Robustness of Temporal Logic Specifications

Georgios E. Fainekos

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

Inside the M2A™ Capsule:
1. Optical dome
2. Lens holder
3. Lens
4. Illuminating LEDs (Light Emitting Diodes)
5. CMOS (Complementary Metal-Oxide-Semiconductor) Imager
6. Battery
7. ASIC (Application Specific Integrated Circuit) Transmitter
8. Antenna
Embedded in: Robotics

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-depended 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 TL specifications for continuous time signals*, TCS (Submitted)

☑️ **From discrete time to continuous time**
  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, *Temporal Logic Motion Planning for Dynamic Robots*, Automatica (Accepted)
  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

Does the system satisfy the specification?

Cyber-Physical System

Algorithm/Process

Specification

Model-based code generation

Implementation

Where and how the system fails?

YES

NO
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 \(t = 0\):
\[
x(0) = -A^{-1}bU_{in}(0)
\]

Property:
\[
\Phi = G_{p_1} \land F_{[0,0.85]}G_{p_2}
\]
\[
\mathcal{O}(p_1) = [-1.5, 1.5]
\]
\[
\mathcal{O}(p_2) = [0.8, 1.2]
\]

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**
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, Jadabaie, ...
  - systematic simulations / model based testing:
    - Krogh, Maler, Dang, Lee, Sokolsky, Kumar, Esposito, LaValle, Vardi, ...

- In Practice: Simulations!
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: \[ \Phi ::= T \mid \bot \mid p \mid \neg p \mid \Phi_1 \lor \Phi_2 \mid \Phi_1 \land \Phi_2 \mid \Phi_1 U_I \Phi_2 \mid \Phi_1 R_I \Phi_2 \]

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) \[ F_I \Phi ::= T U_I \Phi \]

Always (globally) \[ G_I \Phi ::= \bot R_I \Phi \]

Koymans '90, Specifying real-time properties with metric temporal logic
**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

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

Truth Value \( \{\bot, T\} \)

Monitoring Algorithm

[A/D Boolean abstraction]

[Other papers: 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:
\[ G(p_1 \rightarrow F_{\leq} p_2) \]
LTL to motion planning

\[ F(p_2 \land F(p_3 \land F(p_4 \land \neg(p_2 \lor p_3) \lor p_1))) \]

Fainekos, Kress-Gazit and Pappas, *Hybrid Controllers for Path Planning*, CDC 2005
Robustness of Temporal Logics

\[ \Phi = G(p_1 \to F_{\leq 2} p_2) \]

Monitor/Tester

Robustness parameter
\[ \varepsilon \in \mathbb{R} \cup \{ \pm \infty \} \]


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

\[
d_{dist}(x, C) := \inf \{ d(x, y) \mid y \in cl(C) \}
\]

\[
d_{depth}(x, C) := d_{dist}(x, X \setminus C)
\]

\[
D_{ist}(x, C) := \begin{cases} 
- d_{ist}(x, C) & \text{if } x \not\in C \\
 d_{depth}(x, C) & \text{if } x \in C 
\end{cases}
\]
Definition of robustness for signals

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

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

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

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

Input:
- Discrete time signal

Input:
- LTL / MTL formula & Observation map

Monitor/Tester

Output:
\[ \varepsilon \in \mathbb{R} \cup \{\pm \infty\} \]
Intuition - Example

Specification: $Fp = T \cup p$

$$[\phi_1 \cup \phi_2]_D(\mu, i) = \begin{cases} (K^\infty(0, I) \cap [\phi_2]_D(\mu, i)) \cup \\ \cup \left([\phi_1]_D(\mu, i) \cap [\phi_1 \cup_{I - \delta(i)} \phi_2]_D(\mu, i + 1)\right) & \text{if } i < \max N \\ K^\infty(0, I) \cap [\phi_2]_D(\mu, i) & \text{otherwise} \end{cases}$$
Running TaLiRo on a Dell PowerEdge 1650

\[ s(i) = \sin \tau(i) + \sin 2\tau(i) \]
\[ \tau(i) = 0.2i \]

\[ O(p_1) = [1.5, +\infty) \]

\[ G(p_1 \to F_{(0,0,1.0)} \neg p_1) \]

<table>
<thead>
<tr>
<th>signal’s time domain</th>
<th>number of samples</th>
<th>computation time (sec)</th>
<th>robustness</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0, 21.99]</td>
<td>110</td>
<td>0.00</td>
<td>0.097603</td>
</tr>
<tr>
<td>[0, 188.49]</td>
<td>943</td>
<td>0.03</td>
<td>0.097603</td>
</tr>
<tr>
<td>[0, 6283.2]</td>
<td>31,416</td>
<td>1.05</td>
<td>0.092065</td>
</tr>
<tr>
<td>[0, 21991.48]</td>
<td>1,099,558</td>
<td>37.61</td>
<td>0.091793</td>
</tr>
</tbody>
</table>
Guaranteed correctness under noise and uncertainty

\[ F_{I2}(p_2 \wedge F_{I3}(p_3 \wedge F_{I4}(p_4 \wedge \neg(p_2 \vee p_3) U_{I1} p_1))) \]

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

MTL formula → Signal dynamics

Sampling Conditions → TL Robustness

Bounds on the continuous time robustness estimate

YES NO

Fainekos and Pappas, Robust Sampling for MITL specifications, FORMATS 2007
Fainekos and Pappas, Robustness of TL specifications for continuous time signals, TCS (Submitted)
Given a system $\Sigma$, we can define the \textit{robustness degree} as

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

$$
\rho(s,s') = \sup \{d(s(t),s'(t)) \mid t \in R\}
$$
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:
\[
\Phi = Gp_1 \wedge F_{[0,T]}Gp_2 \\
\mathcal{O}(p_1) = [-1.5,1.5] \\
\mathcal{O}(p_2) = [0.8,1.2]
\]

Initial conditions:
\[
U_{in}(0) \in [-0.2,0.2]
\]
Robust TL testing of analog systems

Closed-loop system $\Sigma$

\[
\begin{align*}
\dot{x} &= f(x) \\
y &= g(x)
\end{align*}
\]

$X_0 \subseteq X$

LTL / MTL

\[
\Phi = G p_1 \land F_{[0,\tau]} G p_2
\]

Simulator / Tester

\[
B_\rho(\mathcal{L}(\Sigma), \delta) \subseteq \mathcal{L}(\Phi)
\]

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 $\Sigma$:
\[
\begin{align*}
\dot{x} &= f(x) \\
y &= g(x)
\end{align*}
\]
$X_0 \subseteq X$

Specification $\Phi$

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

$Proj_0 (P\Phi \cap \mathcal{L}(\Sigma))$

$\varepsilon$ robustness parameter

$B_\rho(\sigma, |\varepsilon|)$
Achieving coverage I

Closed-loop system $\Sigma$:
\[
\begin{align*}
\dot{x} &= f(x) \\
y &= g(x)
\end{align*}
\]
$X_0 \subseteq X$

Specification $\Phi$

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

Good news!
Coverage with a finite number of simulations
Computing bisimulation functions

Quadratic Bisimulation Functions for Deterministic Linear Systems

\[ \dot{x} = Ax \]
\[ y =Cx \]

\[ V(x) = \sqrt{x^T M x} \]
is a bisimulation function if
\[ M \geq C^T C \]
\[ A^T M + M A \leq 0 \]

Approximate Bisimulations for Constrained Linear Systems
Antoine Girard and George J. Pappas

Bisimulation Functions using Sum Of Squares Relaxation

\[ \dot{x} = f(x) \]
\[ y = g(x) \]

\[ V(x_1, x_2) = \sqrt{q(x_1, x_2)} \]
is a bisimulation function if
\[ q(x_1, x_2) - \|g_1(x_1) - g_2(x_2)\|^2 \text{ is SOS} \]
\[ - \frac{\partial q(x_1, x_2)}{\partial x_1} f_1(x_1) - \frac{\partial q(x_1, x_2)}{\partial x_2} f_2(x_2) \text{ is SOS} \]

Approximate Bisimulations for Nonlinear Dynamical Systems
Antoine Girard and George J. Pappas
Achieving coverage II

Closed-loop system $\Sigma$:
$$\begin{align*}
\dot{x} &= f(x) \\
y &= g(x)
\end{align*}$$
$X_0 \subseteq X$

Specification $\Phi$

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

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

Closed-loop system $\Sigma$:
\[
\begin{align*}
\dot{x} &= f(x) \\
y &= g(x)
\end{align*}
\]
$X_0 \subseteq X$

Specification $\Phi$

\[\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)\]

Observation!
A robust system with respect to the property requires less simulations
Coverage certificates

Closed-loop system $\Sigma$:
\[
\dot{x} = f(x) \quad X_0 \subseteq X
\]
Specification $\Phi$

\[\mathcal{L}(\Sigma) \subseteq \mathcal{L}(\Phi)\]

Good news! We get coverage guarantees after $K$ iterations.
Main results

**Theorem:** Let $V$ be a bisimulation function, let $(x_1,y_1)$ be a trajectory of $\Sigma$, $\varepsilon$ be the robustness parameter of $\Phi$ 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 $\Phi$ wrt $y_1$ is greater or equal to $\delta$.

**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 $\{x_1,...,x_r\} \subseteq X_0$ such that

for all $x \in X_0$, there exists $x_i$, such that $V(x,x_i) \leq \zeta$

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

Theorem: Let \((x_1, y_1), \ldots, (x_r, y_r)\) be trajectories of \(\Sigma\) such that \(\text{Disc}(X_0, \zeta) = \{x_1(0), \ldots, x_r(0)\}\). Let \(\varepsilon_i\) be the robustness parameter of \(\Phi\) wrt \(y_i\). Then,

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

Proposition: If \(\Sigma_1\) is \(\delta\)-approximately simulated by \(\Sigma_2\) 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 and Pappas, *MTL Robust Testing for LPV Systems*, RTSS 2008 (Submitted)
Consider the linear system with dynamics

\[
A = \begin{bmatrix} 0.025 & -2.5 \\ 0.5 & -1 \end{bmatrix}
\]

\[
C = \begin{bmatrix} 1 \\ 0 \end{bmatrix}
\]

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

\[
\begin{align*}
M & \geq C^T C \\
A^T M + MA & \leq 0
\end{align*}
\]

\[
\Rightarrow M = \begin{bmatrix}
1.0940 & -0.3895 \\
-0.3895 & 2.6142
\end{bmatrix}
\]

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
Verification example – 2nd iteration
Verification example – 3rd iteration

![Graph showing time series for y(1)(t) and y(2)(t)]
Experimental Results
(MATLAB toolbox)

Property:

\[
\Phi = G p_1 \land F_{[0,\tau]} G p_2 \\
O(p_1) = [-\theta, \theta], \quad O(p_2) = [0.8, 1.2]
\]

<table>
<thead>
<tr>
<th>(\theta)</th>
<th>(T=0.8)</th>
<th>(T=1.2)</th>
<th>(T=1.6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\theta=1.4)</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>(\theta=1.5)</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>(\theta=1.6)</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

from Zhi Han’s PhD Thesis 2005
Experimental Results
(MATLAB toolbox)

Property:
\[ \Phi = G p_1 \land F_{[0,\tau]} G p_2 \]
\[ \Theta(p_1) = [-\theta, \theta], \quad \Theta(p_2) = [0.8, 1.2] \]

<table>
<thead>
<tr>
<th>(T)</th>
<th>(\theta=1.4)</th>
<th>(\theta=1.5)</th>
<th>(\theta=1.6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.8</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>1.2</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>1.6</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

from Zhi Han's PhD Thesis 2005
Experimental Results
(MATLAB toolbox)

Property:
\[ \Phi = G p_1 \land F_{[0,\tau]} G p_2 \]
\[ \mathcal{O}(p_1) = [-\theta, \theta], \mathcal{O}(p_2) = [0.8, 1.2] \]

<table>
<thead>
<tr>
<th>θ</th>
<th>T=0.8</th>
<th>T=1.2</th>
<th>T=1.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>θ=1.4</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>θ=1.5</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>θ=1.6</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

\[ T=1.6 \]

from Zhi Han's PhD Thesis 2005
Experimental Results
(MATLAB toolbox)

Property:

\[ \Phi = G_p_1 \land F_{[0,T]} G_p_2 \]

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

<table>
<thead>
<tr>
<th>Time (ns)</th>
<th>( T=0.8 )</th>
<th>( T=1.2 )</th>
<th>( T=1.6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \theta = 1.4 )</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>( \theta = 1.5 )</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>( \theta = 1.6 )</td>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

from Zhi Han's PhD Thesis 2005
Experimental Results

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?

Julius, Fainekos, Anand, Lee, Pappas,
Robust Test Generation and Coverage for Hybrid Systems, HSCC 2007
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
Acknowledgements:

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