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

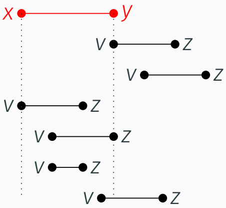
Point-based vs. interval-based model checking

- 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

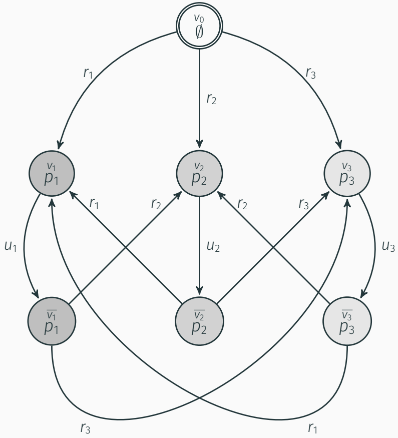
HS features a modality for any Allen ordering relation between pairs of intervals (except for equality)

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

- 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 ψ over a track ρ of a Kripke structure $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$:

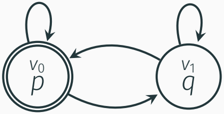
- $\mathcal{K}, \rho \models p$ iff $p \in \bigcap_{w \in \mathrm{states}(\rho)} \mu(w)$, for any letter $p \in \mathcal{AP}$ (homogeneity assumption);
- negation, disjunction, and conjunction are standard;
- $\mathcal{K}, \rho \models \langle A \rangle\, \psi$ iff there is a track ρ' s.t. $\mathrm{lst}(\rho)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

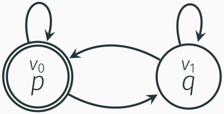
BE-descriptors



BE_2-descriptor for the track $\rho = v_0 v_1 v_0^4 v_1$
(only the part for prefixes is shown)

- $(v_0, \{v_0, v_1\}, v_1)$
  - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \emptyset, v_1)$

BE-descriptors



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

(only the part for prefixes is shown)

- $(v_0, \{v_0, v_1\}, v_1)$
  - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \{v_0, v_1\}, v_0)$
    - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \{v_1\}, v_0)$
    - $(v_0, \emptyset, v_1)$
  - $(v_0, \emptyset, v_1)$

- FACT 1: For any Kripke structure $\mathcal{K}$ the number of different descriptors of bounded depth k is finite
- FACT 2: Two tracks ρ and ρ' 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

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

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

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

Acta Informatica, 2016

Theorem

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

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Interval Temporal Logic MC: the Border Between Good and Bad HS Fragments.

In *IJCAR*, LNAI 9706, pages 389–405. Springer, 2016

The logic $A\overline{A}B\overline{BE}$

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

The logic $A\overline{A}B\overline{BE}$

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

Some fundamental facts:

- we can restrict our attention on prefixes (B_k-descriptors suffice)

The logic $A\overline{A}B\overline{BE}$

In this paper, we focus our attention on the HS fragment $A\overline{A}B\overline{BE}$, which is obtained from full HS ($A\overline{A}BE\overline{BE}$) 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

The logic $A\overline{A}B\overline{BE}$

In this paper, we focus our attention on the HS fragment $A\overline{A}B\overline{BE}$, which is obtained from full HS ($A\overline{A}BE\overline{BE}$) 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

The logic $A\overline{A}B\overline{BE}$

In this paper, we focus our attention on the HS fragment $A\overline{A}B\overline{BE}$, which is obtained from full HS ($A\overline{A}BE\overline{BE}$) 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

Prefix-bisimilarity

Definition (Prefix-bisimilarity)

The tracks ρ and ρ' are h-prefix bisimilar if the following conditions inductively hold:

- for $h = 0$:
  $\mathrm{fst}(\rho) = \mathrm{fst}(\rho')$, $\mathrm{lst}(\rho) = \mathrm{lst}(\rho')$, and $\mathrm{states}(\rho) = \mathrm{states}(\rho')$.
- for $h > 0$:
  ρ and ρ' are 0-prefix bisimilar and for each proper prefix ν of ρ (resp., proper prefix ν' of ρ'), there exists a proper prefix ν' of ρ' (resp., proper prefix ν of ρ) such that ν and ν' are $(h-1)$-prefix bisimilar.

- h-prefix bisimilarity is an equivalence relation over $\mathrm{Trk}_{\mathcal{K}}$.
- h-prefix bisimilarity propagates downwards.

h-prefix bisimilarity $\Rightarrow$ h-equivalence

Proposition

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

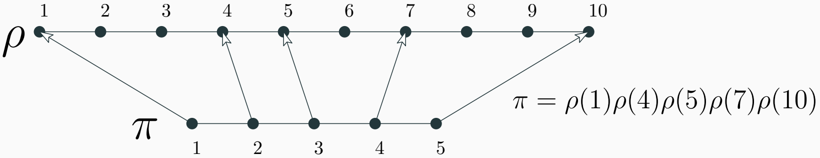
$$\mathcal{K}, \rho \models \psi \iff \mathcal{K}, \rho' \models \psi.$$

Induced track

Definition (Induced track)

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

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



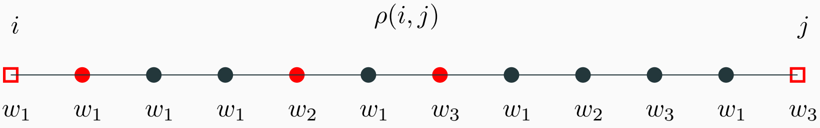
If π is induced by $\rho \Rightarrow \mathrm{fst}(\pi) = \mathrm{fst}(\rho)$, $\mathrm{lst}(\pi) = \mathrm{lst}(\rho)$, and $|\pi| \leq |\rho|$.

Prefix-skeleton sampling

Definition (Prefix-skeleton sampling)

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

- for $h = 1$: P_1 is the prefix-skeleton sampling of ρ;
- 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) ρ is such that $|P_h| \leq (|W| + 2)^h$.

Now what?

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

Now what?

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

1. we first compute the $(h+1)$-prefix sampling P_{h+1} of ρ;

Now what?

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

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

1. we first compute the $(h+1)$-prefix sampling P_{h+1} of ρ;
2. then for all the pairs of consecutive ρ-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. ρ' is just the ordered concatenation of all these tracks.

Now what?

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

1. we first compute the $(h+1)$-prefix sampling P_{h+1} of ρ;
2. then for all the pairs of consecutive ρ-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. ρ' is just the ordered concatenation of all these tracks.

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

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

Algorithm 1 $\texttt{ModCheck}(\mathcal{K}, \psi)$

$h \leftarrow \mathrm{d_B}(\psi)$

$u \leftarrow \mathit{New}(\texttt{Unravelling}(\mathcal{K}, w_0, h))$ ▷ *w_0 initial state of $\mathcal{K}$*

while $u.\texttt{hasMoreTracks}(\,)$ **do**

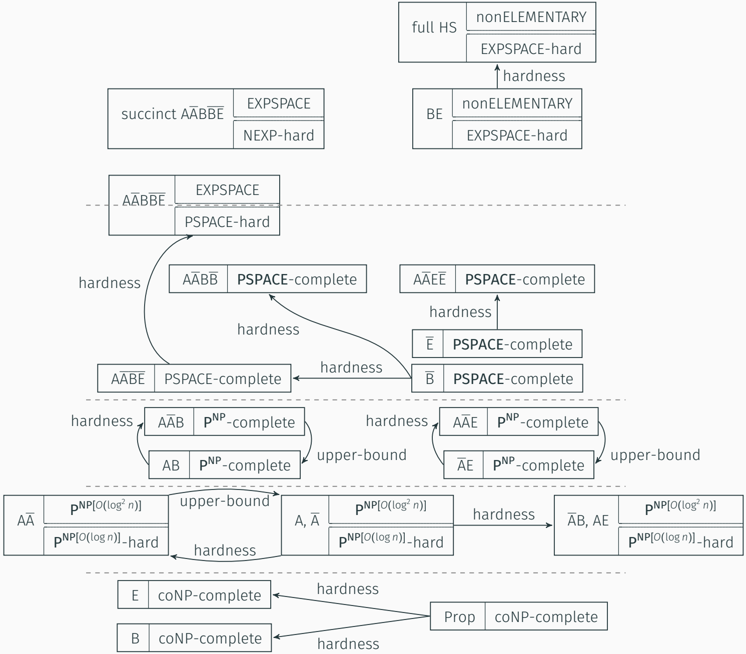
    $\tilde{\rho} \leftarrow u.\texttt{getNextTrack}(\,)$

    if $\texttt{Check}(\mathcal{K}, h, \psi, \tilde{\rho}) = 0$ **then**

        return 0: "$\mathcal{K}, \tilde{\rho} \not\models \psi$" ▷ *Counterexample found* ✗

return 1: "$\mathcal{K} \models \psi$" ▷ *Model checking OK* ✓

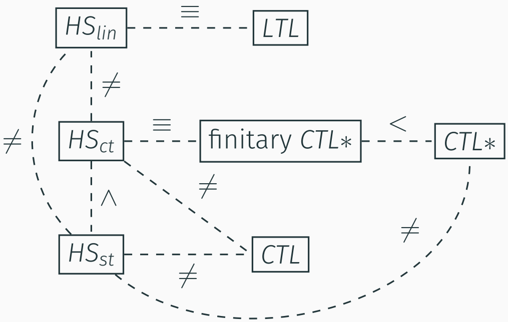
Complexity picture



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



References I

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Interval Temporal Logic MC: the Border Between Good and Bad HS Fragments.
In *IJCAR*, LNAI 9706, pages 389–405. Springer, 2016.

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Model Checking the Logic of Allen's Relations Meets and Started-by is P^{NP}-Complete.
In *GandALF*, 2016.

A. Molinari, A. Montanari, A. Murano, G. Perelli, and A. Peron.
Checking interval properties of computations.
Acta Informatica, 2016.

References II

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.
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*, pages 473–483, 2016.