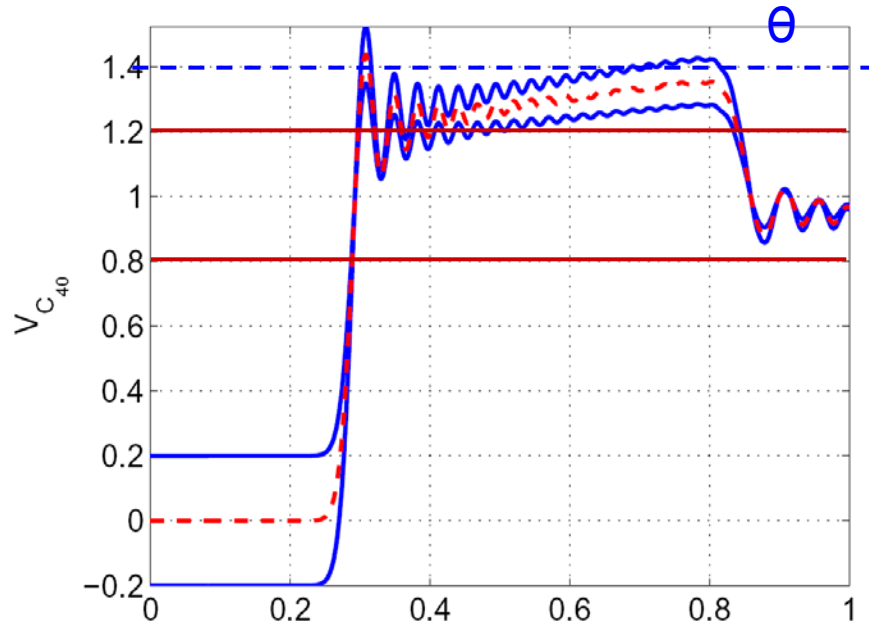
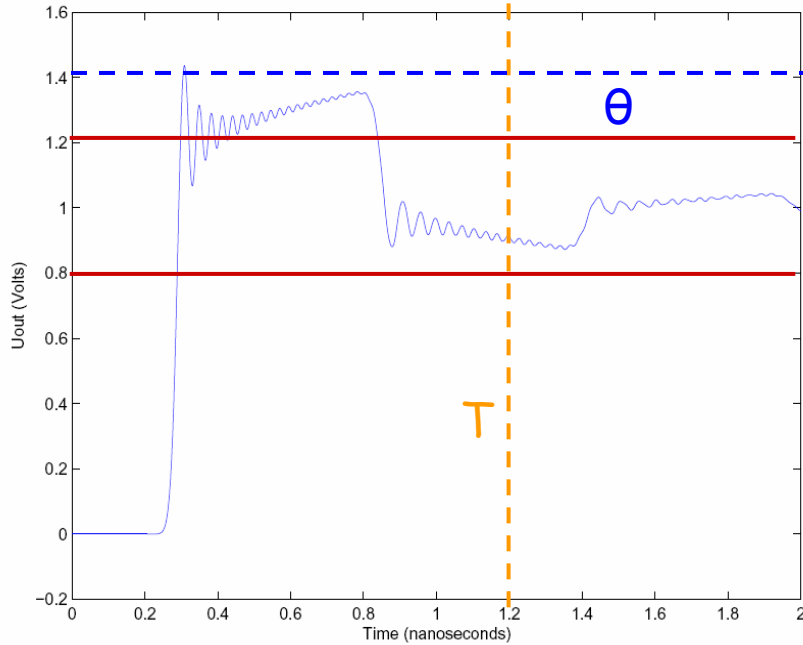
-0.1526

Experimental Results (MATLAB toolbox)

Property:

$$\Phi = G p_1 \wedge F_{[0,T]} G p_2$$

$$\mathcal{O}(p_1) = [-\theta, \theta], \quad \mathcal{O}(p_2) = [0.8, 1.2]$$



from Zhi Han's PhD Thesis 2005

	T=0.8	T=1.2	T=1.6
θ=1.4	False 1	False 1	False 1
θ=1.5	False 1	False 15	False 13
θ=1.6	False 1	True 17	True 7

-0.0298

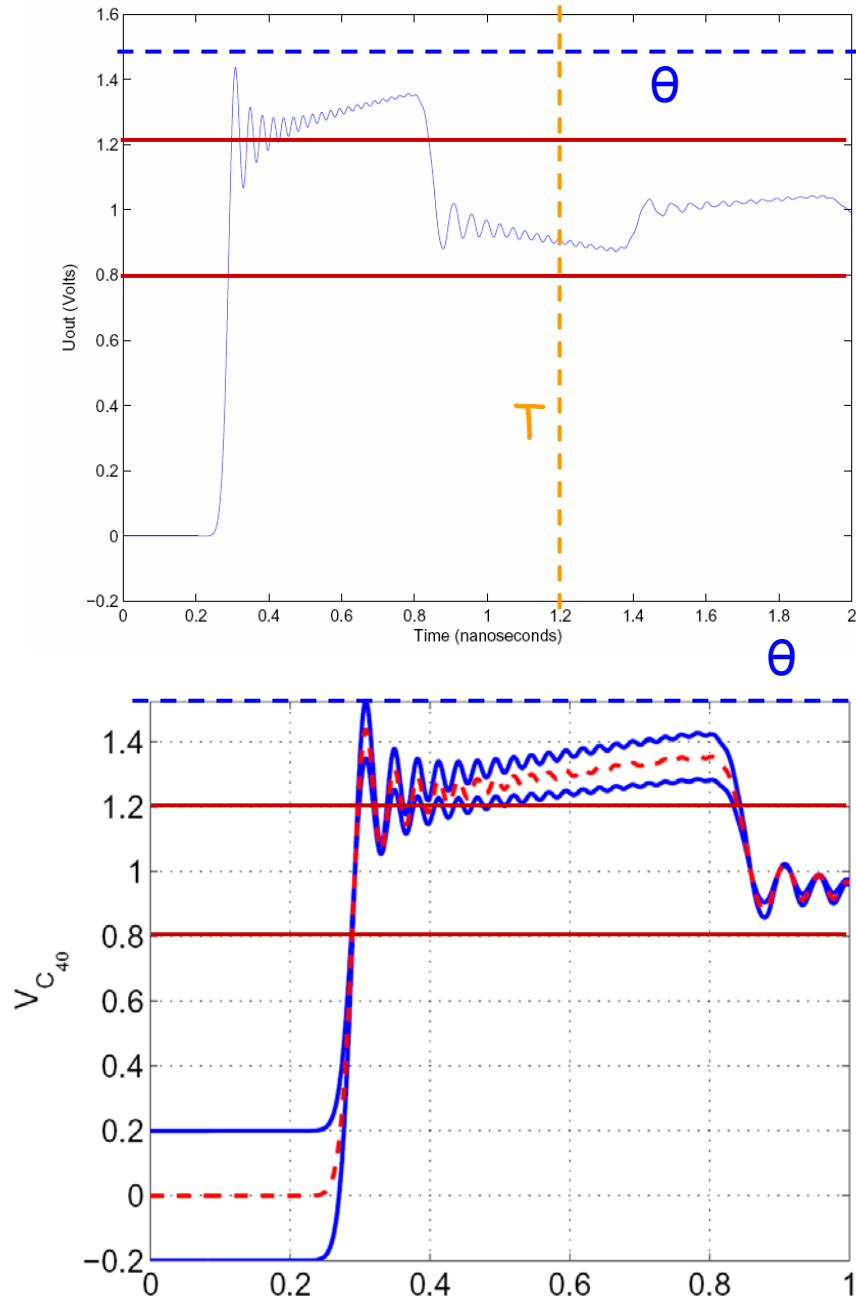
Experimental Results

(MATLAB toolbox)

Property:

$$\Phi = G p_1 \wedge F_{[0,T]} G p_2$$

$$\mathcal{O}(p_1) = [-\theta, \theta], \quad \mathcal{O}(p_2) = [0.8, 1.2]$$

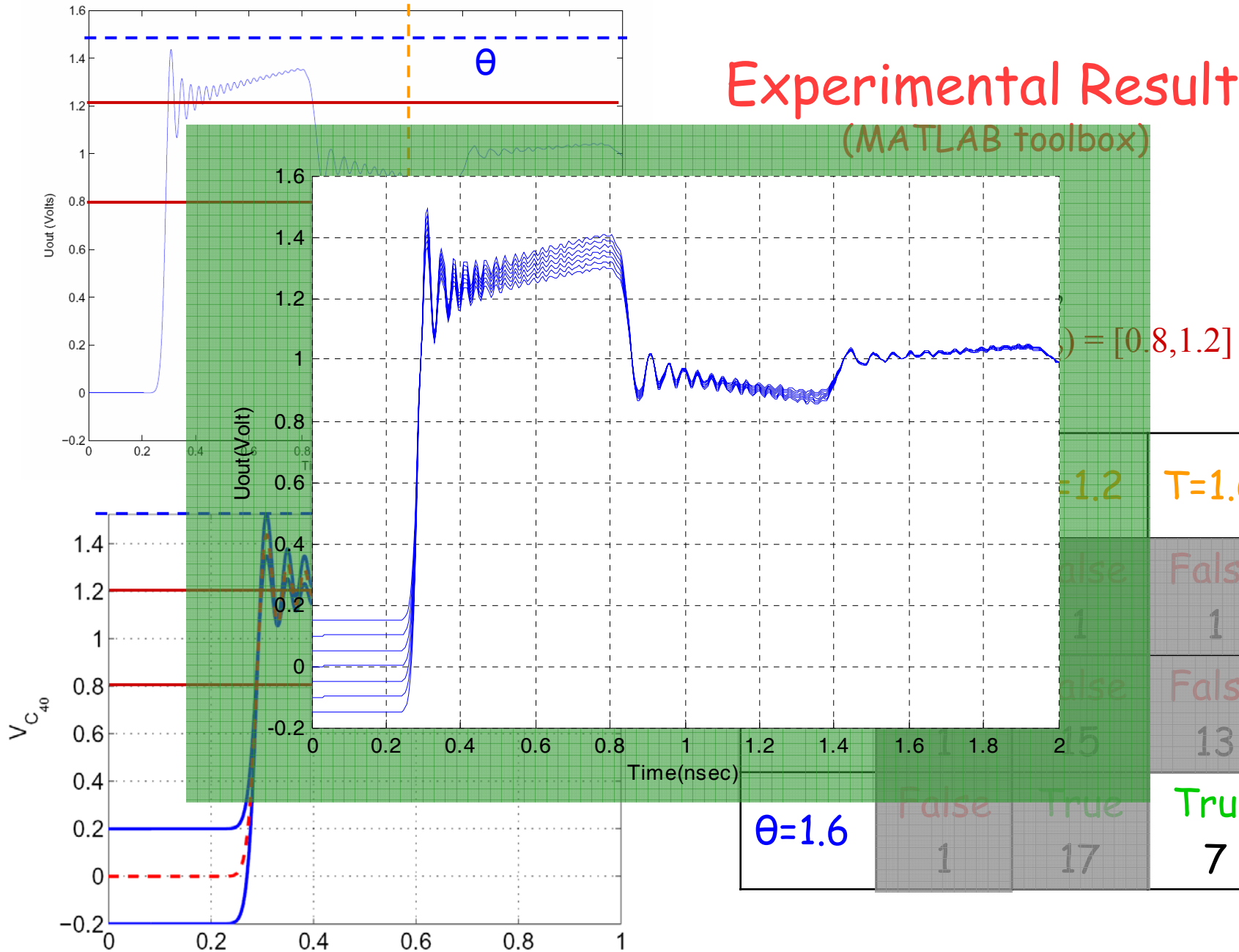


from Zhi Han's PhD Thesis 2005

	T=0.8	T=1.2	T=1.6
$\theta=1.4$	False 1	False 1	False 1
$\theta=1.5$	False 1	False 15	False 13
$\theta=1.6$	False 1	True 17	True 7

Experimental Results

(MATLAB toolbox)



from Zhi Han's PhD Thesis 2005



Talk Overview

Introduction

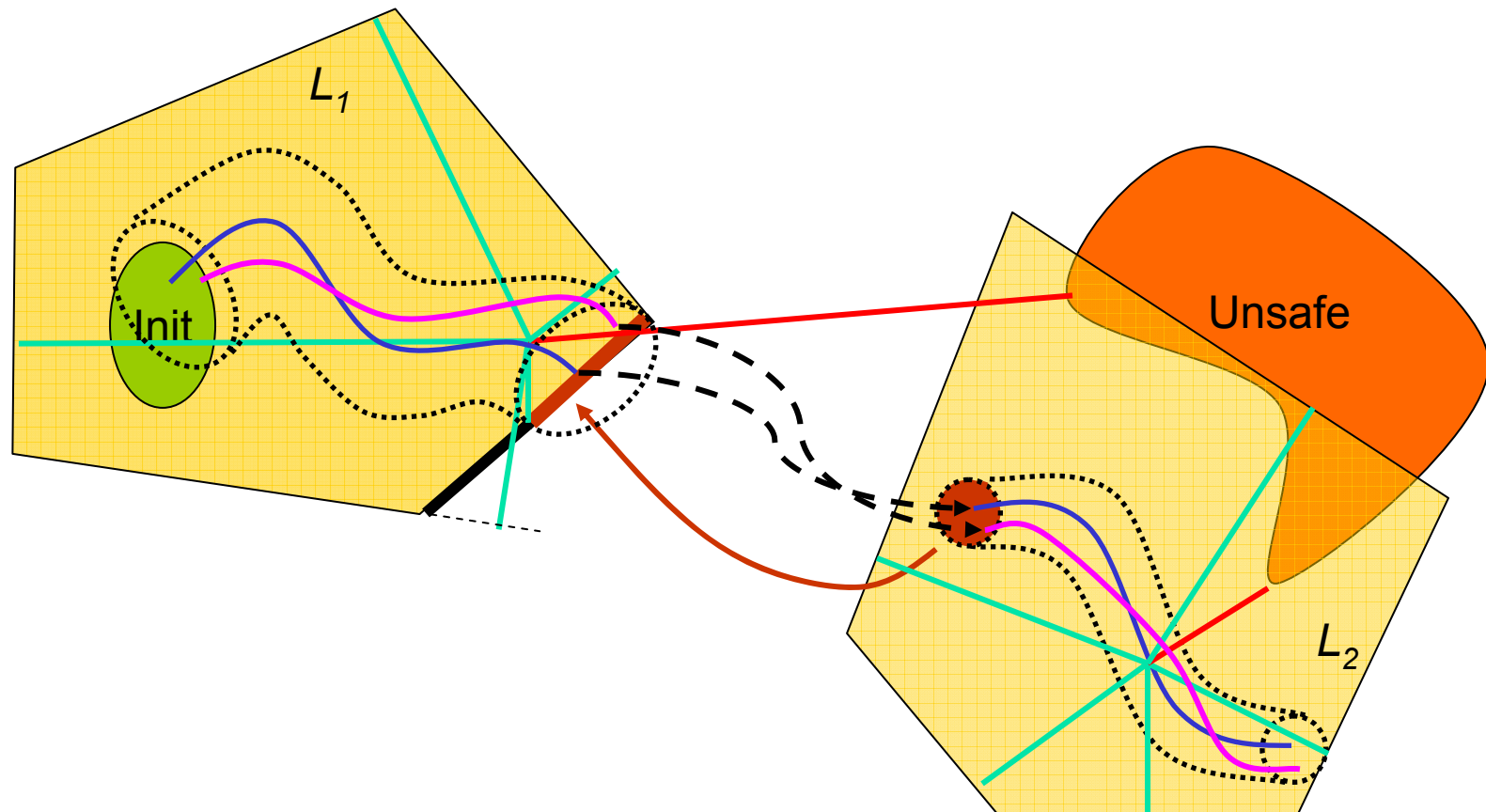
- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

How robust is a hybrid test trajectory?



Talk Overview

Introduction

- Application areas
- Challenges
- Thesis Contributions

Testing / Verification (Towards Certification)

- Problem
- Specification language (MTL)
- Robustness of Temporal Logic Specifications for signals
 - ◆ From Discrete Time to Continuous Time
 - ◆ From Signals to Systems
- Analog system robust testing / verification
 - ◆ Hybrid system robust testing

Final remarks - Future work

Main Contributions

- ✓ Testing / Verification (toward Certification)
 - ✓ Robust temporal logic testing
 - ✓ Semantics which maintains topological information
 - ✓ Applications in signal testing/monitoring
 - ✓ Analog system robust temporal logic testing
 - ✓ Combining logic with system dynamics
 - ✓ Applications in analog system verification
 - ✓ Hybrid system robust testing
 - ✓ Robustness wrt to switching conditions
 - ✓ Applications in embedded systems and mixed-signal circuits
- ✓ From discrete time to continuous time
 - ✓ How specification can guide sampling?
- ✓ Automated Synthesis of hybrid controllers
 - ✓ Non-reactive planning (bottom up)
 - ✓ Kinematic & dynamic model motion planning
 - ✓ Reactive planning (bottom up)
 - ✓ Distributed multi-robot planning
 - ✓ Top-down hybrid system synthesis
 - ✓ Human-Robot interfaces
- ✓ UAV testbed platform development

Thank you !

Acknowledgements:

Rajeev Alur, Madhukar Anand, Selcuk Bayraktar, Edmund M. Clarke,
Antoine Girard, A. Agung Julius, Hadas Kress-Gazit,
Insup Lee, Savvas G. Loizou, George J. Pappas, Oleg Sokolsky

Funding:

UPenn, NSF EHS 0311123, NSF ITR 0324977, ARO MURI DAAD 19-02-01-0383.