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

- **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
• 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
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>$[x, y] \mathcal{R}_{A}[v, z] \iff y = v$</td>
<td></td>
</tr>
<tr>
<td>before</td>
<td>⟨L⟩</td>
<td>$[x, y] \mathcal{R}_{L}[v, z] \iff y &lt; v$</td>
<td></td>
</tr>
<tr>
<td>started-by</td>
<td>⟨B⟩</td>
<td>$[x, y] \mathcal{R}_{B}[v, z] \iff x = v \land z &lt; y$</td>
<td></td>
</tr>
<tr>
<td>finished-by</td>
<td>⟨E⟩</td>
<td>$[x, y] \mathcal{R}_{E}[v, z] \iff y = z \land x &lt; v$</td>
<td></td>
</tr>
<tr>
<td>contains</td>
<td>⟨D⟩</td>
<td>$[x, y] \mathcal{R}_{D}[v, z] \iff x &lt; v \land z &lt; y$</td>
<td></td>
</tr>
<tr>
<td>overlaps</td>
<td>⟨O⟩</td>
<td>$[x, y] \mathcal{R}_{O}[v, z] \iff x &lt; v &lt; y &lt; z$</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.
Truth of a formula $\psi$ over a track $\rho$ of a Kripke structure $K = (\mathcal{AP}, \mathcal{W}, \delta, \mu, w_0)$:

- $K, \rho \models p$ 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**

**FACT 1:** For any Kripke structure $K$ the number of different descriptors of bounded depth $k$ is finite.

**FACT 2:** Two tracks $\rho$ and $\rho'$ of a Kripke structure $K$ described by the same $BE_k$-descriptor are $k$-equivalent.

$BE_2$-descriptor for the track $\rho = v_0 v_1 v_0^4 v_1$

(only the part for prefixes is shown)
**BE-descriptors**

**BE₂-descriptor for the track** \( \rho = v_0v_1v_0'v_1 \)

(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

Theorem

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

Reference


Acta Informatica, 2016
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 $A\overline{A}B\overline{B}E\overline{E}$, which is obtained from full HS ($A\overline{A}BE\overline{E}E\overline{E}$) by removing modality $\langle\langle\overline{E}\rangle\rangle$.
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 ($\overline{A\overline{A}B\overline{B}E\overline{B}E}$) 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 $A\bar{A}B\bar{B}\bar{E}$, which is obtained from full HS ($A\bar{A}\bar{B}E\bar{B}E$) 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.
In this paper, we focus our attention on the HS fragment $\overline{A\overline{A}BBE}$, which is obtained from full HS ($A\overline{A}BE\overline{B}E\overline{B}E\overline{E}$) 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
In this paper, we focus our attention on the HS fragment $A\bar{A}BB\bar{E}$, which is obtained from full HS ($A\bar{A}BEBE\bar{E}$) by removing modality $\langle E \rangle$.

Some fundamental facts:

- we can restrict our attention on prefixes ($B_r$-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 \( h = 0 \):
  \[
  \text{fst}(\rho) = \text{fst}(\rho'), \text{lst}(\rho) = \text{lst}(\rho'), \text{and states}(\rho) = \text{states}(\rho').
  \]

- 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 $\overline{AABBEE}$ 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 $|\pi| \leq |\rho|$. 

![Diagram](image.png)
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 $P$.

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

**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 $P_{h+1}$, we consider a track induced by $(i; j)$, with no repeated occurrences of any state, except at most the first and last ones (hence no longer than $(j \cdot W + 2)h+2$);
3. $\rho'$ is just the ordered concatenation of all these tracks.

$\rho'$ can be proved to be $h$-prefix bisimilar, $\rho'$ is indistinguishable from $\rho$ w.r.t. the fulfilment of any $A_{AB\exists}$ formula, with $B$-nesting of $d_B(\cdot)$ less than or equal to $h$; by the previous bound on $j_{\rho_j}$, we have $j_{\rho'_j}(j \cdot W + 2)h+2$. 
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 $\rho$;
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 $(|W| + 2)$);
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.
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 $\overline{AABBEE}$ 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: \( u \leftarrow \text{New}(\text{Unravelling}(\mathcal{K}, w_0, h)) \)
3: while \( u.\text{hasMoreTracks}() \) do
4: \( \tilde{\rho} \leftarrow u.\text{getNextTrack}() \)
5: if \( \text{Check}(\mathcal{K}, h, \psi, \tilde{\rho}) = 0 \) then
6: return 0: “\( \mathcal{K}, \tilde{\rho} \not\models \psi \)”
7: return 1: “\( \mathcal{K} \models \psi \)”

\(< w_0 \ initial \ state \ of \ \mathcal{K} >\)

\(< \text{Counterexample \ found} \ \chi >\)

\(< \text{Model \ checking \ OK} \ \checkmark >\)
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

\[ HS_{\text{lin}} \cong LTL \]
\[ HS_{\text{ct}} \cong \text{finitary } CTL^* \]
\[ HS_{\text{st}} \cong CTL \]
\[ CTL^* \cong CTL \]


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.*  