Almost Everywhere Verification of Timed Properties

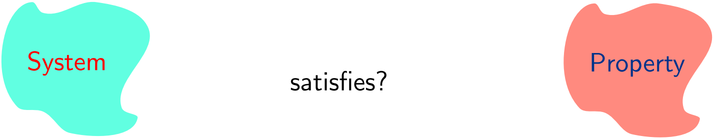
Houda Bel mokadem[1]-Béatrice Bérard[2]-Patricia Bouyer[1]
François Laroussinie[1]

(1) LSV – CNRS & ENS de Cachan – France

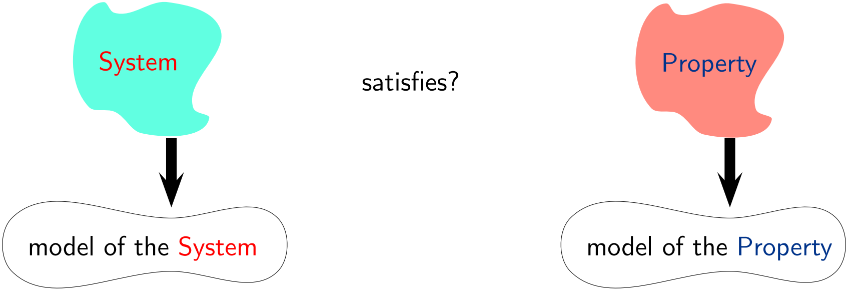
(2) LAMSADE – CNRS & Université Paris-Dauphine

MeFoSyLoMa – January 2006

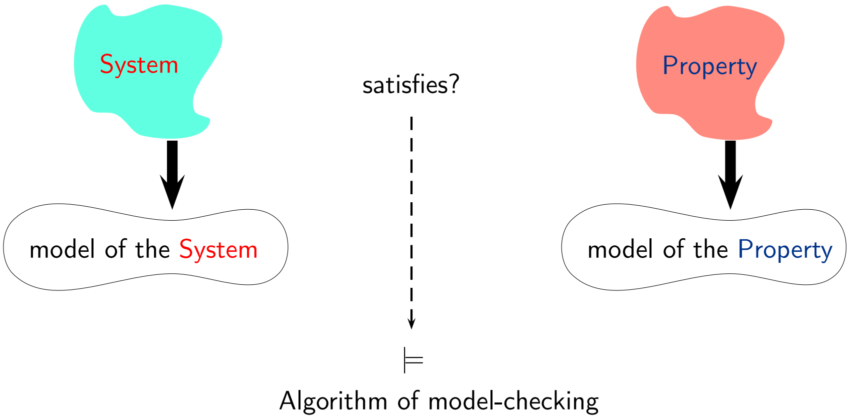
Verification by model-checking



Verification by model-checking



Verification by model-checking



Which model?

- For Systems:
  finite automata, Kripke structures, timed automata, hybrid automata, cost automata, Petri nets ...

- For Properties:
  LTL, TPTL, MTL, CTL, TCTL...
  Pnueli: Using temporal logic for expressing the properties.

Which model?

- For Systems:
  finite automata, Kripke structures, timed automata, hybrid automata, cost automata, Petri nets . . .

- For Properties:
  LTL, TPTL, MTL, CTL, TCTL...
  Pnueli: Using temporal logic for expressing the properties.

Expressiveness/Complexity

Outline

- CTL and Timed CTL
- Extension of TCTL: TCTL^{ext}
- Expressiveness power
  - TCTL $\prec$ TCTL^{ext}
  - TCTL^{a} $\prec$ TCTL^{ext}
- Model-checking
- Conclusion and future work

Outline

Definitions: CTL and TCTL

- CTL:
  - atomic propositions P_1 $P_2 \ldots$
  - boolean operators $\neg\varphi$ $\varphi \wedge \psi$
  - temporal operators $\mathrm{EX}\varphi$ $\mathrm{AX}\varphi$ $\mathrm{E}\varphi\mathrm{U}\psi$ $\mathrm{A}\varphi\mathrm{U}\psi$

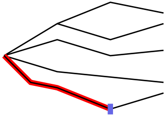
where P_i are atomic propositions.

- TCTL:
  - atomic propositions and boolean operators
  - temporal operators + "subscript $\sim c$" $\mathrm{E}\varphi\mathrm{U}_{\sim c}\psi$ $\mathrm{A}\varphi\mathrm{U}_{\sim c}\psi$

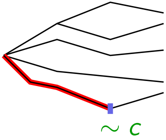
where $\sim \in \{<, >, \leq, \geq, =\}, c \in \mathbb{N}$

Semantics

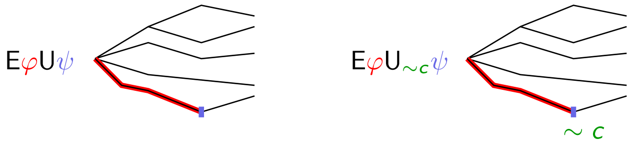
$\mathsf{E}\varphi\mathsf{U}\psi$



$\mathsf{E}\varphi\mathsf{U}_{\sim c}\psi$



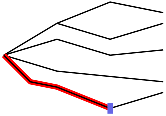
Semantics



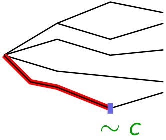
- problem $\longrightarrow$ AF alarm

Semantics

$\mathsf{E}\varphi\mathsf{U}\psi$



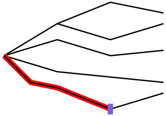
$\mathsf{E}\varphi\mathsf{U}_{\sim c}\psi$



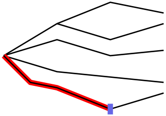
- problem $\longrightarrow$ AF alarm
- A($\neg$ (give-money) U pin-ok)

Semantics

$E\varphi U\psi$



$E\varphi U_{\sim c}\psi$



- problem $\longrightarrow$ AF alarm
- A(¬ (give-money) U pin-ok)

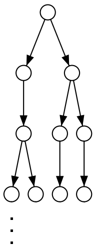
- problem $\longrightarrow$ $AF_{<1}$ alarm

CTL Model-checking

Discrete Transition System

Applying inductively labeling procedure

Example: if $\phi = \mathsf{EX}\psi$

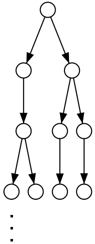


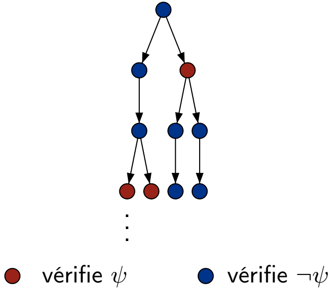
CTL Model-checking

Discrete Transition System

Applying inductively labeling procedure

Example: if $\phi = \mathsf{EX}\psi$



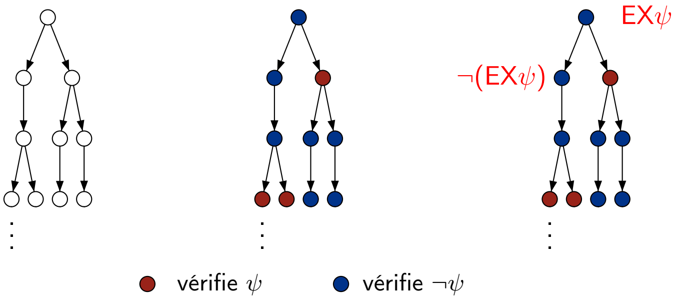


CTL Model-checking

Discrete Transition System

Applying inductively labeling procedure

Example: if $\phi = \mathsf{EX}\psi$



TCTL Model-checking

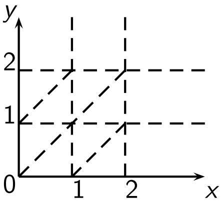
Timed automaton

TCTL Model-checking

Timed automaton

The region abstraction: Equivalence of finite index

- Compatibility between regions and constraints
- Compatibility between regions and time elapsing

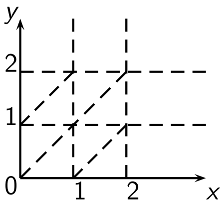


TCTL Model-checking

Timed automaton

The region abstraction: Equivalence of finite index

- Compatibility between regions and constraints
- Compatibility between regions and time elapsing



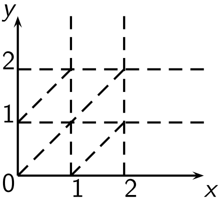
The regions are consistent with the truth of TCTL formulae
i.e $(v \cong v' \;\Rightarrow\; (\ (q,v) \models \Phi \;\Leftrightarrow\; (q,v') \models \Phi\ )\ )$.

TCTL Model-checking

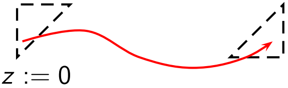
Timed automaton

The region abstraction: Equivalence of finite index

- Compatibility between regions and constraints
- Compatibility between regions and time elapsing



The regions are consistent with the truth of TCTL formulae
i.e $(v \cong v' \;\Rightarrow\; (\,(q,v) \models \Phi \;\Leftrightarrow\; (q,v') \models \Phi\,)\,)$.



TCTL Model-checking

Timed automaton

The regions are consistent with the truth of TCTL formulae
i.e $(v \cong v' \;\Rightarrow\; (\,(q, v) \models \Phi \;\;\Leftrightarrow\;\; (q, v') \models \Phi\,)\,)$.

Region graph: Timed automaton $\bigotimes$ region abstraction

$\Rightarrow$ Discrete Transition System

Applying CTL labeling procedure

TCTL Model-checking

Timed automaton

The regions are consistent with the truth of TCTL formulae
i.e $(v \cong v' \;\Rightarrow\; (\,(q,v) \models \Phi \;\Leftrightarrow\; (q,v') \models \Phi\,)\,)$.

Region graph: Timed automaton $\bigotimes$ region abstraction

$\Rightarrow$ Discrete Transition System

Applying CTL labeling procedure

Example:

$$\mathrm{E}\varphi\mathrm{U}_{\sim c}\psi \Leftrightarrow \mathrm{E}\varphi\mathrm{U}(\psi \wedge P_{\sim c})$$

where $P_{\sim c}$ is atomic proposition

Outline

TCTL^{ext}: Motivation

- Context:

  Verification of programs with boolean or integer variables

- Problem:
  - When modeling a given system, the abstracting phase can lead to a model where some variables have different values at a given point in time
  - In this work, we want to ignore these transient states
  - For this, we introduce a new until modality

Example: Two-hand relays

A safety device:

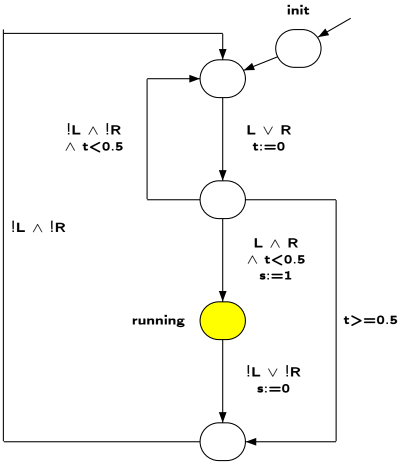
- both hands must be used to start some machine by pressing the two buttons simultaneously (within 0.5s)
- the machine stops as soon as one button is released.
- to ensure that operator is outside the danger zone

Example: Properties

P: When the machine is running, the two buttons are pushed

Example: Properties

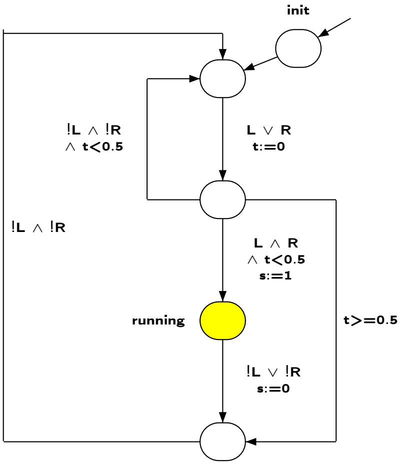
P: When the machine is running, the two buttons are pushed



P:
$s{=}1 \Rightarrow (L{=}1 \text{ and } R = 1)$

Example: Properties

P: When the machine is running, the two buttons are pushed



P:
$s=1 \Rightarrow (L=1 \text{ and } R = 1)$

- P is not always true
- P is almost everywhere true

TCTL^{ext}: Definition and semantics

- TCTL (Timed CTL):
  - atomic propositions P_1 $P_2 \dots$
  - boolean operators $\neg\varphi$ $\varphi \wedge \psi$
  - temporal operators $\mathsf{E}\varphi\mathsf{U}_{\sim c}\psi$ $\mathsf{A}\varphi\mathsf{U}_{\sim c}\psi$

$$\sim \in \{<, >, \leq, \geq, =\}, c \in \mathbb{N}$$

TCTL^{ext}: Definition and semantics

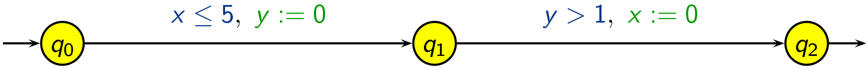
- TCTL (Timed CTL):
  - atomic propositions P_1 $P_2 \dots$
  - boolean operators $\neg\varphi$ $\varphi \wedge \psi$
  - temporal operators $\mathsf{E}\varphi\mathsf{U}_{\sim c}\psi$ $\mathsf{A}\varphi\mathsf{U}_{\sim c}\psi$

$\sim \in \{<, >, \leq, \geq, =\}, c \in \mathbb{N}$

- + "almost everywhere" operators
  - $\mathsf{E}\varphi\mathsf{U}^{a}_{\sim c}\psi$ $\mathsf{A}\varphi\mathsf{U}^{a}_{\sim c}\psi$

Timed automata (example)

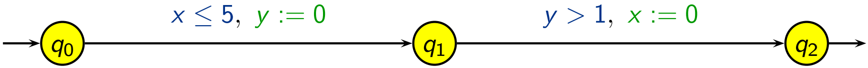
x, y : clocks



$$
\begin{array}{cccccccccc}
\rho & q_0 & \xrightarrow{4.1} & q_0 & \rightarrow_a & q_1 & \xrightarrow{1.4} & q_1 & \rightarrow_a & q_2 \\
x & 0 & & 4.1 & & 4.1 & & 5.5 & & 0 \\
y & 0 & & 4.1 & & 0 & & 1.4 & & 1.4 \\
 & p & & p' & & p'' & & & &
\end{array}
$$

Timed automata (example)

x, y : clocks



	p		p'		p''				
ρ	q_0	$\xrightarrow{4.1}$	q_0	$\rightarrow_a$	q_1	$\xrightarrow{1.4}$	q_1	$\rightarrow_a$	q_2
x	0		4.1		4.1		5.5		0
y	0		4.1		0		1.4		1.4

➜ $p <_\rho p' <_\rho p''$

➜ $\hat{\mu}$ measure on ρ: $\hat{\mu}(p \overset{\sigma}{\hookrightarrow} p'') = 4.1$ $\quad \hat{\mu}(p' \overset{\sigma}{\hookrightarrow} p'') = 0$

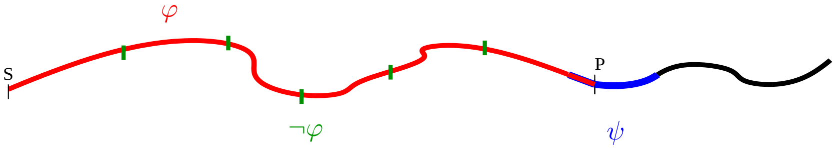
Semantics

A TCTL^{ext} formula is interpreted over a configuration $s = (q, v)$.

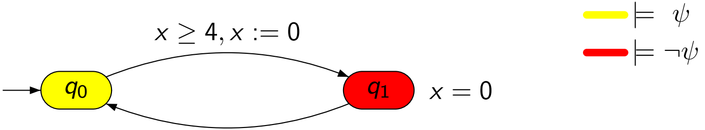
$$s \models \mathsf{E}\varphi\mathsf{U}^{a}_{\sim c}\psi \Leftrightarrow \quad \exists\, \rho \in \mathrm{Exec}(s) \text{ s.t. } \rho \models \varphi\mathsf{U}^{a}_{\sim c}\psi$$

$$\rho \models \varphi\mathsf{U}^{a}_{\sim c}\psi \quad \Leftrightarrow \quad \exists\sigma \text{ s.t. } \hat{\mu}(\sigma) > 0, \exists p \in \sigma,\ \mathrm{Time}(\rho^{\leq p}) \sim c$$

$$\forall p' \in \sigma, s_{p'} \models \psi,\ \hat{\mu}(\{p' \mid p' <_{\rho} p \wedge s_{p'} \not\models \varphi\}) = 0$$



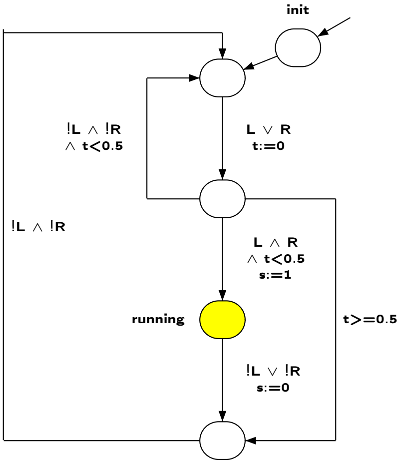
Example



$$(q_0, 0) \models \mathsf{AG}^{\mathsf{a}}\psi \quad \text{but} \quad (q_0, 0) \not\models \mathsf{AG}\psi$$

where $\mathsf{AG}^{\mathsf{a}}\ \psi$ means " ψ holds almost everywhere "

Model of two-hand relays



$AG^a(s=1 \Rightarrow (L=1 \text{ and } R = 1))$ is true

Outline

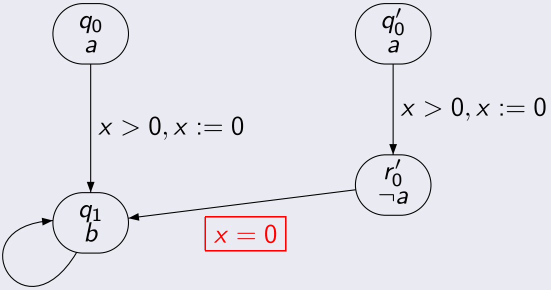
Expressivity

Theorem

- U cannot be expressed by U^a.

proof

A :



$(q_0, 0) \equiv_{\mathrm{TCTL^a}} (q_0', 0)$, but $(q_0, 0) \models \mathrm{E}(a\mathrm{U}b)$, $(q_0', 0) \not\models \mathrm{E}(a\mathrm{U}b)$

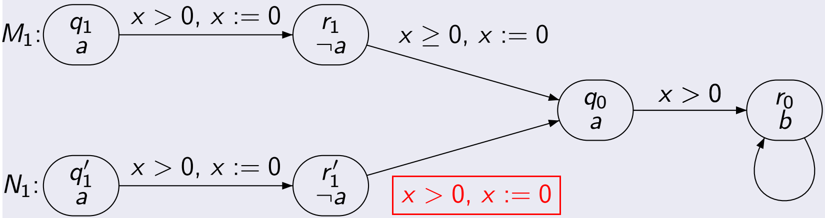
TCTL^a is the fragment of TCTL^{ext} with only U^a modalities.

Expressivity

Theorem

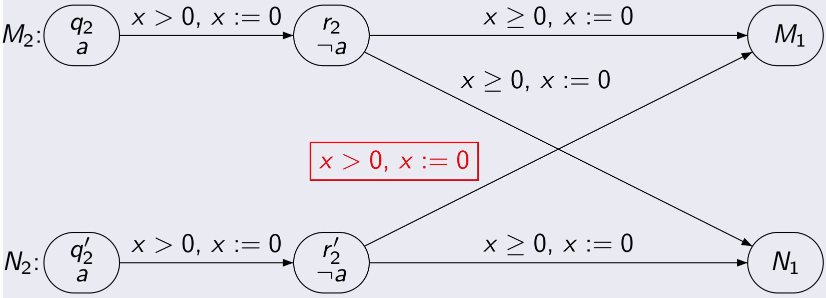
- U^a cannot be expressed by U.

proof



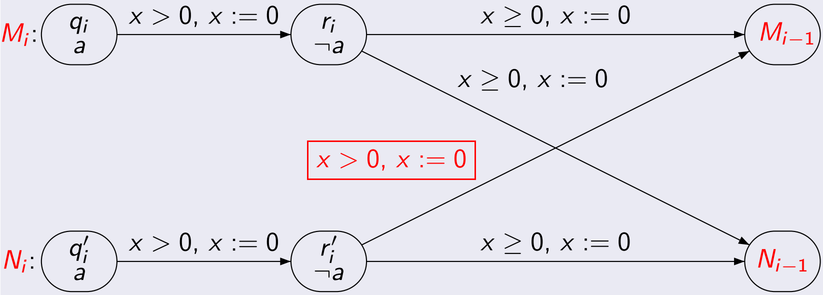
- M_1 and N_1 satisfy the same TCTL formulae of size equal to 1
- but, $M_1 \models E(aU(\neg a \wedge EF_{=0}a))$ and $N_1 \not\models E(aU(\neg a \wedge EF_{=0}a))$

Expressivity

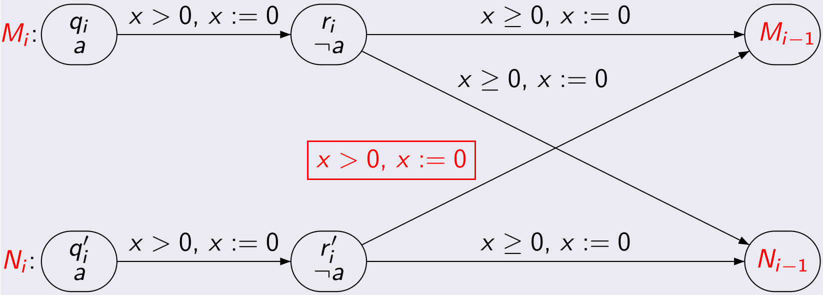


- $M_2 \models E(aU(\neg a \wedge EF_{=0}a))$ and $N_2 \models E(aU(\neg a \wedge EF_{=0}a))$
- but, $\varphi := E(aU(\neg a \wedge EF_{=0}(a \wedge E(aU(\neg a \wedge EF_{=0}a)))))$ we have: $M_2 \models \varphi$ and $N_2 \not\models \varphi$

Expressivity

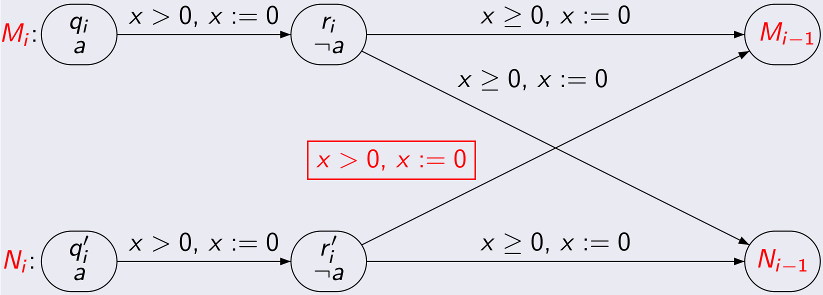


Expressivity



- M_i and N_i satisfy the same TCTL formulae whose size is less than i

Expressivity



- M_i and N_i satisfy the same TCTL formulae whose size is less than i
- but, $M_i \models E(aU^{a}_{>0}b)$ and $N_i \not\models E(aU^{a}_{>0}b)$

Outline

TCTL^{ext} model-checking

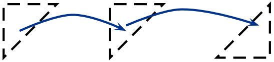
- The standard regions are consistent with the truth of TCTL^{ext} formulae

TCTL^{ext} model-checking

- The standard regions are consistent with the truth of TCTL^{ext} formulae
- We can extend the labeling procedures for verifying U^a

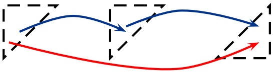
TCTL^{ext} model-checking

- The standard regions are consistent with the truth of TCTL^{ext} formulae
- We can extend the labeling procedures for verifying U^a



TCTL^{ext} model-checking

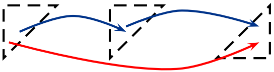
- The standard regions are consistent with the truth of TCTL^{ext} formulae
- We can extend the labeling procedures for verifying U^a



$EG^a_{<c}\varphi \Leftrightarrow E^+(p_b \vee \varphi)Up_{=c}$

TCTL^{ext} model-checking

- The standard regions are consistent with the truth of TCTL^{ext} formulae
- We can extend the labeling procedures for verifying U^a



$$EG^a_{<c}\varphi \Leftrightarrow E^+(p_b \vee \varphi)Up_{=c}$$

- Same complexity

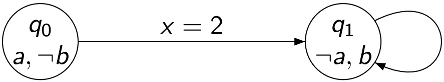
Theorem

Model checking TCTL^{ext} over timed automata is PSPACE-complete.

Outline

Conclusion

- Adding new modalities U^a increase the expressive power of TCTL.
- Model-checking for TCTL^{ext} is PSPACE-complete
- Future work:
  - extend the algorithms on zones to verify U^a
  - extend the results with intervals of size a parameter Δ



$\varphi = \mathsf{E} a \mathsf{U}_{=1} b$

$(q_0, 0) \not\models \mathsf{AG}(\neg\varphi)$ but $(q_0, 0) \models \mathsf{AG}^a(\neg\varphi)$