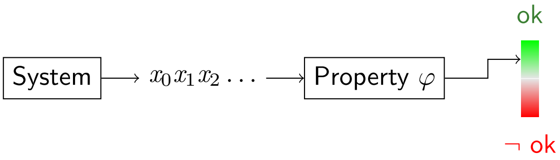
Robust Online Monitoring of Signal Temporal Logic

Garvit Juniwal[1], Shromona Ghosh[1], Alexandre Donzé[1], Sanjit A. Seshia[1], Jyotirmoy V. Deshmukh[2], Xiaoqing Jin [2]

[1]University of California, Berkeley

[2]Toyota Technical Center

Robut Online Monitoring

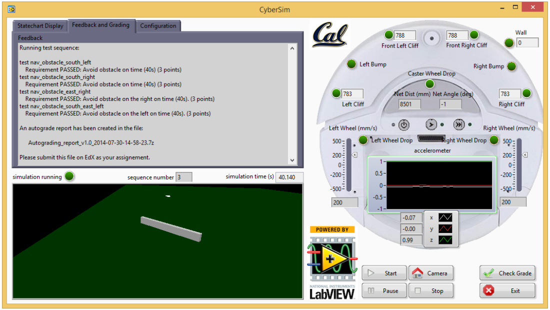


- System is a Cyber-Physical System
- φ is written in Signal Temporal Logic (STL)

Motivations

- Runtime verification
- Cutting simulation time (stops whenever true or false occurs)
- Quantitative satisfaction for partial traces used to guide toward falsification (T. Dreossi et al, *Efficient Guiding Strategies for Testing of Temporal Properties of Hybrid Systems NFM'15 ⇒ combines Rapidly Exploring Random Trees (RRT) with STL*)

Motivating Example: Autograding a CPS lab Assignment [1]



Automatic feedback and autograding: fault encoding in STL + env. test cases

Robust Online Monitoring: cutting simulation time + partial credit

---

[1] (Donze, Juniwal, Jensen, Seshia, *CPSGrader: Synthesizing Temporal Logic Testers for Auto-Grading an Embedded Systems Lab, EMSOFT'14*)

1. Signal Temporal Logic
2. Robust Online Monitoring of STL
3. Experimental Results

Signal Temporal Logic: Syntax

Signals are functions from $\mathbb{R}^n$ to $\mathbb{R}$.

E.g.: positions (x,y,z), orientation θ, sensor values (acc. ax,ay,az), etc.

We denote by $x(\tau)$ the value of signal x at time τ.

Atomic predicates are inequalities over signal values at **symbolic** time t

E.g.: $x(t) > 0.5$, $z(t) < 4$, $|lws(t) + rws(t)| > 100$, etc.

Temporal operators are $\Diamond$, $\Box$, $\mathbf{U}$, equiped with a time interval

e.g. $\Diamond_{[0,2]}(x(t) > 0.5)$, $\Box_{[0,40]}(y(t) < 0.3)$, $\varphi \mathbf{U}_{[1,2.5]} \psi$, etc.

Signal Temporal Logic: Syntax

Signals are functions from $\mathbb{R}^n$ to $\mathbb{R}$.

E.g.: positions (x,y,z), orientation θ, sensor values (acc. ax,ay,az), etc.

We denote by $x(\tau)$ the value of signal x at time τ.

Atomic predicates are inequalities over signal values at **symbolic** time t

E.g.: $x(t) > 0.5$, $z(t) < 4$, $|lws(t) + rws(t)| > 100$, etc.

Temporal operators are $\Diamond$, $\Box$, $\mathbf{U}$, equiped with a time interval

e.g. $\Diamond_{[0,2]}(x(t) > 0.5)$, $\Box_{[0,40]}(y(t) < 0.3)$, $\varphi\mathbf{U}_{[1,2.5]}\psi$, etc.

Signal Temporal Logic: Syntax

Signals are functions from $\mathbb{R}^n$ to $\mathbb{R}$.

E.g.: positions (x,y,z), orientation θ, sensor values (acc. ax,ay,az), etc.

We denote by $x(\tau)$ the value of signal x at time τ.

Atomic predicates are inequalities over signal values at **symbolic** time t

E.g.: $x(t) > 0.5$, $z(t) < 4$, $|lws(t) + rws(t)| > 100$, etc.

Temporal operators are $\Diamond$, $\Box$, $\mathbf{U}$, equiped with a time interval

e.g. $\Diamond_{[0,2]}(x(t) > 0.5)$, $\Box_{[0,40]}(y(t) < 0.3)$, $\varphi \mathbf{U}_{[1,2.5]} \psi$, etc.

STL Semantics

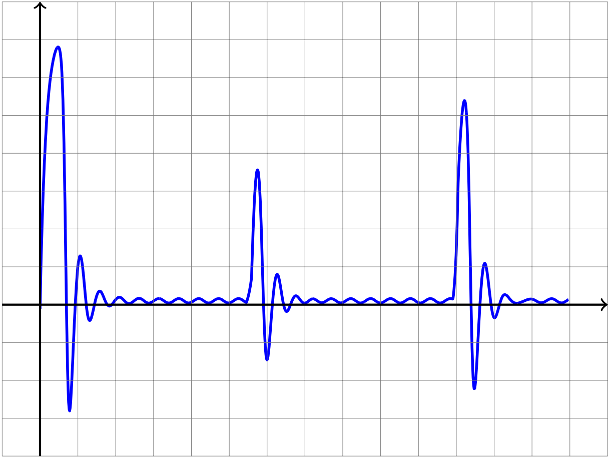
A **formula** φ is true if it is true **at time 0**

A **subformula** ψ is evaluated on **future values** depending on its temporal operators

Examples

- $\varphi = (x(t) > 0.5)$ is true iff $x(t) > 0.5$ is true when t is replaced by 0, i.e., at the first value of the signal.
- $\varphi = \Diamond_{[0,1.3]}(x(t) > 0.5)$ is true iff $x(t) > 0.5$ is true when t is replaced by any value in [0,1.3].
- $\varphi = \Box_{[0,1.3]}(\psi)$ is true iff ψ is true at all time in $[0, 1.3]$, i.e., for all suffixes of signals starting at a time in $[0, 1.3]$

STL Examples



STL Examples

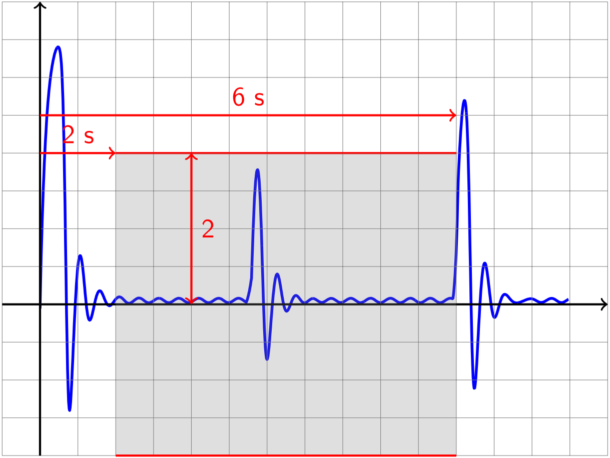
The signal is never above 3.5

$$\varphi := \square\ (x(t) < 3.5)$$

STL Examples

Between 2s and 6s the signal is between -2 and 2

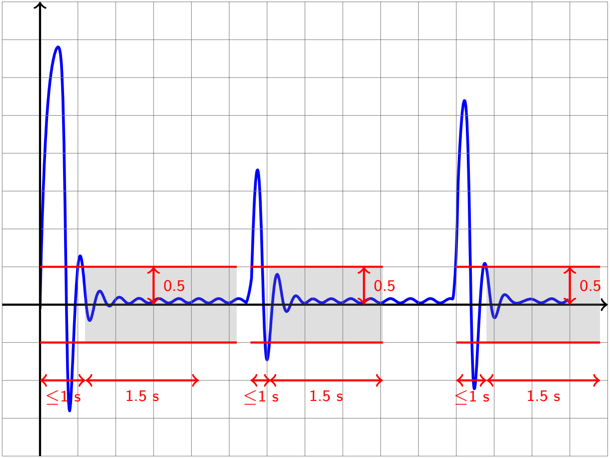
$$\varphi := \square_{[2,6]} \; (|x(t)| < 2)$$



STL Examples

Always $|x| > 0.5 \Rightarrow$ *after 1 s,* $|x|$ *settles under 0.5 for 1.5 s*

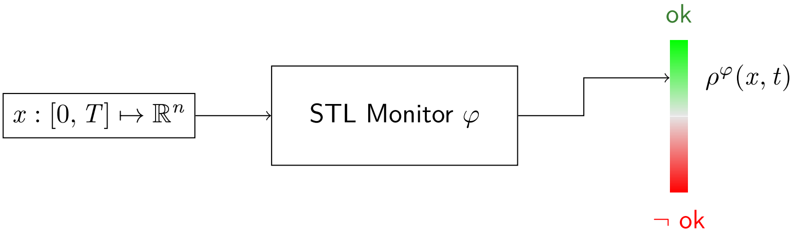
$$\varphi := \square(|x(t)| > .5 \rightarrow \diamond_{[0,1.]}\ (\square_{[0,1.5]}|x(t)| < 0.5))$$



Robust Monitoring

Given a formula φ, a signal x and a time t, compute a quantitative satisfaction function such that:

$$\rho^{\varphi}(x,t) > 0 \Rightarrow x,t \models \varphi$$
$$\rho^{\varphi}(x,t) < 0 \Rightarrow x,t \not\models \varphi$$



STL Robust Semantics, Examples

STL Robust Semantics, Examples

Between 2s and 6s the signal is between -2.5 and 2.5

$$\varphi := \Box_{[2,6]} \; (|x(t)| < 2.5)$$

STL Robust Semantics, Examples

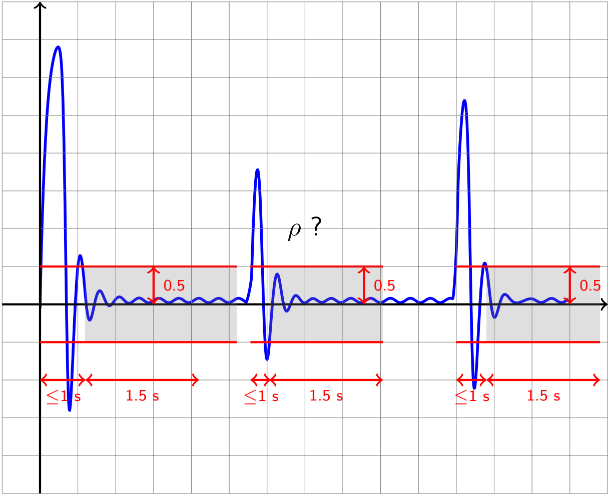
Between 2s and 6s the signal is between -1 and -1

$$\varphi := \Box_{[2,6]} \; (|x(t)| < 2.5)$$

STL Robust Semantics, Examples

Always $|x| > 0.5 \Rightarrow$ *after 1 s,* $|x|$ *settles under 0.5 for 1.5 s*

$$\varphi := \Box(x(t) > .5 \rightarrow \Diamond_{[0,1.]}\ (\Box_{[0,1.5]} x(t) < 0.5))$$



Robust Satisfaction Signal

Defined inductively on the structure of the formula:

$$
\begin{array}{rcl}
\rho^{\mu}(x,t) & = & f(x_1(t),\ldots,x_n(t)) \\
\rho^{\neg\varphi}(x,t) & = & -\rho^{\varphi}(x,t) \\
\rho^{\varphi_1 \wedge \varphi_2}(x,t) & = & \min(\rho^{\varphi_1}(x,t), \rho^{\varphi_2}(w,t)) \\
\rho^{\Box_{[a,b]}\varphi}(x,t) & = & \inf\limits_{\tau \in t+[a,b]} (\rho^{\varphi}(x,\tau)) \\
\rho^{\varphi_1 \mathbf{U}_{[a,b]} \varphi_2}(x,t) & = & \sup\limits_{\tau \in t+[a,b]} (\min(\rho^{\varphi_2}(x,\tau), \inf\limits_{s \in [t,\tau]} \rho^{\varphi_1}(x,s))
\end{array}
$$

Efficient offline algorithm (Donzé, Ferrère, Maler, CAV'13)

Challenge with online monitoring

Robust semantics on incomplete traces.

Example: what is $\Diamond_{[0,10]}(x > 0)$ for $x : [0,5] \mapsto \mathbb{R}$?

Robust Satisfaction Signal

Defined inductively on the structure of the formula:

$$
\begin{array}{lcl}
\rho^{\mu}(x,t) & = & f(x_1(t),\ldots,x_n(t)) \\
\rho^{\neg\varphi}(x,t) & = & -\rho^{\varphi}(x,t) \\
\rho^{\varphi_1 \wedge \varphi_2}(x,t) & = & \min(\rho^{\varphi_1}(x,t), \rho^{\varphi_2}(w,t)) \\
\rho^{\Box_{[a,b]}\varphi}(x,t) & = & \inf_{\tau \in t+[a,b]} (\rho^{\varphi}(x,\tau)) \\
\rho^{\varphi_1 \mathbf{U}_{[a,b]} \varphi_2}(x,t) & = & \sup_{\tau \in t+[a,b]} (\min(\rho^{\varphi_2}(x,\tau), \inf_{s\in[t,\tau]} \rho^{\varphi_1}(x,s))
\end{array}
$$

Efficient offline algorithm (Donzé, Ferrère, Maler, CAV'13)

Challenge with online monitoring

Robust semantics on incomplete traces.

Example: what is $\Diamond_{[0,10]}(x > 0)$ for $x : [0,5] \mapsto \mathbb{R}$?

Robust Online Monitoring with Partial Traces

At each step, we compute an upper bound and a lower bound for ρ.

- Whene $[\underline{\rho}, \bar{\rho}]$ becomes positive or negative, satisfaction is established.
- Connection with Boolean semantics on partial traces (weak vs strong satisfaction) (C.Eisner et al, *Reasoning with temporal logic on truncated paths*, CAV'03.)

Robust Online Monitoring with Partial Traces

At each step, we compute an upper bound and a lower bound for ρ.

- Whene $[\underline{\rho}, \bar{\rho}]$ becomes positive or negative, satisfaction is established.
- Connection with Boolean semantics on partial traces (weak vs strong satisfaction) (C.Eisner et al, *Reasoning with temporal logic on truncated paths*, CAV'03.)

Robust Online Monitoring with Partial Traces

At each step, we compute an upper bound and a lower bound for ρ.

- Whene $[\underline{\rho}, \bar{\rho}]$ becomes positive or negative, satisfaction is established.
- Connection with Boolean semantics on partial traces (weak vs strong satisfaction) (C.Eisner et al, *Reasoning with temporal logic on truncated paths,* CAV'03.)

Robust Online Monitoring with Partial Traces

At each step, we compute an upper bound and a lower bound for ρ.

- Whene $[\underline{\rho}, \bar{\rho}]$ becomes positive or negative, satisfaction is established.
- Connection with Boolean semantics on partial traces (weak vs strong satisfaction) (C.Eisner et al, *Reasoning with temporal logic on truncated paths*, CAV'03.)

Robust Online Monitoring with Partial Traces

At each step, we compute an upper bound and a lower bound for ρ.

- Whene $[\underline{\rho}, \bar{\rho}]$ becomes positive or negative, satisfaction is established.
- Connection with Boolean semantics on partial traces (weak vs strong satisfaction) (C.Eisner et al, *Reasoning with temporal logic on truncated paths*, CAV'03.)

Bounded Horizon Formulas

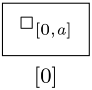
$$\Box_{[0,a]} \Big(\neg(y > 0) \vee \Diamond_{[b,c]}(x > 0)\Big)$$

The algorithm starts by determining the horizon of each operator:

Bounded Horizon Formulas

$$\square_{[0,a]}\left(\neg(y>0)\vee\lozenge_{[b,c]}(x>0)\right)$$

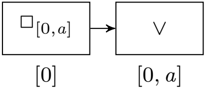
The algorithm starts by determining the horizon of each operator:



Bounded Horizon Formulas

$$\square_{[0,a]} \Big(\neg(y > 0) \vee \Diamond_{[b,c]}(x > 0) \Big)$$

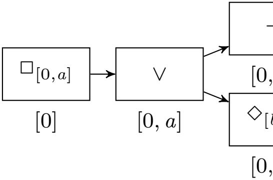
The algorithm starts by determining the horizon of each operator:



Bounded Horizon Formulas

$$\Box_{[0,a]} \left(\neg(y > 0) \vee \Diamond_{[b,c]}(x > 0)\right)$$

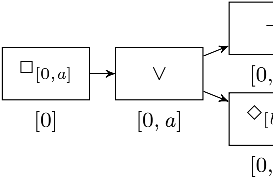
The algorithm starts by determining the horizon of each operator:

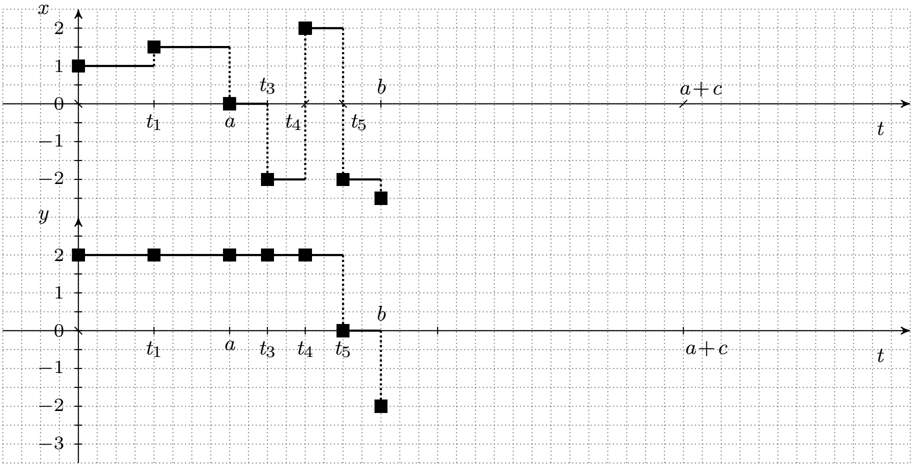


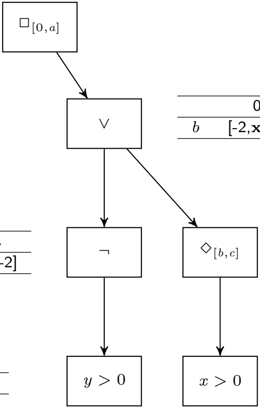
Bounded Horizon Formulas

$$\Box_{[0,a]}\left(\neg(y > 0) \vee \Diamond_{[b,c]}(x > 0)\right)$$

The algorithm starts by determining the horizon of each operator:




x
2
1
0
−1
−2
t1
a
t3
t4
t5
b
a+c
t
y
2
1
0
−1
−2
−3
t1
a
t3
t4
t5
b
a+c
t



	0
b	[-2,$\mathbf{x}_{\text{sup}}$)

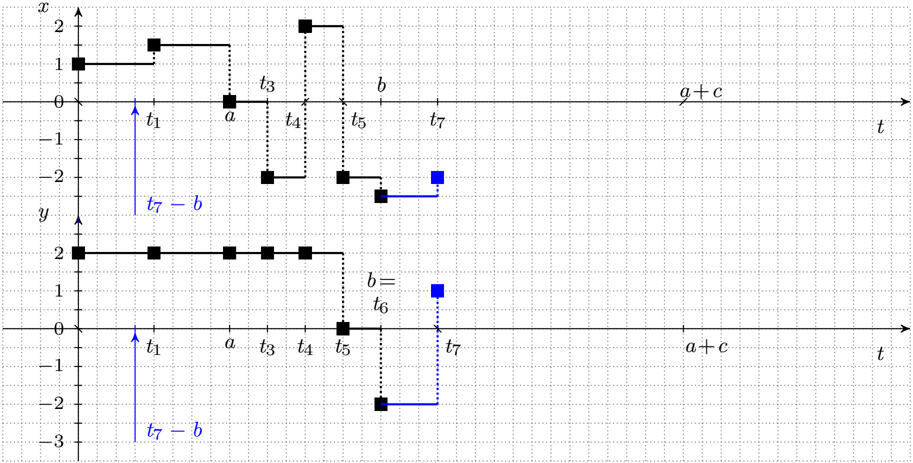
	0	a
b	[-2,$\mathbf{x}_{\text{sup}}$)	[-2,$\mathbf{x}_{\text{sup}}$)

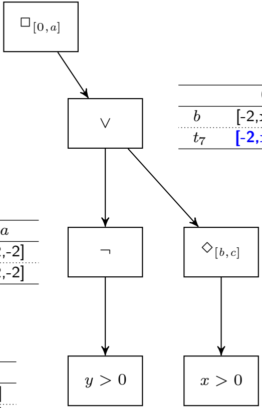
	0	a
b	[-2,-2]	[-2,-2]

	0	a
b	[-2.5,$\mathbf{x}_{\text{sup}}$)	$(\mathbf{x}_{\text{inf}}, \mathbf{x}_{\text{sup}})$

	0	a
b	[2,2]	[2,2]

	b	$a+c$
b	[-2.5,-2.5]	$(\mathbf{x}_{\text{inf}}, \mathbf{x}_{\text{sup}})$


x
2
1
0
−1
−2
t_3
b
$a+c$
t_1
a
t_4
t_5
t_7
t
$t_7 - b$
y
2
1
0
−1
−2
−3
$b =$
t_6
t_1
a
t_3
t_4
t_5
t_7
$a+c$
t
$t_7 - b$



	0
b	[-2,$\mathbf{x}_{\text{sup}}$)
t_7	**[-2,$\mathbf{x}_{\text{sup}}$)**

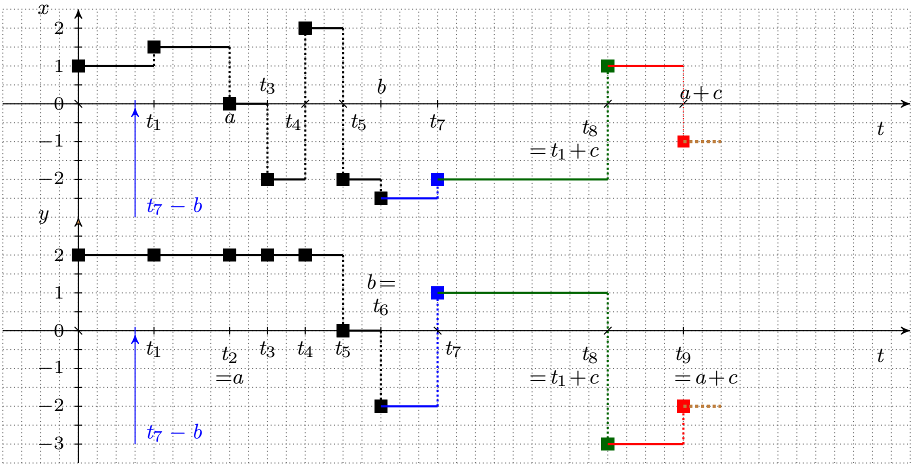
	0	$t_7 - b$	a
b	[-2,$\mathbf{x}_{\text{sup}}$)	$--$	[-2,$\mathbf{x}_{\text{sup}}$)
t_7	**[-2,$\mathbf{x}_{\text{sup}}$)**	**[-2,$\mathbf{x}_{\text{sup}}$)**	[-2,$\mathbf{x}_{\text{sup}}$)

	0	a
b	[-2,-2]	[-2,-2]
t_7	[-2,-2]	[-2,-2]

	0	$t_7 - b$	a
b	[-2.5,$\mathbf{x}_{\text{sup}}$)	$--$	($\mathbf{x}_{\text{inf}}$, $\mathbf{x}_{\text{sup}}$)
t_7	**[-2,$\mathbf{x}_{\text{sup}}$)**	**[-2,$\mathbf{x}_{\text{sup}}$)**	($\mathbf{x}_{\text{inf}}$, $\mathbf{x}_{\text{sup}}$)

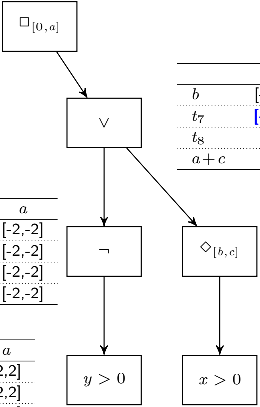
	0	a
b	[2,2]	[2,2]
t_7	[2,2]	[2,2]

	b	t_7	$a + c$
b	[-2.5,-2.5]	$--$	($\mathbf{x}_{\text{inf}}$, $\mathbf{x}_{\text{sup}}$)
t_7	[-2.5,-2.5]	**[-2,-2]**	($\mathbf{x}_{\text{inf}}$, $\mathbf{x}_{\text{sup}}$)



x
2
1
0
−1
−2
t_3
b
$a+c$
t_1
a
t_4
t_5
t_7
t_8
$=t_1+c$
t
t_7-b
y
2
1
0
−1
−2
−3
$b=$
t_6
t_1
t_2
$=a$
t_3
t_4
t_5
t_7
t_8
$=t_1+c$
t_9
$=a+c$
t
t_7-b

	0
b	$[-2,\mathbf{x}_{sup})$
t_7	**$[-2,\mathbf{x}_{sup})$**
t_8	**$[1,\mathbf{x}_{sup})$**
$a+c$	**[1,1]**



	0	$t_7 - b$	$t_8 - c$	a
b	$[-2,\mathbf{x}_{sup})$	$--$	$[-2,\mathbf{x}_{sup})$	$[-2,\mathbf{x}_{sup})$
t_7	**$[-2,\mathbf{x}_{sup})$**	**$[-2,\mathbf{x}_{sup})$**	$[-2,\mathbf{x}_{sup})$	$[-2,\mathbf{x}_{sup})$
t_8	**[1,1]**	**$[1,\mathbf{x}_{sup})$**	**$[1,\mathbf{x}_{sup})$**	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
$a+c$	**[1,1]**	**[1,1]**	**[1,1]**	**[1,1]**

	0	a
b	[-2,-2]	[-2,-2]
t_7	[-2,-2]	[-2,-2]
t_8	[-2,-2]	[-2,-2]
$a+c$	[-2,-2]	[-2,-2]

	0	$t_7 - b$	$t_8 - c$	a
b	$[-2.5,\mathbf{x}_{sup})$	$--$	$--$	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
t_7	**$[-2,\mathbf{x}_{sup})$**	**$[-2,\mathbf{x}_{sup})$**	$--$	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
t_8	**[1,1]**	**$[1,\mathbf{x}_{sup})$**	**$[1,\mathbf{x}_{sup})$**	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
$a+c$	**[1,1]**	**[1,1]**	**[1,1]**	**[1,1]**

	0	a
b	[2,2]	[2,2]
t_7	[2,2]	[2,2]
t_8	[2,2]	[2,2]
$a+c$	[2,2]	[2,2]

	b	t_7	t_8	$a+c$
b	[-2.5,-2.5]	$--$	$--$	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
t_7	[-2.5,-2.5]	**[-2,-2]**	$--$	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
t_8	[-2.5,-2.5]	[-2,-2]	**[1,1]**	$(\mathbf{x}_{inf}, \mathbf{x}_{sup})$
$a+c$	[-2,-2]	[-2,-2]	[1,1]	**[-1,-1]**

Unbounded Horizon Formulas

Theorem

For ψ bounded and non-zeno signals, each φ listed below can be monitored in an online fashion using bounded memory.

1. $\Box\psi$, $\Diamond\psi$
2. $\varphi\mathbf{U}\psi$,
3. $\Box\Diamond\psi$ *(dually* $\Diamond\Box\psi$*)*,
4. $\Box(\varphi \vee \Diamond\psi)$ *(dually* $\Diamond(\varphi \wedge \Box\psi)$*)*,
5. $\Diamond(\varphi \wedge \Diamond\psi)$, $\Box(\varphi \vee \Box\psi)$

Proof sketch for 1.

$$\begin{aligned}\rho^{\Box\psi}_{n+1} &= \min(\rho^{\psi}_0, \rho^{\psi}_1, \ldots, \rho^{\psi}_n, \rho^{\psi}_{n+1}) = \min(\min(\rho^{\psi}_0, \rho^{\psi}_1, \ldots, \rho^{\psi}_n), \rho^{\psi}_{n+1}) \\ &= \min(\rho^{\Box\psi}_n, \rho^{\psi}_{n+1})\end{aligned}$$

If for all n, ρ^{ψ}_n needs at most $O(k)$ units of memory, then so does $\rho^{\Box\psi}_n$

Unbounded Horizon Formulas

Theorem

For ψ bounded and non-zeno signals, each φ listed below can be monitored in an online fashion using bounded memory.

1. $\Box\psi$, $\Diamond\psi$
2. $\varphi\mathbf{U}\psi$,
3. $\Box\Diamond\psi$ *(dually $\Diamond\Box\psi$)*,
4. $\Box(\varphi \vee \Diamond\psi)$ *(dually $\Diamond(\varphi \wedge \Box\psi)$)*,
5. $\Diamond(\varphi \wedge \Diamond\psi)$, $\Box(\varphi \vee \Box\psi)$

Proof sketch for 1.

$$\begin{aligned}\rho^{\Box\psi}_{n+1} &= \min(\rho^{\psi}_{0}, \rho^{\psi}_{1}, \ldots, \rho^{\psi}_{n}, \rho^{\psi}_{n+1}) = \min(\min(\rho^{\psi}_{0}, \rho^{\psi}_{1}, \ldots, \rho^{\psi}_{n}), \rho^{\psi}_{n+1}) \\ &= \min(\rho^{\Box\psi}_{n}, \rho^{\psi}_{n+1})\end{aligned}$$

If for all n, ρ^{ψ}_{n} needs at most $O(k)$ units of memory, then so does $\rho^{\Box\psi}_{n}$

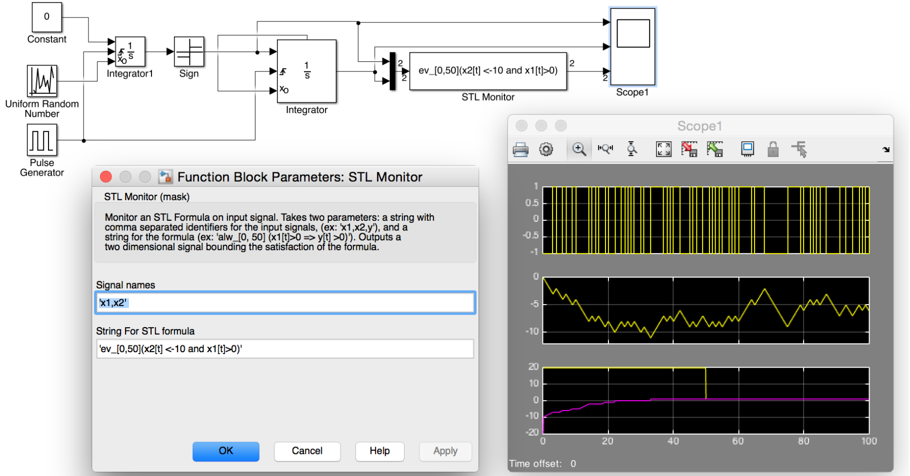
Experimental Results

Evaluation of online monitoring for autograding a CPS lab assignement

STL Test	#Tr	#ET	Simulation Time (mins)		Overhead (secs)	
			Offline	Online	Naïve	Alg. 2
avoid_front	1776	466	296	258	553	9
avoid_left	1778	471	296	246	1347	30
avoid_right	1778	583	296	226	1355	30
hill_climb$_1$	1777	19	395	394	919	11
hill_climb$_2$	1556	176	259	238	423	7
hill_climb$_3$	1556	124	259	248	397	7
keep_bump	1775	468	296	240	12E3	268
what_hill	1556	71	259	268	19E3	1526

(#Tr:number of traces, #ET: number of early termination)

Implementation in Simulink



Experimental Results

Diesel engine model (~3000 blocks) with the following requirements:

$$\varphi_{overshoot} = \square_{[a,b]}(\mathbf{x} < c)$$
$$\varphi_{transient} = \square_{[a,b]}(|\mathbf{x}| > c \implies (\Diamond_{[0,d]}|\mathbf{x}| < e))$$

Results with different valuations of parameters (a, b, c, d, e)

Requirement	#Tr	#ET	Time taken (hours)	
			Offline	Online
$\varphi_{overshoot}(\nu_1)$	1000	801	33.3803	26.1643
$\varphi_{overshoot}(\nu_2)$	1000	239	33.3805	30.5923
$\varphi_{overshoot}(\nu_3)$	1000	0	33.3808	33.4369
$\varphi_{transient}(\nu_4)$	1000	595	33.3822	27.0405
$\varphi_{transient}(\nu_5)$	1000	417	33.3823	30.6134

Related Work

- Rosu, Havelund, LTL runtime verification, rewriting
- Nickovic et al, STL incremental monitoring, past operators
- Ouaknine et al, MTL online monitoring, rewriting
- Fainekos et al, MTL robust monitoring, past operators, predictors

Future Work

- Further tweaking and optimization
- Generalization of results on unbounded horizon formulas
- Active vs passive monitoring
- Implementation on embedded platforms

Related Work

- Rosu, Havelund, LTL runtime verification, rewriting
- Nickovic et al, STL incremental monitoring, past operators
- Ouaknine et al, MTL online monitoring, rewriting
- Fainekos et al, MTL robust monitoring, past operators, predictors

Future Work

- Further tweaking and optimization
- Generalization of results on unbounded horizon formulas
- Active vs passive monitoring
- Implementation on embedded platforms