Efficient Robust Monitoring for STL

Alexandre Donzé[1], **Thomas Ferrère**[2], Oded Maler[2]

[1] University of California, Berkeley, EECS dept
[2] Verimag, CNRS and Grenoble University

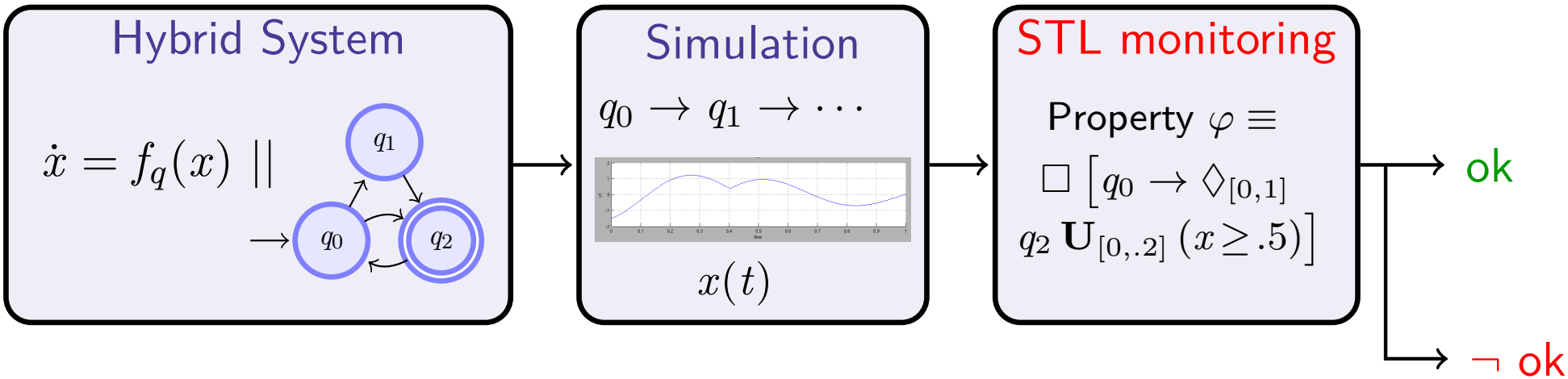
May 28, 2013

Overview

- Signal Temporal Logic (STL): temporal specifications for continuous and hybrid systems
- Quantitative satisfaction of STL can accomodate noise/approximation, increase coverage

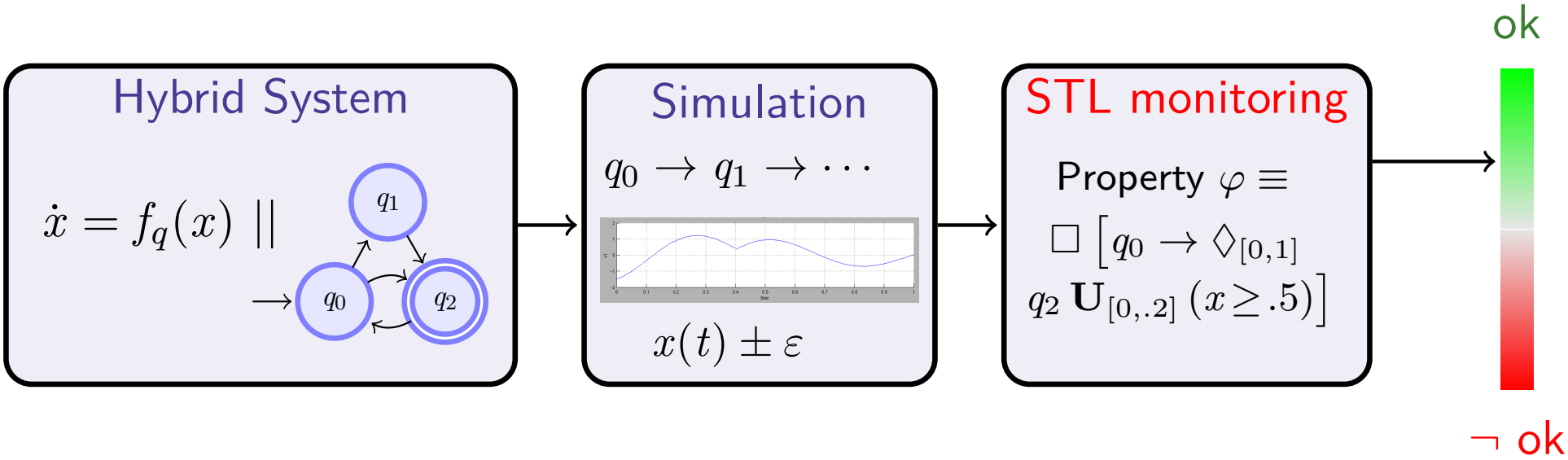
Overview

- Signal Temporal Logic (STL): temporal specifications for continuous and hybrid systems
- Quantitative satisfaction of STL can accomodate noise/approximation, increase coverage



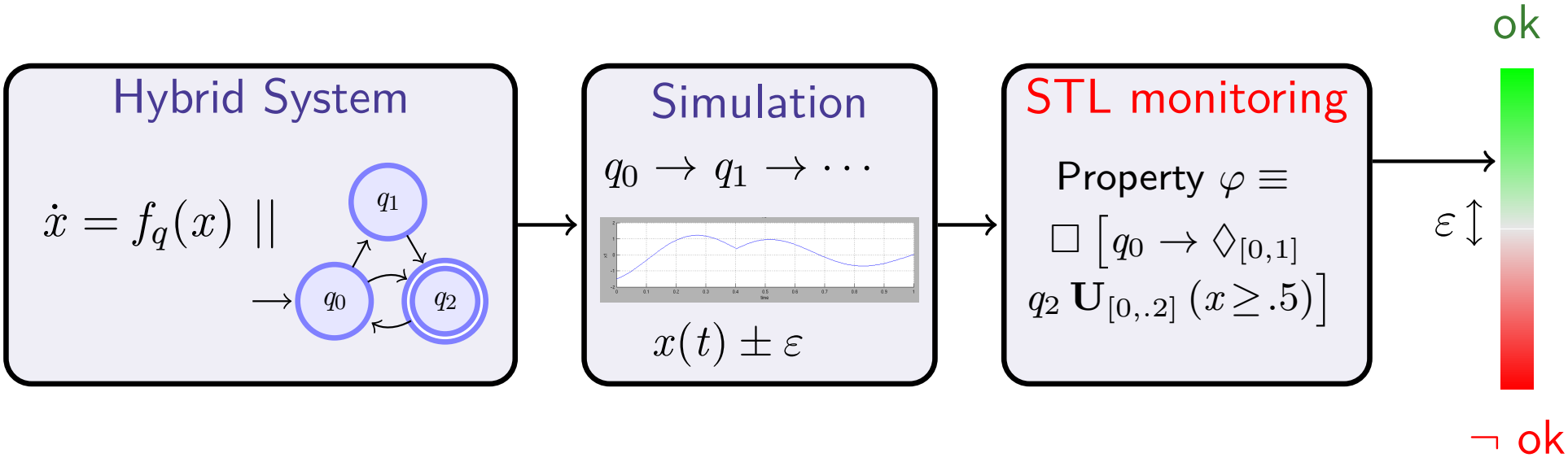
Overview

- Signal Temporal Logic (STL): temporal specifications for continuous and hybrid systems
- Quantitative satisfaction of STL can accomodate noise/approximation, increase coverage



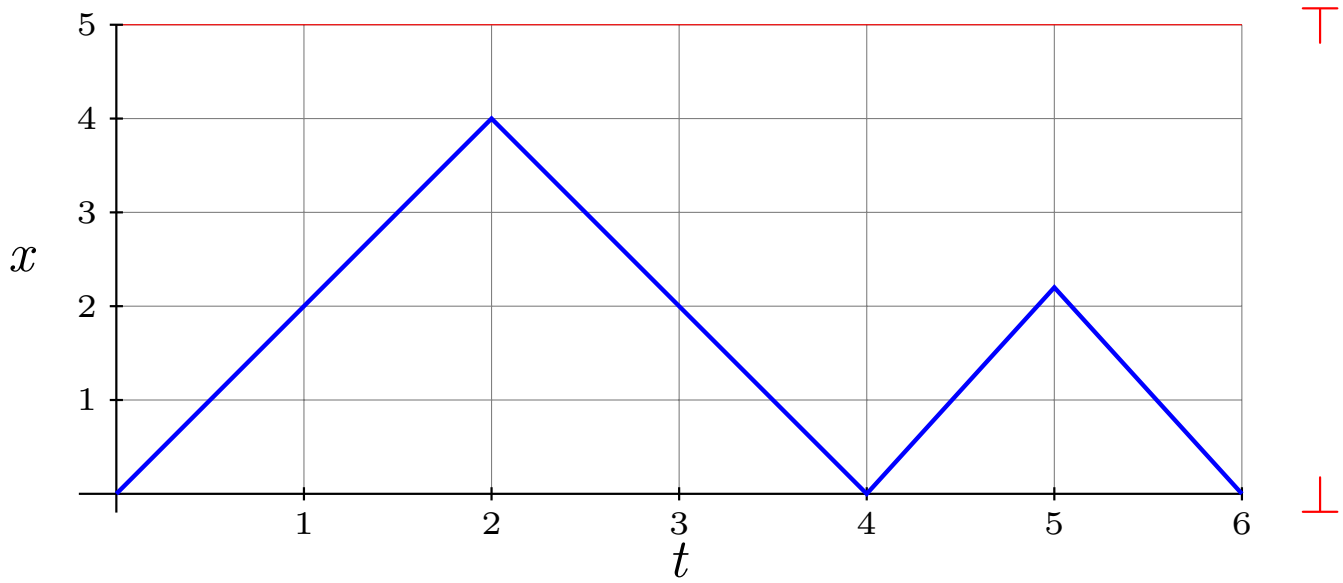
Overview

- Signal Temporal Logic (STL): temporal specifications for continuous and hybrid systems
- Quantitative satisfaction of STL can accomodate noise/approximation, increase coverage



Overview

Example: Boolean Monitoring

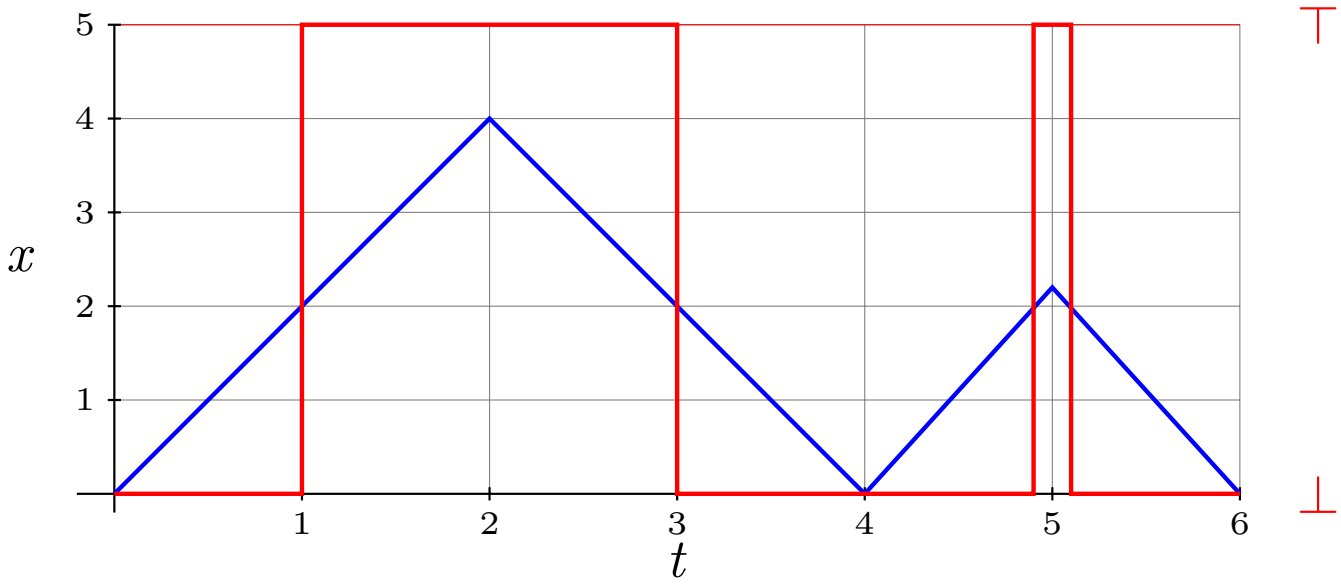


Satisfaction signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]} (x \geq 2)$

Overview

Example: Boolean Monitoring

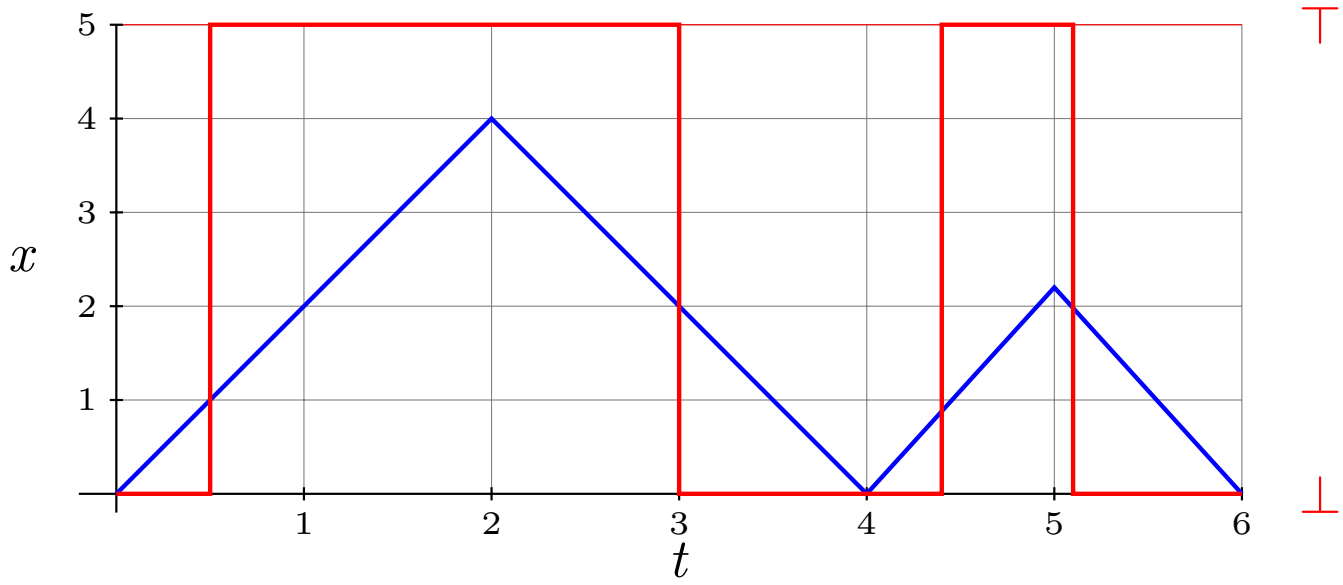


Satisfaction signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]} (x \geq 2)$

Overview

Example: Boolean Monitoring

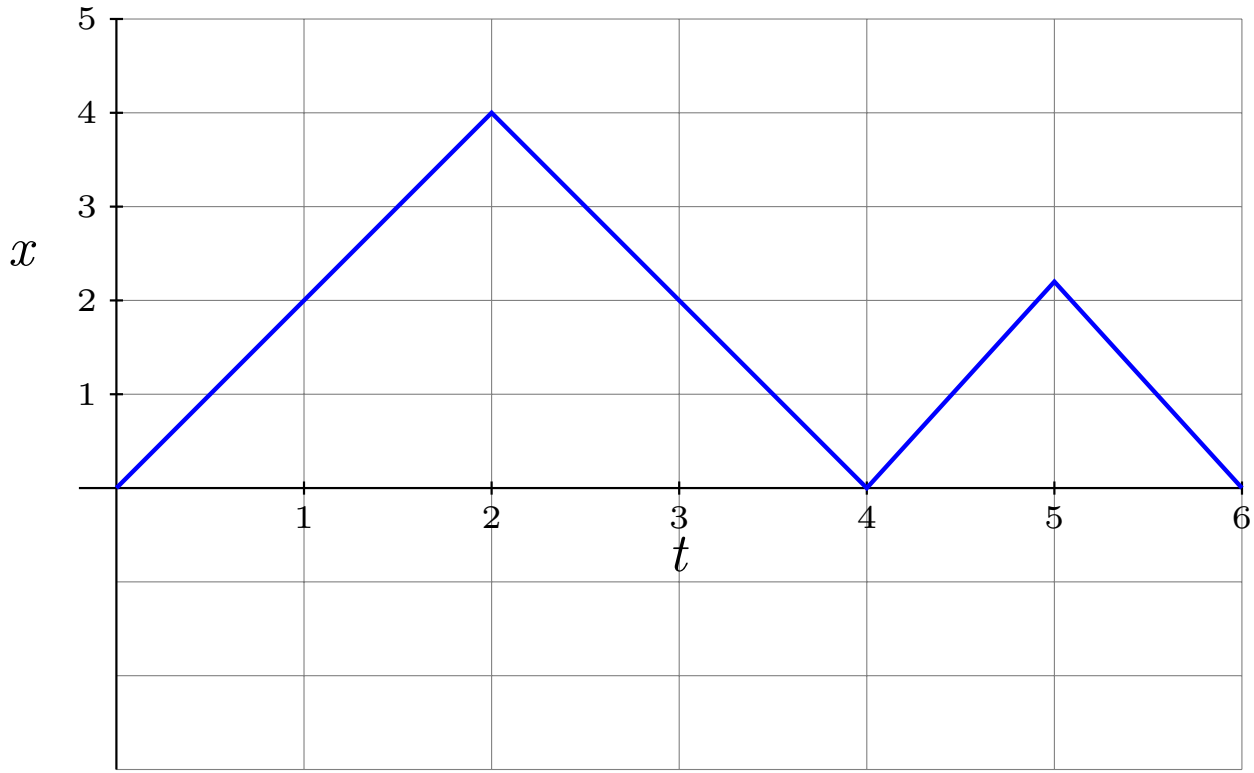


Satisfaction signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]} (x \geq 2)$

Overview

Example: Robust Monitoring

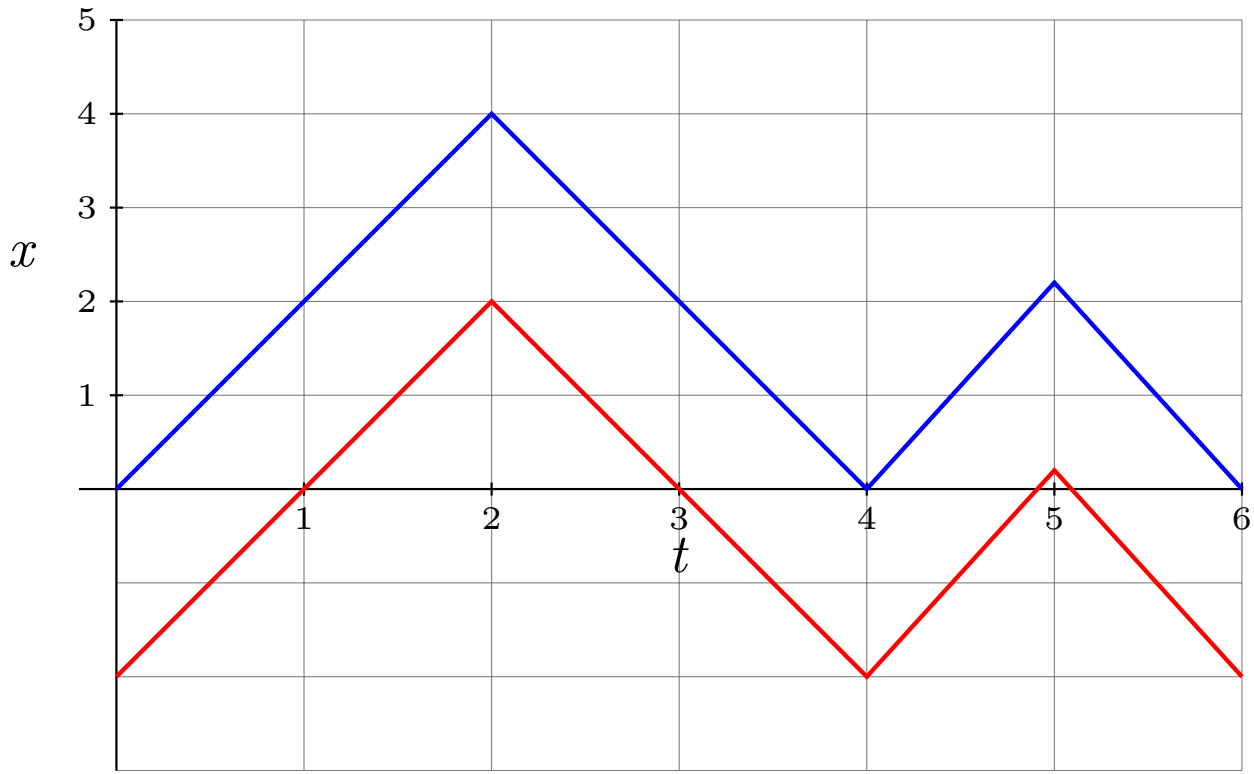


Robustness signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]} (x \geq 2)$

Overview

Example: Robust Monitoring

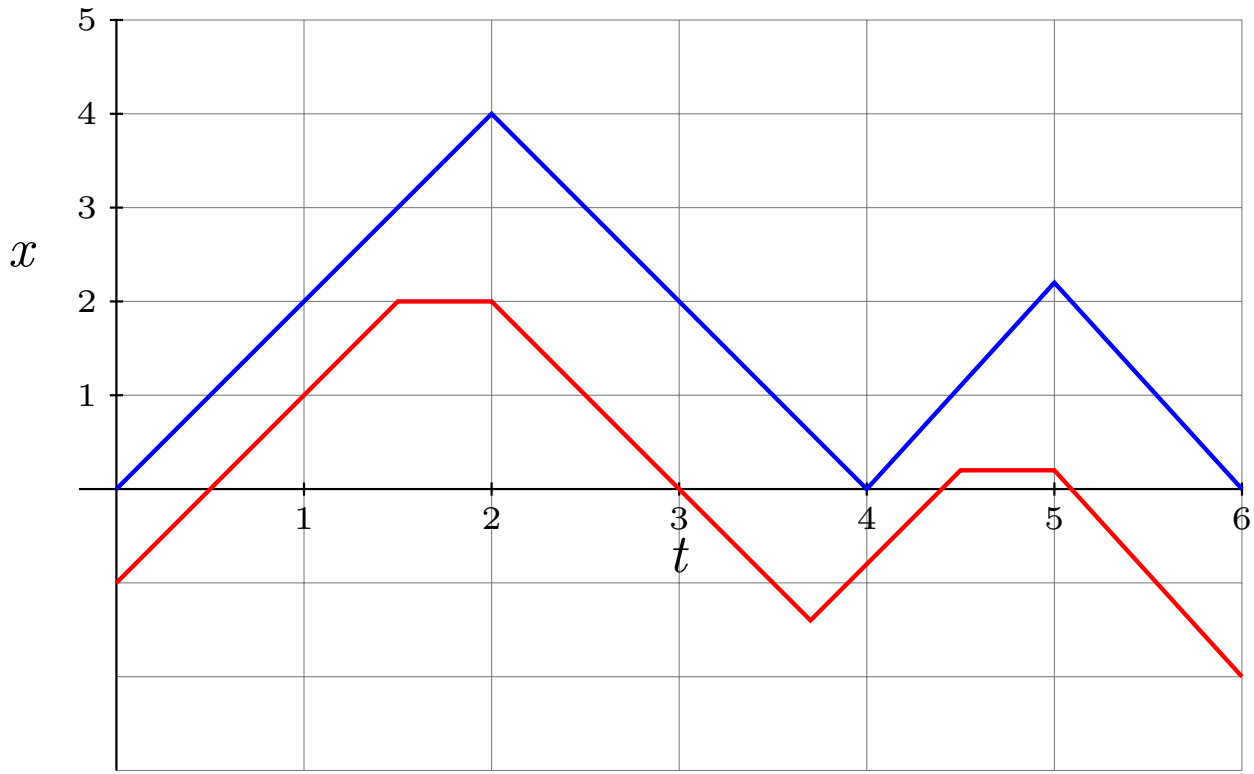


Robustness signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]}\,(x \geq 2)$

Overview

Example: Robust Monitoring



Robustness signal of :

- $\varphi = x \geq 2$
- $\varphi = \Diamond_{[0,0.5]} (x \geq 2)$

Outline

1. Signal Temporal Logic
2. Robust Monitoring Algorithms
3. Complexity and Evalutation

Outline

1. Signal Temporal Logic
2. Robust Monitoring Algorithms
3. Complexity and Evalutation

Formal Definitions

Definition (STL Syntax)

$$\varphi := \text{true} \mid x_i \geq c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \, \mathbf{U}_I \, \varphi$$

with I closed interval of $\mathbb{R}^+$

Definition (STL Semantics)

The validity of a formula φ with respect to a trace w at time t is

$$\begin{aligned}
w, t &\vDash \text{true} \\
w, t &\vDash x_i \geq c \iff x_i^w(t) \geq c \\
w, t &\vDash \neg\varphi \iff w, t \nvDash \varphi \\
w, t &\vDash \varphi \wedge \psi \iff w, t \vDash \varphi \text{ and } w, t \vDash \psi \\
w, t &\vDash \varphi \, \mathbf{U}_I \, \psi \iff \exists t' \in t + I \text{ s.t. } w, t' \vDash \psi \\
&\qquad \text{and } \forall t'' \in [t, t'], \; w, t'' \vDash \varphi
\end{aligned}$$

Additionally: $\Diamond_I \varphi := \top \, \mathbf{U}_I \, \varphi$ and $\Box_I \varphi := \neg \Diamond_I \neg\varphi$.

Formal Definitions

Definition (STL Syntax)

$$\varphi := \text{true} \mid x_i \geq c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \, \mathbf{U}_I \, \varphi$$

with I closed interval of $\mathbb{R}^+$

Definition (STL Semantics)

The validity of a formula φ with respect to a trace w at time t is

$$\begin{aligned}
&w, t \vDash \text{true} \\
&w, t \vDash x_i \geq c \quad &\iff \quad &x_i^w(t) \geq c \\
&w, t \vDash \neg\varphi \quad &\iff \quad &w, t \nvDash \varphi \\
&w, t \vDash \varphi \wedge \psi \quad &\iff \quad &w, t \vDash \varphi \text{ and } w, t \vDash \psi \\
&w, t \vDash \varphi \, \mathbf{U}_I \, \psi \quad &\iff \quad &\exists t' \in t + I \text{ s.t. } w, t' \vDash \psi \\
& & &\text{and } \forall t'' \in [t, t'], \; w, t'' \vDash \varphi
\end{aligned}$$

Additionally: $\Diamond_I \varphi := \top \, \mathbf{U}_I \, \varphi$ and $\Box_I \varphi := \neg \Diamond_I \neg\varphi$.

Monitoring

Truth value of a formula for a given trace defines a Boolean signal

Definition (Satisfaction Signal)

$$\chi(\varphi, w, .) := t \mapsto \begin{cases} \top \text{ if } w, t \vDash \varphi \\ \bot \text{ otherwise} \end{cases}$$

Procedure: by bottom-up computation of $\chi(\psi, x, .)$ for each subformula $\psi \in \varphi$

From Boolean to quantitative semantics

Boolean algebra $(\{\top, \bot\}, <, -)$	Real algebra $(\mathbb{R} \cup \{\top, \bot\}, <, -)$
$p \vee p \sim p$	–
$p \wedge \mathsf{true} \sim p$	–
$p \vee (q \wedge r) \sim (p \wedge q) \vee (p \wedge r)$	–
$\neg p \wedge \neg q \sim \neg(p \vee q)$	–
$p \vee \neg p \sim \mathsf{true}$	x

Satisfaction Signal

$$
\begin{aligned}
\chi(\mathsf{true}, w, t) &= \top \\
\chi(x_i \geq c, w, t) &= \begin{cases} \top \text{ if } x_i(t) \geq c, \\ \bot \text{ otherwise} \end{cases} \\
\chi(\neg\varphi, w, t) &= -\chi(\varphi, w, t) \\
\chi(\varphi \wedge \psi, w, t) &= \min\{\chi(\varphi, w, t), \chi(\varphi, w, t)\} \\
\chi(\varphi \,\mathbf{U}_I\, \psi, w, t) &= \sup_{t' \in t+I} \min\{\chi(\psi, w, t'), \inf_{t'' \in [t,t']} \chi(\varphi, w, t'')\}
\end{aligned}
$$

Quantitative Semantics

$$
\begin{aligned}
\rho(\mathsf{true}, w, t) &= \top \\
\rho(x_i \geq c, w, t) &= x_i(t) - c \\
\rho(\neg\varphi, w, t) &= -\rho(\varphi, w, t) \\
\rho(\varphi \wedge \psi, w, t) &= \min\{\rho(\varphi, w, t), \rho(\psi, w, t)\} \\
\rho(\varphi \,\mathbf{U}_I\, \psi, w, t) &= \sup_{t' \in t+I} \min\{\rho(\psi, w, t'), \inf_{t'' \in [t,t']} \rho(\varphi, w, t'')\}
\end{aligned}
$$

Property of Robustness Estimate

- Sign indicates satisfaction status
- Absolute value indicates tolerance

Theorem (Faneikos and Pappas 2009)

$$\rho(\varphi, w, t) > 0 \Rightarrow w, t \vDash \varphi$$
$$w, t \vDash \varphi \text{ and } \|w - w'\|_\infty < \rho(\varphi, w, t) \quad \Rightarrow \quad w', t \vDash \varphi$$

Property of Robustness Estimate

- Sign indicates satisfaction status
- Absolute value indicates tolerance

Theorem (Faneikos and Pappas 2009)

$$\rho(\varphi, w, t) > 0 \Rightarrow w, t \vDash \varphi$$
$$w, t \vDash \varphi \text{ and } \|w - w'\|_\infty < \rho(\varphi, w, t) \quad \Rightarrow \quad w', t \vDash \varphi$$

Corollary

$$\rho(\varphi, w, t) < 0 \Rightarrow w, t \nvDash \varphi$$
$$w, t \nvDash \varphi \text{ and } \|w - w'\|_\infty < -\rho(\varphi, w, t) \quad \Rightarrow \quad w', t \nvDash \varphi$$

Until Rewrite

The rewrite extends from Boolean to quantitative semantics

- unbounded until
  $\varphi \, \mathbf{U}_{[a,+\infty)} \, \psi \;\sim\; \Box_{[0,a]} \, (\varphi \, \mathbf{U} \, \psi)$
- bounded until
  $\varphi \, \mathbf{U}_{[a,b]} \, \psi \;\sim\; \Diamond_{[a,b]} \, \psi \wedge \varphi \, \mathbf{U}_{[a,+\infty)} \, \psi$

Until Rewrite

The rewrite extends from Boolean to quantitative semantics

- unbounded until
  $\varphi \, \mathbf{U}_{[a,+\infty)} \, \psi \;\sim\; \Box_{[0,a]} \, (\varphi \, \mathbf{U} \, \psi)$
- bounded until
  $\varphi \, \mathbf{U}_{[a,b]} \, \psi \;\sim\; \Diamond_{[a,b]} \, \psi \wedge \varphi \, \mathbf{U}_{[a,+\infty)} \, \psi$

Outline

1 Signal Temporal Logic

2 Robust Monitoring Algorithms

3 Complexity and Evalutation

Preliminaries

- Signals: timed words $(t_i, y(t_i))_{i \leq n_y}$, with linear interpolation
- Procedure: inductive computation of robustness signals $\rho(\varphi, x, .)$ on the formula structure
- Sampling: continuity, piecewise-affine property are preserved

Boolean operators

Negation

- Input signal: $(t_i, y(t_i))_{i \leq n_y}$
- Output signal: $(t_i, -y(t_i))_{i \leq n_y}$

Conjunction

- Input signals: $(t_i, y(t_i))_{i \leq n_y}$, $(t'_i, y'(t'_i))_{i \leq n_{y'}}$
- Output signal: $(r_i, z(r_i))_{i \leq n_z}$
  Time sequence r contains t, t', and punctual intersections $y \cap y'$
  Value $z(r_i) = \min\{y(r_i), y'(r_i)\}$

Boolean operators

Negation

- Input signal: $(t_i, y(t_i))_{i \leq n_y}$
- Output signal: $(t_i, -y(t_i))_{i \leq n_y}$

Conjunction

- Input signals: $(t_i, y(t_i))_{i \leq n_y}$, $(t'_i, y'(t'_i))_{i \leq n_{y'}}$
- Output signal: $(r_i, z(r_i))_{i \leq n_z}$
  Time sequence r contains t, t', and punctual intersections $y \cap y'$
  Value $z(r_i) = \min\{y(r_i), y'(r_i)\}$

Untimed Until

Induction Property: for all $s < t$

- Boolean Semantics $w, s \vDash \varphi \,\mathbf{U}\, \psi \iff$
  $w_{\restriction [s,t)}, s \vDash \varphi \,\mathbf{U}\, \psi$ or $\left(w_{\restriction [s,t)}, s \vDash \Box\, \varphi \text{ and } w, t \vDash \varphi \,\mathbf{U}\, \psi\right)$

- Quantitative Semantics $\rho(\varphi \,\mathbf{U}\, \psi, w, t) =$
  $\max\left\{\rho(\varphi \,\mathbf{U}\, \psi, w_{\restriction [s,t)}, s), \min\{\rho(\Box\, \varphi, w_{\restriction [s,t)}, s), \rho(\varphi \,\mathbf{U}\, \psi, w, t)\}\right\}$

Untimed Until

Induction Property: for all $s < t$

- Boolean Semantics $w, s \vDash \varphi \,\mathbf{U}\, \psi \iff$
  $w_{\restriction [s,t)}, s \vDash \varphi \,\mathbf{U}\, \psi$ or $\left(w_{\restriction [s,t)}, s \vDash \Box\, \varphi \text{ and } w, t \vDash \varphi \,\mathbf{U}\, \psi\right)$

- Quantitative Semantics $\rho(\varphi \,\mathbf{U}\, \psi, w, t) =$
  $\max\left\{\rho(\varphi \,\mathbf{U}\, \psi, w_{\restriction [s,t)}, s), \min\{\rho(\Box\, \varphi, w_{\restriction [s,t)}, s), \rho(\varphi \,\mathbf{U}\, \psi, w, t)\}\right\}$

Timed Eventually

Definition: $\rho(\Diamond_{[a,b]}\,\varphi, w, t) = \sup_{t' \in [t+a, t+b]} \rho(\varphi, w, t) = \sup_{[t+a,t+b]} y$

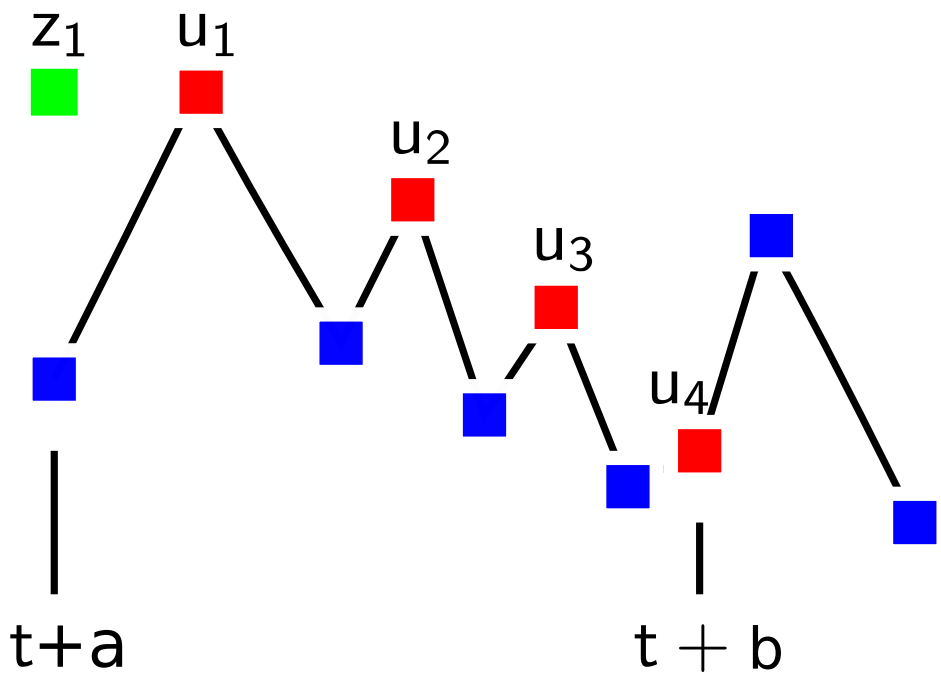
The maximum is reached at $t+a, t+b$, or at sample point in $\{t_i \mid t_i \in (t+a, t+b]\}$

Theorem (Lemire 2006)

The maximum of a sequence of over a shifting window can be computed in linear time

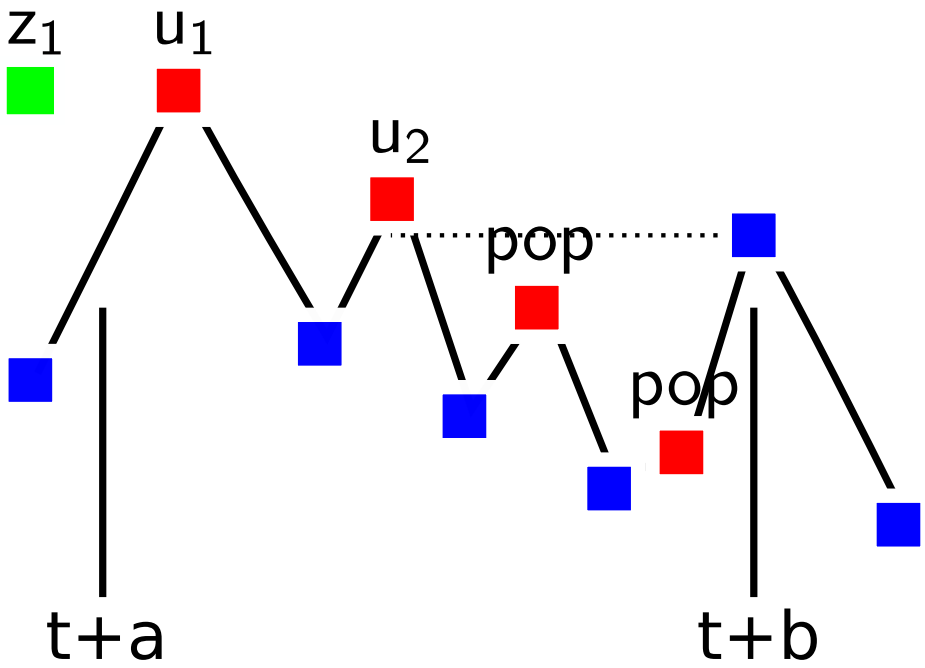
Idea: we maintain an ordered set M such that $\max\{y(t_i) | i \in M\} = \max\{y(t_i) \mid t_i \in (t+a, t+b]\}$

Timed Eventually: two steps in the algorithm



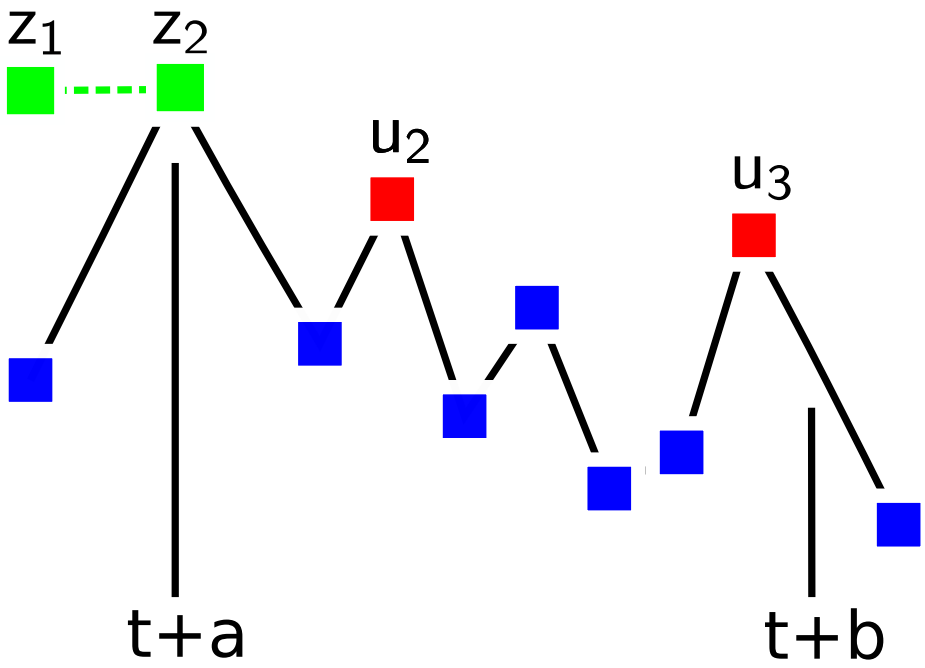
Maximum candidates $\{y(t_i)|i \in M\} = \{u_1, u_2, u_3, u_4\}$

Timed Eventually: two steps in the algorithm



Maximum candidates $\{y(t_i)|i \in M\} = \{u_1, u_2, u_3\}$

Timed Eventually: two steps in the algorithm



Maximum candidates $\{y(t_i)|i \in M\} = \{u_2, u_3\}$

Outline

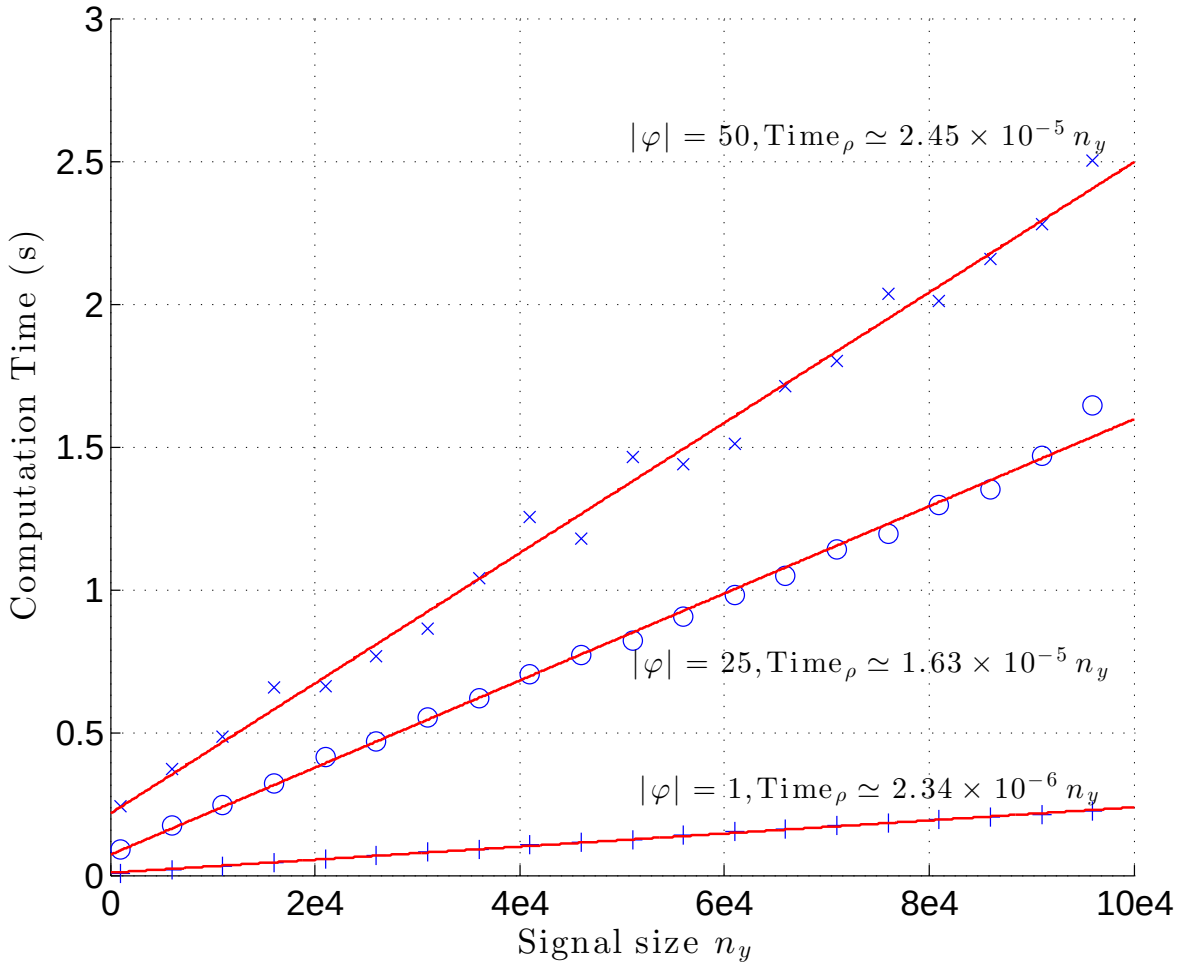
1. Signal Temporal Logic
2. Robust Monitoring Algorithms
3. Complexity and Evalutation

Worst-case Complexity

- For each subformula $\psi \in \varphi$, computation time linear in the input size
- Problem: size of robustness signal can increase exponentially with formula height
- Computation time in $\mathcal{O}(|\varphi| \cdot d^{\mathrm{h}(\varphi)} \cdot |x|)$

Experimentation: Random Signals

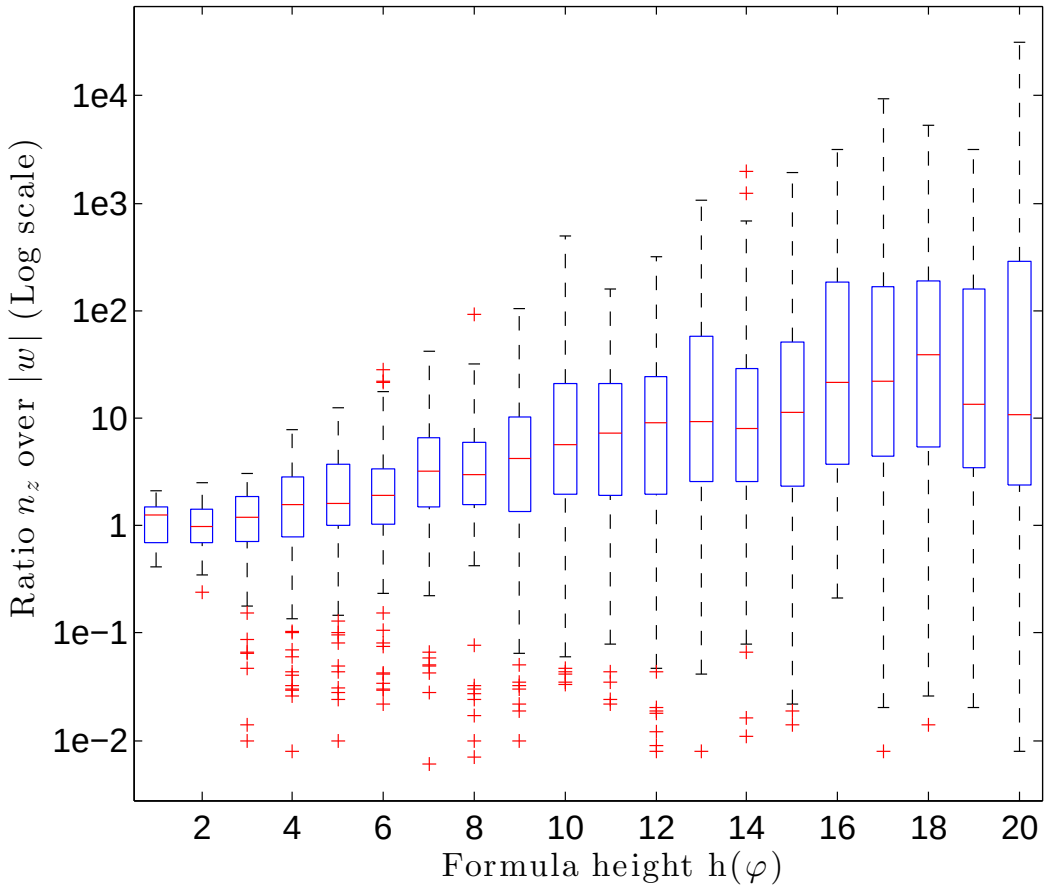
Computation is linear in size of input trace



Experimentation: Random Formulas

Exponential growth rate of robustness signal size with formula height

- average: $d \simeq 1.12$
- worst-case: $d \simeq 1.7$



Conclusion

Summary

- Enhancement to "Boolean" monitoring with reasonable computational overhead
- Piecewise affine signals: practical model for robustness computation

Perspectives

- Simulation-based approaches for verification, parameter synthesis
- Time-robustness as opposed to space-robustness