Interval Temporal Logic Model Checking: the Border Between Good and Bad HS Fragments

International Joint Conference on Automated Reasoning
Coimbra, Portugal, 2016

Laura Bozzelli, Alberto Molinari, Angelo Montanari, Adriano Peron (*), Pietro Sala

June 28, 2016

(*) University of Napoli "Federico II", Dept. of Electrical Engineering and Information Technologies (DIETI)

Model checking

- Model checking: the desired properties of a system are checked against a model of the system
  - the model is a (finite) state-transition graph
  - system properties are specified by a temporal logic (e.g., LTL, CTL, CTL*, . . .)

- Distinctive features of model checking:
  - exhaustive verification of all the possible behaviours
  - fully automatic process
  - a counterexample is produced for a violated property

Point-based vs. interval-based model checking

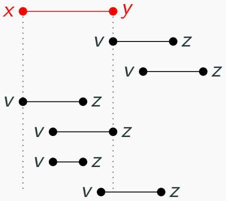
- Model checking is usually point-based:
  - properties express requirements over points (snapshots) of a computation (states of the state-transition system)
  - they are specified by means of point-based temporal logics such as LTL and CTL

- Interval-based model checking:
  - Interval-based properties express conditions on computation stretches: accomplishments, actions with duration, and temporal aggregations
  - they are specified by means of interval temporal logics, e.g., HS

The logic HS

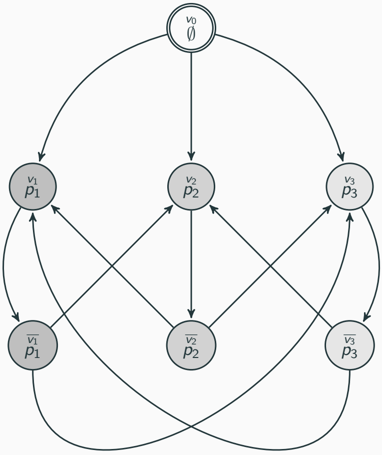
HS features a modality for any Allen ordering relation between pairs of intervals (except for equality)

Allen rel.	HS	Definition	Example
meets	$\langle A \rangle$	$[x,y]\mathcal{R}_A[v,z] \iff y = v$	
before	$\langle L \rangle$	$[x,y]\mathcal{R}_L[v,z] \iff y < v$	
started-by	$\langle B \rangle$	$[x,y]\mathcal{R}_B[v,z] \iff x = v \wedge z < y$	
finished-by	$\langle E \rangle$	$[x,y]\mathcal{R}_E[v,z] \iff y = z \wedge x < v$	
contains	$\langle D \rangle$	$[x,y]\mathcal{R}_D[v,z] \iff x < v \wedge z < y$	
overlaps	$\langle O \rangle$	$[x,y]\mathcal{R}_O[v,z] \iff x < v < y < z$	



All modalities can be expressed by means of $\langle A \rangle$, $\langle B \rangle$, $\langle E \rangle$ and their transposed modalities only

Kripke structures



An example of Kripke structure

- $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$
- HS formulas are interpreted over (finite) state-transition systems whose states are labelled with sets of proposition letters (Kripke structures)

- An interval is a track (finite path) in a Kripke structure

HS semantics and model checking

Truth of a formula ψ over a track ρ of a Kripke structure $\mathcal{K}$:

- $\mathcal{K}, \rho \models p$ iff $p \in \bigcap_{w \in \mathsf{states}(\rho)} \mu(w)$, for any letter $p \in \mathcal{AP}$ (homogeneity assumption);
- negation, disjunction, and conjunction are standard;
- $\mathcal{K}, \rho \models \langle \mathsf{A} \rangle\, \psi$ iff there is a track ρ' s.t. $\mathsf{lst}(\rho) = \mathsf{fst}(\rho')$ and $\mathcal{K}, \rho' \models \psi$;
- $\mathcal{K}, \rho \models \langle \mathsf{B} \rangle\, \psi$ iff there is a prefix ρ' of ρ s.t. $\mathcal{K}, \rho' \models \psi$;
- $\mathcal{K}, \rho \models \langle \mathsf{E} \rangle\, \psi$ iff there is a suffix ρ' of ρ s.t. $\mathcal{K}, \rho' \models \psi$;
- the semantic clauses for $\langle \overline{\mathsf{A}} \rangle$, $\langle \overline{\mathsf{B}} \rangle$, and $\langle \overline{\mathsf{E}} \rangle$ are similar

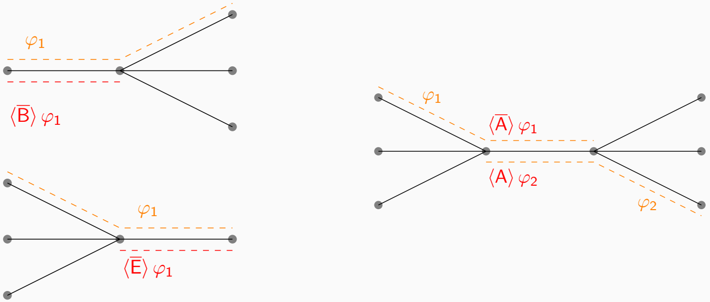
Model Checking

$\mathcal{K} \models \psi \iff$ for all *initial* tracks ρ of $\mathcal{K}$, it holds that $\mathcal{K}, \rho \models \psi$

Possibly infinitely many tracks!

HS state semantics

- The semantics features branching both in the past and in the future.



- HS with state semantics is not comparable w.r.t. to *LTL*, *CTL* and *CTL**.

Decidability of HS model checking

Theorem

The model checking problem for full HS on Kripke structures is decidable (with a non-elementary algorithm)

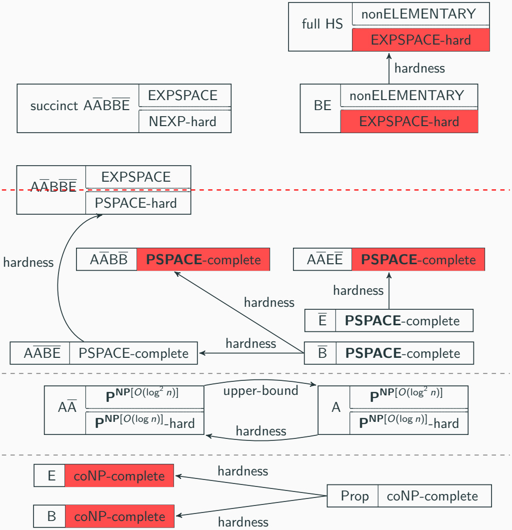
Reference

A. Molinari, A. Montanari, A. Murano, G. Perelli, and A. Peron. Checking interval properties of computations.

Acta Informatica, 2015.

Accepted for publication

Complexity picture



The fragment BE

Theorem

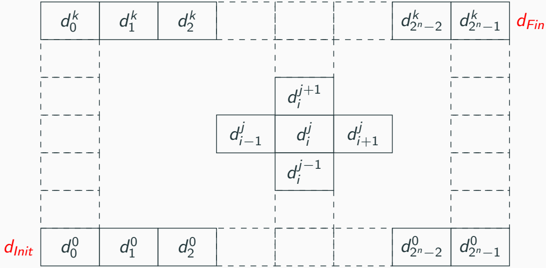
The model checking problem for BE *on Kripke structures is EXPSPACE-hard*

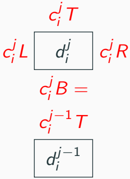
Proved by a polynomial-time reduction from a domino-tiling problem for grids with rows of single exponential length:

- For an instance $\mathcal{I}$ of the problem we build in polynomial time a Kripke structure $\mathcal{K}_{\mathcal{I}}$ and a BE formula $\varphi_{\mathcal{I}}$;
- there exists an initial track of $\mathcal{K}_{\mathcal{I}}$ satisfying $\varphi_{\mathcal{I}}$ if and only if there exists a tiling of $\mathcal{I}$;
- Hence, $\mathcal{K}_{\mathcal{I}} \models \neg\varphi_{\mathcal{I}}$ iff there does not exist a tiling of $\mathcal{I}$.

BE hardness: Encoding of a tiling

Instance of tiling problem: $(C, \Delta, n, d_{init}, d_{final})$, where C is a finite set of colors, $\Delta \subseteq C^4$ is a set of tuples (c_B, c_L, c_T, c_R)





String encoding of a tiling

row 0								row 1							
d_0^0	$0\cdots00$	d_1^0	$1\cdots00$	$\cdots$	$d_{2^n-1}^0$	$1\cdots11$	\$	d_0^1	$0\cdots00$	d_1^1	$1\cdots00$	$\cdots$	$d_{2^n-1}^1$	$1\cdots11$	\$
column 0		column 1			column 2^n-1			column 0		column 1			column 2^n-1		

BE hardness: $\mathcal{K}_\mathcal{I}$ and $\varphi_\mathcal{I}$

- For $\mathcal{AP} = \Delta \cup \{\$\} \cup \{0, 1\}$, the Kripke structure $\mathcal{K}_\mathcal{I}$ is defined as $\mathcal{K}_\mathcal{I} = (\mathcal{AP}, \mathcal{AP}, \mathcal{AP} \times \mathcal{AP}, \mu, d_{init})$, where $\mu(p) = \{p\}$, for any $p \in \mathcal{AP}$.
- The formula $\varphi_\mathcal{I}$ checks that an initial track of $\mathcal{K}_\mathcal{I}$ is a correct encoding of a tiling.
  It exploits the following features of BE:
  - Measuring the length of a track: the formula $length_i$ characterizes the tracks of length i.

$$length_i := (\underbrace{\langle \mathrm{B} \rangle \dots \langle \mathrm{B} \rangle}_{i-1} \top) \ \wedge \ (\underbrace{[B] \dots [B]}_{i} \bot).$$

  - Constraining arbitrary subtracks with the derived operator $\langle \mathrm{G} \rangle$ and its dual $[G]$, which allow us to select arbitrary subtracks of a given track:

$$\langle \mathrm{G} \rangle \, \psi := \psi \vee \langle \mathrm{B} \rangle \, \psi \vee \langle \mathrm{E} \rangle \, \psi \vee \langle \mathrm{B} \rangle \, \langle \mathrm{E} \rangle \, \psi.$$

The fragments $\mathsf{A}\overline{\mathsf{A}}\mathsf{E}\overline{\mathsf{E}}$ and $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$

- A **PSPACE** MC algorithm for $\mathsf{A}\overline{\mathsf{A}}\mathsf{E}\overline{\mathsf{E}}$ and $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$ can be devised by exploiting a polynomial size model-track property.
- Polynomial size model-track property: if a track ρ of a Kripke structure $\mathcal{K}$ satisfies a formula φ, then there is a track π, whose length is polynomial in the sizes of φ and $\mathcal{K}$, that satisfies φ.
- The MC algorithm to decide $\mathcal{K} \models \varphi$ searches a counterexample, i.e. a track ρ such that $|\rho| \leq |W| \cdot (2|\varphi| + 3)^2$ and $\mathcal{K}, \rho \models \neg\varphi$.

Algorithm 1 `ModCheck`$(\mathcal{K}, \varphi)$

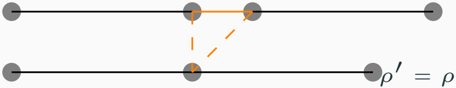
for all initial $\tilde{\rho} \in \mathsf{Trk}_{\mathcal{K}}$ s.t. $|\tilde{\rho}| \leq |W| \cdot (2|\varphi| + 3)^2$ **do**
    if `Check`$(\mathcal{K}, \varphi, \tilde{\rho}) = 0$ **then**
        return 0: "$\mathcal{K}, \tilde{\rho} \not\models \varphi$" $\triangleleft$ *Counterexample found*
return 1: "$\mathcal{K} \models \varphi$"

The fragment $A\bar{A}E\bar{E}$: Polynomial-size model-track property

- Contraction technique (permitted by homogeneity assumption):

$Pattern(\rho, i) = Pattern(\rho, j)$ $\quad Pattern(\rho, k) = \{p \in \mathcal{AP} : \mathcal{K}, \rho^{k[} \models p\}$

$\rho(i) = \rho(j)$



ρ

$\rho' = \rho(0, i) \cdot \rho^{(j+1)[}$

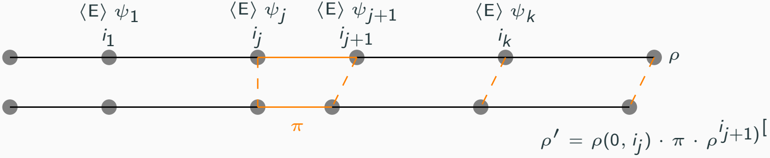
- $\forall i \leq h \leq j, \forall p \in \mathcal{AP} : \mathcal{K}, \rho^{h[} \models p$ iff $\mathcal{K}, \rho^{j[} \models p$;
- ρ' is well-formed w.r. to ρ.

Proposition

For any track ρ of $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$, there exists a track π of $\mathcal{K}$, which is well-formed with respect to ρ, such that $|\pi| \leq |W| \cdot (|\mathcal{AP}| + 1)$.

The fragment $\mathsf{A\overline{A}E\overline{E}}$: Polynomial-size model-track property

- Contraction technique by well-formedness contraction:



- $\langle \mathsf{E} \rangle\, \psi_j$ is a subformula of φ s.t. $\mathcal{K}, \rho \models \langle \mathsf{E} \rangle\, \psi_j$ for $1 \leq j \leq k$;
- i_j is the greatest index of ρ such that $\mathcal{K}, \rho^{i_j[} \models \psi_j$;
- π is well-formed w.r.t. to $\rho(i_j, i_{j+1})$ and $|\pi| \leq |W| \cdot (|\mathcal{AP}| + 1)$;
- $\rho' \models \varphi$.

Theorem

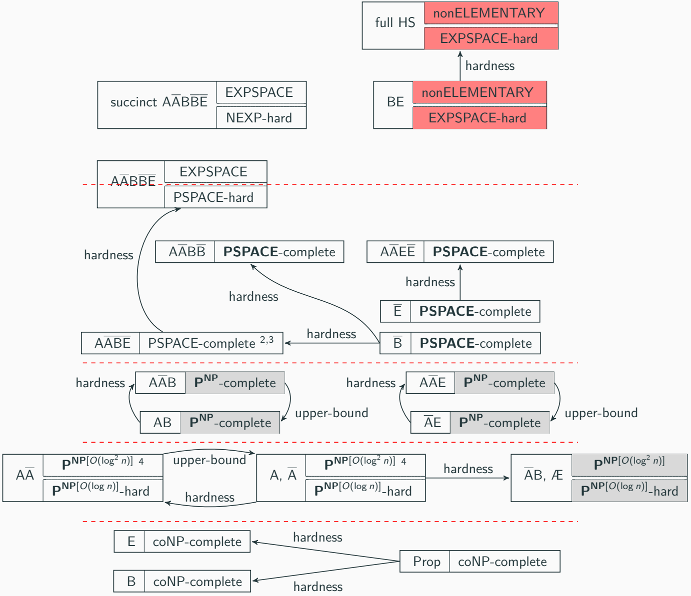
Let $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$, $\rho \in \mathsf{Trk}_{\mathcal{K}}$, and φ be an $\mathsf{A\overline{A}E\overline{E}}$ formula (in NNF) such that $\mathcal{K}, \rho \models \varphi$. Then, there is $\overline{\rho} \in \mathsf{Trk}_{\mathcal{K}}$, induced by ρ, such that $\mathcal{K}, \overline{\rho} \models \varphi$ and $|\overline{\rho}| \leq |W| \cdot (|\varphi| + 1)^2$.

Model checking routine

Algorithm 2 $\texttt{Check}(\mathcal{K}, \psi, \tilde{\rho})$

if $\psi = p$, for $p \in \mathcal{AP}$ **then**
    if $p \in \bigcap_{s \in \texttt{states}(\tilde{\rho})} \mu(s)$ **then**
        return 1 **else return** 0
else if $\psi = \varphi_1 \wedge \varphi_2$ **then**
    if $\texttt{Check}(\mathcal{K}, \varphi_1, \tilde{\rho}) = 0$ **then**
        return 0
    else
        return $\texttt{Check}(\mathcal{K}, \varphi_2, \tilde{\rho})$
else if $\psi = \langle \mathrm{A} \rangle \varphi$ **then**
    for all $\rho \in \mathrm{Trk}_{\mathcal{K}}$ such that $\mathrm{fst}(\rho) = \mathrm{lst}(\tilde{\rho})$, and $|\rho| \leq |W| \cdot (2|\varphi| + 1)^2$ **do**
        if $\texttt{Check}(\mathcal{K}, \varphi, \rho) = 1$ **then**
            return 1
    return 0
else if $\psi = \langle \mathrm{E} \rangle \varphi$ **then**
    for each $\overline{\rho}$ suffix of $\tilde{\rho}$ **do**
        if $\texttt{Check}(\mathcal{K}, \varphi, \overline{\rho}) = 1$ **then**
            return 1
    return 0
else if $\psi = \langle \overline{\mathrm{E}} \rangle \varphi$ **then**
    for all $\rho \in \mathrm{Trk}_{\mathcal{K}}$ such that $\mathrm{lst}(\rho) = \mathrm{fst}(\tilde{\rho})$, and $2 \leq |\rho| \leq |W| \cdot (2|\varphi| + 1)^2$ **do**
        if $\texttt{Check}(\mathcal{K}, \varphi, \rho \star \tilde{\rho}) = 1$ **then**
            return 1
    return 0
else if $\psi = \neg\varphi$ **then**
    return $1 - \texttt{Check}(\mathcal{K}, \varphi, \tilde{\rho})$
… $\triangleleft$ $\psi = \langle \overline{\mathrm{A}} \rangle \varphi$ is analogous to $\psi = \langle \mathrm{A} \rangle \varphi$

Complexity picture: future work



Future work

- Determining the precise complexity of full HS (automata-based approach)
- $A\overline{A}B$ and $A\overline{A}E$ are $\mathbf{P}^{NP}$-complete;
- Investigating other possible HS semantics, in particular to compare HS with LTL/CTL (in particular, linear track semantics, computation tree semantics);
- Relaxing the homogeneity assumption.

References

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Interval Temporal Logic Model Checking: the Border Between Good and Bad HS Fragments.
In *IJCAR*, 2016.

A. Molinari, A. Montanari, A. Murano, G. Perelli, and A. Peron.
Checking interval properties of computations.
Acta Informatica, 2015.
Accepted for publication.

A. Molinari, A. Montanari, and A. Peron.
Complexity of ITL model checking: some well-behaved fragments of the interval logic HS.
In *TIME*, pages 90–100, 2015.

A. Molinari, A. Montanari, and A. Peron.
Constraining cycle alternations in model checking for interval temporal logic.
In *ICTCS*, 2015.

A. Molinari, A. Montanari, and A. Peron.
A model checking procedure for interval temporal logics based on track representatives.
In *CSL*, pages 193–210, 2015.

A. Molinari, A. Montanari, A. Peron, and P. Sala.
Model Checking Well-Behaved Fragments of HS: the (Almost) Final Picture.
In *KR*, 2016.