Interval Temporal Logic Model Checking
Based on Track Bisimilarity and Prefix Sampling

ICTCS 2016, Lecce, Italy

Laura Bozzelli, Alberto Molinari, Angelo Montanari, Adriano Peron, Pietro Sala
September 7–9, 2016
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 and the like

- **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 such as HS and its fragments
The logic HS

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

<table>
<thead>
<tr>
<th>Allen rel.</th>
<th>HS</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>meets</td>
<td>⟨A⟩</td>
<td>[x, y]Ra[v, z] ⇔ y = v</td>
<td></td>
</tr>
<tr>
<td>before</td>
<td>⟨L⟩</td>
<td>[x, y]Rl[v, z] ⇔ y &lt; v</td>
<td></td>
</tr>
<tr>
<td>started-by</td>
<td>⟨B⟩</td>
<td>[x, y]Rb[v, z] ⇔ x = v ∧ z &lt; y</td>
<td></td>
</tr>
<tr>
<td>finished-by</td>
<td>⟨E⟩</td>
<td>[x, y]Re[v, z] ⇔ y = z ∧ x &lt; v</td>
<td></td>
</tr>
<tr>
<td>contains</td>
<td>⟨D⟩</td>
<td>[x, y]Rd[v, z] ⇔ x &lt; v ∧ z &lt; y</td>
<td></td>
</tr>
<tr>
<td>overlaps</td>
<td>⟨O⟩</td>
<td>[x, y]Ro[v, z] ⇔ x &lt; v &lt; y &lt; z</td>
<td></td>
</tr>
</tbody>
</table>

All modalities can be expressed by means of ⟨A⟩, ⟨B⟩, ⟨E⟩ and their transposed modalities only
An example of Kripke structure

- 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/trace) in a Kripke structure
HS semantics and model checking

Truth of a formula $\psi$ over a track $\rho$ of a Kripke structure $K = (\mathcal{AP}, W, \delta, \mu, w_0)$:

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

Model Checking

$K \models \psi \iff$ for all initial tracks $\rho$ of $K$, it holds that $K, \rho \models \psi$

Possibly infinitely many tracks!
**BE-descriptors**

\[ \rho = v_0 v_1 v_0^4 v_1 \]

(only the part for prefixes is shown)
**FACT 1:** For any Kripke structure $\mathcal{K}$ the number of different descriptors of bounded depth $k$ is finite

**FACT 2:** Two tracks $\rho$ and $\rho'$ of a Kripke structure $\mathcal{K}$ described by the same $BE_k$-descriptor are $k$-equivalent
Decidability of HS model checking

<table>
<thead>
<tr>
<th>Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>The model checking problem for full HS on Kripke structures is decidable (non-elementary algorithm)</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Acta Informatica, 2016</em></td>
</tr>
</tbody>
</table>
### Decidability of HS model checking

**Theorem**

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

**Reference**


**Theorem**

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

**Reference**

In this paper, we focus our attention on the HS fragment $\overline{AABBE}$, which is obtained from full HS ($\overline{AABEBE}$) by removing modality $\langle E \rangle$. 

Some fundamental facts:

• We can restrict our attention on prefixes ($B_k$-descriptors suffice).
• The size of the tree representation of $B_k$-descriptors is larger than necessary (redundancy) and it prevents their efficient exploitation in model checking algorithms.
• A track representative can be chosen to represent a (possibly infinite) set of tracks with the same $B_k$-descriptor.
• A bound, which depends on both the number $|W|$ of states of the Kripke structure and the $B_k$-nesting depth $k$, can be given to the length of track representatives.
In this paper, we focus our attention on the HS fragment $A\overline{A}B\overline{B}E$, which is obtained from full HS ($A\overline{A}BE\overline{B}E$) by removing modality $\langle E \rangle$.

Some fundamental facts:

- we can restrict our attention on prefixes ($B_k$-descriptors suffice)
In this paper, we focus our attention on the HS fragment $\text{A}\text{B}\text{B}\text{E}$, which is obtained from full HS ($\text{A}\text{A}\text{B}\text{E}\text{B}\text{E}$) by removing modality $\langle \text{E} \rangle$.

Some fundamental facts:

- we can restrict our attention on prefixes ($B_k$-descriptors suffice)
- the size of the tree representation of $B_k$-descriptors is larger than necessary (redundancy) and it prevents their efficient exploitation in model checking algorithms
The logic $\overline{AABBE}$

In this paper, we focus our attention on the HS fragment $\overline{AABBE}$, which is obtained from full HS ($\overline{AABEBE}$) by removing modality $\langle E \rangle$.

Some fundamental facts:

- we can restrict our attention on prefixes ($B_k$-descriptors suffice)
- the size of the tree representation of $B_k$-descriptors is larger than necessary (redundancy) and it prevents their efficient exploitation in model checking algorithms
- a track representative can be chosen to represent a (possibly infinite) set of tracks with the same $B_k$-descriptor
In this paper, we focus our attention on the HS fragment $\overline{A\overline{A}B\overline{B}E}$, which is obtained from full HS ($\overline{A\overline{A}B\overline{E}B\overline{E}}$) by removing modality $\langle E \rangle$

Some fundamental facts:

- we can restrict our attention on prefixes ($B_k$-descriptors suffice)
- the size of the tree representation of $B_k$-descriptors is larger than necessary (redundancy) and it prevents their efficient exploitation in model checking algorithms
- a track representative can be chosen to represent a (possibly infinite) set of tracks with the same $B_k$-descriptor
- a bound, which depends on both the number $|W|$ of states of the Kripke structure and the $B$-nesting depth $k$, can be given to the length of track representatives
### Definition (Prefix-bisimilarity)

The tracks $\rho$ and $\rho'$ are **$h$-prefix bisimilar** if the following conditions inductively hold:

- **for** $h = 0$:
  
  $\text{fst}(\rho) = \text{fst}(\rho')$, $\text{lst}(\rho) = \text{lst}(\rho')$, and $\text{states}(\rho) = \text{states}(\rho')$.

- **for** $h > 0$:
  
  $\rho$ and $\rho'$ are 0-prefix bisimilar and for each proper prefix $\nu$ of $\rho$ (resp., proper prefix $\nu'$ of $\rho'$), there exists a proper prefix $\nu'$ of $\rho'$ (resp., proper prefix $\nu$ of $\rho$) such that $\nu$ and $\nu'$ are $(h - 1)$-prefix bisimilar.

- $h$-prefix bisimilarity is an equivalence relation over $\text{Trk}_{K}$.  

- $h$-prefix bisimilarity propagates downwards.
Proposition

Let $h \geq 0$, and $\rho$ and $\rho'$ be two $h$-prefix bisimilar tracks of a Kripke structure $\mathcal{K}$. For each $\mathsf{AABBE}$ formula $\psi$, with $B$-nesting of $\psi$ less than or equal to $h$, it holds that

$$\mathcal{K}, \rho \models \psi \iff \mathcal{K}, \rho' \models \psi.$$
Definition (Induced track)

Let $\rho$ be a track of length $n$ of a Kripke structure $\mathcal{K}$. A track induced by $\rho$ is a track $\pi$ of $\mathcal{K}$ such that there exists an increasing sequence of $\rho$-positions $i_1 < \ldots < i_k$, where $i_1 = 1$, $i_k = n$, and

$$\pi = \rho(i_1) \cdots \rho(i_k).$$

If $\pi$ is induced by $\rho \Rightarrow \text{fst}(\pi) = \text{fst}(\rho)$, $\text{lst}(\pi) = \text{lst}(\rho)$, and $|\pi| \leq |\rho|$.
Definition (Prefix-skeleton sampling)

Let $\rho$ be a track of a Kripke structure $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$.
Given two $\rho$-positions $i$ and $j$, with $i \leq j$, the prefix-skeleton sampling of $\rho(i, j)$ is the minimal set $P$ of $\rho$-positions in the interval $[i, j]$ satisfying:

- $i, j \in P$;
- for each state $w \in W$ occurring along $\rho(i + 1, j - 1)$, the minimal position $k \in [i + 1, j - 1]$ such that $\rho(k) = w$ is in $P$.

$$P = \{i, i + 1, i + 4, i + 6, j\}$$
**Definition (h-prefix sampling)**

For each $h \geq 1$, the $h$-prefix sampling of $\rho$ is the minimal set $P_h$ of $\rho$-positions inductively satisfying the following conditions:

- for $h = 1$: $P_1$ is the prefix-skeleton sampling of $\rho$;
- for $h > 1$:
  - $P_h \supseteq P_{h-1}$ and
  - for all pairs of consecutive positions $i, j$ in $P_{h-1}$, the prefix-skeleton sampling of $\rho(i, j)$ is in $P_h$.

**Property**

The $h$-prefix sampling $P_h$ of (any) $\rho$ is such that $|P_h| \leq (|W| + 2)^h$. 
Now what?

From a track $\rho$, we can derive another track $\rho'$, induced by $\rho$ and $h$-prefix bisimilar to $\rho$, such that $|\rho'| \leq (|W| + 2)^{h+2}$ in this way:

1. we first compute the $(h+1)$-prefix sampling $P_{h+1}$ of $\rho$;
2. then for all the pairs of consecutive $\rho$-positions $i, j \in P_{h+1}$, we consider a track induced by $\rho(i, j)$, with no repeated occurrences of any state, except at most the first and last ones (hence no longer than $(|W| + 2)$);
3. $\rho'$ is just the ordered concatenation of all these tracks.

$\rho$ and $\rho'$ can be proved to be $h$-prefix bisimilar, $\Rightarrow \rho'$ is indistinguishable from $\rho$ w.r.t. the fulfilment of any $A_{AB}BE$ formula $\psi$, with $B$-nesting of $\psi$ (abbreviated $d_B(\psi)$) less than or equal to $h$; by the previous bound on $|P_h|$, we have $|\rho'| \leq (|W| + 2)^{h+2}$. 

14
From a track $\rho$, we can derive another track $\rho'$, induced by $\rho$ and $h$-prefix bisimilar to $\rho$, such that $|\rho'| \leq (|W| + 2)^{h+2}$ in this way:

1. we first compute the $(h + 1)$-prefix sampling $P_{h+1}$ of $\rho$;
From a track $\rho$, we can derive another track $\rho'$, induced by $\rho$ and $h$-prefix bisimilar to $\rho$, such that $|\rho'| \leq (|W| + 2)^{h+2}$ in this way:

1. we first compute the $(h + 1)$-prefix sampling $P_{h+1}$ of $\rho$;
2. then for all the pairs of consecutive $\rho$-positions $i, j \in P_{h+1}$, we consider a track induced by $\rho(i, j)$, with no repeated occurrences of any state, except at most the first and last ones (hence no longer than $(|W| + 2))$;
From a track $\rho$, we can derive another track $\rho'$, induced by $\rho$ and $h$-prefix bisimilar to $\rho$, such that $|\rho'| \leq (|W| + 2)^{h+2}$ in this way:

1. we first compute the $(h + 1)$-prefix sampling $P_{h+1}$ of $\rho$;
2. then for all the pairs of consecutive $\rho$-positions $i, j \in P_{h+1}$, we consider a track induced by $\rho(i, j)$, with no repeated occurrences of any state, except at most the first and last ones (hence no longer than $(|W| + 2)$);
3. $\rho'$ is just the ordered concatenation of all these tracks.
From a track $\rho$, we can derive another track $\rho'$, induced by $\rho$ and $h$-prefix bisimilar to $\rho$, such that $|\rho'| \leq (|W| + 2)^{h+2}$ in this way:

1. we first compute the $(h + 1)$-prefix sampling $P_{h+1}$ of $\rho$;
2. then for all the pairs of consecutive $\rho$-positions $i, j \in P_{h+1}$, we consider a track induced by $\rho(i, j)$, with no repeated occurrences of any state, except at most the first and last ones (hence no longer than $(|W| + 2)$);
3. $\rho'$ is just the ordered concatenation of all these tracks.

$\rho$ and $\rho'$ can be proved to be $h$-prefix bisimilar,\n$\Rightarrow$ $\rho'$ is indistinguishable from $\rho$ w.r.t. the fulfilment of any $\overline{A\overline{A}B\overline{B}}E$ formula $\psi$, with $B$-nesting of $\psi$ (abbreviated $d_B(\psi)$) less than or equal to $h$;

by the previous bound on $|P_h|$, we have $|\rho'| \leq (|W| + 2)^{h+2}$. 
Algorithm 1 ModCheck(\(\mathcal{K}, \psi\))

1: \(h \leftarrow d_{B}(\psi)\)
2: \(u \leftarrow \text{New(Unravelling}(\mathcal{K}, w_{0}, h))\) \(\triangleq w_{0}\) initial state of \(\mathcal{K}\)
3: \textbf{while} \(u.\text{hasMoreTracks}()\) \textbf{do}
4: \(\tilde{\rho} \leftarrow u.\text{getNextTrack}()\)
5: \textbf{if} \(\text{Check}(\mathcal{K}, h, \psi, \tilde{\rho}) = 0\) \textbf{then}
6: \textbf{return} 0: “\(\mathcal{K}, \tilde{\rho} \not\models \psi\)” \(\triangleq\) Counterexample found \(\times\)
7: \textbf{return} 1: “\(\mathcal{K} \models \psi\)” \(\triangleq\) Model checking OK \(\checkmark\)
Current and future work

• Comparison of HS model checking with LTL, CTL, and CTL* one (to this end, we introduced two semantic variants of the problem respectively based on the linear-past semantics and the linear semantics) - DONE

• Application: Planning as Model Checking in Interval Temporal Logic - IN PROGRESS

• Determining the precise complexity of full HS (and of a little subset of its fragments)

• Relaxing the homogeneity assumption
Expressiveness comparison

\[ HS_{\text{lin}} \equiv LTL \]

\[ HS_{\text{ct}} \neq \text{finitary } CTL^* \]

\[ HS_{\text{st}} \neq CTL \]

\[ CTL^* \}

\[ \neq \]

\[ \neq \]

\[ \neq \]

\[ \neq \]


A. Molinari, A. Montanari, and A. Peron.  
Complexity of ITL model checking: some well-behaved fragments of the interval logic HS.  

A. Molinari, A. Montanari, and A. Peron.  
A model checking procedure for interval temporal logics based on track representatives.  

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