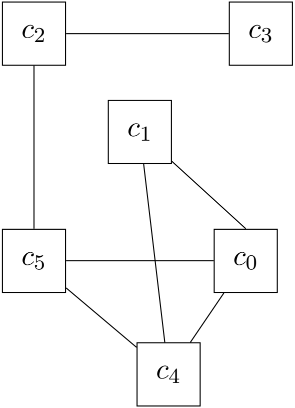
Reasoning with Metric Temporal Logic and Resettable Skewed Clocks

Alberto Bombardelli   Stefano Tonetta

Fondazione Bruno Kessler - Trento, Italy
University of Trento, Italy

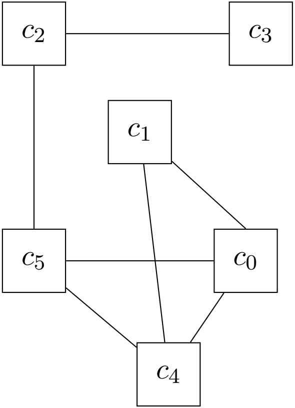
May 16, 2023

Motivation



DRTS: Distributed Real Time Systems

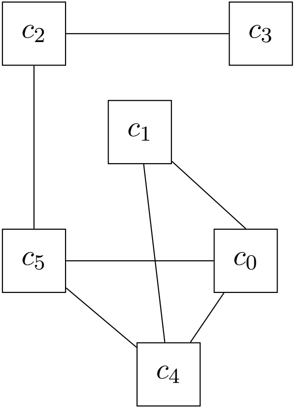
Motivation



DRTS: Distributed Real Time Systems

- **Multiple components**

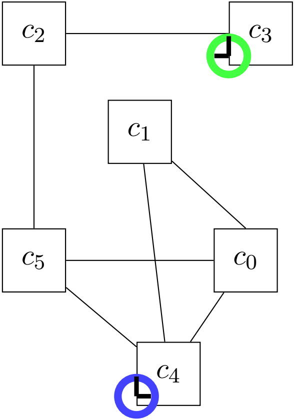
Motivation



DRTS: Distributed Real Time Systems

- **Multiple components**
- **Message passing**

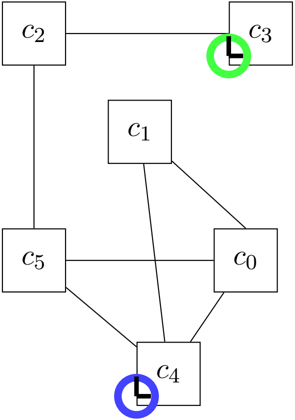
Motivation



DRTS: Distributed Real Time Systems

- **Multiple components**
- **Message passing**
- **Local time**

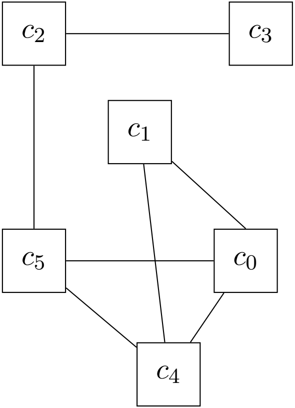
Motivation



DRTS: Distributed Real Time Systems

- **Multiple components**
- **Message passing**
- **Local time**
- **Synchronization** e.g. Berkeley algorithm

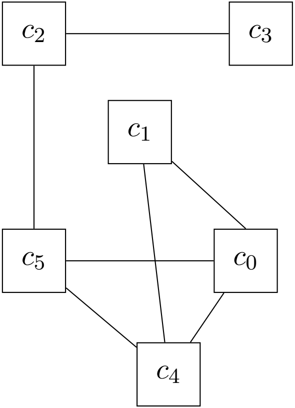
Motivation



DRTS: Distributed Real Time Systems

- **Multiple components**
- **Message passing**
- **Local time**
- **Synchronization** e.g. Berkeley algorithm
- **Timing constraints**

Motivation

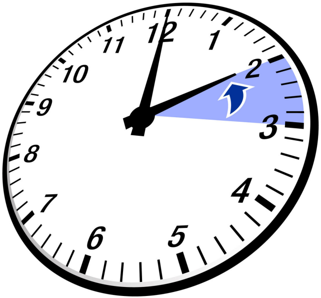


DRTS: Distributed Real Time Systems

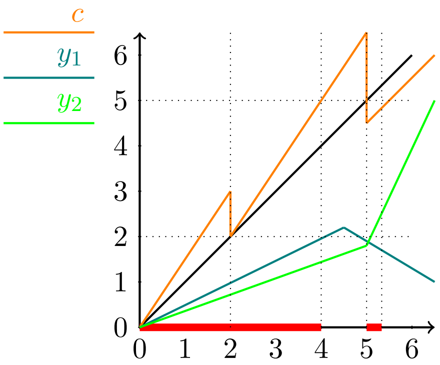
- **Multiple components**
- **Message passing**
- **Local time**
- **Synchronization** e.g. Berkeley algorithm
- **Timing constraints**

Verification of timed properties: MTL

Clock synchronization: Non-monotonicity problem

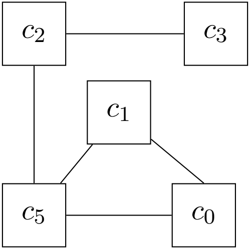


- Distributed MTL: $U_{\mathcal{I}}^{c}$
- Time can decrease with resets
- Timed model checking relies on *time monotonicity*
- Non-monotonic MTL only studied theoretically (data-words + decidability) (Carapelle *et al.*, 2014)

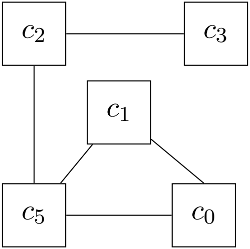


- $\varphi_i := G_{\leq 5}^{c}(y_i \leq 2)\ \forall i \in \{1,2\}$
- φ_i holds iff $y_i \leq 2$ holds in [0,4] and [5, 16/3]

Application: Compositional verification

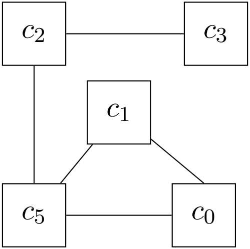


$$\models \varphi_{sys}$$

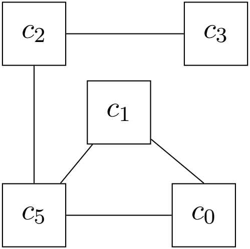


$$\models \varphi_{sys} \xrightarrow{\text{Sync.}} SyncAlg \models \varphi_{sync}$$

Application: Compositional verification



$$\begin{tikzcd} & SyncAlg \models \varphi_{sync} \\ \models \varphi_{sys} \arrow[ur, bend left, "\text{Sync.}"] \arrow[r, bend left, "\text{Local}"] & M_i \models \varphi_{sync} \to \varphi_i \end{tikzcd}$$



$\models \varphi_{sys}$

Sync. $\rightarrow$ $SyncAlg \models \varphi_{sync}$

Local $\rightarrow$ $M_i \models \varphi_{sync} \rightarrow \varphi_i$

Global $\rightarrow$ $\bigotimes_i (\varphi_i) \land \varphi_{sync} \rightarrow \varphi_{sys}$

Background

Notion of time:

Background

Notion of time:

Discrete: $\bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \dots$

- Singular intervals $[\bullet]$ (only 1 time point)

Notion of time:

Discrete: $\bullet\!\longrightarrow\!\bullet\!\longrightarrow\!\bullet\!\longrightarrow \dots$

Super-dense: $(\text{—})[\bullet](\text{—}](\text{—})[\bullet] \dots$

- Singular intervals $[\bullet]$ (only 1 time point)
- Open intervals (—) (densely infinite time points)

Background

Notion of time:

Discrete: $\bullet\!\longrightarrow\!\bullet\!\longrightarrow\!\bullet\!\longrightarrow \ldots$ Super-dense: (—)[•](—](—)[•] ...

- Singular intervals [•] (only 1 time point)
- Open intervals (—) (densely infinite time points)

Metric Temporal Logic (MTL):

- Extend LTL with bounds on modalities, e.g. $F_{\leq 5}a$
- $F_{\leq 5}a$ means *"a will become true once in at most 5 time units"*

Background

Notion of time:

Discrete: $\bullet\!\longrightarrow\!\bullet\!\longrightarrow\!\bullet\!\longrightarrow \ldots$ Super-dense: (—)[•](—](—)[•] . . .

- Singular intervals [•] (only 1 time point)
- Open intervals (—) (densely infinite time points)

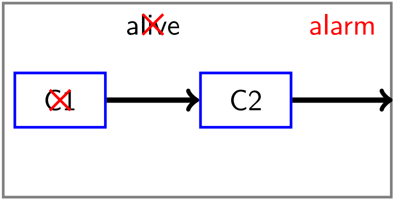
Metric Temporal Logic (MTL):

- Extend LTL with bounds on modalities, e.g. $F_{\leq 5}a$
- $F_{\leq 5}a$ means "*a will become true once in at most 5 time units*"

Distributed MTL:

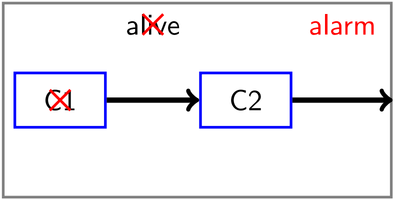
- Extend MTL referring bounds to clock values, $F^{c}{}_{\leq 5}a$
- $F^{c}{}_{\leq 5}a$ means "*a will become true once in at most 5 clock time units*"
- Clock assumptions:
  1. Clocks are *differentiable* in *dense* intervals $\frac{d\pi(t)(c)}{dt} \in [1-\epsilon, 1+\epsilon]$
  2. Clocks diverge

Example



$$G(fault \rightarrow G^{cl_1}_{\leq p} \neg alive) \wedge$$
$$G(G^{cl_2}_{\leq p} \neg alive \rightarrow (F^{cl_2}_{\leq p} alarm)) \rightarrow$$
$$G(fault \rightarrow F^{cl}_{\leq p} alarm)$$

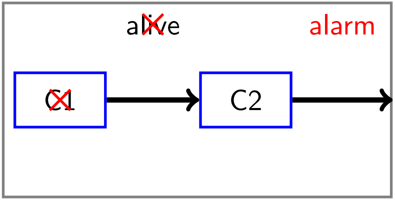
Example



If clocks are **perfect**: *Valid*

$$G(fault \rightarrow G^{cl_1}_{\leq p} \neg alive) \wedge$$
$$G(G^{cl_2}_{\leq p} \neg alive \rightarrow (F^{cl_2}_{\leq p} alarm)) \rightarrow$$
$$G(fault \rightarrow F^{cl}_{\leq p} alarm)$$

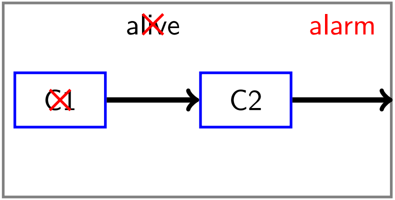
Example



$$G(fault \to G^{cl_1}_{\leq \tilde{p}} \neg alive) \wedge$$
$$G(G^{cl_2}_{\leq p} \neg alive \to (F^{cl_2}_{\leq p} alarm)) \to$$
$$G(fault \to F^{cl}_{\leq \tilde{p}} alarm)$$

Valid with $\tilde{p} = p(1 + 2\epsilon/(1-\epsilon))$ and **no reset**

Example

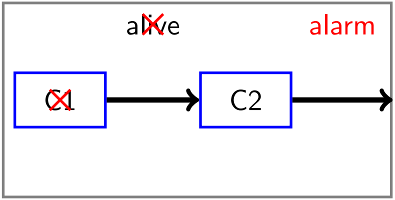


$$G(fault \rightarrow G^{cl_1}_{\leq p+4\tilde{q}} \neg alive) \wedge$$
$$G(G^{cl_2}_{\leq p} \neg alive \rightarrow (F^{cl_2}_{\leq p} alarm)) \rightarrow$$
$$G(fault \rightarrow F^{cl}_{\leq p+4\tilde{q}} alarm)$$

with $\tilde{q} = q(1 + 2\epsilon/(1-\epsilon))$

If $cl1$ and $cl2$ are synchronized to cl every q : property **Valid** ($q \ll p$)

Example



$$G(fault \rightarrow G^{cl_1}_{\leq p+4\tilde{q}} \neg alive) \wedge$$
$$G(G^{cl_2}_{\leq p} \neg alive \rightarrow (F^{cl_2}_{\leq p} alarm)) \rightarrow$$
$$G(fault \rightarrow F^{cl}_{\leq p+4\tilde{q}} alarm)$$

with $\tilde{q} = q(1 + 2\epsilon/(1-\epsilon))$

If $cl1$ and $cl2$ are synchronized to cl every q : property **Valid** $(q \ll p)$

"Compositional" case:

- $\psi_{sync} :=$
  $G \bigwedge_{i \in \{1,2\}} (F^{cl_i}_{\leq q}(next(cl_i) = cl) \wedge (change(cl_i) \rightarrow next(cl_i) = cl))$
- Prove $\psi_{sync} \rightarrow G(|cl_1 - cl_2| \leq r)$
- Prove $G(|cl_1 - cl_2| \leq r)$ entails the property

MTLSK(Bombardelli & Tonetta, 2023)

Syntax:

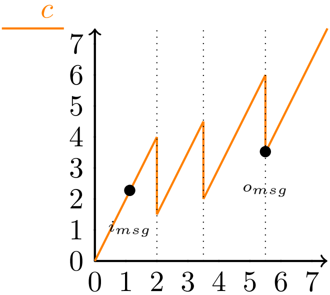
$$\text{MTLSK} : \phi := \cdots \mid \overbrace{\phi_1 U^c_{\mathcal{I}} \phi_2}^{\text{"Distributed until"}} \mid \overbrace{\phi_1 \overline{U}^c_{\mathcal{I}} \phi_2}^{\text{"Strict distr. until"}} \quad (\mathcal{I} \text{ is an interval of } \mathbb{R})$$

MTLSK(Bombardelli & Tonetta, 2023)

Syntax:

$$\text{MTLSK}: \phi := \cdots \mid \overbrace{\phi_1 U^c_{\mathcal{I}} \phi_2}^{\text{"Distributed until"}} \mid \overbrace{\phi_1 \overline{U}^c_{\mathcal{I}} \phi_2}^{\text{"Strict distr. until"}} \quad (\mathcal{I} \text{ is an interval of } \mathbb{R})$$

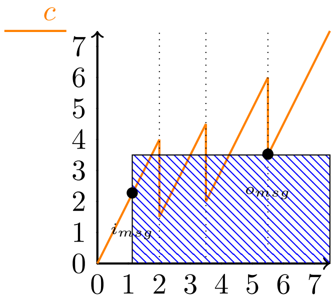
Semantics (by example)



Syntax:

$$\text{MTLSK}: \phi := \cdots \mid \overbrace{\phi_1 U^c_{\mathcal{I}} \phi_2}^{\text{"Distributed until"}} \mid \overbrace{\phi_1 \overline{U}^c_{\mathcal{I}} \phi_2}^{\text{"Strict distr. until"}} \quad (\mathcal{I} \text{ is an interval of } \mathbb{R})$$

Semantics (by example)



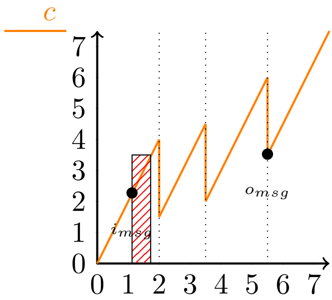
$$\varphi_{blue} := G(r(i_{msg}) \rightarrow F^c_{\leq 5/4} s(o_{msg}))$$

MTLSK(Bombardelli & Tonetta, 2023)

Syntax:

$$\text{MTLSK} : \phi := \cdots \mid \overbrace{\phi_1 U^c_{\mathcal{I}} \phi_2}^{\text{"Distributed until"}} \mid \overbrace{\phi_1 \overline{U}^c_{\mathcal{I}} \phi_2}^{\text{"Strict distr. until"}} \quad (\mathcal{I} \text{ is an interval of } \mathbb{R})$$

Semantics (by example)



$$\varphi_{blue} := G(r(i_{msg}) \rightarrow F^c_{\leq 5/4} s(o_{msg}))$$

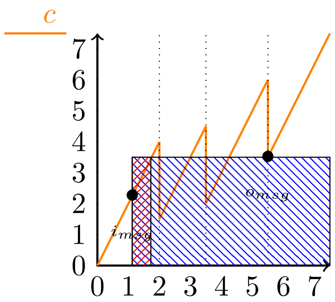
$$\varphi_{red} := G(r(i_{msg}) \rightarrow \overline{F}^c_{\leq 5/4} s(o_{msg}))$$

MTLSK(Bombardelli & Tonetta, 2023)

Syntax:

$$\text{MTLSK}: \phi := \cdots \mid \overbrace{\phi_1 U^c_{\mathcal{I}} \phi_2}^{\text{"Distributed until"}} \mid \overbrace{\phi_1 \overline{U}^c_{\mathcal{I}} \phi_2}^{\text{"Strict distr. until"}} \quad (\mathcal{I} \text{ is an interval of } \mathbb{R})$$

Semantics (by example)



$$\varphi_{blue} := G(r(i_{msg}) \to F^c_{\leq 5/4} s(o_{msg}))$$

$$\varphi_{red} := G(r(i_{msg}) \to \overline{F}^c_{\leq 5/4} s(o_{msg}))$$

φ_{blue} holds. φ_{red} does not hold.

Contribution

Verification of a parametrized fragment of MTLSK:

- Extends boolean logic with theories over reals (arithmetic, next, ...).
- Parameterized bounds ($F^c_{\leq p}$ where p is a parameter).
- Limits bounds to $\lhd p$ and $\rhd p$ where $\lhd \in \{<, \leq\}, \rhd \in \{\geq, >\}$.

Contribution

Verification of a parametrized fragment of MTLSK:

- Extends boolean logic with theories over reals (arithmetic, next, ...).
- Parameterized bounds ($F^c_{\leq p}$ where p is a parameter).
- Limits bounds to $\lhd p$ and $\rhd p$ where $\lhd \in \{<, \leq\}, \rhd \in \{\geq, >\}$.

High level idea:

Reduce to LTL-$\mathcal{T}$ model checking (inspired by (Cimatti *et al.*, 2019)):

1. Consider a "convenient" intermediate logic
2. Encode $MTLSK$ into that logic
3. Discretize model + logic (from $(—)\longrightarrow\bullet$to $\bullet\longrightarrow\bullet\longrightarrow\bullet$)
4. Encode intermediate logic to LTL-$\mathcal{T}$

Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

Can we apply it to MTLSK?

Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

Can we apply it to MTLSK? (Spoiler: No!)

Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

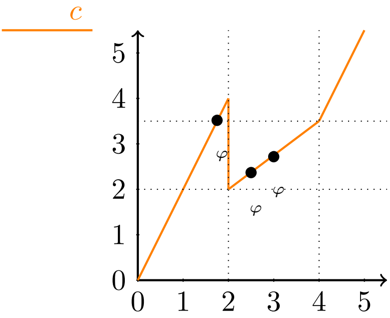
- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

Can we apply it to MTLSK? (Spoiler: No!)

Example 1:

Is $F^{c}_{\leq 3}\varphi$ satisfied?

$c\ at\ next\ \varphi - c \leq 3?$



Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

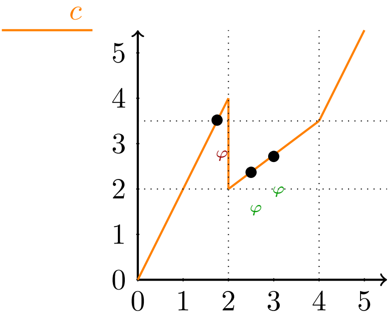
Can we apply it to MTLSK? (Spoiler: No!)

Example 1:

Is $F^{c}_{\leq 3}\varphi$ satisfied? Yes!

$c\ at\ next\ \varphi - c \leq 3?$ No! :(

Problem: at next does not consider points after the reset



Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

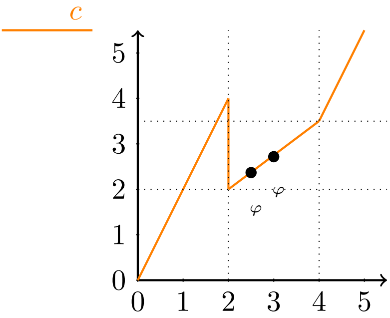
- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

Can we apply it to MTLSK? (Spoiler: No!)

Example 2:

Is $\overline{F}^{c}_{\leq 3}\varphi$ satisfied?

$c\ at\ next\ \varphi - c \leq 3?$



Encoding: part 1-2

($MTL_{0,+\infty}$)(Cimatti et al., 2019):

- What is the value of time at the first encounter of φ?
- Exploit time monotonicity.
- $F_{\leq p}\varphi \approx time\ at\ next\ \varphi - time \leq p$

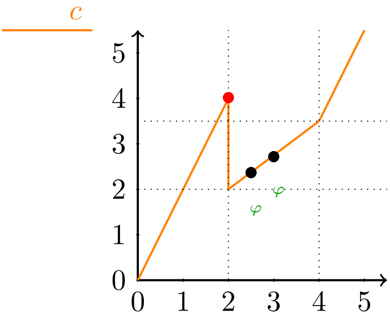
Can we apply it to MTLSK? (Spoiler: No!)

Example 2:

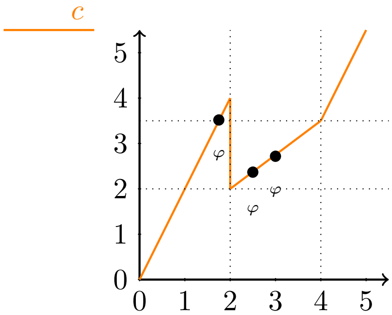
Is $\overline{F}^{c}_{\leq 3}\varphi$ satisfied? No! :(

$c\ at\ next\ \varphi - c \leq 3$? Yes!

Problem: at next does not consider points surpassing the threshold!

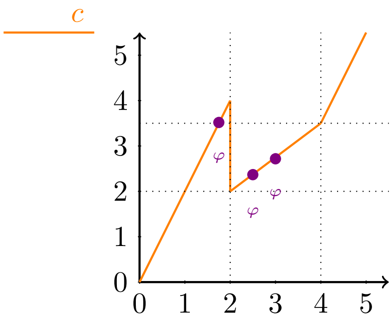


- $F^{c}_{\lhd p}\varphi$:
- $F^{c}_{\rhd p}\varphi$:
- $\overline{F}^{c}_{\lhd p}\varphi$:



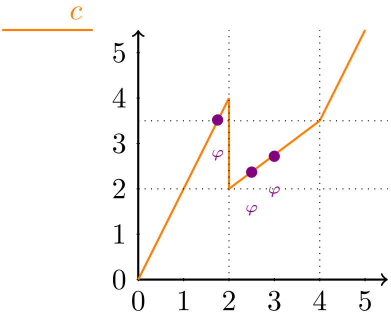
Encoding: part 1-2 (contd)

- $F^{c}_{\lhd p}\varphi$:   Is $min(\blacksquare_{\varphi}) - c \lhd p$
- $F^{c}_{\rhd p}\varphi$:
- $\overline{F}^{c}_{\lhd p}\varphi$:



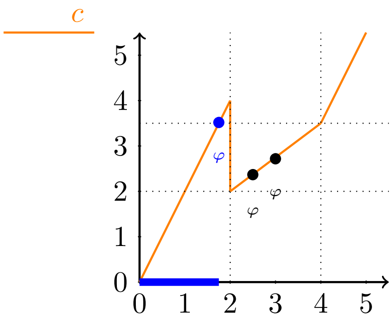
Encoding: part 1-2 (contd)

- $F^c_{\lhd p}\varphi$: Is $min(\blacksquare_\varphi) - c \lhd p$
- $F^c_{\rhd p}\varphi$: Is $max(\blacksquare_\varphi) - c \rhd p$
- $\overline{F}^c_{\lhd p}\varphi$:



Encoding: part 1-2 (contd)

- $F^{c}_{\lhd p}\varphi$: Is $min(\blacksquare_{\varphi}) - c \lhd p$
- $F^{c}_{\rhd p}\varphi$: Is $max(\blacksquare_{\varphi}) - c \rhd p$
- $\overline{F}^{c}_{\lhd p}\varphi$: Is $max(\blacksquare_{\varphi}) - c \lhd p$



Encoding: part 3-4

Discretization:

Produce an equisatisfiable φ_D as follows:

1. *Global time* encoded as *real* diverging variable
2. In each open interval every subformula φ' do not change its value
3. Each interval encoded as two points: $(\text{—}) \Rightarrow \bullet\!\longrightarrow\!\bullet$
4. Clocks are encoded as differences w.r.t. *time varable*

Encoding: part 3-4

Discretization:

Produce an equisatisfiable φ_D as follows:

1. *Global time* encoded as *real* diverging variable
2. In each open interval every subformula φ' do not change its value
3. Each interval encoded as two points: $(\text{—}) \Rightarrow \bullet \longrightarrow \bullet$
4. Clocks are encoded as differences w.r.t. *time varable*

Intermediate logic to LTL-$\mathcal{T}$:

- Operators mapped to equisat monitors
- Encoding min/max in discrete time is easier
- Technicalities/assumptions to guarantees existence of min/max.

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
    - Most tautologies proved in less than 10 sec

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
    - Most tautologies proved in less than 10 sec
    - Half of the tautologies were proved in less that 2 sec

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
   - Most tautologies proved in less than 10 sec
   - Half of the tautologies were proved in less that 2 sec
   - All the invalid formulae were disproved by BMC in less than 2 second

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
   - Most tautologies proved in less than 10 sec
   - Half of the tautologies were proved in less that 2 sec
   - All the invalid formulae were disproved by BMC in less than 2 second
2. Parametric models on amount of components

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
    - Most tautologies proved in less than 10 sec
    - Half of the tautologies were proved in less that 2 sec
    - All the invalid formulae were disproved by BMC in less than 2 second
2. Parametric models on amount of components
3. Timed simplification of Wheel Brake System

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
   - Most tautologies proved in less than 10 sec
   - Half of the tautologies were proved in less that 2 sec
   - All the invalid formulae were disproved by BMC in less than 2 second
2. Parametric models on amount of components
3. Timed simplification of Wheel Brake System
4. Experiments instantiated parameters λ and ϵ

Results

Implementation:

- Implemented inside timed nuXmv(Cimatti *et al.*, 2019)
- Algorithm klive ic3-ia(Cimatti *et al.*, 2014a) and kzeno(Cimatti *et al.*, 2014b) (in lockstep with BMC) and BMC.
- Use of model parameters λ (max dist. c time during discrete transitions) and ϵ (derivative drift w.r.t. time)

Experiments:

1. ≈ 60 valid and ≈ 40 invalid properties to validate semantics
2. Parametric models on amount of components
3. Timed simplification of Wheel Brake System
4. Experiments instantiated parameters λ and ϵ

Overall:

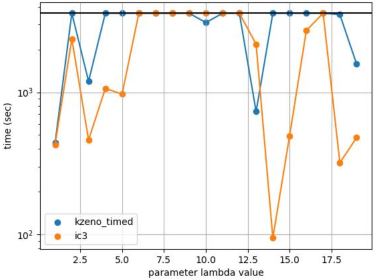
- ≈ 400 valid instances (per alg.): < 2 sec ≈ 40, < 10 sec ≈ 90, < 2 min ≈ 190 and < 10 min ≈ 270
- ≈ 240 invalid instances (BMC): < 2 sec ≈ 220, < 10 sec $= 228$, < 2 min $= 231$ and < 10 min $= 232$

Result table (subset)

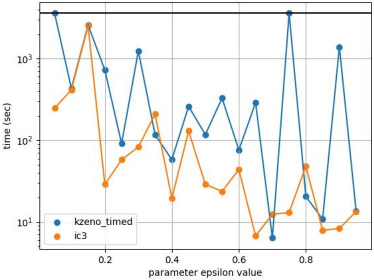
Formula	Time in sec.	λ	ϵ	alg	valid
$G(\overline{F}^{c}_{\leq p} a \rightarrow F^{c}_{\leq p} a)$	2.81	any	any	ic3	True
$F(c = p) \rightarrow F(((\overline{G}^{c}_{\leq p} a) \wedge (\overline{G}^{c}_{\geq p} \neg a)) \rightarrow \perp)$	3.62	any	0.4	kzeno	True
$(q \geq p) \rightarrow G((\overline{G}^{c}_{\leq q} a) \rightarrow (\overline{G}^{c}_{\leq p} a))$	0.38	any	any	ic3	True
$G^{c}_{\leq p} a \rightarrow G(a \vee c > p)$	9.03	any	any	kzeno	True
$G^{c}_{\leq p} a \rightarrow G(a \vee c > p)$	1.09	any	any	ic3	True
$(q \geq p) \rightarrow G((G^{c}_{\geq p} a) \rightarrow (G^{c}_{\geq q} a))$	2.22	any	any	ic3	True
$\Phi_{exp} := q = p(2 + \epsilon) + 2\lambda \wedge (G(fault \rightarrow G\neg alive) \wedge G(\overline{G}^{cl}_{\leq p} \neg alive \rightarrow (\overline{F}^{cl}_{\leq p} alarm))) \rightarrow G(fault \rightarrow F_{[0,q]} alarm)$	94.26	14.0	0.1	ic3	True
$(G((\mathit{Reset}(cl1) \rightarrow next(cl1) = cl) \wedge (\neg \mathit{Reset}(cl))) \wedge GF^{cl}_{\leq q}(next(cl) = cl1)) \rightarrow G(cl - cl1 \leq q * (1 + 2\epsilon/(1 - \epsilon)))$	7.05	any	any	kzeno	True
$G(f \rightarrow \overline{G}^{cl1}_{\leq p} \neg alv) \wedge G(\overline{G}^{cl2}_{\leq p-4r} \neg alv \rightarrow (\overline{F}^{cl2}_{\leq p} alm))) \rightarrow G(f \rightarrow \overline{F}^{cl}_{\leq p+2r} alm)$	19.86	any	any	ic3	True
$G(F^{c}_{\leq p} a \rightarrow \overline{F}^{c}_{\leq p} a)$	0.27	any	any	bmc	False
$G((a \vee Xa) \rightarrow (F^{c}_{\leq 0} a \wedge F^{c}_{\geq 0} a))$	0.18	any	any	bmc	False
Bounded Response invalid with 11 clocks	1.36	any	any	bmc	False

Table: Some MTLSK properties and their verification results.

Results - λ and ϵ

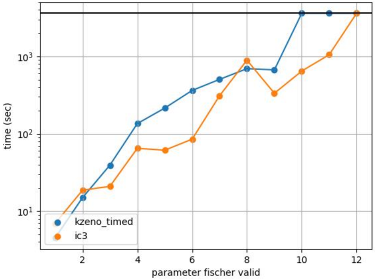


(a) λ evaluation

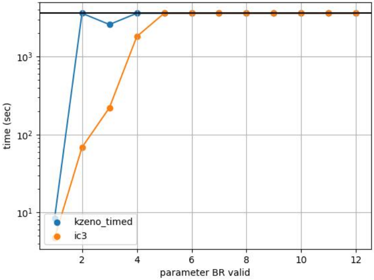


(b) ϵ evaluation

Results - parametric formulae



(a) Fischer experimental evaluation



(b) BR experimental evaluation

Conclusion and future work

Conclusion

- Studied non-monotonic MTL encoding to discrete LTL
- MTLSK verification implemented as an extension of *timed nuXmv* with *interval semantics*.

Conclusion and future work

Conclusion

- Studied non-monotonic MTL encoding to discrete LTL
- MTLSK verification implemented as an extension of *timed nuXmv* with *interval semantics*.

Future work:

- Efficient techniques to find counterexample using BMC as in(Bu *et al.*, 2010)
- Study async compositional with I/O components as in(Bombardelli & Tonetta, 2022)
- Case studies on Biphase Mark protocol, 8N1 protocol, ...
- Relax constraints on clocks for synchronization algorithms

Questions?

Notion of time

Time model $\tau = \langle \underbrace{T}_{\text{Temporal Domain}}, \overbrace{<}^{\text{Total order}}, \underbrace{\mathbf{0}}_{\text{Minimum element}}, \overbrace{\nu}^{\nu : T \to \mathbb{R}_0^+} \rangle$

Notion of time

Time model $\tau = \langle \underbrace{T}_{\text{Temporal Domain}}, \overbrace{<}^{\text{Total order}}, \underbrace{\mathbf{0}}_{\text{Minimum element}}, \overbrace{\nu}^{\nu : T \to \mathbb{R}_0^+} \rangle$

- *Discrete:* (pointwise)$T = \mathbb{N}, \mathbf{0} = 0, \nu(0), \nu(1), \ldots$ is a non-decreasing divergent sequence
- *Dense:* (monotonic) $T = \mathbb{R}_0^+, \mathbf{0} = 0, \nu(r) = r$
- *Super-dense:* (weakly-monotonic)
  1. $T \subset \mathbb{N} \times \mathbb{R}_0^+$ s.t. $I_0, \mathcal{I}_1, \ldots$ are almost-adiacents time intervals over $\mathbb{R}_0^+$and $I_i = \{r \mid \langle i, r \rangle \in T\}$
  2. $\mathbf{0}$= $\langle 0, 0 \rangle$, $\nu(\langle i, r \rangle) = r$
  3. $\langle i, r \rangle < \langle i', r' \rangle$ iff $i < i'$ or $i = i'$ and $r < r'$

Υ rewriting

LTL-min-max:

If $\pi, t \models \varphi U \psi$ then $\pi(t)(min\Delta^c_{\varphi U \psi}) = \min(\pi(t)(U^c_{\varphi U \psi})) - \pi(t)(c)$

If $\pi, t \models (\varphi U \psi) \wedge F(\neg\varphi \vee G\neg\psi)$ then

$\pi(t)(max\Delta^c_{\varphi U \psi}) = \max(\pi(t)(U^c_{\varphi U \psi})) - \pi(t)(c)$

If $\pi, t \models F\varphi$ then $\pi(t)(maxbef\Delta^c_{\varphi}) = \max(Bef^c_{\pi}(t, \varphi)) - \pi(t)(c)$

$\pi(t)(U^c_{\varphi U \psi}) := \{\pi(t')(c) | t' \geq t : \pi, t' \models \psi$ and for all $t \leq t'' < t' : \pi, t'' \models \varphi\}$

$\pi(t)(Bef^c_{\varphi}) := \{\pi(t')(c) | t' \geq t :$ for all $t < t'' < t' : \pi, t'' \not\models \varphi\}$.

Υ rewriting

LTL-min-max:

If $\pi, t \models \varphi U \psi$ then $\pi(t)(min\Delta^c_{\varphi U \psi}) = \min(\pi(t)(U^c_{\varphi U \psi})) - \pi(t)(c)$
If $\pi, t \models (\varphi U \psi) \wedge F(\neg\varphi \vee G\neg\psi)$ then
$\pi(t)(max\Delta^c_{\varphi U \psi}) = \max(\pi(t)(U^c_{\varphi U \psi})) - \pi(t)(c)$
If $\pi, t \models F\varphi$ then $\pi(t)(maxbef\Delta^c_{\varphi}) = \max(Bef^c_{\pi}(t, \varphi)) - \pi(t)(c)$

$\pi(t)(U^c_{\varphi U \psi}) := \{\pi(t')(c) | t' \geq t : \pi, t' \models \psi$ and for all $t \leq t'' < t' : \pi, t'' \models \varphi\}$
$\pi(t)(Bef^c_{\varphi}) := \{\pi(t')(c) | t' \geq t :$ for all $t < t'' < t' : \pi, t'' \not\models \varphi\}$.

Υ :

$$\Upsilon(\varphi U^c_{\lhd p} \psi) := \Upsilon(\varphi U \psi) \wedge min\Delta_{\Upsilon(\varphi U \psi)} \lhd p$$
$$\Upsilon(\varphi U^c_{\rhd p} \psi) := \Upsilon(G(\varphi \wedge F\psi)) \vee \Upsilon(\varphi U \psi) \wedge max\Delta_{\Upsilon(\varphi U \psi)} \rhd p$$
$$\Upsilon(\varphi \overline{U}^c_{\lhd p} \psi) := \Upsilon(\varphi U \psi) \wedge maxbef\Delta^c_{\Upsilon(\psi)} \lhd p$$

$\mathcal{D}$ discretization (based on (Cimatti *et al.*, 2019))

$$
\begin{aligned}
\phi_D :=& \psi_{time} \wedge \bigwedge_{c \in C} \psi^c_{clock} \wedge \psi_\iota \wedge \mathcal{D}(\phi) \\
\psi_{time} :=& time = 0 \wedge G(time' - time = \delta) \wedge G(\delta > 0 \rightarrow \bigwedge_{v \in V} (v' = v)) \\
\psi^c_{clock} :=& \mathit{diff}_c = 0 \wedge G(\mathit{diff}_c{}' - \mathit{diff}_c = \delta_c - \delta) \wedge \\
& G((\delta > 0 \rightarrow \delta_c \in [\delta(1-\epsilon), \delta(1+\epsilon)]) \wedge (\delta = 0 \rightarrow |\mathit{diff}_c| \leq \lambda)) \\
\psi_\iota :=& \iota \wedge G((\iota \wedge \delta = 0 \wedge X\iota) \vee (\iota \wedge \delta > 0 \wedge X\neg\iota) \vee (\neg\iota \wedge \delta > 0 \wedge X\iota)) \wedge \\
& G((\zeta' - \zeta = \delta) \vee (\zeta \geq 1 \wedge \zeta = 0)) \wedge GF(\zeta \geq 1 \wedge \zeta' = 0)
\end{aligned}
$$

$\mathcal{D}$ discretization (contd)

$$
\begin{aligned}
\mathcal{D}(X\varphi) &:= \iota \wedge X(\iota \wedge \mathcal{D}(\varphi)) \\
\mathcal{D}(\tilde{X}\varphi) &:= (\neg\iota \wedge \mathcal{D}(\varphi)) \vee X(\neg\iota \wedge \mathcal{D}(\varphi)) \\
\mathcal{D}(\varphi U \psi) &:= \mathcal{D}(\psi) \vee (\mathcal{D}(\varphi) U \tilde{\psi}) \\
\mathcal{D}(min\Delta^c_{\varphi U \psi}) &:= ite(\mathcal{D}(\psi) \wedge 0 \leq min\Delta^c_{\mathcal{D}(\varphi)U\tilde{\psi}}, 0, min\Delta^c_{\mathcal{D}(\varphi)U\tilde{\psi}}) \\
\mathcal{D}(max\Delta^c_{\varphi U \psi}) &:= ite(\mathcal{D}(\psi) \wedge 0 \geq max\Delta^c_{\mathcal{D}(\varphi)U\tilde{\psi}}, 0, max\Delta^c_{\mathcal{D}(\varphi)U\tilde{\psi}}) \\
\mathcal{D}(maxbef\Delta^c_{\varphi}) &:= maxbef\Delta^c_{\mathcal{D}(\varphi)}
\end{aligned}
$$

where $\tilde{\psi} = \mathcal{D}(\psi) \wedge (\iota \vee \mathcal{D}(\varphi))$.

LTL-min-max discrete time encoding

$$\mathcal{R}epl(\Psi, min\Delta^c_{\varphi U\psi}) := G(\varphi U\psi \rightarrow \rho_{min\Delta^c_{\varphi U\psi}} =$$
$$ite(\psi \wedge (\neg(\varphi\tilde{U}\psi) \vee 0 \leq \rho'_{min\Delta^c_{\varphi U\psi}} + \delta_c), 0, \rho'_{min\Delta^c_{\varphi U\psi}} + \delta_c) \wedge$$
$$(F(\psi \wedge \rho_{min\Delta^c_{\varphi U\psi}} = 0))) \rightarrow \Psi\lceil min\Delta^c_{\varphi U\psi} / \rho_{min\Delta^c_{\varphi U\psi}} \rfloor$$

LTL-min-max discrete time encoding

$$\mathcal{R}epl(\Psi, min\Delta^c_{\varphi U \psi}) := G(\varphi U \psi \rightarrow \rho_{min\Delta^c_{\varphi U \psi}} =$$
$$ite(\psi \wedge (\neg(\varphi \tilde{U} \psi) \vee 0 \leq \rho'_{min\Delta^c_{\varphi U \psi}} + \delta_c), 0, \rho'_{min\Delta^c_{\varphi U \psi}} + \delta_c) \wedge$$
$$(F(\psi \wedge \rho_{min\Delta^c_{\varphi U \psi}} = 0))) \rightarrow \Psi\lceil min\Delta^c_{\varphi U \psi} / \rho_{min\Delta^c_{\varphi U \psi}} \rfloor$$

$$\mathcal{R}epl(\Psi, maxbef\Delta^c_{\varphi}) := G(F\varphi \rightarrow$$
$$\rho_{maxbef\Delta^c_{\varphi}} = ite(\varphi \vee 0 \geq \rho'_{maxbef\Delta^c_{\varphi}} + \delta_c, 0, \rho'_{maxbef\Delta^c_{\varphi}} + \delta_c)) \rightarrow$$
$$\Psi\lceil maxbef\Delta^c_{\varphi} / \rho_{maxbef\Delta^c_{\varphi}} \rfloor$$

Bibliography

Bombardelli, Alberto, & Tonetta, Stefano. 2022.
Asynchronous Composition of Local Interface LTL Properties.
Pages 508–526 of: NFM.

Bombardelli, Alberto, & Tonetta, Stefano. 2023.
Metric Temporal Logic with Resettable Skewed Clocks - version with proofs.
In: DATE.
To appear, preproceeding version available at
`https://es-static.fbk.eu/people/bombardelli/papers/date23/extended_abstract.pdf`.

Bu, Lei, Cimatti, Alessandro, Li, Xuandong, Mover, Sergio, & Tonetta, Stefano. 2010.
Model Checking of Hybrid Systems Using Shallow Synchronization.
Pages 155–169 of: FMOODS/FORTE.
LNCS, vol. 6117.

Carapelle, Claudia, Feng, Shiguang, Gil, Oliver Fernandez, & Quaas,